Table of Contents

Table of Contents 1
NGFW 7.0.1 Руководство администратора 6
- Введение 7
  - Безопасность сети и защита от сетевых угроз 8
    - Межсетевое экранирование 9
    - Обнаружение и предотвращение вторжений 10
    - Защита от DOS-атак и сетевого флуда 11
    - Антивирусная проверка трафика 12
    - Проверка почтового трафика 13
    - Работа с внешними системами безопасности 14
    - Управление АСУ ТП 15
    - Настройка политик безопасности при помощи сценариев 16
  - Улучшение производительности и надежности интернета 17
    - Поддержка кластеризации и отказоустойчивости 18
    - FTP поверх HTTP 19
    - Поддержка нескольких провайдеров 20
    - Управление пропускной способностью 21
    - Поддержка WCCP 22
  - Управление трафиком и контроль доступа в интернет 23
    - Маршрутизация трафика и публикация ресурсов 24
    - Аутентификация и авторизация пользователей 25
    - Поддержка гостевого портала 26
    - Проксирование приложений 27
  - Журналы и отчеты 28
    - Журналы и отчеты(описание) 29
  - Другие функции 30
    - Ролевой доступ администраторов к элементам управления UserGate NGFW 31
    - Использование оповещений 32
    - Типы интерфейсов 33
    - DNS-фильтрация 34
    - Функция балансировщика нагрузки 35
  - Контент-фильтрация и контроль приложений 36
    - Интернет-фильтрация 37
    - Выборочная блокировка рекламы 38
    - Активация безопасного поиска 39
    - Блокировка приложений социальных сетей 40
    - Инжектирование кода на веб-страницы 41
    - Инспектирование SSL-трафика 42
    - VPN и веб-портал 43
  - Совместимость с аппаратными платформами 44
    - Совместимость версий UserGate NGFW с аппаратными платформами 45
- Первоначальная настройка 46
  - Описание 47
  - Требования к сетевому окружению 48
  - Развертывание виртуального образа 49
  - Подключение к UserGate NGFW 50
  - Автоматизация развертывания UserGate NGFW с помощью Cloud-init 52
- Лицензирование 54
  - Лицензирование (Описание) 55
- Настройка устройства 56

Общие настройки 57
Управление устройством 59
Кластеризация и отказоустойчивость 62
Управление доступом к консоли NGFW 66
Управление сертификатами 68
Расширение системного раздела 71
Системные утилиты 72
Настройка сети 73
Настройка зон 74
Настройка интерфейсов 76
Настройка шлюзов 81
Настройка DHCP 82
Настройка DNS 83
Виртуальные маршрутизаторы 84
WCCP 91
Пользователи и устройства 92
Пользователи и группы 93
Серверы аутентификации 94
Профили аутентификации 98
Настройка Captive-портала 99
Профили MFA (мультифакторной аутентификации) 102
Пользователи терминальных серверов 104
Прокси-агент для Windows 106
Управление гостевыми пользователями 107
Radius accounting 108
Агент аутентификации для Windows 109
Политики сети 110
Описание 111
Межсетевой экран 112
NAT и маршрутизация 114
Балансировка нагрузки 119
Пропускная способность 121
Политики безопасности 122
Общие сведения 123
Фильтрация контента 124
Веб-безопасность 126
Инспектирование туннелей 127
Инспектирование SSL 128
Инспектирование SSH 130
Система обнаружения и предотвращения вторжений 132
Сценарии 135
Работа с внешними ICAP-серверами 136
Защита почтового трафика 142
Защита от DoS атак 144
Глобальный портал 146
Описание 147
Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси 148
Веб-портал (SSL VPN) 150
Настройка VPN 152
Описание 153
VPN для защищенного соединения офисов (Site-to-Site VPN) 154
VPN для удаленного доступа клиентов (Remote access VPN) 159

IPsec over GRE 162
GRE over IPsec 163
Библиотеки элементов 164
Описание 165
Морфология 166
Сервисы 168
Группы сервисов 169
IP-адреса 170
Useragent браузеров 171
Типы контента 172
Списки URL 173
Календари 175
Полосы пропускания 176
Шаблоны страниц 177
Категории URL 178
Измененные категории URL 182
Приложения 183
Почтовые адреса 184
Номера телефонов 185
Профили СОВ 186
Профили оповещений 187
Профили Netflow 188
Профили LLDP 189
Профили SSL 190
Профили пересылки SSL 193
Интерфейс командной строки (CLI) 194
Общие положения 195
Общие положения (Описание) 196
Команды, доступные до первичной инициализации узла 198
Команды, доступные до первичной инициализации узла (Описание) 199
Первоначальная инициализация 200
Первоначальная инициализация (Описание) 201
Команды диагностики и мониторинга 202
Команды диагностики и мониторинга (Описание) 203
Режим конфигурации 209
Режим конфигурации (описание) 210
Настройка устройства 213
Настройка устройства (Описание) 214
Настройка кластеров 219
Настройка управления доступом к консоли NGFW 221
Настройка сертификатов 224
Настройка параметров устройства 226
Настройка телеметрии 228
Настройка прокси-сервера 229
Настройка параметров устройства 230
Настройки сети 232
Зоны 233
Интерфейсы 236
Шлюзы 245
DHCP 246
DNS-настройки 247
Настройка виртуальных маршрутизаторов 249

Настройка WCCP 258
Настройка правил с использованием UPL 260
Настройка правил с использованием UPL (Описание) 261
Настройка раздела Пользователи и устройства 262
Настройка групп пользователей 263
Настройки пользователей 264
Настройка серверов аутентификации 265
Настройка профилей аутентификации 268
Captive-портал 269
Настройка Captive-профилей 271
Настройка терминальных серверов 273
Настройка профилей MFA (мультифакторной аутентификации) 274
Настройка применения политик к пользователям 276
Настройка раздела Политики сети 277
Настройка правил межсетевого экрана 278
Настройка правил NAT и маршрутизации 280
Настройка балансировки нагрузки 285
Настройка правил пропускной способности 288
Настройка раздела Политики безопасности 290
Настройка фильтрации контента 291
Настройка веб-безопасности 293
Настройка правил инспектирования туннелей 295
Настройка инспектирования SSL 296
Настройка инспектирования SSH 298
Настройка СОВ 300
Настройка сценариев 302
Настройка правил защиты почтового трафика 305
Настройка правил ICAP 307
Настройка ICAP-серверов 309
Настройка правил защиты DoS 310
Настройка профилей DoS 312
Настройка глобального портала 313
Настройка веб-портала 314
Настройка правил reverse-прокси 315
Настройка серверов reverse-прокси 317
Настройка удалённого доступа (VPN) 318
Настройка серверных правил 319
Настройка клиентских правил 320
Настройка сетей VPN 321
Настройка профилей безопасности VPN 321
Настройка библиотек 324
Настройка библиотек (Описание) 325
Platform Management Controller Command Line Interface 339
Общие сведения 340
Работа с заводскими параметрами 341
Управление платформой 342
Управление настройками сети 343
Управление пользователями 345
Работа в режиме загрузчика 346
Дашборд 347
Приборная панель (DashBoard) 348
Диагностика и мониторинг 349

Мониторинг трафика 350
Маршруты 351
VPN 352
Веб-портал 353
Захват пакетов 354
Запросы в белый список 355
Трассировка правил 356
Ping 357
Traceroute 358
Запрос DNS 359
LLDP соседи 360
Статистика LLDP 361
Оповещения 362
Оповещения 363
SNMP 364
Журналы и отчеты 370
Журналы 371
Описание 372
Журнал событий 373
Журнал веб-доступа 374
Журнал трафика 375
Журнал СОВ 376
Журнал АСУ ТП 377
Журнал инспектирования SSH 378
История поиска 379
Поиск и фильтрация данных 380
Экспорт журналов 382
Отчеты 384
Описание 385
Шаблоны отчетов 386
Правила отчетов 387
Гостевой портал 388
Управление гостевыми пользователями 389
Помощь 390
Помощь(Описание) 391
ADMIN 392
ADMIN (описание) 393
Приложения 394
Установка сертификата локального удостоверяющего центра 395
Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0 401
Описание форматов журналов 404
Опции DHCP 416
Требования к сетевому окружению 418

Введение

Безопасность сети и защита от сетевых угроз

Межсетевое экранирование

Documentation: ☑
Version: 5.x, 6.1.9, 7.x, 7.0.1
Product: NGFW

Межсетевой экран нового поколения UserGate NGFW фильтрует трафик, проходящий через определенные протоколы (например, TCP, UDP, IP), тем самым обеспечивая защиту сети от хакерских атак и разнообразных типов вторжений, основанных на использовании данных протоколов.

Обнаружение и предотвращение вторжений

Version: 7.0.1, 6.1.9, 5.x

Documentation: ☑

Система обнаружения и предотвращения вторжений (СОВ) позволяет распознавать вредоносную активность внутри сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз в режиме реального времени, а также предоставление отчетов.

Администратор может создавать различные СОВ-профили (наборы сигнатур, релевантных для защиты определенных сервисов) и задавать правила СОВ, определяющие действия для выбранного типа трафика, который будет проверяться модулем СОВ в соответствии с назначенными профилями.

Защита от DOS-атак и сетевого флуда

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

NGFW позволяет задать параметры защиты каждой зоны сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP), указав порог уведомления - количество запросов с одного IP-адреса, после которого происходит запись в журнал - и порог отбрасывания пакетов - количество запросов, после которого пакеты отбрасываются с соответствующей записью в журнале.

Возможно настроить исключения, например, для зон, использующих IP-телефонию и поэтому отправляющих большое количество UDP-пакетов.

Антивирусная проверка трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0
Product: NGFW
Documentation:

Потоковый антивирус UserGate позволяет обеспечить антивирусную проверку трафика без ущерба для производительности и быстродействия сети. Модуль использует обширную базу сигнатур.

Проверка почтового трафика

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1, 7.1.0
Product: NGFW

NGFW способен обрабатывать транзитный почтовый трафик (SMTP(S), POP3(S)), анализируя его источник, а также содержание письма и вложений, что гарантирует надежную защиту от спама, pharming- и phishing- атак. NGFW также предоставляет возможность гибкой настройки фильтрации почтового трафика по группам пользователей.

Работа с внешними системами безопасности

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

Имеется возможность передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. Администратор может указать, какой трафик требуется передавать на ICAP, а также настроить работу с фермами серверов.

Управление АСУ ТП

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: ☑

В новой версии платформы появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП) и управления ей. Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий. Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

Настройка политик безопасности при помощи сценариев

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря автоматизации безопасности при помощи механизма сценариев (SOAR — Security Orchestration, Automation and Response).

Эта концепция находится на пике популярности и позволяет администратору создавать сценарии (запускаемые по плану или при обнаружении атаки), где прописываются автоматические действия в ответ на те или иные события. Такой подход обеспечивает гибкую настройку политик безопасности, сокращает участие человека благодаря автоматизации повторяющихся задач, а также дает возможность приоритизировать сценарии для скорейшей реакции на критичные угрозы.

Улучшение производительности и надежности интернета

Поддержка кластеризации и отказоустойчивости

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

UserGate NGFW поддерживает 2 типа кластеров: кластер конфигурации, позволяющий задать единые настройки узлам в рамках кластера, и кластер отказоустойчивости, призванный обеспечить бесперебойную работу сети. Кластер отказоустойчивости может работать в двух режимах: Актив-Актив и Актив-Пассив. Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другие.

FTP поверх HTTP

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Модуль FTP поверх HTTP позволяет обращаться к содержимому FTP-сервера из браузера пользователя.

Поддержка нескольких провайдеров

Documentation:

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

При подключении системы к нескольким провайдерам UserGate NGFW позволяет настроить для каждого из них свой шлюз для обеспечения доступа к интернету. Администратор также может настроить балансировку трафика между провайдерами, указав вес каждого шлюза, или указать один из шлюзов как основной с переключением на других провайдеров в случае недоступности основного шлюза.

Управление пропускной способностью

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Правила управления пропускной способностью служат для ограничения канала для определенных пользователей, хостов, сервисов или приложений.

Поддержка WCCP

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Поддержка протокола WCCP позволяет использовать NGFW в инфраструктуре с WCCP-серверами, например, маршрутизаторами Cisco.

Управление трафиком и контроль доступа в интернет

Маршрутизация трафика и публикация ресурсов

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1, 7.1.0

NGFW позволяет использовать как статическую, так и динамическую маршрутизацию. Динамическая маршрутизация осуществляется по протоколам OSPF и BGP, что позволяет использовать NGFW в сложной маршрутизируемой сети предприятия.

Администратор может создавать в системе правила NAT (для предоставления пользователям доступа в интернет), а также правила безопасной публикации внутренних ресурсов в интернет с использованием reverse-прокси для HTTP/HTTPS и DNAT для других протоколов.

Аутентификация и авторизация пользователей

Documentation: ☑

Product: UserGate NGFW

Version: 6.1.9, 7.0.1

Платформа поддерживает различные механизмы аутентификации пользователей: Captive-портал, Kerberos, NTLM, при этом учетные записи могут поступать из различных источников - LDAP, Active directory, FreeIPA, TACACS+, RADIUS, SAML IDP. Аутентификация SAML IDP, Kerberos или NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory на NGFW.

Администратор может настроить правила безопасности, ширину канала, правила межсетевого экранирования, контентной фильтрации и контроля приложений для отдельных пользователей, групп пользователей, а также всех известных или неизвестных пользователей. Дополнительно к этому продукт поддерживает применение правил безопасности к пользователям терминальных служб с помощью специальных агентов (Terminal Services Agents), а также использование агента авторизации для Windows-платформ.

Для обеспечения большей безопасности учетных записей рекомендуется использовать мультифакторную аутентификацию с помощью токенов TOTP (Time-based One Time Password Algorithm), SMS или электронной почты.

Поддержка гостевого портала

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1, 7.1.0

NGFW позволяет предоставлять пользователям временный доступ к сети, что актуально, например, для публичных Wi-Fi сетей. Профили могут быть как созданы администратором, так и зарегистрированы самими пользователями с подтверждением через email или SMS. Платформа позволяет указывать отдельные настройки безопасности для временных пользователей.

Проксирование приложений

Documentation:
Product: NGFW
Version: 6.1.9, 7.0.1, 7.1.0

Для пользователей, работающих с ОС Windows, можно настроить прокси-агент, позволяющий использовать возможности прокси приложениям, не умеющим работать с прокси-серверами. Прокси-агент также может быть использован для предоставления таким приложениям доступа в интернет в случаях, когда NGFW не является шлюзом по умолчанию.

Журналы и отчеты

Журналы и отчеты(описание)

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Платформа позволяет осуществлять мониторинг работы системы в режиме реального времени при помощи журналов событий, веб-доступа, СОВ и трафика. Для удобства анализа администратор может настроить автоматический экспорт журналов на сервера SSH, FTP и Syslog. С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Другие функции

Ролевой доступ администраторов к элементам управления UserGate NGFW

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

По умолчанию в системе существует один суперадминистратор, который может создавать учетные записи других администраторов и выдавать им права на просмотр и изменение различных разделов.

Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

Использование оповещений

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

UserGate NGFW поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается как управление с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps).

Помимо этого, система позволяет создавать профили оповещений, уведомляющие пользователей об определенных событиях по протоколам SMTP (email) и SMPP (SMS).

Типы интерфейсов

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

UserGate NGFW позволяет добавлять и настраивать тегированные VLAN-интерфейсы, а также объединять ряд физических интерфейсов в один логический агрегированный интерфейс (бонд) с использованием протокола LACP (link aggregation control protocol) для повышения пропускной способности или для отказоустойчивости канала. Помимо этого, существует возможность объединения интерфейсов в мост (bridge) для осуществления фильтрации трафика на уровне L2 без внесения изменений в сетевую инфраструктуру компании.

DNS-фильтрация

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

NGFW позволяет осуществлять настройку работы с DNS-серверами, а также настраивать сервис DNS-прокси, позволяющий перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Платформа также позволяет подключить фильтрацию DNS-запросов пользователей.

Функция балансировщика нагрузки

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

NGFW позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена для внутренних серверов, публикуемых в интернет (DNAT или reverse-прокси), внутренних серверов без публикации.

Контент-фильтрация и контроль приложений

Интернет-фильтрация

Documentation:
Version: 5.x, 6.1.9, 7.0.1, 7.1.0
Product: NGFW

Использование модуля интернет-фильтрации обеспечивает административный контроль за использованием интернета, загружаемыми данными. Модуль обеспечивает блокировку посещения потенциально опасных ресурсов, а также, когда это необходимо, сайтов, не связанных с работой.

Для анализа безопасности сайтов, запрашиваемых пользователями, используются репутационные сервисы, типы контента (фото, видео, тексты и др.), специальные морфологические словари, предоставляемые UserGate, а также черные и белые списки URL и Useragent, с помощью которых администратор может запретить или разрешить работу с определенным типом браузеров. NGFW предоставляет возможность создавать собственные черные и белые списки, словари, типы контента, морфологические словари и Useragent, применяя их как правила к пользователям и группам пользователей.

Выборочная блокировка рекламы

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation:

Даже безопасные сайты могут содержать нежелательные изображения на баннерах, содержимое которых не зависит от владельца ресурса. UserGate NGFW решает эту проблему, блокируя баннеры и защищая пользователей от негативного контента.

Активация безопасного поиска

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

NGFW позволяет принудительно активировать функцию безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. Такая защита позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту. Также можно заблокировать поисковые системы, в которых не реализована функция безопасного поиска.

Блокировка приложений социальных сетей

Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0
Documentation:

NGFW дает возможность блокировки игр и других приложений для наиболее популярных социальных сетей, таких, как Facebook, VK, Одноклассники. Администраторы могут разрешать использование социальных сетей в целом, при этом контролируя и ограничивая непродуктивные действия.

Инжектирование кода на веб-страницы

Version: 5.x, 6.1.9, 7.0.1, 7.1.0
Product: NGFW
Documentation:

Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователями. Эта возможность может быть использована для получения различных метрик, сокрытия некоторых элементов веб-страниц, а также показа рекламы или другой информации.

Инспектирование SSL-трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation:

UserGate NGFW позволяет фильтровать не только обычный, но и зашифрованный трафик (протоколы HTTPS, SMTPS, POP3S), дешифруя их при помощи технологии MITM (Man In The Middle) и подписывая доверенным корневым сертификатом с последующим шифрованием после анализа. Система позволяет настроить выборочную проверку трафика, например, не расшифровывать ресурсы категории «Финансы».

VPN и веб-портал

Version: 5.x, 6.1.9, 7.0.1

Documentation: ☑

VPN (Virtual Private Network) служит для того, чтобы настраивать виртуальные логические сети поверх других сетей, например, интернет. NGFW поддерживает два типа VPN-сетей: Remote Access VPN (модель клиент-сервер) и Site-to-Site VPN (модель сервер-сервер).

Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. NGFW поддерживает работу со стандартными клиентами большинства популярных операционных систем: Windows, Linux, Mac OS X, iOS, Android и других.

Веб-портал (SSL VPN) позволяет предоставить безопасный доступ сотрудникам компании к внутренним веб-ресурсам, серверам SSH и серверам терминальных служб без необходимости установки специального клиента VPN, используя только протокол HTTPS.

Совместимость с аппаратными платформами

Совместимость версий UserGate NGFW с аппаратными платформами

Documentation:
Product: NGFW
Version: 7.0.1

В таблице представлена матрица совместимости версий UserGate NGFW с моделями аппаратных платформ.

Важно!Доступность тех или иных версий продукта зависит от используемой аппаратной платформы. Перед обновлением обязательно сверьтесь с матрицей совместимости для вашего устройства.

Платформа	Версия UserGate NGFW								
	6.1.9	7.0.1	7.1.0	7.2.0	7.3.0	7.3.3	7.4.0	7.5.0	7.5.1
B50-B								•	•
C100	•					•		•	
C150		•	•	•	•	•	•	•	•
C151								•	•
D200	•	•	•	•	•	•	•	•	•
D250								•	•
D500	•	•	•	•	•	•	•	•	•
E1000	•	•	•	•	•	•	•	•	•
E1010					•	•	•	•	•
E3000	•	•	•	•	•	•	•	•	•
E3010					•	•	•	•	•
F8000	•	•	•	•	•	•	•	•	•
F8010					•	•	•	•	•
FG				•	•	•	•	•	•
X10									•

Первоначальная настройка

Описание

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Межсетевой экран UserGate поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины межсетевой экран UserGate поставляется с десятью Ethernet-интерфейсами. В случае поставки в виде ПАК — может содержать от 2 до 64 Ethernet-портов.

Требования к сетевому окружению

Documentation: ☑
Product: NGFW
Version: 7.0.1

Для корректной работы межсетевого экрана UserGate должен иметь доступ до следующих серверов, расположенных в сети интернет:

- Сервер регистрации — reg2.usergate.com, порты TCP 80, 443.
- Сервер обновления списков и ПО UserGate — updates.usergate.com, порты TCP 80, 443.

При создании кластера конфигурации необходимо обеспечить прохождение следующих протоколов между узлами:

- Обеспечение репликации настроек — порты TCP 4369, TCP 9000-9100.
- Сервис веб-консоли — TCP 8001.

Подробнее о требованиях сетевой доступности читайте в Приложение 4. Требования к сетевому окружению .

Развертывание виртуального образа

Documentation: ☑
Product: NGFW
Version: 7.0.1, 7.1.0

UserGate NGFW Virtual Appliance позволяет быстро развернуть виртуальную машину, с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox, и Qcow2 для систем виртуализации QEMU-KVM. Для Microsoft Hyper-v поставляется образ диска виртуальной машины.

ПримечаниеДля корректной работы виртуальной машины рекомендуется использовать минимум 12 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом, выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru.
Шаг 2. Импортируйте образ в свою систему виртуализации	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины.
Шаг 3. Настройте параметры виртуальной машины	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb и добавьте по 1Gb на каждые 100 пользователей.
Шаг 4. Важно! Самостоятельно добавьте дополнительный диск, нужного размера	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 200Gb или более. Рекомендованный размер — 300Gb или более. Для систем виртуализации QEMU-KVM: размер системной области, по умолчанию, составляет 8Гб. Система, при первом запуске, сама определит наличие дополнительного диска и расширит свои системные разделы. Команда для добавления диска размером 100 ГБ для систем QEMU-KVM: qemu-img create -f qcow2 -o preallocation=metadata,refcount_bits=16,lazy_refcounts=on,cluster_size=4K имя-вашего-диска.qcow2 100G
Шаг 5. Настройте виртуальные сети	UserGate поставляется с четырьмя интерфейсами, назначенными в зоны: • **Management** — первый интерфейс виртуальной машины. • **Trusted** — второй интерфейс виртуальной машины. • **Untrusted** — третий интерфейс виртуальной машины. • **DMZ** — четвертый интерфейс виртуальной машины.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину UserGate. Во время загрузки выберите **Support Menu** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага UserGate настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте.

Подключение к UserGate NGFW

Documentation:
Product: NGFW
Version: 7.0.1

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления.	**При наличии DHCP-сервера** Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate. После загрузки NGFW укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить NGFW. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Произвести первоначальную инициализацию в интерфейсе командной строки или подключиться к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом: https://NGFW_IP_address:8001. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI).
Шаг 2. Выбрать язык.	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль.	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Настроить зоны, IP-адреса интерфейсов, подключить UserGate в сеть предприятия.	В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). • Зона Untrusted (Internet). • Зона DMZ. • Зона Cluster. • Зона VPN for remote access. • Зона VPN for Site-to-Site. • Зона Tunnel inspection zone.
Шаг 5. Настроить шлюз в Интернет.	В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, подключенном в интернет, зона **Untrusted**. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов.
Шаг 6. Указать системные DNS-серверы.	В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Настройка DNS.
Шаг 7. Настроить время сервера.	В разделе **UserGate → Настройки → Настройка времени сервера** настроить синхронизацию времени с серверами NTP.
Шаг 8. Зарегистрировать NGFW.	Для регистрации продукта ввести ПИН-код и заполнить форму. Для активации системы необходим доступ NGFW в Интернет. Более подробно о лицензировании продукта читайте в главе Лицензирование.
Шаг 9. Создать правила NAT.	В разделе **NAT и Маршрутизация** создать необходимые правила NAT. Для доступа в интернет пользователей сети **Trusted** правило NAT уже создано: «**NAT from Trusted to Untrusted**». Подробно о правилах NAT читайте в главе NAT и маршрутизация.
Шаг 10. Создать правила межсетевого экрана.	В разделе **Межсетевой экран** создать необходимые правила межсетевого экрана. Для неограниченного доступа в интернет пользователей сети **Trusted** правило межсетевого экрана уже создано — «**Allow trusted to untrusted**», необходимо только включить его. Подробно о правилах межсетевого экрана читайте в главе Межсетевой экран.
Шаг 11. Создать дополнительных администраторов (опционально).	В разделе **Администраторы UserGate** создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).
Шаг 12. Настроить авторизацию пользователей (опционально).	В разделе **Пользователи и устройства** создать необходимые методы авторизации пользователей. Самый простой вариант - это создать локальных пользователей NGFW с заданными IP-адресами или использовать систему без идентификации пользователей (использовать пользователя **Any** во всех правилах). Для других вариантов авторизации пользователей смотрите главу Пользователи и устройства.
Шаг 13. Создать правила контентной фильтрации (опционально).	В разделе **Фильтрация контента** создать правила фильтрации HTTP(S). Более подробно о фильтрации контента читайте в главе Фильтрация контента.
Шаг 14. Создать правила веб-безопасности (опционально).	В разделе **Веб-безопасность** создать дополнительные правила защиты веб. Более подробно о веб-безопасности читайте в главе Веб-безопасность.
Шаг 15. Создать правила инспектирования SSL (опционально).	В разделе **Инспектирование SSL** создать правила для перехвата и расшифровывания HTTPS-трафика. Более подробно о дешифровании HTTPS читайте в главе Инспектирование SSL.

После выполнения вышеперечисленных действий NGFW готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

Автоматизация развертывания UserGate NGFW с помощью Cloud-init

Documentation:
Product: NGFW
Version: 7.0.1, 7.1.0

Cloud-init — индустриальный стандарт для кросс-платформенной инициализации виртуальных машин (инстансов) в облаках провайдеров. Межсетевой экран UserGate поддерживает возможность первоначальной настройки с помощью механизма Cloud-init. Настройка межсетевого экрана осуществляется с помощью двух модулей:

- Настройка с помощью команд CLI (файл с заголовком #utm-config). Возможно использовать все CLI-команды для полной настройки инстанса.
- Активация лицензии (файл с заголовком #utm-license).

Другие модули Cloud-init не поддерживаются.

Пример файла конфигурации с CLI командами (user-data):

```
#utm-config
#set password for initial Administrator (Admin). Obligatory comand.
password 123
#Set addresses and settings for network interfaces:
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
set network interface adapter port2 \
ip-addresses [ 172.16.8.9/24 ] \
enabled on \
zone "Untrusted"
set network interface adapter port3 \
ip-addresses [ 172.16.7.9/24 ] \
enabled on \
zone "DMZ"
#Create network gateway to Internet:
create network gateway \
ip 172.16.8.2 \
default on \
interface port2 \
virtual-router default \
enabled on
#Create firewall rule to allow traffic from Trusted to untrusted security zones:
create network-policy firewall \
position 1 upl-rule ALLOW \
src.zone = Trusted \
dst.zone = Untrusted \
enabled(true) \
name("Cloud-Init: Allow from Trusted to Untrusted")
```

В данный файл можно добавлять все доступные для администратора команды CLI. Подробно о CLI-командах смотрите в разделе Интерфейс командной строки (CLI).

— обозначает начало комментария, обратный слэш — переход на следующую строку.

Если необходимо активировать создаваемый инстанс, то это можно сделать через указание параметров для лицензирования в отдельном файле. Следует учитывать, что активация возможна только при наличии у инстанса доступа в сеть интернет. Пример содержимого файла для активации лицензии (vendor-data):

```
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email:  email@company.com
user_name: Alexander
last_name: Petrov
company: UserGate
country: Russia
region: Novosibirsk
```

Оба файла можно объединить в один файл, используя multipart формат:

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0
--//
Content-Type: text/utm-config; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config.txt"
#utm-config
password 123
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
set network interface adapter port2 \
ip-addresses [ 172.16.8.9/24 ] \
enabled on \
zone "Untrusted"
set network interface adapter port3 \
ip-addresses [ 172.16.7.9/24 ] \
enabled on \
zone "DMZ"
create network gateway \
ip 172.16.8.2 \
default on \
interface port2 \
virtual-router default \
enabled on
create network-policy firewall \
position 1 upl-rule ALLOW \
src.zone = Trusted \
dst.zone = Untrusted \
enabled(true) \
name("Cloud-Init: Allow from Trusted to Untrusted")
--//
Content-Type: text/utm-license; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license.txt"
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email:  email@company.com
user_name: Alexander
last_name: Petrov
company: UserGate
```

country: Russia
region: Novosibirsk
--//

Настройки могут быть переданы в NGFW:

1. Методами, реализуемыми облачными провайдер, например, у провайдера Digital Ocean при создании виртуальной машины (droplet) настройки необходимо вставить в опциональное поле **User data** (**Select additional options → User data**). Аналогичным образом настройки можно передать и у других поставщиков облачных услуг.

2. Через подключаемый iso-диск. Диск должен содержать файлы meta-data, user-data, vendor-data следующего содержимого:

meta-data: instance-id: vm1 user-data — с CLI-командами настройки инстанса:

```
#utm-config
#set password for initial Administrator (Admin). Obligatory comand.
password 123
#Set addresses and settings for network interfaces:
set network interface adapter port1 \
ip-addresses [ 172.16.6.9/24 ] \
enabled on \
zone "Trusted"
...
```

vendor-data — с информацией о лицензировании (опционально):

```
#utm-license
pin_code: UGN4-XXXX-YYYY-ZZZZ-AAAA
reg_name: UG-test
email: email@company.com
...
```

Для создания iso-диска в Linux можно использовать следующую утилиту:

```
mkisofs -joliet -rock -volid "cidata" -output nocloud.iso meta-data user-data vendor-data
```

Полученный iso-диск необходимо подключить к виртуальной машине UserGate. После успешной первой загрузки виртуальная машина получит все настройки, указанные для нее в созданных файлах.

Лицензирование

Лицензирование (Описание)

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1
Внимание!Лицензионные ключи версий 6 и 7 *несовместимы*! Перед обновлением до версии 7, необходимо запросить у менеджера ключ для 7-й версии.

Базовая лицензия

Лицензирование UserGate осуществляется по параметрам производительности платформы и зависит от:

- типа аппаратной платформы (для программно-аппаратного комплекса);
- количества поддерживаемых ядер виртуальной машины (для виртуального образа);

При попытке регистрации некорректного оборудования ключом с ограничением по производительности появится ошибка: **Введенный ПИН-код выписан для другого устройства UserGate, или конфигурация сервера не соответствует лицензированным характеристикам, например, увеличено число ядер процессора**.

Примечание Если виртуальная машина зарегистрирована корректным ключом, а в дальнейшем в неё будут добавлены дополнительные ядра, то активным в виртуальной машине будет только разрешенное лицензией количество ядер.

Базовая лицензия на продукт является бессрочной (без обновлений).

Дополнительно лицензируемые модули

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение: • обновлений ПО NGFW; • обновлений сигнатур системы обнаружения вторжений; • обновлений сигнатур приложений L7. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений необходимо продление лицензии.
Модуль Advanced Threat Protection (ATP)	Модуль ATP включает в себя следующие опции: • Годовая подписка на базу категорий сайтов UserGate URL filtering. • Годовая подписка на обновляемые списки URL (списки запрещенных сайтов Роскомнадзора, список phishing-сайтов, Белый список UserGate, Черный список UserGate итд.). • Годовая подписка на морфологические базы, предоставляемые компанией UserGate. • Годовая подписка на работу сервиса веб-безопасности (блокировка рекламы, история поиска, безопасный поиск, блокировка приложений социальных сетей). Модуль выписывается на 1 год, по истечении данного срока: • UserGate URL filtering перестает работать. • Фильтрация с помощью морфологии перестает работать. • Списки URL продолжают работать, но обновления будут недоступны. • Сервис веб-безопаности (блокировка рекламы, история поиска, безопасный поиск, блокировка приложений социальных сетей) перестает работать.
Модуль Mail security	Mail security включает в себя годовую подписку на проверку почтового трафика с помощью модуля антиспама UserGate.
Модуль Потоковый антивирус UserGate	Модуль включает в себя подписку на потоковый антивирус UserGate сроком на 1 год. По истечению данного срока антивирус UserGate перестает работать.
Модуль Cluster	Модуль включает лицензию на работу NGFW в режиме "кластер".

Порядок регистрации

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в **Дашборд**.	Нажать на пиктограмму **Дашборд** в правом верхнем углу.
Шаг 2. В разделе **Информация о лицензии** зарегистрировать продукт.	В разделе **Лицензия** нажать на ссылку **Нет лицензии**, ввести ПИН-код и заполнить регистрационную форму.

Настройка устройства

Общие настройки

Documentation: ☑
Version: 6.1.9, 7.0.1
Product: UserGate NGFW

Раздел **Общие настройки** определяет базовые установки NGFW:

Наименование	Описание
Часовой пояс	Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п.
Язык интерфейса по умолчанию	Язык, который будет использоваться по умолчанию в консоли.
Режим авторизации веб-консоли	Способ аутентификации пользователя (администратора) при входе в веб-консоль управления. Возможны следующие варианты: • **По имени и паролю**. Администратор должен ввести имя и пароль для получения доступа к веб-консоли. • **По X.509-сертификату**. Для авторизации по сертификату необходимо иметь сертификат пользователя, подписанный сертификатом удостоверяющего центра веб-консоли и установленный в браузер. При включении этого режима авторизации режим авторизации по имени и паролю отключается. Вернуть режим авторизации по имени и паролю можно с помощью команд CLI.
Профиль SSL для веб-консоли	Выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробно о профилях SSL смотрите в главе Профили SSL.
Профиль SSL для страниц блокировки/авторизации	Выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации Captive-портала. Подробно о профилях SSL смотрите в главе Профили SSL.
Настройка времени сервера	Настройка параметров установки точного времени. • **Использовать NTP** — использовать сервера NTP из указанного списка для синхронизации времени. • **Основной сервер NTP** — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org. • **Запасной сервер NTP** — адрес запасного сервера точного времени. • **Время на сервере** — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Модули	Позволяет настроить модули UserGate: • **HTTP(S)-прокси порт** — позволяет указать нестандартный (дополнительный) номер порта, который будет использоваться для подключения к встроенному прокси-серверу. По умолчанию используется порт TCP 8090; при изменении порт продолжает функционировать. **Важно!** Нельзя использовать следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100. • **Домен auth captive-портала** — служебный домен, который используется UserGate при авторизации пользователей через Captive-портал. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя auth.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **Домен logout captive-портала** — служебный домен, который используется пользователями UserGate для окончания сессии (logout). Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то разрешение адресов (resolving) настроено автоматически. По умолчанию используется имя logout.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **Домен страницы блокировки** — служебный домен, который используется для отображения страницы блокировки пользователям. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя block.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **FTP поверх HTTP** — включение или отключение модуля, позволяющего получать доступ к содержимому FTP-серверов из пользовательского браузера. Требуется явное указание прокси-сервера для протокола FTP в браузере пользователя. Администратор может ограничивать доступ к ресурсам FTP с помощь правил контентной фильтрации (только по условиям Пользователи и URL). • **FTP поверх HTTP домен** — служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. Необходимо, чтобы пользователи могли резолвить указанный здесь домен в IP-адрес интерфейса UserGate, к которому они подключены. Если в качестве DNS-сервера у пользователей указан IP-адрес сервера UserGate, то резолвинг настроен автоматически. По умолчанию используется имя ftpclient.captive, которое может быть изменено на другое доменное имя, принятое в организации. • **SNMP Engine ID** — каждое устройство UserGate имеет уникальный идентификатор SNMPv3 Engine ID. По умолчанию Engine ID генерируется на основании имени узла UserGate. При редактировании Engine ID необходимо указать длину, тип и значение идентификатора. Длина может быть определена как **фиксированная** (не более 8 байт) или **динамическая** (не более 27 байт). Фиксированная длина идентификатора применима только для типа **text**. Engine ID может быть сформирован в формате: ◦ **IPv4** (ip4). ◦ **IPv6** (ip6). ◦ **MAC-адрес** (mac). ◦ **Текст** (text). ◦ **Октеты** (octets). • **Пароль агентов терминального сервиса** — настройка пароля для подключения агентов авторизации терминальных серверов.
Настройка кэширования HTTP	Настройка кэша прокси-сервера: • **Включен**/**Выключен** — включение или отключение кэширования. • **Исключения кэширования** — список URL, которые не будут кэшироваться. • **Максимальный размер объекта**, Мбайт — объекты с размером более, чем указано в данной настройке, не будут кэшироваться. Рекомендуется оставить значение по умолчанию — 1 Мбайт. • **Размер RAM-кэша**, Мбайт — размер оперативной памяти, отведенный под кэширование. Не рекомендуется ставить более 20% от объема оперативной памяти системы. **Внимание!** Данный функционал нужен только при очень медленном интернет соединении. В обычных условиях его включение приводит к задержкам и лишнему использованию ресурсов.

Наименование	Описание
Log Analyzer	Настройки модуля LogAn: • **Локальный сервер**/**Внешний сервер**. Выберите внешний сервер, если у вас есть внешний сервер Log Analyzer, в противном случае выберите локальный сервер. • **Состояние** — показывает текущее состояние сервиса статистики. **Важно!** При указании внешнего LogAn обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.
Web-портал	Настройки для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (SSL VPN). Подробное описание данных настроек смотрите в главе Веб-портал.
Настройка PCAP	Настройка записи трафика при срабатывании сигнатур системы обнаружения вторжений. Настройка захвата пакетов: • **Без захвата**. • **Один пакет**. • **Предшествующие пакеты** (от 4 до 30 пакетов). • **Предшествующие и последующие пакеты** (предшествующие: от 4 до 30; последующие: от 2 до 15). **Важно!** Большой размер PCAP может вести к значительному замедлению обработки данных.
Настройка учета изменений	При включении данной опции и создания **Типов изменений** любое изменение в конфигурацию, вносимое администратором через веб-консоль, будет требовать указание типа изменения и описания вносимого изменения. В качестве типов изменения могут быть, например, указаны: • Распоряжение. • Приказ. • Регламентные работы, и т.д. Количество типов изменений не ограничено.
Агент UserGate Management Center	Настройки для подключения устройства к центральной консоли управления, позволяющей управлять парком устройств UserGate из одной точки; для подключения к UGMC используются порты TCP 2022 и TCP 9712. • **Включен**/**Выключен** — включение или отключение управления с помощью UGMC. • **Адрес UserGate Management Center** — адрес UGMC. • **Код устройства** — токен, требуемый для подключения к UGMC. UGMC может использоваться как источник обновления ПО и сигнатур.
Расписание скачивания обновлений	Настройки для управления скачиванием обновлений программного обеспечения UserGate (UGOS) и обновляемыми библиотеками, предоставляемыми по подписке (база категорий URL-фильтрации, СОВ, списки IP-адресов, URL, типов контента и другие). • **Обновления ПО** — настройка расписания проверки наличия новых обновлений UGOS и скачивания обновлений. • **Обновления библиотек** — настройка расписания проверки наличия новых обновлений библиотек и скачивания библиотек. Чекбокс **Единое расписание для всех обновлений** применяет расписание ко всем библиотекам, иначе для каждой библиотеки необходимо настроить собственное расписание. При задании расписания возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.

Управление устройством

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Раздел **Управление устройством** определяет следующие настройки NGFW:

- Кластеризация.
- Настройки диагностики.
- Операции с сервером.
- Резервное копирование.
- Экспорт и импорт настроек.

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UserGate при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• **Off** — ведение журналов диагностики отключено. • **Error** — журналировать только ошибки работы сервера. • **Warning** — журналировать только ошибки и предупреждения. • **Info** — журналировать только ошибки, предупреждения и дополнительную информацию. • **Debug** — максимум детализации. Рекомендуется установить значение параметра **Детализация диагностики** в **Error** (только ошибки) или **Off** (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность NGFW.
Журналы диагностики	• **Скачать журналы** — скачать диагностические журналы для передачи их в службу поддержки UserGate; для скачивания доступны журналы веб-консоли и/или журналы системы. Для скачивания необходимо выбрать журналы и нажать **Начать архивирование журналов**; после архивирования журналы будут доступны для скачивания (кнопка **Скачать**). • **Очистить журналы** — очистить содержимое журналов.
Удаленный помощник	• **Включено**/**Отключено** — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к NGFW для диагностики и решения проблем. Для успешной активации удаленного помощника UserGate должен иметь доступ к серверу удаленного помощника по протоколу SSH. • **Идентификатор удаленного помощника** — полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • **Токен удаленного помощника** — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• **Перезагрузить** — перезагрузка NGFW. • **Выключить** — выключение NGFW.
Обновления	Выбор канала обновлений ПО NGFW • **Стабильные** — проверка наличия стабильных обновлений ПО. • **Бета** — проверка наличия экспериментальных обновлений.

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления NGFW в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе Лицензирование UserGate). При наличии обновлений в разделе **Управление устройством → Операции с сервером** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя NGFW.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния NGFW, как это описано в разделе Системные утилиты. Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажать на ссылку **Установить сейчас**. Система установит скачанные обновления, по окончании установки NGFW будет перезагружен.

Управление резервным копированием

Данный раздел позволяет управлять резервным копированием NGFW: настройка правил экспорта конфигурации, создание резервной копии, восстановление NGFW.

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе **Управление устройством → Управление резервным копированием** нажать **Создание резервной копии**. Система сохранит текущие настройки сервера под следующим именем: backup_PRODUCT_NODE-NAME_DATE.gpg, где *PRODUCT* — тип продукта: NGFW, LogAn, MC; *NODE-NAME* — имя узла UserGate; *DATE* — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки **Остановить**. Запись о создании резервной копии отобразится в журнале событий устройства.

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе **Управление устройством → Управление резервным копированием** нажать **Восстановление из резервной копии** и указать путь к ранее созданному файлу настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства.

Дополнительно администратор может настроить сохранение файлов на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе **Управление устройством → Управление резервным копированием** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль**/**Повторите пароль** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки. В случае использование SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать **Настроить SSH-ключ** и указать **Сгенерировать ключи** или **Импортировать ключ**. **Важно!** При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей /**home**/**user**/**.ssh**/ в файле **authorized_keys**. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка **Проверить соединение**); при проверке соединения fingerprint помещается в known_hosts, без проверки файлы не будут отправляться. **Важно!** Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Экспорт и импорт настроек

Администратор имеет возможность сохранить текущие настройки NGFW в файл и впоследствии восстановить эти настройки на этом же или другом NGFW. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

ПримечаниеЭкспорт настроек является кластерной функцией, т.е. экспортируется конфигурация всех узлов кластера. При импорте конфигурации будет предложен выбор нужного узла кластера для восстановления.
ПримечаниеЭкспорт/импорт настроек не восстанавливает состояние кластера и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать UserGate с помощью имеющегося ПИН-кода и заново создать кластер, если это необходимо.
ПримечаниеВ случае использования мультифакторной аутентификации через TOTP, ключи TOTP не сохраняются; необходима повторная инициализация.

Имеется возможность сделать экспорт всех настроек (за исключением вышеперечисленных), либо сделать только экспорт сетевых настроек. При экспорте только сетевых настроек сохраняется информация о:

- Настройки DNS.
- Настройки DHCP.
- Настройки всех интерфейсов, включая туннели.
- Настройки шлюзов.
- Настройки виртуальных маршрутизаторов (VRF).
- Настройки WCCP.
- Настройки зон.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажать на ссылку **Экспорт → Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит текущие настройки сервера под именем utm-utmcore@nodename_version-YYYYMMDD_HHMMSS.bin, где nodename — имя NGFW version — версия UGOS YYYYMMDD_HHMMSS — время выгрузки настроек в часовом поясе UTC, например: utm-utmcore@heashostatot_6.1.1.10462R-1_20210511_095942

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе **Управление устройством → Экспорт и импорт настроек** нажать **Импорт** и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен.

ПримечаниеДля корректного импорта правил, использующих обновляемые списки UserGate (приложения, категории URL и т.п.), необходимо наличие лицензии на модули SU и ATP, а также загруженных списков UserGate.

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе **Управление устройством → Экспорт и импорт настроек** нажать кнопку **Добавить**, указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера: • **Тип сервера** — FTP или SSH. • **Адрес сервера** — IP-адрес сервера. • **Порт** — порт сервера. • **Логин** — учетная запись на удаленном сервере. • **Пароль**/**Подтверждение пароля** — пароль учетной записи. • **Путь на сервере** — путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.

Кластеризация и отказоустойчивость

Technology: Clustering and HA
Version: 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

NGFW поддерживает 2 типа кластеров:

1. **Кластер конфигурации**. Узлы, объединенные в кластер конфигурации, поддерживают единые настройки в рамках кластера.
2. **Кластер отказоустойчивости**. До 4-х узлов кластера конфигурации могут быть объединены в кластер отказоустойчивости, поддерживающий работу в режиме Актив-Актив или Актив-Пассив. Возможно собрать несколько кластеров отказоустойчивости.

ВажноВ кластере поддерживается работа разных версий виртуального исполнения и моделей аппаратных устройств UserGate, а так же смешанные кластера для аппаратных и виртуальных исполнений.

Кластер конфигурации

Ряд настроек уникален для каждого из узлов кластера, например, настройка сетевых интерфейсов и IP-адресация. Список уникальных настроек:

Наименование	Описание
Настройки, уникальные для каждого узла	Настройки Log Analyzer. Настройки диагностики. Настройки интерфейсов. Настройки шлюзов. Настройки DHCP. Маршруты. Настройки OSPF. Настройки BGP.

Для создания кластера конфигурации необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выполнить первоначальную настройку на первом узле кластера.	Смотрите главу Первоначальная настройка.
Шаг 2. Настроить на первом узле кластера зону, через интерфейсы которой будет выполняться репликация кластера.	В разделе **Зоны** создать выделенную зону для репликации настроек кластера или использовать существующую (**Cluster**). В настройках зоны разрешить следующие сервисы: • Консоль администрирования • Кластер Не используйте для репликации зоны, интерфейсы которых подключены к недоверенным сетям, например, к интернету.
Шаг 3. Указать IP-адрес, который будет использоваться для связи с другими узлами кластера.	В разделе **Управление устройством** в окне **Кластер конфигурации** выбрать текущий узел кластера и нажать на кнопку **Редактировать.** Указать IP-адрес интерфейса, входящего в зону, настроенную на шаге 2.
Шаг 4. Сгенерировать **Секретный код** на первом узле кластера.	В разделе **Управление устройством** нажать на кнопку **Сгенерировать секретный код.** Полученный код скопировать в буфер обмена. Данный секретный код необходим для одноразовой авторизации второго узла при добавлении его в кластер.
Шаг 5. Подключить второй узел в кластер.	Подключиться к веб-консоли второго узла кластера, выбрать язык установки. Указать интерфейс, который будет использован для подключения к первому узлу кластера и назначить ему IP-адрес. Оба узла кластера должны находиться в одной подсети, например, интерфейсам eth2 обоих узлов назначены IP-адреса 192.168.100.5/24 и 192.168.100.6/24. В противном случае необходимо указать IP-адрес шлюза, через который будет доступен первый узел кластера. Указать IP-адрес первого узла, настроенный на шаге 3, вставить секретный код и нажать на кнопку **Подключить**. Если IP-адреса кластера, настроенные на шаге 2, назначены корректно, то второй узел будет добавлен в кластер и все настройки первого кластера реплицируются на второй. Состояние узлов кластера конфигурации можно определить по цветовой индикации напротив названия узла UserGate в разделе **UserGate → Управление устройством → Кластер конфигурации**: • **Зелёный**: узел доступен. • **Жёлтый**: происходит синхронизация между узлами кластера конфигурации. • **Красный**: связь до узла потеряна, узел недоступен.
Шаг 6. Назначить зоны интерфейсам второго узла.	В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу корректную зону. Зоны и их настройки получены в результате репликации данных с первого узла кластера.
Шаг 7. Настроить параметры, индивидуальные для каждого узла кластера (опционально).	Настроить шлюзы, маршруты, параметры OSPF, BGP, индивидуальные для каждого из узлов.

До четырех узлов кластера конфигурации можно объединить в отказоустойчивый кластер. Самих кластеров отказоустойчивости может быть несколько, например, в кластер конфигурации добавлены узлы A, B, C и D на основе которых создано 2 кластера отказоустойчивости - A-B и C-D.

Поддерживаются 2 режима кластера отказоустойчивости - **Актив-Актив** и **Актив-Пассив**. Состояние узлов кластера можно определить по цвету индикатора около названия узла UserGate в разделе **UserGate → Управление устройством → Кластеры отказоустойчивости** :

- **Красный**: нет связи с соседними узлами конфигурации.
- **Жёлтый**: кластер отказоустойчивости не запущен на узле.

Отсутствие индикатора напротив названия узла говорит о доступности узла кластера.

Кластер отказоустойчивости Актив-Пассив

В режиме Актив-Пассив один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных. На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии.

ПримечаниеРежим Актив-Пассив поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой, за исключением сессий, использующих прокси сервер, например, трафик HTTP/S.

При переходе роли мастер на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети(Таймеры: Adver - 1сек, MasterDown - 3сек), например, если он выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в интернет (смотрите раздел Настройка шлюзов), и доступ в интернет отсутствует через все имеющиеся шлюзы.

  Если хост, указанный в свойствах проверки сети, недоступен на всех узлах кластера, то кластер отказоустойчивости будет отключен.
- Сбой в работе ПО NGFW.

Отключение одного или нескольких сетевых интерфейсов, на которых назначены виртуальные IP-адреса понижает приоритет узла, но не обязательно приведет к изменению роли сервера. Переход на запасной узел произойдет, если приоритет запасного узла окажется выше, чем мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла равен 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, у которого отсутствует физическое подключение к сети. Соответственно, для кластера отказоустойчивости, состоящего из двух узлов, при пропадании физического подключения к сети одного интерфейса на мастер-узле, роль мастера переместится на запасной сервер, если на запасном сервере все кластерные интерфейсы подключены к сети (приоритет мастер-сервера будет равен 248, приоритет резервного - 249). При восстановлении физического подключения на первоначальном мастер-узле роль мастера вернется обратно на него, поскольку его приоритет вернется в значение 250 (справедливо для случая если виртуальные адреса сконфигурированы на двух и более интерфейсах. Если на одном, то роль мастера не возвращается).

Отключение одного или нескольких кластерных сетевых интерфейсов **на запасном узле**, понижает приоритет узла, тем не менее данный запасной узел может стать мастер-узлом при безусловном переходе роли, или в случае, когда приоритет мастер узла станет меньше, чем приоритет данного запасного узла.

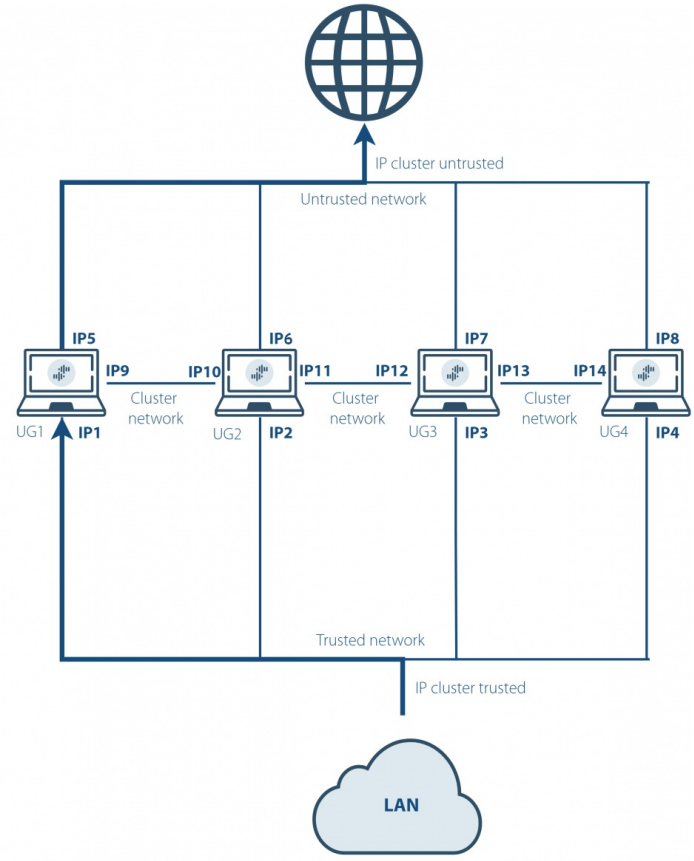
ПримечаниеЕсли кластерные IP-адреса назначены VLAN-интерфейсам, то отсутствие подключения на физическом интерфейсе будет трактоваться кластером отказоустойчивости как потеря соединения на всех VLAN-интерфейсах, созданных на данном физическом интерфейсе.

ПримечаниеДля уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, NGFW посылают служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. Пакет GARP отсылается NGFW каждую минуту и при переезде роли мастера на запасной узел.

Ниже представлена пример сетевой диаграммы отказоустойчивого кластера в режиме Актив-Пассив. Интерфейсы настроены следующим образом:

- **Зона Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Untrusted**: IP5, IP6, IP7, IP8 и IP cluster (Untrusted).
- **Зона Cluster**: IP9, IP10, IP11, IP12, IP13, IP14. Интерфейсы в зоне Cluster используются для репликации настроек.

Оба кластерных IP-адреса находятся на узле UG1. Если узел UG1 становится недоступным, то оба кластерных IP-адреса перейдут на следующий узел, который станет мастер узлом, например, UG2.



Отказоустойчивый кластер в режиме Актив-Пассив

Кластер отказоустойчивости Актив-Актив

В режиме Актив-Актив один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера. На каждом из узлов кластера выбираются сетевые интерфейсы, которым администратор назначает виртуальные IP-адреса. Между этими интерфейсами передаются VRRP-объявления (ADVERTISEMENT) — сообщения, с помощью которых узлы обмениваются информацией о своем состоянии.

Виртуальные IP-адреса всегда находятся на интерфейсах Мастер-узла, поэтому Мастер-узел получает ARP-запросы клиентов и отвечает на них, последовательно отдавая MAC-адреса всех узлов отказоустойчивого кластера, обеспечивая равномерное распределение трафика на все узлы кластера, учитывая при этом необходимость неразрывности пользовательских сессий.

ПримечаниеБалансировка трафика будет работать только в одном широковещательном домене. Для примера, если для клиентов VIP-адрес будет шлюзом по умолчанию, то балансировка трафика будет работать, так как разным клиентам будут поочередно отдаваться разные MAC-адреса узлов, но в случае, если между NGFW и клиентами находится маршрутизатор, то балансировка работать не будет, так как ARP-запрос на VIP-адрес пошлет только сам маршрутизатор и ему вернется MAC-адрес только одного из узлов, через который он и отправит весь трафик.
ПримечаниеРежим Актив-Актив поддерживает синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой, за исключением сессий, использующих прокси сервер, например, трафик HTTP/S.

При переходе роли мастер на резервный сервер на него переносятся **все** виртуальные IP-адреса **всех** кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети(Таймеры: Adver - 1сек, MasterDown - 3сек), например, если он выключен или отсутствует сетевая доступность узлов.

- На узле настроена проверка доступа в интернет (смотрите раздел Настройка шлюзов), и доступ в интернет отсутствует через все имеющиеся шлюзы.
- Сбой в работе ПО NGFW.

Отключение одного или нескольких сетевых интерфейсов **мастер-узла**, на которых назначены виртуальные IP-адреса, понижает приоритет узла, но не обязательно приведет к изменению роли сервера. Переход на запасной узел произойдет, если приоритет запасного узла окажется выше, чем мастер-узла. По умолчанию приоритет узла, назначенный мастер-узлу, равен 250, приоритет резервного узла равен 249. Приоритет узла уменьшается на 2 для каждого кластерного интерфейса, у которого отсутствует физическое подключение к сети. Соответственно, для кластера отказоустойчивости, состоящего из двух узлов, при пропадании физического подключения к сети одного интерфейса на мастер-узле, роль мастера переместится на запасной сервер, если на запасном сервере все кластерные интерфейсы подключены к сети (приоритет мастер-сервера будет равен 248, приоритет резервного - 249). При восстановлении физического подключения на первоначальном мастер-узле роль мастера вернется обратно на него, поскольку его приоритет вернется в значение 250.

Отключение одного или нескольких кластерных сетевых интерфейсов **на запасном узле**, понижает приоритет узла, а также исключает данный узел из балансировки трафика. Тем не менее данный запасной узел может стать мастер-узлом при безусловном переходе роли, или в случае, когда приоритет мастер узла станет меньше, чем приоритет данного запасного узла.

ПримечаниеЕсли кластерные IP-адреса назначены VLAN-интерфейсам, то отсутствие подключения на физическом интерфейсе будет трактоваться кластером отказоустойчивости как потеря соединения на всех VLAN-интерфейсах, созданных на данном физическом интерфейсе.

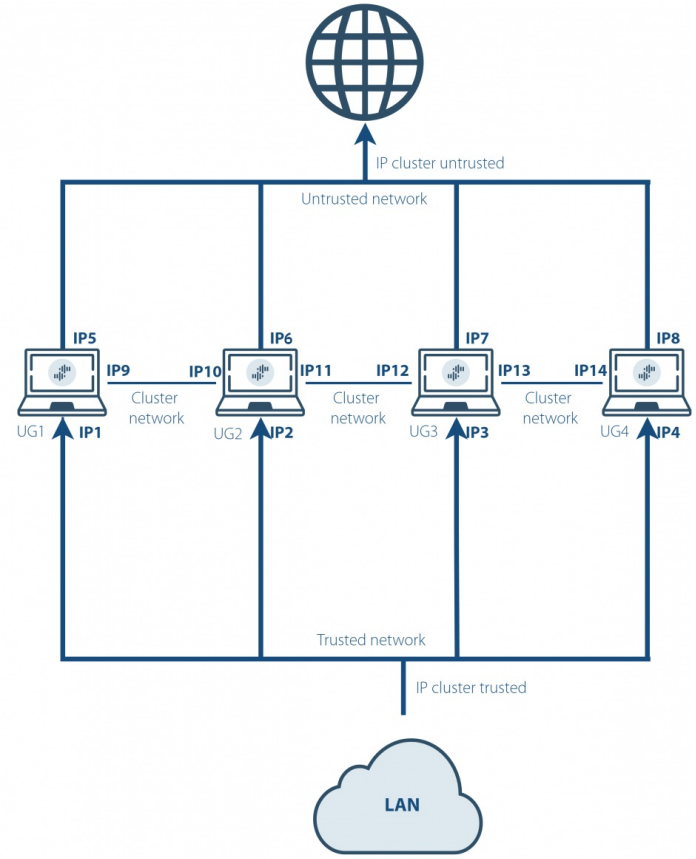
Примечание

Для уменьшения времени, требуемого сетевому оборудованию для перевода трафика на запасной узел при переключении, NGFW посылают служебное оповещение GARP (Gratuitous ARP), извещающий сетевое оборудование о смене MAC-адресов для всех виртуальных IP-адресов. В режиме Актив-Актив пакет GARP отсылается NGFW только при переходе роли мастера на запасной узел.

Ниже представлен пример сетевой диаграммы отказоустойчивого кластера в режиме **Актив-Актив**. Интерфейсы настроены следующим образом:

- **Зона Trusted**: IP1, IP2, IP3, IP4 и IP cluster (Trusted).
- **Зона Untrusted**: IP5, IP6, IP7, IP8 и IP cluster (Untrusted).
- **Зона Cluster**: IP9, IP10, IP11, IP12, IP13, IP14. Интерфейсы в зоне Cluster используются для репликации настроек.

Оба кластерных IP-адреса находятся на узле UG1. Если узел UG1 становится недоступным, то оба кластерных IP-адреса перейдут на следующий сервер, который станет мастер сервером, например, UG2.



Отказоустойчивый кластер в режиме Актив-Актив

ПримечаниеДля корректной обработки трафика необходимо, чтобы обратный трафик от сервера к клиенту вернулся через тот же узел NGFW, через который он был инициирован от клиента, то есть, чтобы сессия пользователя всегда проходила через один и тот же узел кластера. Самое простое решение данной задачи - это использование NAT из сети клиента в сеть сервера (NAT из Trusted в Untrusted).

Для создания отказоустойчивого кластера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать кластер конфигурации.	Создать кластер конфигурации, как это описано на предыдущем шаге.
Шаг 2. Настроить зоны, интерфейсы которых будут участвовать в отказоустойчивом кластере.	В разделе **Зоны** следует разрешить сервис VRRP для всех зон, где планируется добавлять кластерный виртуальный IP-адрес (зоны **Trusted** и **Untrusted** на диаграммах выше).
Шаг 3. Создать кластер отказоустойчивости.	В разделе **Управление устройством → Кластер отказоустойчивости** нажать на кнопку **Добавить** и указать параметры кластера отказоустойчивости.
Шаг 4. Указать виртуальный IP-адрес для хостов auth.captive, logout.captive, block.captive, ftpclient.captive.	Если предполагается использовать авторизацию с помощью Captive-портала, то необходимо, чтобы системные имена хостов auth.captive и logout.captive, которые используются процедурами авторизации в Captive, резолвились в IP-адрес, назначенный в качестве кластерного виртуального адреса. Более детально эти параметры описаны в разделе Общие настройки.

Параметры отказоустойчивого кластера:

Наименование	Описание
Включено	Включение/отключение отказоустойчивого кластера.
Название	Название отказоустойчивого кластера.
Описание	Описание отказоустойчивого кластера.
Режим кластера	Режим отказоустойчивого кластера: • **Актив-Актив** — нагрузка распределяется на все узлы кластера. • **Актив-Пассив** — нагрузка идет на Мастер-узел и переключается на запасной узел в случае недоступности Мастер-узла.
Синхронизировать сессии	Включает режим синхронизации пользовательских сессий между всеми узлами, входящими в кластер отказоустойчивости. Включение данной опции делает переключение пользователей с одного устройства на другое прозрачным для пользователей, но добавляет существенную нагрузку на платформу NGFW. Имеет смысл только для режима кластера Актив-Пассив.
Мультикаст идентификатор кластера	В одном кластере конфигурации может быть создано несколько кластеров отказоустойчивости. Для синхронизации сессий используется определенный мультикастовый адрес, определяемый данным параметром. Для каждой группы кластеров отказоустойчивости, в которой должна поддерживаться синхронизация сессий, требуется установить уникальный идентификатор.
Идентификатор виртуального роутера (VRID)	Идентификатор виртуального роутера должен быть уникален для каждого VRRP-кластера в локальной сети. Если в сети не присутствуют сторонние кластеры VRRP, то рекомендуется оставить значение по умолчанию.
Узлы	Выбираются узлы кластера конфигурации для объединения их в кластер отказоустойчивости. Здесь же можно назначить роль Мастер-сервера одному из выбранных узлов.
Виртуальные IP-адреса	Назначаются виртуальные IP-адреса и их соответствие интерфейсам узлов кластера.

Управление доступом к консоли NGFW

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1
Product: NGFW

Доступ к веб-консоли NGFW регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети. Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

ПримечаниеПри первоначальной настройке NGFW создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора.	В разделе **Администраторы → Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора.	В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант: • **Добавить локального администратора** — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • **Добавить пользователя LDAP** — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • **Добавить группу LDAP** — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • **Добавить администратора с профилем авторизации** - создать пользователя, назначить созданный ранее профиль администратора и профиль авторизации (необходимы корректно настроенные серверы авторизации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Разрешения для API	Список объектов, доступных для делегирования доступа при работе через программный интерфейс (API). Объекты описаны документации API. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для веб-консоли	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Разрешения для CLI	Позволяет разрешить доступ к CLI. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.

Администратор NGFW может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей.	В разделе **Администраторы → Администраторы** нажать кнопку **Настроить**.
Шаг 2. Заполнить необходимые поля.	Указать значения следующих полей: • **Сложный пароль** — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как — минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • **Число неверных попыток аутентификации** — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на **Время блокировки**. • **Время блокировки** — время, на которое блокируется учетная запись.

ПримечаниеДополнительные параметры защиты учетной записи администратора применимы только к локальным учетным записям. Если в качестве администратора устройства выбирается учетная запись из внешнего каталога (например, LDAP), то параметры защиты для такой учетной записи определяются этим внешним каталогом.

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8001).

ПримечаниеНе рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе **Контроль доступа** разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе Настройка зон.

Дополнительной мерой усиления безопасности доступа к консоли может быть включение режима авторизации администраторов с использованием сертификатов.

Для включения данного режима необходимо выполнить следующие действия (в качестве примера используется утилита openssl):

Наименование	Описание
Шаг 1. Создать учетные записи дополнительных администраторов.	Произвести настройку, как это описано ранее в этой главе, например, создать учетную запись администратора с именем Administrator54.
Шаг 2. Создать или импортировать существующий сертификат типа УЦ авторизации веб-консоли.	Создать или импортировать существующий сертификат удостоверяющего центра (достаточно только публичного ключа) в соответствии с главой Управление сертификатами. **Важно!** Существующий сертификат удостоверяющего центра — сертификат, которым непосредственно подписаны сертификаты администраторов, а не корневой. Например, для создания УЦ с помощью утилиты openssl требуется выполнить команды: openssl req -x509 -subj '/C=RU/ST=Moscow/O= MyCompany /CN=ca.mycompany.com' -newkey rsa:2048 -keyout ca-key.pem -out ca.pem -nodes openssl rsa -in ca-key.pem -out ca-key.pem В файле ca-key.pem будет находиться приватный ключ сертификата, в ca.pem — публичный ключ. Импортировать публичный ключ в UserGate.
Шаг 3. Создать сертификаты для учетных записей администраторов.	С помощью средств сторонних утилит (например, openssl) создать сертификаты для каждого из администраторов. Необходимо, чтобы поле сертификата **Common name** в точности совпадало с именем учетной записи администратора, как она была создана в UserGate. Для openssl и пользователя Administrator54 команды будут следующими: openssl req -subj '/C=RU/ST=Moscow/O= MyCompany /CN=Administrator54' -out admin.csr -newkey rsa:2048 -keyout admin-key.pem -nodes
Шаг 4. Подписать сертификаты администраторов, созданным на шаге 2 сертификатом удостоверяющего центра.	С помощью средств сторонних утилит (например, openssl) подписать сертификаты администраторов сертификатом удостоверяющего центра веб-консоли. Для openssl команды будут следующими: openssl x509 -req -days 9999 -CA ca.pem -CAkey ca-key.pem -set_serial 1 -in admin.csr -out admin.pem openssl pkcs12 -export -in admin.pem -inkey admin-key.pem -out admin.p12 -name 'Administrator54 client certificate' Файл admin.p12 содержит подписанный сертификат администратора.
Шаг 5. Добавить подписанные сертификаты в ОС, с которой администраторы будут авторизоваться в веб-консоль.	Добавить подписанные сертификаты администраторов (admin.p12 в нашем примере) в ОС (или в браузер Firefox, если он используется для доступа к консоли), с которой администраторы будут авторизоваться в веб-консоль. Более подробно смотрите руководство по используемой вами ОС.
Шаг 6. Переключите режим авторизации веб-консоли в авторизацию по сертификатам x.509.	В разделе **Настройки** поменяйте **Режим авторизации веб-консоли** на **По X.509 сертификату**.

ПримечаниеПереключить режим авторизации веб-консоли можно с помощью команд CLI.

В разделе **Администраторы → Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования NGFW. При необходимости любую из сессий администраторов можно сбросить (закрыть).

Управление сертификатами

Version: 5.x, 6.1.9, 7.0.1
Documentation: ☑

Общие сведения

UserGate использует защищенный протокол HTTPS для управления устройством, может перехватывать и дешифровать транзитный трафик пользователей, передаваемый по протоколу SSL (HTTPS, SMTPS, POP3S), а также может производить авторизацию администраторов в веб-консоль на основе их сертификатов.

Для выполнения данных функций NGFW использует различные типы сертификатов:

Наименование	Описание
SSL веб-консоли	Используется для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW.
SSL Captive-портала	Используется для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. Этот сертификат должен быть выпущен со следующими параметрами: • Subject name — значение, установленное для домена **Домен Auth captive-портала**, определенного на странице **Настройки**. • Alternative names — необходимо указать все домены, для которых используется данный сертификат, как они заданы на странице **Настройки**: ◦ домен Auth captive-портала. ◦ домен Logout captive-портала. ◦ домен страницы блокировки. ◦ домен FTP поверх HTTP. ◦ домен для веб-портала, указанный в настройках веб-портала. По умолчанию используется подписанный с помощью сертификата инспектирование SSL сертификат, выпущенный для домена auth.captive, со следующими параметрами: • Subject name = auth.captive • Alternative names = auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive Если администратор не загрузил свой собственный сертификат для обслуживания этой роли, то NGFW самостоятельно в автоматическом режиме перевыпускает данный сертификат при изменении администратором одного из доменов на странице **Настройки** (домены для auth.captive, logout.captive, block.captive, ftpclient.captive, sslvpn.captive).
SSL инспектирование	Сертификат класса удостоверяющего центра. Он используется для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. Например, при перехвате HTTPS-трафика сайта yahoo.com оригинальный сертификат, выданный: Subject name = yahoo.com Issuer name = VeriSign Class 3 Secure Server CA — G3, подменяется на Subject name = yahoo.com Issuer name = компания, как она указана в сертификате центра сертификации, заведенного в NGFW. Данный сертификат также используется для создания сертификата по умолчанию для роли SSL Captive-портала.
SSL инспектирование (промежуточный)	Промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата.
SSL инспектирование (корневой)	Корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. Для корректной работы необходим только публичный ключ сертификата.
Пользовательский сертификат	Сертификат, который назначается пользователю NGFW. Пользователь может быть, как заведен локально, так и получен из LDAP. Сертификат может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси.
УЦ авторизации веб-консоли	Удостоверяющий центр авторизации администраторов для доступа к веб-консоли. Для успешной авторизации сертификат администратора должен быть подписан сертификатом этого типа.
SAML server	Используется для работы NGFW с сервером SSO SAML IDP. Подробно о настройке работы NGFW с сервером авторизации SAML IDP смотрите в соответствующем разделе руководства.
Веб-портал	Сертификат, используемый для веб-портала. Если данный сертификат не указан явно, то NGFW использует сертификат SSL Captive-портала, выпущенный сертификатом для инспектирования SSL. Подробно о настройке веб-портала смотрите в соответствующем разделе руководства.

Сертификатов для SSL веб-консоли, SSL Captive-портала и сертификатов SSL-инспектирования может быть несколько, но только один сертификат каждого типа может быть активным и использоваться для выполнения своих задач. Сертификатов типа УЦ авторизации веб-консоли может быть несколько, и каждый из них может быть использован для проверки подлинности сертификатов администраторов.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку **Создать** в разделе **Сертификаты**.

Наименование	Описание
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата. • **Страна** — страна, в которой выписывается сертификат. • **Область или штат** — область или штат, в котором выписывается сертификат. • **Город** — город, в котором выписывается сертификат. • **Название организации** — название организации, для которой выписывается сертификат. • **Common name** — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • **E-mail** — email вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в NGFW. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата (SSL веб-консоли, инспектирование SSL, УЦ авторизации веб-консоли). В случае, если вы выбрали SSL веб-консоли, NGFW перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата. Сертификат инспектирования SSL начинает работать немедленно после того, как его выбрали. Более детально об инспектировании HTTPS смотрите в главе Инспектирование SSL.

NGFW позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • **Экспорт сертификата** — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. Подробнее об этом читайте в Приложение 1. Установка сертификата локального удостоверяющего центра. • **Экспорт CSR** — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности NGFW не разрешает экспорт приватных ключей сертификатов.

ПримечаниеПользователи могут скачать себе для установки сертификат инспектирования SSL с NGFW по прямой ссылке: http://NGFW_IP:8002/cps/ca

Для импорта сертификата необходимо иметь файлы сертификата и — опционально — приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку **Импорт**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата. • **Файл сертификата**: загрузите файл, содержащий данные сертификата. • **Приватный ключ**: загрузите файл, содержащий приватный ключ сертификата. • **Пароль** для приватного ключа, если таковой требуется. • **Цепочка сертификатов** - файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле.

Использование корпоративного УЦ для создания сертификата инспектирования SSL

Если в компании уже существует внутренний УЦ или цепочка удостоверяющих центров, то можно указать в качестве сертификата для инспектирования SSL сертификат, созданный внутренним УЦ. В случае, если внутренний УЦ является доверяемым для всех пользователей компании, то перехват SSL будет происходить незаметно, пользователи не будут получать предупреждение о подмене сертификата.

Рассмотрим более подробно процедуру настройки NGFW. Допустим, что в организации используется внутренний УЦ на базе Microsoft Enterprise CA, интегрированный в Active Directory. Структура УЦ следующая:



Пример структуры корпоративного УЦ

Необходимо выписать с помощью Sub CA2 сертификат для UserGate и настроить его в качестве сертификата для инспектирования SSL. Необходимо выписать сертификат NGFW SSL decrypt в качестве удостоверяющего центра.

ПримечаниеNGFW не поддерживает алгоритм подписи rsassaPss. Необходимо, чтобы вся цепочка сертификатов, которая используется для выписывания сертификата для инспектирования SSL, не содержала данного алгоритма подписи.

Для выполнения этой задачи следует выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать CSR-запрос на создание сертификата в UserGate.	Нажать на кнопку **Создать → Новый CSR**. Заполнить необходимые поля и создать CSR. Будет создан приватный ключ и файл запроса. С помощью кнопки **Экспорт** скачать файл запроса.
Шаг 2. Создать сертификат на основе подготовленного CSR.	В Microsoft CA создать сертификат на основе полученного на предыдущем шаге CSR-файла с помощью утилиты certreq: certreq.exe -submit -attrib "CertificateTemplate:SubCA" HTTPS_csr.pem или с помощью веб-консоли Microsoft CA, указав в качестве шаблона «Подчиненный центр сертификации». Обратитесь к документации Microsoft за более подробной информацией. По окончании процедуры вы получите сертификат (публичный ключ), подписанный УЦ Sub CA2.
Шаг 3. Скачать полученный сертификат.	Из веб-консоли Microsoft CA скачать созданный сертификат (публичный ключ).
Шаг 4. Загрузить сертификат в созданный ранее CSR.	В NGFW выбрать созданный ранее CSR и нажать кнопку **Редактировать**. Загрузить файл сертификата и нажать **Сохранить**.
Шаг 5. Указать тип сертификата - инспектирование SSL.	В NGFW выбрать созданный ранее CSR и нажать кнопку **Редактировать**. В поле **Используется** указать **SSL инспектирование**.
Шаг 6. Скачать сертификаты для промежуточных УЦ (Sub CA1 и Sub CA2).	В веб-консоли Microsoft CA выбрать и скачать сертификаты (публичные ключи) для УЦ Sub CA1 и Sub CA2.
Шаг 7. Загрузить сертификаты Sub CA1 и Sub CA2 в UserGate.	С помощью кнопки **Импорт** загрузить скачанные на предыдущем шаге сертификаты для Sub CA1 и Sub CA2.
Шаг 8. Установить тип — инспектирование SSL (промежуточный) для сертификатов Sub CA1 и Sub CA2.	В NGFW выбрать загруженные сертификаты и нажать кнопку **Редактировать**. Указать в поле **Используется** — **Инспектирование SSL (промежуточный)** для обоих сертификатов.
Шаг 9. Загрузить сертификат Root CA в NGFW (опционально).	С помощью кнопки **Импорт** загрузить корневой сертификат организации в NGFW. С помощью кнопки **Редактировать** указать в поле **Используется** — **Инспектирование SSL (корневой)**.

Расширение системного раздела

Version: 7.0.1, 7.1.0
Product: NGFW, UGMC, LogAn, SIEM
Documentation:

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить **новый** диск необходимого размера в свойствах виртуальной машины UserGate.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate войти в раздел **Support menu**. В открывшемся разделе выбрать **Expand data partition** и запустить процесс расширения раздела.
Шаг 3. Проверить размер системного раздела.	После завершения процесса расширения загрузить узел и в разделе **Дашборд → Диски** проверить размер системного раздела.

Системные утилиты

Version: 7.0.1
Product: NGFW
Documentation: ☑

Системные утилиты доступны администратору во время загрузки NGFW через меню загрузки (boot menu). Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB (при наличии соответствующих разъемов на устройстве) или используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к NGFW. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

Наименование	Описание
UGOS NGFW	Загрузка NGFW с выводом диагностической информации о загрузке в последовательный порт.
UGOS NGFW (failsafe)	Загрузка NGFW в упрощённом видеорежиме.
Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
Restore previous version	Раздел доступен после обновления и дает возможность произвести откат к тому состоянию системы, в котором она была на момент установки обновления.

Раздел системных утилит (Support menu) позволяет выполнить следующие действия:

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Expand data partition	Увеличение раздела для хранения данных. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины NGFW. **Важно!** Для расширения системного раздела с сохранением данных и настроек NGFW необходимо средствами гипервизора добавить **новый** диск и затем выполнить операцию **Expand data partition**, как указано в статье руководства администратора Расширение системного раздела.
Create backup	Создать полную копию диска NGFW на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление NGFW с внешнего USB носителя.
Factory reset	Сброс состояния NGFW. Версия ПО останется той, которая была установлена при запуске команды. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

Настройка сети

Настройка зон

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Зона в NGFW — это логическое объединение сетевых интерфейсов. Политики безопасности NGFW используют зоны интерфейсов, а не непосредственно интерфейсы. Это дает необходимую гибкость политикам безопасности, а также существенно упрощает управление отказоустойчивым кластером. Зоны одинаковы на всех узлах кластера, то есть данная настройка является глобальной для кластера.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов, подключенных к сети партнера и т.п.

По умолчанию NGFW поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление NGFW.
Trusted	Зона для подключения доверенных сетей, например, LAN-сетей.
Untrusted	Зона для интерфейсов, подключенных к недоверенным сетям, например, к интернету.
DMZ	Зона для интерфейсов, подключенных к сети DMZ.
Cluster	Зона для интерфейсов, используемых для работы кластера.
VPN for Site-to-Site	Зона, в которую помещаются все клиенты типа Офис-Офис, подключаемые к NGFW по VPN.
VPN for remote access	Зона, в которую помещаются все мобильные пользователи, подключаемые к NGFW по VPN.
Tunnel inspection zone	Зона для инспектирования туннелей. Зона, которой будут принадлежать все адреса источников и назначения инкапсулированных в туннель пакетов.

Администраторы NGFW могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

ПримечаниеМожно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону.	Нажать на кнопку **Добавить** и дать название зоне
Шаг 2. Настроить параметры защиты зоны от DoS (опционально).	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • **Агрегировать** — если установлено, то считаются все пакеты, входящие в интерфейсы данной зоны. Если не установлено, то считаются пакеты отдельно для каждого IP-адреса. • **Порог уведомления** — при превышении количества запросов над указанным значением происходит запись события в системный журнал. • **Порог отбрасывания пакетов** — при превышении количества запросов над указанным значением NGFW начинает отбрасывать пакеты и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления — 3000 запросов в секунду, для порога отбрасывания пакетов — 6000 запросов в секунду. Рекомендуется включать защиту от флуда на всех интерфейсах, за исключением интерфейсов зоны **Cluster**. Необходимо увеличить пороговое значение отбрасывания пакетов для протокола UDP, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN. **Исключения защиты от DoS** — позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для сервиса IP-телефонии, так как он шлет большое количество UDP-пакетов. **Важно!** NGFW позволят произвести более гранулированную защиту от DoS атак. Для получения дополнительной информации обратитесь в раздел Защита от DoS атак.

Наименование	Описание
Шаг 3. Настроить параметры контроля доступа зоны (опционально).	Указать предоставляемые NGFW сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы. Сервисы: • **Ping** — позволяет пинговать NGFW. • **SNMP** — доступ к NGFW по протоколу SNMP (UDP 161). • **Captive-портал** и **страница блокировки** — необходимы для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • **XML-RPC** для управления — позволяет управлять продуктом по API (TCP 4040). • **Кластер** — сервис, необходимый для объединения нескольких узлов NGFW в кластер (TCP 4369, TCP 9000-9100). • **VRRP** — сервис, необходимый для объединения нескольких узлов NGFW в отказоустойчивый кластер (IP протокол 112). • **Консоль администрирования** — доступ к веб-консоли управления (TCP 8001). • **DNS** — доступ к сервису DNS-прокси (TCP 53, UDP 53). • **HTTP(S)-прокси** — доступ к сервису HTTP(S)-прокси (TCP 8090). • **Агент авторизации** — доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • **SMTP(S)-прокси** — сервис фильтрации SMTP-трафика от спама. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел Защита почтового трафика. • **POP3(S)-прокси** — сервис фильтрации POP3-трафика от спама. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел Защита почтового трафика. • **CLI по SSH** — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **VPN** — доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • **SCADA** — сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • **Reverse-прокси** — сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. Более подробно смотрите раздел Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси. • **Web-портал**- сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. Более подробно смотрите раздел Веб-портал. • **Log Analyzer** — сервис для подключения к анализатору журналов Log Analyzer (TCP 2023 и 9713). • **OSPF** — сервис динамической маршрутизации OSPF. Более подробно смотрите раздел OSPF. • **BGP**- сервис динамической маршрутизации BGP. Более подробно смотрите раздел BGP. • **NTP service** — разрешает доступ к сервису точного времени, запущенному на NGFW. • **Сборщик логов** — сервис для разрешения получения информации с удалённых устройств по протоколу Syslog (по умолчанию используется порт TCP 514). (Присутствует начиная с версии 7.1) Подробнее о требованиях сетевой доступности читайте в Приложение 4. Требования к сетевому окружению.
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально).	Атаки на основе IP-спуфинга позволяют передать пакет из внешней сети, например, из **Untrusted**, во внутреннюю, например, в **Trusted**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес внутренней сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены. С помощью чекбокса **Инвертировать** администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, для зоны Untrusted можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 и включить опцию **Инвертировать**.

Настройка интерфейсов

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN-интерфейсы. Раздел отображает все интерфейсы каждого узла кластера. Настройки интерфейсов специфичны для каждого из узлов, то есть не глобальны.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.
- Указать тип интерфейса — Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
- Назначить зону интерфейсу.
- Назначить профиль Netflow для отправки статистических данных на Netflow коллектор.
- Назначить профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Доступно только для интерфейсов типа адаптер.
- Изменить физические параметры интерфейса — MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
- Настроить работу DHCP-релея на выбранном интерфейсе. Для этого необходимо включить DHCP-релей, указать в поле **Адрес NGFW** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.
- Мост.
- PPPoE.
- VPN.
- Tunnel.

Создание интерфейса VLAN

С помощью кнопки **Добавить VLAN** администратор может создавать сабинтерфейсы. При создании VLAN необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает VLAN.
Название	Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN.
Описание	Опциональное описание интерфейса.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Mirror. Интерфейсу, работающему в режиме Layer 3, можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса. Интерфейс, работающий в режиме Mirror, может получать трафик со SPAN-порта сетевого оборудования для его анализа.
Тег VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов.
Имя узла	Имя узла в кластере, на котором создается данный VLAN.
Интерфейс	Физический интерфейс, на котором создается VLAN.
Зона	Зона, которой принадлежит VLAN.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
DHCP-релей	Настройка работы DHCP-релея на VLAN-интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес NGFW** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает бонд.
Название	Название бонда.
Имя узла	Узел кластера NGFW, на котором будет создан бонд.
Зона	Зона, к которой принадлежит бонд.

Наименование	Описание
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • **XOR.** Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • **IEEE 802.3ad** — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • **Adaptive transmit load balancing.** Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • **Adaptive load balancing.** Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • **Отключено** — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • **Active** — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • **Follow** — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • **Layer 2** — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • **Layer 2+3** — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • **Layer 3+4** — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
DHCP-релей	Настройка работы DHCP-релея на бонд-интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес NGFW** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Создание моста (bridge)

Сетевой мост работает на канальном уровне сетевой модели OSI (L2), при получении из сети кадра сверяет MAC-адрес последнего и, если он не принадлежит данному сегменту, передает (транслирует) кадр дальше; если кадр принадлежит данному сегменту, мост ничего не делает.

Интерфейс мост можно использовать в NGFW аналогично обычному интерфейсу. Кроме этого, через мост можно настроить фильтрацию передаваемого контента на уровне L2 без внесения изменений в сетевую инфраструктуру компании. Простейшая схема использования NGFW в качестве решения, обеспечивающего контентную фильтрацию на уровне L2, выглядит следующим образом:

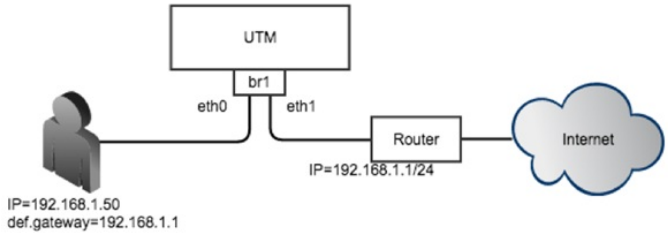


Рисунок 4 Использование моста

При создании моста можно указать режим его работы — Layer 2 или Layer 3.

ПримечаниеОдновременное использование мостов L2 и L3 на устройствах NGFW невозможно — это ограничения архитектуры.

При выборе режима Layer 2 создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила АСУ ТП и Mail security. Контентная фильтрация работает в этом режиме.

Внимание! Функционал DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.

При выборе режима Layer 3 создаваемому мосту необходимо назначить IP-адрес и указать маршруты в сети, подключенные к интерфейсам моста. В данном режиме могут быть использованы все механизмы фильтрации, доступные в NGFW.

Если мост создается в ПАК NGFW, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить 2 интерфейса в байпас мост. Байпас мост автоматически переключает два выбранных интерфейса в режим байпас (закорачивает их, пропуская весь трафик мимо NGFW) в случаях если:

- Электропитание ПАК NGFW отключено.
- Система внутренней диагностики обнаружила проблему в работе ПО NGFW.

Более подробно о сетевых интерфейсах, поддерживающих режим байпас смотрите в спецификации на оборудование ПАК NGFW.

С помощью кнопки **Добавить мост** администратор может объединить несколько физических интерфейсов в новый тип интерфейса — мост. Необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает интерфейс мост.
Название	Название интерфейса.
Имя узла	Узел кластера NGFW, на котором создать интерфейс мост.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Layer 2.
Зона	Зона, к которой принадлежит интерфейс мост.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow.
Интерфейсы моста	Два интерфейса, которые будут использованы для построения моста.
Интерфейсы байпас моста	Пара интерфейсов, которые можно использовать для построения байпас моста. Требуется поддержка оборудования ПАК NGFW.
STP (Spanning Tree Protocol)	Включает использование STP для защиты сети от петель.
Forward delay	Задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP.
Maximum age	Время, по истечении которого STP-соединение считается потерянным.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
DHCP-релей	Настройка работы DHCP-релея на bridge-интерфейсе. Необходимо включить DHCP-релей, указать в поле **Адрес NGFW** IP-адрес интерфейса, на котором добавляется функция релея, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Интерфейс PPPOE

PPPoE (**Point-to-point protocol over Ethernet**) — сетевой протокол канального уровня передачи кадров PPP через Ethernet. С помощью кнопки **Добавить**, выбрав **Добавить PPPoE**, администратор может создать PPPoE интерфейс. При создании необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает интерфейс PPPoE.
Имя узла	Узел кластера NGFW, на котором создать интерфейс PPPoE.
Интерфейс	Указать интерфейс, на котором будет создаваться интерфейс PPPoE.
Зона	Зона, к которой принадлежит интерфейс PPPoE.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow.
MTU	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet.
Логин	Имя пользователя для соединения PPPoE.
Пароль	Пароль пользователя для соединения PPPoE.
Переподключаться автоматически	Включает переподключение соединения при обрыве связи.

Наименование	Описание
Тип аутентификации	Протоколы аутентификации, использующиеся в протоколе PPP: • **CHAP** — Challenge Handshake Authentication Protocol — протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём. • **PAP** — Password Authentication Protocol — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом (без шифрования).
Интервал между попытками подключения (сек.)	Интервал времени в секундах после разрыва соединения перед повторным запуском.
Маршрут по умолчанию	Устанавливает интерфейс PPPoE в качестве маршрута по умолчанию.
Интервал проверки соединения (сек.)	Интервал проверки соединения.
Количество неуспешных проверок	Количество неуспешных проверок соединения, после которого NGFW считает, что соединение отсутствует и разрывает его.
Использовать DNS-сервер провайдера	Если опция включена, то NGFW использует DNS-серверы, выданные провайдером.
Количество попыток подключения	Количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены.
PPPoE сервис	Имя сервиса необходимо прописывать в случае предоставления провайдером. Если имя сервиса не используется, поле необходимо оставить пустым.

Интерфейс VPN

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах NGFW, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры:

Наименование	Описание
Название	Название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса.
Описание	Описание интерфейса.
Зона	Зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону.
Профиль Netflow	Профиль Netflow, используемый для данного интерфейса. Не обязательный параметр.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow.
Режим	Тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес. Для использования интерфейса, используемого в роли клиента, необходимо выбрать Динамический режим.
MTU	Размер MTU для выбранного интерфейса.

По умолчанию в системе уже созданы 3 VPN-интерфейса:

- **tunnel1**, который рекомендовано использовать для Remote access VPN.
- **tunnel2**, который рекомендовано использовать для серверной части Site-to-Site VPN.
- **tunnel3**, который рекомендовано использовать для клиентской части Site-to-Site VPN.

Интерфейс туннель

Интерфейс туннель — это виртуальный сетевой адаптер, который может использоваться для создания соединения точка-точка через IP-сеть. Поддерживаются следующие типы туннельных интерфейсов:

- GRE — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47.
- IPIP — это протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP пакета в другой IP пакет, это добавление внешнего заголовка с Source IP — точкой входа в туннель, и Destination IP — точкой выхода из туннеля.
- VXLAN — это протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789.

Для создания туннельного интерфейса в разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить туннель.** Задайте следующие параметры:

Наименование	Описание
Включено	Включение или выключение данного интерфейса.
Название	Название интерфейса, должно быть в виде greN, где N — это порядковый номер туннельного интерфейса.
Описание	Описание интерфейса.
Зона	Зона, к которой будет относится данный интерфейс.

Наименование	Описание
Режим	Режим работы туннеля — GRE, IPIP, VXLAN.
MTU	Размер MTU для выбранного интерфейса.
Локальный IP	Локальный адрес point-to-point интерфейса.
Удаленный IP	Удаленный адрес point-to-point интерфейса.
IP интерфейса	IP-адрес, назначенный туннельному интерфейсу.
VXLAN ID	Идентификатор VXLAN. Только для типа туннеля VXLAN.

Настройка Netflow

Netflow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Анализатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

NGFW может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс NGFW, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль Netflow.	В разделе **Библиотеки → Профили Netflow** нажать на кнопку **Добавить** и создать профиль Netflow. Подробнее о профиле Netflow смотрите раздел Профили Netflow.
Шаг 2. Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо собирать статистику.	В разделе **Сеть → Интерфейсы** в настройках конкретного сетевого интерфейса указать созданный профиль Netflow.

Настройка шлюзов

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1
Product: NGFW

Для подключения NGFW к интернету необходимо указать IP-адрес одного или нескольких шлюзов. Если для подключения к интернету используется несколько провайдеров, то необходимо указать несколько шлюзов. Настройка шлюза уникальна для каждого из узлов кластера.

Пример настройки сети с двумя провайдерами:

- Интерфейс eth1 с IP-адресом 192.168.11.2 подключен к интернет-провайдеру 1. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс eth2 с IP-адресом 192.168.12.2 подключен к интернет-провайдеру 2. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок **Балансировка** и указать **Вес** каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз). При распределении трафика между шлюзами с разными весами происходит: 1.Вычисление хэша от адресов источника и назначения. 2.Выбор шлюза Трафик распределяется с учётом весов. Пусть настроены 2 шлюза: • **n1**, **n2** — сессии, проходящие через шлюзы. • **w1**, **w2** — веса шлюзов. Тогда сессии между шлюзами будут распределяться согласно **n1**/**w1 = n2**/**w2**.
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить **Проверку сети**, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет (с помощью ping) с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли(в случае если в текущей сессии не менялся порядок сортировки отбражаемых шлюзов,смена порядка сортировки не влияет на процесс выбора шлюза). По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

Состояние шлюза (доступен — зеленый, не доступен — красный) определяется следующим образом:

Наименование	Описание
Проверка сети отключена	Шлюз считается доступным, если NGFW может получить его MAC-адрес с помощью ARP-запроса. Проверка наличия доступа в интернет через этот шлюз не производится. Если MAC-адрес шлюза не может быть определен, шлюз считается недоступным.
Проверка сети включена	Шлюз считается доступным, если: • NGFW может получить его MAC-адрес с помощью ARP-запроса. • Проверка наличия доступа в интернет через этот шлюз завершилась успешно. В противном случае шлюз считается недоступным.

Настройка DHCP

Version: 7.0.1, 7.1.0
Product: NGFW
Documentation: ☑

Служба DHCP (Dynamic Host Configuration Protocol) позволяет автоматизировать процесс выдачи сетевых настроек клиентам в локальной сети. В сети с DHCP-сервером каждому сетевому устройству можно динамически назначать IP-адрес, адрес шлюза, DNS.

NGFW может также выступать в качестве DHCP-релея, обеспечивая передачу DHCP-запросов от клиентов, находящихся в различных сетях, на центральный DHCP-сервер. Более подробно о настройке DHCP-релея можно посмотреть в разделе Настройка интерфейсов.

В NGFW можно создать несколько диапазонов адресов для выдачи по DHCP. DHCP работает на каждом узле отказоустойчивого кластера независимо. Для обеспечения отказоустойчивости сервиса DHCP в кластере необходимо настроить DHCP на обоих узлах, указав непересекающиеся диапазоны IP-адресов.

Для создания диапазона DHCP необходимо нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного диапазона DHCP.
Узел	Узел кластера, на котором создается данный диапазон.
Интерфейс	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона.
Диапазон IP	Диапазон IP-адресов, выдаваемый клиентам DHCP.
Маска	Маска подсети, выдаваемая клиентам DHCP.
Время аренды	Время в секундах, на которое выдаются IP-адреса.
Домен	Название домена, выдаваемое клиентам DHCP.
Шлюз	IP-адрес шлюза, выдаваемый клиентам DHCP.
Серверы имен	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
Зарезервированные адреса	MAC-адреса и сопоставленные с ними IP-адреса.
Игнорируемые MAC	Список MAC-адресов, игнорируемых DHCP-сервером.
DHCP PXE boot	Адрес сервера и имя загрузочного файла, передаваемого на запрос PXE boot.
DHCP опции	Номер опции и ее значение (список опций доступен в Приложение 5. Опции DHCP).

Выданные IP-адреса отображаются в панели **Арендованные адреса**. Администратор может освободить любой выданный адрес, выделив адрес и нажав на кнопку **Освободить**.

ПримечаниеЧтобы выдача адресов по DHCP работала на интерфейсе, который находится в зоне с включенной защитой от IP-спуфинга, необходимо в свойствах зоны во вкладке Защита от IP-спуфинга указать диапазоны выдаваемых IP-адресов, а также адрес 0.0.0.0.

Настройка DNS

Version: 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

В разделе **Настройки → Сеть → DNS** вы можете управлять списком системных DNS-серверов UserGate NGFW, а также настроить его работу в качестве DNS-прокси для других сетевых устройств.

Настройка системных DNS-серверов

Системные DNS-серверы необходимы для разрешения доменных имен в IP-адреса. В блоке параметров **Системные DNS-серверы** вы можете добавлять, редактировать или удалять DNS-серверы, которые использует UserGate NGFW.

Настройка сервиса DNS-прокси

Сервис DNS-прокси предназначен для обработки DNS-запросов пользователей и позволяет изменять их в соответствии с заданными правилами. Сервис поддерживает два режима работы:

- явный режим — клиенты отправляют DNS-запросы непосредственно на DNS-прокси;
- режим перехвата — DNS-прокси автоматически перехватывает транзитные DNS-запросы.

Важно!Для корректной работы DNS-прокси необходимо разрешить доступ к сервису «DNS» в параметрах контроля доступа соответствующей зоны.

Для использования сервиса DNS-прокси в режиме перехвата:

В разделе **Настройки → Сеть → DNS** в блоке **Настройка DNS-прокси** укажите значения следующих параметров.

Параметр	Описание
DNS-фильтрация	Включение или отключение фильтрации DNS-запросов. При включении функции UserGate NGFW перехватывает DNS-запросы пользователей и отправляет их от своего имени. Если запрашиваемый домен попадает под действие запрещающего правила контентной фильтрации, запрос блокируется. Для использования DNS-фильтрации требуется лицензия на модуль ATP. **Важно!**Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают. **Важно!**Правила контентной фильтрации, использующие список IP-адресов на вкладке «Назначение» → «Адрес доставки» , не обрабатываются модулем DNS-фильтрации. Обработка таких правил выполняется средствами модуля контентной фильтрации.
Кэширование DNS	Включение или отключение кэширования ответов DNS. Функция позволяет сохранять полученные DNS-ответы и использовать их при повторных запросах. Рекомендуется оставить функцию включенной, так как это уменьшает время обработки запросов и повышает скорость доступа пользователей к ресурсам
Лимит DNS-запросов в секунду на пользователя	Максимальное количество DNS-запросов, которое один пользователь может отправить за секунду. Запросы, превышающие установленный лимит, отбрасываются. Значение по умолчанию — 100 запросов в секунду. Не рекомендуется существенно увеличивать значение параметра, поскольку это может снизить эффективность защиты от DNS-флуда и других атак, направленных на отказ в обслуживании DNS-сервиса
Максимальное время жизни для DNS-записей (сек)	Максимальный период, в течение которого DNS-записи могут храниться в кэш-памяти DNS-прокси. По истечении этого времени запись считается устаревшей и должна быть обновлена посредством нового DNS-запроса
Рекурсивные DNS-запросы	Включение или отключение возможности выполнения рекурсивных DNS-запросов. Если опция включена, DNS-прокси самостоятельно запрашивает DNS-серверы для полного разрешения доменного имени. Рекомендуется оставить функцию включенной для обеспечения корректной обработки DNS-запросов
Тайм-аут (мсек)	Максимальное время ожидания ответа от DNS-сервера на один запрос. Если ответ не поступил до истечения указанного времени, запрос считается неудачным
Только A и AAAA DNS-записи для неизвестных пользователей (защита от VPN поверх DNS)	При включении параметра для пользователей, не прошедших аутентификацию, разрешаются только DNS-запросы типов A и AAAA. Запросы остальных типов отклоняются. Этот параметр позволяет ограничивать возможности DNS-туннелирования для предотвращения создания каналов передачи данных через DNS-протокол
Число попыток	Максимальное количество повторных запросов, которые DNS-прокси может выполнить при отсутствии ответа от DNS-сервера. Если ответ не будет получен после указанного числа попыток, запрос завершится ошибкой

С помощью правил DNS-прокси можно настроить обработку запросов для отдельных доменов на определенных DNS-серверах. Такой механизм удобно использовать для разрешения внутренних доменных имен компании, например доменов Active Directory, которые не публикуются в интернете и доступны только во внутренней сети.

Для создания правила DNS-прокси:

1. В разделе **Настройки → Сеть → DNS** в блоке **DNS-прокси → Правила DNS** нажмите **Добавить.**
2. Укажите необходимые параметры:
   - На вкладке **Общие** укажите название, описание правила и его место в списке правил DNS.
   - На вкладке **Домены** укажите список доменов. Допускается использование символа «*» для указания шаблона доменов.
   - На вкладке **Серверы DNS** укажите IP-адреса DNS-серверов, на которые необходимо пересылать запросы для указанных доменов.

Вы также можете вручную задавать статические записи типа host (A-записи), которые будут использоваться сервисом DNS-прокси для фиксированного сопоставления доменных имен и IP-адресов.

Для создания статической записи:

1. В разделе **Настройки → Сеть → DNS** в блоке **DNS-прокси → Статические записи** нажмите **Добавить**.
2. Укажите необходимые параметры:
   - название и описание правила;
   - доменное имя (FQDN) статической записи (например, www.example.com);
   - список IP-адресов, которые UserGate NGFW будет возвращать при запросе указанного доменного имени.

Виртуальные маршрутизаторы

Version: 6.1.9, 7.0.1
Product: UserGate NGFW
Documentation: ☑

В крупных сетях зачастую множество логических сетей используют для прохождения трафика одни и те же сетевые устройства. Данный трафик должен быть разделен на сетевых устройствах, в первую очередь для уменьшения риска несанкционированного доступа между сетями.

Виртуальные маршрутизаторы или **Virtual Routing and Forwarding (VRF)** обеспечивают разделение трафика путем разделения сетевых интерфейсов в независимые группы. Трафик из одной группы интерфейсов не может попасть в другие группы интерфейсов.

Каждый виртуальный маршрутизатор имеет свою собственную таблицу маршрутизации. Таблица маршрутизации виртуального роутера может содержать запись о маршрутах, заданных статически или полученных с помощью протоколов динамической маршрутизации — BGP, OSPF, RIP.

В рамках разных виртуальных маршрутизаторов допускается использовать одинаковые IP-сети (IP overlapping).

Интерфейсы, не вошедшие ни в один из виртуальных маршрутизаторов, автоматически назначены в виртуальный маршрутизатор — **Виртуальный маршрутизатор по умолчанию.**

Виртуальные маршрутизаторы имеют следующие ограничения:

Следующие сервисы могут быть использованы только в Виртуальном маршрутизаторе по умолчанию:

- WCCP.
- ICAP.
- DNS.
- Авторизация.
- Балансировка нагрузки
- Любой сетевой трафик, генерируемый самим устройством — проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS сообщений, SNMP трапов и т.п.
- Действие правил NAT, DNAT, Port forwarding распространяются на все виртуальные маршрутизаторы.
- Зоны глобальны, то есть настройки зоны, и принадлежность интерфейсов к зонам распространяются на все виртуальные маршрутизаторы.

ПримечаниеВиртуальный маршрутизатор по умолчанию необходим для корректной работы NGFW. Он используется для проверки лицензии, получения обновлений, работы DNS-служб.

Для добавления виртуального маршрутизатора необходимо выполнить следующие действия:

Примечание! Следующие префиксы не могут быть использованы для задания имени виртуального маршрутизатора: port, gre, egress, ingress, tun, tap, erspan, ppp, bond, bridge, pimreg.
Примечание!При создании виртуального маршрутизатора его имя не должно содержать заглавных букв, и должно иметь длину не менее трех символов.

Наименование	Описание
Шаг 1. Создать виртуальный маршрутизатор.	В разделе **Сеть → Виртуальные маршрутизаторы** нажмите добавить и задайте имя и описание нового виртуального маршрутизатора. Укажите имя узла, на котором создается данный виртуальный маршрутизатор при наличии кластера.
Шаг 2. Добавить интерфейсы в созданный виртуальный маршрутизатор.	В закладке **Интерфейсы** укажите интерфейсы, которые должны быть помещены в данный виртуальный маршрутизатор. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, не могут быть добавлены; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, VPN и другие.
Шаг 3. Добавить статические маршруты (опционально).	Добавьте маршруты (кроме маршрута по умолчанию), которые будут применены к трафику в данном виртуальном маршрутизаторе. Подробнее читайте в разделе Статические маршруты. Маршрут по умолчанию добавляется в разделе **Сеть → Шлюзы**. Подробнее о настройке шлюзов читайте в разделе Настройка шлюзов.
Шаг 4. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации OSPF (опционально).	Настройте протокол OSPF для построения динамической карты маршрутов. Более подробно смотрите раздел руководства OSPF.
Шаг 5. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации BGP (опционально).	Настройте протокол BGP для построения динамической карты маршрутов. Более подробно смотрите раздел руководства BGP.
Шаг 6. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации RIP (опционально).	Настройте протокол RIP для построения динамической карты маршрутов. Более подробно смотрите раздел руководства RIP.
Шаг 7. Настроить мультикастинг (опционально).	Настройте параметры мультикастинга в данном виртуальном маршрутизаторе. Более подробно смотрите раздел руководства Мультикастинг.

Статические маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей. Маршрут применяется локально к тому узлу кластера и в тот виртуальный маршрутизатор, в котором он создается.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Задать название и описание данного маршрута.	В разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Статические маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута.

Наименование	Описание
Шаг 3. Указать тип данного маршрута.	Возожно указать следующие типы маршрутов: • Unicast — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • Blackhole — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата. • Unreachable — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • Prohibit — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13).
Шаг 4. Указать адрес назначения.	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 5. Указать шлюз.	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с NGFW.
Шаг 6. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то NGFW сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 7. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

Протоколы динамической маршрутизации

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов.

Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически.

ПримечаниеЕсли в системе настроены статические шлюзы, то маршруты по умолчанию, полученные от протоколов динамической маршрутизации, игнорируются.

NGFW поддерживает работу трех протоколов маршрутизации — OSPF, BGP, RIP.

Внимание!Перед настройкой и использовании протоколов динамической маршрутизации необходимо задать соответствующие разрешения на вкладках *Контроль доступа* нужных зон.

OSPF

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации — вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол OSPF.

OSPF (Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы (АС). Подробно о работе протокола OSPF читайте в соответствующей технической документации.

ПримечаниеПри работе протокола OSPF в кластере отказоустойчивости в режиме Active-Passive, узел, который обладает ролью Slave, автоматически назначает стоимость для всех своих интерфейсов и для списков редистрибуции в 2 раза выше, чем установленная на узле стоимость. Тем самым обеспечивается приоритет Master-узла в маршрутизации трафика.

Для настройки OSPF в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить OSPF-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **OSPF** и настройте OSPF-роутер.

При настройке OSPF-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает использование данного OSPF-роутера.
Идентификатор роутера	IP-адрес роутера. Должен быть уникальным и задан в формате IPv4 (для удобства может совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору).
Redistribute	Распространять другим OSPF-роутерам маршруты в непосредственно подключенные к NGFW сети (connected) или статические маршруты, добавленные администратором для данного виртуального маршрутизатора (kernel).
Метрика	Установить метрику распространяемым маршрутам. Для задания метрики по-умолчанию укажите в этом поле значение 0. Метрика по-умолчанию для Мастер ноды кластера равна 20. Метрика по-умолчанию для запасной ноды равна 40.
Default originate	Оповещать другие роутеры о том, что данный роутер имеет маршрут по умолчанию.

При настройке интерфейсов OSPF укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного интерфейса.
Интерфейс	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор.
Стоимость	Стоимость канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1.

Наименование	Описание
Приоритет	Целое число от 0 до 255. Чем больше значение, тем выше шанс у маршрутизатора стать назначенным маршрутизатором (designated router) в сети для рассылки LSA. Значение 0 делает назначение для данного маршрутизатора невозможным. Значение по умолчанию 1.
Интервал hello	Время в секундах, через которое маршрутизатор посылает hello-пакеты. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд.
Интервал dead	Интервал времени в секундах, по истечении которого соседний маршрутизатор считается неработающим. Время исчисляется от момента приема последнего пакета hello от соседнего маршрутизатора. Значение по умолчанию 40 секунд.
Интервал повторения	Устанавливает временный интервал перед повторной отсылкой пакета LSA. Значение по умолчанию 5 секунд.
Задержка передачи	Устанавливает примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию 1 секунда.
Аутентификация **Вкл**	Включает требование аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов.
Тип авторизации	Может быть: • **Plain** — передача ключа в открытом виде для аутентификации роутеров. Необходимо указать значение поля **Ключ**. • **Digest** — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Необходимо указать **Ключ** и **MD5 key ID**. Эти параметры должны быть идентичными на всех роутерах для нормальной работы. Значение параметра Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.

При настройке области OSPF укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данной области.
Имя	Имя для данной области.
Стоимость	Стоимость LSA, анонсируемых в stub-области.
Идентификатор области	Идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Идентификатор области должен совпадать для установления соседства OSPF.
Тип авторизации	Может быть: • **Нет** — не требовать авторизацию OSPF-пакетов. • **Plain** — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. • **Digest** — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Идентификация на уровне интерфейсов имеет приоритет над авторизацией на уровне зоны.
Тип области	Определяет тип области. Поддерживаются следующие типы областей: • **Нормальная** — обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты. • **Тупиковая (Stub)** — тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. • **NSSA** — Not-so-stubby. Зона NSSA определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR).
Не суммировать	Запрещает инжекцию суммированных маршрутов в тупиковые типы областей.
Интерфейсы	Выбор интерфейсов OSPF, на которых будет доступна данная зона.
Виртуальные линки	Специальное соединение, которое позволяет соединять, например, разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение или как backup на случай выхода из строя основных соединений. Можно указать идентификаторы маршрутизаторов, которые доступны через данную зону.

ПримечаниеUserGate NGFW использует следующие типы сети:

- point-to-point — для интерфейсов GRE;
- point-to-multipoint — для интерфейсов VPN;
- broadcast — для физических интерфейсов, бондов и VLAN.

BGP

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол BGP.

BGP (Border Gateway Protocol) — динамический протокол маршрутизации, относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP — External Gateway Protocol). На текущий момент является основным протоколом динамической маршрутизации в интернете. Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протоколы внутридоменной маршрутизации для определения маршрутов

внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети. Подробно о работе протокола BGP читайте в соответствующей технической документации.

Для настройки BGP в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить BGP-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **BGP** и настройте BGP-роутер.
Шаг 3. Задать фильтры и Routemap (опционально) для ограничения количества получаемых маршрутов.	В разделе **Фильтры** нажать на кнопку **Добавить** и настроить параметры Routemap/фильтров. Добавить столько Routemap/фильтров, сколько необходимо для работы BGP в вашей организации.
Шаг 4. Добавить хотя бы одного BGP-соседа (пира).	В разделе **BGP-соседи** нажать на кнопку **Добавить** и настроить параметры маршрутизатора, относящегося к соседней АС. Добавить столько соседей, сколько необходимо. **Важно!** Согласно требованиям RFC-8212 для каждого соседа необходимо обязательно указать входящие и исходящие фильтры. Без входящих фильтров роутер не будет принимать маршруты с данного соседа, при отсутствии исходящих фильтров роутер не будет анонсировать маршруты на данного соседа. Если интерфейсу NGFW, с которого устанавливается подключение к соседу, назначено несколько IP-адресов, то при настройке BGP-соседа, в случае отсутствия правила NAT, принудительно устанавливающего адрес источника для BGP-сессии с этим соседом, в качестве адреса NGFW необходимо указывать основной (primary) IP-адрес, т.е. адрес, который стоит первым в списке в настройках интерфейса.

При настройке BGP-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного BGP-роутера.
Идентификатор роутера	IP-адрес роутера. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору.
Номер автономной системы (АС)	Автономная система — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе.
Redistribute	Позволяет распространять другим BGP-маршрутизаторам маршруты в непосредственно подключенные к NGFW-сети (connected), статические маршруты, добавленные администратором для данного виртуального маршрутизатора (kernel), или маршруты, полученные по протоколу OSPF.
Multiple path	Включает балансировку трафика на маршруты с одинаковой стоимостью.
Сети	Список сетей, относящихся к данной АС.

Для добавления BGP-соседей нажмите кнопку **Добавить** и укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного соседа.
Host	IP-адрес соседа.
Описание	Произвольное описание соседа.
Удаленная ASN	Номер автономной системы, к которой относится сосед.
Вес	Вес данных маршрутов, получаемых от данного соседа.
TTL	Максимальное количество хопов, разрешенное до этого соседа.
Allowas-in	По-умолчанию BGP маршрутизатор отбрасывает маршрут если видит в AS path собственный номер автономной системы. Эта директива позволяет маршрутизатору нарушить данное правило. Номер — указывает количество раз, которое может встречаться в AS Path номер AS BGP-соседа. Возможны значения от 0 до 10 (0 — origin).
Анонсировать себя в качестве следующего перехода (next-hop-self) для BGP	Заменять значение next-hop-self на собственный IP-адрес, если сосед является BGP.
Multihop для eBPGP	Указывает, что до этого соседа непрямое соединение (более одного хопа).
Route reflector client	Указывает, является ли этот сосед клиентом Route reflector.
Soft reconfiguration	Использовать soft reconfiguration (без разрыва соединений) для обновления конфигурации.
Default originate	Анонсировать этому соседу маршрут по умолчанию.
Аутентификация	Включает аутентификацию для данного соседа и задает пароль для аутентификации.
Фильтры BGP-соседей	Ограничивает информацию о маршрутах, получаемых от соседей или анонсируемых к ним.
Routemaps	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами.

Routemap позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов. Для создания routemap необходимо указать следующие параметры:

ВниманиеДля анонсирования маршрутов они должны присутствовать в таблице маршрутизации!

Наименование	Описание
Название	Имя для данного routemap.
Действие	Устанавливает действие для данного routemap, может принимать значения: • **Разрешить** — разрешает прохождение данных, попадающих под условия routemap. • **Запретить** — запрещает прохождение данных, попадающих под условия routemap.
Сравнивать по	Условия применения routemap, может принимать значения: • **IP**. Если выбрано данное условие, то в закладке IP-адреса надо добавить все необходимые IP-адреса для данного условия. • **AS путь**. Если выбрано данное условие, то в закладке AS-путь надо добавить все необходимые номера автономных сетей для данного условия. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (_), который интерпретируется как: • Пробел. • Запятая. • Начало строки. • Конец строки. • AS set delimiter { and }. • AS confederation delimiter (and). • **Community**. Если выбрано данное условие, то в закладке Community надо добавить строки всех необходимых BGP community для данного условия.
Установить next hop	Установить для отфильтрованных маршрутов значение next hop в указанный IP-адрес.
Установить вес	Установить для отфильтрованных маршрутов вес в указанное значение.
Установить метрику	Установить для отфильтрованных маршрутов метрику в указанное значение.
Установить предпочтение	Установить для отфильтрованных маршрутов предпочтение в указанное значение.
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для данного маршрута.
Community	Установить значение для BGP community для отфильтрованных маршрутов.

Фильтр позволяет фильтровать маршруты при перераспределении. При создании фильтров необходимо указать следующие параметры:

Наименование	Описание
Название	Имя для данного фильтра.
Действие	Устанавливает действие для данного фильтра, может принимать значения: • **Разрешить** — разрешает прохождение данных, попадающих под условия фильтра. • **Запретить** — запрещает прохождение данных, попадающих под условия фильтра.
Фильтровать по	Условия применения фильтра, может принимать значения: • **IP**. Если выбрано данное условие, то в закладке **IP-адреса** надо добавить все необходимые IP-адреса для данного условия. Адреса могут быть указаны в следующих форматах: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0/8::11 — маршруты, у которых первый октет 10 и префикс от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13. • **AS путь**. Если выбрано данное условие, то в закладке **AS-путь** надо добавить все необходимые номера автономных сетей для данного условия.

Пример настройки BGP для кластера NGFW приведен в статье Варианты настройки BGP для кластера Актив-Пассив.

RIP

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол RIP.

RIP (Routing Information Protocol) — протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками (хоп, hop) в качестве метрики маршрутизации. Подробно о работе протокола RIP читайте в соответствующей технической документации.

Для настройки RIP в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.

Наименование	Описание
Шаг 2. Включить RIP-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **RIP** и настройте RIP-роутер.
Шаг 3. Указать сети RIP.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **RIP** и укажите сети RIP, для которых будет работать RIP протокол.
Шаг 4. Настройте интерфейсы RIP.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **RIP** и произведите настройку интерфейсов RIP.

При настройке RIP-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает использование данного RIP-роутера.
Версия RIP	Определяет версию протокола RIP. Как правило используется версия протокола 2.
Метрика по умолчанию	Стоимость маршрута. Обычно метрика равна 1 и не может превышать 15.
Административное расстояние	Стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).
Отправлять себя в качестве маршрута по умолчанию	Оповещать другие роутеры о том, что данный роутер имеет маршрут по умолчанию.

Маршрутизатор RIP будет слать обновления маршрутной информации только с интерфейсов, для которых заданы **сети RIP**. Необходимо указать как минимум одну сеть для корректной работы протокола. При настройке сетей RIP администратор может указать сеть в виде CIDR, например, 192.168.1.0/24, либо указать сетевой интерфейс, с которого будут отправлять обновления.

При настройке интерфейсов RIP укажите следующие параметры:

Наименование	Описание
Интерфейс	Выберите интерфейс, который будет использоваться для работы протокола RIP. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор.
Посылать версию	Укажите версию протокола RIP, которую маршрутизатор будет отсылать.
Принимать версию	Укажите версию протокола RIP, которую маршрутизатор будет принимать.
Пароль	Строка для авторизации, которая будет посылаться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль.
Split horizon	Метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который прибыло обновление.
Poison reverse	Метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута в 16 и отсылает его соседу, от которого его получил.
Пассивный режим	Устанавливает режим работы интерфейса, при котором он принимает обновления RIP, но не отсылает их.

Параметры редистрибуции маршрутов позволяют указать какие из маршрутов необходимо отправлять соседям. Возможно задать для редистрибуции маршруты, полученные через протоколы динамической маршрутизации OSPF, BGPG, а также маршруты в непосредственно подключенные к NGFW сети (connected) или маршруты, добавленные администратором в разделе **Маршруты** (kernel).

Мультикастинг

Технология IP мультикастинга позволяет существенно сократить передаваемый объем трафика, доставляя единый поток информации одновременно к тысячам и более потребителей, что особенно эффективно для доставки голосового и видео трафика. Традиционные методы доставки трафика — это unicast (доставка от точки к точке) и broadcast (широковещательная посылка трафика). Мультикастинг (multicast) позволяет доставить трафик к группе хостов (мультикаст-группа). Хосты (получатели), которые хотят получать данный трафик, должны вступить (присоединиться) к соответствующей мультикаст-группе. Для присоединения хостов к мультикаст-группе используется протокол Internet Group Management Protocol (IGMP). Мультикаст-группа идентифицируется групповым адресом. Для мультикастовых адресов выделена подсеть класса D с верхними 4 битами, установленными в 1110. Таким образом диапазон адресов для мультикаст-трансляций определен как 224.0.0.0 — 239.255.255.255.

Далее маршрутизаторы должны обеспечить эффективную доставку трафика от источника трансляции к получателям. Protocol Independent Multicast (PIM) используется на маршрутизаторах для достижения данной цели.

Маршрутизаторы в мультикастинговой среде можно разделить на First Hop Router (FHR), Rendezvous Point (RP), Last Hop Router (LHR). FHR находится ближе всего к источнику трансляции и отвечает за регистрацию источника трансляции в сети. RP является каталогом доступных мультикаст-источников для Any Source Multicast (ASM) режима. LHR находится ближе всего к приемнику мультикаст-трансляции. Клиенты (приемники трансляции) в локальных сетях, подключенных к LHR, используют протокол IGMP для регистрации себя в необходимой мультикаст-группе, посылая сообщение IGMP membership report.

NGFW может быть использован в качестве LHR для локальных сетей, подключенных к нему. Для регистрации клиентов (приемников) NGFW поддерживает протоколы IGMPv3 и IGMPv2.

Для взаимодействия с другими мультикаст-маршрутизаторами NGFW может использовать только режим работы PIM Sparse Mode (PIM-SM). Это режим, в котором мультикаст-трафик отсылается только на те приемники, которые явно запросили это. Приемники должны периодически подтверждать свое желание получать мультикаст-трафик.

NGFW поддерживает режимы работы Source Specific Multicast (SSM) и Any Source Multicast (ASM).

Режим работы Source Specific Multicast (SSM) используется, когда приемник трафика явно указывает известный ему адрес источника трансляции. В данном режиме используется следующая адресация:

rtp://<src_ip>@<group_address>:<port>

где src_ip — адрес источника трансляции, group_address — мультикастовый групповой адрес, port — порт. Например:

rtp://10.10.10.10@239.0.0.5:4344

Режим работы Any Source Multicast (ASM). В этом режиме приемник трансляции указывает мультикаст-группу, с которой хочет получать трансляцию. Для работы данного режима необходимо наличие маршрутизатора с ролью Rendezvous Point (RP). RP определяет источник трансляции для этой группы для данного приемника. После чего источник и приемник выбирают лучший сетевой путь для пересылки данного мультикаст-трафика. В данном режиме используется следующая адресация:

rtp://@<group_address>:<port>

где group_address — мультикастовый групповой адрес, port — порт. Например:

rtp://@239.0.0.5:4344

Для настройки работы NGFW в качестве LHR мультикаст-роутера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настроить мультикаст-роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Мультикаст маршрутизатор** и настройте его.
Шаг 2. Указать интерфейсы, на которых должен работать данный роутер.	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Интерфейсы** и произведите настройку интерфейсов. Будут доступны только те интерфейсы, которые относятся к данному виртуальному маршрутизатору.
Шаг 3. Задать Rendezvous points для режима ASM (опционально).	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Rendezvous points** и укажите их адреса.
Шаг 4. Установить необходимые ограничения на доступные мультикаст-группы для режима ASM (опционально).	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Rendezvous points** и укажите адреса разрешенных мультикаст-групп в закладке **Разрешенные группы ASM**. Если оставить этот список пустым, то будут разрешены все групповые адреса.
Шаг 5. Установить необходимые ограничения на доступные мультикаст-группы для режима SSM (опционально).	В консоли NGFW в разделе **Сеть → Виртуальные маршрутизаторы** выберите в меню **Разрешенные группы SSM** и укажите адреса разрешенных мультикаст-групп Если оставить этот список пустым, то будут разрешены все групповые адреса.

При настройке мультикаст-роутера возможно указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает мультикаст-роутер в данном виртуальном маршрутизаторе.
Использовать ECMP	Разрешает распределение трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP). Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если данная опция отключена, то весь трафик на определенный хост назначения будет пересылаться только через один из роутеров (next hop).
Использовать ECMP rebalance	Если при включенной опции один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). При отключенной опции перераспределяются только те потоки, которые передавались через отключенный интерфейс.
JOIN/PRUNE интервал	Интервал в секундах (60-600) отправки сообщений соседям PIM о мультикаст-группах, трафик которых маршрутизатор хочет принимать или более не хочет принимать.
Интервал register suppress	Интервал в секундах (5-60000), после которого маршрутизатор отсылает сообщение register suppress.
Keep-alive таймер	Интервал в секундах (31-60000), через который маршрутизатор будет посылать сообщения keepalive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.

При настройке интерфейсов можно задать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного интерфейса для мультикастинга.
Интерфейс	Выберите интерфейс, который будет использоваться для работы мультикаста. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор.
Интервал отправки HELLO сообщений	Интервал отправки PIM HELLO сообщений в секундах (1-180). PIM Hello сообщения отправляются периодически со всех интерфесов, для которых включена поддержка мультикастинга. Эти сообщения позволяют узнать маршрутизатору о соседних маршрутизаторах, поддерживающих мультикастинг.
Приоритет выбора DR	Приоритет при выборе Designated router (DR) от 1 до 4294967295, с помощью которого администратор может управлять процессом выбора DR для локальной сети.
Принимать IGMP	Принимать сообщения IGMP report и IGMP query на данном интерфейсе.
Использовать IGMPv2	Использовать версию IGMP v2, по умолчанию используется IGMP v3.

При настройке Rendevouz points можно указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данный RP.
Название	Название данного RP.
IP-адрес	Unicast IP-адрес данного RP.
Разрешенные руппы SSM	Список разрешенных групповых адресов для any source multicast с данного RP. Любые сети из диапазона 224.0.0.0/4. Нет ограничений, если ничего не задано.

Разрешенные группы SSM — настройка мультикаст-роутера, определяющая список разрешенных групповых адресов для source specific multicast. Могут быть укзаны любые сети из диапазона 232.0.0.0/8. Нет ограничений, если ничего не задано.

Исключения из SPT — настройка мультикаст-роутера, задающая список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree.

WCCP

Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0
Documentation: ☑

Web Cache Communication Protocol (WCCP) — разработанный компанией Cisco протокол перенаправления контента. Предоставляет механизм перенаправления потоков трафика в реальном времени, имеет встроенные масштабирование, балансировку нагрузки, отказоустойчивость. При использовании WCCP, WCCP-сервер принимает HTTP-запрос от клиентского браузера и перенаправляет его на один или несколько WCCP-клиентов. WCCP-клиент получает данные из интернет и возвращает их в браузер клиента. Доставка данных клиенту может происходить как через WCCP-сервер, так и минуя его, в соответствии с правилами маршрутизации.

NGFW может выступать в качестве WCCP-клиента. В качестве WCCP-сервера обычно выступает маршрутизатор. Для трафика, полученного через WCCP, можно применять все доступные механизмы фильтрации.

Сервисная группа WCCP — это набор серверов WCCP (роутеры, коммутаторы) и клиентов WCCP (NGFW) с общими настройками перенаправления трафика. Сервера, указанные в одной сервисной группе, должны иметь идентичные настройки.

Для настройки WCCP-клиента в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настройте WCCP сервер.	Произведите настройку сервера WCCP в соответствии с инструкцией на WCCP-сервер.
Шаг 2. Настроить сервисные группы WCCP.	В консоли NGFW в разделе **Сеть → WCCP** нажать на кнопку **Добавить** и создать одну или несколько сервисных групп WCCP.

При создании сервисной группы укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает данную сервисную группу.
Название	Имя сервисной группы.
Описание	Описание сервисной группы.
Сервисная группа	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
Приоритет	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
Пароль	Пароль, необходимый для аутентификации NGFW в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
Способ перенаправления трафика	Определяет способ перенаправления трафика с серверов WCCP на NGFW. Возможны значения: • **gre** — используя туннель Generic Routing Encapsulation (GRE). • **L2** — используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес NGFW. Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2. **Важно!** Для трафика, полученного через WCCP-туннель, в качестве IP источника NGFW будет использовать IP-адрес компьютера клиента, а зона источника не будет определена, поэтому в правилах фильтрации для зоны источника не следует явно указывать зону (оставить Any).
Способ возврата трафика	Определяет способ перенаправления трафика с NGFW на серверы WCCP. Возможны значения: • **gre** — используя туннель Generic Routing Encapsulation (GRE). • **L2** — используя перенаправление L2. В этом случае NGFW (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер). Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
Порты для перенаправления	Порты для перенаправления. Укажите здесь порты назначения трафика. При необходимости указать несколько портов, укажите их через запятую, например: 80, 442, 8080 Для перенаправления трафика на основании значений портов источника необходимо поставить флажок **Порт источника**. **Важно!** NGFW может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на NGFW с другими портами, будет отправляться в интернет без фильтрации.
Протокол	Укажите протокол — TCP или UDP.
Роутеры WCCP	Укажите IP-адреса серверов WCCP (роутеры).
Способ назначения	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. Возможны варианты: • Хэш — распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета. Альтернативный хэш — если указан, то WCCP-сервер будет использовать его при превышении определенного количества пакетов, отправленных на WCCP-клиента с использованием обычного хэша. Поля IP-пакета, используемые для получения хэша, должны отличаться для вычисления основного и альтернативного хэшей. • Маска — распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP.

Пользователи и устройства

Пользователи и группы

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1
Product: NGFW

Политики безопасности, правила межсетевого экрана, правила веб-безопасности и многие другие возможности NGFW могут быть применены к пользователям или группам пользователей. Возможность применения политик только к тем пользователям, которым это необходимо, позволяет администратору гибко настроить свою сеть в соответствии с потребностями организации.

Идентификация пользователя — это базисная функция NGFW. Пользователь считается идентифицированным, если система однозначно связала пользователя с IP-адресом устройства, с которого пользователь подключается к сети. NGFW использует различные механизмы для идентификации пользователей:

- Идентификация по явно указанному IP-адресу
- Идентификация по имени и паролю
- Идентификация пользователей терминальных серверов Microsoft с помощью специального агента терминального сервиса
- Идентификация пользователей с помощью агента авторизации (для Windows-систем)
- Идентификация с помощью протоколов NTLM, Kerberos

Идентификация пользователей по имени и паролю возможна через Captive-портал, который, в свою очередь, может быть настроен на идентификацию пользователей с помощью каталогов Active Directory, Radius, TACACS+, NTLM, Kerberos или локальной базы пользователей.

NGFW определяет следующие типы пользователей:

Наименование	Описание
Пользователь **Unknown**	Представляет множество пользователей, не идентифицированных системой.
Пользователь **Known**	Представляет множество пользователей, идентифицированных системой. Методы идентификации пользователей могут быть различными и более подробно будут описаны далее в этой главе.
Пользователь **Any**	Любой пользователь является объединением множеств пользователей **Known** и **Unknown**.
Определенный пользователь	Конкретный пользователь, определенный и идентифицированный в системе, например, пользователь DOMAIN\User, идентифицированный с помощью авторизации в домене Active Directory.

Пользователи и группы пользователей могут быть заведены на самом устройстве NGFW — это так называемые **локальные пользователи и группы** или могут быть получены с внешних каталогов, например, Microsoft Active Directory.

Группы

Группы пользователей позволяют объединить пользователей для более удобного управления политиками безопасности.

Пользователи

В данном разделе можно добавить локальных пользователей. Здесь же можно временно отключить пользователей или включить их заново.

Обязательными параметрами для создания локального пользователя являются имя пользователя и логин. Остальные параметры являются необязательными, но для корректной идентификации необходимо указать:

- Логин и пароль — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
- IP-адрес или диапазон, MAC-адрес для идентификации с помощью комбинации MAC и IP-адресов. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанных MAC и/или IP-адреса.
- VLAN ID для идентификации пользователя по тегу VLAN. В данном случае необходимо обеспечить, чтобы данный пользователь всегда получал доступ в сеть с указанного VLAN.
- Почтовые адреса — email пользователя. Если указан, может быть использован для отсылки пользователю информации по электронной почте, например, 2-й фактор многофакторной организации.
- Номера телефонов — телефоны пользователя. Если указан, может быть использован для отсылки пользователю информации по SMS, например, 2-й фактор многофакторной организации.

В случае, если у пользователя указан и логин, и пароль, и IP/MAC/VLAN адреса, система использует идентификацию по адресу, то есть идентификация по адресу является более приоритетной.

Учетные записи пользователей LDAP здесь не отображаются, но эти пользователи также могут быть использованы в политиках безопасности.

Серверы аутентификации

Documentation: ☑
Version: 7.0.1
Product: NGFW

Серверы аутентификации — это внешние источники учетных записей пользователей, например, LDAP-сервер, или серверы, производящие аутентификацию для NGFW, например, RADIUS, TACACS+, Kerberos, SAML. Система поддерживает следующие типы серверов аутентификации:

Серверы аутентификации RADIUS, TACACS+, NTLM, SAML могут осуществлять только аутентификацию пользователей, в то время как LDAP-коннектор позволяет также получать информацию о пользователях и их свойствах.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA. Пользователи и группы могут быть использованы при настройке правил фильтрации.
- Осуществлять авторизацию пользователей через домены Active Directory/FreeIPA с использованием методов аутентификации Captive-портал, Kerberos, NTLM.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то NGFW получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, NGFW будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username @domain. Данный пользователь уже должен быть заведен в домене.
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена. Список доменов, указанный здесь будет использован для выбора на странице авторизации Captive-портала при включении соответствующей опции. Более подробно о настройке Captive-портала смотрите раздел Настройка Captive-портала.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.
Kerberos keytab	Здесь можно загрузить keytab-файл для аутентификации Kerberos. Подробно об аутентификации Kerberos и создании keytab-файла смотрите в разделе Метод аутентификации Kerberos.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

ПримечаниеДля авторизации пользователей с помощью LDAP-коннектора необходимо, чтобы пользователи входили в доменную группу Domain users.

Настройка LDAP-коннектора завершена. Для авторизации LDAP-пользователей по имени и паролю необходимо создать правила Captive-портала. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Для добавления пользователя или группы пользователей LDAP в правила фильтрации необходимо нажать на **Добавить пользователя LDAP**/**Добавить группу LDAP**, в поле поиска указать как минимум один символ, входящий в имена искомых объектов, после чего нажать на **Поиск** и выбрать желаемые группы/пользователей.

Сервер аутентификации пользователей RADIUS

Сервер RADIUS позволяет производить аутентификацию пользователей на серверах RADIUS, то есть NGFW выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер NGFW посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Сервер RADIUS не может предоставить список пользователей в NGFW, поэтому, если пользователи не были заведены в NGFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере RADIUS) или **Unknown** (не прошедших авторизацию).

Для создания сервера аутентификации RADIUS необходимо нажать на кнопку **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Хост	IP-адрес сервера RADIUS.
Порт	UDP-порт, на котором сервер RADIUS слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.

После создания сервера аутентификации необходимо настроить Captive-портал для использования метода RADIUS. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Сервер аутентификации пользователей TACACS+

Сервер TACACS+ позволяет производить аутентификацию пользователей на серверах TACACS+. При авторизации через TACACS+ NGFW посылает на серверы TACACS+ информацию с именем и паролем пользователя, а сервер TACACS+ отвечает, успешно прошла аутентификация или нет.

Сервер TACACS+ не может предоставить список пользователей в NGFW, поэтому, если пользователи не были заведены в NGFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших авторизацию).

Для создания сервера аутентификации TACACS+ необходимо нажать на кнопку **Добавить**, выбрать **Добавить TACACS+-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	Порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт TCP 49.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+. **Внимание!** Чтобы данная опция работала, необходимо также настроить её на стороне сервера TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Сервер аутентификации пользователей SAML IDP

Сервер аутентификации SAML IDP (Security Assertion Markup Language Identity Provider) позволяет авторизовать пользователей с помощью развернутой на предприятии системе Single Sign-On (SSO), например, Microsoft Active Directory Federation Service. Это позволяет пользователю, единожды авторизовавшись в системе SSO, прозрачно проходить авторизацию на всех ресурсах, поддерживающих аутентификацию SAML. NGFW может быть настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для авторизации клиента.

Сервер SAML IDP не может предоставить свойства пользователей в NGFW поэтому, если не настроено подключение к домену AD с помощью LDAP-коннектора, в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере SAML) или **Unknown** (не прошедших аутентификацию).

Для использования авторизации с помощью сервера SAML IDP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать DNS-записи для NGFW.	На контроллере домена создать DNS-запись, соответствующую NGFW, для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть **Trusted**.
Шаг 2. Настроить DNS-серверы на NGFW.	В настройках NGFW в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 3. Изменить адрес **Домен auth captive-портала**.	Изменить адрес **Домен auth captive-портала** в разделе **Настройки** на созданную на предыдущем шаге запись DNS. Подробно об изменении адреса домена Auth Captive-портала смотрите в разделе Общие настройки.
Шаг 4. Настроить сервер SAML IDP.	Добавить на сервере SAML IDP запись о сервис-провайдере NGFW, указывая созданное на шаге 1 FQDN имя.
Шаг 5. Создать сервер аутентификации пользователей SAML IDP.	Создать в NGFW сервер аутентификации пользователей SAML IDP.

Для создания сервера аутентификации пользователей SAML IDP необходимо в разделе **Пользователи и устройства → Серверы аутентификации** нажать на кнопку **Добавить**, выбрать **Добавить SAML IDP-сервер** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Описание	Описание сервера аутентификации.
SAML metadata URL	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML. При нажатии на кнопку **Загрузить** происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла. Это предпочтительный метод настройки сервера аутентификации SAML IDP. Подробно о сервере SAML смотрите в соответствующей документации.
Сертификат SAML IDP	Сертификат, который будет использован в SAML-клиенте. Возможны варианты: • Создать новый сертификат из скачанного — если при настройке был использован метод загрузки xml- файла, то сертификат автоматически создается и ему назначается роль SAML IDP (смотрите раздел Управление сертификатами). • Использовать существующий сертификат. Сертификат уже должен быть создан или импортирован в разделе **Сертификаты**, и ему не должна быть назначена роль. После создания и сохранения сервера аутентификации этому сертификату будет назначена роль SAML IDP. • Не использовать сертификат.
Single sign-on URL	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single sign-on binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты **POST** и **Redirect**. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
Single logout URL	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Наименование	Описание
Single logout binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты **POST** и **Redirect**. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Сервер аутентификации NTLM

Аутентификация NTLM позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации с помощью NTLM NGFW работает с контроллерами домена, выполняющими проверку пользователя с целью получения доступа в Интернет.

Сервер NTLM не может предоставить список пользователей в NGFW, поэтому, если пользователи не были заведены в NGFW предварительно (например, локальные пользователи или полученные из домена AD с помощью LDAP-коннектора), в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере NTLM) или **Unknown** (не прошедших аутентификацию).

Аутентификация NTLM может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан. Настройка NGFW не отличается от режима работы авторизации.

Для настройки авторизации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить синхронизацию времени с контроллером домена.	В настройках NGFW включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 2. Создать DNS-запись для NGFW.	На контроллере домена создать DNS-записи, соответствующие NGFW для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть **Trusted**.
Шаг 3. Изменить адрес **Домен Auth Captive-портала**.	Изменить адрес **домена Auth Captive-портала** и опционально адрес **домена Logout Captive-портала** в разделе **Настройки**. Для домена **Auth Captive-портала** необходимо указать созданную на предыдущем шаге запись DNS. Для домена **Logout Captive-портала** необходимо указать созданную на предыдущем шаге запись DNS. Подробно об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала.
Шаг 4. Добавить NTLM-сервер.	В разделе **Серверы аутентификации** нажать на кнопку **Добавить**, выбрать **Добавить NTLM-сервер** и указать название и имя домена Windows. Для корректной работы аутентификации NTLM, необходимо, чтобы указанное здесь имя домена резолвилось в IP-адреса контроллеров домена.
Шаг 5. Создать правило Captive-портала с аутентификацией NTLM.	Настроить Captive-портал для использования метода аутентификации NTLM. Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 6. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе **Зоны** разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью NTLM
Шаг 7. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса NGFW в качестве адреса прокси сервера. **Важно!** Вместо IP-адреса можно использовать доменное имя, но для NTLM важно, чтобы это имя было не из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos. **Важно!** В настройках NGFW имена, используемые в качестве домена для auth.captive и logout.captive, не должны быть из домена Active Directory, иначе Windows-компьютер будет пытаться использовать аутентификацию Kerberos.
Шаг 8. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в **Панель управления → Свойства браузера → Безопасность** , выберите зону **Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя** и установите **Автоматический вход в сеть с текущем именем пользователя и паролем** (**Control panel → Internet options → Security** , выберите зону **Internet → Custom level → User Authentication → Logon** и установите **Automatic logon with current name and password**). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации Kerberos

Аутентификация Kerberos позволяет прозрачно (без запроса имени пользователя и его пароля) авторизовать пользователей домена Active Directory. При авторизации через Kerberos NGFW работает с контроллерами домена, которые выполняют проверку пользователя, получающего доступ в Интернет.

Аутентификация Kerberos может работать как при явном указании прокси-сервера в браузере пользователя (это стандартный режим), так и в прозрачном режиме, когда прокси-сервер в браузере не указан.

Для авторизации с помощью Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для NGFW.	На контроллере домена создать DNS-записи, соответствующие NGFW, для использования в качестве доменов для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть **Trusted**. **Важно!** Для корректной работы создайте записи типа A, не используйте CNAME-записи.
Шаг 2. Создать пользователя для NGFW.	Создать пользователя в домене AD, например, kerb @domain.loc с опцией **password never expires**. Установите пароль пользователю kerb. **Важно!** Не используйте символы национальных алфавитов, например, кириллицу, в именах пользователя kerb или в организационных единицах Active Directory, где вы планируете создать учетную запись пользователя kerb. **Важно!** Не используйте в качестве пользователя для Kerberos пользователя, созданного для работы LDAP-коннектора. Необходимо использовать отдельную учетную запись.

Наименование	Описание
Шаг 3. Создать keytab-файл.	На контроллере домена, создать keytab файл, выполнив следующую команду **из-под администратора** (команда в одну строку!): ktpass.exe /princ HTTP/auth.domain.loc@DOMAIN.LOC /mapuser kerb@DOMAIN.LOC /crypto ALL /ptype KRB5_NT_PRINCIPAL /pass * /out C:\utm.keytab Введите пароль пользователя kerb. **Важно!** Команда чувствительна к регистру букв. В данном примере: auth.domain.loc — DNS-запись, созданная для сервера UserGate на шаге 1 DOMAIN.LOC — Kerberos realm domain, обязательно большими буквами! kerb@DOMAIN.LOC — имя пользователя в домене, созданное на шаге 2, имя realm-домена обязательно большими буквами!
Шаг 4. Настроить DNS-серверы на UserGate.	В настройках UserGate в качестве системных DNS-серверов указать IP-адреса контроллеров домена.
Шаг 5. Настроить синхронизацию времени с контроллером домена.	В настройках UserGate включить синхронизацию времени с серверами NTP, в качестве основного и — опционально — запасного NTP-сервера указать IP-адреса контроллеров домена.
Шаг 6. Изменить адрес **Домен auth captive-портала**.	Изменить адрес **Домен auth captive-портала** и опционально адрес **Домен logout captive-портала** в разделе **Настройки** на созданные на предыдущем шаге записи DNS. Подробно об изменении адресов доменов смотрите в разделе Общие настройки.
Шаг 7. Создать LDAP-коннектор и загрузить в него keytab-файл.	Создать сервер аутентификации типа LDAP-коннектор и загрузить полученный на предыдущем шаге keytab-файл. **Важно!** Не используйте в качестве пользователя для LDAP-коннектора, пользователя, созданного ранее для работы Kerberos. Необходимо использовать отдельную учетную запись. Подробно о настройке LDAP-коннектора смотрите раздел LDAP-коннектор.
Шаг 8. Создать правило Captive-портала с аутентификацией по Kerberos.	Настроить Captive-портал для использования метода аутентификации Kerberos. Более подробно о Captive-портале рассказывается в разделе Настройка Captive-портала.
Шаг 9. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе **Зоны** разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью Kerberos.
Шаг 10. Для авторизации в стандартном режиме настроить прокси-сервер на компьютерах пользователей.	На компьютерах пользователей указать обязательное использование прокси-сервера в виде FQDN-имени UserGate, созданного на шаге 3.
Шаг 11. Для авторизации в прозрачном режиме настроить автоматическую проверку подлинности пользователя браузером для всех зон.	На компьютерах пользователей зайдите в **Панель управления → Свойства браузера → Безопасность** , выберите зону **Интернет → Уровень безопасности → Другой → Проверка подлинности пользователя** и установите **Автоматический вход в сеть с текущем именем пользователя и паролем** (**Control panel → Internet options → Security** , выберите зону **Internet → Custom level → User Authentication → Logon** и установите **Automatic logon with current name and password**). Повторите данную настройку для всех других зон, настроенных на данном компьютере (Local intranet, Trusted sites).

Метод аутентификации HTTP Basic

Аутентификация Basic позволяет авторизовать пользователей с явно указанным прокси сервером по базе локальных и LDAP-пользователей. Не рекомендуется использовать данный тип аутентификации поскольку имя пользователя и пароль передаются в открытом виде по сети. Аутентификация HTTP Basic можно использовать для автоматической авторизации утилит командной строки, которым необходим доступ в Интернет, например:

curl -x 192.168.179.10:8090 -U user: password http://www.msn.com

Для авторизации по HTTP Basic необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-запись для NGFW.	На контроллере домена создать DNS-записи, соответствующие NGFW для использования в качестве домена для auth.captive и logout.captive, например, auth.domain.loc и logout.domain.loc. В качестве IP-адреса укажите адрес интерфейса NGFW, подключенного в сеть **Trusted**.
Шаг 2. Изменить адрес **Домен Auth Captive-портала**.	Изменить адрес **домена Auth Captive-портала** и опционально адрес **домена Logout Captive-портала** в разделе **Настройки**. Для домена **Auth Captive-портала** необходимо указать созданную на предыдущем шаге запись DNS. Для домена **Logout Captive-портала** необходимо указать созданную на предыдущем шаге запись DNS. Подробно об изменении адресов доменов Auth Captive-портала и Logout Captive-портала смотрите в разделе Настройка Captive-портала.
Шаг 3. Создать правило Captive-портала с аутентификацией по HTTP Basic.	Настроить Captive-портал для использования метода аутентификации HTTP Basic. При настройке, помимо метода **HTTP Basic**, необходимо добавить базу пользователей, по которой будет проверяться аутентификация (например, добавить методы аутентификации Локальный пользователь или Сервер LDAP). Более подробно о Captive-портале рассказывается в следующих главах руководства.
Шаг 4. Разрешить доступ к сервису HTTP(S) для зоны.	В разделе **Зоны** разрешить доступ к сервису HTTP(S)-прокси для зоны, к которой подключены пользователи, авторизующиеся с помощью HTTP Basic.
Шаг 5. Настроить прокси-сервер на компьютерах пользователей	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса NGFW в качестве адреса прокси сервера.

Профили аутентификации

Version: 7.0.1
Product: NGFW
Documentation: ☑

Профиль аутентификации позволяет указать набор способов и параметров авторизации пользователей, которые в дальнейшем можно будет использовать в различных подсистемах NGFW, например, Captive-портал, VPN, веб-портал и т.д. Чтобы создать профиль аутентификации, необходимо в разделе **Пользователи и устройства → Профили аутентификации** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Профиль MFA	Профиль мультифакторной аутентификации. Должен быть предварительно создан в разделе **Профили MFA**, если планируется использовать мультифакторную аутентификацию. Профиль определяет способ доставки одноразового пароля для второго метода аутентификации. Более подробно о настройке профиля MFA смотрите в соответствующей главе далее. **Важно!** Мультифакторная аутентификация возможна только с методами аутентификации, позволяющими ввести пользователю одноразовый пароль, то есть только те, где пользователь явно вводит свои учетные данные в веб-форму страницы авторизации. В связи с этим, мультифакторная аутентификация невозможна для методов аутентификации Kerberos и NTLM.
Время бездействия до отключения	Данный параметр определяет, через сколько секунд NGFW переведет пользователя из **Known users** в **Unknown users** при неактивности пользователя (отсутствии сетевых пакетов с IP-адреса пользователя).
Время жизни авторизованного пользователя	Данный параметр определяет, через сколько секунд NGFW переведет пользователя из **Known users** в **Unknown users**. По происшествии указанного времени пользователю потребуется повторно авторизоваться на Captive-портале.
Число неудачных попыток авторизации	Разрешенное количество неудачных попыток авторизации через Captive-портал до блокировки учетной записи пользователя.
Время блокировки пользователя	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации.
Методы аутентификации	Созданные ранее методы аутентификации пользователей, например, сервер аутентификации Active Directory или RADIUS. Если указано более одного метода аутентификации, то они будут использоваться в порядке, в котором они перечислены в консоли. Также возможно использование встроенных механизмов аутентификации, таких как: • **Локальный пользователь** — аутентификация по базе данных локально заведенных пользователей. • **Принять политику** — не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип аутентификации необходимо применять совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • **HTTP Basic** — аутентификация с помощью устаревшего метода HTTP Basic. • **Аутентификация Kerberos** — аутентификация по протоколу Kerberos.

Настройка Captive-портала

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Captive-портал позволяет авторизовать неизвестных пользователей (**Unknown users**) с помощью методов авторизации с использованием каталогов Active Directory, Radius, TACACS+, SAML IDP, Kerberos, NTLM или локальной базы пользователей. Кроме этого, с помощью Captive-портала можно настроить самостоятельную регистрацию пользователей с подтверждением идентификации через SMS или e-mail.

Следует помнить, что:

- Идентифицированные пользователи, например, у которых в свойствах пользователя явно указан IP-адрес, идентифицированные с помощью агентов авторизации терминальных серверов или для систем Windows, не авторизуются на Captive-портале. Такие пользователи уже относятся к типу **Known users** и не требуют дополнительной идентификации.
- Авторизация с помощью Captive-портала возможна только для протоколов HTTP и HTTPS. Например, если вы создали правило межсетевого экрана, разрешающее доступ в интернет по протоколу FTP только для пользователя **Known users,** то пользователи не смогут получить доступ в интернет по этому протоколу до тех пор, пока они не станут идентифицированными, то есть не запустят у себя браузер и не пройдут авторизацию на Captive-портале.
- Для авторизации пользователей, работающих по протоколу HTTPS, необходимо настроить инспектирование SSL, иначе авторизация работать не будет.
- Если Captive-портал использует метод авторизации Active Directory, то пользователь должен указывать в качестве логина свое доменное имя в формате DOMAIN\username или username@domain.

Настройка Captive-портала сводится к следующим шагам:

Наименование	Описание
Шаг 1. Создать метод авторизации, например, авторизация с помощью домена Active Directory.	В консоли NGFW в разделе **Пользователи и устройства → Серверы аутентификации** нажать на кнопку **Добавить** и создать сервер авторизации.
Шаг 2. Создать профиль аутентификации, в котором указать необходимые методы авторизации.	В консоли NGFW в разделе **Пользователи и устройства → Профили аутентификации** нажать на кнопку **Добавить** и создать профиль авторизации, используя созданный ранее метод авторизации.
Шаг 3. Создать Captive-профиль, в котором указать необходимые профили аутентификации.	В консоли NGFW в разделе **Пользователи и устройства → Captive-профили** нажать на кнопку **Добавить** и создать Captive-профиль, используя созданный ранее профиль авторизации.
Шаг 4. Создать правило Captive-портала.	Правило Captive-портала определяет трафик, к которому должны быть применены методы идентификации пользователей, указанные в Captive-профиле. В консоли NGFW в разделе **Пользователи и устройства → Captive-портал** нажать на кнопку **Добавить** и создать правило Captive-портала.
Шаг 5. Настроить DNS для доменов auth.captive и logout.captive.	Служебные доменные имена **auth.captive** и **logout.captive** используются NGFW для авторизации пользователей. Если клиенты используют в качестве DNS-сервера NGFW, то ничего делать не надо. В противном случае необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса NGFW, который подключен в клиентскую сеть. Альтернативное решение — настроить параметры **Домен auth captive-портала** и **Домен logout captive-портала**. Более детально эти параметры описаны в разделе Общие настройки.

Создание методов авторизации подробно рассматривалось в предыдущих главах. Рассмотрим более подробно создание Captive-профиля и правил Captive-портала.

Чтобы создать Captive-профиль, необходимо в разделе **Captive-профили** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Название Captive-профиля.
Описание	Описание Captive-профиля.
Шаблон страницы авторизации	Выбрать шаблон страницы авторизации. Создавать страницы авторизации можно в разделе **Библиотеки → Шаблоны страниц**. Если необходимо настроить самостоятельную регистрацию пользователей с подтверждением по SMS или e-mail, то следует выбрать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).
Метод идентификации	Метод, с помощью которого NGFW запомнит пользователя. Возможны 2 варианта: • **Запоминать IP-адрес**. После успешной авторизации пользователя через Captive-портал NGFW запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относятся к данному пользователю. Данный метод позволяет идентифицировать данные, передаваемые по любому из протоколов семейства TCP/IP, но не будет корректно работать при наличии NAT-подключения между пользователями и NGFW. Это рекомендуемое значение, устанавливаемое по умолчанию. • **Запоминать cookie**. После успешной авторизации пользователя через Captive-портал NGFW добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя. Данный метод позволяет авторизовать пользователей, находящихся за NAT-устройством, но авторизуется только протокол HTTP(S) и только в том браузере, в котором происходила авторизация через Captive-портал. Кроме этого, для авторизации HTTPS-сессий пользователя NGFW будет принудительно дешифровать все HTTPS-соединения. Для правил межсетевого экрана пользователь, идентифицированный по cookie, будет всегда определен как **Unknown user.**
Профиль аутентификации	Созданный ранее профиль авторизации, определяющий методы аутентификации.
URL для редиректа	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
Разрешить браузерам запомнить авторизацию	Включает возможность сохранить авторизацию в браузере на указанное время в часах. Для сохранения авторизационной информации используются cookie.
Предлагать выбор домена AD/LDAP на странице авторизации Captive-портала	Если в качестве метода аутентификации используется авторизация с помощью Active Directory, то при включении данного параметра пользователь сможет выбрать имя домена из списка на странице авторизации. Если данный параметр не включен, пользователь должен явно указывать домен в виде DOMAIN\username или username@domain.

Наименование	Описание
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.
HTTPS для страницы аутентификации	Использовать HTTPS при отображении страницы авторизации Captive-портала для пользователей. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. Более подробно о сертификатах смотрите в разделе Управление сертификатами.

Для настройки самостоятельной регистрации пользователей с подтверждением пароля с помощью SMS или e-mail необходимо настроить параметры на вкладке **Регистрация гостевых пользователей**. Следует помнить, что в этом случае необходимо использовать соответствующий тип шаблона (Captive portal: SMS auth/ Captive portal: Email auth).

Наименование	Описание
Профиль оповещения	Профиль оповещения, который будет использоваться для отсылки информации о созданном пользователе и его пароле. Может использоваться 2 типа — SMS и email. Более подробно о создания профиля оповещения смотрите в главе Профили оповещений.
От	Указать, от имени кого будут отправляться оповещения.
Тема оповещения	Тема оповещения (только для email-оповещений).
Письмо оповещения	Тело письма сообщения. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль.
Дата и время окончания	Время, когда учетная запись временного пользователя будет отключена.
Время жизни	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена.
Длина пароля	Определяет длину пароля для создаваемого пользователя.
Сложность пароля	Определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спец. символы.
Группы	Группа для временных пользователей, в которую будут помещены создаваемые пользователи. О группах для временных пользователей читайте в главе Гостевой портал.

Чтобы создать правило Captive-портала, необходимо нажать на кнопку **Добавить** в разделе **Captive-портал** и указать необходимые параметры:

Наименование	Описание
Название	Название правила Captive-портала.
Описание	Описание правила Captive-портала.
Captive-профиль	Выбрать Captive-профиль, созданный ранее. Доступно действие **Не использовать аутентификацию**, при выборе которого авторизация не будет требоваться.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Источник	Адреса источника. В качестве источника можно указать определенную зону, например, зону LAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Адреса назначения. В качестве адресов можно указать определенную зону, например, зону WAN и диапазон адресов IP. Могут быть использованы IP-адреса стран (GeoIP). **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Категории	Категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию.
URL	Списки URL, для которых будет применяться правило.
Время	Время, когда данное правило будет активно.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.

Наименование	Описание
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Таким образом, создав несколько правил Captive-портала, можно настроить различные политики идентификации пользователей для различных зон, адресов, категорий сайтов и времени.

ПримечаниеУсловия, указанные во вкладках правила, применяются согласно логике "И", то есть требуют совпадения всех указанных условий для того, чтобы правило сработало. Если необходимо использовать логику "ИЛИ", то это достигается путем создания нескольких правил.

ПримечаниеПравила применяются в порядке, в котором они отображаются в консоли. Вы можете изменить порядок правил с помощью соответствующих кнопок.

ПримечаниеПри обработке правил применяется только первое сработавшее правило.

В случае, если необходимо сменить пользователя после его авторизации в системе или выйти из системы, необходимо перейти на URL http://logout.captive и нажать на кнопку **Выйти**.

Профили MFA (мультифакторной аутентификации)

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

Мультифакторная аутентификация — это метод идентификации и аутентификации пользователя, где используются два или более различных типа идентификационных данных. Введение дополнительного уровня безопасности обеспечивает более эффективную защиту учетной записи от несанкционированного доступа.

NGFW поддерживает мультифакторную аутентификацию с использованием имени пользователя и пароля в качестве первого типа аутентификации и следующих типов в качестве второго:

- **TOTP** (Time-based One Time Password) токена в качестве второго. TOTP-токен создает одноразовый пароль на основе времени, то есть время является параметром; более подробно о TOTP можно прочитать в https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm. В качестве TOTP-токена могут выступать различные устройства либо программное обеспечение, установленное на смартфоны пользователей, например, Google Authenticator.
- **SMS** — получение одноразового пароля по SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory.
- **Email** — получение одноразового пароля по электронной почте. Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory.

Чтобы настроить мультифакторную аутентификацию, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Настроить авторизацию с помощью Captive-портала.	Мультифакторная авторизация работает только при авторизации пользователей с помощью Captive-портала. Смотрите раздел для подробной информации.
Шаг 2. Создать профиль мультифакторной авторизации.	В разделе консоли **Пользователи и устройства → Профили MFA** создать профиль мультифакторной авторизации. При создании профиля указать необходимые настройки доставки второго фактора авторизации. Возможно создать 3 типа доставки: • **MFA через TOTP** — доставка второго фактора авторизации с помощью токенов TOTP. • **MFA через SMS** — доставка второго фактора авторизации с помощью SMS. • **MFA через email** — доставка второго фактора авторизации с помощью email.

Для способа доставки **MFA через TOTP** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Инициализация TOTP	Для получения токенов TOTP необходимо произвести первоначальную инициализацию устройства или ПО клиента. Для этого требуется ввести уникальный ключ в устройство или ПО клиента. Передать первоначальный код для инициализации TOTP можно следующими средствами: • Показать на странице Captive-портала после первой успешной авторизации. Для этого варианта необходимо выбрать **Показать ключ на странице Captive -портала**. • Выслать с помощью SMS. Для отправки SMS у каждого пользователя должен быть указан номер телефона в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки SMS (профиль SMPP). • Выслать с помощью email Для отправки сообщения у каждого пользователя должен быть указан адрес электронной почты в его локальной учетной записи в NGFW или в доменной учетной записи в Active Directory. Для этого варианта необходимо выбрать подходящий, созданный ранее профиль отсылки email (профиль SMTP).
Показывать QR -код	Показывать QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.

В случае, если пользователь утратил токен, администратор может потребовать повторной инициализации TOTP-токена. Для этого ему необходимо выбрать данного пользователя в списке пользователей (**Пользователи и устройства → Пользователи**) и выбрать действие **Сбросить ключ TOTP**. При следующей авторизации пользователю будет предложено заново проинициализировать свой токен.

Для способа доставки **MFA через SMS** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.
Профиль отправки MFA	Профиль SMPP, который будет использован для отправки паролей с помощью сообщений SMS. Подробно о настройке профилей отсылки сообщений через SMS смотрите в разделе Профили оповещений.
От	Указать, от имени кого будут отправляться оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Для способа доставки **MFA через email** необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля MFA.
Описание	Описание профиля MFA.

Наименование	Описание
Профиль отправки MFA	Профиль SMTP, который будет использован для отправки паролей с помощью сообщений электронной почты. Подробно о настройке профилей отсылки сообщений по электронной почте смотрите в разделе Профили оповещений.
От	Указать, от имени кого будут отправляться оповещения.
Тема	Тема оповещения.
Содержимое	Тело письма сообщения. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль.
Время жизни MFA кода	Срок действия одноразового пароля.

Пользователи терминальных серверов

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation:

Терминальный сервер служит для удаленного обслуживания пользователя с предоставлением рабочего стола или консоли. Как правило, один терминальный сервер предоставляет свой сервис нескольким пользователям, а в некоторых случаях десяткам или даже сотням пользователей. Проблема идентификации пользователей терминального сервера состоит в том, что у всех пользователей сервера будет определен один и тот же IP-адрес, и NGFW не может корректно идентифицировать сетевые подключения пользователей. Для решения данной проблемы предлагается использование специального агента терминального сервиса. Каждому пользователю выделяется диапазон портов, с использованием которых происходит соединение пользователя, т.е. исходные порты подменяются на порты из выделенного для пользователя диапазона.

Агент терминального сервиса должен быть установлен на все терминальные серверы, пользователей которых необходимо идентифицировать. Агент представляет собой сервис, который передает на NGFW информацию о пользователях терминального сервера и об их сетевых соединениях. В силу специфики работы протокола TCP/IP, агент терминального сервиса может идентифицировать трафик пользователей, передаваемый только с помощью TCP и UDP протоколов. Протоколы, отличные от TCP/UDP, например, ICMP, не могут быть идентифицированы.

Для корректной идентификации пользователей, в случае использования на терминальных серверах авторизации Active Directory, требуется настроенный сервер Active Directory коннектор.

Чтобы начать работу с аутентификацией пользователей на терминальных серверах, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис агент аутентификации на необходимой зоне.	В разделе **Сеть → Зоны** разрешить сервис **Агент аутентификации** для той зоны, со стороны которой расположены серверы терминального доступа.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли NGFW в разделе **UserGate → Настройки → Модули** напротив записи **Пароль агентов терминального сервиса** нажать на кнопку **Настроить** и задать пароль агентов терминального сервера.
Шаг 3. Установить агент терминального сервера.	Установить агент терминального сервера на все серверы, для которых необходимо идентифицировать пользователей. При установке следует задать IP-адрес NGFW и заданный на предыдущем шаге пароль.
Шаг 4. Добавить необходимые серверы в консоли NGFW.	В разделе **Пользователи и устройства → Терминальные серверы** необходимо добавить агентов терминального сервера, указав имя и адрес хоста. После получения данных с указанного в настройках хоста и совпадении пароля, указанного в пункте 2, авторизация пользователей будет включена автоматически. При обновлении версии NGFW агенты терминальных серверов, которые ранее отображались в веб-консоли, будут продолжать работать.

UserGate теперь будет получать информацию о пользователях.

Агент терминального сервера позволяет авторизовывать не только доменных, но и локальных пользователей терминального сервера. Для этого необходимо добавить в файл конфигурации (%ALLUSERSPROFILE%\Entensys\Terminal Server Agent\tsagent.cfg) следующий параметр:

LocalDomain = 1

После изменения файла конфигурации сервис терминального агента нужно перезапустить.

Таких пользователей также необходимо добавить в NGFW как локальных. О добавлении пользователей читайте в разделе Пользователи. При добавлении необходимо указать **Логин** в формате: «*имя компьютера_имя пользователя*»; пароль указывать не нужно.

ПримечаниеИмя компьютера должно состоять из букв, цифр и знака подчёркивания. Использование тире в имени компьютера возможно только в том случае, если используются только доменные пользователи.

Параметры терминального сервера могут быть изменены путём внесения изменений в файл конфигурации агента авторизации для терминальных серверов. После внесения изменений агент авторизации необходимо перезапустить.

Ниже представлен список параметров файла tsagent.cfg:

- **TimerUpdate**: периодичность отправки данных (указывается в секундах).
- **MaxLogSize**: максимальный размер журнала работы сервиса (указывается в Мбайт).
- **SharedKey**: пароль для подключения агента.
- **SystemAccounts**: может принимать значения **0** или **1**. При значении параметра **SystemAccounts=1** включает передачу информации о соединениях системных аккаунтов (system, local service, network service) и портах, используемых для соединения, на NGFW.
- **FQDN**: может принимать значения **0** или **1**. Значение параметра **FQDN=1** соответствует использованию FQDN (Fully Qualified Domain Name), например, «example.com» вместо «example».
- **ServerPort**: номер порта NGFW, принимающего соединение от агента авторизации. По умолчанию используется порт UDP:1813.
- **ServerAddress**: IP-адрес устройства UserGate, принимающего соединение от агента авторизации.
- **UserCount**: максимальное количество пользователей.
- **BlockDNS**: может принимать значения **0** или **1**. При **BlockDNS=1** происходит замена порта источника на свободный порт из выделенного для пользователя диапазона при DNS запросе (UDP:53); при **BlockDNS=0** — отправка трафика происходит без замены порта.
- **BlockUDP**: может принимать значения **0** или **1**. Значение параметра **BlockUDP=1** соответствует замене порта источника на свободный порт из выделенного для пользователя диапазона при отправке трафика UDP; при **BlockUDP=0** — отправка трафика происходит без замены порта.
- **ExcludeIP**: в случае, если на терминальном сервере настроены несколько IP-адресов, то все они будут использованы для аутентификации пользователей. Параметр ExcludeIP позволяет ограничить аутентификацию пользователей с определённых IP-адресов терминального сервера:
  - IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
  - Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
  - Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
  - Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP** . Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore** .
- **ExcludePorts**: диапазон, порты из которого не будут подменяться на порты из выделенного для пользователя диапазона портов (диапазон портов указывается следующим образом: **ExcludePorts=port1-port2**).
- **NAT_IP**: необходим при наличии NAT между терминальным сервером и UserGate: замена IP-адреса терминального сервера на один из адресов указанного диапазона. Адреса указываются в следующем виде: **NAT_IP="12.3.4-1.1.1.1;2.2.2.2-5.5.5.5"**.

Для исключения из рассылки определенных адресов и/или подсетей терминальным агентом помимо добавления параметра **ExcludeIP** в файл конфигурации tsagent.cfg он может быть активирован и в реестре сервера следующим образом:

- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать только для данного пользователя.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

Прокси-агент для Windows

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation:

Для пользователей, работающих на операционной системе Windows, существует возможность предоставить доступ в интернет через явно указанный прокси-сервер программам, которые не поддерживают работу через прокси-сервер. Иногда также возникает необходимость предоставить таким программам доступ в интернет в случае, когда NGFW не является шлюзом в интернет по умолчанию для пользовательских компьютеров. Для подобных случаев можно использовать прокси-агент. Прокси-агент пересылает все TCP-запросы, идущие не на локальные адреса, на NGFW, который выступает для них прокси-сервером.

ПримечаниеПрокси-агент не авторизует пользователя на NGFW, таким образом, если необходима авторизация, то потребуется настроить один из способов авторизации пользователей, например, установить агент авторизации для Windows.

Установить прокси-агент возможно вручную либо с использованием политик Active Directory.

Прокси-клиент может быть установлен на пользовательский компьютер под управлением ОС Windows 7/8/10/11 со следующими минимальными требованиями к системе: от 2 ГБ оперативной памяти, процессор с тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске.

Если устанавливаете не политикой, то для настройки агента необходимо создать текстовый файл utmagent.cfg в директории %ALLUSERSPROFILE%\Entensys\UTMAgent\. В файле конфигурации следует указать:

ServerName=10.255.1.1

ServerHttpPort=8090

LocalNetwork=192.168.1.0/24; 192.168.0.0/24; 192.168.30.0/24;

где ServerName и ServerHttpPort — IP-адрес и порт прокси-сервера на NGFW, по умолчанию это порт 8090.

ПримечаниеLocalNetwork — список сетей, которые не нужно направлять в прокси. Сеть интерфейсов машины не направляется в прокси по умолчанию.

Если запрос от программы, установленной на компьютере, происходит на адрес, находящийся в одной подсети с адресом интерфейса компьютера, то этот запрос не перехватывается прокси-агентом и не перенаправляется на адрес прокси-сервера. Аналогично, если какая-либо программа, установленная на этом компьютере, обращается на адрес из подсети, указанной в параметре LocalNetwork, то этот запрос также не перенаправляется агентом на прокси-сервер.

Сервис прокси-агента слушает локальный порт 8080.

После создания или изменения файла конфигурации необходимо перезапустить сервис прокси-агента.

Если вы устанавливаете через GPO, прокси-агент поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft

Все необходимые параметры для корректной работы прокси-агента задаются при настройке групповой политики. При установке параметры вносятся в реестр пользовательского компьютера и имеют приоритет перед файлом .cfg. При удалении агента политикой значения реестра не удаляются, сохраняясь в ветке реестра:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Entensys\UTMAgent

Управление гостевыми пользователями

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

NGFW позволяет создавать списки гостевых пользователей. Данная возможность может быть полезна для гостиниц, публичных Wi-Fi, сетей интернет, где необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время.

Гостевые пользователи могут быть созданы заранее администратором системы или пользователям может быть предоставлена возможность самостоятельной регистрации в системе с подтверждением через SMS или email.

Для создания списка гостевых пользователей администратором необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать администратора гостевых пользователей (опционально).	• В разделе **Администраторы** нажать кнопку **Добавить** и создать профиль администратора, разрешающий **Гостевой портал** для чтения и записи в закладке **Разрешения для веб-консоли**. Данный профиль дает доступ в консоль управления временными пользователями. • Создать учетную запись администратора и назначить ей созданную роль. Более подробно о создании администраторов NGFW смотрите соответствующий раздел руководства.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа гостевых пользователей.	В консоли NGFW в разделе **Группы** нажать на кнопку **Добавить** и создать группу, отметив поле **Группа для гостевых пользователей.** Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Подключиться к консоли управления Гостевого портала.	В браузере перейти на адрес https://IP_NGFW:8001/ta Для авторизации необходимо использовать логин и пароль администратора устройства или администратора гостевых пользователей, созданного на шаге 1.
Шаг 4. Создать список пользователей.	В консоли нажать на кнопку **Добавить** и заполнить поля: • Количество пользователей. • Комментарий. • **Дата и время окончания** — время, когда учетная запись гостевого пользователя будет отключена. • **Длина пароля** — определяет длину пароля для создаваемого пользователя. • **Сложность пароля** — определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спецсимволы. • **Время жизни** — продолжительность времени с момента первой авторизации гостевого пользователя, по истечении которого учетная запись будет отключена. • **Группа** — созданная на шаге 2 группа, в которую будут помещены создаваемые пользователи.

Список созданных пользователей можно посмотреть в разделе **Пользователи** консоли управления временными пользователями.

Для самостоятельной регистрации пользователей в системе необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профиль оповещения SMPP (для подтверждения через SMS) или SMTP (для подтверждения через email).	В разделе **Библиотеки → Профили оповещений** нажать кнопку **Добавить** и создать профиль оповещения SMPP или SMTP. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа временных пользователей.	В консоли NGFW в разделе **Группы** нажать на кнопку **Добавить** и создать группу, отметив поле **Группа для гостевых пользователей.** Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Создать профиль Captive-портала, в котором указать использование профиля оповещений, для отсылки информации о созданной учетной записи.	В разделе **Пользователи и устройства** в подразделе **Captive-профили** создать профиль, указав в нем использование созданного ранее профиля оповещения. Указать в качестве страницы авторизации шаблон **Captive portal: email auth** или **Captive portal: SMS auth,** в зависимости от способа отправки оповещения. Настроить сообщение оповещения, группу, в которую будут помещены временные пользователи, времена действия учетной записи. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений.
Шаг 4. Создать правило Captive-портала, которое будет использовать созданный на предыдущем шаге Captive-профиль.	В разделе **Пользователи и устройства → Captive-портал** создать правило, которое будет использовать созданный ранее Captive-профиль. Более подробно о создании правил Captive-портала смотрите раздел руководства Настройка Captive-портала.

Radius accounting

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: ☑

NGFW может прозрачно аутентифицировать пользователей, уже прошедших аутентификацию на внешнем сервере RADIUS. NGFW не взаимодействует с сервером RADIUS, а только отслеживает информацию RADIUS accounting, перенаправленную от RADIUS клиента. RADIUS accounting содержит информацию об имени и IP-адресе пользователя. Для настройки нужно выполнить следующие шаги:

Наименование	Описание
Шаг 1. Завести пользователя в NGFW.	Завести необходимых локальных пользователей в NGFW. Смотрите раздел Пользователи.
Шаг 2. Разрешить сервис Агент авторизации на требуемой зоне.	В разделе **Сеть → Зоны**, выберите зону, на интерфейс которой планируется отсылать RADIUS-accounting. Разрешите сервис **Агент авторизации**. Более подробно о настройке зон смотрите в разделе Настройка зон.
Шаг 3. Настроить пароль агентов терминального сервиса.	В консоли NGFW в разделе **UserGate → Настройки → Модули** напротив записи **Пароль агентов терминального сервиса** нажмите на кнопку **Настроить** и укажите пароль агента терминального сервиса. Данный пароль будет использоваться в качестве RADIUS secret при настройке сервера RADIUS.
Шаг 4. Добавить источник RADIUS accounting в веб-консоли NGFW.	В разделе **Пользователи и устройства → Терминальные серверы** необходимо добавить источник информации RADIUS accounting, указав имя и IP-адрес хоста.
Шаг 5. Настроить RADIUS accounting.	Настроить отсылку информации RADIUS accounting на NGFW, указав в качестве IP-адреса сервера IP-адрес UserGate, порт — UDP 1813. Указать RADIUS secret, совпадающий с паролем агента для терминального сервера, указанным на шаге 3. Имя пользователя необходимо передавать в атрибуте RADIUS User-Name (type=1), IP-адрес пользователя — в атрибуте RADIUS Framed-IP-Address (type=8), а IP-адрес сервера RADIUS — в атрибуте RADIUS NAS_IP_Address (type=4). Более подробно о настройке сервера RADIUS смотрите в руководстве на используемый вами сервер RADIUS и RADIUS клиент. **Важно!** Период обновления информации RADIUS accounting должен быть не более 120 секунд.

После выполнения данной настройки, NGFW будет сопоставлять имя пользователя и присылаемый сервером RADIUS accounting IP-адрес пользователя. В зависимости от передаваемой информации NGFW будет вести себя следующим образом:

Наименование	Описание
RADIUS сервер прислал имя пользователя, который не заведен на NGFW.	На Accounting-запрос будет ответ Accounting reject. Данные о пользователях не изменятся.
RADIUS сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Start или Interim-Update.	Указанному пользователю присвоится переданный IP-адрес. Имя пользователя начнет отображаться в журналах для данного IP-адреса. Пользовательские правила начнут применяться для трафика данного IP-адреса. Если у пользователя уже был IP-адрес, отличный от переданного, то пользователю будет присвоено 2 и более IP-адресов. Если пользователю уже присвоен данный IP-адрес, то ничего не происходит. Если этот IP-адрес присвоен другому пользователю, то он будет удален у того пользователя и будет присвоен пользователю, указанному в запросе.
RADIUS сервер прислал имя существующего пользователя и указал тип Acct-Status-Type = Stop.	У указанного пользователя удалится переданный IP-адрес. Имя пользователя перестанет отображаться в журналах для данного IP адреса. Пользовательские правила перестанут применяться для трафика данного IP-адреса.

Агент аутентификации для Windows

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation:

Для пользователей, работающих на операционной системе Windows, входящих в домен Active Directory, существует еще один способ аутентификации — использовать специальный агент аутентификации. Агент представляет собой сервис, который передает на NGFW информацию о пользователе, его имя и IP-адрес, соответственно, NGFW будет однозначно определять все сетевые подключения данного пользователя, и аутентификация другими методами не требуется. Чтобы начать работу с пользователями посредством агента аутентификации, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис агент аутентификации на необходимой зоне.	В разделе **Сеть → Зоны** разрешить сервис **Агент аутентификации** для той зоны, со стороны которой находятся пользователи.
Шаг 2. Задать пароль агентов терминального сервера.	В консоли NGFW в разделе **UserGate → Настройки → Модули** напротив записи **Пароль агентов терминального сервиса** нажать на кнопку **Настроить** и задать пароль агентов терминального сервера.
Шаг 3. Установить агент аутентификации.	Установить агент аутентификации на все компьютеры, для которых необходимо идентифицировать пользователей. Агент аутентификации может быть установлен на пользовательский компьютер под управлением ОС Windows 7/8/10/11 со следующими минимальными требованиями к системе: от 2 ГБ оперативной памяти, процессор с тактовой частотой не ниже 2 ГГц и 200 Мб свободного пространства на жестком диске. Агент аутентификации поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. С помощью административного шаблона администратор может задать IP-адрес и порт сервера UserGate, и заданный на предыдущем шаге пароль. Более подробно о развертывании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft. Агент может быть установлен и без использования групповых политик. Для этого необходимо установить агент из инсталлятора и указать необходимые параметры для подключения к серверу UserGate в следующих ключах реестра: [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client] "ServerIP"="" "ServerPort"="1813" "SharedKey"=""

NGFW теперь будет получать информацию о пользователях. В политиках безопасности можно использовать имена пользователей, как они указаны в Active Directory, для этого необходим настроенный LDAP-коннектор. Если коннектор не настроен, то можно использовать пользователей **Known** и **Unknown**.

ПримечаниеВ параметрах агента в качестве адреса назначения «ServerIP» следует указывать IP-адрес интерфейса UserGate NGFW, на который поступают запросы агента, или FQDN, разрешающийся в этот IP-адрес.
Примечание Журнал агента аутентификации можно найти здесь:
\Users\<username>\AppData\Roaming\Entensys\Entensys Auth Client\entsagent.log

Установленный агент аутентификации отсылает информацию обо всех IP-адресах, назначенных на интерфейсы устройства. В некоторых сценариях может возникнуть необходимость исключать из этой информации определенные IP-адреса с помощью указания сети или диапазона в настройках агента.

Исключить рассылку определенных адресов и/или подсетей агентом аутентификации можно с помощью параметра **ExcludeIP.** Параметр ExcludeIP может иметь следующие настройки:

- IP-адреса в формате x.x.x.x и/или адреса подсетей в формате x.x.x.x/n, указываются через точку с запятой (например, **ExcludeIP=x.x.x.x/n; x.x.x.x**).
- Допускается использование пробелов между адресами в списке, они игнорируются (например, **ExcludeIP=x.x.x.x/n; x.x.x.x;y.y.y.y**).
- Если в строке есть ошибки в написании адресов, они будут отражены в логах при старте агента. Будут использованы только правильно указанные адреса. Количество используемых адресов из списка записывается в лог при старте агента.
- Если в результате фильтрации будут исключены все адреса из рассылки, то делается запись в лог (один раз) в виде: **GetIPAddressList: IP list is blocked by ExceptIP** . Если позже будет сформирована непустая рассылка, то делается запись в лог в виде: **GetIPAddressList: IP list is not blocked by ExceptIP anymore** .

Параметр ExcludeIP может быть активирован в системе несколькими способами:

- Добавлен в файл конфигурации агента tsagent.cfg, который создается в разделе: \users\<username>..ApplicationData\Entensys. После внесения изменений агент аутентификации необходимо перезапустить В этом случае настройки параметра будут действовать только для пользователя, под учетной записью которого создан файл.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать только для данного пользователя.
- Добавлен в качестве строкового параметра в ветку реестра Windows [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client]. В этом случае настройки параметра будут действовать для всех пользователей данной системы.

Порядок поиска настроек параметра ExcludeIP в системе следующий: сначала параметр ищется в ветке реестра [HKEY_LOCAL_MACHINE\Software\Policies\Entensys\Auth Client], затем в ветке реестра [HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client], затем в файле tsagent.cfg.

Политики сети

Описание

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Раздел **Политики сети** содержит следующие подразделы:

- Межсетевой экран.
- NAT и маршрутизация.
- Балансировка нагрузки.
- Пропускная способность.

С помощью политик сети администратор может настроить необходимый доступ в интернет для своих пользователей, опубликовать внутренние ресурсы сети в интернете, управлять скоростью передачи данных для определенных сервисов и приложений.

ПримечаниеПравила, созданные в данных разделах, применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила.

Для предоставления пользователям доступа в интернет необходимо:

Наименование	Описание
Шаг 1. Создать правило NAT (опционально).	Если необходима подмена адресов трафика. Смотрите раздел NAT и маршрутизация.
Шаг 2. Создать разрешительное правило межсетевого экрана.	Смотрите раздел Межсетевой экран.

Для публикации внутреннего ресурса в интернете необходимо:

Наименование	Описание
Шаг 1. Создать правило DNAT или правило reverse-прокси.	Смотрите раздел Правила DNAT и Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси.

Чтобы указать для определенного сервиса или адреса выход в интернет через альтернативного провайдера, необходимо:

Наименование	Описание
Шаг 1. Создать правило Policy-based routing.	Смотрите раздел Policy-based routing.

Для того чтобы запретить или разрешить определенный тип трафика, проходящий через UserGate, необходимо:

Наименование	Описание
Шаг 1. Создать правило межсетевого экрана.	Смотрите раздел Межсетевой экран.

Для того чтобы распределить трафик между несколькими внутренними серверами, необходимо:

Наименование	Описание
Шаг 1. Создать правило Балансировки нагрузки.	Смотрите раздел Балансировка нагрузки.

Для того чтобы ограничить скорость для определенного сервиса или приложения, необходимо:

Наименование	Описание
Шаг 1. Создать правило Пропускной способности.	Смотрите раздел Пропускная способность.

Межсетевой экран

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через NGFW. В качестве условий правила могут выступать зоны и IP-адреса источника/назначения, пользователи и группы, сервисы и приложения.

События срабатывания правил межсетевого экрана отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила, то любой транзитный трафик через NGFW запрещен.

Чтобы создать правило межсетевого экрана, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Межсетевой экран** и указать необходимые параметры.

Для срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	**Запретить**: блокирует трафик. **Разрешить**: разрешает трафик.
Отбросить и	Настройка данного параметра доступна для правил, блокирующих трафик (выбрано действие **Запретить**). Параметр может принимать одно из следующих значений: • **Не выбран**. • **Посылать ICMP host unreachable**: блокировка трафика с отправкой ICMP-сообщения. • **Посылать TCP reset**: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. **Важно!** При выборе действия **Посылать TCP reset** необходимо указание сервиса (вкладка **Сервис**), использующего протокол TCP. • **Посылать TCP reset в обе стороны**: блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. **Важно!** Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Журналировать каждый пакет**. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP или HTTPS.

Наименование	Описание
Приложения	Список приложений, для которых применяется данное правило. Определение приложения происходит после установления соединения между клиентом и сервером и передачи трафика в обоих направлениях. Максимальный объём такого трафика - 1 Кбайт. Поэтому правило, разрешающее приложение, будет применяться к любому трафику, подходящему под другие критерии правила, пока приложение не будет определено. Аналогично, срабатывание блокирующего правила (разрыв сессии), которое в качестве одного из условий использует приложение, произойдёт только после определения приложения.
Время	Интервалы времени, когда правило активно.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний, а также таблица срабатываний по приложениям. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

NAT и маршрутизация

Documentation:
Product: NGFW
Version: 7.0.1

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, DNAT, Порт-форвардинга, Policy-based routing и Network mapping. NGFW поддерживает NAT/DNAT для сложных протоколов, которые могут использовать динамические порты для своей работы. Поддерживаются протоколы FTP, PPTP, SIP, H323.

События срабатывания правил NAT, DNAT, порт-форвардинга, Policy-based routing и Network mapping отображаются в журнале трафика (**Журналы и отчёты → Журнал трафика**) при включении опции **Журналирование** в параметрах правил.

ПримечаниеGeoIP не может использоваться в качестве адреса источника трафика в правилах NAT и в качестве адреса назначения трафика в правилах NAT, DNAT и порт-форвардинг.

Правила NAT

Как правило, для предоставления пользователям доступа в интернет необходимо создать хотя бы одно правило NAT из зоны **Trusted** в зону **Untrusted**.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.
ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило NAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **NAT**.
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, то система будет использовать первый адрес из списка доступных IP-адресов, назначенных интерфейсам зоны назначения. Допускается указание диапазона IP-адресов, например: 192.168.10.10-192.168.10.20 В этом случае NGFW будет использовать все указанные адреса при Source NAT. Рекомендуется явно указывать SNAT IP для повышения производительности работы межсетевого экрана.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Флажок **Инвертировать** не влияет на работу при использовании мак адресов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

ПримечаниеРекомендуется создавать общие правила NAT, например, правило NAT из локальной сети (обычно зона Trusted) в интернет (обычно зона Untrusted), а разграничение доступа по пользователям, сервисам, приложениям осуществлять с помощью правил межсетевого экрана.

Правила DNAT

Правила DNAT обычно используются для публикации внутренних ресурсов сети в интернет. Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси. Более подробно о публикации ресурсов с помощью правил reverse-прокси описано в главе Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси. Для публикации серверов, работающих по протоколам, отличным от HTTP/HTTPS, необходимо использовать публикацию DNAT.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения

порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило DNAT, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **DNAT**.
SNAT IP (внешний адрес)	Явно указывает IP-адрес, на который будет заменен адрес источника. Если SNAT IP не указан, то адрес источника будет заменён на адрес интерфейса NGFW, с которого отправлен пакет. Допускается указание диапазона IP-адресов, например: 192.168.10.10-192.168.10.20 **Важно!** Для замены адреса источника на указанный адрес необходимо во вкладке **DNAT** активировать Флажок **Включить SNAT**.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Флажок **Инвертировать** не влияет на работу при использовании мак адресов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Один из внешних IP-адресов NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Сервис	Тип сервиса, который необходимо опубликовать, например, HTTP. Если не указан сервис, то будут опубликованы все сервисы. **Важно!** Нельзя опубликовать сервисы, которые используют следующие порты, поскольку они используются внутренними сервисами UserGate: 2200, 8001, 4369, 9000-9100.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернет.
Включить SNAT	При включении данной опции NGFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Правила порт-форвардинга

Правила порт-форвардинга работают аналогично правилам DNAT за исключением того, что эти правила позволяют изменить номер порта, по которому публикуется внутренний сервис. Чтобы создать правило порт-форвардинга, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **Порт-форвардинг**.

Наименование	Описание
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Флажок **Инвертировать** не влияет на работу при использовании мак адресов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов.
Порт-форвардинг	Переопределения портов публикуемых сервисов: • **Оригинальный порт назначения** — номер TCP/UDP-порта, на который пользователи шлют запросы. **Важно!** Нельзя использовать следующие порты, поскольку они используются внутренними сервисами NGFW: 2200, 8001, 4369, 9000-9100. • **Новый порт назначения** — номер TCP/UDP-порта, на который будут пересылаться запросы пользователей на внутренний публикуемый сервер.
Адрес назначения DNAT	IP-адрес компьютера в локальной сети, который публикуется в интернете.
Включить SNAT	При включении данной опции NGFW будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Policy-based routing

Правила policy-based routing обычно используются для указания определенного маршрута в интернет для определенных хостов и/или сервисов. Например, в организации используются 2 провайдера и необходимо весь HTTP-трафик пересылать через провайдера 1, а весь остальной — через провайдера 2. Для этого необходимо указать в качестве шлюза по умолчанию в интернет-шлюз провайдера 2 и настроить правило policy-based routing для HTTPS-трафика через шлюз провайдера 1.

ПримечаниеПравила PBR не заменяют и не влияют на работу правил NAT. Для трансляции адресов, после правила PBR необходимо поставить соответствующее правило NAT.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило policy-based routing, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **Policy-based routing**.
Шлюз	Выбор одного из существующих шлюзов. Вы можете добавить шлюз в разделе **Сеть → Шлюзы**. **Важно!** Выбранный шлюз может относиться к определенному виртуальному маршрутизатору.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет**. В этом случае информация не будет записываться.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Флажок **Инвертировать** не влияет на работу при использовании мак адресов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Network mapping

Правила Network mapping позволяют подменить адрес сети источника или назначения. Как правило, это необходимо, если имеется несколько сетей с одинаковой адресацией, например, 192.168.1.0/24, и их необходимо объединить в единую маршрутизируемую сеть. Без подмены адресов сетей такое объединение совершить невозможно. Network mapping изменяет только адрес сети, оставляя адрес хоста без изменений, например, при замене сети источника с 192.168.1.0/24 на 192.168.2.0/24 хост 192.168.1.1 будет изменен на 192.168.2.1.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Чтобы создать правило **Network mapping**, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → NAT и маршрутизация** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Тип	Выбрать **Network mapping**.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Флажок **Инвертировать** не влияет на работу при использовании мак адресов. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

Наименование	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Network mapping	Задаются параметры подмены сетей. **Направление**: • Входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле **Новая IP-сеть**/**маска**. • Исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в поле **Новая IP-сеть**/**маска.** • **Новая IP-сеть**/**маска** — адрес сети, на которую будет производится замена.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Балансировка нагрузки

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

NGFW позволяет осуществлять балансировку нагрузки на различные сервисы, находящиеся внутри локальной сети. Балансировка может быть предоставлена:

- Для внутренних серверов, публикуемых в интернете (DNAT).
- Для внутренних серверов без публикации.
- Для балансировки трафика, пересылаемого на внешние серверы (ферму) ICAP-серверов.
- Для балансировки трафика на серверы, публикуемые через reverse-прокси.

Балансировщик распределяет запросы, поступающие на IP-адрес виртуального сервера, на IP-адреса реальных серверов, используя при этом различные методы балансировки. Чтобы настроить балансировку, необходимо в разделе **Политики сети → Балансировка нагрузки** создать правила балансировки.

Для создания правила балансировки для серверов TCP/IP необходимо выбрать пункт **Добавить балансировщик TCP/IP** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
IP-адрес виртуального сервера	Необходимо выбрать из списка IP-адресов, назначенных на сетевые интерфейсы. При необходимости администратор может добавить дополнительные IP-адреса на желаемый интерфейс.
Порт	Порт, для которого необходимо производить балансировку нагрузки.
Протокол	Протокол — TCP или UDP — для которого необходимо производить балансировку нагрузки.
Метод балансировки	Возможны 4 различных метода распределения нагрузки на реальные серверы: • **Round robin**: каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • **Weighted round robin**: работает аналогично Round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. • **Least connections**: новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений. • **Weighted least connections**: работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.
Реальные серверы	Добавляется пул реальных серверов, на которые перенаправляется трафик. Для каждого из серверов необходимо указать: • **IP-адрес** сервера. • **Порт** сервера. Порт, на который пересылать запросы пользователей. • **Вес**. Данный коэффициент используется для неравномерного распределения нагрузки на реальные серверы для режимов балансировки **weighted round robin** и **weighted least connections**. Чем больше вес, тем больше будет нагрузка на сервер. • **Режим**. Может быть три варианта: ◦ **Шлюз**: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ **Маскарадинг**: для перенаправления трафика на виртуальный сервер используется DNAT ◦ **Маскарадинг с подменой IP-источника (SNAT)** : аналогично маскарадингу, но при этом NGFW подменяет IP-адрес источника на свой. **Внимание!** Поскольку в режиме *Шлюз* балансировщик не изменяет заголовки пакетов, то обратный трафик от реального сервера должен обеспечиваться средствами маршрутизации. Т.е. шлюз для обратного трафика должен отличаться от адреса NGFW.
Аварийный режим	Аварийный режим используется, когда не доступен ни один из реальных серверов. Для активации аварийного режима необходимо включить его и указать: • **IP-адрес** сервера. • **Порт** сервера. Порт, на который пересылать запросы пользователей. • **Режим**. Может быть три варианта: ◦ **Шлюз**: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ **Максарадинг**: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ **Маскарадинг с подменой IP-источника (SNAT)** : аналогично маскарадингу, но при этом NGFW подменяет IP-адрес источника на свой.
Мониторинг	С помощью мониторинга можно настроить проверку реальных серверов на определение их работоспособности. Если проверка прошла неуспешно для реального сервера, он исключается из балансировки.
Режим	Способ мониторинга реальных серверов. Возможны варианты: • **ping** — проверить доступность узла с помощью утилиты ping. • **connect** — проверить работоспособность узла, установив TCP-соединение на определенный порт. • **negotiate** — проверить работоспособность узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. Для настройки этого режима следует выбрать тип сервиса (HTTP или DNS), строки **Запрос** и **Ожидаемый ответ.** Например, для HTTP-запроса: ◦ Запрос: /robots.txt ◦ Ожидаемый ответ: Disallow: /bin/ Строка запроса тут указывает на путь на реальных серверах, который будет использован в HTTP-запросе. Строка ожидаемого ответа содержит фрагмент возвращаемой веб-страницы.

Наименование	Описание
Интервал проверки	Интервал времени, через который должна выполняться проверка.
Время ожидания	Интервал времени ожидания ответа на проверку.
Число неудачных попыток	Количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки.

ПримечаниеПравила балансировки имеют более высокий приоритет и применяются до правил NAT/DNAT/Маршрутизации.

Балансировщик серверов ICAP позволяет распределить нагрузку на внешние серверы или ферму серверов ICAP, например, на внешнюю ферму серверов с антивирусным ПО. Данный балансировщик затем может быть использован в правилах ICAP. Для создания балансировщика серверов ICAP необходимо выбрать пункт **Добавить балансировщик ICAP** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
ICAP-профили	Выбрать ICAP-профили серверов, на которые будет распределяться нагрузка. Более подробно о работе с серверами ICAP читайте в разделе Работа с внешними ICAP-серверами.

Балансировщик серверов reverse-прокси позволяет распределить нагрузку на внутренние серверы или ферму серверов, публикуемую с помощью правил reverse-прокси. Данный балансировщик затем может быть использован в правилах reverse-прокси. Для создания балансировщика reverse-прокси необходимо выбрать пункт **Добавить балансировщик reverse-прокси** и указать следующие параметры:

Наименование	Описание
Включен	Включает или отключает данное правило.
Название	Название правила балансировки.
Описание	Описание правила балансировки.
Reverse-прокси профили	Выбрать reverse-прокси профили серверов, на которые будет распределяться нагрузка. Более подробно о публикации с помощью reverse-прокси читайте в разделе Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси.

Пропускная способность

Documentation: ☑
Product: NGFW
Version: 7.0.1

Правила управления пропускной способностью используются для ограничения канала для определенных пользователей, хостов, сервисов, приложений.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Чтобы создать правило пропускной способности, необходимо нажать на кнопку **Добавить** в разделе **Политики сети → Пропускная способность** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Полоса пропускания	Выбрать одну из полос пропускания. Полоса пропускания может опционально изменять метки приоритизации трафика DSCP. Создать дополнительные полосы пропускания можно в разделе Полосы пропускания.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. **Важно!** Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Журналирование	Записывает в журнал информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Журналировать каждый пакет**. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства. • **Нет**. В этом случае информация не будет записываться.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Пользователи или группы пользователей, к которым применится правило.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP, HTTPS или другой.
Приложения	Список приложений, для которых необходимо ограничить полосу пропускания.
Время	Время, когда данное правило активно.

Политики безопасности

Общие сведения

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1
Product: NGFW

С помощью политик безопасности администратор может:

- Настроить фильтрацию HTTP-контента, например, запретить некоторым пользователям доступ к определенным категориям сайтов в заданное время или настроить антивирусную проверку веб-контента.
- Настроить опции веб-безопасности, например, включить принудительный безопасный поиск и блокировку рекламы.
- Настроить правила инспектирования SSL, например, для всех пользователей расшифровывать HTTPS для категории "Форумы" и для определенной группы — "Социальные сети". После того как HTTPS расшифрован, к нему могут быть применены политики фильтрации контента и веб-безопасности.
- Включить и настроить параметры СОВ.
- Настроить проверку почтовых протоколов SMTP и POP3 на наличие спама.
- Настроить журналирование или блокировку определенных команд АСУ ТП.
- Настроить выборочную передачу трафика на анализ на внешние серверы ICAP, например, на DLP-системы.
- Настроить публикацию HTTP/HTTPS серверов.

События срабатывания данных правил регистрируются в соответствующих журналах статистики.

Правила фильтрации контента, веб-безопасности и инспектирования SSL доступны в журнале веб-доступа (**Журналы и отчёты → Журнал веб-доступа**).

Правила система обнаружения и предотвращения вторжений — в журнале СОВ (**Журналы и отчёты → Журнал СОВ**).

Правила АСУ ТП — в журнале АСУ ТП (**Журналы и отчёты → Журнал АСУ ТП**).

Правила Защита от DoS атак — в журнале трафика (**Журналы и отчёты → Журнал трафика**).

Все правила журналируются только при включении опции **Журналирование** в параметрах правил.

Фильтрация контента

Version: 7.0.1
Product: NGFW
Documentation:

С помощью правил фильтрации контента администратор может разрешить или запретить определенный контент, передаваемый по протоколам HTTP и HTTPS, если настроено инспектирование HTTPS. Более того, NGFW может блокировать HTTPS-трафик без дешифрования контента, но только в случае применения правил блокирования по категориям контентной фильтрации NGFW URL filtering или по спискам URL, в которых указаны только имена хостов. В этих случаях NGFW использует SNI (Server Name Indication), а при отсутствии SNI — значения хоста из SSL-сертификата из пользовательских запросов для определения домена.

В качестве условий правила могут выступать:

- Пользователи и группы.
- Наличие на веб-страницах определенных слов и выражений (морфология).
- Принадлежность сайтов категориям.
- URL.
- Зона и IP-адрес источника.
- Зона и IP-адрес назначения.
- Тип контента.
- Информация о реферере.
- Время.
- Useragent браузера пользователя.
- HTTP-метод.

ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЕсли не создано ни одного правила, то передача любого контента разрешена.

Чтобы создать правило контентной фильтрации, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Фильтрация контента** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	**Запретить** — блокирует веб-страницу. **Предупредить** — предупреждает пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал. **Разрешить** — разрешает посещение.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Проверять потоковым антивирусом UserGate	Доступно только для правил с действием **Запретить**, т.е. при наличии вируса на странице ресурс будет запрещен. Если в правиле присутствуют другие условия (категории, время, и т.д.), то антивирусная проверка будет выполняться только при совпадении всех условий правила.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. **Важно!** Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Страница блокировки	Указывает страницу блокировки, которая будет показана пользователю при блокировке доступа к ресурсу. Можно использовать внешнюю страницу, указав **Использовать внешний URL**, либо указать страницу блокировки NGFW. В этом случае можно выбрать желаемый шаблон страницы блокировки, который можно создать в разделе Шаблоны страниц.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

Наименование	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Категории	Списки категорий UserGate URL filtering 4.0. Использование категорий требует наличия специальной лицензии. UserGate URL filtering 4.0 — это крупнейшая база электронных ресурсов, разделенных для удобства оперирования на 72 категории. В руках администратора находится управление доступом к таким категориям, как порнография, вредоносные сайты, онлайн-казино, игровые и развлекательные сайты, социальные сети и многие другие. **Важно!** Начиная с версии UserGate 5.0.6R6 администратор может переопределить категорию на любой сайт, на который, по его мнению, категория назначена не верно или не назначена совсем. Более подробно процедура изменения категории сайта описана в разделе Запросы в белый список. **Важно!** Блокировка по категориям сайтов может быть применена к трафику HTTPS без его дешифрования, но без показа страницы блокировки.
URL	Списки URL. При наличии соответствующей лицензии доступны для использования списки URL, обновляемые разработчиками UserGate, такие, как «Черный список UserGate», «Белый список UserGate», «Черный список Роскомнадзора», «Черный список фишинговых сайтов», «Поисковые системы без безопасного поиска». Администраторы также могут создавать собственные списки URL. Более подробно о работе со списками URL читайте в главе Списки URL. **Важно!** Блокировка по спискам URL может быть применена к трафику HTTPS без его дешифрования, если в списках указаны только имена хостов (доменов), но без показа страницы блокировки.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе Типы контента.
Морфология	Список баз словарей морфологии, по которым будут проверяться веб-страницы. При наличии соответствующей лицензии для использования доступны словари, обновляемые компанией UserGate, в том числе список материалов, запрещенных Министерством Юстиции Российской Федерации, словари по темам «Суицид», «Терроризм», «Порнография», «Нецензурные выражения», «Азартные игры», «Наркотики», «Защита детей ФЗ-436». Словари доступны на русском, английском, немецком, японском и арабском языках. Администраторы также могут создавать собственные словари. Более подробно о работе с морфологическими словарями читайте в главе Морфология.
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари.
Useragent	Useragent пользовательских браузеров, для которых будет применено данное правило. Администратор может добавить необходимые ему Useragent в разделе Useragent браузеров.
HTTP метод	Метод, используемый в HTTP-запросах, как правило, это POST или GET.
Рефереры	Список URL, в котором указаны рефереры для текущей страницы, таким образом правило сработает, если для данной страницы referer совпадет со списком указанных URL. Данный функционал удобно использовать, чтобы, например, разрешить доступ к сетям CDN (Content Delivery Network) только посещая определенные сайты, но запретить открытие контента CDN напрямую.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. **Важно!** При настроенном инспектировании данных, передаваемых по протоколу TLS/SSL, и срабатывании правила контентной фильтрации **Default allow**, созданного по умолчанию, счётчик будет срабатывать только для правила инспектирования SSL. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Веб-безопасность

Version: 7.0.1
Product: NGFW
Documentation:

С помощью раздела **Веб-безопасность** администратор может включить дополнительные параметры веб-безопасности для протоколов HTTP и HTTPS, если настроено инспектирование HTTPS. Доступны следующие параметры:

- Блокировка рекламы. Посещение безопасного сайта может быть связано с принудительным просмотром изображений нежелательного характера, размещенных, например, сбоку на странице. NGFW решает эту проблему, выступая в качестве «баннерорезки».
- Функция «Инжектировать скрипт» позволяет вставить необходимый код во все веб-страницы, просматриваемые пользователем. Инжектируемый скрипт будет вставлен в веб-страницы перед тегом </head>.
- Принудительное включение безопасного поиска для поисковых систем Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube. С помощью данного инструмента блокировка нежелательного контента осуществляется средствами поисковых порталов, что позволяет добиться высокой эффективности, например, при фильтрации откликов на запросы по графическому или видеоконтенту.
- Включение журналирования поисковых запросов пользователей.
- Блокировка приложений социальных сетей. Социальные сети играют большую роль в нашей повседневной жизни, но многие из них предоставляют игровые приложения, использование которых не приветствуется большинством компаний. NGFW может блокировать приложения, не затрагивая при этом обычную функциональность социальных сетей.

В качестве условий правила могут выступать:

- Источник трафика.
- Пользователи и группы.
- Время.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила, то дополнительные функции веб-безопасности не применяются.

Чтобы создать правило контентной фильтрации необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Веб-безопасность** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Блокировать рекламу	Активирует блокировку рекламы. Нажав на **Исключения,** администратор может выбрать URL-список сайтов, для которых блокировать рекламу не требуется.
Инжектор	Позволяет вставить произвольный код во все веб-страницы. Для редактирования вставляемого кода необходимо нажать на кнопку **Код инжектора.**
Безопасный поиск	Принудительно включает функцию безопасного поиска.
История поиска	Активирует запись поисковых запросов пользователей в журнал.
Блокировать приложения социальных сетей	Блокирует приложения в популярных социальных сетях.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Инспектирование туннелей

Version: 7.0.1
Product: NGFW
Documentation: ☑

Раздел позволяет администратору настроить инспекцию данных, передающихся с использованием следующих протоколов туннелирования:

- **GRE** (Generic Routing Encapsulation) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты.
- **GTP-U** (General Packet Radio Service (GPRS) Tunneling Protocol for User Data) — протокол, используемый для переноса пользовательских данных в базовой сети GPRS и между сетью радиодоступа и базовой сетью.
- **Нешифрованный IPsec** (IPsec Null Encryption) — протокол туннелирования для передачи по IPsec-туннелю нешифрованного трафика.

NGFW позволяет производить инспектирование туннелей. При включении данной настройки, все туннели, попадающие под правила инспектирования, будут раскрываться; трафик, передаваемый внутри этих туннелей, будет обрабатываться с помощью правил МЭ, СОВ, L7. После фильтрации трафик будет завернут обратно в туннель и передан по оригинальному адресу назначения.

По умолчанию, в NGFW создана зона для инспектирования туннелей — **Tunnel inspection zone**. Данной зоне будут принадлежать все адреса источников и назначения инкапсулированных в туннель пакетов.

ПримечаниеВсе адреса источников и назначений инкапсулированных в туннель пакетов могут принадлежать только одной зоне.

Включить инспектирование и назначить другую зону для инспектируемых туннелей можно в разделе **UserGate → Настройки** модуль **Зона для инспектируемых туннелей**.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Чтобы создать правило инспектирования туннелей, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование туннелей** и указать необходимые параметры; будут проверяться все туннели, подходящие под заданные условия.

Наименование	Описание
Включено	Включение/отключение правила инспектирования туннелей.
Название	Название правила инспектирования.
Описание	Описание правила инспектирования.
Действие	Действия правила инспектирования: • **Инспектировать**. • **Не расшифровывать**.
Инспектирование туннелей	Выбор типа туннеля, который необходимо инспектировать: • **GRE**. • **GTP-U**. • **Нешифрованный IPsec**.
Вставить	Место вставки создаваемого правила в списке правил — наверх, вниз или выше выбранного существующего правила.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса.

ПримечаниеФлаг *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Инспектирование SSL

Version: 7.0.1
Product: NGFW
Documentation:

С помощью данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу TLS/SSL, это в первую очередь HTTPS, а также почтовые протоколы SMTPS и POP3S. В UserGate используется известная технология man-in-the-middle (MITM), при которой контент расшифровывается на сервере, а затем анализируется.

Инспектирование SSL необходимо для корректной работы правил фильтрации контента и правил веб-безопасности. Дешифрование SMTPS и POP3S необходимо для блокирования спама.

С помощью правил данного раздела можно настроить инспектирование HTTPS только для определенных категорий, например, «Вредоносное ПО», «Анонимайзеры», «Ботнеты» и при этом не расшифровывать другие категории, например, «Финансы», «Правительство» и т.п. Для определения категории сайта используется информация, передаваемая в HTTPS-запросе - **SNI** (Server Name Indication), а если SNI отсутствует, то поле **Subject Name** в сертификате сервера. Содержимое поля **Subject Alternative Name** игнорируется.

После дешифрования данные шифруются сертификатом, выписанным центром сертификации, указанным в разделе **Сертификаты**. Чтобы браузеры пользователя не выдавали предупреждение о подмене сертификата, необходимо добавить сертификат центра сертификации в доверенные корневые сертификаты. Более подробно это описано в разделе Приложение 1. Установка сертификата локального удостоверяющего центра.

Аналогично браузерам пользователя некоторые почтовые серверы и пользовательские почтовые программы не принимают почту, если сертификат был подменен. В этом случае необходимо произвести в почтовых программах настройки, отключающие проверку сертификатов, или добавить исключения для сертификата UserGate. Подробно о том, как это сделать, смотрите в документации на почтовое ПО.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила, то SSL не перехватывается и не дешифруются, соответственно, контент, передаваемый по SSL, не фильтруется.

Чтобы создать правило инспектирования SSL, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование SSL** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Действие	**Расшифровать**. **Не расшифровывать**. **Расшифровать и переслать**. В случае успешной расшифровки трафика SSL/TLS копия трафика будет переслана в соответствии с правилом и профилем инспектирования SSL. При выборе данного действия необходимо указать **Профиль пересылки SSL** (о настройке профилей пересылки читайте в разделе Профили пересылки SSL.
Профиль SSL	Выбор профиля SSL. Параметры, указанные в данном профиле, будут использованы как для установки SSL-соединения от браузера пользователя к серверу UserGate, так и при построении SSL-соединения от сервера UserGate к запрашиваемому веб-ресурсу. Подробно о профилях SSL смотрите в главе Профили SSL.
Блокировать сайты с некорректными сертификатами	Позволяет блокировать доступ к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат истек, отозван, выписан на другое доменное имя или не доверяемым центром сертификации.
Проверять по списку отозванных сертификатов	Проверять сертификат сайта в списке отозванных сертификатов (CRL) и блокировать, если он там найден.
Блокировать сертификаты с истекшим сроком действия	Блокировать сертификаты, срок действия которых истек.
Блокировать самоподписанные сертификаты	Блокировать самоподписанные сертификаты.
Пользователи	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идентификации пользователей читайте в главе Пользователи и устройства.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

Наименование	Описание
Адрес назначения	Списки IP-адресов назначения трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса.
Сервис	Сервис, для которого необходимо дешифровать трафик. Может быть HTTPS, SMTPS, POP3S.
Категории	Списки категорий UserGate URL filtering 4.0.
Домены	Списки доменов. Доменные имена, для которых применяется данное правило. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена (www.example.com, а не http://www.example.com/home/). Более подробно о работе со списками URL читайте в главе Списки URL.
Время	Время, когда правило активно. Администратор может добавить необходимые ему временные интервалы в разделе Календари.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

По умолчанию создано правило инспектирования **SSL Decrypt all for unknown users**, которое необходимо для авторизации неизвестных пользователей через Captive-портал.

Инспектирование SSH

Documentation: ☑
Product: NGFW
Version: 7.0.1

При помощи данного раздела администратор может настроить инспекцию данных, передаваемых по протоколу SSH (Secure Shell). SSH также позволяет создавать шифрованные туннели для практически любых сетевых протоколов.

Правила данного раздела могут инспектировать SSH-трафик для определённых пользователей и/или их групп, зон и адресов источников и получателей данных, а также типов сервисов, передаваемых через SSH-туннель. Имеется календарь для применения каждого правила в выбранные дни недели и время суток.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеЕсли не создано ни одного правила или все правила отключены, то SSH не перехватывается и не дешифруется, то есть передаваемые по SSH данные не инспектируются.

Чтобы включить возможность инспектирования контента SSH необходимо:

Наименование	Описание
Шаг 1. Разрешить сервис SSH-прокси на необходимой зоне.	В разделе **Сеть → Зоны** разрешить сервис **SSH-прокси** для той зоны, со стороны которой будет инициирован трафик SSH.
Шаг 2. Создать необходимые правила инспектирования SSH.	Правило инспектирования SSH определяет критерии и действия, применяемые к трафику SSH.

Чтобы создать правило инспектирования SSH, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Инспектирование SSH** и указать необходимые параметры.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Расшифровывать или не расшифровывать передаваемые данные.
Записывать в журнал правил	Регистрировать срабатывание правила в соответствующем журнале статистики (лог-файле).
Блокировать удаленный запуск shell	Не разрешать удаленному пользователю запуск shell (интерпретатора командной строки, оболочки).
Блокировать удаленное выполнение по SSH	Не разрешать удаленному пользователю выполнение любых команд и скриптов по SSH.
Редактировать команду SSH	Команда linux, которую требуется передать, в формате ssh user@host 'command' Например, ssh root@192.168.1.1 reboot
Блокировать SFTP	Блокировать соединение SFTP (Secure File Transfer Protocol).
Вставить	Место вставки создаваемого правила в списке правил - наверх, вниз или выше выбранного существующего правила.
Пользователи	Список пользователей и групп, для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для применения правил к конкретным пользователям или к пользователям типа Known необходимо настроить идентификацию пользователей. Подробнее об идентификации пользователей читайте в главе Пользователи и устройства.
Источник	Зоны и/или списки IP-адресов источника трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса.
Адрес назначения	Списки IP-адресов назначения трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. Более подробно о работе со списками IP-адресов читайте в главе IP-адреса.
Сервис	Сервис, для которого необходимо дешифровать трафик. Поле обязательно для заполнения.

Наименование	Описание
Время	Временной интервал, в течение которого правило активно. Можно добавить разнообразные периоды в разделе Календари.
Использование	Статистика срабатывания данного правила: общее количество срабатываний, время первого и последнего срабатываний. Чтобы сбросить счётчик срабатываний, необходимо выделить правила в списке и нажать **Сбросить счётчики**.
История	Время создания и последнего изменения правила, а также записи журнала событий, относящиеся к данному правилу: добавление, обновление правила, изменение позиции правила в списке и т.п.

Система обнаружения и предотвращения вторжений

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Система обнаружения и предотвращения вторжений (СОВ), или Intrusion Detection and Prevention System (IDPS), позволяет распознавать вредоносную активность внутри сети или со стороны интернета. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз, а также предоставление отчетов. Выявление проблем безопасности осуществляется с помощью использования эвристических правил и анализа сигнатур известных атак. База данных правил и сигнатур предоставляется и обновляется разработчиками UserGate при наличии соответствующей лицензии. СОВ отслеживает и блокирует подобные атаки в режиме реального времени. Возможными мерами превентивной защиты являются обрыв соединения, оповещение администратора сети и запись в журнал.

Для начала работы СОВ необходимо:

Наименование	Описание
Шаг 1. Создать необходимые профили СОВ.	Профиль СОВ — это набор сигнатур, релевантных для защиты определенных сервисов. Администратор может создать необходимое количество профилей СОВ для защиты различных сервисов. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты сервиса. Например, для защиты сервиса, работающего по протоколу TCP, не стоит добавлять сигнатуры, разработанные для протокола UDP. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.
Шаг 2. Создать требуемые правила СОВ.	Правила СОВ определяют действие СОВ для выбранного типа трафика, который будет проверяться модулем СОВ в соответствии с назначенными профилями СОВ.

Для настройки профилей СОВ необходимо создать профиль в разделе **Библиотеки → Профили СОВ** и затем добавить в него необходимые сигнатуры. Сигнатуры СОВ поставляются и постоянно обновляются UserGate при наличии соответствующей подписки. Каждая сигнатура имеет определенные поля:

Наименование	Описание
Сигнатура	Название сигнатуры.
Уровень угрозы	Риск сигнатуры по 5-бальной шкале.
Протокол	Протокол, для которого разработана данная сигнатура: • IP. • ICMP. • TCP. • UDP.
ОС	Операционная система, для которой разработана данная сигнатура.

Наименование	Описание
Категория	Категория сигнатуры — группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • adware pup. • attack_response — сигнатуры, определяющие ответы на известные сетевые атаки. • coinminer — скачивание, установка, деятельность известных майнеров. • dns — известные уязвимости DNS. • dos — сигнатуры известных Denial of services атак. • exploit — сигнатуры известных эксплоитов. • ftp — известные FTP-уязвимости. • imap — известные IMAP-уязвимости. • info — потенциальная утечка информации. • ldap — известные LDAP-уязвимости. • malware — скачивание, установка, деятельность известных malware. • misc — другие известные сигнатуры. • netbios — известные уязвимости протокола NETBIOS. • phishing — сигнатуры известных phishing атак. • pop3 — известные уязвимости протокола POP3. • rpc — известные уязвимости протокола RPC. • scada — известные уязвимости протокола SCADA. • scan — сигнатуры, определяющие попытки сканирования сети на известные приложения. • shellcode — сигнатуры, определяющие известные попытки запуска программных оболочек. • smtp — известные уязвимости протокола SMTP. • snmp — известные уязвимости протокола SNMP. • sql — известные уязвимости SQL. • telnet — известные попытки взлома по протоколу telnet. • tftp — известные уязвимости протокола TFTP. • user_agents — сигнатуры подозрительных Useragent. • voip — известные уязвимости протокола VoIP. • web_client — сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • web_server — сигнатуры, определяющие известные попытки взлома различных веб-серверов. • web_specific_apps — сигнатуры, определяющие известные попытки взлома различных веб приложений. • worm — сигнатуры, определяющие сетевую активность известных сетевых червей.
Класс	Класс сигнатуры определяет тип атаки, которая детектируется данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Поддерживаются следующие классы: • arbitrary-code-execution — попытка запуска произвольного кода. • attempted-admin — попытка получения административных привилегий. • attempted-dos — попытка совершения атаки Denial of Service. • attempted-recon — попытка атаки, направленной на утечку данных. • attempted-user — попытка получения пользовательских привилегий. • bad-unknown — потенциально плохой трафик. • command-and-control — попытка общения с C&C центром • default-login-attempt — попытка логина с именем/паролем по умолчанию. • denial-of-service — обнаружена атака Denial of Service. • exploit-kit — обнаружен exploit kit • misc-activity — прочая активность. • misc-attack — обнаружена атака. • shellcode-detect — обнаружен исполняемый код. • string-detect — обнаружена подозрительная строка. • suspicious-login — попытка логина с использованием подозрительного имени пользователя. • trojan-activity — обнаружен сетевой троян. • web-application-attack — обнаружена атака на веб-приложение.
Описание	Более подробное описание сигнатуры.

При добавлении сигнатур в профиль СОВ администратор может использовать гибкую возможность фильтрации сигнатур, например, выбрать только те сигнатуры, которые имеют очень высокий риск, протокол — TCP, категория — botcc, класс — все.

Правила СОВ определяют трафик, к которому применяется профиль СОВ и действие, которое модуль СОВ должен предпринять при срабатывании сигнатуры. При срабатывании сигнатуры доступна запись трафика. Настройка захвата пакетов производится в разделе **UserGate → Настройки → Настройка PCAP** . Загрузка и просмотр файлов PCAP доступны в журнале СОВ.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеФлажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

ПримечаниеПравилами СОВ анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур в любом из направлений производится действие, настроенное в правилах.

ПримечаниеЕсли не создано ни одного правила, то СОВ ничего не анализирует и не защищает от угроз.

Для настройки правил СОВ необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → СОВ** и заполнить поля правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: • **Разрешить** — не блокировать трафик. • **Журналировать** — не блокировать и записать в журнал. • **Запретить** — блокировать и записать в журнал.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут UserGate производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP, DNS или другие.
Профили	Список профилей СОВ, сигнатуры которых будут использованы в данном правиле СОВ. Профили СОВ задаются для правил с действиями **Запретить** и **Журналировать**. Для разрешающих правил задать профиль СОВ невозможно; такая реализация позволяет настроить исключения для определённого типа трафика.
Профили исключения	Список профилей СОВ, сигнатуры которых будут исключены из сигнатур, указанных в профилях в разделе **Профили СОВ**; могут быть использованы только в правилах с действием **Запретить** или **Журналировать**. Данная возможность позволяет использовать централизованно создаваемые профили сигнатур, например, Профиль UserGate, изменять содержимое которых администратор не может, но при этом исключить из этого профиля ряд сигнатур, которые избыточны или создают ложные срабатывания.

Сценарии

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря концепции SOAR (Security Orchestration, Automation and Response). NGFW реализует данную концепцию с помощью механизма сценариев. Сценарий является дополнительным условием в правилах межсетевого экрана и в правилах пропускной способности, позволяя администратору настроить реакцию NGFW на определенные события, произошедшие за некое продолжительное время. Примером работы сценариев могут являться решение следующих задач:

- Заблокировать или ограничить пропускную способность на 30 минут пользователя, у которого за последние 10 минут было обнаружено 5 попыток использования приложения torrent.
- Заблокировать или ограничить пропускную способность пользователя или группы пользователей, указанной в правиле, при срабатывании одного из следующих триггеров — открытие пользователем сайтов, относящихся к группе категорий Threats, срабатывание СОВ сигнатур высокого риска для трафика данного пользователя, блокировка вируса в трафике данного пользователя.
- Заблокировать или ограничить пропускную способность пользователя, если он выбрал лимит трафика в 10 Гб за месяц.

ПримечаниеСценарий является дополнительным условием в правилах межсетевого экрана и в правилах пропускной способности. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.

Для начала работы со сценариями необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать необходимые сценарии.	В разделе **Политики безопасности → Сценарии** создать необходимые сценарии.
Шаг 2. Указать созданные сценарии в правилах межсетевого экрана или в правилах пропускной способности.	Добавить созданный сценарий в правила межсетевого экрана или в правила пропускной способности. Более подробно о работе с правилами межсетевого экрана или пропускной способности смотрите раздел Политики сети.

При создании сценария необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает сценарий.
Название	Название сценария.
Описание	Описание сценария.
Применить для	Возможны варианты: • Одного пользователя — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий. • Всех пользователей — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в поле Пользователи/Группы правила.
Продолжительность	Время в минутах, в течении которого сценарий будет активным после его активации. Столько же будет работать правило межсетевого экрана или пропускной способности, в котором используется данный сценарий.
Условия	Задаются условия срабатывания сценария. Для каждого условия можно указать количество срабатываний за определенное время, необходимое для срабатывания сценария. Если выбрано несколько условий, то необходимо указать, сработают ли сценарий при совпадении одного или всех условий.
Условия срабатывания	Возможны следующие условия для использования в сценарии: • **Категория URL** — совпадения указанных категорий UserGate URLF в трафике пользователя. • **Обнаружен вирус**. • **Приложение** — обнаружено указанное приложение в трафике пользователя. • **СОВ** — сработка системы обнаружения вторжений. • **Типы контента** — обнаружены указанные типы контента в трафике пользователя. • **Размер пакета** — размер пакета в трафике пользователя превысил указанное значение. • **Сессий с одного IP** — количество сессий с одного IP-адреса превысило указанное значение. • **Объем трафика** — объем трафика пользователя превысил определенный лимит за указанную единицу времени. • **Проверка состояния** — проверка состояния какого-либо ресурса, который должен быть доступен с NGFW. Проверка может осуществляться с помощью команды icmp ping, запроса DNS или выполнения HTTP GET.

Работа с внешними ICAP-серверами

Product: NGFW
Documentation: ☑
Version: 7.0.1

Описание

NGFW позволяет передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. В данном случае NGFW будет выступать в роли ICAP-клиента.

NGFW поддерживает гибкие настройки при работе с ICAP-серверами, например, администратор может задать правила, согласно которым на ICAP-серверы будет направляться только выборочный трафик, или настроить работу с фермой ICAP-серверов.

Общие настройки

Для того, чтобы настроить работу NGFW с внешними серверами ICAP, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать ICAP-сервер.	В разделе **Политики безопасности → ICAP-серверы** нажать на кнопку **Добавить** и создать один или более ICAP-серверов.
Шаг 2. Создать правило балансировки на ICAP-серверы (опционально).	В случае, если требуется балансировка на ферму ICAP-серверов, создать в разделе **Политики сети → Балансировка нагрузки** балансировщик ICAP-серверов. В качестве серверов используются ICAP-серверы, созданные на предыдущем шаге.
Шаг 3. Создать правило ICAP.	В разделе **Политики безопасности → Правила ICAP** создать правило, которое будет задавать условия пересылки трафика на ICAP-серверы или фермы серверов. **Важно!** Правила ICAP применяются сверху вниз в списке правил. Срабатывает только первое правило, для которого совпали все условия, указанные в настройках правила.

Для создания ICAP-сервера в разделе **Политики безопасности → ICAP-серверы** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
Название	Название ICAP-сервера.
Описание	Описание ICAP-сервера.
Адрес сервера	IP-адрес ICAP-сервера.
Порт	TCP-порт ICAP-сервера, значение по умолчанию 1344.
Максимальный размер сообщения	Определяет максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
Период проверки доступности сервера ICAP	Устанавливает время в секундах, через которое NGFW посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен.
Пропускать при ошибках	Если эта опция включена, то NGFW не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен (не отвечает на запрос OPTIONS).
Reqmod путь	• **Включено** — включает использование режима Reqmod. • **Путь на сервере ICAP для работы в режиме Reqmod** . Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах: • /path — путь на сервере ICAP; • icap://icap-server:port/path — указание полного URI для режима reqmod.
Respmod путь	• **Включено** — включает использование режима Respmod. • **Путь на сервере ICAP для работы в режиме Respmod** . Задайте путь, в соответствии с требованиями, указанных в документации на используемый у вас ICAP-сервер. Возможно указать путь в форматах: • /path — путь на сервере ICAP; • icap://icap-server:port/path — указание полного URI для режима respmod.
Посылать имя пользователя	• **Включено** — включает отсылку имени пользователя на ICAP-сервер. • **Кодировать в base64** — кодировать имя пользователя в base64, это может потребоваться, если имена пользователей содержат символы национальных алфавитов. • **Название заголовка**, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию — X-Authenticated-User.
Посылать IP-адрес	• **Включено** — включает отсылку IP-адреса пользователя на ICAP-сервер. • **Название заголовка**, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Ip.
Посылать MAC-адрес	• **Включено** — включает отсылку MAC-адреса пользователя на ICAP-сервер. • **Название заголовка**, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию — X-Client-Mac.

Для создания правила балансировки на серверы ICAP в разделе **Политики сети → Балансировка нагрузки** необходимо выбрать **Добавить → Балансировщик ICAP** и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает правило.

Наименование	Описание
Название	Название правила.
Описание	Описание правила.
ICAP-серверы	Список серверов ICAP, на которые будет распределяться нагрузка, созданный на предыдущем шаге.

Для создания ICAP-правила необходимо нажать **Добавить** в разделе **Политики безопасности → ICAP-правила** и заполнить необходимые поля.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.
ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: • **Пропустить** — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. • **Переслать** — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера. Это стандартный режим работы большинства ICAP-серверов. • **Переслать и игнорировать** — переслать данные на ICAP-сервер и игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика.
ICAP-серверы	ICAP-сервер или балансировщик серверов ICAP, куда NGFW будет пересылать запросы.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей, групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей.
Адрес назначения	IP-адреса, GeoIP или списки URL (хостов) назначения трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Типы контента	Списки типов контента. Предусмотрена возможность управления видеоконтентом, аудио контентом, изображениями, исполняемыми файлами и другими типами. Администраторы также могут создавать собственные группы типов контента. Более подробно о работе с типами контента читайте в главе Типы контента.
Категории	Списки категорий UserGate URL filtering.
URL	Списки URL.
HTTP метод	Метод, используемый в HTTP-запросах, как правило, это POST или GET. Если не используется SSL Inspection, то возможно применение метода CONNECT.
Сервис	Возможны варианты: • HTTP — веб-трафик. • SMTP — почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа. • POP3 — почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа. **Важно!** Перед использованием сервисов SMTP и POP3 в правилах ICAP необходимо создать правило защиты почтового трафика для данных сервисов. Подробнее о защите почтового трафика смотрите в разделе Защита почтового трафика.

Работа с несколькими серверами ICAP

UserGate поддерживает работу с несколькими серверами ICAP. В общем случае без балансировки данные передаются на ICAP сервера по порядку их перечисления, в случае если сервер ICAP не отвечает: поведение UserGate зависит от настройки **Действие** в правилах ICAP:

- **Пропустить** - запрос не передаются на ICAP сервер
- **Переслать** - запрос передается на сервер и ожидается ответ, если ответ не поступает, запрос отправляется следующему по списку ICAP серверу.

- **Переслать и игнорировать** - запрос передается на сервер, ответ не ожидается.

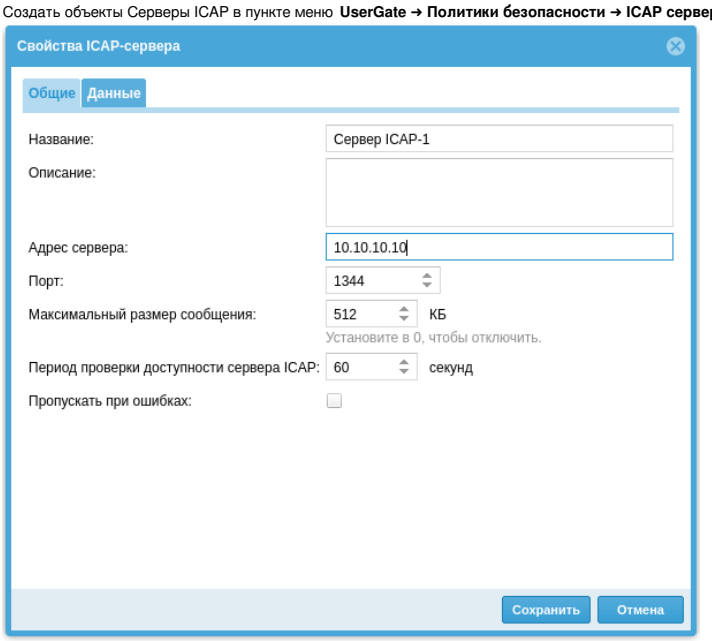
Балансировка нагрузки ICAP серверов

В UserGate возможна балансировка нагрузки на ICAP сервера. Реализовать это возможно двумя способами:

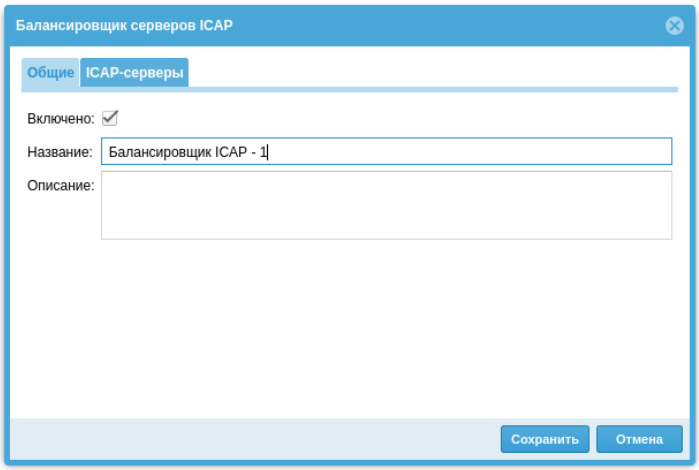
1. Балансировщик ICAP серверов:

Для настройки необходимо:

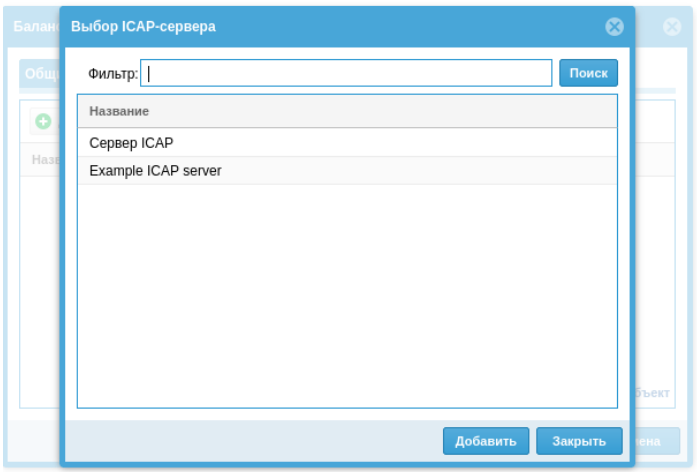
- Создать объекты Серверы ICAP в пункте меню **UserGate → Политики безопасности → ICAP серверы** как указано в примере ниже:



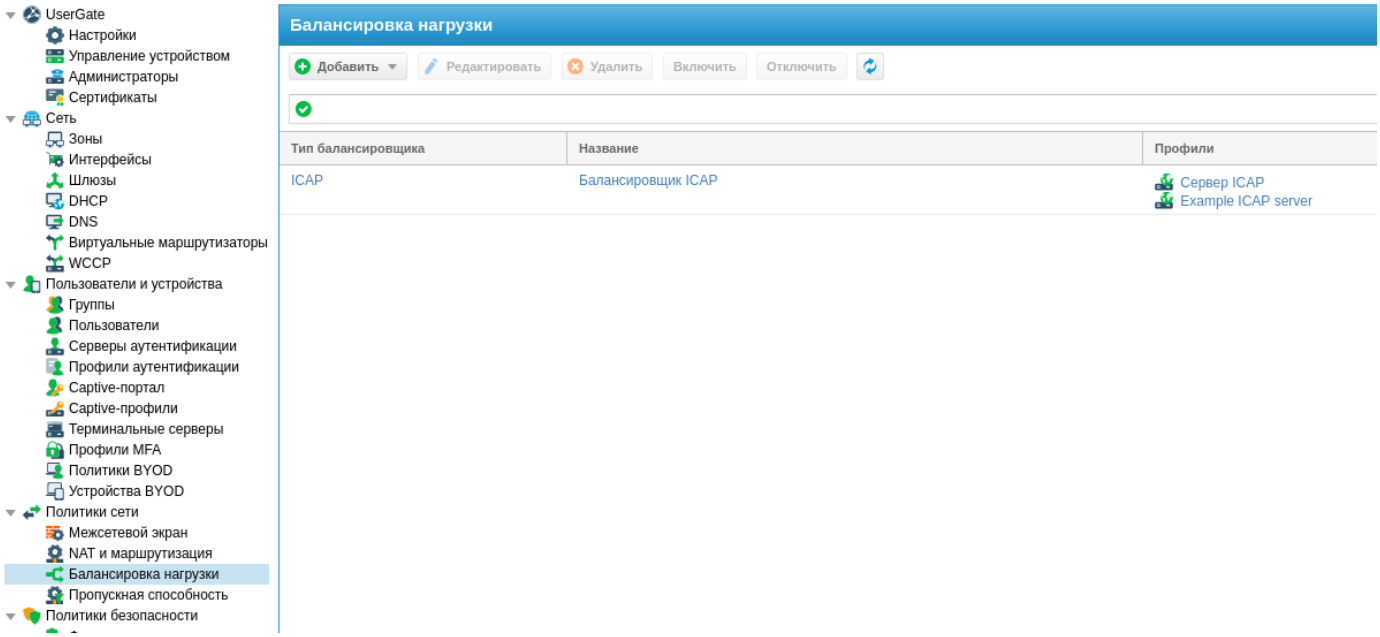
- Создать "Балансировщик ICAP", для этого в пункте **UserGate → Политики сети → Балансировка нагрузки** , следует нажать кнопку **Добавить** и выбрать пункт **Добавить балансировщик ICAP,** далее установить чекбокс **Включено** и ввести название балансировщика:



- Далее на вкладке **ICAP-серверы**, необходимо добавить ранее созданные ICAP серверы используя кнопку **Добавить**:



- И нажать кнопку **Сохранить**. В результате будет создан **Балансировщик ICAP**:



- После этого можно будет выбрать созданный балансировщик в настройке **ICAP-правил**.

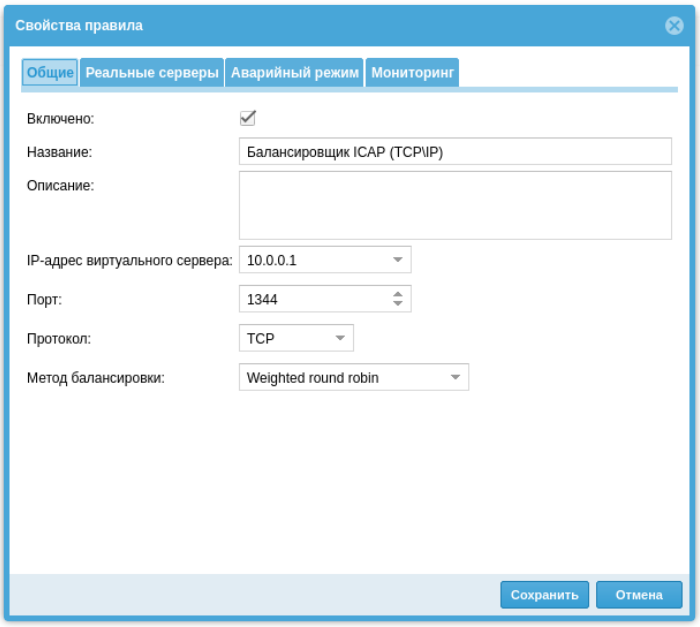
Внимание!Данный способ балансировки не проверяет доступность ICAP серверов участвующих в балансировке. В случае недоступности ICAP серверов, поведение UserGate будет регламентироваться значением настройки *Действие* в ICAP правилах(см. выше).

Балансировка TCP\IP

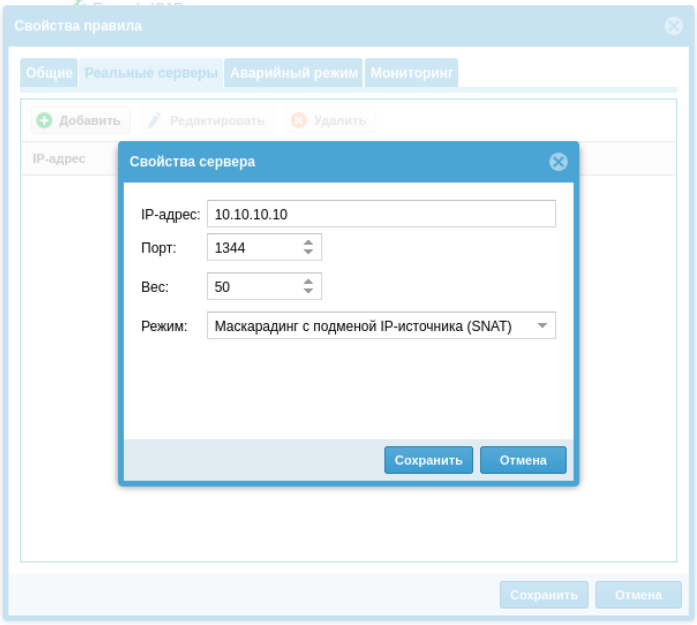
ПримечаниеДанный способ балансировки ICAP серверов является предпочтительным, хоть и более сложным, из-за наличия механизма проверки доступности и аварийного режима.

Второй вариант балансировки серверов ICAP возможен с использованием **Балансировщика TCP\IP**.

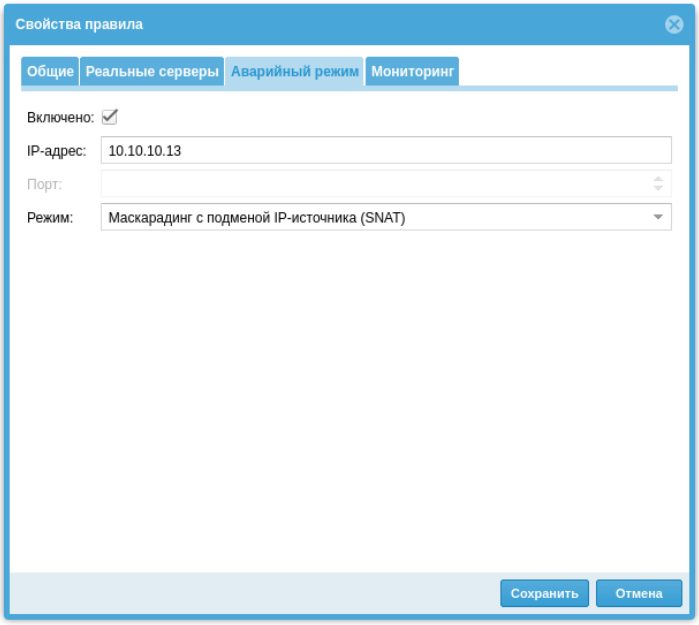
- В меню **UserGate → Политики сети → Балансировка нагрузки** нажимаем кнопку **Добавить** Выбираем **Балансировщик TCP\IP,** укзываем название, виртуальный IP адрес балансировщика (один из интерфейсов UserGate), порт реального сервера ICAP (по умолчанию 1344):



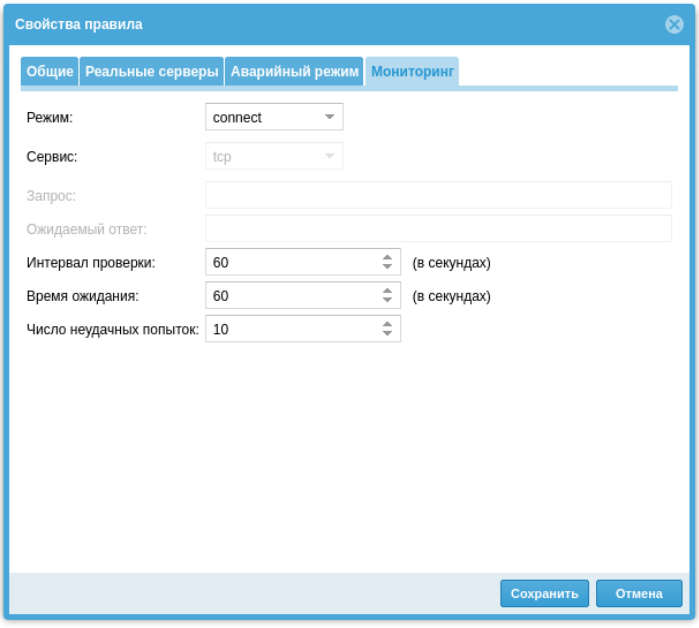
- На вкладке **Реальные серверы** нужно указать IP адреса и порты реальных ICAP серверов, режим работы следует выбрать **Маскарадинг с подменой IP-источника (SNAT)** :



- На вкладке Аварийный режим, можно указать резервный сервер ICAP, который примет запросы в случае недоступности основных серверов ICAP. Пример настройки приведен ниже:



- На вкладке мониторинг можно настроить параметры проверки доступности серверов, участвующих в балансировке, можно выбрать метод, интервал проверки и количество неудачных попыток, для признания узла недоступным. Пример настройки приведен ниже:



ПримечаниеМетод *Connect* проверки сервера позволяет проверить, что сервер отвечает по указанному порту. Это надежнее метода *ping.*

- Теперь можно создать ICAP сервер используя виртуальный IP адрес балансировщика TCP\IP и далее использовать этот сервер в правилах ICAP.

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Защита почтового трафика

При наличии настроенной проверки почтового трафика, NGFW может проверять трафик по протоколам SMTP и POP3. IMAP не поддерживается, в том числе, и при настройке SSL инспектирования. Проверяться может и зашифрованный трафик этих протоколов.

Поддерживается 2 типа проверки:

- блокировка SMTP по наличию IP адреса сервера-отправителя в одной из баз DNSBL; наиболее эффективный метод быстро и с минимальными затратами ресурсов отсечь сообщения от очевидных и явных спамеров;
- маркировка сообщений по результатам проверки на спам; требует наличия также лицензии на модуль Mail security.

Внимание! Блокировка по результатам антиспам проверки НЕ рекомендуется. Рекомендуется принятие решения "спам/не спам" на стороне почтового сервера (или дополнительного антиспам приложения), где маркировка выставляемая NGFW была бы одним из критериев, с большим весом.

Посмотреть статистику работы антиспам модуля можно в дашборде, подключив соответствующие виджеты "Сводные показатели защиты почты" или "Графики защиты почты".

Важно! В журналах работа антиспама не отображается.

В настройках антиспам можно задать как белый, так и черный список IP адресов. Здесь речь идет именно об IP адресах, от которых сразу не будет приниматься соединение (для черных списков) без анализа каких-то дополнительных данных. В самих правилах можно добавлять списки адресов на вкладках envelope from / envelope to. Если в правиле будет стоять действие Блокировать, то это правило будет работать как черный список, если Пропустить — как белый.

В этих списках можно использовать символ * в значении "любой". То есть *@domain.com обозначает все адреса этого домена.

Раздел **Защита почтового трафика** позволяет настроить проверку транзитного почтового трафика на предмет наличия в нем спам-сообщений. Поддерживается работа с почтовыми протоколами POP3(S) и SMTP(S). Защита почтового трафика требует наличия соответствующего модуля в лицензии NGFW.

Как правило, необходимо защищать почтовый трафик, входящий из интернета на внутренние почтовые серверы компании, и, в некоторых случаях, защищать исходящий почтовый трафик от серверов или пользовательских компьютеров.

Для защиты почтового трафика, приходящего из интернета на внутренние почтовые серверы, необходимо:

Наименование	Описание
Шаг 1. Опубликовать почтовый сервер в сеть Интернет.	Смотрите раздел Правила DNAT. Рекомендуется создать отдельные правила DNAT для SMTP и POP3 протоколов, а не публиковать оба протокола в одном правиле. Обязательно укажите в качестве сервиса протокол SMTP, а не TCP.
Шаг 2. Включить поддержку сервисов SMTP(S) и POP3(S) в зоне, подключенной к сети Интернет.	Смотрите раздел Настройка зон.
Шаг 3. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для защиты почтового трафика в случаях, когда не требуется публиковать почтовый сервер, действия сводятся к следующим шагам:

Наименование	Описание
Шаг 1. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Для настройки правил фильтрации почтового трафика необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Защита почтового трафика** и заполнить поля правила.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЕсли не создано ни одного правила, то почтовый трафик не проверяется.

ПримечаниеДля срабатывания правила необходимо, чтобы совпали все условия, указанные в параметрах правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Действие, применяемое к почтовому трафику при совпадении всех условий правила: • **Пропустить** — пропускает трафик без изменений. • **Маркировать** — маркирует почтовые сообщения специальным тэгом в теме письма или дополнительном поле. • **Блокировать с ошибкой** — блокирует письмо, при этом сообщает об ошибке доставки письма серверу SMTP для SMTP(S)-трафика или клиенту POP3 для POP3(S)-трафика. • **Блокировать без ошибки** — блокирует письмо без уведомления о блокировке.
Проверка	Метод проверки почтового трафика: • **Проверка антиспамом UserGate** — проверяет почтовый трафик на наличие спама. • **DNSBL проверка** — антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам.
Заголовок	Поле, куда помещать тег маркировки.
Маркировка	Текст тега, который маркирует письмо.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Назначение	IP-адреса, GeoIP или списки URL (хостов) назначения трафика. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Пользователи или группы пользователей, к которым применяется данное правило.
Сервис	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило.
Envelop from	Почтовый адрес отправителя письма, указанный в поле **Envelope from**. Только для протокола SMTP.
Envelop to	Почтовый адрес адресата письма, указанный в поле **Envelope to**. Только для протокола SMTP.

Рекомендуемые настройки защиты от спама следующие.

Для протокола SMTP(S):

- Первое правило в списке — **блокировка с помощью DNSBL**. Рекомендуется оставить списки **Envelope from**/**Envelope to** пустыми. В этом случае DNSBL будет отбрасывать подключения SMTP-серверов, замеченных в распространении спама, еще на этапе коннекта. При наличии email адресатов в этих списках система будет вынуждена принимать сообщения целиком для анализа этих полей, что увеличит нагрузку на сервер и ухудшит производительность проверки почтового трафика.
- Второе правило — **маркировка** писем с помощью антиспама UserGate. Здесь можно использовать любые исключения, в том числе и по **Envelope from**/**Envelope to**.

Для протокола POP3(S):

- Действие — **Маркировать**.
- Проверка — **Антиспам UserGate**.

Настройки антиспама

Настройки BATV

BATV (Bounce Address Tag Validation) — технология, помогающая различать реальные возвраты писем от возвратов спама.

Подделка адресов отправителей (особенно тех, кто не использует SenderPolicyFramework и YahooDomainKeys для защиты от подделки своих адресов) широко применяется спамерами. Часть спама принимается MX'ами получателей, но при недоставке на следующий сервер — relay может возвращаться отправителю. А так как адрес отправителя поддельный, реальные невинные владельцы адресов получают возврат спама, который не посылали. Также часть писем спам-рассылок маскируется под возвращаемые письма, поскольку некоторые антиспам-проверки предполагают, что возвращаемые письма не могут содержать спам-сообщения, чем и пользуются злоумышленники. Для отличия реальных возвращаемых писем от поддельных и применяется технология BATV.

Отключать прием возвращаемых писем нельзя, т.к. это нарушает связность сети (нормальные письма тоже иногда не доставляются и возвращаются), поэтому требуется как-то отличать нормальные возвраты от возвращаемого чужого спама. Тогда и была предложена технология BATV. Использование BATV может быть полезно в тех системах, где контентные фильтры спама не справляются с детектированием спама в возвращаемых письмах.

Может быть включена, либо выключена. Других настроек не предполагается.

Серверы DNSBL

DNSBL проверка — антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам.
DNSBL или спам-база — это черный список доменных имен и ip-адресов, замеченных в распространении спам сообщений.

Внимание!Появление в этом списке того или иного сервера, не является однозначным признаком принадлежности писем с этого сервера к спам-рассылкам. Частота ложных срабатываний в этой технологии зависит от используемых списков DNSBL и определяется индивидуально. В любом случае, появление сервера в списках DNSBL должно квалифицироваться как дополнительный, но не основной признак спам-рассылки.

В сети существуют десятки различных DNSBL, каждый из которых использует свои собственные критерии для добавления и исключения из своего списка IP адреса или домена. Большинство спам-фильтров используют различные DNSBL для проверки того, чтобы входящие электронные письма не отправлялись с сайтов, доменные имена которых занесены в черный список. Как правило, DNSBL являются первой линией защиты от спама.
Например, в список серверов добавляются адреса серверов DNSBL: cbl.abuseat.org, zen.spamhaus.org и т.д. Белый и черный список добавляет или убирает определенные адреса из этой проверки.

Белый список DNSBL

Список серверов исключенных из DNSBL проверки.

Черный список DNSBL

Список запрещенных серверов в дополнение к тем, что есть списках DNSBL.

Защита от DoS атак

Documentation: ☑
Product: NGFW
Version: 7.0.1

NGFW позволяет гранулировано настроить параметры защиты сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP). Грубая настройка производится в свойствах зон (смотрите раздел Настройка зон), более точная настройка производится в данном разделе. Используя правила защиты DoS, администратор может указать специфические настройки защиты от DoS атак для определенного сервиса, протокола, приложения и т.п. Чтобы создать правила защиты DoS администратору необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профили DoS защиты.	В разделе **Политики безопасности → Профили DoS** нажать на кнопку **Добавить** и создать один или более профилей DoS защиты.
Шаг 2. Создать правила защиты DoS.	В разделе **Политики безопасности → Правила защиты DoS** создайте правила, используя профили защиты, созданные на предыдущем шаге.

Настройка профиля защиты DoS подобна настройке защиты от DoS на зонах NGFW. При создании профиля необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Агрегировать	Данная настройка регулирует, будет ли NGFW суммировать количество пакетов, проходящих в секунду, для всех IP-адресов источника трафика, или будет производить подсчет индивидуально для каждого IP-адреса. В случае активации данной настройки необходимо устанавливать достаточно высокие значения количества пакетов/сек в настройках закладки **Защита DoS** и в закладке **Защита ресурсов**.
Защита DoS	Данная настройка позволяет указать параметры защиты от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • **Порог уведомления** — при превышении количества запросов над указанным значением происходит запись события в системный журнал. • **Порог отбрасывания пакетов** — при превышении количества запросов над указанным значением NGFW начинает отбрасывать пакеты, и записывает данное событие в системный журнал.
Защита ресурсов	Данная настройка позволяет ограничить количество сессий, которые будут разрешены для защищаемого ресурса, например, опубликованного сервера: • **Включено**: включает ограничение количества сессий. • **Ограничить число сессий**: задается число сессий.

Чтобы создать правило защиты DoS, необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → Правила защиты DoS** и указать необходимые параметры.

ПримечаниеПравила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

ПримечаниеЧекбокс Инвертировать меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	**Запретить** — безусловно блокирует трафик подобно действию правил Межсетевого экрана. **Разрешить** — разрешает трафик, защита от DoS не применяется. Может быть использовано для создания исключений. **Защитить** — применить профиль защиты от DoS атак.
Профиль DoS	В случае, если выбрано действие **Защитить**, необходимо указать профиль защиты DoS. Если при использовании профиля DoS с защитой ресурсов не использовать дополнительные условия, например адрес назначения, то будут учитываться все транзитные соединения.
Сценарий	Указывает сценарий, который должен быть активным для срабатывания правила. Подробно о работе сценариев смотрите в разделе Сценарии. **Важно!** Сценарий является дополнительным условием. Если сценарий не активировался (не сработали одно или несколько триггеров сценария), то правило не сработает.
Записывать в журнал правил	Записывает в журнал трафика информацию о трафике при срабатывании правила. Возможны варианты: • **Журналировать начало сессии**. В этом случае в журнал трафика будет записываться только информация о начале сессии (первый пакет). Это рекомендуемый вариант журналирования. • **Журналировать каждый пакет**. В этом случае будет записываться информация о каждом передаваемом сетевом пакете. Для данного режима рекомендуется включать лимит журналирования для предотвращения высокой загрузки устройства.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей или групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Более подробно об идеунтификации пользователей читайте в главе Пользователи и устройства.
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Сервис	Тип сервиса, например, HTTP или HTTPS.
Время	Интервалы времени, когда правило активно.

Глобальный портал

Описание

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Веб-портал и reverse-прокси, наряду с правилами DNAT/Порт-форвардинга, позволяют опубликовать ресурсы, находящиеся внутри компании, пользователям из интернета.

При наличии публикаций внутренних ресурсов с помощью DNAT/Порт-форвардинга, Reverse-прокси и веб-портала порядок обработки правил следующий:

1. Правила DNAT/Порт-форвардинга.
2. Правила веб-портала. Если имя хоста в запросе совпало с именем хоста веб-портала, и номер порта в запросе совпал с номером порта, указанного для работы веб-портала, то отрабатывают правила веб-портала.
3. Правила Reverse-прокси.

Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Для публикации серверов HTTP/HTTPS рекомендуется использовать публикацию с помощью правил reverse-прокси.

В отличие от публикации с помощью правил DNAT, публикация с использованием reverse-прокси предоставляет следующие преимущества:

- Публикация по HTTPS серверов, работающих по HTTP и наоборот.
- Балансировка запросов на ферму веб-серверов.
- Возможность ограничения доступа к публикуемым серверам с определенных Useragent.
- Возможность подмены доменов и путей публикуемых серверов.

Чтобы опубликовать сервер, используя reverse-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервер reverse-прокси.	В разделе **Глобальный портал → Серверы reverse-прокси** нажать на кнопку **Добавить** и создать один или более публикуемых веб-серверов.
Шаг 2. Создать правило балансировки на серверы reverse-прокси (опционально).	В случае, если требуется балансировка на ферму публикуемых серверов, создать в разделе **Политики сети → Балансировка нагрузки** балансировщик reverse-прокси. В качестве серверов используются серверы reverse-прокси, созданные на предыдущем шаге.
Шаг 3. Создать правило reverse-прокси.	В разделе **Глобальный портал → Правила reverse-прокси** создать правило, которое будет задавать условия публикации серверов или фермы серверов. **Важно!** Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в настройках правила.
Шаг 4. Разрешить сервис Reverse-прокси на зоне, с которой необходимо разрешить доступ к внутренним ресурсам.	В разделе **Сеть → Зоны** разрешите сервис Reverse-прокси для зоны, с которой необходимо разрешить доступ к внутренним ресурсам (обычно зона Untrusted).

Для создания сервера reverse-прокси разделе **Глобальный портал → Серверы reverse-прокси** необходимо нажать на кнопку **Добавить** и заполнить следующие поля:

Наименование	Описание
Название	Название публикуемого сервера.
Описание	Описание публикуемого сервера.
Адрес сервера	IP-адрес публикуемого сервера.
Порт	TCP-порт публикуемого сервера.
HTTPS до сервера	Определяет, требуется ли использовать протокол HTTPS до публикуемого сервера.
Проверять SSL-сертификат	Включает/отключает проверку валидности SSL-сертификата, установленного на публикуемом сервере.
Не изменять IP-адрес источника	Оставляет оригинальный IP-адрес источника в пакетах, пересылаемых на публикуемый сервер. Если отключено, то IP-адрес источника заменяется на IP-адрес UserGate.

Для создания правила балансировки на серверы reverse-прокси в разделе **Политики сети → Балансировка нагрузки** необходимо выбрать **Добавить → Балансировщик reverse-прокси** и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Серверы reverse-прокси	Созданный на предыдущем шаге список серверов reverse-прокси, на которые будет распределяться нагрузка.

Для создания правила reverse-прокси необходимо нажать на кнопку **Добавить** в разделе **Глобальный портал → Правила reverse-прокси** и заполнить необходимые поля.

Примечание Правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нём условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки Выше/Ниже, Наверх/Вниз или перетаскивание мышью для изменения порядка применения правил.

Примечание Флажок *Инвертировать* меняет действие условия на противоположное, что соответствует логическому «НЕ» (отрицание).

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.

Наименование	Описание
Сервер reverse-прокси	Сервер reverse-прокси или балансировщик reverse-прокси, куда NGFW будет пересылать запросы.
Порт	Порт, на котором NGFW будет слушать входящие запросы.
Использовать HTTPS	Включает поддержку HTTPS.
Сертификат	Сертификат, используемый для поддержки HTTPS-соединения.
Авторизовать по сертификату	Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов NGFW, ему должна быть назначена роль **Пользовательский сертификат** и назначен соответствующий пользователь NGFW. Более подробно о пользовательских сертификатах читайте в разделе Управление сертификатами.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. **Важно!** Строки с символом '*' в таких списках не работают (игнорируются). Каждые 5 минут NGFW производит разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни NGFW автоматически обновляет значение IP-адреса. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Пользователи	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типа **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей. Данная вкладка доступна только при использовании HTTPS и авторизации пользователя по сертификату.
Назначение	Адрес назначения должен быть назначен на интерфейс, на который приходит входящее соединение. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15. **Важно!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; • условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.
Useragent	UserAgent пользовательских браузеров, для которых будет применено данное правило.
Подмена путей	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на http://www.example.com/path1 в http://www.example.loc/path2 **Изменить с** - домен и/или путь URL, которые требуется изменить. **Изменить на** - домен и/или путь URL, на которые требуется заменить старые. Если указан домен в поле **Изменить с**, то правило публикации будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.

Веб-портал (SSL VPN)

Documentation: ☑
Product: NGFW
Version: 7.0.1

Веб-портал позволяет предоставить доступ к внутренним веб-ресурсам, терминальным и ssh-серверам компании для удаленных или мобильных пользователей, используя при этом только протокол HTTPS. Данная технология не требует установки специального клиента VPN, достаточно обычного браузера.

ПримечаниеЕсли на целевых HTTP-ресурсах настроена аутентификация Kerberos или NTLM, то NGFW может производить аутентификацию по технологии SSO (необходим настроенный LDAP-коннектор с загруженным keytab-файлом).

Для настройки веб-портала необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Включить и настроить веб-портал.	В разделе **Настройки → Веб-портал** включить и настроить параметры веб-портала. Подробные значения настроек будут описаны далее в этой главе.
Шаг 2. Разрешить доступ к сервису веб-портала на необходимых зонах.	В разделе **Сеть → Зоны** разрешить сервис веб-портала для выбранных зон (обычно зона Untrusted). Данное разрешение откроет доступ к порту сервиса, который был указан в настройках веб-портала на предыдущем шаге.
Шаг 3. Добавить внутренние ресурсы в веб-портал.	В разделе **Глобальный портал → Веб-портал** добавить URL внутренних ресурсов, к которым необходим доступ пользователей. Подробные значения настроек будут описаны далее в этой главе.

При настройке веб-портала (раздел **Настройки → Веб-портал)** необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает/Выключает веб-портал.
Имя хоста	Имя хоста, которое пользователи должны использовать, чтобы подключаться к сервису веб-портала. Данное имя должно резолвиться службами DNS в IP-адрес интерфейса NGFW, входящего в зону, на которой разрешен сервис веб-портала.
Порт	Порт TCP, который будет использоваться сервисом веб-портала. Порт вместе с именем хоста образуют URL для подключения пользователей в виде: https://имя_хоста:порт.
Профиль аутентификации	Профиль аутентификации пользователей, который будет использоваться для аутентификации пользователей, подключающихся к веб-порталу. Профиль аутентификации задает метод аутентификации, например, AD-коннектор или локальный пользователь. Также в профиле аутентификации можно указать требование использовать мультифакторную аутентификацию для доступа к веб-порталу. Более подробно о профилях аутентификации смотрите раздел руководства Профили аутентификации.
Шаблон страницы аутентификации	Выбрать шаблон страницы аутентификации, который будет использоваться для отображения формы для ввода логина и пароля. Создать свою страницу аутентификации можно в разделе Шаблоны страниц.
Шаблон портала	Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Создать свою страницу аутентификации можно в разделе Шаблоны страниц.
Предлагать выбор домена AD/LDAP на странице аутентификации	Показывать выбор домена на странице аутентификации веб-портала.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице аутентификации веб-портала. Рекомендуемая опция для защиты от ботов, подбирающих пароли пользователей.
Профиль SSL	Выбор профиля SSL для построения защищенного канала для отображения веб-портала. Подробно о профилях SSL смотрите в главе Профили SSL.
Сертификат	Сертификат, который будет использоваться для создания HTTPS-соединения. Если выбран режим **Автоматически**, то используется сертификат, выпущенный сертификатом SSL дешифрования для роли SSL Captive-портала. Более подробно о ролях сертификатов смотрите в разделе руководства Управление сертификатами.
Аутентификация пользователя по сертификату	Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов NGFW, ему должна быть назначена роль **Пользовательский сертификат** и назначен соответствующий пользователь NGFW. Более подробно о пользовательских сертификатах читайте в разделе Управление сертификатами.

Настройке веб-портала (раздел **Глобальный портал → Веб портал**) сводится к тому, что необходимо создать записи публикации URL внутренних веб-ресурсов. Для каждого URL необходимо создать закладку и заполнить следующие поля:

Наименование	Описание
Включено	Включает или отключает закладку.
Название	Название закладки.
Описание	Описание закладки.
URL	URL ресурса, который необходимо опубликовать через веб-портал. Указывайте полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. **Важно!** Для публикации терминальных серверов необходимо отключить опцию, требующую Network Level Authentication в свойствах RDP доступа на серверах терминального доступа. Аутентификацию пользователей для доступа к серверам в данном случае будет выполнять веб-портал в соответствии со своими настройками.
Домен прямого доступа	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену.

Наименование	Описание
Иконка	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку.
Вспомогательные URL	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Например, основной URL http://www.example.com получает часть медиаконтента со вспомогательного URL http://cdn.example.com.
Пользователи	Список пользователей и/или групп пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL.

Очередность закладок веб-портала определяет порядок отображения их пользователю. Администратор может менять очередность закладок с помощью кнопок **Выше**/**Ниже**, **Наверх**/**Вниз** или перетаскивая закладки с помощью мыши.

Настройка VPN

Описание

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1

VPN (Virtual Private Network — виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, интернет). NGFW позволяет создавать VPN-подключения следующих типов:

- VPN-сервер для удаленного доступа клиентов (**Remote access VPN**). В данном случае NGFW выступает в качестве сервера, а пользователи других устройств выступают в качестве клиентов VPN. NGFW поддерживает работу со стандартными клиентами большинства популярных операционных систем, например, таких, как Windows, Linux, Mac OS X, iOS, Android и другие.
- VPN для защищенного соединения офисов (Site-to-Site VPN). В данном случае один NGFW выступает в качестве сервера, а другой NGFW выступает в роли клиента. Клиент инициирует соединение с сервером. Подключение сервер-сервер позволяет объединить разобщенные офисы компании в единую логическую сеть.

Для создания туннелей используется протокол Layer 2 Tunnelling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec. Поддерживается многофакторная аутентификация пользователей при подключении к сервису VPN.

VPN для защищенного соединения офисов (Site-to-Site VPN)

Product: UserGate NGFW
Version: 6.1.9, 7.0.1
Technology: VPN

Хотя настройка NGFW для выполнения роли VPN-сервера близка к настройке сервера для удаленного доступа, мы рекомендуем произвести все настройки отдельно, поскольку часть настроек может отличаться.

Настройка сервера, выполняющего роль VPN-сервера для объединения офисов:

Наименование	Описание
Шаг 1. Создать локального пользователя для авторизации сервера, выступающего в роли VPN-клиента.	В разделе **Пользователи и устройства → Пользователи** создать пользователей для каждого из удаленных NGFW, выступающих в роли VPN-клиентов, задать пароли. Рекомендуется поместить всех созданных пользователей в группу, которой будет дан доступ для подключения по VPN. По умолчанию для этой цели в NGFW создана группа **VPN servers.**
Шаг 2. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе **Сеть → Зоны** отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервис VPN. Как правило, это зона **Untrusted.**
Шаг 3. Создать зону, в которую будут помещены подключаемые по VPN серверы.	В разделе **Сеть → Зоны** создать зону, в которую будут помещены подключаемые по VPN серверы. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Рекомендуется использовать уже существующую по умолчанию зону **VPN for Site-to-Site**.
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе **Политики сети → Межсетевой экран** создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны. По умолчанию в NGFW создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted** , разрешающее весь трафик из зоны **VPN for Site-to-Site** в **Trusted** и **Untrusted** зоны. Правило выключено по умолчанию. Чтобы трафик передавался клиенту из нужной зоны сервера через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения **VPN for Site-to-Site**.
Шаг 5. Создать профиль авторизации.	В разделе **Пользователи и устройства → Профили авторизации** создать профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей с целью получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP. Подробно о профилях авторизации смотрите в разделе данного руководства Профили авторизации.

Наименование	Описание
Шаг 6. Создать профиль безопасности VPN.	Профиль безопасности определяет такие настройки, как общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов. Для создания профиля безопасности необходимо перейти в раздел **VPN → Профили безопасности**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** — название профиля безопасности. • **Описание** — описание профиля. • **Версия протокола IKE (Internet Key Exchange)** . Протокол IKE используется для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1. • **Режим IKE**: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. ◦ **Основной режим**. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. ◦ **Агрессивный режим**. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен. • **Аутентификация с пиром**. Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). • **Общий ключ** — строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа**. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **Интервал проверки dead peer detection** — для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал: 10 секунд; значение 0 отключает проверку. • **Неудачных попыток** — максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • **Diffie-Hellman группы**: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **Алгоритмы авторизации и шифрования**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **Время жизни ключа**. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • **Максимальный размер данных, шифруемых одним ключом**. Время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **Алгоритмы авторизации и шифрования**. Алгоритмы используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. По умолчанию в NGFW создан профиль безопасности **Site-to-Site VPN profile**, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, необходимо изменить общий ключ шифрования.
Шаг 7. Создать VPN-интерфейс.	VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах NGFW, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений. **Внимание!** Редактирование кластерного интерфейса возможно только для узла кластера cluster(даже если кластер не собран и узел всего один). В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры: • **Название** — название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • **Описание** — описание интерфейса. • **Зона** — зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 3. • **Профиль Netflow** — профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • **Режим** — тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес. • **MTU** — размер MTU для выбранного интерфейса. По умолчанию в системе уже создан VPN-интерфейс tunnel2, который рекомендовано использовать для Site-to-Site VPN.

Наименование	Описание
Шаг 8. Создать сеть VPN.	VPN-сеть определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и — опционально — маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов. **Важно!** Добавление сетей VPN лучше делать в технологическое окно, так как при добавлении новой сети VPN происходит рестарт сервиса из за чего текущие VPN соединения прерываются на несколько десятков секунд. Для создания туннеля VPN перейдите в раздел **VPN → Сети VPN**, нажмите кнопку **Добавить** и заполните следующие поля: • **Название** — название сети. • **Описание** — описание сети. • **Диапазон IP-адресов**, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес. • Укажите **DNS-серверы**, которые будут переданы клиенту, или отметьте чекбокс **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. **Важно!** Можно указать не более двух DNS-серверов. • Укажите **маршруты**, передаваемые клиенту в виде бесклассовой адресации (CIDR). В NGFW создана сеть **Site-to-Site VPN network** с настройками по умолчанию. Для использования этой сети в ней необходимо добавить маршруты, передаваемые на сервер-клиент. Чтобы VPN-сервер узнал о подсетях клиента, необходимо прописать статический маршрут на сервере, указав в качестве адреса назначения адрес VPN-туннеля, используемый на сервере-клиенте.
Шаг 9. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть и профиль VPN. Для создания правила необходимо перейти в раздел **VPN → Серверные правила**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** — название правила. • **Описание** — описание правила. • **Профиль безопасности** — профиль безопасности VPN, созданный ранее. • **Сеть VPN** — сеть VPN, созданная ранее. • **Профиль авторизации** — профиль авторизации, созданный ранее. • **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**. **Важно!** Обработка трафика происходит по следующей логике: ◦ условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; ◦ условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. • **Назначение** — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 2. • **Интерфейс** — созданный ранее интерфейс VPN. • **Пользователи** — группа учетных записей серверов или отдельные учетные записи серверов, которым разрешено подключаться по VPN. По умолчанию в NGFW создано серверное правило **Site-to-Site VPN rule**, в котором используются необходимые настройки для Site-to-Site VPN, а доступ к VPN разрешен членам локальной группе **VPN servers.** **Важно!** Для применения различных серверных правил к разным клиентам необходимо использовать параметры *Исходная зона* и *Адрес источника*. Параметр *Пользователь* не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.

Для настройки сервера, выступающего в роли VPN-клиента, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону, в которую будут помещен интерфейс, используемый для подключения по VPN.	В разделе **Сеть → Зоны** создать зону, в которую будут помещены интерфейсы, используемые для подключения по VPN. Эту зону в дальнейшем можно будет использовать в политиках безопасности. Рекомендуется использовать уже существующую по умолчанию зону **VPN for Site-to-Site**.
Шаг 2. Создать разрешающее правило межсетевого экрана для трафика в созданную зону.	Создать разрешающее правило межсетевого экрана в разделе **Политики сети → Межсетевой экран**. По умолчанию в NGFW создано правило межсетевого экрана **VPN for Site-to-Site to Trusted and Untrusted**, разрешающее весь трафик между зонами **VPN for Site-to-Site**, **Trusted** и **Untrusted**. Чтобы трафик передавался на сервер из нужной зоны сервера-клиента через VPN-туннель, необходимо создать разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения **VPN for Site-to-Site**.

Наименование	Описание
Шаг 3. Создать профиль безопасности VPN.	Профиль безопасности определяет такие настройки, как общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей безопасности и использовать их для построения соединений с разными типами клиентов. Для создания профиля необходимо перейти в раздел **VPN → Профили безопасности VPN**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** — название профиля безопасности. • **Описание** — описание профиля. • **Версия протокола IKE (Internet Key Exchange)**. Протокол IKE используется для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1. • **Режим IKE**: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. ◦ **Основной режим**. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. ◦ **Агрессивный режим**. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен. • **Аутентификация с пиром**. Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). • **Общий ключ** — строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа**. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **Интервал проверки dead peer detection** — для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал: 10 секунд; значение 0 отключает проверку. • **Неудачных попыток** — максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • **Diffie-Hellman группы**: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **Алгоритмы авторизации и шифрования**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **Время жизни ключа**. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • **Максимальный размер данных, шифруемых одним ключом**. Время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **Алгоритмы авторизации и шифрования**. Алгоритмы используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. По умолчанию в NGFW создан профиль Client VPN profile, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, то необходимо изменить общий ключ шифрования.
Шаг 4. Создать VPN-интерфейс.	VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах NGFW, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений. В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры: • **Название** — название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • **Описание** — описание интерфейса. • **Зона** — зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 1. • **Профиль Netflow** — профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • **Режим** — тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Для использования интерфейса в качестве клиентского VPN, необходимо использовать режим получения адреса — Динамический. • **MTU** — размер MTU для выбранного интерфейса. По умолчанию в системе уже создан VPN-интерфейс tunnel3, который рекомендовано использовать для клиентского подключения Site-to-Site VPN. **Важно!** Если при настройке туннельного интерфейса на стороне сервера был выбран уже существующий интерфейс tunnel2 с настройками по умолчанию, то на клиенте при подключении к серверу возникнет конфликт IP-адресов, поскольку на клиенте также существует аналогичный интерфейс tunnel2 с тем же диапазоном адресов. Для корректной работы диапазоны адресов туннельных интерфейсов не должны пересекаться. Рекомендуется изменить диапазон адресов на клиенте на уникальный.
Шаг 5. Создать клиентское правило VPN.	Создать клиентское правило VPN, которое будет инициировать подключение к VPN-серверу. Для создания правила необходимо перейти в раздел **VPN → Клиентские правила**, нажать кнопку **Добавить** и заполнить следующие поля: • **Включено** — включение/отключение данного правила. • **Название** — название правила. • **Описание** — описание правила. • **Профиль безопасности VPN** — созданный ранее профиль безопасности VPN. • **Интерфейс** — созданный ранее VPN-интерфейс. • **Адрес сервера** — IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне **Untrusted** на NGFW, выполняющего роль VPN-сервера. • **Протокол VPN** — Возможно выбрать вариант L2TP/IPsec или IPsec туннель для подключения к VPN-серверу. • **Подсети для VPN** — IP адрес сети, которая будет доступна для клиентов со стороны NGFW и со стороны VPN-сервера. • **Имя пользователя и пароль** (только для протокола L2TP) — имя и пароль пользователя, созданного на шаге 1 при подготовке VPN-сервера.

ПримечаниеВ сценарии site-to-site VPN-подключение по протоколам L2TP/IPsec полностью поддерживается между устройствами UserGate. Клиентское подключение UserGate NGFW к VPN-серверам

сторонних производителей по протоколам L2TP/IPsec не поддерживается. При работе UserGate NGFW в режиме VPN-сервера L2TP/IPsec передача маршрутов выполняется через payload L2TP.

После завершения настройки VPN-сервера и VPN-клиента клиент инициирует соединение на сервер, и в случае корректности настроек, поднимается VPN-туннель. Для отключения туннеля выключите клиентское (на клиенте) или серверное правило VPN (на сервере).

VPN для удаленного доступа клиентов (Remote access VPN)

Documentation: ☑
Version: 6.1.9, 7.0.1

Для подключения VPN-клиентов к корпоративной сети необходимо настроить NGFW для выполнения роли VPN-сервера. Для этого необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить сервис VPN на зоне, к которой будут подключаться VPN-клиенты.	В разделе **Сеть → Зоны** отредактировать параметры контроля доступа для той зоны, к которой будут подключаться VPN-клиенты, разрешить сервис VPN. Как правило, это зона **Untrusted.**
Шаг 2. Создать зону, в которую будут помещены подключаемые по VPN клиенты.	В разделе **Сеть → Зоны** создать зону, в которую будут помещены подключаемые по VPN клиенты. Эту зону в дальнейшем можно использовать в политиках безопасности. Рекомендуется использовать уже существующую по умолчанию зону **VPN for remote access**.
Шаг 3. Создать правило NAT для созданной зоны.	Клиенты подключаются к VPN с использованием Point-to-Point протокола. Чтобы трафик мог ходить из созданной на предыдущем шаге зоны, необходимо создать правило NAT из этой зоны во все необходимые зоны. Создайте соответствующее правило в разделе **Политики сети → NAT и маршрутизация**. По умолчанию в NGFW создано правило **NAT from VPN for remote access to Trusted and Untrusted** , разрешающее подмену адресов из зоны **VPN for remote access** в зоны **Trusted** и **Untrusted**.
Шаг 4. Создать разрешающее правило межсетевого экрана для трафика из созданной зоны.	В разделе **Политики сети → Межсетевой экран** создать правило межсетевого экрана, разрешающее трафик из созданной зоны в другие зоны. По умолчанию в NGFW создано правило межсетевого экрана **VPN for remote access to Trusted and Untrusted** , разрешающее весь трафик из **зоны VPN for remote access** в зоны **Trusted** и **Untrusted**.
Шаг 5. Создать профиль аутентификации.	В разделе **Пользователи и устройства → Профили аутентификации** создать профиль авторизации для пользователей VPN. Допускается использовать тот же профиль авторизации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной авторизации, такие как Kerberos, NTLM, SAML IDP. VPN поддерживает многофакторную аутентификацию. Второй фактор может быть получен через одноразовые коды TOTP. Для ввода второго фактора аутентификации пользователь при подключении к VPN серверу должен указать свой пароль в виде: пароль:одноразовый_код где пароль — это пароль пользователя : — разделитель одноразовый_код — второй фактор аутентификации. Подробно о профилях авторизации смотрите в разделе данного руководства Профили аутентификации. **Внимание!** В версиях NGFW старше 6.1.8 данный раздел носит название *Профили авторизации*

Наименование	Описание
Шаг 6. Создать профиль безопасности VPN.	Профиль безопасности VPN определяет такие настройки, как общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Допускается иметь несколько профилей и использовать их для построения соединений с разными типами клиентов. Для создания профиля необходимо перейти в раздел **VPN → Профили безопасности VPN**, нажать кнопку **Добавить** и заполнить следующие поля: • **Название** — название профиля безопасности. • **Описание** — описание профиля. • **Версия протокола IKE (Internet Key Exchange)**. Протокол IKE используется для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1. • **Режим IKE**: Основной или Агрессивный. Разница между режимами: в агрессивном режиме используется меньшее количество пакетов, что позволяет достичь более быстрого установления соединения. Агрессивный режим не передает некоторые параметры согласования, что требует предварительной идентичной настройки их на точках подключения. ◦ **Основной режим**. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. ◦ **Агрессивный режим**. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен. • **Аутентификация с пиром**. Общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key). • **Общий ключ** — строка, которая должна совпадать на сервере и клиенте для успешного подключения. Далее необходимо задать параметры первой и второй фаз согласования. Во время первой фазы происходит согласование защиты IKE. Аутентификация происходит на основе общего ключа в режиме, выбранном ранее. Необходимо указать следующие параметры: • **Время жизни ключа**. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы. • **Интервал проверки dead peer detection** — для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа. Минимальный интервал проверки: 10 секунд; значение 0 отключает проверку. • **Неудачных попыток** — максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным. • **Diffie-Hellman группы**: выбор группы Диффи-Хеллмана, которая будет использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **Алгоритмы авторизации и шифрования**. Алгоритмы используются в порядке, в котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. **Важно**При работе с операционными системами Windows и Android необходимо отключать проверку dead peer detection. Во второй фазе осуществляется выбор способа защиты IPsec подключения. Необходимо указать: • **Время жизни ключа**. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще. • **Максимальный размер данных, шифруемых одним ключом**. Время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа** и **Максимальный размер данных, шифруемых одним ключом**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. • **Алгоритмы авторизации и шифрования**. Алгоритмы используются в порядке, котором они отображены. Для изменения порядка перетащите необходимую пару вверх/вниз или используйте кнопки **Выше**/**Ниже**. По умолчанию в NGFW создан серверный профиль **Remote access VPN profile**, задающий необходимые настройки. Если вы собираетесь использовать этот профиль, то необходимо изменить общий ключ шифрования. Для упрощения настройки соединения с устройствами других вендоров по умолчанию созданы дополнительные профили безопасности (**Cisco compatible VPN profile** — для работы с устройствами Cisco и **Fortinet compatible VPN profile** — для работы с устройствами Fortinet).
Шаг 7. Создать VPN-интерфейс.	VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах NGFW, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений. В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN.** Задайте следующие параметры: • **Название** — название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса. • **Описание** — описание интерфейса. • **Зона** — зона, к которой будет относится данный интерфейс. Все клиенты, подключившиеся по VPN к NGFW, будут также помещены в эту зону. Укажите зону, созданную на шаге 2. • **Профиль Netflow** — профиль Netflow, используемый для данного интерфейса. Не обязательный параметр. • **Режим** — тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (**Site-2-Site VPN** или **Remote access VPN**, то необходимо использовать статический IP-адрес. • **MTU** — размер MTU для выбранного интерфейса. По умолчанию в системе уже создан VPN-интерфейс **tunnel1**, который рекомендовано использовать для **Remote access VPN**.

Наименование	Описание
Шаг 8. Создать сеть VPN.	VPN-сеть определяет сетевые настройки, которые будут использованы при подключении клиента к серверу. Это в первую очередь назначение IP-адресов клиентам внутри туннеля, настройки DNS и — опционально — маршруты, которые будут переданы клиентам для применения, если клиенты поддерживают применение назначенных ему маршрутов. Допускается иметь несколько туннелей с разными настройками для разных клиентов. **Важно!** Добавление сетей VPN лучше делать в технологическое окно, так как при добавлении новой сети VPN происходит рестарт сервиса из за чего текущие VPN соединения прерываются на несколько десятков секунд. Для создания туннеля VPN перейдите в раздел **VPN → Сети VPN**, нажмите кнопку **Добавить** и заполните следующие поля: • **Название** — название сети. • **Описание** — описание сети. • **Диапазон IP-адресов**, которые будут использованы клиентами и сервером. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес. • Укажите **DNS-серверы**, которые будут переданы клиенту, или отметьте чекбокс **Использовать системные DNS**, в этом случае клиенту будут назначены DNS-серверы, которые использует NGFW. **Важно!** Можно указать не более двух DNS-серверов. • Укажите **маршруты**, передаваемые клиенту в виде бесклассовой адресации (CIDR). В NGFW создана сеть **Remote access VPN network** с рекомендуемыми настройками.
Шаг 9. Создать серверное правило VPN.	Создать серверное правило VPN, используя в нем созданные ранее сеть VPN, интерфейс VPN и профиль VPN. Для создания правила необходимо перейти в раздел **VPN → Серверные правила**, нажать кнопку **Добавить** и заполнить следующие поля: • **Включено** — включает/отключает правило. • **Название** — название правила. • **Описание** — описание правила. • **Профиль безопасности** — профиль безопасности, созданный ранее. • **Сеть VPN** — сеть VPN, созданная ранее. • **Профиль авторизации** — профиль авторизации, созданный ранее. • **URL инициализации TOTP** — url, по которому пользователь может провести первоначальную инициализацию своего TOTP-устройства в случае, если настроена многофакторная авторизация TOTP для авторизации VPN. • **Интерфейс** — интерфейс VPN, созданный ранее. • **Источник** — зоны и адреса, с которых разрешено принимать подключения к VPN. Как правило, клиенты находятся в сети интернет, следовательно, следует указать зону **Untrusted**. **Важно!** Обработка трафика происходит по следующей логике: - условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов; - условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов. • **Назначение** — один или несколько адресов интерфейса, на который будет происходить подключение клиентов. Интерфейс должен принадлежать зоне, указанной на шаге 1. • **Пользователи** — группа пользователей или отдельные пользователи, которым разрешено подключаться по VPN. По умолчанию в NGFW создано серверное правило **Remote access VPN rule**, в котором используются необходимые настройки для **Remote Access VPN**, а доступ к VPN разрешен членам локальной группы **VPN users.** **Важно!** Для применения различных серверных правил к разным клиентам необходимо использовать параметры *Исходная зона* и *Адрес источника*. Параметр *Пользователь* не является условием выбора серверного правила, проверка пользователя происходит уже после установления соединения VPN.
Шаг 10. Настроить VPN на клиентском компьютере.	Для настройки клиентского подключения к VPN на компьютере пользователя необходимо указать следующие параметры: • Используйте тип подключения VPN — L2TP over IPsec. • В качестве IP-адреса VPN-сервера укажите IP-адрес интерфейса зоны, указанной на шаге 1. • В качестве общего ключа (pre-shared key, shared secret) используйте общий ключ, указанный вами на шаге 6. • Укажите протокол PAP для авторизации пользователя. • В качестве имени пользователя укажите имя учетной записи пользователя в формате username @domain, например, testuser@testdomain.loc • В настройках VPN-подключения отключите использование основного шлюза в удалённой сети. **Важно!** Операционные системы Microsoft Windows требуют изменения параметров реестра для корректной работы с VPN-сервером L2TP/IPsec. Операционные системы Windows версий 10 и выше, по умолчанию, не поддерживают L2TP-подключения к серверам, которые находятся за вышестоящими маршрутизаторами с функционалом NAT. Для возможности установки соединения необходимо внести следующие правки в реестр ОС Windows: • в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent** создать параметр **DWORD (32 бита)** с названием **AssumeUDPEncapsulationContextOnSendRule** и значением **2**; • в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters** изменить значение параметра **AllowL2TPWeakCrypto** на **1**. **Важно!** После внесения изменений в реестр их необходимо применить, например, перезагрузив компьютер. Для получения более подробной информации обратитесь к статье Microsoft (https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/configure-l2tp-IPsec-server-behind-nat-t-device).

IPsec over GRE

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1, 6.1.9

При совместном использовании GRE и IPsec могут быть созданы 2 типа соединений: IPsec over GRE и GRE over IPsec.

При использовании соединения IPsec over GRE происходит передача шифрованного трафика по незащищённому GRE-туннелю, т.е. сначала происходит инкапсуляция IPsec, а затем инкапсуляция GRE.

Для настройки IPsec over GRE необходимо:

Наименование	Описание
Шаг 1. Настройка туннеля GRE.	Подробнее о настройке туннельного интерфейса GRE читайте в разделе Интерфейс туннель. **Важно!** При настройке туннельного GRE интерфейса в качестве адресов источника (локальный IP) и назначения (удалённый IP) должны быть указаны внешние IP-адреса интерфейсов устройства.
Шаг 2. Настройка Site-to-Site VPN-соединения.	Подробнее о настройке Site-to-Site VPN-соединения читайте в разделе VPN для защищенного соединения офисов (Site-to-Site VPN) . **Важно!** При настройке клиентского правила VPN в качестве адреса сервера необходимо указать IP-адрес туннельного интерфейса GRE.

Недостаток IPsec over GRE: не поддерживается передача многоадресных и широковещательных пакетов. Эта проблема отсутствует при использовании соединения GRE over IPsec.

GRE over IPsec

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1, 6.1.9

GRE over IPsec позволяет использовать преимущества GRE (поддержка многоадресной и широковещательной рассылки) и IPsec (передача трафика в зашифрованном виде). При использовании соединения GRE over IPsec происходит инкапсуляция в GRE пакеты, а затем их передача по зашифрованному каналу связи (инкапсуляция IPsec).

Для настройки GRE over IPsec необходимо:

Наименование	Описание
Шаг 1. Настройка Site-to-Site VPN-соединения.	Подробнее о настройке Site-to-Site VPN-соединения читайте в разделе VPN для защищенного соединения офисов (Site-to-Site VPN) .
Шаг 2. Настройка туннеля GRE.	Подробнее о настройке туннельного интерфейса GRE читайте в разделе Интерфейс туннель. **Важно!** При настройке туннельного GRE интерфейса в качестве адресов источника (локальный IP) и назначения (удалённый IP) должны быть указаны IP-адреса VPN-интерфейсов.

Библиотеки элементов

Описание

Product: NGFW
Version: 5.x, 6.1.9, 7.0.1
Documentation:

Данный большой раздел содержит в себе все записи, адреса-сайтов, IP-адреса, шаблоны и прочие элементы, которые используются при настройке правил NGFW.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми, потому что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, имеют механизм автоматического обновления. Автоматическое обновление элементов требует наличия специальной лицензии. Более подробно о лицензии на продукт вы можете прочитать в главе Лицензирование.

Морфология

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Морфологический анализ — механизм, который распознает отдельные слова и словосочетания на веб-сайте. Если в тексте содержится достаточное для блокировки количество указанных слов и словосочетаний, то доступ к сайту блокируется.

Морфологический анализ выполняется как при проверке запроса пользователя, так и при получении ответа от веб-сервера и до его передачи пользователю. Получив ответ от веб-сервера, NGFW просматривает текст на странице и подсчитывает его суммарный «вес», исходя из «весов» слов, указанных в морфологических категориях. Если «вес» страницы превышает «вес» морфологической категории, правило срабатывает. При подсчете «веса» страницы учитываются все словоформы (леммы) запрещенных слов. Для поиска словоформ NGFW использует встроенные словари русского, английского, японского, арабского и немецкого языков.

Существует возможность подписки на словари, предоставляемые UserGate. Данные словари нельзя редактировать. Для использования этих словарей необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе Лицензирование.

Наименование	Описание
Соответствие списку запрещенных материалов Министерством Юстиции Российской Федерации	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции Российской Федерации.
Соответствие списку запрещенных материалов республики Казахстан	Морфологический словарь, содержащий перечень слов и фраз, запрещенных Министерством Юстиции республики Казахстан.
Суицид	Морфологический словарь, содержащий перечень слов и фраз суицидальной направленности.
Терроризм	Морфологический словарь, содержащий перечень слов и фраз террористической направленности.
Нецензурная лексика	Морфологический словарь, содержащий перечень слов и фраз, относящихся к нецензурной лексике.
Азартные игры	Морфологический словарь, содержащий перечень слов и фраз, относящихся к азартным играм.
Наркотики	Морфологический словарь, содержащий перечень слов и фраз наркотической направленности.
Соответствие ФЗ-436 (Защита детей)	Морфологический словарь, содержащий перечень слов и фраз тематик, нежелательных для детей.
Порнография	Морфологический словарь, содержащий перечень слов и фраз порнографической направленности.
Бухгалтерия (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в бухгалтерии.
Маркетинг (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в маркетинге.
Персональные данные (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, встречающихся в персональных данных.
Финансы (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в финансах.
Юридический (DLP)	Морфологический словарь, содержащий перечень терминов, слов и фраз, используемых в юриспруденции.

Для фильтрации по морфологическому содержанию страницы требуется:

Наименование	Описание
Шаг 1. Создать одну или несколько морфологических категорий и указать вес каждой категории.	Нажать на кнопку **Добавить**, задать название новой категории и ее вес.
Шаг 2. Указать список запрещенных фраз с весами.	Нажать на кнопку **Добавить** и указать необходимые слова или фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки.
Шаг 3. Создать правило фильтрации контента, содержащее одну или несколько морфологических категорий.	Смотрите раздел Фильтрация контента.

Администратор имеет возможность создать свой словарь и централизованно распространять его на все межсетевые экраны UserGate, имеющиеся в организации. Для создания такой морфологической базы необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми фразами.	создать файл **list.txt** со списком слов в следующем формате: !word1 !word2 !word3 word4 50 ... Lastword Вес словаря в таком случае равен 100, вес слова можно указать. По умолчанию он равен 100.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.

Наименование	Описание
Шаг 3. Создать файл с версией словаря.	Создать файл **version.txt**, внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать морфологическую категорию указать URL для обновления словаря.	На каждом UserGate создать морфологическую базу. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

ПримечаниеПри создании морфологических словарей не рекомендуется добавлять фразы, содержащие более трех слов, без использования символа «!» перед словами. Необходимо помнить, что при построении морфологической базы каждое из слов будет преобразовано во все существующие формы (склонения, спряжения, множественные числа, времена и т.д.), и результирующее количество фраз будет достаточно большим. При добавлении длинных фраз необходимо использовать модификатор «!» перед словами, модификация которых не нужна, как правило, это различные предлоги и союзы. Например, фразу «как уйти из жизни безболезненно» правильно добавить в виде «!как уйти !из !жизни безболезненно». Это сократит количество возможных вариантов фраз, но при этом оставит все фразы с требуемым смыслом.

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Сервисы

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Раздел сервисы содержит список общеизвестных сервисов, основанных на протоколе TCP/IP, например, таких, как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил NGFW. Первоначальный список сервисов поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового сервиса необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервис.	Нажать на кнопку **Добавить**, дать сервису название, ввести комментарий.
Шаг 2. Указать протокол и порт.	Нажать на кнопку **Добавить**, выбрать из списка необходимый протокол, указать порты назначения и, опционально, порты источника. Для указания диапазона портов можно использовать — (тире), например, 33333—33355.

Группы сервисов

Documentation: ☑
Product: NGFW
Version: 7.0.1

В данном разделе пользователь может управлять (создавать/обновлять/удалять) группами объектов сервисов. Группы сервисов могут быть использованы при настройке политик безопасности NGFW.

Для создания группы сервисов:

Наименование	Описание
Шаг 1. Создать группу.	На панели **Группы сервисов** нажать на кнопку **Добавить**, указать название и, опционально, описание группы сервисов.
Шаг 2. Добавить сервисы в группу.	На панели **Элементы** нажать **Добавить** и выбрать сервисы для добавления в группу. Для добавления всех сервисов использовать кнопку **Добавить все**.

IP-адреса

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил NGFW. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать список.	На панели **Группы** нажать на кнопку **Добавить**, дать название списку IP-адресов.
Шаг 2. Указать адрес обновления списка (не обязательно).	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе.
Шаг 3. Добавить IP-адреса.	На панели **Адреса из выбранной группы** нажать на кнопку **Добавить** и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл **list.txt** со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: x.x.x.x y.y.y.y z.z.z.z
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip.**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом NGFW создать список IP-адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. **Примечание**URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Useragent браузеров

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

С помощью фильтрации по Useragent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список Useragent поставляется вместе с продуктом. Для фильтрации по типу Useragent необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список Useragent.	В панели **Категории** нажать на кнопку **Добавить** и задать название нового списка UserAgent, опционально, описание списка и URL обновления.
Шаг 2. Добавить необходимые Useragent браузеров в новый список.	В панели **Шаблоны useragent** добавить необходимый Useragent. Исчерпывающий список строк Useragent представлен тут: http://www.useragentstring.com/pages/useragentstring.php
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Смотрите раздел Фильтрация контента.

Администратор имеет возможность создавать свои списки Useragent и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми Useragent.	Создать файл **list.txt** со списком **Useragent**.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip и version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список Useragent и указать URL для обновления.	На каждом NGFW создать список Useragent. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Типы контента

Product: NGFW
Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1

С помощью фильтрации типов контента можно блокировать загрузку файлов определенного типа, например, запретить все файлы типа *.doc.

Существует возможность подписки на типы контента, предоставляемые разработчиками UserGate. Данные списки типов контента нельзя редактировать, их можно использовать при определении правил фильтрации контента. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе Лицензирование.

Для фильтрации по типу контента необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список типов контента. Если используется предопределенный список UserGate, перейдите к шагу 3.	В панели **Категории** нажать на кнопку **Добавить**, задать название нового списка типа контента, опционально, описание списка и URL обновления.
Шаг 2. Добавить необходимые типы контента в новый список.	Добавить необходимый тип контента в данный список в формате MIME. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml. Например, для блокировки документов типа *.doc необходимо добавить тип контента «application/msword».
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Смотрите раздел Фильтрация контента.

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл **list.txt** со списком типов контента.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip.**
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список типа контента и указать URL для обновления.	На каждом NGFW создать список типа контента. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Списки URL

Documentation: ☑
Version: 6.1.9, 7.0.1

Страница предназначена для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет собственные обновляемые списки. Для использования этих списков необходима соответствующая лицензия. Подробнее о лицензии на продукт — в разделе «Лицензирование».

Наименование	Описание
Список поисковых систем без безопасного поиска	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля.
Соответствие списку запрещенных URL Министерства Юстиции РФ	Данный список содержит URL, запрещенные Министерством Юстиции Российской Федерации.
Соответствие списку запрещенных URL Республики Казахстан	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан.
Список образовательных учреждений	Список доменных имен образовательных учреждений РФ.
Список фишинговых сайтов	Данный список содержит URL фишинговых сайтов.
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru.
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru.

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список URL.	В панели **Списки URL** нажать на кнопку **Добавить**, задать название нового списка. Выбрать **Тип** списка — **Локальный** или **Обновляемый**. Для обновляемого списка указать **URL обновления** и настроить **Расписание скачивания обновлений**. Установить категорию создаваемого списка в поле **Чувствительность к регистру** (доступно начиная с релиза 6.1.9.12143R HF8): • **Чувствительный к регистру** — список адресов URL, чувствительных к регистру букв в адресе. • **Нечувствительный к регистру** — список адресов URL, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах. • **Домен** — список адресов доменов для использования в правилах DNS-фильтрации. При добавлении в этот список записи вида: «http://test.ru» добавится запись: «test.ru». **Внимание!**Категория списка задается при его создании. Изменить категорию после создания списка нельзя.
Шаг 2. Добавить необходимые записи в новый список.	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «$» и «*»: «*» — любое количество любых символов; «^» — начало строки; «$» — конец строки. Символы «?» и «#» не могут быть использованы.
Шаг 3. Создать правило фильтрации контента, содержащее один или несколько списков.	Подробнее — в разделе «Фильтрация контента».

Если URL-запись начинается с «http://», «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S) фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

Если вы хотите заблокировать точный адрес, используйте символы «^» и «$»: ^http://domain.com/exacturl$.

Для блокирования точного URL всех дочерних папок используйте символ «^»: ^http://domain.com/exacturl/.

Для блокирования домена со всеми возможными URL используйте запись такого вида: domain.com.

Внимание!Спецсимволы не работают в списках-исключениях для блокировки рекламы. В этих списках применение спецсимволов не рекомендуется.

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com; mail.yahoo.com. А также: qweryahoo.com.	Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com; http://mail.yahoo.com; https://mail.yahoo.com; http://sport.yahoo.com/123; http://qwertyahoo.com/.

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
^mail.yahoo.com$	Заблокирован только mail.yahoo.com.	Заблокированы только: http://mail.yahoo.com; https://mail.yahoo.com.
^mail.yahoo.com/$	Ничего не заблокировано.	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/$	Ничего не заблокировано.	Заблокирован только: http://finance.yahoo.com/personal-finance/.
^yahoo.com/12345/	Ничего не заблокировано.	Заблокированы: http://yahoo.com/12345/whatever/; https://yahoo.com/12345/whatever/.

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все межсетевые экраны UserGate. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл **list.txt** со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip**.**
Шаг 3. Создать файл с версией списка.	Создать файл version.txt, внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt, чтобы они были доступны для скачивания.
Шаг 5. Создать список и указать URL для обновления.	На каждом NGFW создать список URL. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. **Примечание**URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0 — воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — для выбора всех значений. • Дефис (-) — для указания диапазона значений. • Запятая (,) — в качестве разделителя значений. • Косая черта (/) — для указания шага между значениями.

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл list.zip.md5, содержащий чек-сумму файла list.zip. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш list.zip, после чего сохраняется в формате md5. Например, содержимое файла list.zip.md5:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Календари

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах NGFW. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать календарь.	В панели **Группы** нажать на кнопку **Добавить**, указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели **Элементы** нажать на кнопку **Добавить** и добавить интервал. Дать название интервалу и указать время.

Полосы пропускания

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую возможно в дальнейшем использовать в правилах управления полосой пропускания. Более подробно о правилах управления полосой пропускания смотрите в главе Пропускная способность.

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления новой полосы пропускания необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать полосу пропускания.	Нажать на кнопку **Добавить**, дать название, описание.
Шаг 2. Указать скорость.	Указать скорость в Кбит/сек.
Шаг 3. Указать значение DSCP для QoS.	Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63.

Шаблоны страниц

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

С помощью шаблонов страниц администратор может управлять видом страницы блокировки и страницы авторизации Captive-портала. Администратор может использовать разные шаблоны для разных правил фильтрации контента и правил Captive-портала.

NGFW поставляется с различными типами шаблонов — шаблоны страниц блокировки, Captive-портала, веб-портала, инициализации TOTP и др. Они могут использованы как образцы для создания пользовательских шаблонов, например, в фирменном стиле компании или на необходимом языке.

Наименование	Описание
Шаблоны **Blockpage (EN)** и **Blockpage (RU)**	Стандартные шаблоны блокировки на английском и русском языках.
Шаблоны **Captive portal user auth (EN)** и **Captive portal user auth (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль). При успешной авторизации пользователь получает доступ в Интернет.
Шаблоны **Captive portal user auth + policy (EN)** и **Captive portal user auth + policy (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль), правила пользования сетью (соглашение об использовании), а также требует принятия пользователем правил политики доступа. При успешной авторизации пользователь получает доступ в Интернет.
Шаблоны **Captive portal: email auth (EN)** и **Captive portal: email auth (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя письмом по email. Для корректной работы данных шаблонов необходимо настроить раздел **Оповещения** в Captive-профиле.
Шаблон **Captive portal: SMS auth (EN)** и **Captive portal: SMS auth (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя с помощью SMS. Для корректной работы данных шаблонов необходимо настроить раздел **Оповещения** в Captive-профиле.
Шаблон **Captive portal policy (EN)** и **Captive portal policy (RU)**	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. При согласии с политикой доступа пользователь получает доступ в интернет. Для работы данного шаблона требуется установить метод **Принять политику** в качестве метода аутентификации в Captive-профиле.
Шаблоны **Captive portal user session (EN)** и **Captive portal user session (RU)**	Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps.
Шаблоны **Content warning (EN)** и **Content warning (RU)**	Шаблоны на английском и русском языках, содержащие страницу предупреждения, отображаемую при срабатывании правила контентной фильтрации с действием **Предупредить.**
Шаблоны **FTP client (EN)** и **FTP client (RU)**	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP.
Шаблоны **SSL VPN (EN)** и **(RU)**	Шаблоны на английском и русском языках для отображения страницы веб-портала.
Шаблоны **SSL VPN RDP (EN)** и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал.
Шаблоны **SSL VPN SSH (EN)** и **(RU)**	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал.
Шаблоны **TOTP INIT PAGE (EN)** и **TOTP INIT PAGE (RU)**	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей.

Для создания собственного шаблона необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Экспортировать существующий шаблон, поставляемый по умолчанию.	Выбрать один из существующих шаблонов, нажать на кнопку **Экспорт** и сохранить шаблон в файле.
Шаг 2. Изменить экспортированный шаблон.	Используя редактор, изменить содержание шаблона. Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут испортить внутреннюю структуру шаблона. Используйте простые редакторы текста.
Шаг 3. Создать новый шаблон.	Нажать на кнопку **Добавить**, выбрать соответствующий тип шаблона, задать название шаблону и сохранить его.
Шаг 4. Импортировать измененный на шаге 2 шаблон.	Выделить вновь созданный шаблон, нажать на кнопку **Импорт** и выбрать файл с измененным шаблоном.

Категории URL

Version: 5.x, 6.1.9, 7.0.1
Documentation: ☑
Product: NGFW

Элемент библиотеки **Категории URL** позволяет создать группы категорий UserGate URL filtering для более удобного использования в правилах фильтрации контента. Например, администратор может создать группу категорий «Бизнес категории» и поместить в нее необходимые категории.

Для использования категорий UserGate URL filtering требуется наличие специальной лицензии.

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы.

Наименование	Описание
Threats	Набор категорий, рекомендованных для блокировки в целях обеспечения безопасности сети.
Parental Control	Набор категорий, рекомендованных для блокировки в целях защиты детей от нежелательного контента.
Productivity	Набор категорий, рекомендованных для блокировки в целях повышения эффективности работы сотрудников.
Safe categories	Набор категорий, считаемых безопасными для посещения. Рекомендуется отключать морфологическую проверку, перехват HTTPS-трафика для данной группы категорий в целях уменьшения количества ложных срабатываний.
Recommended for morphology checking	Набор категорий, рекомендованных для проверки с помощью морфологического анализа. Из этого набора исключены такие категории, как «Новости», «Финансы», «Правительство», «Информационная безопасность», «Детские сайты» и ряд других в целях уменьшения количества ложных срабатываний. Этот же набор категорий рекомендуется использовать для перехвата трафика HTTPS.
Recommended for virus check	Набор категорий, рекомендованных для антивирусной проверки.

Для добавления новой группы категорий необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу категорий.	В панели **Группы URL** категорий нажать на кнопку **Добавить**, дать название группе.
Шаг 2. Добавить категории.	Выделить созданную группу и в панели **Категории**, нажать на кнопку **Добавить** и выбрать необходимые категории из списка.

В системе определены следующие категории URL:

ID	Уровень риска	Название	Описание
0	Высокий (4)	Неизвестная тематика / Unknown	Сайты без принадлежности к какой-либо категории.
1	Высокий (4)	Реклама и всплывающие окна / Advertisements and Pop-Ups	Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее).
2	Низкий (2)	Алкоголь и табак / Alcohol and Tobacco	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции
3	Очень высокий (5)	Анонимайзеры / Anonymizers	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхождения средств веб-фильтрации и т.д.
4	Очень низкий (1)	Искусство / Arts	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.
5	Очень низкий (1)	Бизнес / Business	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности.
6	Очень низкий (1)	Транспорт / Transportation	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами, сообщества, клубы автолюбителей и т.д.
7	Средний (3)	Чаты / Chat	Сайты, позволяющие осуществлять общение в режиме реального времени.
8	Очень низкий (1)	Детские сайты / Kids sites	Сайты, ориентированные на детскую аудиторию
9	Низкий (2)	Форумы и новостные ленты / Forums and Newsgroups	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.
10	Очень высокий (5)	Заражённые сайты / Compromised	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения.
11	Очень низкий (1)	Компьютеры и технологии / Computers and Technology	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.
12	Средний (3)	Преступная деятельность / Criminal Activity	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения.

ID	Уровень риска	Название	Описание
13	Средний (3)	Сайты знакомств / Dating and Personals	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.
0	Высокий (4)	Неизвестная тематика / Unknown	Сайты без принадлежности к какой-либо категории.
14	Высокий (4)	Download-архивы / Download Sites	Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты.
1	Высокий (4)	Реклама и всплывающие окна / Advertisements and Popups	Сайты, содержащие рекламу (баннеры, всплывающие окна и прочее).
15	Очень низкий (1)	Образование / Education	Сайты, содержащие учебные заведения и школы всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.
2	Низкий (2)	Алкоголь и табак / Alcohol and Tobacco	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции.
16	Низкий (2)	Развлечения / Entertainment	Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.
3	Очень высокий (5)	Анонимайзеры / Anonymizers	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхода средств фильтрации трафика.
17	Низкий (2)	Финансы / Finance	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.
4	Очень низкий (1)	Искусство / Arts	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.
18	Высокий (4)	Азартные игры / Gambling	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.
5	Очень низкий (1)	Бизнес / Business	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах, необходимых предприятиям любого размера для успешной деятельности.
19	Низкий (2)	Игры / Games	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
6	Очень низкий (1)	Транспорт / Transportation	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами, сообщества любителей автомобилей и т.д.
20	Очень низкий (1)	Правительство / Government	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.
7	Средний (3)	Чаты / Chat	Сайты, позволяющие осуществлять общение в режиме реального времени.
21	Низкий (2)	Ненависть и нетерпимость / Hate and Intolerance	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
8	Очень низкий (1)	Детские сайты / Kids sites	Сайты, ориентированные на детскую аудиторию
22	Низкий (2)	Здоровье и медицина / Health and Medicine	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной,
9	Низкий (2)	Форумы и новостные ленты / Forums and Newsgroups	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги. рецептами лекарств, и т.д.
23	Низкий (2)	Заражённые сайты / Compromised	Сайты, информация о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами. В
10	Очень высокий (5)	Наркотики / Illegal Drug	категорию также входят ресурсы из группы высокого риска заражения.
24	Очень низкий (1)	Поиск работы / Job Search	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по
11	Очень низкий (1)	Компьютеры и технологии / Computers and Technology	трудоустройству и рекрутинговых компаний. Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.
25	Средний (3)	Военные сайты / Military	Информация о военных организациях, военной истории.
12	Средний (3)	Преступная деятельность / Criminal Activity	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном
26	Высокий (4)	Потоковое мультимедиа и загрузки / Streaming Media and Downloads	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.
27	Очень низкий (1)	Новости / News	Новостные сайты: онлайн-журналы, новостные ленты и т.д.
13	Средний (3)	Сайты знакомств / Dating and Personals	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.
28	Низкий (2)	Некоммерческие и неправительственные организации / Non-profit and NGOs	Сайты, посвященные клубам, сообществам, союзам и некоммерческим организациям. Значительное число данных структур созданы в образовательных или благотворительных целях.
14	Высокий (4)	Download-архивы / Download Sites	Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты.
29	Низкий (2)	Нудизм / Nudity	Ресурсы, содержащие изображение частичной или полной наготы. Категория включает в себя сайты, рекламирующие и распродающие нижнее белье или купальную одежду или купальные костюмы.
15	Очень низкий (1)	Образование / Education	Сайты, содержащие учебные заведения и школы всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.
30	Средний (3)	Персональные сайты / Personal Sites	Персональные сайты, созданные отдельными людьми или группами лиц, блоги.
16	Низкий (2)	Развлечения / Entertainment	Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.
31	Очень высокий (5)	Фишинг и мошенничество / Phishing and Fraud	Сайты, которые используются для обмана или в мошеннических целях (например, фишинг), такие как кражи финансовой или другой информации посредством учетной записи пользователя. Эти сайты чаще всего являются искусно выполненной подделкой популярных
17	Низкий (2)	Финансы / Finance	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний, порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.
32	Очень низкий (1)	Политика / Politics	Сайты, посвященные политическим партиям или занимающиеся политической пропагандой, а также предоставляющие информацию о группах интересов, выборах, законодательстве или вопросе лоббирования. Категория включает в себя сайты, которые предлагают сведения о правах и
18	Высокий (4)	Азартные игры / Gambling	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами. их защите.
19	Низкий (2)	Игры / Games	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
33	Очень высокий (5)	Порнография и насилие / Pornography/Sexually Explicit	Сайты, которые содержат контент сексуального содержания. Категория включает в себя продукцию для взрослых, такую как секс-игрушки, компакт-диски и видео. Сайты из данной группы позволяют заказывать эскорт-услуги, получить сведения о стриптиз-клубах, почитать
20	Очень низкий (1)	Правительство / Government	эротические рассказы и текстовые описания порно актов. Находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.
34	Низкий (2)	Недвижимость / Real Estate	Информация об аренде, покупке или продаже недвижимости или земельных участков. Рекомендации по покупке или продаже жилых помещений. Агентства недвижимости, услуги по аренде, переезду, улучшению жилищных условий.
21	Низкий (2)	Ненависть и нетерпимость / Hate and Intolerance	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
35	Низкий (2)	Религия / Religion	Сайты, посвященные вопросу веры, человеческой духовности и религиозным убеждениям, в том числе сайты церквей, синагог, мечетей и других молитвенных домов.
22	Низкий (2)	Здоровье и медицина / Health and Medicine	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной,
36	Очень низкий (1)	Рестораны и еда / Restaurants and Dining	рецептами лекарств, и т.д. Сайты, содержащие списки, обзоры заведений общественного питания. Категория включает в себя сайты с рецептами, инструкциями и советами, продуктами питания и советами по выбору вина.
23	Низкий (2)	Наркотики / Illegal Drug	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами.
37	Очень низкий (1)	Поисковые системы и порталы / Search Engines and Portals	Сайты, позволяющие осуществлять поиск в интернете по новостям, изображениям, каталогам и другим видам онлайн-контента. Категория включает в себя порталы и каталоги сайтов, такие как белые/желтые страницы.
24	Очень низкий (1)	Поиск работы / Job Search	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.
38	Низкий (2)	Покупки / Shopping	Интернет-магазины, каталоги, аукционы, рекламные объявления. Категория не включает в себя ресурсы, посвященные товарам и услугам из более узких категорий, таких как здравоохранение и медицина.
25	Средний (3)	Военные сайты / Military	Информация о военных организациях, военной истории.
39	Средний (3)	Социальные сети / Social Networking	Сайты социальных сетей, пользователи которых могут общаться, взаимодействовать, обмениваться сообщениями, файлами.
26	Высокий (4)	Потоковое мультимедиа и загрузки / Streaming Media and Downloads	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.

ID	Уровень риска	Название	Описание
41	Очень низкий (1)	Неизвестная тематика / Unknown	Сайты команд или спортивных ассоциаций, международные и национальные, спортивные колледжи. Ресурсы, содержащие результаты и расписания игр, спортивные журналы и газеты, виртуальный спорт и спортивные лиги.
1	Высокий (4)	Спорт / Sports	Сайты без принадлежности к какой-либо категории.
42	Очень высокий (5)	Вредоносное ПО / Malware	Сайты, содержащие нежелательные программы, автоматически загружающиеся и устанавливающиеся на ПК пользователей. Вирусы вносят изменения в системы, а хакеры получают данные с компьютера без ведома и согласия его владельца.
1	Высокий (4)	Реклама и всплывающие окна / Advertisements and Pop-Ups	Сайты, содержащие рекламную рассылку (баннеры, всплывающие окна и прочее).
43	Низкий (2)	Фондовый рынок / Stock trading	Сайты по торговле ценными бумагами и управления инвестиционными активами. Также включает информацию о финансово-инвестиционной стратегии, котировках и новостях.
2	Низкий (2)	Алкоголь и табак / Alcohol and Tobacco	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции
44	Очень низкий (1)	Переводчики / Translators	Сайты, на которых возможен онлайн-перевод веб-страниц на другие языки. Данные ресурсы могут использоваться для обхода заданных отличающихся списков просмотра сайтов осуществляется с URL-сайта онлайн-переводчика.
3	Очень высокий (5)	Анонимайзеры / Anonymizers	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхождения средств веб-фильтрации и т.д.
45	Очень низкий (1)	Путешествия / Travel	Авиакомпании, агентства по бронированию авиабилетов, планирование поездок, предварительные заказы, аренда транспортных средств, описание мест назначения, реклама гостиниц и казино.
4	Очень низкий (1)	Искусство / Arts	Сайты, посвященные искусству, в том числе различным театрам, музеям, галереям, фотографии, танцевальным коллективам и т.д.
5	Очень низкий (1)	Бизнес / Business	Сайты, содержащие отображение текстовые описания и аргументации физических насилия против людей, животных или
46	Низкий (2)	Насилие / Violence	организаций сообществ. Категория включает в себя ресурсы с иллюстрациями ужасов природы, а также сайты, содержащие ненормативную лексику.
6	Очень низкий (1)	Транспорт / Transportation	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами,
47	Низкий (2)	Оружие / Weapons	Сайты, содержащие изображения, обзоры и описания оружия. В категории также входят интернет-магазины орудий и оружия, в том числе для занятия спортом.
7	Средний (3)	Чаты / Chat	Сайты, позволяющие осуществлять общение в режиме реального времени.
48	Высокий (4)	Веб-почта / Web-based Email	Порталы, позволяющие завести собственные почтовые аккаунты для написания, чтения, отправки и получения электронных писем.
8	Очень низкий (1)	Детские сайты / Kids sites	Сайты, ориентированные на детскую аудиторию
49	Средний (3)	Общие / General	Сайты, которые не попадают в другие категории, например, пустые веб-страницы.
9	Низкий (2)	Форумы и новостные ленты / Forums and Newsgroups	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.
50	Низкий (2)	Подписка/регистрация / Leisure and Recreation	Сайты, связанные с рекреационной деятельностью и увлечениями, включая ресурсы, посвященные зоопаркам, центрам общественного отдыха, бассейнам, паркам развлечениям и хобби, таким как садоводство, литература, искусства и ремесла, домашний декор и т.д.
10	Очень высокий (5)	Заражённые сайты / Compromised	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В
51	Низкий (2)	Онлайн-обучение / Online training and tools	категорию также входят ресурсы из группы высокого риска заражения. Дистанционное образование, онлайн-курсы, профессиональное обучение, программы обучения, повышения квалификации.
52	Низкий (2)	Компьютеры и технологии / Computers and Technology	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных
11	Очень низкий (1)	Юриспруденция / Legal	устройствах, технологиях и услугах. Сайты юридических фирм, обсуждение и анализ юридических вопросов.
53	Низкий (2)	Местные достопримечательности /	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о
12	Средний (3)	Преступная деятельность / Criminal Activity	том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д. В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения.
54	Низкий (2)	Справочная информация / Reference and Research	Профессиональные или образовательные справочные материалы, в том числе онлайн-словари, карты, переписи, альманахи, каталоги библиотек, генеалогии, и научной информации.
13	Средний (3)	Сайты знакомств / Dating and Personals	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для
55	Очень низкий (1)	Форумы с технической или бизнес-информацией / Technical or business forums and news groups	сватовства, знакомств, ресурсы, предлагающие эскорт-услуги. Сайты с обсуждениями, относящимися к деловой или технической тематикам.
14	Высокий (4)	Download-архивы / Download Sites	Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты.
56	Очень низкий (1)	Техническая информация / Technical information and documentation	Сайты, которые предоставляют информацию к техической документации и информации.
15	Очень низкий (1)	Образование / Education	Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические материалы.
57	Высокий (4)	Персональные хранилища / Personal Storage	Сайты, которые позволяют загружать файлы и резервные копии для удаленного хранения данных.
16	Низкий (2)	Развлечения / Entertainment	Сайты, предлагающие пользователю телеканалы, кино, музыку и видео (в том числе видео по запросу). Категория также включает в себя сайты знаменитостей и развлекательные новости.
58	Низкий (2)	CDNs	Сети предоставления контента
17	Низкий (2)	Финансы / Finance	Сайты, связанные с банками, финансами, платежами или инвестициями. В категорию входят интернет-ресурсы банков, брокерских компаний,
59	Низкий (2)	Ненсурная лексика / Profanity	порталы для онлайн-торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д. Сайты, содержащие нецензурную лексику.
18	Высокий (4)	Азартные игры / Gambling	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.
60	Низкий (2)	Профессиональные социальные сети / Professional social networks	Подмножество веб-сайтов социальных сетей, которое включает в себя контент, предназначенный исключительно для бизнеса и профессионалов.
19	Низкий (2)	Игры / Games	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
61	Очень высокий (5)	Ботнеты / Botnets	Сайты, которые управляют сетями ботов через командно-контрольные центры.
20	Очень низкий (1)	Правительство / Government	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.
62	Низкий (2)	Религиозные культы / Cults	Сайты, связанные с нетрадиционной религиозной практикой, обычно называемой культами. Подобные движения считаются ложными, неортодоксальными, экстремистскими. Члены культов зачастую живут под руководством харизматического лидера.
21	Низкий (2)	Ненависть и нетерпимость / Hate and Intolerance	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
63	Низкий (2)	Мода и красота / Fashion and Beauty	Сайты о моде, ювелирных изделиях, гламуре, красоте, модельном бизнесе, косметике или связанных со всем перечисленным товарах или услугах. Включает отзывы, сравнения, а также общую информацию, полезную потребителю.
22	Низкий (2)	Здоровье и медицина / Health and Medicine	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной,
64	Низкий (2)	Поздравительные открытки / Greeting cards	рецептами лекарств, и т.д. Сайты, которые позволяют людям получать и отправлять поздравительные открытки.
23	Низкий (2)	Наркотики / Illegal Drug	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении
65	Очень высокий (5)	Хакерство / Hacking	Сайты, которые предоставляют или содержат рекомендации о том, как получить несанкционированный доступ к компьютерным системам с целью кражи информации, совершения мошеннических действий, советы по созданию вирусов или совершению других видов незаконной деятельности, связанной с кражей цифровой информации.
24	Очень низкий (1)	Поиск работы / Job Search	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.
66	Очень высокий (5)	Криптомайнеры / Cryptocurrency Mining	Сайты, которые используют технологии майнинга криптовалют без разрешения пользователя.
25	Средний (3)	Военные сайты / Military	Информация о военных организациях, военной истории.
67	Очень высокий (5)	Нелегальное ПО / Illegal Software	Сайты, которые незаконно распространяют программное обеспечение или защищенные авторским правом материалы, такие как фильмы, музыка, незаконные серийные номера, генераторы ключей.
26	Высокий (4)	Потоковое мультимедиа и загрузки / Streaming Media and Downloads	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.

ID	Уровень риска	Название	Описание
68	Высокий (4)	Обмен картинками / Image Sharing	Порталы для размещения цифровых фотографий и изображений, фотоальбомы и фотообменники.
0	Высокий (4)	Неизвестная тематика / Unknown	Сайты без принадлежности к какой-либо категории.
69	Низкий (2)	Информационная безопасность / Information Security	Сайты, которые предоставляют информацию о законной защите данных, в том числе о новых угрозах и способах борьбы с ними.
1	Высокий (4)	Реклама и всплывающие окна / Advertisements and Popups	Сайты, содержащие графическую рекламу (баннеры, всплывающие окна и прочее).
70	Средний (3)	Сервисы мгновенных сообщений / Instant Messaging	Сайты, которые позволяют создавать и использовать аккаунт в службах обмена мгновенными сообщениями, таких как ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, и т.п.
2	Низкий (2)	Алкоголь и табак / Alcohol and Tobacco	Сайты, посредством которых реализуется продвижение или продажа алкогольной и табачной продукции
71	Очень низкий (1)	Сетевые ошибки / Network Errors	Сайты, которым не присвоен IP-адрес.
3	Очень высокий (5)	Анонимайзеры / Anonymizers	Сайты, предоставляющие возможность анонимного посещения других сайтов и ресурсов интернета. Анонимайзеры также могут применяться для обхождения средств веб-фильтрации и т.д.
72	Средний (3)	Паркованные домены / Parked Domains	К паркованным доменам относятся URL-адреса с ограниченным контентом, конечные точки перехода с рекламных объявлений. Подобные ресурсы могут приносить прибыль, но, как правило, не несут в себе полезной для пользователя информации. Категория также включает в себя
4	Очень низкий (1)	Искусство / Arts	Сайты, находящиеся на реконструкции, папки и базовые страницы веб серверов. Сайты, посвященные искусству в том числе различным галереям, музеям, фотографии, танцевальным коллективам и т.д.
73	Высокий (4)	Пиринговые сети / Peer-to-Peer	К данной категории относятся корпоративные веб-сайты, а также интернет-ресурсы, содержащие информацию об услугах и продуктах,
5	Очень низкий (1)	Бизнес / Business	Сайты, позволяющие осуществлять прямой обмен файлами между пользователями вне зависимости от центрального сервера. необходимых предприятиям любого размера для успешной деятельности.
74	Высокий (4)	Частные IP-адреса / Private IP Addresses	Сайты, посвященные автотранспорту и его покупке. Категория включает в себя интернет-ресурсы производителей, дилеров, сайты с обзорами,
6	Очень низкий (1)	Транспорт / Transportation	Включает наборы IP-адресов, определенные в RFC 1918. сообщества, клубы автолюбителей и т.д.
7	Средний (3)	Чаты / Chat	Сайты, позволяющие осуществлять общение в режиме реального времени
75	Низкий (2)	Школьное мошенничество / School Cheating	Сайты с ответами на различные школьные тесты, написанными эссе, рефератами, исследовательскими или курсовыми работами.
8	Очень низкий (1)	Детские сайты / Kids sites	Сайты, ориентированные на детскую аудиторию
76	Низкий (2)	Половое воспитание / Sex Education	Сайты, связанные с сексуальным образованием, включая такие темы, как уважение к партнеру, аборты, бисексуальный образ жизни, противозачаточные средства, заболевания, передаваемые половым путем и беременность.
9	Низкий (2)	Форумы и новостные ленты / Forums and Newsgroups	Ленты новостей, форумы, доски объявлений. Категория не включает в себя персональные блоги.
77	Средний (3)	Сайты сомнительного содержания / Tasteless	Сайты с оскорбительным контентом, такого рода как юмор "ниже пояса", ужасный или даже пугающий контент, шокирующие изображения крови, ран или жестокого обращения с животными.
10	Очень высокий (5)	Заражённые сайты / Compromised	Сайты, контроль над которыми был захвачен злоумышленниками для распространения вредоносных программ без ведома владельцев. В категорию также входят ресурсы из группы высокого риска заражения.
78	Низкий (2)	Жестокое обращение с детьми / Child Abuse Images	Сайты, содержащие фотографии, иллюстрирующие случаи жестокого обращения с детьми.
11	Очень низкий (1)	Компьютеры и технологии / Computers and Technology	Сайты, содержащие обзоры продуктов, новости и информация о компьютерах, программном обеспечении, оборудовании, периферийных устройствах, технологиях и услугах.
79	Очень низкий (1)	Нетрадиционная сексуальная ориентация / Gay, Lesbian or Bisexual	Сайты, содержащие материалы о геях, лесбиянках, трансгендерах.
12	Средний (3)	Преступная деятельность / Criminal Activity	Сайты, предлагающие советы и рекомендации по совершению противоправных или преступных действий, а также содержащие информацию о том, как скрыть следы преступления. На подобных ресурсах можно узнать о том, как совершить убийство, создать бомбу, взломать замки и т.д.
80	Низкий (2)	Литература и книги / Literature and Books	В данную категорию также включены сайты о незаконном использовании электронных устройств, хакерстве, мошенничестве и незаконном распространении программного обеспечения. Сайты, содержащие опубликованные книги, новеллы, рассказы, включая фантастику, биографии.
81	Низкий (2)	Здоровое питание и диеты / Nutrition and Diet	Сайты, посвященные правильному питанию, снижению веса, диетам.
13	Средний (3)	Сайты знакомств / Dating and Personals	Сайты, способствующие налаживанию межличностных отношений, таких как знакомства и брак. Категория включает в себя сайты для сватовства, знакомств, ресурсы, предлагающие эскорт-услуги.
82	Низкий (2)	Домашние животные / Pets and Animals	Сайты, посвященные продуктам и сервисам для домашних и других животных.
14	Высокий (4)	Download-архивы / Download Sites	Сайты, которые содержат доступное для скачивания программное обеспечение. Данная категория также включает в себя некоторые Peer-to-Peer сайты.
84	Низкий (2)	Обновления / Updates	Сайты обновлений программного обеспечения, обновлений операционных систем, обновлений
15	Очень низкий (1)	Образование / Education	Сайты, поддерживаемые учебными заведениями и школами всех типов, включая дистанционное обучение. Включает в себя общеобразовательные и справочные материалы, такие как словари, энциклопедии, интерактивные курсы, учебные пособия и методические
85	Средний (3)	Чат-бот с искусственного интеллекта / Chat-bot AI	Сайты, предоставляющие доступ к чат-ботам искусственного интеллекта, подобным Chat GPT. материалы.
16	Низкий (2)	Развлечения / Entertainment	Сайты, предлагающие полезную информацию о культуре, искусстве, кино, видео (в том числе видео по запросу). Категория также включает в себя
97	Низкий (2)	Репутация: Низкий риск / Reputation: Low risk	сайты с низкой репутационной оценкой риска. Как правило, это сайты, не имеющие известных вредоносных свойств, но относящиеся к категориям, в которых сайты нарушителей безопасности появляются. новости.
98	Средний (3)	Репутация: Средний риск / Reputation: Medium risk	Сайты, с средним репутационным риском. Как правило, это сайты, которые могут содержать интернет-ресурсы бизнеса, брокерских и дилерских
17	Низкий (2)		организаций, а также торговли на бирже. На данных ресурсах также можно узнать котировки акций, информацию об управлении фондами, страховых компаниях, кредитных союзах и т.д.
99	Очень высокий (5)	Репутация: Высокий риск / Reputation: High risk	Сайты с высоким репутационным риском. Сайты с известными уязвимостями.
18	Высокий (4)	Азартные игры / Gambling	Сайты, связанные с азартными играми, лотереями, казино и букмекерскими агентствами.
19	Низкий (2)	Игры / Games	Сайты, связанные с компьютерными или другими видами игр. Ресурсы содержат информацию о разработчиках игр, кодах и читах.
20	Очень низкий (1)	Правительство / Government	Сайты, находящиеся в ведении правительственных или военных организаций, ведомств или учреждений, в том числе отделений полиции, пожарной охраны, таможенных бюро, аварийных служб, гражданской обороны, служб борьбы с терроризмом и больниц.
21	Низкий (2)	Ненависть и нетерпимость / Hate and Intolerance	Интернет-ресурсы, посвященные вопросу поощрения ущемления прав людей в зависимости от расы, религии, пола, возраста, инвалидности, сексуальной ориентации или национальности.
22	Низкий (2)	Здоровье и медицина / Health and Medicine	Сайты, содержащие информацию, относящуюся к поддержанию здоровья, медицинским услугам, фитнесу и благополучию. В данную категорию также включены интернет-ресурсы, связанные с медицинским оборудованием, больницами, аптеками, сестринским делом, медициной, рецептами лекарств, и т.д.
23	Низкий (2)	Наркотики / Illegal Drug	Сайты с информацией о приобретении, производстве и использовании незаконных или рекреационных наркотиков, а также злоупотреблении отпускаемыми по рецепту лекарствами.
24	Очень низкий (1)	Поиск работы / Job Search	Сайты, содержащие списки вакансий, оказывающие помощь в поиске работы. В категорию входят интернет-ресурсы агентств по трудоустройству и рекрутинговых компаний.
25	Средний (3)	Военные сайты / Military	Информация о военных организациях, военной истории.
26	Высокий (4)	Потоковое мультимедиа и загрузки / Streaming Media and Downloads	Сайты, содержащие потоковый контент, например, интернет-радио, интернет-телевидение или MP3-live. Категория включает в себя фан- или официальные сайты музыкантов, групп или звукозаписывающих компаний.

Измененные категории URL

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Библиотека **Измененные категории URL** предназначена для переопределения категорий сайтов. Назначенные пользователем категории имеют приоритет над категориями, определенными специалистами UserGate. Переопределение может потребоваться при ошибочной категоризации сайта или при отсутствии у него категории.

Для переопределения категории:

1. Проверьте категорию сайта. В разделе **Настройки → Библиотеки → Измененные категории URL** введите адрес сайта в строку проверки и нажмите **Проверить категорию**.
2. Если текущая категория не соответствует требуемой, нажмите **Добавить** и назначьте сайту до двух новых категорий.

После сохранения изменений сайт будет добавлен в список переопределений. Для каждой записи отображаются дата изменения, имя администратора, выполнившего изменение, исходные и назначенные категории.

При дальнейших проверках система будет возвращать категории, назначенные пользователем, а также специальную категорию **Переопределенные пользователем категории**.

Для массового назначения категорий сайтам можно импортировать список переопределений из файла в формате TXT и CSV.

Каждая строка файла должна содержать следующие поля, разделенные запятыми:

A,B,C,D,E

где:

- A — доменное имя сайта, для которого необходимо переопределить категорию;
- B — идентификатор назначаемой категории;
- C — идентификатор ранее определенной категории (опциональный информационный параметр); укажите 0, если категория ранее не была определена;
- D — временная метка в формате UTC Timestamp (получить значение можно по ссылке);
- E — комментарий или описание (опциональный параметр).

Идентификаторы категорий URL можно посмотреть по ссылке.

ПримечаниеУдаление записи из библиотеки не приводит к восстановлению исходной категории сайта. Назначенная ранее измененная категория сохраняется.

Пример текстового файла импорта со списком переопределений:

test1test1.ru,69,0,Admin,1780368107,Тест 1
test2test2.ru,69,0,Admin,1780368108,Тест 2
test3test3.ru,69,0,Admin,1780368109,Тест 3

Приложения

Documentation: ☑
Version: 7.0.1, 6.1.9, 5.x

Элемент библиотеки **Приложения** позволяет создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика. Например, администратор может создать группу приложений «Бизнес приложения» и поместить в нее необходимые приложения.

Для добавления новой группы приложений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу приложений.	В панели **Группы приложений** нажать на кнопку **Добавить**, дать название группе.
Шаг 2. Добавить приложения.	Выделить созданную группу и в панели **Приложения**, нажать на кнопку **Добавить** и выбрать необходимые приложения из списка.

Почтовые адреса

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов.	В панели **Группы почтовых адресов** нажать на кнопку **Добавить**, дать название группе.
Шаг 2. Добавить почтовые адреса в группу.	Выделить созданную группу, в панели **Почтовые адреса** нажать на кнопку **Добавить** и добавить необходимые почтовые адреса.

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл **list.txt** со списком почтовых адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом NGFW создать список адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52  list.zip
```

Номера телефонов

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров.	В панели **Группы телефонных номеров** нажать на кнопку **Добавить**, дать название группе.
Шаг 2. Добавить номера телефонов в группу.	Выделить созданную группу, в панели **Группа телефонных номеров** нажать на кнопку **Добавить** и добавить необходимые номера.

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл **list.txt** со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем **list.zip**.
Шаг 3. Создать файл с версией списка.	Создать файл **version.txt**, внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте **list.zip** и **version.txt**, чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом NGFW создать список адресов. При создании указать тип списка **Обновляемый** и адрес, откуда необходимо загружать обновления. NGFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

UserGate может проверять чек-сумму файлов обновляемых списков. Для приведенного примера межсетевой экран будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной.
Получить чек-сумму в linux можно командой:

md5sum list.zip

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

04d7d1223ba8ff02396355a2bc3b3d52 list.zip

Профили СОВ

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1

Профиль СОВ — это набор сигнатур, релевантных для защиты определенных сервисов. Администратор может создать необходимое количество профилей СОВ для защиты различных сервисов. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты сервиса. Например, для защиты сервиса, работающего по протоколу TCP, не стоит добавлять сигнатуры, разработанные для протокола UDP. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора. Более подробно о создании и использовании профилей СОВ смотрите в разделе Система обнаружения и предотвращения вторжений.

Профили оповещений

Version: 5.x, 6.1.9, 7.0.1
Documentation: ☑
Product: NGFW

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail.
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Авторизация	Включает авторизацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL -- 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Профили Netflow

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Профиль Netflow позволяет указать параметры необходимые для отсылки информации на коллектор Netflow. Для создания профиля Netflow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили Netflow** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля Netflow.
Описание	Описание профиля Netflow.
IP-адрес Netflow коллектора	IP-адрес сервера, куда сенсор будет отправлять статистику.
Порт Netflow коллектора	UDP порт, на котором коллектор будет принимать статистику.
Версия протокола	Версия протокола Netflow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе.
Таймаут активного потока (сек)	При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию — 1800 секунд.
Таймаут неактивного потока (сек.)	Время, резервируемое на завершение неактивного потока. Значение по умолчанию — 15 секунд.
Количество потоков	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию — 2000000, установите 0 для снятия ограничения.
Отправлять информацию NAT	Отправлять информацию о NAT преобразованиях в статистику Netflow.
Частота отправки шаблона (пакетов)	Количество пакетов, после которых шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
Период отправки старого шаблона (сек.)	Время, через которое старый шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Профили LLDP

Documentation: ☑
Product: NGFW
Version: 7.0.1

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевым устройствам, работающим в локальной сети, объявлять о своём существовании и передавать свои характеристики и получать аналогичные сведения. Информация, собранная при помощи операции LLDP, хранится в сетевом устройстве.

Для создания профиля безопасности необходимо нажать **Добавить** в разделе **Библиотеки → Профили LLDP** и указать следующие параметры:

Наименование	Описание
Название	Название профиля LLDP.
Описание	Описание профиля LLDP.
Статус порта	Режим: • **Приём и передача данных LLDP** — NGFWe будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • **Только приём данных LLDP** — NGFW не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • **Только передача данных LLDP** — NGFW будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей.

Профили SSL

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, которые в дальнейшем могут быть использованы в правилах инспектирования SSL, в настройках веб-консоли, страницы авторизации, страницы блокировки, веб-портале.

Для создания профиля SSL необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля SSL.
Описание	Описание профиля SSL.
Протоколы SSL	**Минимальная версия TLS** — устанавливает минимальную версию TLS, которая может быть использована в данном профиле. **Максимальная версия TLS** — устанавливает максимальную версию TLS, которая может быть использована в данном профиле. Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем.

Наименование	Описание
Наборы алгоритмов шифрования	Данный раздел позволяет выбрать необходимые алгоритмы шифрования и цифровой подписи. Возможные значения указаны в виде строк, в которых перечислены алгоритм и подпись. Администратор может указать только те наборы алгоритмов и подписей, которые считает нужным для безопасной работы организации. Список поддерживаемых комбинаций следующий: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256 • TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384 • TLS ECDH ECDSA WITH AES 256 GCM SHA384 • TLS ECDH RSA WITH 3DES EDE CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA256 • TLS ECDH RSA WITH AES 128 GCM SHA256 • TLS ECDH RSA WITH AES 256 CBC SHA • TLS ECDH RSA WITH AES 256 CBC SHA384 • TLS ECDH RSA WITH AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH 3DES EDE CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA256 • TLS ECDHE ECDSA WITH AES 128 GCM SHA256 • TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS GOST2012256 WITH 28147 CNT IMIT • TLS GOSTR341001 WITH 28147 CNT IMIT • TLS RSA WITH 3DES EDE CBC SHA • TLS RSA WITH AES 128 CBC SHA • TLS RSA WITH AES 128 CBC SHA256 • TLS RSA WITH AES 128 GCM SHA256 • TLS RSA WITH AES 256 CBC SHA • TLS RSA WITH AES 256 CBC SHA256 • TLS RSA WITH AES 256 GCM SHA384
Установка алгоритмов шифрования для стандартных протоколов	Данный раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле **Выберите протокол для установки алгоритмов** необходимые версии протоколов TLS, нажать на кнопку **Применить**, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно последовательно добавить несколько версий протокола TLS.

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором как есть, либо изменены/удалены при необходимости. Созданы следующие профили

SSL:

Наименование	Описание
Default SSL profile	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.1 до TLS v.1.2. Это наиболее распространенные версии протоколов, используемые в сети интернет в данное время. Данный профиль используется по умолчанию в: • Правилах инспектирования трафика SSL. • Для страницы авторизации Captive-портала. • Для страницы блокировки. • В веб-портале.
Default SSL profile (TLSv1.3)	Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется.
Default SSL profile (GOST)	Содержит алгоритмы и подписи, соответствующие TLS с ГОСТ-алгоритмами (TLS GOST2012256 with 28147 CNT IMIT и TLS GOSTR341001 with 28147 CNT IMIT). Может быть использован в организациях, где требуется использование данных алгоритмов, например, для веб-портала. Поддержка данных протоколов должна также быть обеспечена со стороны используемых браузеров. По умолчанию не используется.
Default SSL profile (web console)	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.0 до TLS v.1.2. Данный профиль используется по умолчанию для предоставления SSL-доступа в веб-консоль. **Важно!** Изменение данного профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа в веб-консоль!

Профили пересылки SSL

Documentation: ☑
Product: NGFW
Version: 7.0.1

Профили пересылки SSL работают совместно с правилами инспектирования SSL и позволяют указать устройства, на которые необходимо отправить копию расшифрованного трафика. Копия трафика будет отправлена в случае успешной расшифровки передаваемого трафика в соответствии с правилом инспектирования и выбранным профилем SSL.

Для создания профиля пересылки необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили пересылки SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля пересылки SSL.
Описание	Описание профиля пересылки SSL.
Тип пересылки	Доступные типы пересылки: • **L2**. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • **L3** туннель: копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адреса источника и назначения.
MAC-адрес назначения	MAC-адрес устройства, на которое необходимо переслать копию расшифрованного трафика. Параметр указывается при выборе типа пересылки L2.
Пересылать на интерфейс	Название интерфейса, на который необходимо пересылать копию расшифрованного трафика. Параметр указывается при выборе типа пересылки L2.
GRE IP-адрес источника	IP-адрес источника туннеля GRE. Параметр указывается при выборе типа пересылки L3.
GRE IP-адрес назначения	IP-адрес назначения туннеля GRE. Параметр указывается при выборе типа пересылки L3.

Интерфейс командной строки (CLI)

Общие положения

Общие положения (Описание)

Documentation: ☑
Product: NGFW
Version: 7.0.1

UserGate NGFW имеет возможность управления через интерфейс командной строки — CLI (Command Line Interface). С помощью CLI администратор может выполнять команды диагностики и мониторинга, производить настройку устройства, а также перезагружать или выключать устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании NGFW), через последовательный порт или с помощью SSH по сети.

CLI имеет два режима работы — режим диагностики и мониторинга, и режим конфигурации.

В **режиме диагностики и мониторинга** доступны команды, позволяющие посмотреть следующее:

- Доступность сетевых ресурсов.
- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Произвести отслеживание пакетов по установленным правилам.
- Мониторинг трафика.
- Информацию о маршрутах.
- Мониторинг состояния кластера.
- Мониторинг заблокированных СОВ IP-адресов.
- Отображение системной информации.
- Диагностику работы протоколов динамической маршрутизации.
- Информацию об авторизованных пользователях.

Приглашение командной строки в режиме диагностики и мониторинга имеет следующий вид:

Admin@NGFW>

Настройка устройства производится в режиме конфигурации.

Для перехода в **режим конфигурации** используется команда:

Admin@NGFW> configure

После перехода в режим конфигурации приглашение командной строки будет выглядеть следующим образом:

Admin@NGFW**#**

Для просмотра подсказки о текущих возможных значениях или для автодополнения команд в обоих режимах работы CLI необходимо нажать клавишу **Tab**. В подсказке могут использоваться следующие вспомогательные символы:

***** — обязательное поле в командах create и ряде других команд;

+ — необязательное/вариативное поле;

> — вложенное поле, после его введения предыдущий список полей становится недоступным, появляется новый список полей, которые можно ввести.

Например:

```
Admin@UGOS# set network virtual-router default
+ interfaces          List of network interfaces attached to this virtual router
> routes              List of static network routes
```

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к NGFW.	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство NGFW не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, пароль — без пароля.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к NGFW.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к NGFW.
Шаг 2. Запустить терминал.	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI.	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство NGFW не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, пароль — без пароля.

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны.	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.

Наименование	Описание
Шаг 2. Запустить SSH-терминал.	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес NGFW, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: ssh *Admin@IPNGFW* -p *2200*
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство NGFW не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, пароль — без пароля.

После успешной авторизации в CLI пользователь попадает в режим диагностики и мониторинга, появляется строка, ожидающая ввода команды.

Для просмотра доступных команд, текущих возможных значений команды или автодополнения необходимо использовать клавишу **Tab**.

Для отмены ввода текущей команды используется сочетание **Ctrl + C**; для просмотра истории команд — ↑, ↓.

Все команды интерфейса командной строки имеют следующую структуру:

<action> <level> <filter> <configuration_info>

где <action>: действие, которое необходимо выполнить.

<level>: уровень конфигурации; уровни соответствуют разделам веб-интерфейса NGFW.

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

CLI поддерживает ввод команды в несколько строк (многострочный ввод). Для перехода на новую строку необходимо добавить "\" в конце строки. Начиная со второй строки ввод "\" необязателен; чтобы завершить ввод необходимо ввести одну пустую строку:

```
Admin@UGOS# set users user example \
... name username1
... enabled on
... groups [ "Default Group" ]
...
Admin@UGOS#
```

Команды, доступные до первичной инициализации узла

Команды, доступные до первичной инициализации узла (Описание)

Documentation: ☑
Product: NGFW
Version: 7.0.1

Если устройство не прошло первоначальную инициализацию, то в CLI доступны команды диагностики и мониторинга, а в режиме конфигурации CLI — только команды настройки сети, т.е. настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов, а также включение/отключение удалённого доступа к серверу radmin-emergency.

Доступные команды в режиме диагностики

Команды диагностики позволяют просмотреть следующее:

- Доступность сетевых ресурсов.
- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Мониторинг трафика.
- Информацию о маршрутах.
- Отображение системной информации.

Подробнее о синтаксисе и примерах использования команд диагностики читайте в разделе Команды диагностики и мониторинга.

Доступные команды в режиме конфигурации

Для перехода в режим конфигурации используется команда:

Admin@NGFW> configure

После перехода в режим конфигурации приглашение командной строки будет выглядеть следующим образом:

Admin@NGFW#

В режиме конфигурации доступны команды *execute* (команды, которые не относятся к настройке конфигурации устройства — ping, date, traceroute и т.п.), команды настройки сети (настройка зон, интерфейсов, шлюзов и виртуальных маршрутизаторов), а также команды включения/отключения удалённого доступа к серверу radmin-emergency.

Подробнее о синтаксисе и примерах использования команд *execute* читайте в разделе Режим конфигурации.

Подробнее о синтаксисе и примерах использования команд настройки сети читайте в следующих разделах:

- Команды настройки зон.
- Команды настройки интерфейсов.
- Команды настройки шлюзов.
- Команды настройки виртуальных маршрутизаторов.

Подробнее о синтаксисе и примерах использования команд включения/отключения удалённого доступа к серверу radmin-emergency читайте в разделе Настройка управления устройством.

Подробнее о первоначальной инициализации устройства с помощью CLI читайте в разделе Первоначальная инициализация.

Первоначальная инициализация

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Первоначальная инициализация

Первичную инициализацию NGFW с использованием интерфейса командной строки можно произвести нескольким способами.

Установка как главного узла.

Для настройки NGFW в качестве главного узла используется команда:

Admin@UGOS# execute install node master

Необходимо указать параметры:

Параметр	Описание
login	Задать логин администратора.
password	Задать пароль учётной записи администратора. Указание пароля также доступно при нажатии **Enter** после указания логина администратора; необходимо дважды ввести пароль учётной записи.

Установка как дополнительного узла кластера.

Для настройки NGFW в качестве дополнительного узла кластера используется команда:

Admin@UGOS# execute install node slave

Необходимо указать параметры:

Параметр	Описание
interface	Интерфейс для подключения к кластеру.
slave-ip	IP-адрес, который будет назначен на интерфейс, использующийся для подключения к кластеру.
gateway-address	IP-адрес шлюза. Шлюз необходимо указывать, если узлы кластера находятся в разных подсетях.
master-ip	IP-адрес мастер-сервера.
master-secret	Секретный код, использующийся для подключения узла в кластер.
login	Логин администратора NGFW.
password	Пароль учётной записи администратора.

Настройка через UGMC

Для настройки NGFW в качестве дополнительного узла кластера используется команда:

Admin@UGOS# execute install node mc

Необходимо указать параметры:

Параметр	Описание
login	Логин администратора UserGate.
password	Пароль учётной записи администратора.
mc-ip	IP-адрес сервера UGMC.
device-code	Уникальный код устройства, использующийся для подключения узла к UGMC.

После первичной инициализации будет доступно полное управление из CLI.

Команды диагностики и мониторинга

Команды диагностики и мониторинга (Описание)

Product: UserGate NGFW
Version: 7.0.1

Команды диагностики позволяют просмотреть следующее:

- Статистику и информацию об интерфейсах.
- Информацию о записях ARP.
- Произвести отслеживание пакетов по установленным правилам.
- Мониторинг трафика.
- Информацию о маршрутах.

Статистика интерфейсов

Для отображения статистики интерфейса и информации о нём используется следующая команда:

Admin@UGOS> show network interface <interface-name>

Также доступно отображение только информации или только статистики интерфейса:

Admin@UGOS> show network interface <interface-name> info

Admin@UGOS> show network interface <interface-name> statistic

ARP-записи

Для просмотра информации о записях ARP:

Admin@UGOS> show network arp

При просмотре записей доступно использование фильтров. Параметры фильтрации:

Параметр	Описание
node-name	Название узла кластера, ARP-записи которого необходимо отобразить. Далее необходимо указать интерфейс или IP-адрес хоста: Admin@UGOS> show network arp node-name <node-name> interface <iface-name> Admin@UGOS> show network arp node-name <node-name> host <ip>
interface	Название интерфейса NGFW.
host	IP-адрес устройства.

Просмотр записей ARP также доступен в режиме конфигурации; команды идентичны командам в режиме диагностики и мониторинга.

ПримечаниеВ режиме диагностики и мониторинга действия производятся с системными записями; в режиме конфигурации - со статическими записями ARP.

Добавление статических ARP-записей доступно в режиме конфигурации с использованием следующей команды:

Admin@UGOS# set network arp

Необходимо указать:

Параметр	Описание
node-name	Название узла кластера, на котором будет создана запись ARP. Далее необходимо указать название интерфейса, IP и MAC-адреса устройства.
interface	Название интерфейса NGFW.
host	IP-адрес устройства.
mac	MAC-адрес устройства.

Команды удаления системных и статических ARP-записей имеют аналогичную структуру, отличается действие, которое необходимо выполнить:

- **clear**: удаление системных записей в режиме диагностики и мониторинга;
- **delete**: удаление статических записей в режиме конфигурации.

Далее будет представлен формат команд удаления на примере команд режима диагностики и мониторинга.

Для удаления системной записи:

Admin@UGOS> clear network arp interface <iface-name> host <ip>

Чтобы удалить запись на другом узле кластера:

Admin@UGOS> clear network arp interface <iface-name> node-name <node-name> host <ip>

Следующая команда позволяет удалить все системные записи на заданном интерфейсе (можно указать несколько интерфейсов):

Admin@UGOS> clear network arp interfaces [<iface-name1> <iface-name2> ...]

Для удаления всех системных записей интерфейса другого узла:

Admin@UGOS> clear network arp interfaces [<iface-name1> <iface-name2> ...] node-name <node-name>

Отслеживание пакетов

Чтобы произвести отслеживание пакетов, используется следующая команда:

Admin@UGOS> show network trace

Будет отображена следующая информация: IP-адреса источника и назначения, протокол, названия портов источника и назначения NGFW, номера TCP/UDP портов источника и назначения. Команда также доступна в режиме конфигурации.

Чтобы выйти из режима отслеживания пакетов — **Ctrl+C**.

Правила отслеживания пакетов создаются и настраиваются в режиме конфигурации на уровне **network**. Для создания правила используется следующая команда:

Admin@UGOS# create network trace-rules

Далее указываются следующие параметры:

Параметр	Описание
enabled	Включение/отключение правила отслеживания пакетов: • **on**. • **off**.
name	Название правила. Если название правила не было задано, то оно задаётся автоматически в формате: trace_rule_N (где N — порядковый номер создаваемого правила отслеживания пакетов).
zones-in	Список зон источников трафика.
source-ip-lists	Список групп IP-адресов источника пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки читайте в разделе Настройка IP-адресов.
source-ip-addresses	Список IP-адресов источника пакета.
dest-ip-lists	Список групп IP-адресов назначения пакета. Подробнее о создании групп IP-адресов с использованием интерфейса командной строки читайте в разделе Настройка IP-адресов.
dest-ip-addresses	Список IP-адресов назначения пакета.
services	Тип сервиса. Подробнее читайте в разделе Настройка сервисов.

Для изменения правила:

Admin@UGOS# set network trace-rules <trace-rule-name>

Для изменения доступны параметры, представленные в таблице выше.

Для удаления правила отслеживания пакетов используется следующая команда:

Admin@UGOS# delete network trace-rules <trace-rule-name>

Также доступно удаление значений отдельных параметров правил. Для удаления доступны:

- **zones-in**.
- **source-ip-lists**.
- **source-ip-addresses**.
- **dest-ip-lists**.
- **dest-ip-addresses**.
- **services**.

Чтобы просмотреть существующие правила отслеживания пакетов:

Admin@UGOS# show network trace-rules

или

Admin@UGOS# show network trace-rules <trace-rule-name>

Мониторинг трафика

Следующая команда используется для мониторинга трафика:

Admin@UGOS> show traffic

Параметр	Описание
flows	Отображает информацию о входящем (IP и MAC-адреса источника и назначения, порты источника и назначения, протокол, тег VLAN, время жизни сессии, состояние сессии) и исходящем (IP-адреса источника и назначения, тег VLAN) потоках. Доступна фильтрация по: • **source-ip** — IP-адрес источника. • **source-port** — порт источника. • **source-mac** — MAC-адрес источника • **dest-ip** — IP-адрес назначения. • **dest-port** — порт назначения. • **dest-mac** — MAC-адрес назначения. • **vlan-tag** — тег VLAN.

Параметр	Описание
connections	Представлена информация о соединениях (протокол и его номер; время жизни записи; IP-адреса источника и назначения, порты источника и назначения; IP-адреса источника и назначения, порты источника и назначения, которые ожидаются в ответе; статус сессии (UNREPLIED или ASSURED); количество переданных и принятых пакетов и байтов; зона источника; является ли эта сессия, сессией известного NGFW пользователя и т.п.). Фильтрация доступна по: • **protocol** — протокол. • **source-ip** — IP-адрес источника. • **dest-ip** — IP-адрес назначения. • **expect** — отображение неустановленных соединений: ◦ **on**. ◦ **off**.

LLDP

Использованием следующей команды доступен просмотре информации LLDP:

Admin@UGOS> show lldp

Для просмотра доступны:

Параметр	Описание
neighbors	Список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP. • **Chassis ID** — идентификатор шасси. • **SysName** — имя системы. • **SysDescr** — описание системы, содержит информацию об оборудовании и операционной системе устройства. • **Management** — адрес соседнего устройства (содержит адреса IPv4 и IPv6, номер интерфейса указанного адреса управления). • **Capability** — функции устройства (например, маршрутизатор, коммутатор и т.п.). • **Port ID** — идентификатор порта с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit). • **PortDescr** — описание порта. • **TTL** — время жизни передаваемых пакетов LLDP.
statistics	Статистика интерфейсов, в настройках которых был указан профиль LLDP: • **Interface** — название интерфейса. • **Transmitted** — общее количество кадров LLDP, переданных через интерфейсе. • **Received** — общее количество кадров LLDP, полученных на интерфейсе. • **Discarded** — число полученных на этом интерфейсе кадров LLDP, которые были отброшены. • **Unrecognized** — количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе. • **Ageout** — в каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется. • **Inserted** — количество добавлений записей с информацией о соседях LLDP. • **Deleted** — количество удалений записей о соседях LLDP.

Маршруты

Данный раздел необходим для проведения диагностики и мониторинга маршрутной информации на NGFW.

Для просмотра всех маршрутов, содержащихся в маршрутизаторе по умолчанию, используется команда:

Admin@UGOS> show network route

Параметр	Описание
ip	IP-адрес, маршрут до которого необходимо отобразить.
connected	Маршруты к сетям, которые подключены непосредственно к интерфейсам NGFW. Данные маршруты помечены символом **C** в списке маршрутов.
kernel	Отображение маршрутов, добавленных администратором; маршруты помечены символом **K** в списке маршрутов.
summary	Количество активных подключений и записей FIB (Forwarding Information Base).
ospf	Отображение маршрутов, полученных- с помощью протокола динамической маршрутизации OSPF. Данные маршруты помечены символом **O** в списке маршрутов.
bgp	Отображение маршрутов, полученных с помощью протокола динамической маршрутизации BGP; маршруты помечены символом **B** в списке маршрутов.
rip	Отображение маршрутов, полученных- с помощью протокола динамической маршрутизации RIP; маршруты помечены символом **R** в списке маршрутов.
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> | **all**).

Мониторинг OSPF

Диагностика и мониторинг OSPF производится с использованием команд, представленных ниже. Отображение информации OSPF:

Admin@UGOS> show network ospf

Параметр	Описание
virtual-router	Виртуальный маршрутизатор, для которого необходимо отобразить общую информацию об OSPF: (<vrf-name> | **all**).
route	Отображение маршрутов, полученных по протоколу динамической маршрутизации OSPF.
database	Отображена информация: • **Router Link States**: пакеты LSA (Link State Advertisement) Type 1 (Router LSA) передаются маршрутизаторами в пределах одной зоны; используются для передачи информации соседним маршрутизаторам, находящихся в той же зоне, о собственных интерфейсах и своих соседях. • **Network Link States**: пакеты LSA Type 2 (Network LSA) генерируются выделенным маршрутизатором (Designated Router, DR) для описания всех маршрутизаторов, подключённых к его сегменту напрямую. • **Summary Link States**: пакеты LSA Type 3 (Summary LSA) формируются с помощью пограничных маршрутизаторов (Area Border Routers, ABR). Пакеты содержат суммарное сообщение о непосредственно подключенной к ним зоне, сообщают информацию в другие зоны, к которым подключен ABR и передаются в несколько зон по всей сети. • **ASBR-Summary Link States**: пакеты LSA Type 4 (ASBR Summary LSA) сообщают о присутствии автономного пограничного маршрутизатора (Autonomous System Border Router, ASBR) в других областях.
neighbor	Отображение информации о соседях: • Идентификатор соседа (идентификатор маршрутизатора). • Приоритет. Маршрутизатор с наивысшим приоритет становится выделенным маршрутизатором — Designated Router, DR. Если приоритеты маршрутизаторов равны, то будет выбран маршрутизатор с наибольшим идентификатором. • Состояние, например, Full/DR, Full/BDR, Full/Drother. • Интервал простоя — время, через которое соединение с OSPF-соседом будет разорвано, если не будет получен пакет Hello. • IP-адрес интерфейса, к которому подключен сосед. • Интерфейс, на котором сформировано соседство маршрутизаторов. Доступно указание дополнительных параметров: • **interface-name** — будут отображены соседи, с которыми установлена смежность на указанном интерфейсе. • **all** — отображение таблицы со всеми соседях. • **detail** — отображение подробной информации о соседях.
interface	Отображение информации об интерфейсах OSPF. Дополнительно: • **interface-name** — отображение информации об указанном интерфейсе. • **traffic** — статистика переданных и принятых пакетов OSPF (Hello, Database Description, Link State Request, Link State Update, Link State Acknowledgment).
border-routers	Отображение информации о пограничных маршрутизаторах.

Команда для перезапуска процесса OSPF:

Admin@UGOS> clear network ospf

Параметр	Описание
virtual-router	Виртуальный маршрутизатор, на котором необходимо перезапустить OSPF (<vrf-name> | **all**).
interface	Интерфейс, на котором необходимо перезапустить процесс OSPF.

Мониторинг BGP

В данном разделе представлены команды диагностики и мониторинга BGP.

Для отображения таблицы BGP маршрутизатора по умолчанию:

Admin@UGOS> show network bgp

Параметр	Описание
virtual-router	Виртуальный маршрутизатор, маршруты которого необходимо отобразить (<vrf-name> | **all**).
ip	IP-адрес, маршрут до которого необходимо отобразить.
statistics	Отображение статистики BGP.
neighbors	Отображение информации о BGP-соседях (доступно отображение информации об определённом соседе; необходимо указание IP-адреса соседа). Дополнительные параметры, доступные при указании соседа: • **received-routes** — принятые маршруты до применения к ним входящей политики (Routemap и фильтры). • **advertised-routes** — маршруты, которые анонсируются указанному соседу.
summary	Просмотр краткой информации о соседях.

Для выполнения повторного запроса информации у BGP-соседей (обрыв TCP-сессии):

Admin@UGOS> clear network bgp

Далее доступно указание параметров:

Параметр	Описание

Параметр	Описание
ip	IP-адрес соседа, с которым произойдет обрыв соединения для обновления информации.
virtual-router	Название виртуального маршрутизатора, которому принадлежит BGP-сосед.

В случае, если на соседних устройствах поддерживается метод Route Refresh, то можно избежать полной реинициализации сессии с соседом, отправив специальное сообщение типа ROUTE REFRESH. Отправка данного сообщения позволяет обновить информацию без прерывания в маршрутизации.

Для обновления информации без обрыва сессии с соседом используется команда:

Admin@UGOS> clear network bgp ip <neighbor-ip> soft in | out
Admin@UGOS> clear network bgp virtual-router <vrf-name> ip <neighbor-ip> soft in | out

Мониторинг RIP

В данном разделе представлены команды диагностики и мониторинга RIP.

Для отображения информации RIP из таблицы маршрутизатора по умолчанию (адрес сети, полученный по RIP; адрес Next Hop; метрика маршрута; тэг маршрута, предназначенный для разделения внутренних и внешних маршрутов; интервал времени, по истечении которого маршрут будет признан недействительным, если информация о нём не была получена):

Admin@UGOS> show network rip

Далее доступно использование следующих параметров:

Параметр	Описание
status	Текущий статус RIP: версия, таймеры, фильтры, распространяемые маршруты и т.п.
virtual-router	Виртуальный маршрутизатор, информацию о маршрутах RIP которого необходимо отобразить: <vrf-name> | **all**.

Мониторинг мультикаст

Для просмотра таблицы маршрутизации мультикаст-трафика на маршрутизаторе по умолчанию:

Admin@UGOS> show network mroute

Далее доступно использование следующих параметров:

Параметр	Описание
count	Отображение статистики о группе и источнике.
virtual-router	Выбор виртуального маршрутизатора: <vrf-name> | **all**.
summary	Суммарная информация о каждой записи в таблице мультикаст-маршрутизации.
fill	Таблица маршрутизации мультикаст-трафика. Доступно указание параметра: • **ip** — отображение записи для определённого IP-адреса; далее необходимо указать IP-адрес.
ip	Отображение записи для определённого IP-адреса; необходимо указать IP-адрес.

Мониторинг IGMP

Мониторинг работы протокола IGMP (Internet Group Management Protocol) доступен с использованием следующей команды (указание параметров является обязательным). Для отображения информации для маршрутизатора по умолчанию:

Admin@UGOS> show network igmp

Если необходимо отобразить информацию для определённого виртуального маршрутизатора или всех:

Admin@UGOS> show network igmp virtual-router <vrf-name> | all

Далее необходимо указать один из параметров:

Параметр	Описание
statistics	Статистика по сообщениям: • IGMP Membership Query — сообщение сервера клиенту, в котором сервер просит обновить подписку на получаемые клиентом группы иначе, сервер перестанет вещать группу/группы в данный сегмент сети. • IGMP Leave — сообщение клиента серверу; клиент сообщает, что желает убрать мультикаст-группу из списка получаемых. • IGMP Membership Report — сообщение клиента серверу; клиент желает получать трафик этой группы.
join	Отображение информации о группах IGMP.
sources	Отображение информации об источниках мультикаст-трафика.
groups	Отображение мультикаст-групп, полученных по протоколу IGMP. Отображается следующая информация: • Общее количество групп. • Интерфейс, через который группа доступна. • Адрес группы. • Режим INCLUDE или EXCLUDE. • Таймер, определяющий время, через которое маршрутизатор перестанет пересылать трафик на интерфейс, если не будет получен ответный IGMP Membership Report. • Время, в течение которого группа известна.

Параметр	Описание
interface	Отображение информации об интерфейсе, связанной с мультикаст-маршрутизацией: • Название интерфейса, его статус и адрес. • Версия IGMP. • Опрашиватель и его адрес (Querier). • Таймер, который обнуляется каждый раз, как приходит сообщение Query с меньшим IP-адресом. Доступно указание: • **interface-name** — название интерфейса. • **detail** — подробная информация об интерфейсе.

Мониторинг PIM

Мониторинг работы протокола PIM (Protocol-Independent Multicast) доступен с использованием следующей команды (указание параметров является обязательным). Для отображения информации для маршрутизатора по умолчанию:

Admin@UGOS> show network pim

Если необходимо отобразить информацию для определённого виртуального маршрутизатора или всех:

Admin@UGOS> show network pim virtual-router <vrf-name> | all

Далее необходимо указать один из параметров:

Параметр	Описание
vxlan-groups	Информация о группах VXLAN, использующихся в мультивещании.
statistics	Статистика протокола.
join	Отображение информации о группах PIM протокола.
neighbor	Информация о соседях: • Интерфейс, через который была получена информация о соседе. • Адрес соседа. • Время, с последнего начала работы PIM. • Время, в течении которого сосед доступен. • Приоритет DR.
next-hop	Записи о адресах next-hop.
state	Информация об известных S, G маршрутах, IIF (Incoming Interface), OIL (Outgoing Interface List).
rp-info	Отображение информации о Rendezvous Point (RP): адрес, разрешённые ASM группы с данного RP.
interface	Информация об интерфейсах, настроенных для работы PIM: название и адрес интерфейса, адрес DR и т.п. Также доступно указание параметров: • **interface-name** — название интерфейса. • **traffic** — статистика отправленных/полученных сообщений. • **detail** — подробная информация об интерфейсе.
group-type	Список разрешённых групповых адресов для SSM (Source Specific Multicast).
secondary	Отображение информации об интерфейсе с указанием дополнительного IP-адреса.

Режим конфигурации

Режим конфигурации (описание)

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Для перехода в режим конфигурации используется команда:

Admin@UGOS> configure

После перехода в режим конфигурации командная строка будет следующей:

Admin@UGOS#

Наименование	Описание
<action>	В режиме конфигурации доступны следующие действия: • **execute** — выполнение команд, которые не относятся к конфигурации NGFW (ping, date, traceroute и т.п.) Команда доступна независимо от уровня конфигурации (<level>). • **set** — редактирование всех объектов, а также включение различных параметров, например, radmin. • **end** — переход на один уровень выше. • **show** — отображение текущих значений. Можно использовать на любом уровне конфигурации — будет отображено всё, что находится глубже текущего уровня. • **edit** — переход на какой-либо уровень конфигурации. Уровень конфигурации будет отображён над командной строкой. • **top** — возврат на самый верхний уровень конфигурации. • **exit** — выход из режима конфигурации. • **export** — экспорт конфигурации. • **import** — импорт конфигурации. • **create** — создание новых объектов. • **delete** — удаление объекта или параметра из списка параметров. Например, для просмотра информации о всех интерфейсах необходимо выполнить команду: Admin@UGOS# show network interface С использованием следующей команды производится переход на уровень **network interface**: Admin@UGOS# edit network interface Текущий уровень будет отображён над командной строкой: [network interface] Admin@UGOS# После перехода на уровень **network interface** для отображения всех интерфейсов используется команда show без указания уровня: [network interface] Admin@UGOS# show
<level>	Уровни в командной строке повторяют веб-интерфейс NGFW • **security-policy** — соответствует разделу веб-интерфейса **Политики безопасности**. • **network** — соответствует разделу веб-интерфейса **Сеть**. • **settings** — соответствует разделу веб-интерфейса **NGFW**. • **global-portal** — соответствует разделу веб-интерфейса **Глобальный портал**. • **network-policy** — соответствует разделу веб-интерфейса **Политики сети**. • **vpn** — соответствует разделу веб-интерфейса **VPN**. • **users** — соответствует разделу веб-интерфейса **Пользователи и устройства**.
<filter>	Идентификатор объекта, к которому происходит обращение. Идентификация происходит по имени объекта. Если имеются объекты с одинаковыми именами или удобнее идентифицировать объект по другому параметру, то используются круглые скобки, в которых необходимо указать <configuration_info> (рассмотрено далее в разделе). В результате будет найден объект, для которого совпали все поля, указанные в круглых скобках. Например, необходимо вывести информацию об интерфейсе port0 на другом узле кластера. Если использовать команду: Admin@UGOS# show network interface adapter port0 то будет отображена информация об интерфейсе port0 текущего узла NGFW. Чтобы отобразить информацию об интерфейсе port0 другого узла (например, с именем another_node), необходимо в скобках явно указать имя узла: Admin@UGOS# show network interface adapter (node-name another_nodename interface port0) **Важно!** Круглые скобки должны быть отделены пробелами с обеих сторон.
<configuration_info>	Набор пар: параметр-аргумент. Параметр — имя поля, для которого нужно установить аргумент. Аргумент может быть одиночным или множественным. **Одиночный аргумент** — значение, соответствующее параметру. Если строка содержит пробелы, то необходимо использовать кавычки. Например, необходимо создать группу с именем VPN users: Admin@UGOS# create users group "VPN users" **Множественные аргументы** используются для установки множества значений какого-либо параметра; записываются в квадратных скобках и разделяются пробелами. Например, необходимо в группу VPN users добавить пользователей user1 и user2. Параметру **users** необходимо задать аргумент [user1 user2]: Admin@UGOS# set users group "VPN users" users [user1 user2] **Важно!** Квадратные скобки должны быть отделены пробелами с обеих сторон.

Команды execute

Команды имеет следующую структуру:

Admin@UGOS# execute <command-name>

Доступны следующие команды:

Параметр	Описание
update	Обновление: • **software-updates** — обновление программного обеспечения. • **libraries-updates** — обновление библиотек. Доступно обновление сразу всех библиотек или отдельных библиотек.
traceroute	Трассировка соединения до определённого хоста. Доступны параметры: • **interface <iface-name>** — интерфейс, с которого будут отправляться пакеты. • **not-map-ip** — не искать hostname для IP-адреса при отображении. • **use-icmp-echo** — использовать ICMP echo.
license	Команда регистрации продукта имеет следующую структуру: Admin@UGOS# execute license activate online <pin-code> Укажите код активации продукта вместо <pin-code>.
terminate	Закрытие сессий администраторов. Подробнее читайте в разделе Настройка сессий администраторов.
cache	Очистка кэша LDAP-записей: • **ldap-clear**.
ping	Выполнение ping определенного хоста. Можно задать следующие параметры: • **count** — количество отправляемых echo-запросов. Если параметр не задан, то отправка пакетов будет происходить, пока соединение не будет прервано пользователем (чтобы прервать отправку: Ctrl+C). • **numeric** — не резолвить имена. • **timestamp** — отображение временных меток. • **interval** — интервал времени, через который будет производиться отправка пакетов; указывается в секундах. • **ttl** — время жизни пакета. • **interface** — адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping.
reboot	Перезагрузка NGFW.
date	Просмотр текущих даты и времени на сервере.
shutdown	Выключение NGFW.
netcheck	Проверка доступности стороннего HTTP/HTTPS-сервера. Могут быть использованы следующие параметры: • **type** — проверка доступности по: ◦ **http**. ◦ **tcp** (если порт не указан, то используется порт 80). • **data** — запрос содержимого сайта. По умолчанию запрашиваются только заголовки. • **timeout** — максимальный таймаут ожидания ответа от веб-сервера.
dig	Проверка записи DNS домена. • **reverse-lookup** — получение хоста по IP-адресу. • **dns** — указание IP-адреса DNS-сервера. • **tcp** — использование протокола TCP вместо UDP.
configuration-cluster	Генерирование секретного кода, необходимого для добавления нового узла в кластер конфигурации: Admin@UGOS# execute configuration-cluster generate-secret-key **Важно!** Для использования данной команды необходимо наличие лицензии на модуль **Cluster**, иначе будет отображена ошибка.

Часть представленных выше команд, кроме команд обновления, регистрации продукта, управления сессиями администраторов и очистки кэша, также доступны в режиме диагностики и мониторинга. Для их выполнения используется команда:

Admin@UGOS> <command-name>

Команды import

Импорт доступен в разделах **Настройки**, **Пользователи**, **Сеть**, **Политики сети**, **Политики безопасности**, **Глобальный портал**, **VPN**.

В разделе настроек NGFW доступен импорт сертификатов. Подробнее читайте в разделе Настройка сертификатов.

В разделах **Пользователи**, **Сеть**, **Политики сети**, **Политики безопасности**, **Глобальный портал**, **VPN** доступен импорт правил, написанных на UPL. При использовании импорта, все существующие правила будут заменены на указанные; можно указать сразу несколько правил.

В разделе **Пользователи** доступен импорт правил Captive-портала. Подробнее о добавлении правил читайте в соответствующем разделе Настройка Captive-портала.

В разделе **Сеть** доступен импорт правил DNS. Подробнее читайте в разделе Настройка правил DNS.

В разделе **Политики сети** доступен импорт правил межсетевого экрана, NAT и маршрутизации, пропускной способности. Подробнее читайте в соответствующих разделах Настройка правил межсетевого экрана, Настройка правил NAT и маршрутизации, Настройка правил пропускной способности.

В разделе **Политики безопасности** доступен импорт правил контентной фильтрации, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, СОВ, защиты почтового трафика, ICAP-правил и правил защиты DoS. О добавлении правил читайте в соответствующих разделах Настройка фильтрации контента, Настройка веб-безопасности, Настройка правил инспектирования туннелей, Настройка инспектирования SSL, Настройка инспектирования SSH, Настройка СОВ, Настройка правил ICAP, Настройка правил защиты DoS.

В разделе **Глобальный портал** доступен импорт правил веб-портала и reverse-прокси. Подробнее о создании правил читайте в разделах Настройка веб-портала и Настройка правил reverse-прокси.

В разделе VPN доступен импорт серверных и клиентских правил, о добавлении которых написано в разделах Настройка серверных правил и Настройка клиентских правил.

Команды export

Доступен экспорт сертификатов и элементов библиотек.

Подробнее об экспорте сертификатов смотрите в разделе Настройка сертификатов.

Для экспорта доступны следующие элементы библиотек: IP-адреса, Useragent браузеров, списки URL, категории URL, изменённые категории URL, типы контента, морфология, почтовые адреса и номера телефонов. Для экспорта элемента библиотеки используется команда:

Admin@UGOS# export libraries <library-name> <list-name>

где <library-name> — название библиотеки элементов (IP-адреса, Списки URL и т.д.).

<list-name> — название элемента библиотеки.

Настройка устройства

Documentation: ☑
Version: 7.0.1
Product: UserGate NGFW

Настройка CLI

Настройка интерфейса командной строки производится на уровне **settings cli**. Чтобы задать уровень детализации диагностики используется следующая команда:

Admin@UGOS# set settings cli log-level <off | error | debug | warning | info>

Уровни детализации:

- **off** — отключить журналирование.
- **error** — только ошибки.
- **debug** — максимальная детализация.
- **warning** — ошибки и предупреждения.
- **info** — ошибки, предупреждения и дополнительная информация.

Для отображения настроек CLI:

Admin@UGOS# show settings cli

Общие настройки NGFW

Общие настройки NGFW задаются на уровне **settings general**. Структура команды для настройки одного из разделов (<settings-module>):

Admin@UGOS# set settings general <settings-module>

Доступна настройка следующих разделов:

Параметр	Описание
admin-console	Настройки интерфейса (уровень **settings general admin-console**): • **timezone**: часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. • **language**: язык интерфейса: ◦ **ru** — русский. ◦ **en** — английский. • **webaccess**: режим авторизации веб-консоли: ◦ **password**: авторизацию по имени и паролю. ◦ **cert**: авторизация по X.509-сертификату. • **web-ssl-profile**: выбор профиля SSL для построения защищенного канала доступа к веб-консоли. Подробнее о профилях SSL смотрите в разделе Настройка профилей SSL. • **response-page-ssl-profile**: выбор профиля SSL для построения защищенного канала для отображения страниц блокировки доступа к веб-ресурсам и страницы авторизации Captive-портала. Подробнее о профилях SSL смотрите в разделе Настройка профилей SSL.
server-time	Настройка параметров установки точного времени (уровень **settings general server-time**): • **ntp-enabled**: включение/отключение использования NTP-серверов: ◦ **on**. ◦ **off**. • **ntp-servers**: указание серверов NTP (основного и запасного): Admin@UGOS# set settings general server-time ntp-servers [server1] Admin@UGOS# set settings general server-time ntp-servers [server1 server2] • **time**: установка времени на сервере; время указывается в часовом поясе UTC в формате yyyy-mm-ddThh:mm:ss (например, 2022-02-15T12:00:00)

Параметр	Описание
modules	Настройка модулей NGFW (уровень **settings general modules**): • **proxy-port**: указать нестандартный номер порта, который будет использоваться для подключения к встроенному прокси-серверу. • **auth-captive**: указать служебный домен, который используется NGFW при авторизации пользователей через Captive-портал. • **logout-captive**: указать служебный домен, который используется пользователями NGFW для окончания сессии (logout). • **block-page-domain**: указать служебный домен, который используется для отображения страницы блокировки пользователям. • **ftp-enabled**: включить/отключить модуль, позволяющий получать доступ к содержимому FTP-серверов из пользовательского браузера. • **ftp-domain**: указать служебный домен, который используется для предоставления пользователям сервиса FTP поверх HTTP. • **zone-enabled**: включить/отключить зону для инспектируемых туннелей: ◦ **on**. ◦ **off**. • **tunnel-inspection-zone**: выбрать зону для инспектируемых туннелей. • **snmp-engine-id**: настроить SNMP Engine ID: ◦ **length** <**fixed** | **dynamic**> — длина идентификатора: фиксированная (не более 8 байт; только для типа text) или динамическая (не более 27 байт). ◦ **type** <**ip4** | **ip6** | **mac** | **text** | **octets**> — формат SNMP Engine ID (IPv4, IPv6, MAC-адрес, текст, октеты). ◦ **value** — значение идентификатора. • **terminal-sever-agent password**: настроить пароль агентов терминального сервиса. • **lldp**: настроить использование протокола канального уровня Link Layer Discovery Protocol (LLDP), который позволяет сетевому оборудованию, работающему в локальной сети, оповещать устройства о своём существовании, передавать им свои характеристики, а также получать от них аналогичную информацию. При настройке необходимо задать значения: ◦ **transmit-delay** — задержка передачи, указывается время ожидания устройства перед отправкой объявлений соседям после изменения TLV в протоколе LLDP или состояния локальной системы, например, изменение имени хоста или адреса управления. Может принимать значения от 1 до 3600; задаётся в секундах. ◦ **transmit-hold** — значение мультипликатора удержания; произведение значений transmit delay и transmit hold определяет время жизни (TTL) пакетов LLDP. Может принимать значения от 1 до 100.
cache	Настройка кэша прокси-сервера (уровень **settings general cache**): • **caching-mode**: включение или отключение кэширования. ◦ **on**. ◦ **off**. • **exclusions**: список URL, которые не будут кэшироваться. Для удаления исключений: Admin@UGOS# delete settings general cache exclusions [<URL>] • **max-cacheable-size**: максимальный размер объектов, которые будут кэшироваться (указывается в Мбайт). • **ram-size**: размер оперативной памяти, отведенный под кэширование (указывается в Мбайт).
log-analyzer	Настройки модуля Log Analyzer (уровень **settings general log-analyzer**): • **use-local-stat-server** — использование локального Log Analyzer: ◦ **on**. ◦ **off**.
proxy-portal	Настройки для предоставления доступа к внутренним ресурсам компании с помощью веб-портала (уровень **settings general proxy-portal**): • **enabled**: включение/отключение использования веб-портала: ◦ **on**. ◦ **off**. • **hostname**: имя хоста. • **port**: порт. • **auth-profile**: выбор профиля аутентификации. Подробнее о настройке профилей авторизации с использованием CLI читайте в разделе Настройка профилей аутентификации. • **auth-template**: выбор шаблона страницы авторизации. • **portal-template**: выбор шаблона портала. • **enable-ldap**: выбор домена AD/LDAP на странице авторизации: ◦ **on**. ◦ **off**. • **use-captcha**: показ CAPTCHA: ◦ **on**. ◦ **off**. • **ssl-profile**: выбор профиля SSL. Подробнее о настройке профилей аутентификации с использованием CLI читайте в разделе Настройка профилей SSL. • **certificate**: выбор сертификата. • **auth-by-cert**: включение/отключение авторизации пользователя по сертификату: ◦ **on**. ◦ **off**.

Параметр	Описание
pcap	Настройка захвата пакетов (уровень **settings general pcap**): • **type**: тип захвата: ◦ **no-capture**: без захвата. ◦ **one-packet**: один пакет. ◦ **previous**: предшествующие пакеты. ◦ **previous-and-following**: предшествующие и последующие пакеты. • **previous-packets**: количество предшествующих пакетов (от 4 до 30 пакетов). • **following-packets**: количество последующих пакетов (от 2 до 15 пакетов).
change-tracker	Настройка учёта изменений (уровень **settings general change-tracker**): • **enabled**: включение/отключение учёта изменений. ◦ **on**. ◦ **off**. • **event-tracker-types**: типы изменений задаются администратором. Для удаления типа изменения используется команда: Admin@UGOS# delete settings general change-tracker event-tracker-types [type1 ...]
management-center	Настройка агента UGMC (уровень **settings general management-center**): • **enabled**: включение/отключение агента UGMC. ◦ **on**. ◦ **off**. • **mc-address**: адрес сервера UGMC. • **device-code**: уникальный код устройства для подключения устройства к UGMC.
updates-schedule	Настройка расписания скачивания обновлений программного обеспечения и библиотек (уровень **settings general updates-schedule**). Для расписания обновления программного обеспечения NGFW: Admin@UGOS# set settings general updates-schedule software-updates schedule advanced Расписание скачивания обновлений библиотек может быть единым: Admin@UGOS# set settings general updates-schedule libraries-updates all schedule advanced или может быть настроено отдельно для каждого элемента: Admin@UGOS# set settings general updates-schedule libraries-updates [lib-module ...] schedule advanced Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа". Команда для просмотра расписания обновлений: Admin@UGOS# show settings general updates-schedule

Настройка управления устройством

Настройка Radmin-emergency

Команда включения/отключения удалённого доступа к серверу для технической поддержки в случаях, когда NGFW не отвечает:

Admin@UGOS# set settings device-mgmt diagnostic radmin-emergency <on | off>

Далее необходимо указать параметры:

Параметр	Описание
interface	Название интерфейса.
ip-addr	IP-адрес и маска интерфейса.
gateway-address	IP-адрес шлюза.

В случаях, когда произошла проблема с ядром NGFW, может пропасть возможность авторизации в CLI. Для активации удаленного помощника в таких случаях администратор может зайти в CLI под учетной записью корневого администратора, которая была создана при инициализации NGFW. Обычно это учетная запись Admin, хотя может быть и другой. Для входа необходимо указать имя в виде Admin@emergency, в качестве пароля — пароль корневого администратора.

Настройка диагностики

Параметры диагностики сервера, необходимые службе технической поддержки при решении проблем, задаются на уровне **device-mgmt diagnostic**. Текущие настройки можно просмотреть с использованием команды:

Admin@UGOS# show settings device-mgmt diagnostic

На уровне **settings device-mgmt diagnostic radmin** можно включить или отключить удалённый доступ к серверу для технической поддержки UserGate (**Radmin**). Команда включения/отключения Radmin:

Admin@UGOS# set settings device-mgmt diagnostic radmin <on | off>

Для просмотра состояния Radmin:

Admin@UGOS# show settings device-mgmt diagnostic radmin

На уровне **settings device-mgmt diagnostic details** с помощью следующей команды можно установить необходимы уровень детализации диагностики (отключено; только ошибки; ошибки и предупреждения; ошибки, предупреждения и дополнительная информация; максимум детализации):

Admin@UGOS# set settings device-mgmt diagnostic details <off | error | warning | info | debug>

Для просмотра состояния уровня детализации диагностики:

Admin@UGOS# show settings device-mgmt diagnostic details

Настройка операций с сервером

Следующая команда позволяет определить канал обновлений:

Admin@UGOS# set settings device-mgmt updates-channel <stable | beta>

Для просмотра наличия обновлений и выбранного канал обновления используется команда:

Admin@UGOS# show settings device-mgmt updates-channel

Экспорт настроек

Создание и настройка правил экспорта настроек происходит на уровне **settings device-mgmt settings-export**.

Для создания правила экспорта настроек:

Admin@UGOS# create settings device-mgmt settings-export

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение правила экспорта настроек NGFW.
name	Название правила экспорта.
description	Описание правила экспорта.
type	Выбор удалённого сервера для экспорта настроек: • **ssh**. • **ftp**.
address	IP-адрес удалённого сервера.
port	Порт сервера.
login	Учётная запись на удалённом сервере.
password	Пароль учётной записи.
path	Путь на сервере, куда будут выгружены настройки.
schedule	Расписание экспорта настроек. Время задаётся в Crontab-формате: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6; 0 — вс). Каждое из поле может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Обновление существующего правила экспорта настроек NGFW производится с использованием следующей команды:

Admin@UGOS# set settings device-mgmt settings-export <rule-name>

Список параметров, доступных для изменения аналогичен списку параметров, доступных при создании правила.

Команда для удаления правила экспорта настроек:

Admin@UGOS# delete settings device-mgmt settings-export <rule-name>

Команда для отображения правила экспорта настроек:

Admin@UGOS# show settings device-mgmt settings-export <rule-name>

Также, для команд обновления, удаления или отображения правил в качестве <filter> возможно использование не только названия правила, но и заданные в существующем правиле параметры (удобно, например, при наличии нескольких правил с одинаковым названием). Параметры, с использованием которых можно произвести идентификацию правила экспорта, аналогичны параметрам команды **set**.

Настройка защиты конфигурации от изменений

Для настройки параметров защиты конфигурации (настроек) продукта от изменения используйте следующую команду:

Admin@UGOS# set settings change-control config <off | log | block>

Проверка целостности конфигурации происходит каждые несколько минут после загрузки NGFW.

- **log** — активирует режим отслеживания изменений конфигурации. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания изменений конфигурации. Требует указания пароля, который был задан при активации режима отслеживания конфигурации.
- **block** — активирует режим отслеживания изменений конфигурации. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через NGFW.

Перед активацией защиты конфигурации администратор производит настройку продукта в соответствии с требованиями организации, после чего "замораживает" настройки (режим **log** или **block**). Любое изменение настроек через веб-интерфейс, CLI или другими способами будет приводить к журналированию и/или блокировке транзитного трафика, в зависимости от выбранного режима.

Для просмотра текущего режима защиты конфигурации от изменений:

Admin@UGOS# show settings change-control config

Настройка защиты исполняемых файлов от изменения

Чтобы настроить защиту параметры защиты исполняемого кода продукта от потенциального несанкционированного изменения:

Admin@UGOS# set settings change-control code <off | log | block>

Проверка целостности исполняемого кода происходит каждый раз после загрузки NGFW

- **log** — активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания.
- **off** — отключает режим отслеживания несанкционированных изменений исполняемого кода. Требует указания пароля, который был задан при активации режима отслеживания исполняемого кода.
- **block** — активирует режим отслеживания несанкционированных изменений исполняемого кода. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений NGFW записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через NGFW. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Для просмотра текущего режима защиты исполняемых файлов:

Admin@UGOS# show settings change-control code

Version: 7.0.1
Documentation:

Настройка кластера конфигурации

Данный раздел находится на уровне **settings device-mgmt configuration-cluster**.

Команда обновления существующего узла кластера:

Admin@UGOS# set settings device-mgmt configuration-cluster <node-name>

Доступно изменение следующих параметров:

Параметр	Описание
name	Изменить имя узла кластера.
description	Обновить описание узла кластера.
ip	Задать IP-адрес интерфейса, входящего в зону, выделенную для кластера.

Команды для удаления и отображения настроек узла кластера:

Admin@UGOS# delete settings device-mgmt configuration-cluster <node-name>
Admin@UGOS# show settings device-mgmt configuration-cluster <node-name>

Настройка кластера отказоустойчивости

Настройка кластеров отказоустойчивости производится на уровне **settings device-mgmt ha-cluster**.

Для создания кластера отказоустойчивости:

Admin@UGOS# create settings device-mgmt ha-cluster

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение кластера отказоустойчивости: • **on**. • **off**.
name	Название кластера отказоустойчивости.
description	Описание кластера отказоустойчивости.
mode	Выбор режима работы кластера: • **active-passive**: режим работы Актив-Пассив (один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные — в качестве резервных). • **active-active**: режим работы Актив-Актив (один из серверов выступает в роли Мастер-узла, распределяющего трафик на все остальные узлы кластера).
master-node	Выбор Мастер-узла (будет отображён список узлов кластера, активных в данный момент).
ha-cluster-id	Настройка синхронизации сессий в кластере: • <num> — мультикаст идентификатор кластера (может принимать значения от 0 до 8). Синхронизация пользовательских сессий (кроме сессий, использующих прокси сервер, например, трафик HTTP/S) включится автоматически. • **off** — отключение синхронизации пользовательских сессий.
virtual-router-id	Идентификатор виртуального маршрутизатора (VRID).
nodes	Выбор узлов кластера конфигурации для объединения их в кластер отказоустойчивости.
virtual-ips	Задание виртуального IP-адреса для кластера и выбор рабочего интерфейса для каждого узла (на зоне выбранного интерфейса должен быть разрешён сервис VRRP; подробнее о настройке зон через CLI читайте в разделе Зоны). Добавление виртуального IP-адреса в кластер: Admin@UGOS# create settings device-mgmt ha-cluster virtual-ips <virtual-ips-filter> <virtual-ip-info> Доступные параметры для <virtual-ips-filter>: • **new**: создать виртуальный IP-адрес для заданного кластера. • <ip>: изменить данные для выбранного виртуального адреса. Доступные параметры для <virtual-ip-info>: • **ip**: задать IP-адрес для кластера отказоустойчивости (указывается в формате IP/mask). • **ha-interfaces**: задать интерфейсы для узлов кластера (указываются в формате node-name/interface).

Для обновления настроек кластера:

Admin@UGOS# set settings device-mgmt ha-cluster <cluster-name>

Список параметров аналогичен списку параметров, доступных при создании кластера отказоустойчивости.

Для удаления кластера:

Admin@UGOS# delete settings device-mgmt ha-clusters <cluster-name>

Также доступно удаление отдельных параметров:

- **nodes**.
- **virtual-ips**.

Для отображения информации о всех кластерах отказоустойчивости:

Admin@UGOS# show settings device-mgmt ha-cluster

Для отображения информации об определённом кластере:

Admin@UGOS# show settings device-mgmt ha-cluster <cluster-name>

Настройка управления доступом к консоли NGFW

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Настройка данного раздела производится на уровне **settings administrators**. В данном разделе описаны настройка параметров защиты учётных записей, настройка администраторов и их профилей.

Общие настройки доступа

Данный раздел позволяет настроить дополнительные параметры защиты учётных записей администраторов. Настройка производится на уровне **settings administrators general**.

Для изменения параметров необходимо использовать следующую команду

Admin@UGOS# set settings administrators general

Далее необходимо указать параметры, которые необходимо изменить:

Параметр	Описание
password	Изменить пароля текущего администратора.
unblock	Разблокировать администратора.
strong-password	Использовать сложный пароль: • **on**. • **off**.
num-auth-attempts	Установить максимальное количество неверных попыток аутентификации.
block-time	Указать время блокировки учётной записи в случае достижения администратором максимального количества попыток аутентификации; указывается в секундах (максимальное значение: 3600 секунд).
min-length	Определить минимальную длину пароля (максимальное значение: 100 символов).
min-uppercase	Определить минимальное количество символов в верхнем регистре (максимальное значение: 100 символов).
min-lowercase	Определить минимальное количество символов в нижнем регистре (максимальное значение: 100 символов).
min-digits	Определить минимальное количество цифр (максимальное значение: 100 символов).
min-special-characters	Определить минимальное количество специальных символов (максимальное значение: 100 символов).
max-characters-repetition	Указать максимальную длину блока из одного и того же символа (максимальное значение: 100 символов).

Для просмотра текущих параметров защиты учётных записей администраторов используйте команду:

Admin@UGOS# show settings administrators general

Настройка учётных записей администраторов

Настройка учётных записей администраторов производится на уровне **settings administrators administrators**.

Для создания учётной записи администратора используется следующая команда:

Admin@UGOS# create settings administrators administrators

Далее необходимо указать тип учётной записи администратора (локальный, пользователь LDAP, группа LDAP, с профилем аутентификации) и указать соответствующие параметры:

Параметр	Описание
local	Добавить локального администратора: • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **password**: пароль администратора.
ldap-user	Добавить пользователя из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **ldap-login**: логин администратора. Структура команды при указании данного параметра: Admin@UGOS# create settings administrators administrators ldap-user ... ldap-login connector <ldap-connector-name> user <domain\user> ... • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.

Параметр	Описание
ldap-group	Добавить группу пользователей из существующего домена (необходим корректно настроенный LDAP-коннектор; подробнее читайте в разделе Настройка LDAP-коннектора): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **ldap-login**: логин администратора. Структура команды при указании данного параметра: Admin@UGOS# create settings administrators administrators ldap-group ... ldap-login connector <ldap-connector-name> group <domain\group> ... • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее.
admin-auth-profile	Добавить администратора с профилем аутентификации (необходимы корректно настроенные серверы аутентификации; подробнее читайте в разделе Настройка серверов аутентификации): • **enabled**: включение/отключение учётной записи администратора: ◦ **on**. ◦ **off**. • **login**: логин администратора. • **description**: описание учётной записи администратора. • **admin-profile**: профиль администратора. Создание профилей администраторов рассмотрено далее. • **auth-profile**: выбор профиля аутентификации из созданных ранее; подробнее о профилях аутентификации читайте в разделе Настройка профилей аутентификации.

Следующая команда используется для обновления профиля (параметры аналогичны параметрам создания профиля администратора):

Admin@UGOS# set settings administrators administrators <admin-type> <admin-login>

Для удаления учётной записи используется команда:

Admin@UGOS# delete settings administrators administrators <admin-type> <admin-login> Для отображения информации о всех учётных записях администраторов:

Admin@UGOS# show settings administrators administrators

Для отображения информации об определённой учётной записи администратора:

Admin@UGOS# show settings administrators administrators <admin-type> <admin-login>

Настройка прав доступа профилей администраторов

Настройка прав доступа профилей администраторов производится на уровне **settings administrators admin-profiles**.

Для создания профиля администратора предназначена следующая команда:

Admin@UGOS# create settings administrators admin-profiles

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля администратора.
description	Описание профиля администратора.
api-permissions	Права доступа к API: • **no-access**: нет доступа. • **read**: только чтение. • **readwrite**: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@UGOS# create settings administrators admin-profiles ... api-permissions <permission> all или Admin@UGOS# create settings administrators admin-profiles ... api-permissions <permission> [object ...]
webui-permissions	Права доступа к веб-интерфейсу UserGate: • **no-access**: нет доступа. • **read**: только чтение. • **readwrite**: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@UGOS# create settings administrators admin-profiles ... webui-permissions <permission> all или Admin@UGOS# create settings administrators admin-profiles ... webui-permissions <permission> [object ...]
cli-permissions	Права доступа к интерфейсу командной строки (CLI): • **no-access**: нет доступа. • **read**: только чтение. • **readwrite**: чтение и запись. Возможно назначение прав сразу на все или на отдельные объекты: Admin@UGOS# create settings administrators admin-profiles ... cli-permissions <permission> all или Admin@UGOS# create settings administrators admin-profiles ... cli-permissions <permission> [object ...]

Следующая команда используется для обновления профиля (параметры аналогичны параметрам создания профиля администратора):

Admin@UGOS# set settings administrators admin-profiles <profile-name>

Чтобы удалить профиль администратора:

Admin@UGOS# delete settings administrators admin-profiles <profile-name>

Для просмотра информации о всех профиля администраторов:

Admin@UGOS# show settings administrators admin-profiles

Для отображения информации об определённом профиле:

Admin@UGOS# show settings administrators admin-profiles <profile-name>

Настройка сессий администраторов

С использованием следующих команд возможен просмотр сессий администраторов, прошедших авторизацию в веб-консоли или CLI, и закрытие сессий (уровень: **settings administrators sessions**).

Просмотр сессий администраторов текущего узла UserGate (возможен просмотр сессии отдельного администратора: необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация):

Admin@UGOS# show settings administrators sessions

Для отображения сессий доступно использование фильтра:

- **ip**: IP-адрес, с которого авторизован администратор.
- **source**: где была произведена авторизация: CLI (**cli**), веб-консоль (**web**) или подключение по SSH (**ssh**).
- **admin-login**: имя администратора.
- **node**: узел кластера UserGate.

Admin@UGOS# show settings administrators sessions (node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login>)

Команда для закрытия сессии администратора; необходимо из предложенного списка выбрать IP-адрес, с которого была произведена авторизация:

Admin@UGOS# execute terminate settings administrators sessions

При закрытии сессии администраторов возможно использование фильтра (<filter>). Параметры фильтрации аналогичны параметрам команды **show**.

Admin@UGOS# execute terminate settings administrators sessions (node <node-name> ip <session-ip> source <cli | web | ssh> admin-login <administrator-login>)

Настройка сертификатов

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Раздел **Сертификаты** находится на уровне **settings certificates**.

Для импорта сертификатов предназначена команда:

Admin@UGOS# import settings certificates

Далее необходимо указать параметры:

Параметр	Описание
name	Название сертификата, которое будет отображено в списке.
description	Описание сертификата.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.
private-key	Приватный ключ в формате PEM.
passphrase	Пароль для приватного ключа или контейнера PKCS12 (необязательное значение).
user	Локальный пользователь, которому будет назначен пользовательский сертификат.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • **user**: имя пользователя в формате domain\user. • **connector**: выбор LDAP сервера.
role	Тип сертификата: • **web-console-cert-chain**: цепочка сертификатов веб-консоли. • **ssl-inspection-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **ssl-inspection-root**: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **user**: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • **ssl-inspection-cert**: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • **captive-portal**: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. • **web-console-ssl**: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW. • **saml**: сертификат, который будет использован в SAML-клиенте. • **none**.

Для экспорта доступны сертификаты, вся цепочка сертификатов и CSR:

Admin@UGOS# export settings certificates <certificate | certificate-and-chain | csr> <certificate-name>

С использованием командной строки возможно создание сертификата и CSR:

Admin@UGOS# create settings certificates <certificate | csr>

Далее необходимо указание следующих параметров:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
country	Страна, в которой выписывается сертификат.
state	Область/штат, в котором выписывается сертификат.
locality	Город, в котором выписывается сертификат.
organization	Название организации, для которой выписывается сертификат.
common-name	Имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.
email	Email компании.

Команда для управления сертификатом:

Admin@UGOS# set settings certificates <certificate-name>

Доступны параметры:

Параметр	Описание
name	Название сертификата.
description	Описание сертификата.
role	Тип сертификата: • **web-console-cert-chain**: цепочка сертификатов веб-консоли. • **ssl-inspection-intermediate**: промежуточный сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **ssl-inspection-root**: корневой сертификат в цепочке удостоверяющих центров, которая использовалась для выдачи сертификата для инспектирования SSL. • **user**: пользовательский сертификат, который может быть использован для авторизации пользователей при их доступе к опубликованным ресурсам с помощью правил reverse-прокси. • **ssl-inspection-cert**: сертификат SSL инспектирования класса удостоверяющего центра, использующийся для генерации SSL-сертификатов для интернет-хостов, для которых производится перехват HTTPS, SMTPS, POP3S трафика. • **captive-portal**: сертификат, использующийся для создания безопасного HTTPS-подключения пользователей к странице авторизации Captive-портала, для отображения страницы блокировки, для отображения страницы Logout Captive-портала и для работы ftp-прокси. • **web-console-ssl**: сертификат, использующийся для создания безопасного HTTPS-подключения администратора к веб-консоли NGFW. • **saml**: сертификат, который будет использован в SAML-клиенте. • **none**.
user	Локальный пользователь, которому будет назначен пользовательский сертификат.
ldap-user	Пользователь LDAP-коннектора, которому будет назначен пользовательский сертификат. • **user**: имя пользователя в формате domain\user. • **connector**: выбор LDAP сервера.
certificate-data	Сертификат в формате PEM.
certificate-chain	Цепочка сертификатов в формате PEM.

Для удаления сертификата:

Admin@UGOS# delete settings certificates <certificate-name>

Команды для просмотра информации об определённом сертификате или о всех сертификатах:

Admin@UGOS# show settings certificates
Admin@UGOS# show settings certificates <certificate-name>

Чтобы удалить сертификат из кэша используется команда:

Admin@UGOS# delete settings certificates-cache <common-name>

Настройка параметров устройства

Documentation:
Version: 7.0.1
Product: UserGate NGFW

Изменение параметров устройства производится на уровне **settings device**. Для изменения используется следующая команда (где <setting-name> — название параметра):

Admin@UGOS# set settings device <setting-name>

Доступно изменение следующих параметров:

Параметр	Описание
module_l7_enabled	Включение/отключение загрузки модуля L7: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка NGFW.
module_sip_enabled	Включение/отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен. **Важно!** После включения для корректной работы модуля необходимо перезагрузить таблицу правил межсетевого экрана (кнопка **Принудительно применить** в разделе **Политики сети → Межсетевой экран**).
module_h323_enabled	Включение/отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен.
module_idps_enabled	Включение/отключение загрузки модуля IDPS: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка NGFW.
module_sunrpc_enabled	Включение/отключение загрузки модуля SunRPC: • **on**. • **off** По умолчанию модуль выгружен.
module_ftp_alg_enabled	Включение/отключение загрузки модуля FTP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** **Важно!** Модуль нужно включать для пассивного режима работы FTP. По умолчанию модуль выгружен.
ha_auth_type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • **ah** — включение подписи. • **pass** — отключение проверки.
fw_drop_invalid	Включение/отключение блокировки пакетов с невалидным набором параметров в полях заголовка: • **on**. • **off** По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной.
fw_established	Включение/отключение создания одного общего правила межсетевого экрана для обратных пакетов: • **on**. • **off** По умолчанию настройка выключена.
decrypt_bypass_optimization	Включение/отключение оптимизации инспектирования SSL: • **on**. • **off** По умолчанию настройка выключена.

Для просмотра текущих настроек используйте команду:

Admin@UGOS# show settings device

или

Admin@UGOS# show settings device <setting-name>

Настройка телеметрии

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Набор команд для просмотра и настройки режима работы телеметрии доступны на уровне **settings telemetry**. Телеметрия позволяет отправлять разработчику анонимную статистику, такую как популярность веб-сайтов, веб-сайты с неизвестной категорией, вирусные атаки, события СОВ, активность малваре. Данные телеметрии имеют вид обезличенных данных и не содержат персональную информацию.

Для включения/отключения телеметрии используйте команду:

Admin@UGOS# set settings telemetry enabled <on | off>

По умолчанию отправка телеметрии включена.

Для просмотра текущего режима:

Admin@UGOS# show settings telemetry

Настройка прокси-сервера

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Набор команд для просмотра и настройки параметров прокси-сервера доступны на уровне **settings proxy**. Позволяет настроить такие параметры, как добавление заголовков HTTP — via и forwarded, а также настройки таймаутов на подключение к сайтам и на загрузку контента. Для изменения параметров прокси-сервера используется команда (где <setting-name> — название параметра):

Admin@UGOS# set settings proxy <setting-name>

Для изменения доступны следующие параметры:

Параметр	Описание
add_via_enabled	Добавление HTTP заголовков Via: • **on**. • **off**. По умолчанию отключено.
add_forwarded_enabled	Добавление HTTP заголовков Forwarded: • **on**. • **off**. По умолчанию отключено.
add_xforwarded_enabled	Добавление HTTP заголовков X-Forwarded-For: • **on**. • **off**. По умолчанию отключено.
http_connection_timeout	Время ожидания, выделяемое на подключение HTTP. По умолчанию — 20 секунд.
http_loading_timeout	Время ожидания, выделяемое на загрузку контента HTTP. По умолчанию — 60 секунд.
proxy_host_rfc	Доступно: • **relaxed** — использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. • **strict** — соблюдать RFC. Данный режим используется по умолчанию.
fmode_enabled	Режим ускорения загрузки контента: • **on**. • **off**. Режим может быть несовместим с работой некоторых сайтов; по умолчанию отключен.
smode_enabled	Режим SYN Proxy: • **on**. • **off**. По умолчанию режим включен.
icap_wait_timeout	Время, которое NGFW ждет ответа от ICAP-сервера; указывается в секундах. Если ответ сервера не был получен в заданный промежуток времени, то в случае, если действие правила **Переслать и игнорировать**, NGFW отправит данные пользователю без модификации, если же действие правила **Переслать**, NGFW не отдаст данные пользователю. Значение по умолчанию — 10 секунд.

Для просмотра текущих настроек используйте команду:

Admin@UGOS# show settings proxy

или

Admin@UGOS# show settings proxy <setting-name>

Настройка параметров устройства

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Изменение параметров устройства производится на уровне **settings device**. Для изменения используется следующая команда (где <setting-name> - название параметра):

Admin@UGOS# set settings device <setting-name>

Доступно изменение следующих параметров:

Параметр	Описание
module_l7_enabled	Включение/отключение загрузки модуля L7: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка NGFW.
module_sip_enabled	Включение/отключение загрузки модуля SIP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен.
module_h323_enabled	Включение/отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** По умолчанию модуль выгружен.
module_idps_enabled	Включение/отключение загрузки модуля IDPS: • **on**. • **off** По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка NGFW.
module_sunrpc_enabled	Включение/отключение загрузки модуля SunRPC: • **on**. • **off** По умолчанию модуль выгружен.
module_ftp_alg_enabled	Включение/отключение загрузки модуля FTP; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT: • **on**. • **off** **Важно!** Модуль нужно включать для пассивного режима работы FTP. По умолчанию модуль выгружен.
ha_auth_type	Использование подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости: • **ah** - включение подписи. • **pass** - отключение проверки.
fw_drop_invalid	Включение/отключение блокировки пакетов с невалидным набором параметров в полях заголовка: • **on**. • **off** По умолчанию настройка находится в выключенном состоянии. Включение данной опции существенно понижает производительность межсетевого экрана; рекомендуется оставить данную настройку выключенной.
fw_established	Включение/отключение создания одного общего правила межсетевого экрана для обратных пакетов: • **on**. • **off** По умолчанию настройка выключена.
decrypt_bypass_optimization	Включение/отключение оптимизации инспектирования SSL: • **on**. • **off** По умолчанию настройка выключена.

Для просмотра текущих настроек используйте команду:

Admin@UGOS# show settings device

или

Admin@UGOS# show settings device <setting-name>

Настройки сети

Зоны

Documentation:
Version: 7.0.1
Product: UserGate NGFW

Данный раздел находится на уровне **network zone**. Команда для создания новой зоны:

Admin@UGOS# create network zone

Далее необходимо указать параметры зоны:

Параметр	Описание
name	Название зоны.
description	Описание зоны.
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то NGFW отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то NGFW отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **enabled**: включение/отключение защиты. ◦ **on**. ◦ **off**. • **aggregate**: ◦ **on** — считаются все пакеты, входящие в интерфейсы данной зоны. ◦ **off** — пакеты считаются отдельно для каждого IP-адреса. • **alert-threshold**: порог уведомления; если количество запросов превышает данный порог, то происходит запись события в системный журнал. • **drop-threshold**: порог отбрасывания пакетов; если количество запросов превышает указанное значение, то NGFW отбрасывает пакеты и записывает данное событие в системный журнал. • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.

Параметр	Описание
enabled-services	Параметры контроля доступа зоны: • **"Any ICMP"**: разрешение использования команды ping адреса NGFW. • **SNMP**: доступ к NGFW по протоколу SNMP (UDP 161). • **response-pages**: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • **rpc**: XML-RPC для управления — позволяет управлять продуктом по API (TCP 4040). • **ha**: сервис, необходимый для объединения нескольких узлов NGFW в кластер (TCP 4369, TCP 9000-9100). • **VRRP**: сервис, необходимый для объединения нескольких узлов NGFW в отказоустойчивый кластер (IP протокол 112). • **"Admin Console"**: доступ к веб-консоли управления (TCP 8001). • **DNS**: доступ к сервису DNS-прокси (TCP 53, UDP 53). • **"HTTP Proxy"**: доступ к сервису HTTP(S)-прокси (TCP 8090). • **"Authorization agent"**: доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • **"SMTP Proxy"**: сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • **"POP3 Proxy"**: сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **VPN**: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • **SCADA**: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • **"REVERSE PROXY"**: сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • **"PROXY PORTAL"**: сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • **"SAML SERVER"**: выбор SAML-сервера в списке сервисов зоны и общих настройках NGFW. • **"Log Analyzer"**: сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный узел в качестве LogAn (TCP 2023 и 9713). • **"Dynamic routing OSPF"**: сервис динамической маршрутизации OSPF. • **"Dynamic routing BGP"**: сервис динамической маршрутизации BGP. • **"SNMP Proxy"**: сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • **"SSH Proxy"**: сервис, использующийся для инициирования трафика SSH. • **Multicast**: сервис мультикастинга. • **NTP**: доступ к сервису точного времени, запущенному на NGFW. • **"Dynamic routing RIP"**: сервис динамической маршрутизации RIP.
service-addresses	Указание разрешённых IP-адресов для сервисов: • **service**: выбор сервисов (список соответствует **enabled-services**). • **allowed-addresses**: разрешённые IP-адреса (задаются в формате IP/mask).
antispoof-enabled	Включение/отключение защиты от IP-спуфинга: • **on**. • **off**.
ip-spoofing-networks	Указание IP-адресов источников, допустимых в данной зоне; адреса указываются в формате <ip> или <ip/mask>. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены.
antispoof-negate	Возможные значения: • **on**. • **off**. При **antispoof-negate on** адреса источников, указанные в значении **ip-spoofing-networks**, будут являться адресами, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными IP-адресами источников.

Для обновления параметров зоны:

Admin@UGOS# set network zone <zone-name>

Для добавления новых сервисов к списку сервисов, разрешённым ранее используйте команду:

Admin@UGOS# set network zone <zone-name> ... enabled-services + [<service-name> ...] ...

Команда удаления зоны или её параметров:

Admin@UGOS# delete network zone <zone-name>

Параметры, доступные для удаления:

Параметр	Описание
dos-protection-syn	Защита зоны от сетевого флуда для протокола TCP (SYN-flood): • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-udp	Защита зоны от сетевого флуда для протокола UDP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.
dos-protection-icmp	Защита зоны от сетевого флуда для протокола ICMP: • **excluded-ips**: список IP-адресов серверов, которые необходимо исключить из защиты.

Параметр	Описание
enabled-services	Параметры контроля доступа зоны: • **"Any ICMP"**: разрешение использования команды ping адреса UserGate. • **SNMP**: доступ к UserGate по протоколу SNMP (UDP 161). • **response-pages**: разрешение для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • **rpc**: XML-RPC для управления — позволяет управлять продуктом по API (TCP 4040). • **ha**: сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • **VRRP**: сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • **"Admin Console"**: доступ к веб-консоли управления (TCP 8001). • **DNS**: доступ к сервису DNS-прокси (TCP 53, UDP 53). • **"HTTP Proxy"**: доступ к сервису HTTP(S)-прокси (TCP 8090). • **"Authorization agent"**: доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • **"SMTP Proxy"**: сервис фильтрации SMTP-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • **"POP3 Proxy"**: сервис фильтрации POP3-трафика от спама и вирусов. Необходим только при публикации почтового сервера в Интернет. • **"CLI over SSH"**: доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • **VPN**: доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • **SCADA**: сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. • **"REVERSE PROXY"**: сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. • **"PROXY PORTAL"**: сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. • **"SAML SERVER"**: выбор SAML-сервера в списке сервисов зоны и общих настройках UserGate. • **"Log Analyzer"**: сервис анализатора журналов Log analyzer. Необходимо включить его, если планируется использовать данный узел в качестве Log analyzer (TCP 2023 и 9713). • **"Dynamic routing OSPF"**: сервис динамической маршрутизации OSPF. • **"Dynamic routing BGP"**: сервис динамической маршрутизации BGP. • **"SNMP Proxy"**: сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • **"SSH Proxy"**: сервис, использующийся для инициирования трафика SSH. • **Multicast**: сервис мультикастинга. • **NTP**: доступ к сервису точного времени, запущенному на NGFW. • **"Dynamic routing RIP"**: сервис динамической маршрутизации RIP.
service-addresses	Разрешённые IP-адреса для сервисов: • **service**: выбор сервисов (список соответствует **enabled-services**). • **allowed-addresses**: разрешённые IP-адреса (задаются в формате IP/mask).
ip-spoofing-networks	При использовании защиты от IP-спуфинга администратор может указать IP-адреса источников, допустимых в данной зоне; адреса указываются в формате <ip> или <ip/mask>. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены.

Следующая команда отобразит настройки зоны:

Admin@UGOS# show network zone <zone-name>

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Список упорядоченных имён сетевых интерфейсов и соответствующие им физические адреса доступен для отображения при выполнении команды (команда доступна и в режиме диагностики и мониторинга и в режиме конфигурации):

Admin@UGOS> show network interface-mapping

Admin@UGOS# show network interface-mapping

Упорядочивание интерфейсов производится в соответствии с номером порта в шине PCI.

Для удаления списка используйте следующие команды в режиме диагностики и мониторинга и в режиме конфигурации соответственно:

Admin@UGOS> clear network interface-mapping

Admin@UGOS# delete network interface-mapping

После перезагрузки NGFW список обновится и станет доступным для отображения. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate.

Далее будет рассмотрена настройка интерфейсов, которая производится на уровне **network interface**.

Настройка adapter

Сетевые адаптеры настраиваются на уровне **network interface adapter**.

Создать сетевой адаптер нельзя. Для обновления существующего сетевого адаптера:

Admin@UGOS# set network interface adapter

Далее необходимо указать параметры сетевого адаптера:

Параметр	Описание
enabled	Включение/отключение сетевого интерфейса: • **on**. • **off**.
description	Описание сетевого интерфейса.
iface-type	Тип интерфейса: • **l3**: интерфейс, работающий в режиме Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_pvlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_pvlan** — NGFGW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# set network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
lldp-profile	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей читайте в разделе Настройка профилей LLDP.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.

Параметр	Описание
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса NGFW, на который добавляется функция релея (принимает значения <ip | none>). • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Команда удаления адаптера или его параметров:

Admin@UGOS# delete network interface adapter <adapter-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Команда для отображения информации о всех сетевых адаптерах:

Admin@UGOS# show network interface adapter

Для отображения информации об адаптере:

Admin@UGOS# show network interface adapter <adapter-name>

Настройка VLAN

Интерфейсы VLAN настраиваются на уровне **network interface vlan**.

Команда для добавления нового VLAN-интерфейса:

Admin@UGOS# create network interface vlan

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VLAN-интерфейса: • **on**. • **off**.
description	Описание интерфейса.
iface-type	Тип интерфейса: • **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **mirror**: интерфейс, работающий в режиме Mirror (может получать трафик со SPAN-порта сетевого оборудования для его анализа).
tag	Тег VLAN. Допускается создание до 4094 интерфейсов.
node-name	Имя узла кластера, на котором создаётся VLAN.
interface	Физический интерфейс, на котором создается VLAN.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.

Параметр	Описание
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса UserGate, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего VLAN:

Admin@UGOS# set network interface vlan <vlan-name>

Параметры, доступные для обновления, аналогичны параметрам создания VLAN, кроме **tag**, **node-name**, **interface** (изменение значений этих параметров недоступно).

Команда удаления VLAN-интерфейса или его параметров:

Admin@UGOS# delete network interface vlan <vlan-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех интерфейсах VLAN:

Admin@UGOS# show network interface vlan

или об определённом интерфейсе:

Admin@UGOS# show network interface vlan <vlan-name>

Настройка bond-интерфейса

Настройка бонд-интерфейса производится на уровне **network interface bond**.

Команда для создания бонд-интерфейса:

Admin@UGOS# create network interface bond

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение интерфейса: • **on**. • **off**.
description	Описание интерфейса.
node-name	Узел кластера, на котором будет создан бонд-интерфейс.
zone	Зона, которой будет принадлежать бонд.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.

Параметр	Описание
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bond1).
bonding	Дополнительные параметры бонд-интерфейса: • **aggr-mode** — режим работы бонда: ◦ **round-robin**: режим Round robin (пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости). ◦ **active-backup**: режим Active backup (только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Данная политика применяется для обеспечения отказоустойчивости). ◦ **xor**: режим XOR (передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и обеспечения отказоустойчивости). ◦ **broadcast**: режим Broadcast (передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости). ◦ **802.3ad**: режим IEEE 802.3ad (режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику). ◦ **transmit**: режим Adaptive transmit load balancing (исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты). ◦ **load**: режим Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. • **mii-monitoring**: периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. • **down-delay**: время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. • **up-delay**: время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. • **lacp-rate**: интервал, с которым будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: ◦ **slow**: запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. ◦ **fast**: запрос партнера на передачу LACPDU-пакетов каждую секунду. • **failover-mac**: определение способа назначения MAC-адресов на объединенные интерфейсы в режиме Active backup при переключении интерфейсов. Возможные значения: ◦ **disabled**: устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. ◦ **active**: MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. ◦ **follow**: MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. • **xmit-hash**: определение хэш-политики передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: ◦ **l2**: использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. ◦ **l2-3**: использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. ◦ **l3-4**: используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы. • **interface**: интерфейсы, которые будут объединены в бонд.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подести задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размер MTU.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса NGFW, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего бонд-интерфейса:

Admin@UGOS# set network interface bond <bond-name>

Параметры, доступные для обновления, аналогичны параметрам создания бонд-интерфейс, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления бонд-интерфейса или его параметров:

Admin@UGOS# delete network interface bond <bond-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.
bonding interface	Интерфейсы, объединённые в бонд.

Чтобы отобразить информацию о всех бонд-интерфейсах:

Admin@UGOS# show network interface bond

или об определённом интерфейсе:

Admin@UGOS# show network interface bond <bond-name>

Настройка bridge-интерфейса

Настройка моста производится на уровне **network interface bridge**.

Чтобы добавить новый bridge-интерфейс:

Admin@UGOS# create network interface bridge

Параметры, которые необходимо указать:

Параметр	Описание
enabled	Включение/отключение моста: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет bridge1).
description	Описание bridge-интерфейса.
node-name	Имя узла кластера, на котором создаётся мост.
zone	Зона, которой будет принадлежать мост.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
bridging	Дополнительные параметры моста: • **iface-type**: режим работы интерфейса: ◦ **l2**: Layer 2 (создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила Mail security; контентная фильтрация в этом режиме работает). ◦ **l3**: Layer 3 (можно назначить IP-адрес и использовать его в правилах межсетевого экрана, контентной фильтрации и других правилах, это стандартный режим работы интерфейса). • **interface**: интерфейсы, которые будут использованы для создания моста. • **stp**: включение/отключение использование STP (Spanning Tree Protocol) для защиты от петель: ◦ **on.** ◦ **off**. • **forward-delay**: задержка перед переключением моста в активный режим (Forwarding), в случае если включен STP (указывается в секундах). • **max-age**: время, по истечении которого STP-соединение считается потерянным (указывается в секундах). • **bypass-pair**: пара интерфейсов, которая будет использована для построения байпас моста. Требуется поддержка оборудования ПАК NGFW.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса.

Параметр	Описание
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подсети задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mac	MAC-адрес интерфейса.
mtu	Указание размера MTU.
dhcp-relay	Настройка работы DHCP-релея на интерфейсе. Необходимо указать: • **enabled**: включение/отключения релея: ◦ **on**. ◦ **off**. • **utm-address**: IP-адрес интерфейса NGFW, на который добавляется функция релея. • **server-address**: адреса серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Обновление существующего bridge-интерфейса:

Admin@UGOS# set network interface bridge <bridge-name>

Параметры, доступные для обновления, аналогичны параметрам создания моста, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда удаления bridge-интерфейса или его параметров:

Admin@UGOS# delete network interface bridge <bridge-name>

Параметры, доступные для удаления:

Параметр	Описание
ip-addresses	Заданный IP-адрес.
dhcp-relay server-address	IP-адрес сервера DHCP.

Чтобы отобразить информацию о всех bridge-интерфейсах:

Admin@UGOS# show network interface bridge

или об определённом интерфейсе:

Admin@UGOS# show network interface bridge <bridge-name>

Настройка PPPoE

Настройка интерфейса PPPoE производится на уровне **network interface PPPoE**.

Для создания интерфейса PPPoE:

Admin@UGOS# network interface PPPoE

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение интерфейса PPPoE: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет ppp1).
description	Описание интерфейса PPPoE.
node-name	Имя узла кластера, на котором создаётся интерфейс.
zone	Зона, которой будет принадлежать интерфейс.
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.

Параметр	Описание
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
pppoe-config	Дополнительные параметры PPPoE интерфейса: • **interface**: интерфейс, на котором будет создаваться интерфейс PPPoE. • **login**: имя пользователя для соединения PPPoE. • **password**: пароль пользователя для соединения PPPoE. • **persist-connection**: автоматическое переподключение при обрыве связи: ◦ **on**. ◦ **off**. • **auth-type**: тип авторизации: ◦ **CHAP**. ◦ **PAP**. • **holdoff**: интервал времени в секундах после разрыва соединения перед повторным запуском. • **default-route**: интерфейс PPPoE в качестве маршрута по умолчанию: ◦ **on**. ◦ **off**. • **lcp-echo-interval**: интервал проверки соединения. • **lcp-echo-failure**: количество неуспешных проверок соединения, после которого UserGate считает, что соединение отсутствует и разрывает его. • **providers-dns**: использование DNS-серверов, выданных провайдером: ◦ **on**. ◦ **off**. • **connection-attempts**: количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены. • **service-name**: имя сервиса необходимо прописывать в случае предоставления провайдером.
mtu	Указание размера MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet.

Обновление существующего интерфейса PPPoE:

Admin@UGOS# set network interface PPPoE <PPPoE-name>

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name** (изменение значения этого параметра недоступно).

Команда удаления интерфейса PPPoE:

Admin@UGOS# delete network interface PPPoE <PPPoE-name>

Чтобы отобразить информацию о всех интерфейсах PPPoE:

Admin@UGOS# show network interface PPPoE

или об определённом интерфейсе:

Admin@UGOS# show network interface PPPoE <PPPoE-name>

Настройка VPN-адаптера

VPN-адаптеры настраиваются на уровне **network interface vpn**.

Чтобы создать VPN-адаптер:

Admin@UGOS# network interface vpn

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение VPN-интерфейса: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в имени интерфейса (например 1, тогда название созданного интерфейса будет tunnel1).
description	Описание VPN-интерфейса.
zone	Зона, которой будет принадлежать интерфейс.

Параметр	Описание
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
netflow-profile	Профиль NetFlow для отправки статистических данных на NetFlow коллектор. Подробнее о настройке профилей NetFlow читайте в разделе Настройка профилей NetFlow.
iface-mode	Режим назначения IP-адреса: • **dhcp**: получение динамического IP-адреса по DHCP. • **manual**: без адреса. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN), то необходимо использовать статический IP-адрес. Статический режим устанавливается автоматически при назначении интерфейсу IP-адреса. Для использования интерфейса, используемого в роли клиента, необходимо выбрать динамический режим.
ip-addresses	Назначение интерфейсу IP-адреса. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подести задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.
mtu	Указание размера MTU для выбранного интерфейса.

Обновление существующего интерфейса VPN:

Admin@UGOS# set network interface vpn <vpn-name>

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name** (изменение значения этого параметра недоступно).

Команда для удаления интерфейса VPN или его параметров:

Admin@UGOS# delete network interface vpn <vpn-name>

Параметры, доступные для удаления: **ip-addresses**.

Чтобы отобразить информацию о всех интерфейсах VPN:

Admin@UGOS# show network interface vpn

или об определённом интерфейсе:

Admin@UGOS# show network interface vpn <vpn-name>

Настройка туннелей

Создание и настройка туннелей производится на уровне **network interface tunnel**.

Для создания туннелей используется команда:

Admin@UGOS# network interface tunnel

Далее необходимо указать параметры:

Параметр	Описание
enabled	Включение/отключение туннеля: • **on**. • **off**.
interface-name	Необходимо ввести номер, который будет отображён в названии туннеля (например 1, тогда название созданного интерфейса будет gre1).
description	Описание туннеля.
node-name	Узел кластера, на котором будет создан туннель.
zone	Зона, которой будет принадлежать интерфейс.

Параметр	Описание
link-info	Настройка параметров сетевого интерфейса: • **bc_forwarding**: управление пересылкой пакетов directed broadcast, приходящих на указанный интерфейс. • **proxy_arp**, **proxy_arp_vlan**: механизм Proxy ARP. Параметр **proxy_arp** — NGFW будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса; **proxy_arp_vlan** — NGFW будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса. Указываются в следующем формате: Admin@UGOS# create network interface <iface-type> ... link-info [key/value] где key — название параметра. Название может состоять из строчных букв латинского алфавита (a — z) и знака подчеркивания (_). value — значение параметра. Параметры могут принимать только целые числовые значения. Например, чтобы включить использование механизма Proxy ARP используйте следующие key/value — proxy_arp/1; для отключения — proxy_arp/0. Поле link-info будет отображено только в случае добавления параметров. **Важно!** Удаление заданных параметров недоступно.
mtu	Размер MTU для выбранного интерфейса.
tunnel-config	Дополнительные параметры интерфейса: • **local-ip**: локальный адрес Point-to-Point интерфейса. • **remote-ip**: удалённый адрес Point-to-Point интерфейса. • **iface-mode**: режим работы туннеля: ◦ **gre**: GRE (протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47). ◦ **ipip**: IPIP (протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP пакета в другой IP пакет, это добавление внешнего заголовка с Source IP — точкой входа в туннель, и Destination — точкой выхода из туннеля). ◦ **vxlan**: VXLAN (протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789). • **vni**: идентификатор VXLAN. Только для типа туннеля VXLAN.
ip-addresses	IP-адрес, назначенный туннельному интерфейсу. Адрес задаётся в следующем виде: **[<ip_address/mask>]** или **[<ip_address/mask> <ip_address/mask>]**, если необходимо назначить несколько IP-адресов (адреса перечисляются через пробел); маска подести задаётся в десятичном виде. **Важно!** Квадратные скобки обязательно должны быть отделены пробелами с обеих сторон.

Обновление существующего туннеля:

Admin@UGOS# set network interface tunnel <tunnel-name>

Параметры, доступные для обновления, аналогичны параметрам создания интерфейса, кроме **interface-name**, **node-name** (изменение значений этих параметров недоступно).

Команда для удаления интерфейса туннель или его параметров:

Admin@UGOS# delete network interface tunnel <tunnel-name>

Параметры, доступные для удаления: **ip-addresses**.

Чтобы отобразить информацию о всех туннелях:

Admin@UGOS# show network interface tunnel

или об определённом интерфейсе:

Admin@UGOS# show network interface tunnel <tunnel-name>

Шлюзы

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Данный раздел находится на уровне **network gateway**.

Для добавления нового шлюза используется команда:

Admin@UGOS# create network gateway

Доступные параметры:

Параметр	Описание
enabled	Включение/отключение шлюза: • **on**. • **off**.
name	Название шлюза.
description	Описание шлюза.
node-name	Имя узла кластера, на котором создаётся шлюз.
interface	Интерфейс, использующийся для выхода в Интернет.
virtual-router	Выбор виртуального маршрутизатора, для которого настраивается шлюз.
ip	IP-адрес шлюза.
weight	Вес шлюза (чем больше вес, тем большая доля трафика идет через шлюз).
balancing	Режим балансировки - весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами: • **on**. • **off**.
default	Использование данного шлюза в качестве шлюза по умолчанию: • **on**. • **off**.

Обновление параметров шлюза:

Admin@UGOS# set network gateway <gateway-name>

Список параметров, доступных для изменения, аналогичен списку, доступному при создании шлюза, кроме **node-name** (изменение значения данного параметра недоступно).

Команда для удаления шлюза:

Admin@UGOS# delete network gateway <gateway-name>

Чтобы отобразить информацию о всех шлюзах:

Admin@UGOS# show network gateway

или об определённом шлюзе:

Admin@UGOS# show network gateway <gateway-name>

DHCP

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Раздел находится на уровне **network dhcp**.

Для создания подсети DHCP, используется команда:

Admin@UGOS# create network dhcp

Далее необходимо указание параметров:

Параметр	Описание
enabled	Включение/отключение использования данного диапазона IP-адресов: • **on**. • **off**.
name	Название подсети.
description	Описание подсети.
node-name	Выбор узла кластера, на котором создается данный диапазон.
interface	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона.
ip-range	Диапазон IP-адресов, выдаваемый клиентам DHCP. Диапазон задаётся в формате: <IP_start-IP_end>.
mask	Маска подсети, выдаваемая клиентам DHCP.
expiration-time	Время в секундах, на которое выдаются IP-адреса.
domain	Название домена, выдаваемое клиентам DHCP.
gateway-address	IP-адрес шлюза, выдаваемый клиентам DHCP.
dns-servers	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
reserved-hosts	MAC-адреса и сопоставленные с ними IP-адреса: • **mac**: MAC-адрес. • **ip**: IP-адрес, сопоставленный MAC-адресу. • **hostname**: имя хоста.
ignored-mac	Список MAC-адресов, игнорируемых DHCP-сервером.
pxe-boot-ip	Адрес сервера PXE.
pxe-boot-filename	Название файла для загрузки с PXE-сервера.
options	Номер опции и ее значение: • **code**: номер опции DHCP. • **values**: значение опции.

Обновление существующей DHCP-подсети:

Admin@UGOS# set network dhcp <dhcp-name>

Параметры, информацию о которых можно обновить, аналогичны параметрам, доступным при создании, кроме параметров **node-name**, **interface** - изменение значений данных параметров недоступно.

Для удаления подсети:

Admin@UGOS# delete network dhcp <dhcp-name>

Также доступно удаление отдельных параметров подсети DHCP:

- **dns-servers**.
- **ignored-mac**.
- **reserved-hosts** (необходимо указать все три значения: **mac**, **ip**, **hostname**).
- **options** (необходимо указать оба значения: **code**, **values**).

Чтобы отобразить информацию о всех созданных подсетях:

Admin@UGOS# show network dhcp

или об определённой подсети DHCP:

Admin@UGOS# show network dhcp <dhcp-name>

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Раздел находится на уровне **network dns**.

Настройка системных DNS-серверов

Настройка системных серверов DNS производится на уровне **network dns system-dns-servers**.

Для добавления новых DNS-серверов или обновления существующего списка используются следующие команды:

Admin@UGOS# set network dns system-dns-servers + [<ip> <ip> ...] Admin@UGOS# set network dns system-dns-servers [<ip> <ip> ...]

Для удаления всего списка адресов серверов DNS:

Admin@UGOS# delete network dns system-dns-servers

Для удаления определённых серверов:

Admin@UGOS# delete network dns system-dns-servers [<ip> <ip> ...]

Для отображения списка системных DNS-серверов используется команда:

Admin@UGOS# show network dns system-dns-servers

Настройка DNS-прокси

DNS-прокси настраивается на уровне **network dns proxy-settings**.

Для обновления настроек DNS-прокси используется следующая команда:

Admin@UGOS# set network dns proxy-settings

Далее необходимо указать параметры, значения которых необходимо изменить:

Параметр	Описание
filtering	Фильтрация DNS-запросов: • **on**. • **off**.
caching	Кэширование ответов DNS: • **on**. • **off**.
limit	Ограничение количества DNS-запросов в секунду для каждого пользователя (значение по умолчанию: 100).
max-ttl	Максимально возможное время жизни для записей DNS.
recursive	Осуществление рекурсивных DNS-запросов: • **on**. • **off**.
dns-timeout	Время до следующей попытки отправления запроса на DNS-сервера (указывается в миллисекундах).
a-aaaa-unknown	Ответы только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS: • **on**. • **off**.
retries	Количество попыток DNS-запроса.
factory-defaults	Сброс до заводских настроек значения выбранного параметра (параметры представлены в данной таблице) или всех параметров (**all**).

Чтобы просмотреть настройки DNS-прокси:

Admin@UGOS# show network dns proxy-settings

Параметры, значения которых можно просмотреть, представлены в таблице выше.

Настройка правил DNS

Правила DNS настраиваются на уровне **network dns rules** с использованием UPL. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Параметры правил DNS:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение использования правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.

Параметр	Описание
name	Название правила. Например: **name("DNS rule example")**.
desc	Описание правила DNS-прокси. Например: **desc("DNS rule example set via CLI")**.
url.domain	Список доменов, на которые необходимо перенаправлять. Допускается использование звёздочки (*) для указания шаблона доменов. Чтобы указать список доменов: **url.domain = "*.example.com"**.
dns_server	Список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены. Для указания сервера: **dns_server(1.2.3.4)**.

Настройка статистических записей DNS-прокси

Раздел находится на уровне **network dns static-records**.

Для добавления статической DNS-записи предназначена команда:

Admin@UGOS# create network dns static-records

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статической записи: • **on**. • **off**.
name	Название записи.
description	Описание DNS-записи.
domain	FQDN (Fully Qualified Name) статической записи, например, www.example.com.
static-dns-ips	Список IP-адресов, которые сервер UserGate будет возвращать при запросе данного FQDN.

Для обновления информации о статических DNS-записях:

Admin@UGOS# set network dns static-records <static-record-name>

Список параметров, доступных для изменения, аналогичен списку команды **create**.

Для удаления статической записи:

Admin@UGOS# delete network dns static-records <static-record-name>

Также возможно удаление из статической записи только значений параметра **static-dns-ips**.

Команда

Admin@UGOS# show network dns static-records

отобразит информацию о всех существующих статических DNS-записях. Для отображения информации об определённой записи:

Admin@UGOS# show network dns static-records <static-record-name>

Настройка виртуальных маршрутизаторов

Technology: Routing
Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

В данном разделе описана настройка статических маршрутов, протоколов динамической маршрутизации OSPF, BGP, RIP и мультикаст-маршрутизации с использованием интерфейса командной строки (настройка рассмотрена в соответствующих разделах). Настройка производится на уровне **network virtual-router**.

Далее представлены команды, использующиеся для общей настройки виртуальных маршрутизаторов.

Команда для добавления нового виртуального маршрутизатора:

Admin@UGOS# create network virtual-router

Далее указываются параметры:

Параметр	Описание
name	Уникальное имя виртуального маршрутизатора.
description	Описание виртуального маршрутизатора
node	Выбор узла NGFW, на котором будет создан виртуальный маршрутизатор (при наличии кластера).
interface	Интерфейсы, которые будут использованы в данном виртуальном маршрутизаторе. Интерфейсы, добавленные в другие виртуальные маршрутизаторы, добавлены быть не могут; любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. В виртуальный маршрутизатор разрешается добавлять интерфейсы всех типов — физические, виртуальные (VLAN), бондинг, VPN и другие.
route	Добавление маршрутов, которые будут применены к трафику в данном виртуальном маршрутизаторе. Подробнее читайте в разделе Настройка статических маршрутов.
ospf	Добавление динамических маршрутов, получаемых по протоколу маршрутизации OSPF. Подробнее читайте в разделе Настройка OSPF.
bgp	Добавление динамических маршрутов, получаемых по протоколу маршрутизации BGP. Подробнее смотрите в разделе Настройка BGP.
rip	Добавление динамических маршрутов, получаемых по протоколу маршрутизации RIP. Подробнее читайте в разделе Настройка RIP.
multicast-router	Настройка мультикастинга в данном виртуальном маршрутизаторе. Подробнее о настройке мультикастинга использованием интерфейса командной строки смотрите в разделе Настройка мультикаст-маршрутизации.

Следующая команда предназначена для изменения параметров виртуального маршрутизатора:

Admin@UGOS# set network virtual-router <virtual-router-name>

Параметры, доступные для обновления, аналогичны параметрам команды **create**, кроме:

- **name**.
- **node-name**.

Чтобы удалить виртуальный маршрутизатор используется команда:

Admin@UGOS# set network virtual-router <virtual-router-name>

Команда для отображения информации о виртуальном маршрутизаторе:

Admin@UGOS# show network virtual-router <virtual-router-name>

Настройка статических маршрутов

Для добавления нового статического маршрута используется команда:

Admin@UGOS# set network virtual-router <virtual-router-name> route new

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение использования статического маршрута: • **on**. • **off**.
name	Имя маршрута.
description	Описание маршрута.

Параметр	Описание
type	Тип маршрута: • **unicast** — стандартный тип маршрута. Пересылает трафик, адресованный на адреса назначения, через заданный шлюз. • **unreachable** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 1). • **prohibit** — трафик отбрасывается. Источнику отправляется ICMP сообщение host unreachable (type 3 code 13). • **blackhole** — трафик отбрасывается (теряется), не сообщая источнику о том, что данные не достигли адресата.
destination-ip	IP-адрес подсети назначения; указывается в формате <ip/mask>.
gateway-address	IP-адрес шлюза, через который будет доступна указанная подсеть; этот IP-адрес должен быть доступен с NGFW.
interface	Интерфейс, через который будет добавлен маршрут.
metric	Метрика маршрута. Если маршрутов в данную сеть несколько: чем меньше метрика, тем приоритетней маршрут

Чтобы изменить параметры созданного ранее статического маршрута, используйте команду:

Admin@UGOS# set network virtual-router <virtual-router-name> route <static-route-name>

Параметры, доступные для изменения, представлены в таблице выше.

Используйте следующую команду для удаления статического маршрута:

Admin@UGOS# delete network virtual-router <virtual-router-name> route <static-route-name>

Для отображения статических маршрутов:

Admin@UGOS# show network virtual-router <virtual-router-name> route

Настройка OSPF

Для настройки OSPF с использованием CLI используйте следующую команду:

Admin@UGOS# set network virtual-router <virtual-router-name> ospf

Далее необходимо указать параметры OSPF-маршрутизатора:

Параметр	Описание
enabled	Включение/отключение OSPF-маршрутизатора: • **on**. • **off**.
router-id	IP-адрес маршрутизатора. Должен быть уникальным и задан в формате IPv4 (для удобства может совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору). При выключении OSPF (**enabled off**) значение **router-id** может быть удалено (**none**).
connected	Распространение другим роутерам OSPF маршрутов в непосредственно подключённые к NGFW сети: • **on**. • **off**.
kernel	Распространение другим роутерам OSPF маршрутов, которые были добавлены администратором: • **on**. • **off**.
metric	Метрика распространяемых маршрутов.
default-originate	Оповещение других маршрутизаторов о том, что у данного роутера настроен маршрут по умолчанию: • **on**. • **off**.

Параметр	Описание
interface	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор. Для добавления интерфейса или изменения параметров добавленного ранее интерфейса используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> ospf interface new Admin@UGOS# set network virtual-router <virtual-router-name> ospf interface <interface-name> Далее указываются следующие параметры: • **enabled <on | off>**: включение/отключение использования интерфейса. • **interface**: название интерфейса, входящего в данный виртуальный маршрутизатор. • **description**: описание интерфейса. • **cost**: стоимость канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1. • **priority**: целое число от 0 до 255. Чем больше значение, тем выше шанс у маршрутизатора стать назначенным маршрутизатором (designated router) в сети для рассылки LSA. Значение 0 делает назначение для данного маршрутизатора невозможным. Значение по умолчанию 1. • **hello-interval**: время, через которое маршрутизатор посылает hello-пакеты; указывается в секундах. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд. • **dead-interval**: время, по истечению которого маршрутизатор считается неработающим; указывается в секундах. Время исчисляется от момента приема последнего пакета hello от соседнего маршрутизатора. Значение по умолчанию 40 секунд. • **retransmit-interval**: временный интервал перед повторной отсылкой пакета LSA; указывается в секундах. Значение по умолчанию 5 секунд. • **transmit-delay**: примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state); задаётся в секундах. Значение по умолчанию 1 секунда. • **authentication**: тип аутентификации. Доступны: ◦ **enabled <on | off>** — включение/отключение требования аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов. ◦ **auth-type** — выбор типа аутентификации: **plain** (передача ключа в открытом виде для аутентификации роутеров) или **digest** (использование MD5-хеша для ключа для аутентификации OSPF-пакетов). ◦ **md5-key-id** — идентификатор ключа. ◦ **key** — ключ. Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.
area	Настройка области OSPF. Для добавления новой области или изменения параметров созданной ранее области используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> ospf area new Admin@UGOS# set network virtual-router <virtual-router-name> ospf area <area-name> Далее указываются следующие параметры: • **enabled <on | off>**: включение/отключение использования данной области. • **name**: название области. • **description**: описание области. • **cost**: стоимость LSA, анонсируемых в stub-области. • **area-id**: идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Идентификатор области должен совпадать для установления соседства OSPF. • **auth-type**: тип авторизации. Доступны следующие значения: ◦ **none** — не требовать авторизацию OSPF-пакетов. ◦ **plain** — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. ◦ **digest** — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Идентификация на уровне интерфейсов имеет приоритет над авторизацией на уровне зоны. • **area-type**: тип области OSPF. Доступны следующие типы: ◦ **normal** — обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты. ◦ **nssa** — Not-So-Stubby Area определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR). ◦ **stub** — тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. • **no-summary**: разрешение/запрет инжекции суммированных маршрутов в тупиковые типы областей: ◦ **on**. ◦ **off**. • **interface**: выбор интерфейсов OSPF, на которых будет доступна данная зона. • **virtual-links**: Специальное соединение, которое позволяет соединять, например, разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение или как backup на случай выхода из строя основных соединений. Можно указать идентификаторы маршрутизаторов, которые доступны через данную зону.

Для удаления настроек OSPF используется команда:

Admin@UGOS# delete network virtual-router <virtual-router-name> ospf

Параметры, доступные для удаления:

- **interface**.
- **area**.

Следующая команда используется для отображения конфигурации OSPF в виртуальном маршрутизаторе:

Admin@UGOS# show network virtual-router <virtual-router-name> ospf

Настройка BGP

Настройка протокола динамической маршрутизации BGP (Border Gateway Protocol) в виртуальном маршрутизаторе производится с использованием следующей команды:

Admin@UGOS# show network virtual-router <virtual-router-name> bgp

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение BGP-маршрутизатора: • **on**. • **off**.
router-id	IP-адрес маршрутизатора. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору. При выключении BGP (**enabled off**) значение **router-id** может быть удалено (**none**).
as-number	Автономная система — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе.
multiple-path	Включение/отключение балансировки трафика на маршруты с одинаковой стоимостью: • **on**. • **off**.
connected	Распространение другим роутерам BGP маршрутов в непосредственно подключённые к NGFW сети: • **on**. • **off**.
kernel	Распространение другим роутерам BGP маршрутов, которые были добавлены администратором: • **on**. • **off**.
ospf-redistribute	Распространение другим роутерам BGP маршрутов, полученных по протоколу OSPF: • **on**. • **off**.
network-addrs	Список сетей, относящихся к данной автономной системе. Необходимо указать в формате <ip/mask>.
routemaps	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами. Для создания routemap или изменения параметров созданного ранее routemap используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> bgp routemaps new Admin@UGOS# set network virtual-router <virtual-router-name> bgp routemaps <routemap-name> Параметры routemap: • **name** — название routemap. • **description** — описание routemap. • **action** — действие: ◦ **allow** — разрешить прохождение данных, попадающих под условия routemap. ◦ **block** — запретить прохождение данных, попадающих под условия routemap. • **match-by** — условие применения routemap. Сравнивать по: ◦ **ip** — сравнение по IP-адресу. ◦ **aspath** — сравнение по AS пути. ◦ **community** — сравнение по Community. • **next-hop** — установка для отфильтрованных маршрутов значения next hop в указанный IP-адрес. • **weight** — установка для отфильтрованных маршрутов веса в указанное значение. • **metric** — установка для отфильтрованных маршрутов метрики в указанное значение. • **preference** — установка для отфильтрованных маршрутов предпочтения в указанное значение. • **as-prepend** — установка значения AS-prepend — список автономных систем, добавляемых для данного маршрута. • **community** — установка значения для BGP community для отфильтрованных маршрутов. • **append-community** — Добавлять community. • **ip-match** — необходимо добавить все необходимые IP-адреса при выборе сравнения по IP-адресу. • **as-path-match** — необходимо добавить все необходимые номера автономных сетей при выборе сравнения по AS-пути. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (_), который интерпретируется как: ◦ Пробел. ◦ Запятая. ◦ Начало строки. ◦ Конец строки. ◦ AS set delimiter { and }. ◦ AS confederation delimiter (and). ◦ **community-match** — необходимо добавить строки всех необходимых BGP community при выборе сравнения по Community.

Параметр	Описание
filters	Фильтр позволяет фильтровать маршруты при перераспределении. Для создания фильтра или изменения параметров созданного ранее фильтра используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> bgp filters new Admin@UGOS# set network virtual-router <virtual-router-name> bgp filters <filter-name> Параметры: • **name** — название фильтра. • **description** — описание фильтра. • **action** — действие: ◦ **allow** — разрешить прохождение данных, попадающих под условия routemap. ◦ **block** — запретить прохождение данных, попадающих под условия routemap. • **filter-by** — условия применения фильтра. Доступно: ◦ **ip** — фильтровать по IP-адресу. ◦ **aspath** — фильтровать по AS пути. • **ip-filter** — необходимо добавить все необходимые IP-адреса при выборе фильтрации по IP-адресу. Адреса могут быть указаны в следующих форматах: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0./8:11 — маршруты, у которых первый октет 10 и префикс от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13. • **as-path-filter** — необходимо добавить все необходимые номера автономных сетей при выборе фильтрации по AS пути.

Параметр	Описание
neighbors	BGP-соседи. Для добавления новых соседей или изменения данных о ранее добавленных соседях используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> bgp neighbors new Admin@UGOS# set network virtual-router <virtual-router-name> bgp neighbors <host-ip> Параметры: • **enabled** — включение/отключение использования соседа: ◦ **on**. ◦ **off**. • **description** — описание BGP-соседа. • **host** — IP-адрес соседа. • **remote-asn** — номер автономной системы, к которой относится сосед. • **weight** — вес маршрутов, получаемых от данного соседа. • **ttl** — максимальное количество хопов, разрешенное до этого соседа. • **allowas-in** — эта функция позволяет получать и обрабатывать маршруты, даже если маршрутизатор обнаруживает собственный номер автономной системы в AS Path в маршруте агрегации. ◦ **on**. ◦ **off**. • **allowas-in-number** — количество раз, которое в AS Path может содержаться номер автономной системы BGP-соседа. Возможны значения от 0 до 10 (0 — origin) • **next-hop-self** — замена значения next-hop-self на собственный IP-адрес, если сосед является BGP: ◦ **on**. ◦ **off**. • **ebgp-multihop** — до этого BGP-соседа непрямое соединение (более одного хопа): ◦ **on**. ◦ **off**. • **route-reflector-client** — определение, является ли BGP-сосед клиентом Route reflector: ◦ **on**. ◦ **off**. • **soft-reconfiguration** — использование soft reconfiguration (без разрыва соединений) для обновления конфигурации: ◦ **on**. ◦ **off**. • **default-originate** — анонс соседу маршрут по умолчанию: ◦ **on**. ◦ **off**. • **send-community** — пересылать community BGP-соседям: ◦ **on**. ◦ **off**. • **enable-auth** — включение/отключение аутентификации для соседа: ◦ **on**. ◦ **off**. • **password** — пароль для аутентификации соседа. • **filter-in** — ограничение информации о маршрутах, получаемых от соседей. • **filter-out** — ограничение информации о маршрутах, анонсируемых соседям. • **routemap-in** — ограничение маршрутизирующей информации, которую BGP получает от соседей. • **routemap-out** — ограничение маршрутизирующей информации, которую BGP отдаёт соседям.

Команда, использующуюся для удаления параметров BGP-маршрутизатора:

Admin@UGOS# delete network virtual-router <virtual-router-name> bgp

Для удаления доступны следующие параметры:

- Адреса сетей, относящихся к данной автономной системе: **network-addrs**.
- Условия применения routemap: **routemaps <routemap-name> ip-match** | **community-match** | **as-path-match** .
- Условия применения фильтра: **filters <filter-name> ip-filter** | **as-path-filter** .
- Фильтры BGP-соседей и routemaps: **neighbors <host-ip> filter-in** | **filter-out** | **routemap-in** | **routemap-out** .

Следующая команда используется для отображения конфигурации BGP в виртуальном маршрутизаторе:

Admin@UGOS# show network virtual-router <virtual-router-name> bgp

Настройка RIP

Настройка протокола маршрутизации RIP (Routing Information Protocol) в виртуальном маршрутизаторе производится с использованием следующей команды:

Admin@UGOS# show network virtual-router <virtual-router-name> rip

Далее указываются параметры:

Параметр	Описание

Параметр	Описание
enabled	Включение/отключение RIP-маршрутизатора: • **on**. • **off**.
rip-version	Версия протокола RIP: • **1**. • **2**. Как правило, используется 2-я версия протокола.
default-metric	Метрика RIP. По умолчанию метрика равна 1; максимальное значение — 15. Значение 16 считается бесконечным.
admin-distance	Стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).
default-originate	Отправлять себя в качестве маршрута по умолчанию.
network-cidr	Указание сети в виде CIDR. Указывается в формате <ip/mask>.
network-interface	Указание сетевого интерфейса, с которого будут отправлять обновления маршрутной информации; указываются интерфейсы, принадлежащие виртуальному маршрутизатору.
redistribute	Распространение маршрутов: • **connected** — распространение другим роутерам RIP маршрутов в непосредственно подключённые к NGFW сети: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ **off**. • **static** — распространение другим маршрутизаторам статических маршрутов: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ **off**. • **kernel** — распространение другим роутерам RIP маршрутов, которые были добавлены администратором: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ **off**. • **ospf-redistribute** — распространение другим RIP-роутерам маршрутов, полученных по OSPF: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ **off**. • **bgp-redistribute** — распространение другим RIP-роутерам маршрутов, полученных по BGP: ◦ <metric> — значение метрики; может принимать значения от 0 до 16. ◦ **off**.

Параметр	Описание
interfaces	Настройка интерфейсов, на которых поддерживается протокол RIP; интерфейсы должны быть добавлены в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces new Admin@UGOS# set network virtual-router <virtual-router-name> rip interfaces <interface-name> Параметры: • **interface** — выбор интерфейса. • **send-version** — версия протокола RIP, которую маршрутизатор будет отсылать. Доступны: ◦ **0**. ◦ **1**. ◦ **2**. ◦ **3**. • **receive-version** -версия протокола RIP, которую маршрутизатор будет принимать. Доступны: ◦ **0**. ◦ **1**. ◦ **2**. ◦ **3**. • **password** — строка для авторизации, которая будет посылаться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль. • **split-horizon** — метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который прибыло обновление. ◦ **on**. ◦ **off**. • **poison-reverse** — метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута в 16 и отсылает его соседу, от которого его получил. ◦ **on**. ◦ **off**. • **passive-mode** — режим работы интерфейса, при котором он принимает обновления RIP, но не отсылает их. ◦ **on**. ◦ **off**.

Команда, использующуюся для удаления параметров RIP-маршрутизатора:

Admin@UGOS# delete network virtual-router <virtual-router-name> rip

Для удаления доступны следующие параметры:

- Интерфейсы RIP: **interfaces**.
- Сети RIP: **network-cidr**.
- Сетевого интерфейса, с которого будут отправлять обновления маршрутной информации: **network-interface**.

Следующая команда используется для отображения конфигурации RIP в виртуальном маршрутизаторе:

Admin@UGOS# show network virtual-router <virtual-router-name> rip

Настройка мультикаст-маршрутизации

Настройка мультикаст маршрутизации в виртуальном маршрутизаторе производится с использованием следующей команды:

Admin@UGOS# show network virtual-router <virtual-router-name> multicast-router

Далее указываются параметры:

Параметр	Описание
enabled	Включение/отключение мультикаст-маршрутизации: • **on**. • **off**.
use-ecmp	Разрешение распределения трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP): • **on**. • **off**. Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если данная опция отключена, то весь трафик на определенный хост назначения будет пересылаться только через один из роутеров (next hop).
use-ecmp-rebalance	Использование ECMP rebalance: • **on** — если один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). • **off** — если один из интерфейсов, через который отсылался трафик, отключился, то перераспределяются только те потоки, которые передавались через отключенный интерфейс.
join-prune	Интервал отправки сообщений соседям PIM о мультикаст-группах, трафик которых маршрутизатор хочет принимать или более не хочет принимать.
register-suppress	Интервал, после которого маршрутизатор отсылает сообщение register suppress.

Параметр	Описание
keep-alive	Интервал, через который маршрутизатор будет посылать сообщения keepalive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.
interfaces	Интерфейс, который будет использоваться для работы мультикаста; для указания доступны только интерфейсы, добавленные в виртуальный маршрутизатор. Для добавления интерфейсов или изменения данных о ранее добавленных интерфейсах используются следующие команды: Admin@UGOS# set network virtual-router <virtual-router-name> multicast-router interfaces new Admin@UGOS# set network virtual-router <virtual-router-name> multicast-router interfaces <interface-name> Далее необходимо указать параметры: • **interface** — выбор интерфейса для работы мультикаст. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор. • **hello-timeout** — интервал отправки PIM HELLO сообщений в секундах. PIM Hello сообщения отправляются периодически со всех интерфейсов, для которых включена поддержка мультикастинга. Эти сообщения позволяют узнать маршрутизатору о соседних маршрутизаторах, поддерживающих мультикастинг. • **dr-priority** — приоритет при выборе Designated router (DR), с помощью которого администратор может управлять процессом выбора DR для локальной сети. • **enable-igmp** — приём сообщений IGMP report и IGMP query на данном интерфейсе. • **use-igmpv2** — использование версии IGMP v2, по умолчанию используется IGMP v3.
rendevouz-points	При настройке Rendevouz points можно указать следующие параметры: • **enabled** — включение/отключение данного RP: ◦ **on**. ◦ **off**. • **name** — название RP. • **ip** — Unicast IP-адрес RP. • **asm-allowed-groups** — список разрешенных групповых адресов для any source multicast с данного RP. Любые сети из диапазона 224.0.0.0/4. Если ничего не задано, то ограничений нет.
ssm-allowed-groups	Настройка мультикаст роутера, определяющая список разрешенных групповых адресов для source specific multicast. Могут быть указаны любые сети из диапазона 232.0.0.0/8; если ничего не задано, то ограничений нет.
spt-exclusions	Настройка мультикаст роутера, задающая список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree.

Следующая команда предназначена для удаления параметров мультикаст-маршрутизатора:

Admin@UGOS# delete network virtual-router <virtual-router-name> multicast-router

Для удаления доступны следующие параметры:

- Интерфейсы, использующиеся для работы мультикаста: **interfaces**.
- Rendevouz points: **rendevouz-points <rp-name>**, а также список разрешенных групповых адресов для any source multicast с данного RP: **rendevouz-points <rp-name> asm-allowed groups**.
- Список разрешенных групповых адресов для source specific multicast: **ssm-allowed-groups**.
- Список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree: **spt-exclusions**.

Для отображения конфигурации мультикастинга в виртуальном маршрутизаторе используйте следующую команду:

Admin@UGOS# show network virtual-router <virtual-router-name> multicast-router

Настройка WCCP

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Настройка WCCP производится на уровне **network wccp**. Для создания сервисной группы WCCP используется следующая команда:

Admin@UGOS# create network wccp

Доступны параметры:

Параметр	Описание
enabled	Включение/отключение сервисной группы: • **on**. • **off**.
name	Название сервисной группы WCCP.
description	Описание сервисной группы.
password	Пароль, необходимый для аутентификации NGFW в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
fwd-type	Способ перенаправления трафика с серверов WCCP на NGFW: • **l2** — используя перенаправление L2.В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес NGFW. • **gre** — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
ret-type	Способ перенаправления трафика с NGFW на серверы WCCP: • **l2** — используя перенаправление L2. В этом случае NGFW (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер). • **gre** — используя туннель GRE (Generic Routing Encapsulation). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
service-group	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
priority	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
ports-to-redirect	Порты для перенаправления (порты назначения трафика). При необходимости указываются несколько портов в формате: **ports-to-redirect + [80 442]** . **Важно!** NGFW может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на NGFW с другими портами, будет отправляться в интернет без фильтрации.
ports-source	Перенаправление трафика на основании значений портов источника: • **on**. • **off**.
protocol	Выбор протокола: • **tcp** — Transmission Control Protocol (TCP). • **udp** — User Datagram Protocol (UDP).
routers-lists	Список IP-адресов серверов WCCP. Подробнее о создании списков IP-адресов с помощью CLI читайте в разделе Настройка IP-адресов.
routers-ips	IP-адреса серверов WCCP.

Параметр	Описание
assignment-type	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. • **wccp-hash** — распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета: ◦ **source-ip** — вычисление хэша по IP-адресу источника. ◦ **source-port** — вычисление хэша по порту источника. ◦ **dest-ip** — вычисление хэша по IP-адресу назначения. ◦ **dest-port** — вычисление хэша по порту назначения. ◦ **alt-source-ip** — вычисление альтернативного хэша по IP-адресу источника. ◦ **alt-source-port**- вычисление альтернативного хэша по порту источника. ◦ **alt-dest-ip** — вычисление альтернативного хэша по IP-адресу назначения. ◦ **alt-dest-port** — вычисление альтернативного хэша по порту назначения. • **wccp-mask** — распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP. ◦ **source-ip** — схема маскирования по IP-адресу источника. ◦ **source-port** — схема маскирования по порту источника. ◦ **dest-ip** — схема маскирования по IP-адресу назначения. ◦ **dest-port** — схема маскирования по порту назначения. ◦ **mask-value** — значение маски схемы маскирования. Для схемы маскирования по порту — 16 бит; по IP-адресу — 32 бита; указываются в шестнадцатеричном формате.

Для задания значений сервисной группы WCCP или обновления информации о ней:

Admin@UGOS# set network wccp <service-group-name>

Далее указываются параметры, значения которых необходимо обновить; параметры представлены в таблице выше.

С использованием следующей команды доступно удаление сервисной группы полностью или некоторых её параметров:

Admin@UGOS# delete network wccp <service-group-name>

Параметры, доступные для удаления:

- **routers-lists**.
- **routers-ips**.
- **ports-to-redirect**.

Следующая команда предназначена для просмотра информации о сервисной группе WCCP:

Admin@UGOS# show network wccp <service-group-name>

Настройка правил с использованием UPL

Настройка правил с использованием UPL (Описание)

Documentation: ☑
Product: NGFW
Version: 7.0.1

UPL — UserGate Policy Language — язык описания политик (конфигурации правил, применяемых для принятия решений по требованиям аутентификации, правам доступа или преобразования контента) UserGate.

Правила настраиваются с использованием действий, условий и свойств.

Для каждого правила настраивается одно из действий. Действия — настройки, которые управляют обработкой транзакции (**OK**, **WARNING**, **PASS**, **DENY**). При настройке правил, в которых не предусмотрено указание действия (например, правила DNS, NAT и маршрутизации, пропускной способности и т.п.), необходимо указать действия **PASS** или **OK**.

Условия задаются знаками равно (=) или не равно (!=), например, зоны, адреса, GeoIP источников и назначения, сервисы, приложения и т.д.; все условия в правиле проверяются по логическому И, т.е. правило сработает, если будут выполнены все условия.

Свойства правил задаются в круглых скобках и используются для указания дополнительной информации, например, название правил, их описание, функция журналирования и т.д.

ПримечаниеПри настройке правил сначала указывается действие, потом условия и затем свойства.

UPL используется для настройки правил в следующих разделах:

- Настройки DNS-прокси (уровень: **network dns dns-proxy dns-rules**).
- Captive-портал (уровень: **users captive-portal**).
- Межсетевой экрана (уровень: **network-policy firewall**).
- NAT и маршрутизация (уровень: **network-policy nat-routing**).
- Пропускная способность (уровень: **network-policy traffic-shaping**).
- Фильтрация контента (уровень: **security-policy content-filtering**).
- Веб-безопасность (уровень: **security-policy web-browsing**).
- Инспектирование туннелей (уровень: **security-policy tunnel-inspection**).
- Инспектирование SSL (уровень: **security-policy ssl-inspection**).
- Инспектирование SSH (уровень: **security-policy ssh-inspection**).
- СОВ (уровень: **security-policy intrusion-prevention**).
- Защита почтового трафика (уровень: **security-policy mail-security**).
- ICAP-правила (уровень: **security-policy icap-rules**).
- Правила защиты DoS (уровень: **security-policy dos-rules**).
- Веб-портал (уровень: **global-portal web-portal**).
- Правила reverse-прокси (уровень: **global-portal reverse-proxy-rules**).
- Серверные правила (уровень: **vpn server-rules**).
- Клиентские правила (уровень: **vpn client-rules**).

Структура команды для создания правила:

Admin@UGOS# create <level> <position> upl-rule <str-upl-syntax>

где <level> — уровень, на котором необходимо создать правило.

<position> — позиция, на которую будет помещено правило.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для обновления существующего правила:

Admin@UGOS# set <level> <position> upl-rule <str-upl-syntax>

где <level> — уровень, на котором необходимо обновить правило.

<position> — номер правила, которое необходимо обновить.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для удаления правила:

Admin@UGOS# delete <level> <position | all>

где <level> — уровень, на котором необходимо удалить правило.

<position> — номер правила, которое необходимо удалить.

<all> — удалить все правила.

Структура команды для отображения правила:

Admin@UGOS# show <level> <position | all>

где <level> — раздел, правила которого нужно отобразить.

<position> — номер правила, которое необходимо отобразить.

<all> — отобразить все правила.

В качестве примера рассмотрим создание правила межсетевого экрана (использован многострочный ввод):

```
Admin@UGOS# create network-policy firewall 1 upl-rule \
...DENY \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = known \
...service = HTTPS \
...time = lib.time("Working hours") \
...rule_log(session)\
...name("Example of firewall rule created in CLI") \
...enabled(true)
```

После создания правило отобразиться в начале списка правил межсетевого экрана (на позиции 1). Данное правило запрещает HTTPS-трафик из зоны Trusted в зону Untrusted пользователям, идентифицированным системой; правило работает в соответствии с расписанием Working hours. При срабатывании правила в журнал будет записана информация о начале сессии.

Настройка раздела Пользователи и устройства

Настройка групп пользователей

Documentation:
Version: 7.0.1
Product: UserGate NGFW

Настройка групп пользователей производится на уровне **users group**.

Для добавления новой группы пользователей используется команда:

Admin@UGOS# create users group

Возможно указать следующие параметры:

Параметр	Описание
name	Название группы пользователей.
description	Описание группы пользователей.
transient	Указать: • **on** — группа для гостевых пользователей. • **off** — не является группой для гостевых пользователей.
users	Добавление пользователей в группу.
ldap-users	Добавление пользователей LDAP. При добавлении пользователей LDAP необходимо указать LDAP-коннектор (**ldap-users connector <ldap-server-name> users + [<domain\user1> domain\user2> ...]**).

Для обновления информации о группе пользователей необходимо воспользоваться следующей командой (параметры, доступные для обновления, аналогичны с параметрами, доступными при создании группы):

Admin@UGOS# set users group <group-name>

С использованием следующих команд можно удалить группу пользователей или отдельных пользователей группы:

Admin@UGOS# delete users group <group-name>

Для удаления локальных пользователей:

Admin@UGOS# delete users group <group-name> users [<user1> <user2> ...]

Для удаления пользователей LDAP:

Admin@UGOS# delete users group <group-name> ldap-users connector <ldap-server-name> users [<domain\user1> <domain\user2> ...]

Для отображения настроек группы используется следующая команда:

Admin@UGOS# show users group <group-name>

Настройки пользователей

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Настройка пользователей производится на уровне **users user**.

Команда для добавления пользователей:

Admin@UGOS# create users user

Доступно указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение пользователя.
name	Имя пользователя.
login	Логин пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
password	Пароль пользователя — для идентификации по имени и паролю. В этом случае потребуется настроить Captive-портал, где пользователь сможет ввести данное имя и пароль для авторизации.
expiration-date	Срок действия учётной записи пользователя. Указывается в формате YYYY-MM-DD.
groups	Группы, в которые будет добавлен пользователь.
static-addresses	Указываются: • **ip**: IP-адреса для идентификации пользователя; пользователь всегда должен получать доступ в сеть с указанных адресов. • **mac**: MAC-адреса для идентификации пользователей; пользователь всегда должен получать доступ в сеть с указанных адресов. • **ip-range**: диапазон IP-адресов для идентификации пользователя; пользователь всегда должен получать доступ в сеть с адреса из указанного диапазона. Диапазон задаётся в формате: <IP_start-IP_end>. • **ip-mac**: идентификация пользователя с помощью комбинации MAC и IP-адресов; пользователь всегда должен получать доступ в сеть с указанных адресов. Указывается в формате <ip-mac>.
emails	Почтовые адреса пользователя.
phones	Номера телефонов пользователя.

Для обновления параметров учётной записи пользователя:

Admin@UGOS# set users user <user-name>

Список доступных параметров аналогичен списку параметров, доступному при создании учётной записи пользователя.

Для удаления учётной записи пользователя используется следующая команда:

Admin@UGOS# delete users user <user-login>

Также имеется возможность удаления определённой информации из учётной записи. Для удаления доступны (при удалении требуется ввод значения параметра):

- **groups**.
- **static-addresses**.
- **emails**.
- **phones**.

Команда для просмотра учётной записи пользователя:

Admin@UGOS# show users user <user-name>

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Раздел Серверы аутентификации позволяет произвести настройку LDAP-коннектора, серверов RADIUS, TACACS+, NTLM, SAML IDP. Настройка серверов аутентификации производится на уровне **users auth-servers** и будет рассмотрена далее в соответствующих разделах.

Для сброса авторизации пользователя по IP-адресу используется команда:

Admin@UGOS# set settings usersession terminate <ip>

Настройка LDAP-коннектора

Настройка LDAP-коннектора производится на уровне **users auth-servers ldap**.

Для создания LDAP-коннектора используется команда:

Admin@UGOS# create users auth-servers ldap

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя LDAP-коннектора.
enabled	Включение/отключение сервера аутентификации.
description	Описание LDAP-коннектора.
ssl	Определяет: • **on** — использование SSL-соединения для подключения к LDAP-серверу. • **off** — подключение к LDAP-серверу без использования SSL-соединения.
address	IP-адрес контроллера или название домена LDAP.
bind-dn	Имя пользователя, которое будет использоваться для подключения к серверу; указывается в формате DOMAIN\username или username @domain. Пользователь должен быть заведён в домене.
password	Пароль пользователя для подключения к домену.
domains	Список доменов, которые обслуживаются указанным контроллером домена.
search-roots	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. Если пути поиска не указаны, то поиск производится по всему каталогу, начиная от корня.

Команда для обновления информации о существующем LDAP-коннекторе имеет следующую структуру:

Admin@UGOS# set users auth-servers ldap <ldap-server-name>

Параметры, доступные для обновления, аналогичны параметрам создания LDAP-коннектора.

Для удаления LDAP-коннектора используется команда:

Admin@UGOS# delete users auth-servers ldap <ldap-server-name>

Также возможно удаления отдельных параметров LDAP-коннектора. Для удаления доступны следующие параметры:

- **domains**.
- **search-roots**.

Структура команды для отображения информации о LDAP-коннекторе:

Admin@UGOS# show users auth-servers ldap <ldap-server-name>

Настройка RADIUS-сервера

Настройка RADIUS-сервера производится на уровне **users auth-servers radius**.

Для создания сервера аутентификации RADIUS используется команда со следующей структурой:

Admin@UGOS# create users auth-servers radius

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя RADIUS-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом RADIUS для аутентификации.
addresses	IP-адрес и UDP-порт, на котором сервер RADIUS слушает запросы (по умолчанию порт 1812); указывается в формате <ip:port>.

Следующая команда используется для обновления информации о сервере RADIUS:

Admin@UGOS# set users auth-servers radius <radius-server-name>

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Для удаления сервера:

Admin@UGOS# delete users auth-servers radius <radius-server-name>

Также возможно удаления отдельных параметров RADIUS-сервера. Для удаления доступны следующие параметры:

- **addresses**.

Структура команды для отображения информации о RADIUS-сервере:

Admin@UGOS# show users auth-servers radius <radius-server-name>

Настройка сервера TACACS+

Настройка сервера TACACS+ производится на уровне **users auth-servers tacacs**.

Для создания сервера аутентификаци TACACS+ используется команда со следующей структурой:

Admin@UGOS# create users auth-servers tacacs

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя сервера TACACS+.
enabled	Включение/отключение сервера.
description	Описание сервера аутентификации.
secret	Общий ключ, используемый протоколом TACACS+ для аутентификации.
address	IP-адрес сервера TACACS+.
port	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию. По умолчанию это порт UDP 1812.
single-connection	Использовать одно TCP-соединение для работы с сервером TACACS+.
timeout	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Следующая команда используется для обновления информации о сервере TACACS+:

Admin@UGOS# set users auth-servers tacacs <tacacs-server-name>

Параметры, которые могут быть обновлены, соответствуют параметрам, указание которых возможно при создании сервера аутентификации.

Для удаления сервера:

Admin@UGOS# delete users auth-servers tacacs <tacacs-server-name>

Структура команды для отображения информации о сервере TACACS+:

Admin@UGOS# show users auth-servers tacacs <tacacs-server-name>

Настройка сервера NTLM

Настройка сервера NTLM производится на уровне **users auth-servers ntlm**.

Для создания сервера аутентификации NTLM используется команда со следующей структурой:

Admin@UGOS# create users auth-servers ntlm

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Имя NTLM-сервера.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
win-domain	Имя домена Windows.

Следующая команда используется для обновления информации о NTLM-сервере:

Admin@UGOS# set users auth-servers ntlm <ntlm-server-name>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Для удаления сервера:

Admin@UGOS# delete users auth-servers ntlm <ntlm-server-name>

Структура команды для отображения информации о сервере NTLM:

Admin@UGOS# show users auth-servers ntlm <ntlm-server-name>

Настройка сервера SAML IDP

Настройка сервера SAML IDP производится на уровне **users auth-servers saml-idp**.

Для создания сервера аутентификации SAML IDP используется следующая команда:

Admin@UGOS# create users auth-servers saml-idp

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название сервера SAML IDP.
enabled	Включение/отключение сервера аутентификации.
description	Описание сервера аутентификации.
metadata-url	URL на сервере SAML IDP, где можно скачать xml-файл с корректной конфигурацией для сервис-провайдера (клиента) SAML.
certificate	Сертификат, который будет использован в SAML-клиенте.
sso-url	URL, используемая в сервере SAML IDP в качестве единой точки входа. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
sso-binding	Метод, используемый для работы с единой точкой входа SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-url	URL, используемый в сервере SAML IDP в качестве единой точки выхода. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.
slo-binding	Метод, используемый для работы с единой точкой выхода SSO. Возможны варианты POST и Redirect. Смотрите документацию на используемый у вас сервер SAML IDP для более детальной информации.

Следующая команда используется для обновления информации о сервере SAML IDP:

Admin@UGOS# set users auth-servers saml-idp <saml-idp-server-name>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды создания сервера аутентификации.

Для удаления сервера:

Admin@UGOS# delete users auth-servers saml-idp <saml-idp-server-name>

Структура команды для отображения информации о сервере SAML IDP:

Admin@UGOS# show users auth-servers saml-idp <saml-idp-server-name>

Настройка профилей аутентификации

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Настройка профилей аутентификации производится на уровне **users auth-profile**.

Для создания профиля аутентификации используется следующая команда:

Admin@UGOS# create users auth-profile

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
mfa	Указание профиля мультифакторной аутентификации (если её необходимо использовать). Для указания профиль MFA должен быть создан заранее. Подробнее о создании профилей MFA с использованием интерфейса командной строки читайте в разделе Настройка профилей MFA (мультифакторной аутентификации).
idle-time	Время бездействия до отключения; указывается в секундах. Через указанный промежуток времени при отсутствии активности пользователь перейдёт в статус Unknown user.
expiration-time	Время жизни авторизованного пользователя; указывается в секундах. Через указанный промежуток времени пользователь перейдёт в статус Unknown user; необходима повторная авторизация пользователя на Captive-портале.
max-attempts	Число неудачных попыток авторизации через Captive-портал до блокировки учётной записи пользователя.
lockout-time	Время, на которое блокируется учетная запись пользователя при достижении указанного числа неудачных попыток авторизации; указывается в секундах.
auth-method	Метод аутентификации: • **local-user-auth**: аутентификация по базе данных локально заведенных пользователей. • **policy-accept**: не требуется аутентификация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети; применяется совместно с профилем Captive-портала, в котором используется страница авторизации Captive portal policy. • **http-basic**: аутентификация с помощью метода HTTP Basic. • **ldap**: аутентификация с использованием LDAP-коннектора. • **radius**: аутентификация с использованием RADIUS-сервера. • **tacacs**: аутентификация с использованием сервера TACACS+. • **ntlm**: аутентификация с использованием NTLM-сервера. • **saml-idp**: аутентификация с использованием сервера SAML IDP.

Следующая команда предназначена для обновления настроек профилей аутентификации:

Admin@UGOS# set users auth-profile <auth-profile-name>

Для обновления доступен список параметров, аналогичный списку параметров команды **create**.

Через интерфейс командной строки возможно удаления всего профиля или отдельных способов аутентификации, заданных в профиле. Для этого используются следующие команды.

Для удаления профиля аутентификации:

Admin@UGOS# delete users auth-profile <auth-profile-name>

Для удаления методов аутентификации, заданных в профиле, необходимо указать метод аутентификации (доступные методы авторизации перечислены в таблице выше):

Admin@UGOS# delete users auth-profile <auth-profile-name> auth-method

Captive-портал

Product: UserGate NGFW
Version: 7.0.1
Documentation:

В данном разделе описана настройка правил Captive-портала; настройка производится на уровне **users captive-portal**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Параметры правил captive-портала:

Параметр	Описание
OK **PASS**	Действия правила Captive-портала: • **OK** — использовать аутентификацию. • **PASS** — не использовать аутентификацию.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила captive-портала. Например: **name("Captive rule example")**.
desc	Описание правила captive-портала. Чтобы задать описание правила: **desc("Captive portal rule example set via CLI")**.
profile	Captive-профиль указывается при использовании аутентификации на captive-портале. Например, **profile("Example Captive profile")**. Подробнее о создании и настройке captive-профилей читайте в разделе Настройка Captive-профилей.
rule_log	Включение/отключение записи срабатывания в журнал правил: • **rule_log(yes)** или **rule_log(true)**. • **rule_log(no)** или **rule_log(false)**. Если параметр не указан, то функция журналирования отключена.
src.zone	Зона источника. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: **category** = **lib.category()**; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: **category** = **"URL category name"**.
url	Списки URL, для которых будет применяться правило. Для указания списка URL: **url = lib.url()**; в скобках необходимо указать название списка URL.

Параметр	Описание
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка Captive-профилей

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Настройка Captive-профилей производится на уровне **users captive-profiles**.

Для создания Captive-профиля необходимо использовать следующую команду:

Admin@UGOS# create users captive-profiles

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название captive-профиля.
description	Описание captive-профиля.
auth-template	Шаблон страницы авторизации.
auth-mode	Метод идентификации, с помощью которого UserGate запомнит пользователя: • **ip** — Запоминать IP-адрес. После успешной авторизации пользователя через Captive-портал UserGate запоминает IP-адрес пользователя, и все последующие соединения с этого IP-адреса будут относятся к данному пользователю; устанавливается по умолчанию. • **cookie** — Запоминать cookie. После успешной авторизации пользователя через Captive-портал UserGate добавляет в браузер пользователя cookie, с помощью которого идентифицирует последующие соединения данного пользователя.
auth-profile	Профиль аутентификации, определяющий методы аутентификации. Подробнее о настройке профилей авторизации с использованием CLI смотрите в разделе Настройка профилей аутентификации.
custom-redirect	URL, куда будет перенаправлен пользователь после успешной авторизации с помощью Captive-портала. Если не заполнено, то пользователь переходит на запрошенный им URL.
use-cookie	Возможность сохранения авторизации в браузере на указанное время. Для сохранения информации используются cookie. • **on**. • **off**.
cookie-exptime	Время, на которое будет сохранена авторизация; задаётся в часах.
enable-ldap	Возможность выбора домена AD/LDAP на странице авторизации: • **on**. • **off**.
use-captcha	Использование CAPTCHA: пользователю будет предложено ввести код, который ему будет показан на странице авторизации Captive-портала: • **on**. • **off**.
use-https	Использование HTTPS при отображении страницы авторизации Captive-портала. Необходимо иметь корректно настроенный сертификат для SSL Captive-портала. • **on**. • **off**.
notification-profile	Профиль оповещения, который будет использоваться для отсылки гостевым пользователям информации о созданном пользователе и его пароле. Подробнее о настройке профилей оповещений с использованием CLI смотрите в разделе Настройка профилей оповещений.
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальные переменные {login} и {password}, которые будут заменены на имя пользователя и его пароль. Текст оповещения обособляется кавычками ("").
exp-time	Дата и время, когда учетная запись временного пользователя будет отключена. Указывается в формате: yyyy-mm-ddThh:mm:ssZ.
session-ttl	Продолжительность времени с момента первой авторизации временного пользователя, по истечении которого его учетная запись будет отключена; задаётся в часах.
password-len	Длина пароля 1 — 15 символов.
password-complexity	Сложность пароля: • **num**: использование только цифр. • **alpha_num**: использование букв и цифр. • **alpha_num_special**: использование букв, цифр и специальных символов.
ta-groups	Группа для временных пользователей, в которую будут помещены создаваемые пользователи.

Для обновления профиля необходимо использовать следующую команду:

Admin@UGOS# set users captive-profiles <captive-profile-name>

При обновлении настроек captive-профиля доступны параметры, аналогичные параметрам, доступным при создании профиля.

Для удаления профиля используется команда:

Admin@UGOS# delete users captive-profiles <captive-profile-name>

Также, с использованием следующей команды, доступно удаление групп для временных пользователей (всегда должна быть указана хотя бы одна группа для временных пользователей):

Admin@UGOS# delete users captive-profiles <captive-profile-name> ta-groups

Команда для отображения настроек captive-профиля:

Admin@UGOS# show users captive-profiles <captive-profile-name>

Настройка терминальных серверов

Version: 7.0.1
Product: UserGate NGFW
Documentation:

В данном разделе описана настройка терминальных серверов с использованием интерфейса командной строки. Настройка производится на уровне **users terminal-servers**.

Для создания терминального сервера необходимо ввести следующую команду:

Admin@UGOS# create users terminal-servers

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	Включение/отключение терминального сервера: • **on**. • **off**.
name	Название терминального сервера.
description	Описание терминального сервера.
host	IP-адрес хоста. Для добавления нескольких адресов укажите их через пробел.

Следующая команда предназначена для обновления параметров (параметры приведены выше в таблице) терминального сервера:

Admin@UGOS# set users terminal-servers <terminal-server-name>

Команда удаления терминального сервера:

Admin@UGOS# delete users terminal-servers <terminal-server-name>

Также возможно удаление отдельных хостов. Для удаления необходимо уточнить их адреса:

Admin@UGOS# delete users terminal-servers <terminal-server-name> host

Для отображения информации о терминальном сервере необходимо использовать команду:

Admin@UGOS# show users terminal-servers <terminal-server-name>

Настройка профилей MFA (мультифакторной аутентификации)

Version: 7.0.1
Product: UserGate NGFW
Documentation: ☑

Данный раздел описывает настройку профилей мультифакторной аутентификации с использованием CLI. Настройка профилей MFA производится на уровне **users mfa-profiles**. Можно создать несколько типов профилей:

- **MFA через TOTP**: использование токена TOTP (Time-based One Time Password) в качестве второго фактора аутентификации.
- **MFA через email**: использование одноразового пароля, полученного по email, в качестве второго фактора аутентификации.
- **MFA через SMS**: использование одноразового пароля, полученного по SMS, в качестве второго фактора аутентификации.

Команда для удаления профиля мультифакторной аутентификации:

Admin@UGOS# delete users mfa-profiles <mfa-name>

Для отображения информации о всех профилях или об определённом профиле MFA используются следующие команды:

Admin@UGOS# show users mfa-profiles
Admin@UGOS# set users mfa-profilesz <mfa-name>

Настройка MFA через TOTP

В зависимости от выбранного способа получения первоначального кода для инициализации TOTP (на странице Captive-портала, по email, по SMS) будет доступен разный список параметров, которые необходимо указать. Получение возможно:

- по email:

  Admin@UGOS# create users mfa-profiles mfa-totp smtp

- по SMS:

  Admin@UGOS# create users mfa-profiles mfa-totp smpp

- отображение на странице Captive-портала после первой успешной авторизации:

  Admin@UGOS# create users mfa-profiles mfa-totp key-on-captiveportal

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
totp-qr-code	QR-код на странице Captive-портала или в электронном письме для облегчения настройки устройства или ПО TOTP клиента.
notification-sender	Отправитель сообщения. Указать имя (в случае использования SMPP-профиля) или email (в случае использования SMTP-профиля).
notification-subject	Тема оповещения при использовании оповещений по email.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").

Для обновления параметров используется следующая команда:

Admin@UGOS# set users mfa-profiles mfa-totp <mfa-totp-name>

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Настройка MFA через email

Команда для добавления нового профиля мультифакторной аутентификации через email:

Admin@UGOS# create users mfa-profiles mfa-email smtp <smtp-profile>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-sender	Email отправителя сообщения.
notification-subject	Тема оповещения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Для обновления параметров используется следующая команда:

Admin@UGOS# set users mfa-profiles mfa-email <mfa-email-profile>

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Настройка MFA через SMS

Команда для добавления нового профиля мультифакторной аутентификации через SMS:

Admin@UGOS# create users mfa-profiles mfa-sms smpp <smpp-profile>

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля MFA.
description	Описание профиля MFA.
notification-sender	Имя отправителя сообщения.
notification-body	Тело письма. В письме можно использовать специальную переменную {2fa_auth_code}, которая будут заменена на одноразовый пароль. Текст оповещения обособляется кавычками ("").
code-lifetime	Срок действия одноразового пароля; указывается в секундах.

Для обновления параметров используется следующая команда:

Admin@UGOS# set users mfa-profiles mfa-sms <mfa-sms-profile>

Параметры, доступные для обновления, совпадают с параметрами, доступными при создании профиля.

Настройка применения политик к пользователям

Version: 7.0.1
Product: NGFW
Documentation:

Для локальных пользователей UserGate политики применяются автоматически.

Если пользователи проходят аутентификацию через LDAP-коннектор, NTLM или Kerberos, то для применения политик к пользователям (в случаях добавления новой LDAP-группы или пользователя в группу, создания правила и применения его к группе LDAP) необходимо сбросить сессии всех пользователей и произвести очистку кэша LDAP-записей на UserGate.

С помощью интерфейса командной строки CLI можно сбросить сессии отдельных пользователей. Команда выполняется в режиме конфигурации (configure), для выполнения команды необходимо знать IP-адрес пользователя:

Admin@UGOS# execute terminate usersession <IP-address>

Для очистки кэша используется команда:

Admin@UGOS# execute cache ldap-clear

Настройка раздела Политики сети

Настройка правил межсетевого экрана

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Параметры правил межсетевого экрана:

Параметр	Описание
PASS **DENY**	Действие правила межсетевого экрана: • **PASS** — разрешить трафик. • **DENY** — запретить трафик.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила межсетевого экрана. Например: **name("Rule example")**.
desc	Описание правила. Например: **desc("Firewall rule example configured in CLI")**.
reject_with	Настройка доступна для правил с действием **Запретить**: • **reject_with(no)**. • **reject_with("host_unreach")** — посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. • **reject_with("tcp_rst")** — посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. **Важно!** При выборе действия **Посылать TCP reset** необходимо указание сервиса, использующего протокол TCP (подробнее о добавлении и настройке сервисов читайте в разделе ов). • **reject_with("tcp_reset-both")** — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: **scenario = "Example of a scenario"**. Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, **rule_log(yes, "3/h", 5)** — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. • **rule_log(session)** — журналировать начало сессии.
fragmented	Указание пакетов, к которым применяется правило межсетевого экрана: • **fragmented(yes)** или **fragmented(true)** — применить правило к только фрагментированным пакетам. • **fragmented(no)** или **fragmented(false)** — применить правило к только нефрагментированным пакетам. • **fragmented(all)** — применить правило ко всем пакетам. Если не указать **fragmented** при создании правила, то правило межсетевого экрана применяется ко всем пакетам.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
user	Пользователи и группы пользователей, для которых применяется правило межсетевого экрана (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
application	Список приложений, для которых применяется данное правило. Доступно указание: • всех групп приложений: **application = lib.category(All)**. • групп приложений: **application = lib.applicationgroup()**; в скобках необходимо указать название группы приложений. • категорий приложений: **application = lib.category()**; в скобках необходимо указать название категорий приложений.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка правил NAT и маршрутизации происходит на уровне **network-policy nat-routing**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Настройка правил типа NAT

При настройке правил типа NAT, необходимо указать следующие параметры:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила NAT. Например: **name("NAT rule example")**.
desc	Описание правила. Например: **desc("NAT rule example set via CLI")**.
nat	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в "", например **snat_target_ip ("1.1.1.1")**.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
dst.zone	Зона назначения трафика. Для указания зоны назначения трафика, например, Untrusted: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.

Настройка правил типа DNAT

При настройке правил типа **DNAT** необходимо указать следующие параметры.

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.

Параметр	Описание
name	Название правила DNAT. Например: **name("DNAT rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("DNAT rule example created via CLI")**.
dnat	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в "", например **snat_target_ip ("1.1.1.1")**.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Чтобы указать зону источника трафика, например Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
target_ip	Адрес назначения DNAT. Для указания адреса назначения: **target_ip("1.1.1.1")**.
target_snat	Изменение IP-адреса источника на адрес NGFW: • **target_snat(yes)** или **target_snat(true)**. • **target_snat(no)** или **target_snat(false)**.

Настройка правил типа Порт-форвардинг

При настройке правил типа **Порт-форвардинг** необходимо указать:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила Порт-форвардинга. Например: **name("Port forwarding rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("Port forwarding rule example created via CLI")**.

Параметр	Описание
port_mapping	Тип правила (указывается в свойствах правила).
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в "", например **snat_target_ip ("1.1.1.1")**.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
port_map	Переопределение портов публикуемых сервисов: Для переопределения необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новый порты назначения. Например, **port_map(tcp, 2000, 2100)**. **Важно!** Нельзя использовать следующие порты, поскольку они используются внутренними сервисами NGFW: 2200, 8001, 4369, 9000-9100.
target_ip	Адрес назначения DNAT. Для указания адреса назначения: **target_ip("1.1.1.1")**.
target_snat	Изменение IP-адреса источника на адрес NGFW: • **target_snat(yes)** или **target_snat(true)**. • **target_snat(no)** или **target_snat(false)**.

Настройка правил типа Policy-based routing

Для настройки правил типа **Policy-based routing** нужно указать:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила типа Policy-based routing. Например: **name("Policy-based routing rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("Policy-based routing rule example set via CLI")**.
route	Тип правила (указывается в свойствах правила).
gateway	Выбор одного из существующих шлюзов: **gateway("1.1.1.1")**. О добавлении шлюзов через CLI читайте в разделе Настройка шлюзов.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: **scenario = "Example of a scenario"**. Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.

Параметр	Описание
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.

Настройка правил типа Network mapping

При настройке правил типа Network mapping необходимо указать следующие параметры:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила типа Network mapping. Например: **name("Network mapping rule example")**.
desc	Описание правила. Чтобы указать описание правила используется: **desc("Network mapping rule example set via CLI")**.
netmap	Тип правила (указывается в свойствах правила).
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.

Параметр	Описание
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
target_ip	Параметр подмены сетей; адрес сети, на которую будет производится замена, например: **target_ip("1.1.1.0")**.
direction	Параметр подмены сетей. Направление: • **direction(input)** — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении **target_ip**. • **direction(output)** — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении **target_ip**.

Настройка балансировки нагрузки

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Настройка правил балансировки нагрузки происходит на уровне **network-policy load-balancing**. Настройка балансировщиков нагрузки TCP/UDP, ICAP и reverse-прокси рассмотрена далее.

Для отображения информации о всех балансировщиках используется команда:

Admin@UGOS# show network-policy load-balancing

Настройка балансировщика TCP/UDP

Настройка данного раздела производится на уровне **network-policy load-balancing tcp-udp**.

Структура команды создания балансировщика нагрузки TCP/UDP следующая:

Admin@UGOS# create network-policy load-balancing tcp-udp

Необходимо указание следующих параметров:

Параметр	Описание
name	Имя балансировщика.
enabled	Включение/отключение балансировщика.
description	Описание балансировщика.
virtual-ip	IP-адрес виртуального сервера.
port	Порт, для которого необходимо производить балансировку нагрузки.
protocol	Протокол — TCP или UDP, для которого необходимо производить балансировку нагрузки.
scheduler	Методы распределения нагрузки на реальные серверы: • **rr** — **round robin** — каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • **wrr** — **weighted round robin** — работает аналогично Round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. • **lc** — **least connections** — новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений. • **wlc — leighted least connections** — работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера.
real-servers	Реальные сервера, на которые будет перенаправляться трафик. Для сервера необходимо указать: • **ip** — IP-адрес сервера. • **port** — порт сервера, на который будут перенаправлять запросы пользователей. • **weight** — коэффициент, использующийся для неравномерного распределения нагрузки на реальные серверы. • **mode** — режим: ◦ **gate** — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ **masq** — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ **masq-snat** — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но NGFW подменяет IP-адрес источника на свой. **Важно!** Задавать реальные серверы лучше последними, т.к. после задания параметров реального сервера невозможно вернуться к заданию остальных параметров балансировщика.

Для обновления существующего балансировщика нагрузки используется следующая команда:

Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name>

Помимо параметров, доступных при создании балансировщика, доступно обновление следующих параметров:

Параметр	Описание
fallback	Настройка аварийного режима: • **enabled** — включение/отключение аварийного режима. • **ip** — IP-адрес сервера. • **port** — порт сервера, на который будут пересылаться запросы пользователей. • **mode** — режим: ◦ **gate** — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ **masq** — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ **masq-snat** — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но NGFW подменяет IP-адрес источника на свой.

Параметр	Описание
monitoring	Настройка мониторинга реальных серверов: • **kind** — тип проверки: ◦ **ping**: проверка доступности узла с использованием утилиты ping. ◦ **connect**: проверка работоспособности узла путём установления TCP-соединения на определённый порт. ◦ **negotiate**: проверка работоспособности узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. • **service** — необходимо указать (**HTTP** или **DNS**) при использовании проверки типа **negotiate**. • **request** — запрос необходимо указать при использовании проверки типа **negotiate**. • **response** — ожидаемый ответ; необходимо указать при использовании проверки типа **negotiate**. • **interval** — интервал времени, через который должна выполняться проверка. • **timeout** — интервал времени ожидания ответа на проверку. • **max-failures** — количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки.

Для удаления существующего балансировщика нагрузки используется следующая команда:

Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name>

Также можно удалить определённые реальные серверы, использующиеся в балансировщике (необходимо уточнить один или несколько параметров реального сервера):

Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name> real-servers

Команды для отображения информации о всех балансировщиках TCP/UDP:

Admin@UGOS# set network-policy load-balancing tcp-udp

Для отображения информации об определённом балансировщике TCP/UDP:

Admin@UGOS# set network-policy load-balancing tcp-udp <balancer-name>

Настройка балансировщика ICAP

Настройка данного раздела производится на уровне **network-policy load-balancing icap**.

Структура команды создания балансировщика нагрузки ICAP следующая:

Admin@UGOS# create network-policy load-balancing icap

Необходимо указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение балансировщика серверов ICAP: • **on**. • **off**.
name	Имя балансировщика.
description	Описание правила балансировки.
icap-server	Указание ICAP-профилей серверов, на которые будет распределяться нагрузка. Подробнее о создании и настройке ICAP-серверов с использованием CLI в разделе Настройка ICAP-серверов.

Команда для обновления параметров балансировщика нагрузки ICAP:

Admin@UGOS# create network-policy load-balancing icap <balancer-name>

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании балансировщика серверов ICAP.

Для удаления существующего балансировщика нагрузки используется следующая команда:

Admin@UGOS# set network-policy load-balancing icap <balancer-name>

Также можно удалить определённые реальные серверы, использующиеся в балансировщике (необходимо указать названия ICAP-серверов):

Admin@UGOS# set network-policy load-balancing icap <balancer-name> real-servers

Команды для отображения информации о всех балансировщиках ICAP:

Admin@UGOS# set network-policy load-balancing icap

Для отображения информации об определённом балансировщике серверов ICAP:

Admin@UGOS# set network-policy load-balancing icap <balancer-name>

Настройка балансировщика reverse-прокси

Настройка правил балансировки reverse-прокси производится на уровне **network-policy load-balancing reverse-proxy**.

Для создания правила балансировки reverse-прокси:

Admin@UGOS# create network-policy load-balancing reverse-proxy

Необходимо указание следующих параметров:

Параметр	Описание
enabled	Включение/отключение балансировщика серверов reverse-proxy: • **on**. • **off**.
name	Имя балансировщика.

Параметр	Описание
description	Описание правила балансировки.
reverse-proxy-servers	Выбор сервера reverse-прокси. Подробнее о создании и настройке серверов reverse-прокси с использованием CLI в разделе Настройка серверов reverse-прокси.

Команда для обновления параметров балансировщика нагрузки reverse-прокси:

Admin@UGOS# set network-policy load-balancing reverse-proxy <balancer-name>

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании балансировщика серверов reverse-прокси.

Для удаления существующего балансировщика нагрузки используется следующая команда:

Admin@UGOS# delete network-policy load-balancing reverse-proxy <balancer-name>

Также можно удалить определённые реальные серверы, использующиеся в балансировщике (необходимо указать названия серверов reverse-прокси):

Admin@UGOS# delete network-policy load-balancing reverse-proxy <balancer-name> real-servers

Команды для отображения информации о всех балансировщиках reverse-прокси:

Admin@UGOS# show network-policy load-balancing reverse-proxy

Для отображения информации об определённом балансировщике серверов reverse-прокси:

Admin@UGOS# show network-policy load-balancing reverse-proxy <balancer-name>

Настройка правил пропускной способности

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка правил пропускной способности производится на уровне **network-policy traffic-shaping**. О структуре команд подробнее читайте в разделе Настройка правил с использованием UPL.

При настройке правил пропускной способности необходимо указать следующее:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила пропускной способности. Например: **name("Traffic shaping rule example")**.
desc	Описание правила. Для задания описания правила: **desc("The example of traffic shaping rule configured in CLI")** .
bandwidth_pool	Полоса пропускания, например, **bandwidth_pool("1 Mbps")**. Подробнее о создании и настройке полос пропускания читайте в разделе Настройка полос пропускания.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: **scenario = "Example of a scenario"** . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, **rule_log(yes, "3/h", 5)** — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()** ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило пропускной способности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика. Для задания зоны назначения используется: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()** ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.

Параметр	Описание
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
application	Список приложений, для которых применяется данное правило. Доступно указание: • всех групп приложений: **application = lib.category(All)**. • групп приложений: **application = lib.applicationgroup()**; в скобках необходимо указать название группы приложений. • категорий приложений: **application = lib.category()**; в скобках необходимо указать название категорий приложений.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка раздела Политики безопасности

Настройка фильтрации контента

Product: UserGate NGFW
Version: 7.0.1
Documentation: ☑

Настройка правил контентной фильтрации производится на уровне **security-policy content-filtering**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Параметр	Описание
PASS **DENY** **WARNING**	Действие правила контентной фильтрации: • **PASS** — разрешить посещение веб-страницы. • **DENY** — блокировать веб-страницу. • **WARNING** — предупредить пользователя о том, что страница нежелательна для посещения. Пользователь сам решает, отказаться от посещения или посетить страницу. Запись о посещении страницы заносится в журнал.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила контентной фильтрации. Для указания названия правила: **name("Content filtering rule example")**.
desc	Описание правила. Например: **desc("Content filtering rule example set via CLI")** .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — включить журналирование.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: **scenario = "Example of a scenario"** . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.
virus_usergate	Проверка потоковым антивирусом UserGate. Настраивается для правил с действием **Запретить**; возможны значения: • **virus_usergate(yes)** или **virus_usergate(true)** — использовать проверку потоковым антивирусом UserGate. • **virus_usergate(no)** или **virus_usergate(false)** — не использовать проверку потоковым антивирусом UserGate.
Страница блокировки	Выбор страницы блокировки; если страница не указана, то используется шаблон страницы по умолчанию. Страница блокировки указывается с использованием круглых скобок после действия, например, DENY("Blockpage (RU)"). Подробнее о настройке страниц блокировки читайте в разделе Настройка шаблонов страниц. Можно использовать внешнюю страницу, задав внешний URL: **redirect(302, "http://www.example.com")**.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило контентной фильтрации (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика, например, **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: **category** = **lib.category()**; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: **category** = **"URL category name"**.
url	Списки URL, для которых будет применяться правило. Для указания списка URL: **url = lib.url()**; в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка типов контента: **response.header.Content-Type = lib.mime()**; в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента.
morphology	Список баз словарей морфологии, по которым будут проверяться веб-страницы. Для задания списка баз словарей морфологии: **morphology = lib.morphology()**; в скобках необходимо указать название списка морфологии. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе `Настройка морфологи`_и.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: **request.header.User-Agent = lib.useragent()**; в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров.
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: **http.method = GET**.
request.header.Referer	Список URL, в котором указаны рефереры для текущей страницы, или категория URL, к которой относится реферер. Чтобы указать список или категорию URL: **request.header.Referer = lib.url()** (в скобках необходимо указать название списка) или **request.header.Referer = "URL category"** Подробнее о настройке списков URL через CLI читайте в разделе Настройка списков URL; о категориях URL — Настройка категорий URL.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка веб-безопасности

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка веб-безопасности производится на уровне **security-policy safe-browsing**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Необходимо указать следующие данные:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила веб-безопасности. Например: **name("Safe browsing rule example")**.
desc	Описание правила, например, **desc("Safe browsing rule example set via CLI")** .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — включить журналирование
enable_adblock	Блокировка рекламы • **enable_adblock(yes)** или **enable_adblock(true)**. • **enable_adblock(no)** или **enable_adblock(false)**.
url_list_exclusions	Список сайтов, для которых блокировать рекламу не требуется: **url_list_exclusions("URL list name")**. О создании и настройке списков URL с использованием CLI читайте в разделе Настройка списков URL.
enable_injector	Инжектирование кода в веб страницы: • **enable_injector(yes)** или **enable_injector(true)**. • **enable_injector(no)** или **enable_injector(false)**.
custom_injector	Код инжектора.
safe_search	Использование функции безопасного поиска: • **safe_search(yes)** или **safe_search(true)**. • **safe_search(no)** или **safe_search(false)**.
search_history_logging	Журналирование поисковых запросов пользователей: • **search_history_logging(no)** или **search_history_logging(false)** — отключить журналирование поисковых запросов пользователей. Если при создании правила **search_history_logging** не указано, функция журналирования отключена. • **search_history_logging(yes)** или **search_history_logging(true)** — включить журналирование поисковых запросов пользователей.
cocial_sites_block	Блокировка приложений социальных сетей: • **cocial_sites_block(yes)** или **cocial_sites_block(true)**. • **cocial_sites_block(no)** или **cocial_sites_block(false)**.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted** . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()** ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1.

Параметр	Описание
user	Пользователи и группы пользователей, для которых применяется правило веб-безопасности (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка правил инспектирования туннелей

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка правил инспектирования туннелей производится на уровне **security-policy tunnel-inspection**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Необходимо задать следующие параметры:

Параметр	Описание
OK **PASS**	Действие правила инспектирования туннелей: • **OK** — Инспектировать. • **PASS** — Не расшифровывать
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила инспектирования туннелей. Например: **name("Tunnel inspection rule example")**.
desc	Описание правила. Например: **desc("Tunnel inspection rule example configured via CLI")** .
service	Тип туннеля: • **service = gre** : инспектирование туннелей GRE. • **service = gtpu** : инспектирование туннелей GTP-U. • **service = ipsec_null** : инспектирование нешифрованных IPsec-туннелей
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted** . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()** ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика, например, **dst.zone = "Tunnel inspection zone"** . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Настройка инспектирования SSL

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка правил инспектирования SSL производится на уровне **security-policy ssl-inspection**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Параметр	Описание
OK **PASS**	Действие правила инспектирования SSL: • **OK** — Расшифровать. • **PASS** — Не расшифровывать • **OK ... forward** — Расшифровать и переслать; **forward** указывается среди свойств правила. При настройке правила с действием Расшифровать и переслать необходимо указать профиль пересылки SSL. Подробнее о создании и настройке с использованием CLI профилей пересылки читайте в разделе Настройка профилей пересылки SSL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила инспектирования SSL. Для указания названия правила: **name("SSL inspection rule example")**.
desc	Описание правила. Например: **desc("SSL inspection rule example configured in CLI")**.
ssl_forward_profile	Профиль пересылки SSL; профиль необходимо указать при настройке правила инспектирования SSL с действием Расшифровать и переслать. Указывается в формате: **ssl_forward_profile("SSL forward profile example")**.
ssl_profile	Профиль SSL; указывается: **ssl_profile("Default SSL profile")**. Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — включить журналирование.
block_invalid_cert	Блокирование доступа к серверам, предоставляющим некорректный сертификат HTTPS, например, если сертификат отозван, выписан на другое доменное имя или недоверенным центром сертификации, срок действия сертификата истёк. Доступно в правилах с действием **Расшифровать**: • **block_invalid_cert(yes)** или **block_invalid_cert(true)** — включение блокировки. • **block_invalid_cert(no)** или **block_invalid_cert(false)** — отключение блокировки.
check_revoc_cert	Проверка сертификата сайта в списке отозванных сертификатов (CRL) и блокирование доступа, если он там найден. Доступно в правилах с действием **Расшифровать**: • **check_revoc_cert(yes)** или **check_revoc_cert(true)** — включение проверки сертификата. • **check_revoc_cert(no)** или **check_revoc_cert(false)** — отключение проверки сертификата.
block_expired_cert	Блокирование сертификатов с истёкшим сроком действия. Доступно в правилах с действием **Расшифровать**: • **block_expired_cert(yes)** или **block_expired_cert(true)** — включить блокировку сертификатов с истёкшим сроком действия. • **block_expired_cert(no)** или **block_expired_cert(false)** — отключить блокировку сертификатов с истёкшим сроком действия.
block_self_signed_cert	Блокирование самоподписанных сертификатов. Доступно в правилах с действием **Расшифровать**: • **block_self_signed_cert(yes)** или **block_self_signed_cert(true)** — включить блокировку самоподписанных сертификатов. • **block_self_signed_cert(no)** или **block_self_signed_cert(false)** — отключить блокировку самоподписанных сертификатов.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSL (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.

Параметр	Описание
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1.
service	Тип сервиса: **HTTPS**, **SMTPS** или **POP3S**. Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**.
category	Списки категорий и категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: **category** = **lib.category()**; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке списков категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: **category** = **"URL category name"**.
url	Списки доменных имён, для которых применяется правило инспектирования SSL. Доменные имена создаются как списки URL за исключением того, что для инспектирования HTTPS могут быть использованы только доменные имена типа www.example.com, а не http://www.example.com/home/. Для указания списка доменов: **url = lib.url()**; в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL с использованием командной строки читайте в разделе Настройка списков URL.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка инспектирования SSH

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка правил SSH-инспектирования производится на уровне **security-policy ssh-inspection**. О структуре команд читайте подробнее в разделе Настройка правил с использованием UPL.

Далее представлены параметры правил инспектирования SSH.

Параметр	Описание
OK **PASS**	Действие правила инспектирования SSH: • **OK** — Расшифровать. • **PASS** — Не расшифровывать
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила инспектирования SSH. Для указания названия правила: **name("SSH inspection rule example")**.
desc	Описание правила. Например: **desc("SSH inspection rule example configured in CLI")** .
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — включить журналирование.
block_ssh_shell	Блокирование удалённого запуска shell (интерпретатора командной строки, оболочки). Доступно в правилах с действием **Расшифровать**: • **block_ssh_shell(yes)** или **block_ssh_shell(true)** — включить блокировку. • **block_ssh_shell(no)** или **block_ssh_shell(false)** -отключить блокировку.
block_ssh_exec	Блокирование удалённого выполнения по SSH. Доступно в правилах с действием **Расшифровать**: • **block_ssh_exec(yes)** или **block_ssh_exec(true)** — включить блокировку. • **block_ssh_exec(no)** или **block_ssh_exec(false)** — отключить блокировку.
ssh_command	Команда linux, которую требуется передать, в формате ssh user@host 'command' Например: **ssh_command("ssh root@192.168.1.1 reboot")**. Редактирование команды SSH доступно в правилах с действием **Расшифровать**.
block_sftp	Блокирование соединения SFTP (Secure File Transfer Protocol). Доступно в правилах с действием **Расшифровать**: • **block_sftp(yes)** или **block_sftp(true)** — включить блокировку соединения. • **block_sftp(no)** или **block_sftp(false)** — отключить блокировку соединения.
user	Пользователи и группы пользователей, для которых применяется правило инспектирования SSH (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()** ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей.

Настройка СОВ

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка системы обнаружения и предотвращения вторжений производится на уровне **security-policy intrusion-prevention**.

Правила СОВ настраиваются на уровне **security-policy intrusion-prevention idps-rules**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Доступны параметры:

Параметр	Описание
PASS **WARNING** **DENY**	Действие правила СОВ: • **PASS** — не блокировать трафик. • **WARNING** — не блокировать трафик и записать информацию в журнал. • **DENY** — блокировать трафик и записать информацию в журнал.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила системы обнаружения и предотвращения вторжений. Например: **name("IDPS rule example")**.
desc	Описание правила. Например: **desc("Intrusion prevention rule example set via CLI")**.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов, MAC-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: **src.ip = 02:00:00:00:00:00**.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
dst.zone	Зона назначения трафика. Для указания зоны назначения трафика, например, Untrusted: **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов, MAC-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL. Для указания MAC-адресов назначения, например 02:00:00:00:00:00, используйте: **dst.ip = 02:00:00:00:00:00**.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
idps_profiles	Профиля СОВ, которые будут использованы в данном правиле: **idps_profiles("IDPS profile example")**. Профили СОВ задаются для правил с действиями **Сбросить** и **Журналировать**. Для разрешающих правил задать профиль СОВ невозможно; такая реализация позволяет настроить исключения для определённого типа трафика.
idps-_profiles_exclusions	Список профилей СОВ, сигнатуры которых будут исключены из сигнатур, указанных в профилях СОВ; могут быть использованы только в правилах с действием **Сбросить** или **Журналировать**: **idps_profiles_exclusions("Example of IDPS profile with exclusions")**. Данная возможность позволяет использовать централизованно создаваемые профили сигнатур, изменять содержимое которых администратор не может, но при этом исключить из этого профиля ряд сигнатур, которые избыточны или создают ложные срабатывания.

Только в CLI доступна настройка режима умного сканирования (сканирование только первых байт каждой сессии). Настройка режима производится на уровне **security-policy intrusion-prevention settings**. Для настройки используется команда:

Admin@UGOS# set security-policy intrusion-prevention settings

Доступны параметры:

Параметр	Описание
intelligent-mode	Включение/отключение режима умного сканирования: • **on**. • **off**.
intelligent-limit	Количество первых килобайт каждой сессии, которые будет сканировать система обнаружения и предотвращения вторжений; необходимо задать значение от 50 до 200 КБ.

Для просмотра состояния режима:

Admin@UGOS# show security-policy intrusion-prevention settings

По умолчанию режим умного сканирования включен; проверяются первые 200 КБ каждой сессии.

Настройка сценариев

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка сценариев происходит на уровне **security-policy scenarios** с использованием UPL (подробнее об UserGate Policy Language читайте в разделе Настройка правил с использованием UPL).

Для задания условий сценариев и их объединения используются определения (definitions). Каждому определению присваивается уникальное пользовательское имя, по которому к нему можно будет обратиться. Условия сценария могут быть написаны в одной строке или разбиты с помощью обратного слэша (как при использовании многострочного ввода).

Для создания/изменения условий сценариев используется функция **def scenario_cond**, которая в общем виде имеет следующую структуру:

```
def scenario_cond <scenario_condition_name>
scenario_conditions
end
```

Параметры, использующиеся для задания разных типов условий, будут рассмотрены в следующих разделах.

Далее, после указания условий, указываются общие свойства сценария, представленные в таблице ниже:

Наименование	Описание
OK	Действие для создания сценария.
scenario_cond	Пользовательское имя определения, содержащего список условий сценария: **scenario_cond = condition_example**.
enabled	Включить/отключить использование сценария: • **enabled(true)**; • **enabled(false)**.
name	Задать имя сценария: **name("Example scenario name")**.
desc	Задать описание сценария: **desc("Description for scenario created as an example")**.
trigger	Применение: • **trigger(one_user)** — при срабатывании сценария, правило, в котором используется сценарий, будет применено только к тому пользователю, для которого сработал сценарий; • **trigger(all_users)** — при срабатывании сценария, правило в котором используется сценарий, будет применено ко всем пользователям, указанным в свойствах правила.
duration	Задать период активности сценария; указывается в минутах.
operation_mode	Задать режим активации сценария: • **operation_mode(all)** — сценарий сработает, если выполнятся все условия; • **operation_mode(any)** — сценарий сработает, если выполнится хотя бы одно из условий.

ПримечаниеПри обновлении сценария необходимо указывать все условия: текущие условия сценария будут заменены на условия, указанные при изменении.

В качестве примера приведена настройка сценария с условием **Объём трафика**. Сценарий будет применён ко всем пользователям в течение минуты; ограничение объёма трафика: 1 ГБ/день:

```
Admin@UGOS# create security-policy scenarios 1 upl-rule \
... def scenario_cond scenario_cond_test
... traffic_limit(2GB) \
... period(day) \
... scond_type(traffic)
... end
... OK \
... scenario_cond = scenario_cond_test
... name(test) \
... trigger(all_users) \
... duration (1)
...
```

Для изменения, например, объёма трафика:

```
Admin@UGOS# set security-policy scenarios 3 upl-rule \
...def scenario_cond scenario_cond_test
...traffic_limit(2GB) \
...period(day) \
...scond_type(traffic)
...end
...OK \
...scenario_cond = scenario_cond_test
```

Условие типа Категория URL

Для создания/обновления условия типа **Категория URL** укажите:

Наименование	Описание
category	Категории или группы категорий сайтов: **category = (lib.category(URL_CATEGORY_GROUP), URL_CATEGORY_NAME)**.
scond_type	Тип условия: **scond_type(url_category)**.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): **count_interval()**.
max_event_count	Количество срабатываний: **max_event_count()**.

Условие типа Обнаружен вирус

При настройке условия типа **Обнаружен вирус** укажите следующее:

Наименование	Описание
scond_type	Тип условия: **scond_type(virus_detection)**.

Условие типа Приложение

Для создания/редактирования условия типа **Приложение** используются параметры, представленные в таблице ниже:

Наименование	Описание
application	Категории приложений или группы приложений: • **application = lib.applicationgroup(APP_GROUP)** или **application = lib.applicationgroup(all)**; • **application = lib.category(APPS_CATEGORY_NAME)**.
scond_type	Тип условия: **scond_type(app)**.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): **count_interval()**.
max_event_count	Количество срабатываний: **max_event_count()**.

Условие типа СОВ

Параметры условия типа **СОВ**:

Наименование	Описание
ips_tl	Уровень угрозы: • **ips_tl(very_low)** - очень низкий; • **ips_tl(low)** - низкий; • **ips_tl(medium)** - средний; • **ips_tl(high)** - высокий; • **ips_tl(very_high)** - очень высокий.
scond_type	Тип условия: **scond_type(ips)**.

Условие типа Типы контента

Параметры условием типа **Типы контента**:

Наименование	Описание
response.header.Content-Type	Тип контента: **response.header.Content-Type = lib.mime(MIME_CATEGORIES_LIST)**.
scond_type	Тип условия: **scond_type(mime_type)**.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): **count_interval()**.
max_event_count	Количество срабатываний: **max_event_count()**.

Условие типа Размер пакета

Для создания и настройки условия типа **Размер пакета** используются следующие параметры:

Наименование	Описание
packet_size	Размер пакета, при превышении которого выполняется условие; указывается следующим образом: • **packet_size(1)** - размер пакета 1 байт; • **packet_size(1KB)** - размер пакета 1 Кбайт; • **packet_size(1MB)** - размер пакета 1 Мбайт; • **packet_size(1GB)** - размер пакета 1 Гбайт.
scond_type	Тип условия: **scond_type(net_packet_size)**.

Условие типа Сессий с одного IP

При настройке условия типа **Сессий с одного IP** используются:

Наименование	Описание
scond_type	Тип условия: **scond_type(sessions_per_ip)**.
sessions_limit	Максимальное количество сессий, разрешённых с одного IP-адреса: **sessions_limit()**.

Условие типа Объём трафика

Чтобы задать или настроить условие типа **Объём трафика** используются следующие параметры:

Наименование	Описание
scond_type	Тип условия: **scond_type(traffic)**.
traffic_limit	Ограничение объёма трафика: • **traffic_limit(1)** - 1 байт трафика; • **traffic_limit(1KB)** - 1 Кбайт трафика; • **traffic_limit(1MB)** - 1 Мбайт трафика; • **traffic_limit(1GB)** - 1 Гбайт трафика.
period	Период времени: • **period(minute)** - минута; • **period(hour)** - час; • **period(day)** - день; • **period(week)** - неделя; • **period(month)** - месяц.

Условие типа Проверка состояния

Для настройки условия типа **Проверка состояния** предназначены параметры:

Наименование	Описание
scond_type	Тип условия: **scond_type(health_check)**.
health_check_method	Метод проверки: • **health_check_method(ping)** - ping; • **health_check_method(dns)** - DNS-запрос; • **health_check_method(get)** - HTTP-метод GET.
url.address	Адрес, на который будут выполняться ping и DNS-запрос: **url.address = "1.1.1.1"**.
url.domain	FQDN для проверки состояния путём выполнения DNS-запроса или URL для метода HTTP GET: **url.domain = "example.ru"**.
gateway	Название используемого шлюза: **gateway()**. **Важно!** Шлюз должен быть предварительно создан.
health_result	Результат выполнения проверки: • **health_result(positive)** - положительный; • **health_result(negative)** - отрицательный.
health_request_timeout	Тайм-аут подключения (в секундах): **health_request_timeout()**.
health_answer_timeout	Время ожидания ответа на запрос HTTP GET (в секундах): **health_answer_timeout()**.
health_type_request	Тип DNS-запроса: • **health_type_request(a)**. • **health_type_request(aaaa)**. • **health_type_request(cname)**. • **health_type_request(ns)**. • **health_type_request(ptr)**.
count_interval	Интервал времени, за которое должно произойти заданное число срабатываний (указывается в минутах): **count_interval()**.
max_event_count	Количество срабатываний: **max_event_count()**.

Настройка правил защиты почтового трафика

Product: UserGate NGFW
Version: 7.0.1
Documentation:

Правила защиты почтового трафика настраиваются на уровне **security-policy mail-security**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Необходимо указать:

Параметр	Описание
PASS **WARNING** **DENY("with error")** **DENY**	Действие правила защиты почтового трафика: • **PASS** — Пропустить — пропустить трафик без изменения. • **WARNING** — Маркировать — маркировать почтовые сообщения специальным тэгом в теме письма или дополнительном поле. • **DENY("with error")** — Блокировать с ошибкой — блокировать письмо и сообщать об ошибке доставки письма серверу SMTP (для SMTP(S)-трафика) или клиенту (для POP3(S)-трафика). • **DENY** — Блокировать без ошибки — блокировать письмо без уведомления о блокировке.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила защиты почтового трафика. Например: **name("Mail security rule example")**.
desc	Описание правила. Например: **desc("Mail security rule example configured in CLI")**.
antispam_usergate	Проверка почтового трафика антиспамом UserGate (задаётся для правил с действием **Маркировать**, **Блокировать с ошибкой** или **Блокировать без ошибки**): • **antispam_usergate(yes)** или **antispam_usergate(true)** — включить проверку. • **antispam_usergate(no)** или **antispam_usergate(false)** — отключить проверку.
dnsbl	Антиспам-проверка с помощью технологии DNSBL. Применима только к SMTP-трафику в правилах с действием **Маркировать**, **Блокировать с ошибкой** или **Блокировать без ошибки**: • **dnsbl(yes)** или **dnsbl(true)** — использовать антиспам-проверку. • **dnsbl(no)** или **dnsbl(false)** — отключить использование антиспам-проверки. При проверке почтового трафика с помощью DNSBL IP-адрес SMTP-сервера отправителя спама блокируется на этапе создания SMTP-соединения, что позволяет существенно разгрузить другие методы проверки почты на спам и вирусы.
mark_hdr	Заголовок. Поле куда помещать тег маркировки; задаётся для правил с действием **Маркировать**: **mark_hdr(Subject)**.
mark	Текст тега, который маркирует письмо; задаётся для правил с действием **Маркировать**, например, **mark("Text for marking emails")**.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты почтового трафика (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика, например, **dst.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Почтовый протокол (POP3 или SMTP), к которому будет применено данное правило. Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**.
envelope_from	Почтовый адрес отправителя письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: **envelope_from = "Sender email group"**. Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов.
envelop_to	Почтовый адрес адресата письма (только для протокола SMTP). Необходимо указать группу почтовых адресов в формате: **envelope_to = "Receiver email group"**. Подробнее о создании и настройке групп почтовых адресов читайте в разделе Настройка почтовых адресов.

Настройка правил ICAP

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Создание и настройка ICAP-правил производится на уровне **security-policy icap-rules**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Необходимо указать:

Параметр	Описание
PASS **OK**	Действие правила ICAP: • **PASS** — Пропустить — не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP. • **OK** — Переслать — переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера (стандартный режим работы большинства ICAP-серверов). • **OK ... ignore** — Переслать и игнорировать — переслать данные ICAP-сервер и игнорировать ответ от ICAP-сервера (вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика); **ignore** указывается среди свойств правила.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила ICAP. Для указания названия правила: **name("ICAP rule example")**.
desc	Описание правила. Например: **desc("ICAP rule example set via CLI")**.
profile	ICAP-серверы, куда UserGate будет пересылать запросы; указывается в формате: **profile("Example ICAP server")**. О настройке серверов ICAP через CLI читайте в разделе Настройка ICAP-серверов.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило ICAP (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
response.header.Content-Type	Списки типов контента, к которым будут применяться правила. Для задания списка: **response.header.Content-Type = lib.mime()**; в скобках необходимо указать название списка типов контента. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка типов контента.

Параметр	Описание
category	Список категорий или категории URL-фильтрации, для которых будет применяться правило. Для URL-фильтрации необходимо иметь соответствующую лицензию. Для указания списка категорий URL: **category** = **lib.category()**; в скобках необходимо указать название списка категорий URL. Подробнее о создании и настройке категорий URL с использованием интерфейса командной строки читайте в разделе Настройка категорий URL. Для указания категории URL: **category** = **"URL category name"**.
url	Списки URL, для которых будет применяться правило. Для указания списка URL: **url = lib.url()**; в скобках необходимо указать название списка URL. Подробнее о создании и настройке списков URL читайте в разделе Настройка списков URL.
http.method	Метод, используемый в HTTP-запросах. Чтобы указать HTTP метод, например, GET: **http.method = GET**.
service	Тип сервиса: **HTTP**, **SMTP** или **POP3**. Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**.

Настройка ICAP-серверов

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Настройка ICAP-серверов производится на уровне **security-policy icap-server**.

Структура команды для создания ICAP-сервера:

Admin@UGOS# create security-policy icap-server

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя ICAP-сервера.
description	Задать описание ICAP-сервера.
ip	Задать IP-адрес ICAP-сервера.
port	Задать TCP-порт ICAP-сервера; значение по умолчанию: 1344.
max-msg-size	Определить максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. По умолчанию: 0 (тело запроса не будет передаваться на ICAP-сервер).
check-icap	Задать период проверки доступности сервера ICAP.
bypass	Если эта опция включена, то UserGate не будет посылать данные на сервер ICAP в случаях, когда ICAP-сервер недоступен.
reqmod-service	Использовать режим Reqmod: • <text> — задать путь на сервере ICAP. • **off** — отключить использование режима Reqmod.
respmod-service	Использовать режим Respmod: • <text> — задать путь на сервере ICAP. • **off** — отключить использование режима Respmod.
user-header	Установить отсылку имени пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки имени пользователя на ICAP-сервер. • **off** — не отсылать имя пользователя на ICAP-сервер.
user-encode	Установить кодировку имени пользователя в Base64: • **on**. • **off**.
ip-header	Установить отсылку IP-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. • **off** — не отсылать IP-адрес пользователя на ICAP-сервер.
mac-header	Установить отсылку MAC-адреса пользователя на ICAP-сервер: • <text> — задать название заголовка, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. • **off** — не отсылать MAC-адрес пользователя на ICAP-сервер.

Структура команды для обновления существующего ICAP-сервера:

Admin@UGOS# set security-policy icap-server <server-name>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового ICAP-сервера.

Структура команды для удаления ICAP-сервера:

Admin@UGOS# delete security-policy icap-server <server-name>

Структура команды для отображения информации об ICAP-сервере:

Admin@UGOS# show security-policy icap-server <server-name>

Настройка правил защиты DoS

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка правил защиты DoS производится на уровне **security-policy dos-rules**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

Параметр	Описание
PASS **WARNING** **DENY**	Действие правила защиты DoS: • **PASS** — разрешить трафик; защита от DoS атак не применяется. • **WARNING** — применить профиль защиты от DoS атак. • **DENY** — безусловно блокировать трафик.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила защиты DoS. Например: **name("DoS rule example")**.
desc	Описание правила. Например: **desc("DoS rule example configured in CLI")** .
profile	Профиль защиты DoS. Выбор профиля доступен только для правил с действием **Защитить** (**WARNING**). Для указания профиля: **profile("DoS profile example")**. О создании и настройке профилей защиты читайте в разделе Настройка профилей DoS.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: **scenario = "Example of a scenario"** . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев.
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: • **rule_log(no)** или **rule_log(false)** — отключить журналирование. Если при создании правила **rule_log** не указано, функция журналирования отключена. • **rule_log(yes)** или **rule_log(true)** — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, **rule_log(yes, "3/h", 5)** — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. • **rule_log(session)** — журналировать начало сессии.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: **src.zone = Trusted** . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()** ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило защиты DoS (локальные или LDAP). Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: **src.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
dst.ip	Добавление списков IP-адресов или доменов назначения. Для указания списка IP-адресов: **dst.ip = lib.network()** ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()** ; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.

Параметр	Описание
dst.geoip	Указание GeoIP назначения; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: **service = "service name"**; для указания нескольких сервисов: **service = (service-name1, service-name2, ...)**. Чтобы указать группу сервисов: **service = lib.service()**; в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: **time = lib.time()**; в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Настройка профилей DoS

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Настройка профилей DoS производится на уровне **security-policy dos-profile**.

Структура команды для создания профиля DoS:

Admin@UGOS# create security-policy dos-profile

Доступно указание следующих параметров:

Параметр	Описание
name	Задать имя профиля.
description	Задать описание профиля.
aggregate	Установить суммирование количества пакетов, проходящих в секунду для всех IP адресов или подсчёт индивидуально для каждого IP-адреса.
dos-protection-syn	Настройка защиты от сетевого флуда для протокола TCP. • **enabled** — установить конфигурацию от сетевого флуда для выбранного протокола. • **alert-threshold** — задать порог уведомлений. • **drop-threshold** — задать порог отбрасывания пакетов.
dos-protection-udp	Настройка защиты от сетевого флуда для протокола UDP. • **enabled** — установить конфигурацию от сетевого флуда для выбранного протокола. • **alert-threshold** — задать порог уведомлений. • **drop-threshold** — задать порог отбрасывания пакетов.
dos-protection-icmp	Настройка защиты от сетевого флуда для протокола ICMP. • **enabled** — установить конфигурацию от сетевого флуда для выбранного протокола. • **alert-threshold** — задать порог уведомлений. • **drop-threshold** — задать порог отбрасывания пакетов.
max-sessions	Установить ограничение количества сессий: • <num> — задать число сессий. • **off** — отключить ограничение числа сессий.

Структура команды для обновления существующих профилей DoS:

Admin@UGOS# set security-policy dos-profile <profile-name>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды добавления нового профиля DoS.

Структура команды для удаления профиля:

Admin@UGOS# delete security-policy dos-profile <profile-name>

Структура команды для отображения информации о профиле DoS:

Admin@UGOS# show security-policy dos-profile <profile-name>

Настройка глобального портала

Настройка веб-портала

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка веб-портала производится на уровне **global-portal web-portal**. О структуре команд подробнее читайте в разделе Настройка правил с использованием UPL.

При настройке закладок веб-портала

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название закладки. Например: **name("Example of bookmark publishing")**.
desc	Описание закладки. Например: **desc("Example of bookmark publishing configured in CLI")**.
url	URL ресурса, который необходимо опубликовать через веб-портал. Необходимо указывать полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. URL указывается как **url = "http://www.example.com"**.
url.domain	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Для указания домена прямого доступа: **url.domain = "example.com"**.
rdp_check_session_alive	Разрыв сессии RDP по завершению авторизации на веб-портале: • **rdp_check_session_alive(yes)** или **rdp_check_session_alive(true)** — разрывать сессию. • **rdp_check_session_alive(no)** или **rdp_check_session_alive(false)** — не разрывать сессию.
ssl_profile	Профиль SSL для построения защищенного канала для отображения веб-портала; указывается: **ssl_profile("SSL profile example")**.
certificate	Сертификат, который будет использоваться для создания HTTPS-соединения. Чтобы задать сертификат: **certificate("Certificate example")**.
icon	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку. Можно указать: • **icon("Default icon name")** — использовать штатную иконку (в скобках указывается название штатной иконки). • **icon("Icon encoded with Base64")** — использовать свою иконку. Необходимо указать содержимое файла, кодированное с использованием Base64. • **icon("http://www.icon-url-example.com")** — указать URL для использования сторонней иконки.
additional_url	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Для указания: **additional_url("http://additional-url-example.com")**.
user	Пользователи и группы пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.

Настройка правил reverse-прокси

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Правила reverse-прокси настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд читайте в разделе Настройка правил с использованием UPL.

При настройке правил reverse-прокси необходимо задать:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название правила reverse-прокси. Например: **name("Reverse proxy rule example")**.
desc	Описание правила. Например: **desc("Reverse proxy rule example set via CLI")** .
profile	Сервер reverse-прокси, куда UserGate будет пересылать запросы. Для указания сервера: **profile("Reverse proxy server example")**.
url.port	Порт, на котором UserGate будет слушать входящие запросы, например, **url.port = 80**.
is_https	Поддержка HTTPS: • **is_https(yes)** или **is_https(true)** — использовать HTTPS. • **is_https(no)** или **is_https(false)** — не использовать HTTPS.
ssl_profile	Профиль SSL; указывается при использовании HTTPS: **ssl_profile("Default SSL profile")**. Подробнее о работе с профилями SSL через CLI читайте в разделе Настройка профилей SSL.
certificate	Сертификат, используемый для поддержки HTTPS-соединения. Указывается при использовании HTTPS: **certificate("Certificate example")**.
cert_auth_enabled	Авторизация по сертификату: • **cert_auth_enabled(yes)** или **cert_auth_enabled(true)** — включить авторизацию по сертификату. • **cert_auth_enabled(no)** или **cert_auth_enabled(false)** — отключить авторизацию по сертификату.
src.zone	Зона источника трафика. Для указания зоны источника, например, Untrusted: **src.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, **src.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
user	Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Один из внешних IP-адресов сервера UserGate, доступный из сети интернет, куда адресован трафик внешних клиентов. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: **dst.ip = lib.url()**; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.

Параметр	Описание
dst.geoip	Указание GeoIP; необходимо указать код страны (например, **dst.geoip = RU**). Коды названий стран доступны по ссылке ISO 3166-1. **Важно!** Существует ограничение на количество GeoIP, которое может быть указано: не более 15.
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено данное правило. Для указания Useragent пользовательских браузеров: **request.header.User-Agent = lib.useragent()**; в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров.
rewrite_path	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на http://www.example.com/path1 в http://www.example.loc/path2. Для этого необходимо указать: **rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2")**.

Настройка серверов reverse-прокси

Documentation: ☑
Product: UserGate NGFW
Version: 7.0.1

Настройка серверов reverse-прокси производится на уровне **global-portal reverse-proxy-servers**.

Для создания сервера reverse-прокси используется следующая команда:

Admin@UGOS# create global-portal reverse-proxy-servers

Доступно указание следующих параметров:

Параметр	Описание
name	Название сервера reverse-прокси.
description	Описание сервера reverse-прокси.
address	Адрес или домен сервера reverse-прокси.
port	TCP-порт сервера reverse-прокси.
https	Использование протокола HTTPS до публикуемого сервера: • **on**: использовать. • **off**: не использовать.
check-cert	Проверка валидности SSL-сертификата, установленного на публикуемом сервере: • **on**: проверять. • **off**: не проверять.
keep-source-ip	Использование оригинального IP-адреса источника в пакетах, пересылаемых на публикуемый сервер: • **on**: оставить оригинальный IP-адрес источника. • **off**: заменить IP-адрес источника на IP-адрес UserGate.

Следующая команда предназначена для обновления параметров сервера reverse-прокси:

Admin@UGOS# set global-portal reverse-proxy-servers <server-name>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера.

Структура команды для удаления сервера:

Admin@UGOS# delete global-portal reverse-proxy-servers <server-name>

Структура команды для отображения информации о сервере reverse-прокси:

Admin@UGOS# show global-portal reverse-proxy-servers <server-name>

Настройка удалённого доступа (VPN)

Настройка серверных правил

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Серверные правила настраиваются на уровне **vpn server-rules**. Подробнее о структуре команд настройки серверных правил читайте в разделе Настройка правил с использованием UPL.

При настройке необходимо указать:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**. Если при создании правила не указывать, то правило будет включено после создания.
name	Название серверного правила VPN. Например: **name("VPN server rule example")**.
desc	Описание правила. Например: **desc("VPN server rule example configured in CLI")** .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, **profile("Client VPN profile")**. Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN.
vpn_network	Сеть VPN. Для указания сети: **vpn_network("VPN network example")**. О настройках сети VPN с использованием интерфейса командной строки читайте в разделе Настройка сетей VPN.
auth_profile	Профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль аутентификации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Чтобы указать профиль аутентификации: **auth_profile("Example user auth profile")**. Подробнее о создании и настройке профилей аутентификации с использованием интерфейса командной строки читайте в разделе Настройка профилей аутентификации.
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: **interface(tunnel1)**. О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера.
src.zone	Зона, с которой разрешено принимать подключения к VPN. Для указания зоны источника, например, Untrusted: **src.zone = Untrusted**. Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны.
src.ip	Добавление списков IP-адресов или доменов, с которых разрешено принимать подключения к VPN. Для указания списка IP-адресов: **src.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: **src.ip = lib.url()**; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локальных пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\\AD_user", "CN=AD group, OU=Example, DC= example, DC=loc") Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов интерфейса, на который будет происходить подключение клиентов. Для указания списка IP-адресов: **dst.ip = lib.network()**; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов.

Настройка клиентских правил

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Клиентские правила настраиваются на уровне **vpn client-rules**. Подробнее о структурах команд настройки клиентских правил читайте в разделе Настройка правил с использованием UPL.

При настройке правил необходимо указать:

Параметр	Описание
PASS **OK**	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • **enabled(yes)** или **enabled(true)**. • **enabled(no)** или **enabled(false)**.
name	Название клиентского правила VPN. Например, **name("VPN client rule example")**.
desc	Описание клиентского правила VPN. Указывается, как **desc("VPN client rule example set in CLI")** .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, **profile("Client VPN profile")**. Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN.
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: **interface(tunnel1)**. О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера.
server_address	IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне Untrusted на сервере UserGate, выполняющего роль VPN-сервера. Задаётся в формате: **server_address("1.2.3.4")**.
service	Протокол VPN: • **l2tp** — L2TP. • **cisco cryptomap** — IPsec туннель. Указывается в формате: **service = l2tp** или **service = "cisco cryptomap"** .
subnet1	IP-адрес подсети, разрешённой со стороны UserGate; указывается в формате: **subnet1("ip/mask")**. Подсети указываются при выборе протокола VPN: IPsec туннель.
subnet2	IP-адрес подсети, разрешённой со стороны Cisco; указывается в формате: **subnet2("ip/mask")**. Подсети указываются при выборе протокола VPN: IPsec туннель.
user	Имя пользователя для авторизации сервера, выступающего в качестве клиента VPN. Указывается только для протокола L2TP в формате **user()**; имя пользователя указывается в скобках.
password	Пароль пользователя VPN. Указывается только для протокола L2TP в формате **password()**; пароль указывается в скобках.

При отображении правил, помимо заданных условий и свойств, будут показаны последняя ошибка VPN, статус подключения.

Настройка сетей VPN

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка VPN-сетей производится на уровне **vpn networks**.

Для создания сети VPN необходимо использовать следующую команду:

Admin@UGOS# create vpn networks

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название VPN-сети.
description	Описание сети VPN.
ip-range	Диапазон IP-адресов, которые будут использованы клиентами и сервером; указывается в формате: <IP_start-IP_end>. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.
mask	Маска сети, например, 255.255.255.0.
use-system-dns	Назначение клиенту DNS-серверов, которые использует UserGate: • **on**: использовать системных DNS-серверов. • **off**: не использовать системных DNS-серверов.
dns-servers	DNS-серверы, которые будут переданы клиенту.
routes-ip	Маршрут VPN. Необходимо указать IP-адрес в формате "A.B.C.D" или "A.B.C.D/m".
routes-ip-list	Маршрут VPN. Необходимо указать группу IP-адресов. Подробнее о создании групп IP-адресов через CLI читайте в разделе Настройка IP-адресов.

Следующая команда предназначена для обновления параметров сети:

Admin@UGOS# set vpn networks <network-name>

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления сети VPN.

Структура команды для удаления сети VPN:

Admin@UGOS# delete vpn networks <network-name>

Также можно удалить отдельные параметры сети:

Admin@UGOS# delete vpn networks <network-name> <network-configuration-name>

Параметры, доступные для удаления:

- **dns-servers**.
- **routes-ip**.
- **routes-ip-list**.

Структура команды для отображения информации о сети VPN:

Admin@UGOS# show vpn networks <network-name>

Настройка профилей безопасности VPN

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Профили безопасности VPN настраиваются на уровне **vpn security-profile**.

Для создания профиля безопасности VPN предназначена следующая команда:

Admin@UGOS# create vpn security-profile

Далее необходимо указать следующие параметры:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
ike-version	Версия протокола IKE (Internet Key Exchange), использующегося для создания защищённого канала связи между двумя сетями. В NGFW используется IKEv1 (**IKEv1**).

Параметр	Описание
ike-mode	Режим IKE: • **main** — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. • **aggressive** — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
peer-auth	Аутентификация с пиром: • **psk** — общий ключ — аутентификация устройств с использованием общего ключа (Pre-shared key).
psk	Общий ключ; должен совпадать на сервере и клиенте для успешного подключения.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • **Group 1 Prime 768 bit**. • **Group 2 Prime 1024 bit**. • **Group 5 Prime 1536 bit**. • **Group 14 Prime 2048 bit**. • **Group 15 Prime 3072 bit**. • **Group 16 Prime 4096 bit**. • **Group 17 Prime 6144 bit**. • **Group 18 Prime 8192 bit**.
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: Admin@UGOS# create vpn security-profile ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name> Доступны: • **auth-alg**: выбор алгоритма аутентификации. ◦ **MD5**. ◦ **SHA1**. ◦ **SHA256**. ◦ **SHA384**. ◦ **SHA512**. • **encrypt-alg**: выбор алгоритма шифрования. ◦ **DES**. ◦ **3DES**. ◦ **AES128**. ◦ **AES192**. ◦ **AES256**.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifesize	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Время жизни ключа может быть задано в байтах. Если заданы оба значения (**Время жизни ключа**, **phase2-key-lifetime** и **Максимальный размер данных, шифруемых одним ключом**, **key-lifesize**), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: **off**.

Параметр	Описание
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: Admin@UGOS# create vpn security-profile ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name> Доступны: • **auth-alg**: выбор алгоритма аутентификации. ◦ **MD5**. ◦ **SHA1**. ◦ **SHA256**. ◦ **SHA384**. ◦ **SHA512**. • **encrypt-alg**: выбор алгоритма шифрования. ◦ **DES**. ◦ **3DES**. ◦ **AES128**. ◦ **AES192**. ◦ **AES256**.

Установка значений профиля безопасности:

Admin@UGOS# set vpn security-profile <profile-name>

Параметры, доступные для обновления, аналогичны параметрам, доступным для указания при создании профиля безопасности. Для добавления новой пары алгоритмов аутентификации и шифрования или группы Диффи-Хеллмана в профиль безопасности используются команды со структурой:

Admin@UGOS# set vpn security-profiles <profile-name> phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>
Admin@UGOS# set vpn security-profiles <profile-name> phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name>
Admin@UGOS# set vpn security-profiles <profile-name> dh-groups + [<dh-group1> <dh-group2> ...]

Команда для удаления профиля безопасности:

Admin@UGOS# delete vpn security-profile <profile-name>

Также доступно удаление следующих параметров профиля безопасности VPN:

- **dh-groups**.
- **phase1-security**.
- **phase2-security**.

Для отображения информации о профиле безопасности VPN используется следующая команда:

Admin@UGOS# show vpn security-profile <profile-name>

Настройка библиотек

Documentation:
Product: UserGate NGFW
Version: 7.0.1

Настройка морфологии

Для создания списка морфологии используется следующая команда:

Admin@UGOS# create libraries morphology

Далее необходимо указать:

Параметр	Описание
name	Название морфологического списка.
description	Описание списка.
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.
threshold	Вес морфологической категории, при превышении которого сработает правило.
url	Если морфологический список является обновляемым, то необходимо указать адрес, с которого необходимо загружать обновления.
words	Слова и фразы, которые необходимо добавить в список. • **word** — слова и фразы. При добавлении слова в морфологический словарь можно использовать модификатор «!» перед словом, например, «!bassterd». В данном случае жаргонное слово не будет преобразовываться в словоформы, что может серьезно уменьшить вероятность ложной блокировки. • **weight** — вес слова или фразы. Если вес не задан, то автоматический устанавливается значение 100. Для добавления слов и фраз: Admin@UGOS# create libraries morphology ... words new word "word or phrase" weight <weight>

Чтобы обновить данные морфологического списка, необходимо использовать следующую команду:

Admin@UGOS# set libraries morphology <morphology-list-name>

Далее указываются параметры, значения которых необходимо обновить (список параметров представлен в таблице выше). Для добавления в список новых слов или фраз необходимо использовать команду:

Admin@UGOS# set libraries morphology <morphology-list-name> words new word "word or phrase" weight <weight>

Чтобы заменить слово в списке:

Admin@UGOS# set libraries morphology <morphology-list-name> words (word "old word or phrase" weight <weight>) word "new word or phrase" weight <weight>

Следующие команды используются для удаления всего морфологического списка или отдельных слов, содержащихся в нём:

Admin@UGOS# delete libraries morphology <morphology-list-name>
Admin@UGOS# delete libraries morphology <morphology-list-name> words (word "word or phrase" weight <weight>)

Команды отображения информации о всех имеющихся морфологических списках:

Admin@UGOS# show libraries morphology

Чтобы отобразить информацию об определённом списке, далее необходимо указать название интересующего морфологического списка. Чтобы просмотреть содержание определённого морфологического списка:

Admin@UGOS# show libraries morphology <morphology-list-name> words

Настройка сервисов

Данный раздел настраивается на уровне **libraries services**.

Для добавления нового сервиса используется следующая команда:

Admin@UGOS# create libraries services

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название сервиса.
description	Описание сервиса.

Параметр	Описание
protocols	Указание сетевого протокола и портов источника/назначения: • **protocol** — сетевой протокол. • **dest-ports** — порт(ы) назначения (указывается номер порта или диапазон портов). • **source-ports** — порт(ы) источника (указывается номер порта или диапазон портов). При создании сервиса для указания значений параметра **protocols**: Admin@UGOS# create libraries service ... protocols new Далее указываются параметры **protocol**, **dest-ports**, **source-ports**.

Для обновления существующего сервиса:

Admin@UGOS# set libraries services <service-name>

Для обновления сетевого протокола и портов источника/назначения сервиса:

Admin@UGOS# set libraries services <service-name> protocols (<protocol-filter>)

<protocol-filter> — фильтр, настроенный с использованием значений параметра protocols.

Далее указываются новые значения параметра **protocols**.

Для добавления сетевого протокола и портов источника/назначения в существующий сервис:

Admin@UGOS# set libraries services <service-name> protocols new

Далее необходимо указать **protocol**, **dest-ports**, **source-ports**.

Чтобы удалить сервис используется следующая команда:

Admin@UGOS# delete libraries services <service-name>

Также возможно удаления из сервиса заданных сетевых протоколов:

Admin@UGOS# delete libraries services <service-name> protocols (<protocol-filter>)

Следующие команды предназначены для отображения информации о всех сервисах или об определённом сервисе:

Admin@UGOS# show libraries services
Admin@UGOS# show libraries services <service-name>

Настройка групп сервисов

Данный раздел находится на уровне **libraries service-groups**. Для создания группы сервисов предназначена следующая команда:

Admin@UGOS# create libraries service-groups

Далее указываются параметры:

Параметр	Описание
name	Название группы сервисов.
description	Описание группы.
services	Сервисы, которые необходимо добавить в группу.

Для обновления информации о группе сервисов (список параметров, доступных для обновления, аналогичен списку параметров команды создания группы):

Admin@UGOS# set libraries service-groups <service-group-name>

Чтобы добавить в группу сервисы:

Admin@UGOS# set libraries service-groups <service-group-name> + [<service1> < service2> ...]

Следующие команды используются для удаления группы сервисов или отдельных сервисов, содержащихся в ней:

Admin@UGOS# delete service-groups <service-group-name>
Admin@UGOS# delete service-groups <service-group-name> services [<service> ...]

Команды отображения информации о всех имеющихся списках:

Admin@UGOS# show libraries service-groups

об определённом списке:

Admin@UGOS# show libraries service-groups <service-group-name>

или списка сервисов, добавленных в группу:

Admin@UGOS# show libraries service-groups <service-group-name> services

Настройка IP-адресов

Данный раздел находится на уровне **libraries ip-list**.

Для создания группы IP-адресов используется следующая команда:

Admin@UGOS# create libraries ip-list

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название списка адресов.
description	Описание списка.

Параметр	Описание
threat-lvl	Уровень угрозы: • **very-low** — очень низкий уровень угрозы. • **low** — низкий уровень угрозы. • **medium** — средний уровень угрозы. • **high** — высокий уровень угрозы. • **very-high** — высокий уровень угрозы.
url	Если список адресов является обновляемым, то необходимо указать URL обновления.
ips	IP-адреса или диапазон IP-адресов, которые необходимо включить в список. Указывается в формате: <ip>, <ip/mask> или <ip_range_start-ip_range_end>.

Для обновления информации о списке (список параметров, доступных для обновления, аналогичен списку параметров команды создания списка):

Admin@UGOS# set libraries ip-list <ip-list-name>

Чтобы добавить в список новые адреса:

Admin@UGOS# set libraries ip-list <ip-list-name> ips + [<ip1> <ip2> ...]

Следующие команды используются для удаления всего списка адресов или IP-адресов, содержащихся в нём:

Admin@UGOS# delete libraries ip-list <ip-list-name>
Admin@UGOS# delete libraries ip-list <ip-list-name> ips [<ip> ...]

Команда отображения информации о всех имеющихся списках:

Admin@UGOS# show libraries ip-list

Чтобы отобразить информацию об определённом списке, необходимо указать название интересующего списка IP-адресов:

Admin@UGOS# show libraries ip-list <ip-list-name>

Также доступен просмотр содержимого списка IP-адресов:

Admin@UGOS# show libraries ip-list <ip-list-name> ips

Настройка Useragent браузеров

Раздел настраивается на уровне **libraries useragents**.

Следующая команда используется для добавления нового списка Useragent браузеров:

Admin@UGOS# create libraries useragents

Далее указываются следующие данные:

Параметр	Описание
name	Название списка Useragent.
description	Описание списка.
url	Если список является обновляемым, то необходимо указать URL обновления.
patterns	Шаблоны Useragent. Список Useragent браузеров доступен по ссылке: http://www.useragentstring.com/pages/useragentstring.php.

Для обновления существующего списка:

Admin@UGOS# set libraries useragents <useragent-list-name>

Далее указываются параметры, которые необходимо обновить. Параметры представлены в таблице выше. Чтобы добавить новые Useragent браузеров:

Admin@UGOS# set libraries useragents <useragent-list-name> + [<useragent1> <useragent2> ...]

Следующие команды используются для удаления всего списка или отдельных Useragent браузеров, содержащихся в нём:

Admin@UGOS# delete libraries useragents <useragent-list-name>
Admin@UGOS# delete libraries useragents <useragent-list-name> patterns [<useragent> ...]

Команды отображения информации о всех имеющихся списках:

Admin@UGOS# show libraries useragents

Чтобы отобразить информацию об определённом списке, необходимо указать название списка Useragent браузеров. Чтобы просмотреть содержание списка Useragent браузеров:

Admin@UGOS# show libraries useragents <useragent-list-name> patterns

Настройка типов контента

Раздел **Типы контента** находится на уровне **libraries content-types**.

Добавление нового списка типов контента доступно с использованием следующей команды:

Admin@UGOS# create libraries content-types

Далее указывается следующая информация:

Параметр	Описание
name	Название списка типов контента.
description	Описание списка.

Параметр	Описание
url	Если список является обновляемым, то необходимо указать URL обновления.
types	Типы контента, которые необходимо добавить в список. Различные типы контента и их описание доступны по ссылке https://www.iana.org/assignments/media-types/media-types.xhtml.

Для обновления информации о списке используется следующая команда:

Admin@UGOS# set libraries content-types <content-types-list-name>

Параметры, доступные для обновления, представлены в таблице выше.

Следующая команда используется для удаления списка с типами контента:

Admin@UGOS# delete libraries content-types <content-types-list-name>

Также доступно удаление отдельных типов контента из списка:

Admin@UGOS# delete libraries content-types <content-types-list-name> types [<mime-type> ...]

Следующие команды используются для отображения информации о списках типов контента:

Admin@UGOS# show libraries content-types
Admin@UGOS# show libraries content-types <content-types-list-name>

Для отображения типов контента, содержащихся в списке, используется команда:

Admin@UGOS# show libraries content-types <content-types-list-name> types

Настройка списков URL

Настройка списков URL производится на уровне **libraries url-list**.

Для добавления нового списка URL предназначена следующая команда:

Admin@UGOS# create libraries url-list

Далее указывается следующая информация:

Параметр	Описание
name	Название списка URL.
description	Описание списка URL.
url	Если список является обновляемым, то необходимо указать URL обновления.
urls	URL, которые необходимо добавить в список.

Для обновления информации о списке URL:

Admin@UGOS# set libraries url-list <url-list-name>

Параметры, значения которых можно обновить, представлены в таблицы выше.

Далее представлены команды, с использованием которых доступно удаление всего списка URL или отдельных адресов URL:

Admin@UGOS# delete libraries url-list <url-list-name>
Admin@UGOS# delete libraries url-list <url-list-name> urls [<url> ...]

Для просмотра информации о всех списках URL, об определённом списке URL или об адресах, входящих в определённый список, используются команды:

Admin@UGOS# show libraries url-list
Admin@UGOS# show libraries url-list <url-list-name>
Admin@UGOS# show libraries url-list <url-list-name> urls

Настройка календарей

Данный раздел находится на уровне **libraries time-sets**.

Для создания группы используется следующая команда:

Admin@UGOS# create libraries time-sets

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название группы.
description	Описание группы.

Параметр	Описание
time-set	Тип повторения: • **daily** — ежедневно: ◦ **interval-name** — название интервала. ◦ **time-from** — время начала (указывается в формате HH:MM). ◦ **time-to** — время окончания (указывается в формате HH:MM). ◦ **all-day on** — весь день. • **weekly** — каждую неделю: ◦ **interval-name** — название интервала. ◦ **time-from** — время начала (указывается в формате HH:MM). ◦ **time-to** — время окончания (указывается в формате HH:MM). ◦ **all-day on** — весь день. ◦ **days [Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun]** — дни недели. • **monthly** — каждый месяц: ◦ **interval-name** — название интервала. ◦ **time-from** — время начала (указывается в формате HH:MM). ◦ **time-to** — время окончания (указывается в формате HH:MM). ◦ **all-day on** — весь день. ◦ **days** — числа месяца (от 1 до 31). • **fixed** — единовременно: ◦ **interval-name** — название интервала. ◦ **time-from** — время начала (указывается в формате HH:MM). ◦ **time-to** — время окончания (указывается в формате HH:MM). ◦ **all-day on** — весь день. ◦ **fixed-date** — нужная дата (указывается в формате YYYY-MM-DD). • **repeating** — повторяющиеся события: ◦ **interval-name** — название интервала. ◦ **time-from** — время начала (указывается в формате HH:MM). ◦ **time-to** — время окончания (указывается в формате HH:MM). ◦ **all-day on** — весь день. ◦ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD). ◦ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD). • **range** — диапазон дат: ◦ **interval-name** — название интервала. ◦ **time-from-enabled <on** | **off>** — включение/отключение указания даты начала интервала. ◦ **fixed-date-from** — дата начала (указывается в формате YYYY-MM-DD). ◦ **time-from** — время начала (указывается в формате HH:MM). ◦ **time-to-enabled <on** | **off>** — включение/отключение указания даты окончания интервала. ◦ **fixed-date-to** — дата окончания (указывается в формате YYYY-MM-DD). ◦ **time-to** — время окончания (указывается в формате HH:MM). Admin@UGOS# create libraries time-sets ... time-set <time-set-type> new Далее указываются параметры, выбранного типа повторения.

Для обновления календаря:

Admin@UGOS# set libraries time-sets <time-sets-name>

Параметры, доступные для обновления, представлены в таблице выше.

Для обновления интервала, заданного в календаре:

Admin@UGOS# set libraries time-sets <time-sets-name> ... time-set <time-set-type> (<time-set-filter>)

Далее указываются новые значения; <time-set-filter> — фильтр из текущих значений интервала.

Добавление нового элемента в существующую группу:

Admin@UGOS# create libraries time-sets <time-sets-name> ... time-set <time-set-type> new

Команда для удаления группы элементов:

Admin@UGOS# delete libraries time-sets <time-sets-name>

Для удаления элемента календаря:

Admin@UGOS# delete libraries time-sets <time-sets-name> <time-set-type> (<time-set-filter>)

Для отображения информации о всех календарях:

Admin@UGOS# show libraries time-sets

Для отображения информации об определённом календаре:

Admin@UGOS# show libraries time-sets <time-sets-name>

Для отображения информации об элементах группы с одинаковым типом повторения:

Admin@UGOS# show libraries time-sets <time-sets-name> <time-set-type>

Настройка полос пропускания

Раздел находится на уровне **libraries bandwidth-pools**.

Для добавления новой полосы пропускания используется следующая команда:

Admin@UGOS# create libraries bandwidth-pools

Далее необходимо задать следующие параметры:

Параметр	Описание
name	Название полосы пропускания.
description	Описание полосы пропускания.
rate	Скорость передачи данных; указывается в Кбит/с.
dscp	Значение DSCP для QoS (при указании будет прописываться в каждый IP-пакет: принимает значения от 0 до 63).

Для обновления параметров полосы пропускания:

Admin@UGOS# set libraries bandwidth-pools <bandwidth-name>

Параметры, доступные для изменения такие же, как и для команды создания полосы пропускания.

Чтобы удалить полосу пропускания:

Admin@UGOS# delete libraries bandwidth-pools <bandwidth-name>

С использованием **show** можно отобразить информацию о всех полосах пропускания:

Admin@UGOS# show libraries bandwidth-pools

или об определённой полосе:

Admin@UGOS# show libraries bandwidth-pools <bandwidth-name>

Настройка шаблонов страниц

Раздел находится на уровне **libraries response-pages**. Доступно создание следующих типов шаблонов страниц (<response-page-type>):

- **blockpage** — страница блокировки.
- **captiveportal-user-auth** — страница авторизации captive-портала.
- **captiveportal-user-session** — captive-портал, сессия пользователя.
- **content-warning** — содержание страницы предупреждения.
- **ftp-client** — страница отображения FTP поверх HTTP.
- **proxy-portal** — страница веб-портала.
- **pp-login-ssh** — страница SSH-логина веб-портала.
- **pp-login-rdp** — страница RDP-логина веб-портала.
- **totp-init-page** — страница инициализации TOTP.

Команда, используемая для создания шаблона страницы:

Admin@UGOS# create libraries response-pages type <response-page-type>

Необходимо указать параметры:

Параметр	Описание
name	Название шаблона страницы.
description	Описание шаблона.

Параметр	Описание
original-template	Выбор базового шаблона. Базовые шаблоны для страницы блокировки (**blockpage**): • **blockpage_en** — шаблон страницы блокировки на английском языке. • **blockpage_ru** — шаблон страницы блокировки на русском языке. Базовые шаблоны для страницы авторизации captive-портала (**captiveportal-user-auth**): • **captiveportal_user_auth_en** — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. • **captiveportal_user_auth_ru** — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. • **captiveportal_user_auth_policy_en** — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. • **captiveportal_user_auth_policy_ru** — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон, помимо формы авторизации, выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. • **captiveportal_user_auth_email_en** — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email. • **captiveportal_user_auth_email_ru** — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по email. • **captiveportal_user_auth_sms_en** — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS. • **captiveportal_user_auth_sms_ru** — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке, позволяющий пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя по SMS. • **captiveportal_user_policy_en** — шаблон страницы авторизации пользователя с помощью captive-портала на английском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод **Принять политику** в качестве метода аутентификации в профиле авторизации. • **captiveportal_user_policy_ru** — шаблон страницы авторизации пользователя с помощью captive-портала на русском языке. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. Для работы данного шаблона требуется установить метод **Принять политику** в качестве метода аутентификации в профиле авторизации. Базовые шаблоны для страницы captive-портал, сессия пользователя (**captiveportal-user-session**): • **captiveportal_user_session_en** — шаблон на английском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps. • **captiveportal_user_session_ru** — шаблон на русском языке, с помощью которого пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps. Базовые шаблоны для страницы предупреждения (**content-warning**): • **content_warning_en** — шаблон страницы предупреждения на английском языке, отображаемый при срабатывании правила контентной фильтрации с действием **Предупредить**. • **content_warning_ru** — шаблон страницы предупреждения на русском языке, отображаемый при срабатывании правила контентной фильтрации с действием **Предупредить**. Базовые шаблоны для страницы отображения FTP поверх HTTP (**ftp-client**): • **ftp_client_en** — шаблон на английском языке для отображения контента FTP-серверов поверх HTTP. • **ftp_client_ru** — шаблон на русском языке для отображения контента FTP-серверов поверх HTTP. Базовые шаблоны для страницы веб-портала (**proxy-portal**): • **proxy_portal_en** — шаблон на английском языке для отображения страницы веб-портала. • **proxy_portal_ru** — шаблон на русском языке для отображения страницы веб-портала. Базовые шаблоны для страницы SSH-логина веб-портала (**pp-login-ssh**): • **pp_login_ssh_en** — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал. • **pp_login_ssh_ru** — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал. Базовые шаблоны для страницы RDP-логина веб-портала (**pp-login-rdp**): • **pp_login_rdp_en** — шаблон на английском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал. • **pp_login_rdp_ru** — шаблон на русском языке для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал. Базовые шаблоны для страницы инициализации TOTP (**totp-init-page**): • **totp_init_page_en** — шаблон на английском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей. • **totp_init_page_ru** — шаблон на русском языке для отображения страницы инициализации устройства TOTP для VPN-пользователей.
default	Использовать шаблон по умолчанию: • **on**. • **off**.

Для установки значений шаблона:

Admin@UGOS# set libraries response-pages type <response-page-type> response-page <response-page-name>

Далее необходимо указать значения параметров; параметры представлены в таблице выше.

Чтобы удалить шаблон страницы, используется следующая команда:

Admin@UGOS# delete libraries response-pages type <response-page-type> response-page <response-page-name>

Для просмотра информации о всех имеющихся шаблонах страниц:

Admin@UGOS# show libraries response-pages

Для просмотра информации об отдельном типе шаблонов страниц:

Admin@UGOS# show libraries response-pages type <response-page-type>

Для просмотра информации об отдельном шаблоне страницы:

Admin@UGOS# show libraries response-pages type <response-page-type> response-page <response-page-name>

Настройка категорий URL

Раздел находится на уровне **libraries url-categories**.

Для создания группы категорий URL используется следующая команда:

Admin@UGOS# create libraries url-categories

Параметры, которые необходимо указать:

Параметр	Описание
name	Название группы URL-категорий.
description	Описание группы.
categories	Категории URL, которые необходимо добавить в группу.

Команда для изменения параметров группы:

Admin@UGOS# set libraries url-categories <list-name>

Для добавления категорий URL в существующую группу:

Admin@UGOS# set libraries url-categories <list-name> categories + [<url-category> ...]

Команды для удаления группы URL-категорий:

Admin@UGOS# delete libraries url-categories <list-name>

или отдельных категорий из группы:

Admin@UGOS# delete libraries url-categories <list-name> categories [<url-category> ...]

Команды для просмотра информации о всех группах URL-категорий:

Admin@UGOS# show libraries url-categories

об определённой группе:

Admin@UGOS# show libraries url-categories <list-name>

Чтобы отобразить список категорий URL, входящих в группу:

Admin@UGOS# show libraries url-categories <list-name> categories

Настройка изменённых категорий URL

Настройка раздела **Изменённые категории URL** производится на уровне **overridden-url-categories**.

Для добавления новой изменённой категории URL:

Admin@UGOS# create libraries overridden-url-categories

Далее необходимо указать параметры:

Параметр	Описание
domain	Доменное имя проверяемого ресурса.
description	Описание изменяемого домена.
categories	Новые категории сайта (можно указать не более 2-х категорий).

Для изменения параметров:

Admin@UGOS# set libraries overridden-url-categories <domain>

Для удаления сайта с изменёнными категориями:

Admin@UGOS# delete libraries overridden-url-categories <domain>

Для отображения всего списка сайтов с изменёнными категориями:

Admin@UGOS# show libraries overridden-url-categories

Для отображения информации об определённом сайте с изменёнными категориями URL:

Admin@UGOS# show libraries overridden-url-categories <domain>

Настройка приложений

Данный раздел настраивается на уровне **libraries applications**.

Для создания группы приложений используется команда:

Admin@UGOS# create libraries applications

Далее указываются параметры:

Параметр	Описание
name	Название группы приложений.
description	Описание группы приложений.
apps	Приложения, которые необходимо добавить в группу.

Для изменения параметров:

Admin@UGOS# set libraries applications <app-group-name>

Чтобы добавить новые приложения в существующую группу, используется команда:

Admin@UGOS# set libraries applications <app-group-name> apps + [<application> ...]

Для удаления группы приложений полностью или отдельных приложений в ней используются команды:

```
Admin@UGOS# delete libraries applications <app-group-name>
Admin@UGOS# delete libraries applications <app-group-name> apps [ <application> ... ]
```

Следующие команды предназначены для отображения информации о всех созданных группах приложений:

```
Admin@UGOS# show libraries applications
```

или об определённой группе:

```
Admin@UGOS# show libraries applications <app-group-name>
```

Также доступно отображение приложений, входящих в определённый список:

```
Admin@UGOS# show libraries applications <app-group-name> apps
```

Настройка почтовых адресов

Раздел находится на уровне **libraries email-list**.

Чтобы добавить новую группу почтовых адресов используется следующая команда:

```
Admin@UGOS# create libraries email-list
```

Далее указываются параметры:

Параметр	Описание
name	Название группы почтовых адресов.
description	Описание группы почтовых адресов.
url	Если список почтовых адресов является обновляемым, то необходимо указать URL обновления.
emails	Почтовые адреса, которые необходимо добавить в данную группу.

Команда, предназначенная для обновления информации о группе почтовых адресов:

```
Admin@UGOS# set libraries email-list <email-list-name>
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании группы почтовых адресов.

Для удаления группы или почтовых адресов из неё используются следующие команды:

```
Admin@UGOS# delete libraries email-list <email-list-name>
Admin@UGOS# delete libraries email-list <email-list-name> emails [ <email> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах, об определённых группах или для просмотра почтовых адресов, входящих в группу:

```
Admin@UGOS# show libraries email-list
Admin@UGOS# show libraries email-list <email-list-name>
Admin@UGOS# show libraries email-list <email-list-name> emails
```

Настройка номеров телефонов

Настройка раздела **Номера телефонов** производится на уровне **libraries phone-list**.

Для создания группы телефонных номеров:

```
Admin@UGOS# create libraries phone-list
```

Далее необходимо указать следующие данные:

Параметр	Описание
name	Название группы телефонных номеров.
description	Описание группы телефонных номеров.
url	Если список почтовых адресов является обновляемым, то необходимо указать URL обновления.
phones	Номера телефонов, которые необходимо добавить в данную группу.

Для обновления информации о группе телефонных номеров используется команда:

```
Admin@UGOS# set libraries phone-list <phone-list-name>
```

Параметры, доступные для обновления, представлены в таблице выше.

Для удаления группы или номеров телефонов из неё используются следующие команды:

```
Admin@UGOS# delete libraries phone-list <phone-list-name>
Admin@UGOS# delete libraries phone-list <phone-list-name> phones [ <phone> ... ]
```

Следующие команды используются для просмотра информации о всех созданных группах:

```
Admin@UGOS# show libraries phone-list
```

или об определённых группах телефонных номеров:

```
Admin@UGOS# show libraries phone-list <phone-list-name>
```

Для просмотра номеров, содержащихся в группе, используется команда:

```
Admin@UGOS# show libraries phone-list <phone-list-name> phones
```

Настройка профилей СОВ

Настройка профилей СОВ производится на уровне **libraries ips-profiles**. Для создания профиля системы обнаружения вторжения используется команда:

```
Admin@UGOS# create libraries ips-profiles
```

Необходимо указание следующих параметров:

Параметр	Описание
name	Название профиля СОВ.
description	Описание профиля СОВ.
signatures	Сигнатур, релевантные для защиты определенных сервисов.

Представленная ниже команда предназначена для обновления существующего профиля СОВ:

Admin@UGOS# set libraries ips-profiles <ips-profile-name>

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании профиля.

С использование **delete** возможно удаление сигнатур из профиля СОВ или профиля полностью:

Admin@UGOS# delete libraries ips-profiles <ips-profile-name> signatures
Admin@UGOS# delete libraries ips-profiles <ips-profile-name>

С использованием следующих команда возможно отображение информации о всех профилях СОВ:

Admin@UGOS# show libraries ips-profiles

или об одном профиле:

Admin@UGOS# show libraries ips-profiles <ips-profile-name>

Также доступен просмотр списка сигнатур, добавленных в профиль:

Admin@UGOS# show libraries ips-profiles <ips-profile-name> signatures

Настройка профилей оповещений

Профили оповещений SMTP (по email) и SMPP (по SMS) настраиваются на уровне **libraries notification-profiles**.

Для добавления нового профиля оповещения SMTP:

Admin@UGOS# create libraries notification-profiles smtp

Далее необходимо указать:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
port	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL — 465. Уточните данное значение у администратора почтового сервера.
connection-security	Варианты безопасности отправки почты; возможны варианты: • **none**. • **starttls**. • **ssl**.
authentication	Включение/отключение авторизации при подключении к серверу SMTP: • **on**. • **off**.
login	Имя учётной записи для подключения к SMTP-серверу.
password	Пароль учётной записи для подключения к SMTP-серверу.

Для создания профиля оповещения по SMS (SMPP):

Admin@UGOS# create libraries notification-profiles smpp

Далее необходимо указать значения следующих параметров:

Параметр	Описание
name	Название профиля.
description	Описание профиля.
host	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS.
port	Порт TCP, который используется для подключения к серверу SMPP. Обычно для протокола SMPP используется порт 2775; при использовании SSL — 3550.
ssl	Включение/отключение шифрования SSL: • **on**. • **off**.

Параметр	Описание
login	Имя учётной записи для подключения к SMPP-серверу.
password	Пароль учётной записи для подключения к SMPP-серверу.
phone-translation-rules	Правила трансляции телефонных номеров. Правила используются для соответствия требованиям провайдера. Например, если необходимо заменить все номера, начинающиеся на +7, на 8: Admin@UGOS# set libraries notification-profiles smpp <profile-name> phone-translation-rules + [+7¦8]
source-ton	Тип номера (Type of Number) для источника сообщения: • **0** — Unknown (Неизвестный). • **1** — International (Международный). • **2** — National (Государственный). • **3** — Network Specific (Сетевой Специальный). • **4** — Subscriber Number (Номер абонента). • **5** — Alphanumeric (Алфавитно-цифровой). • **6** — Abbreviated (Сокращённый).
dest-ton	Тип номера (Type of Number) для адресата: • **0** — Unknown (Неизвестный). • **1** — International (Международный). • **2** — National (Государственный). • **3** — Network Specific (Сетевой Специальный). • **4** — Subscriber Number (Номер абонента). • **5** — Alphanumeric (Алфавитно-цифровой). • **6** — Abbreviated (Сокращённый).
source-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для источника: • **0** — Unknown. • **1** — ISDN/telephone numbering plan (E.163/E.164). • **3** — Data numbering plan (X.121). • **4** — Telex numbering plan (F.69). • **6** — Land Mobile (E.212). • **8** — National numbering plan. • **9** — Private numbering plan. • **10** — ERMES numbering plan (ETSI DE/PS 3 01-3). • **13** — Internet (IP). • **18** — WAP Client Id (to be defined by WAP Forum).
dest-npi	Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата: • **0** — Unknown. • **1** — ISDN/telephone numbering plan (E.163/E.164). • **3** — Data numbering plan (X.121). • **4** — Telex numbering plan (F.69). • **6** — Land Mobile (E.212). • **8** — National numbering plan. • **9** — Private numbering plan. • **10** — ERMES numbering plan (ETSI DE/PS 3 01-3). • **13** — Internet (IP). • **18** — WAP Client Id (to be defined by WAP Forum).

Для обновления информации о профиле оповещения используется команда:

Admin@UGOS# set libraries notification-profiles <smtp | smpp> <profile-name>

Параметры профилей SMTP и SMPP, доступные для изменения, представлены в соответствующих таблицах выше.

Для удаления профиля:

Admin@UGOS# set libraries notification-profiles <smtp | smpp> <profile-name>

Также для профилей оповещений SMPP доступно удаления правил трансляции номеров:

Admin@UGOS# set libraries notification-profiles smpp <profile-name> phone-translation-rules [phone1¦phone2]

Следующие команды предназначены для отображения информации о всех имеющихся профилях оповещений:

Admin@UGOS# show libraries notification-profiles

о всех профилях одного типа:

Admin@UGOS# set libraries notification-profiles <smtp | smpp>

об определённом профиле оповещения:

Admin@UGOS# show libraries notification-profiles <smtp | smpp> <profile-name>

Настройка профилей NetFlow

Раздел находится на уровне **libraries netflow-profiles**.

Команда для создания профиля NetFlow:

Admin@UGOS# create libraries netflow-profiles

Далее необходимо указать параметры профиля:

Параметр	Описание
name	Название профиля NetFlow.
description	Описание профиля.
ip	IP-адрес NetFlow коллектора, куда сенсор будет отправлять статистику.
port	UDP порт, на котором NetFlow коллектор будет принимать статистику.
protocol	Версия протокола NetFlow, которую необходимо использовать (должна совпадать на сенсоре и коллекторе): • **netflow5**. • **netflow9**. • **netflow10**.
active-timeout	Время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока (например, передача большого файла через сеть). Задаётся в секундах; значение по умолчанию: 1800 секунд, максимальное значение — 3600 секунд.
inactive-timeout	Время, резервируемое на завершение неактивного потока; указывается в секундах. Значение по умолчанию — 15 секунд; максимальное значение — 3600 секунд.
max-flows	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. После достижения указанного количества все последующие потоки не будут учитываться (ограничение необходимо для защиты от DoS-атак); значение по умолчанию — 2000000; для снятия ограничения установить 0.
nat-events	Включить/отключить отправку информации о NAT преобразованиях в статистику NetFlow: • **on**. • **off**.
refresh-rate	Количество пакетов, после которого шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
timeout-rate	Время, через которое старый шаблон отправляется на принимающий хост (только для версий протокола NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Чтобы обновить существующий профиль:

Admin@UGOS# set libraries netflow-profiles <profile-name>

Параметры, значения которых можно изменить, представлены в таблице выше.

Следующая команда предназначена для удаления профиля NetFlow:

Admin@UGOS# delete libraries netflow-profiles <profile-name>

Для отображения информации о всех профилях NetFlow или об отдельном профиле используются следующие команды:

Admin@UGOS# show libraries netflow-profiles
Admin@UGOS# show libraries netflow-profiles <profile-name>

Настройка профилей LLDP

Создание и настройка профилей LLDP (Link Layer Discovery Protocol) производятся на уровне **libraries lldp-profiles**.

Команда для создания профиля LLDP:

Admin@UGOS# create libraries lldp-profiles

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля LLDP.
description	Описание профиля.
port-status	Режимы: • **rx** — только приём данных LLDP — UserGate не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • **tx** — только передача данных LLDP — UserGate будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей. • **rx-tx** — приём и передача данных LLDP — UserGate будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей.

Следующая команда предназначена для обновления информации о профиле:

Admin@UGOS# set libraries lldp-profiles <profile-name>

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль LLDP, используя следующую команду:

Admin@UGOS# delete libraries lldp-profiles <profile-name>

Чтобы отобразить информацию о профилях:

```
Admin@UGOS# show libraries lldp-profiles
Admin@UGOS# show libraries lldp-profiles <profile-name>
```

Настройка профилей SSL

Создание и настройка профилей SSL производятся на уровне **libraries ssl-profiles**.

Команда для создания профиля SSL:

```
Admin@UGOS# create libraries ssl-profiles
```

Далее представлены параметры, которые необходимо указать:

Параметр	Описание
name	Название профиля SSL.
description	Описание профиля.
min-tls-version	Минимальная версия TLS, которая может быть использована в данном профиле: • **tls1**. • **tls1.1**. • **tls1.2**.
min-tls-version	Минимальная версия TLS, которая может быть использована в данном профиле: • **tls1**. • **tls1.1**. • **tls1.2**. • **tls1.3**.
ssl-ciphers	Выбор необходимых алгоритмов шифрования и цифровой подписи.
ssl-ciphers-suite	Установка алгоритмов шифрования для стандартных протоколов. Параметр предназначен для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS; необходимо указать версию: • **tls1**. • **tls1.1**. • **tls1.2**. • **tls1.3**.

Следующая команда предназначена для обновления информации о профиле:

```
Admin@UGOS# set libraries ssl-profiles <profile-name>
```

Параметры, доступные для обновления, аналогичны параметрам, указываемым при создании профиля.

Пользователь может удалить профиль SSL полностью или удалить отдельные алгоритмы шифрования и цифровой подписи, заданные в нём:

```
Admin@UGOS# delete libraries ssl-profiles <profile-name>
Admin@UGOS# delete libraries ssl-profiles <profile-name> ssl-ciphers [ cipher ... ]
```

Чтобы отобразить информацию о профилях SSL:

```
Admin@UGOS# show libraries ssl-profiles
Admin@UGOS# show libraries ssl-profiles <profile-name>
```

Настройка профилей пересылки SSL

Данный раздел находится на уровне **libraries ssl-forwarding-profiles**.

Для создания профиля пересылки используется команда:

```
Admin@UGOS# create libraries ssl-forwarding-profiles
```

Далее необходимо указать:

Параметр	Описание
name	Название профиля пересылки SSL.
description	Описание профиля пересылки.
forward-type	Тип пересылки: • **l2**. При настройке необходимо указать MAC-адрес устройства и название интерфейса, на который необходимо переслать копию трафика. • **l3**. Копия расшифрованного трафика передаётся по GRE-туннелю. При настройке необходимо указать GRE IP-адресы источника и назначения.
target-mac	MAC-адрес назначения (указывается при использовании типа пересылки L2).
target-iface	Интерфейс UserGate, с которого будет производиться пересылка (указывается при использовании типа пересылки L2).
gre-source-ip	GRE IP-адрес источника (указывается при использовании типа пересылки L3).
gre-dest-ip	GRE IP-адрес назначения (указывается при использовании типа пересылки L3).

Следующая команда предназначена для обновления параметров профилей пересылки:

Admin@UGOS# set libraries ssl-forwarding-profiles <profile-name>

Для удаления профиля:

Admin@UGOS# delete libraries ssl-forwarding-profiles <profile-name>

Чтобы отобразить информацию о всех имеющихся профилях или об определённом профиле пересылки, используются следующие команды:

Admin@UGOS# show libraries ssl-forwarding-profiles
Admin@UGOS# show libraries ssl-forwarding-profiles <profile-name>

Общие сведения

Documentation: ☑
Version: 7.0.1
Product: UserGate NGFW

Для программно-аппаратных комплексов (ПАК) UserGate C150 и X10 доступен PMC CLI, предназначенный для мониторинга и управления устройством UserGate.

Структура команд PMC CLI идентична структуре команд CLI основного продукта:

<action> <level> <filter> <configuration_info>

где <action>: действие, которое необходимо выполнить (create, set, show, delete).

<level>: уровень конфигурации (platform, network, factory, users).

<filter>: идентификатор объекта, к которому происходит обращение.

<configuration_info>: значение параметров, которые необходимо применить к объекту <filter>.

Также существуют команды, которые позволяют выполнить действия, не относящиеся к конфигурации.

Наименование	Описание
help	Отображение списка доступных команд и краткая информации о них. Помимо **help** возможно использование **?**. Для получения подробного описания команды используйте команду типа: PMC> help <command_name> или PMC> ? <command_name> Например: PMC> ? ping ping - send ICMP ECHO_REQUEST to network host Usage: ping <Address> [size]
aux	Переход в интерфейс командной строки (CLI) основного продукта. Для возвращения в PMC CLI используется комбинация клавиш « **CTRL +]** »
autoboot	Запуск команды автозагрузки.
history	Вывод истории команд.
ping	Отправка сообщение ICMP Echo Request к хостам сети; выполняется 5 раз с интервалом в 1 секунду. В качестве опционального параметра можно задать размер данных в пакете.
reset	Перезапуск устройства.
update	Обновление компонентов программного обеспечения (ПО) или вспомогательных элементов. Для обновления доступны: • **pmc** — обновление прошивки Platform Management Controller. • **pmc-backup** — обновление резервного образа PMC. • **boot** — вспомогательное ПО, занимающееся запуском основного образа. • **sys-recovery** — вспомогательная система, позволяющая удалённо в ручном режиме восстановить работоспособность устройства, например, если основной образ был повреждён. Команда имеет следующую структуру: PMC> update firmware <pmc | pmc-backup | boot | sys-recovery> tftp <address> <filename> где <address> — адрес сервера TFTP. <filename> — название файла обновления. Например, команда обновления прошивки PMC: PMC> update firmware pmc tftp <address> <filename> Обновление приватного ключа SSH: PMC> update key ssh tftp <address> <filename> **Важно!** Ключ должен быть предварительно сгенерирован и сохранён в формате .der.
version	Отображение текущей версии прошивки PMC.

Работа с заводскими параметрами

Version: 7.0.1
Product: NGFW
Documentation:

Данные параметры устанавливаются один раз —в ходе производственного тестирования. Далее параметры доступны только для чтения.

Для отображения параметров:

PMC> show factory

Укажите параметр, чтобы посмотреть его значение:

- sn —серийный номер устройства.
- type —тип устройства.
- mac — физический адрес (MAC-адрес).

Управление платформой

Version: 7.0.1
Product: UserGate NGFW
Documentation:

Данному разделу соответствует уровень конфигурации **platform**. Команды данного уровня позволяют управлять компонентами устройства UserGate.

Наименование	Описание
bypass	Команды управления выполняются на уровне **platform bypass**. Формат команды установки: PMC> set platform bypass <relay-number> <state> PMC> set platform bypass all <state> где <relay-number> - номер конфигурируемого реле. <state> - состояние реле. Возможны следующие значения: • **enable** - глобальная настройка; позволяет использовать функционал реле. При отключенном питании реле будут замкнуты. Значение сохраняется в энергонезависимой памяти (если реле выставлено в состояние **enable**, то после перезапуска устройства реле остаются замкнутыми, пока не будет отправлена команда на размыкание). • **disable** - глобальная настройка; значение сохраняется в энергонезависимой памяти (если реле выставлено в состояние **disable**, то после перезапуска устройства реле разомкнутся в процессе перезапуска PMC). • **on** - замыкание bypass реле (трафик идёт мимо процессора). Состояние сбрасывается после перезапуска. • **off** - размыкание bypass реле (трафик идёт через процессор). Состояние сбрасывается после перезапуска. Для вывода состояний реле используется следующая команда: PMC> show bypass
fan	Данный раздел находится на уровне **platform fan**. Команды данного раздела позволяют управлять режимом и производить мониторинг работы вентилятора охлаждения. Вентилятор может работать в двух режимах: автоматический и ручной. По умолчанию вентилятор работает в автоматическом режиме; скорость вращения регулируется в соответствии с показаниями температуры на процессоре. Для изменения режима работы вентилятора используется следующая команда: PMC> set platform fan mode <auto | manual> В ручном режиме доступно указание скорости вращения вентилятора; скорость выставляется в процентах: PMC> set platform fan speed <0 - 100> Команда для отображения текущего состояния: PMC> show platform fan
soc	Для запуска или остановки процессора необходимо выполнить команду: PMC> set platform soc <start | stop>
therm	Мониторинга температуры хост-процессора и платы производится на уровне **platform therm**. Для просмотра текущего состояния: PMC> show platform therm Для просмотра только значений температур хост-процессора и платы: PMC> show platform therm value
power	Раздел мониторинга источников питания производится на уровне **platform power**. Для отображения информации о рабочем состоянии источников питания используется команда: PMC> show platform power Также доступно указание следующих параметров: • **status** - состояние источников питания. • **measurements** - показания токов и напряжений. Следующая команда предназначена для включения/отключения всего питания, кроме дежурного, т.е. PMC продолжает работу: PMC> set platform power <on | off>

Для отображения информации о всех параметрах, доступных на данном уровне конфигурации:

PMC> show platform

Управление настройками сети

Documentation: ☑
Version: 7.0.1
Product: UserGate NGFW

Команды управления настройками сети доступны на уровне **network**. В данном разделе доступна установки и просмотр следующих параметров:

Наименование	Описание
ip	Статический IP-адрес устройства; значение по умолчанию: 192.168.1.2. Для выставления IP-адреса используется команда: PMC> set network ip <IP_adrress> Чтобы отобразить IP-адрес устройства: PMC> show network ip Также доступен сброс значения параметра до значения по умолчанию: PMC> delete network ip
netmask	Маска подсети; значение по умолчанию: 255.255.255.0. Команда изменения значения маски подсети: PMC> set network netmask <netmask_value> Для отображения текущего значения маски подсети: PMC> show network netmask Также доступен сброс значения параметра до значения по умолчанию: PMC> delete network netmask
gateway	Шлюз по умолчанию; значение по умолчанию: 192.168.1.1. Команда для изменения значения шлюза по умолчанию: PMC> set network gateway <gateway_address> Следующая команда предназначена для отображения текущего адреса шлюза по умолчанию: PMC> show network gateway Чтобы сбросить параметр до значения по умолчанию: PMC> delete network gateway
vlan	Идентификатор VLAN; значение по умолчанию - 0. Устройство получает все пакеты и при отправке не использует VLAN Tag. Если значение отлично от 0, то все пакеты, приходящие с тегом, отличным от выставленного, или без тега, фильтруются. При отправке в Ethernet-заголовок добавляется указанное значение параметра. Для изменения значения: PMC> set network vlan <VLANID_value> Для просмотра текущего значения: PMC> show network vlan Для установки значения по умолчанию: PMC> delete network vlan
arp	Таблица ARP-записей. По умолчанию таблица устройства пустая. При общении с другими узлами сети в таблицу добавляются динамические записи, которые имеют небольшое время жизни и после перезапуска устройства всегда сбрасываются. Существует возможность добавления статических ARP-записей. При добавлении необходимо указать IP и MAC. Если IP-адрес назначения присутствует в таблице, то при отправке пакета устройство не делает ARP-запрос, а сразу подставляет в Ethernet-заголовок MAC-адрес из таблицы. Для добавления статических ARP-записей: PMC> network arp <IP_address> <HW_address> Чтобы отобразить таблицу ARP: PMC> show network arp Следующая команда позволяет очистить таблицу: PMC> delete network arp Помимо очистки всей таблицы доступно удаление отдельной записи ARP; для удаления необходимо указать IP-адрес: PMC> delete network arp <IP_address>
ssh-port	Порт, использующийся для входящих подключений PMC SSH. Значение по умолчанию: 22. Для изменения порта подключения используется команда: PMC> set network ssh-port <port_number> Чтобы отобразить текущее значение параметра: PMC> show network ssh-port Чтобы вернуть значение параметра по умолчанию: PMC> delete network ssh-port

Чтобы отобразить значения всех параметров уровня **network**

PMC> show network

После изменения сетевые настройки хранятся в энергонезависимой памяти.

С использованием действия **delete** производится сброс параметров до значений по умолчанию (всех параметров или конкретного):

PMC> delete network

Управление пользователями

Version: 7.0.1
Product: NGFW
Documentation:

Команды управления пользователями доступны на уровне **users**. В данном разделе доступно создание и удаление пользователей, а также настройка методов авторизации на SSH-сервере. Устройство позволяет завести до 10 пользователей.

Для создания пользователя используется следующая команда:

PMC> create users <username>

Далее пользователю необходимо задать метод авторизации и пароль и/или публичный ключ. До задания метода авторизации пользователь не может быть использован.

По умолчанию всегда есть один пользователь **admin** с паролем по умолчанию **password**.

В качестве методов авторизации доступно использовать пароль и публичный ключ ECDSA. Для пользователя может быть задан один или сразу оба метода авторизации.

Чтобы задать авторизацию по паролю:

PMC> set users <username> password <password_value>

Для задания авторизации по публичному ключу ECDSA:

PMC> set users <username> key <public_key_type> <public_key>

Чтобы отключить один из способов авторизации, удалите ключ или пароль. Используйте команду с действием **delete**.

PMC> delete users <username> <password | key>

Для просмотра информации пользователях (всех или определённого); отображаются логин, метод авторизации, публичный ключ:

PMC> show users
PMC> show users <username>

Работа в режиме загрузчика

Version: 7.0.1
Product: NGFW
Documentation:

Режим загрузчика (PMC-loader) предназначен для обеспечения возможности восстановления работоспособности программно-аппаратного комплекса.

ПримечаниеРежим загрузчика доступен только при подключении через консольный порт.

Для перехода в данный режим необходимо нажать клавишу **Enter** во время вывода следующей строки:

Hit 'Enter' key to stop autoboot: 3

Строка приглашения будет выглядеть следующим образом:

loader>

ПримечаниеВ режиме загрузчика работает таймер неактивности. Если в течении 45 секунд выполнение команд не производилось, то устройство будет перезагружено.

В данном режиме набор доступных команд ограничен. Доступны следующие команды:

- настройка сети без сохранения параметров;
- просмотр версии и factory-параметров;
- отображение уровней напряжений, температуры;
- обновление ПО.

Дашборд

Приборная панель (DashBoard)

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Данный раздел позволяет посмотреть текущее состояние NGFW, его загрузку, количество пользователей, объемы трафика, проходящего через NGFW, работу систем фильтрации, статус лицензии и так далее. Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами NOC (Network Operation Center) и SOC (Security Operation Center).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображаться в Дашборд.
Описание	Опциональное описание виджета.
Количество записей	Максимальное количество записей для отображения.
Группировать по	Поле данных, по которому будут сгруппированы данные в виджете.
Диаграмма	Выбор типа представления данных. Доступны значения: • Число. • Круговая диаграмма. • Вертикальная гистограмма. • Горизонтальная гистограмма. • Таблица. • График. • Карта мира.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных.

ПримечаниеДоступно использование выделения для более подробного ознакомления с определённой частью графика; для возвращения необходимо использовать двойной клик левой кнопкой мыши.

Диагностика и мониторинг

описание

Мониторинг трафика

Product: NGFW
Version: 6.1.9, 7.0.1
Documentation:

Раздел **Мониторинг трафика** позволяет получить список всех пользовательских соединений, установленных через NGFW в реальном времени. Соединением считается уникальное сочетание адреса источника, адреса назначения и пользователя (если определен). Для каждого соединения отображаются мгновенные значения скорости передачи (TX) и скорости приема (RX). Имеется возможность сортировки выводимых данных по каждому столбцу, а также возможность создать блокирующее правило межсетевого экрана или правило ограничения пропускной способности для выбранного из списка IP-адреса источника.

ПримечаниеПроцесс построения данного отчета требует большего количества вычислительных ресурсов NGFW и при большом объеме передаваемого трафика может приводить к высокой загрузке процессора. Не рекомендуется держать данную страницу открытой во избежание излишней нагрузки на МЭ.

Маршруты

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Раздел **Маршруты** позволяет получить список всех маршрутов, указанных на определенном узле UserGate и на определенном виртуальном маршрутизаторе на узле кластера. Для просмотра маршрутов необходимо нажать на кнопку **Фильтр** и указать типы маршрутов, которые необходимо отобразить. Возможно указать следующие типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **C** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **K** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **O** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **B** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

VPN

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Раздел **VPN** отображает всех пользователей и все серверы, подключенные по VPN к данному серверу. Для каждого соединения отображается следующая информация:

- **Пользователь** — имя пользователя, под которым произошла аутентификация соединения.
- **Роль этого сервера** — клиент или сервер.
- **Время сессии** — продолжительность установленного соединения.
- **Туннельный IP** — адрес, назначенный данному клиенту в виртуальной частной сети.
- **IP-адрес** — адрес, с которого инициировано соединение VPN.
- **Geo IP** — страна по Geo IP, откуда установлено соединение.
- **Шифрование** — тип шифрования

Веб-портал

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1

Раздел **Веб-портал** отображает всех пользователей и все серверы, подключенные через веб-портал к данному серверу. Для каждого соединения отображается следующая информация:

- **Имя** — имя пользователя, под которым произошла аутентификация соединения.
- **Начало сессии** — время, когда пользователь подключился к сервису.
- **Продолжительность** — продолжительность соединения.
- **IP источника** — IP-адрес пользователя.
- **Useragent** — useragent пользовательского браузера.

Можно задать период обновления данного окна от 3-х секунд до одной минуты или установить обновление вручную.

Администратор имеет возможность принудительно закрыть определённую сессию. Для этого надо выделить её и нажать кнопку **Закрыть** сессию.

Захват пакетов

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Раздел **Захват пакетов** позволяет записать трафик, удовлетворяющий заданным условиям, в pcap-файл для дальнейшего анализа с помощью сторонних средств, например, wireshark. Это бывает необходимо для диагностирования сетевых проблем.

Раздел состоит из трех частей:

- **Фильтры** — здесь определяются условия, по которым будет записываться трафик. В качестве условий могут выступать адрес источника, порт источника, адрес назначения, порт назначения, протокол Ethernet, протокол IPv4. Список протоколов IPv4 можно посмотреть по ссылке http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.
- **Правила** — в правилах указываются интерфейсы UserGate, на которых необходимо записывать трафик, фильтры, созданные ранее, имя и размер файла, в который записывается перехваченный трафик.
- **Файлы** — сюда помещаются файлы с записанным трафиком. Их можно скачать для анализа или удалить.

Чтобы записать трафик, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать необходимый фильтр.	Опционально. Можно воспользоваться предустановленными фильтрами или писать весь трафик, не фильтруя его.
Шаг 2. Создать правило.	Создать правило, в котором указать имя правила, имя файла, максимальный размер записываемого файла и необходимые фильтры.
Шаг 3. Выбрать необходимое правило и начать запись.	Выбрать необходимое правило и нажать на кнопку **Начать запись**. По окончании прекратить запись, нажав на кнопку **Остановить запись.**
Шаг 4. В разделе **Файлы**, скачать полученный файл.	Скачать pcap-файл для анализа.

Запросы в белый список

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

При блокировке сайтов с помощью правил контентной фильтрации пользователь получает страницу блокировки с указанием причины блокировки, на которой указаны имя правила, категория сайта и/или морфологическая база, черный список, из-за которых сайт был заблокирован. Кроме этого, страница блокировки предлагает пользователю сделать запрос на добавление данного сайта в белый список в случае, если пользователь не согласен с блокировкой ресурса. При нажатии на кнопку **Добавить в белый список** запрос на добавление появляется в списке запросов в разделе **Запросы в белый список**. Администратор может осуществить следующие действия с запросом пользователя:

Наименование	Описание
Добавить в белый список	Добавить данный URL в белый список. Администратору будет предложено изменить URL и выбрать белый список, в который необходимо добавить данный ресурс.
Удалить	Удалить данный запрос из списка запросов.
Отклонить URL	Добавить запрошенный URL в список отклоненных запросов. При последующих блокировках данного URL страница блокировки не будет содержать кнопки **Добавить в белый список**. Список отклоненных доменов и URL отображается в **Окне отклоненных запросов.**
Отклонить домен	Добавить домен запрошенного URL в список отклоненных запросов. При последующих блокировках любого URL данного домена страница блокировки не будет содержать кнопки **Добавить в белый список**. Список отклоненных доменов и URL отображается в **Окне отклоненных запросов.**

Администратор может проверить категорию интернет-ресурса с помощью формы **Проверить URL**. В случае, если ресурс относится к некорректной категории, администратор может сделать запрос на смену категории или изменить категорию самостоятельно локально на своем устройстве.

Для того, чтобы сделать запрос на смену категории, необходимо нажать на кнопку **Предложить категорию**. Запрос на смену категории будет отправлен в компанию UserGate, где будет проверен, и в случае подтверждения будет внесен в ближайшее обновление базы категорий сайтов UserGate URL filtering.

Для того, чтобы сменить категории локально, необходимо нажать на кнопку **Изменить категорию** и назначить до двух новых категорий. Посмотреть все сайты с измененными категориями можно в разделе **Библиотеки → Измененные категории URL.** При последующей проверке категорий для данного сайта в качестве категорий будут возвращены только новые категории и специальная категория, в которую включаются все сайты с измененными категориями - **Переопределенные пользователем категории**. Более подробно об изменении категорий для определенных сайтов описано в разделе руководства Запросы в белый список.

Трассировка правил

Product: NGFW
Version: 6.1.9, 7.0.1
Documentation:

С помощью трассировки правил администратор может посмотреть, какие правила срабатывают при обработке пользовательских HTTP(S)-запросов. Это может быть крайне полезно при определении проблем с доступом к определенным сайтам. Для трассировки правил необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать необходимый фильтр.	Нажать на кнопку **Настроить** в разделе **Диагностика и мониторинг → Трассировка правил** и указать параметры фильтра: • **Строка** — строка в запросе пользователя, например, имя домена, URL, правила контентной фильтрации. • **Пользователь** — пользователь, обработку запросов которого необходимо продиагностировать. • **IP-адрес источника** — IP-адрес, с которого пользователь осуществляет запрос. Фильтр необходим для ограничения вывода диагностической информации. Если его не задать, то могут быть также отображены результаты обработки запросов других пользователей.
Шаг 2. Запустить трассировку.	Нажать на кнопку **Начать.**
Шаг 3. Открыть проблемный сайт.	Попросить пользователя открыть проблемный сайт и наблюдать, какие правила срабатывают при открытии сайта. Будут указаны все правила, которые выполняются во время обработки пользовательского запроса.

ПримечаниеПри трассировке отображаются сработавшие правила ICAP, инспекции SSL и контентной фильтрации.

Администратор может проверить содержание отображаемого в трассировке Интернет-ресурса с помощью формы **Открыть сайт**. С помощью формы **Добавить в белый список** администратор может поместить выбранный ресурс в один из существующих в системе списков URL.

Ping

Documentation: ☑
Product: NGFW, UGMC, LogAn, SIEM
Version: 5.x, 6.1.9, 7.0.1

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить.
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации.
Счетчик	Количество повторов.
Показывать timestamp	Добавляет timestamp в вывод команды.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

Documentation: ☑
Product: NGFW, UGMC, LogAn, SIEM
Version: 5.x, 6.1.9, 7.0.1

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	С какого сетевого интерфейса выполнять команду.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

Documentation: ☑
Product: NGFW, UGMC, LogAn, SIEM
Version: 5.x, 6.1.9, 7.0.1

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	DNS сервер, куда посылать запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

LLDP соседи

Documentation: ☑
Product: NGFW
Version: 7.0.1

Данный раздел отображает список LLDP-совместимых устройств, на которых включена поддержка объявления LLDP.

Наименование	Описание
Chassis ID	Идентификатор шасси; является обязательной TLV-записью LLDP-кадра. У каждого устройства UserGate есть только один Chassis ID. В качестве Chassis ID используется MAC-адрес интерфейса управления.
SysName	Имя системы.
SysDescr	Описание системы, содержит информацию об оборудовании и операционной системе устройства.
Management	Адрес соседнего устройства. Содержит информацию: • IP-адреса интерфейса управления (IPv4 и IPv6). • Номер интерфейса указанного адреса управления.
Capability	Функции устройства (например, маршрутизатор, коммутатор и т.п.).
Port ID	Идентификатор порта, с которого был передан LLDPDU (Link Layer Discovery Protocol Data Unit); является обязательной TLV-записью LLDP-кадра. В качестве идентификатора используется MAC-адрес интерфейса.
PortDescr	Описание порта.
TTL	Время жизни передаваемых пакетов LLDP; является обязательной TLV-записью LLDP-кадра. TTL задаётся в разделе **UserGate → Настройки → Модули** в поле **Настройка LLDP**.

Статистика LLDP

Documentation: ☑
Product: NGFW
Version: 7.0.1, 7.1.0

Данная вкладка отображает статистику интерфейсов, в настройках которых был указан профиль LLDP. Отображается следующая информация:

Наименование	Описание
Interface	Название интерфейса.
Transmitted	Общее количество кадров LLDP, переданных через интерфейсе.
Received	Общее количество кадров LLDP, полученных на интерфейсе.
Discarded	Число полученных на этом интерфейсе кадров LLDP, которые были отброшены.
Unrecognized	Количество кадров LLDP с неподтверждённым содержимым, полученных на этом интерфейсе.
Ageout	В каждом кадре LLDP содержится информация о том, насколько долго является правильной информация LLDP (срок старения). Если в течение срока старения новых кадров не принято, информация LLDP удаляется.
Inserted	Количество добавлений записей с информацией о соседях LLDP.
Deleted	Количество удалений записей о соседях LLDP.

Оповещения

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Правила оповещений

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или отправке пароля пользователю по SMS. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещения.	Смотрите раздел Профили оповещений.
Шаг 2. Создать группы получателей оповещений.	Смотрите разделы Почтовые адреса и Номера телефонов.
Шаг 3. Создать правило оповещения.	Во вкладке **Диагностика и мониторинг** в разделе **Оповещения → Правила оповещений** добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.
От	От кого будет приходить оповещение.
Тема	Тема оповещения.
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

SNMP

Documentation: ☑
Product: UserGate NGFW
Version: 6.1.9, 7.0.1

UserGate NGFW поддерживает мониторинг по протоколам SNMP v2c и SNMP v3. Реализована поддержка как SNMP-запросов (SNMP queries), так и уведомлений (SNMP traps), что позволяет контролировать критически важные параметры устройства с помощью корпоративных платформ SNMP-мониторинга.

Для настройки мониторинга с помощью SNMP:

1. Откройте доступ к сервису SNMP в свойствах зоны интерфейса, к которому будет происходить подключение по протоколу SNMP.
2. Создайте правило SNMP.

Для создания правила SNMP перейдите в раздел **Диагностика и мониторинг → Оповещения → SNMP**, нажмите **Добавить** и укажите значения параметров правила.

Параметр	Описание
Название правила	Название правила
IP-адрес сервера для трапов	IP-адрес сервера для уведомлений и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять уведомления (SNMP traps) на сервер оповещений
Комьюнити	SNMP community — строка для идентификации устройства UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию
Версия	Версия протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMP v2c и SNMP v3
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации SNMP-менеджера
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv
Алгоритм аутентификации	Алгоритм, используемый для аутентификации
Пароль аутентификации	Пароль, используемый для аутентификации
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES
Пароль шифрования	Пароль, используемый для шифрования
События	Выбор типов параметров, доступных для мониторинга по правилу

ПримечаниеНастройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования) на SNMP-менеджере должны совпадать с соответствующими параметрами SNMP на устройстве.

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

Актуальные mib-файлы устройства UserGate с параметрами мониторинга можно скачать из консоли администратора устройства. Для этого перейдите на вкладку **Диагностика и мониторинг**, далее в разделе **Оповещения → SNMP** нажмите **Скачать MIB**.

Компании UserGate присвоен уникальный идентификатор SNMP PEN (Private Enterprise Number) — 45741.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.
- UTM-TRAPS-BINDINGS-MIB.
- UTM-MIB.
- UTM-INTERFACES-MIB.

UTM-TRAPS-MIB

Параметр	Описание
trapCoreCrush	Сбой ядра

Параметр	Описание
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен
trapCoreBootstrapEnd	Загрузка сервера завершена успешно
trapDefaultGatewayChanged	Изменение шлюза по умолчанию
trapHighSessionsCounter	Таблица сессий заполнена на 90%
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен»
trapMemberDown	Узел отказоустойчивого кластера отключен
trapAttackDetected	Обнаружена атака СОВ
trapChecksumFailed	Нарушение целостности бинарных файлов
trapHighCPUUsage	Высокая загрузка центрального процессора (95%)
trapLowMemory	Высокая загрузка памяти (95%)
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов
trapRaidStatus	Изменение статуса RAID
trapPowerSupply	Первый источник питания отключен
trapCableStatus	Кабель был подключен или отключен от интерфейса
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана
trapLDAPServerDown	Сервер LDAP недоступен

UTM-TRAPS-BINDINGS-MIB

Параметр	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий
utmSessionsMax	integer	Максимальное количество активных сессий
utmUsers	integer	Количество активных пользователей на данный момент
utmUsersMax	integer	Максимальное количество активных пользователей
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • 0 — мастер-узел; • 1 — резервный узел; • 3 — ошибка
utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • 1 — связь с узлом потеряна; • 2 — прокси-сервер HTTP недоступен; • 3 — все шлюзы недоступны; • 4 — DNS-сервер недоступен; • 5 — UserGate Management Center недоступен
utmCPUUsage	integer	Загруженность центрального процессора; отображается в %
utmMemory	integer	Использование оперативной памяти; отображается в %
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %

Параметр	Тип данных	Описание
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • no_raid; • 0 — optimal, массив в оптимальном состоянии; • 1 — degraded, полный или частичный выход из строя одного из дисков; • 2 — rebuild, восстановление массива
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • no_raid; • 0 — optimal, массив в оптимальном состоянии; • 1 — degraded, полный или частичный выход из строя одного из дисков. Переход в данный статус произойдет при выходе из строя 2-х дисков; • 2 — partialDegraded, полный или частичный выход из строя одного из дисков; • 3 — failed, не работает из-за наличия ошибки; • 4 — offline, диск не доступен для RAID-контроллера
utmPowerSupply	integer	Количество источников питания: • 1 — один блок питания; • 2 — два блока питания
utmPowerSupplyStatus	integer	Состояние источника питания: • no_power_supplies; • 0 — off, отключен; • 1 — on, включен
utmCSCIfName	string	Название интерфейса
utmCSCStatus	integer	Статус сетевого адаптера: • 0 — unplugged, кабель не подключен; • 1 — plugged, кабель не подключен
utmLDAPServerName	string	Название LDAP-сервера
utmLDAPServerAddress	string	IP-адрес LDAP-сервера

UTM-MIB

Параметр	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается фактическое число загруженных виртуальных процессоров
usersCounter	integer	Количество активных пользователей на текущий момент времени
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %
memoryUsed	integer	Использование оперативной памяти; отображается в %
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %
Sys_power_supply1_status	string	Состояние первого источника питания: • no_power_supplies; • on, подключен; • off, отключен
Sys_power_supply2_status	string	Состояние второго источника питания: • no_power_supplies; • on, подключен; • off, отключен
Sys_raid_status	integer	Текущий статус RAID (Redundant Array of Independent Disks): • no_raid; • 0 — optimal, массив в оптимальном состоянии; • 1 — degraded, полный или частичный выход из строя одного из дисков; • 2 — rebuild, восстановление массива

UTM-INTERFACES-MIB

Параметр	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber
ifDescr	string	Описание интерфейса
ifType	integer	Тип интерфейса, определенный в соответствии с протоколом физического/канального уровней: • 1 — other, неизвестный тип; • 2 — regular1822, определен в BBN Report 1822; • 3 — hdh1822, определен в BBN Report 1822; • 4 — ddn-x25, определен в BBN Report 1822; • 5 — rfc877-x25, определен в стандарте канального уровня сетевой модели OSI X.25; • 6 — ethernet-csmacd, сетевой интерфейс типа Ethernet, независимо от скорости (определен в RFC 3635); • 7 — iso88023-csmacd, определен в IEEE 802.3; • 8 — iso88024-tokenBus, определен в стандарте IEEE 8802.4; • 9 — iso88025-tokenRing, сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5; • 10 — iso88026-man, определен в стандарте ISO 88026 "MAN"; • 11 — starLan, определен в стандарте IEEE 802.3e; • 12 — proteon-10Mbit, Proteon 10 Mbit; • 13 — proteon-80Mbit, Proteon 80 Mbit; • 14 — hyperchannel, высокоскоростной канал, используемы в сети ISDN; • 15 — fddi, сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети; • 16 — lapb, протокол канального уровня, используемым для передачи пакетов стандарта X.25; • 17 — sdlc, протокол канального уровня для системной сетевой архитектуры IBM; • 18 — ds1, способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1; • 19 — e1, европейский аналог T1; • 20 — basicISDN, для связи аппаратуры абонента и ISDN-станции; • 21 — primaryISDN, используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы; • 22 — propPointToPointSerial, определен в стандарте RFC1213; • 23 — ppp, сетевой интерфейс использует подключение PPP (Point-To-Point Protocol); • 24 — softwareLoopback, сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть; • 25 — eon, ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определен в ISO/IEC 8473-1; • 26 — ethernet-3Mbit, сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895; • 27 — nsip, XNS over IP. Предназначен для использования в разнообразных средах передачи данных; • 28 — slip, сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055; • 29 — ultra,-ULTRA Technologies; • 30 — ds3, высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3; • 31 — sip, етевой интерфейс использует протокол для высокоскоростной передачи данных SMDS (Switched Multimegabit Data Service). SMDS определяется в стандарте IETF RFC 1694; • 32 — frame-relay, обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду. Максимальное значение — 4 294 967 295 (≈ 4,29 Гбит/с). Рекомендуется использовать для интерфейсов со скоростью до 4,29 Гбит/с, когда требуется высокая точность
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес)
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • 1 — up, готов для передачи пакетов; • 2 — down, не работает; • 3 — testing, в режиме тестирования; рабочие пакеты не могут быть переданы

Параметр	Тип данных	Описание
ifOperStatus	integer	Текущий статус работы интерфейса: • 1 — up, интерфейс готов для передачи пакетов; • 2 — down, интерфейс не может передавать пакеты данных; • 3 — testing, выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы; • 4 — unknown, интерфейс находится в неизвестном состоянии; • 5 — dormant, сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие; • 6 — notPresent, сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного; • 7 — lowerLayerDown, сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов нижнего уровня не работает
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки
fInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передачи. Одна из возможных причин отбрасывания: освобождение буферного пространства
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок
ifOutQLen	gauge32	Число пакетов в очереди на отправку
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены
ifHCInOctets	counter64	Параметр, аналогичный ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счетчик большей емкости
ifHCInUcastPkts	counter64	Параметр, аналогичный ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счетчик большей емкости
ifHCInMulticastPkts	counter64	Параметр, аналогичный ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счетчик большей емкости
ifHCInBroadcastPkts	counter64	Параметр, аналогичный ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счетчик большей емкости
ifHCOutOctets	counter64	Параметр, аналогичный ifOutOctets — количество байтов, переданное данным интерфейсом, включая служебные; используется счетчик большей емкости
ifHCOutUcastPkts	counter64	Параметр, аналогичный ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
ifHCOutMulticastPkts	counter64	Параметр, аналогичный ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
ifHCOutBroadcastPkts	counter64	Параметр, аналогичный ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счетчик большей емкости
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • 1 — enabled — включено; • 2 — disabled — отключено
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса в Мбит/с. Округление до целых Мбит/с (теряется точность для скоростей < 1 Мбит/с). Рекомендуется применять для высокоскоростных интерфейсов

Параметр	Тип данных	Описание
ifPromiscuousMode	integer	«Неразборчивый режим». Возможные значения: • 1 — true, станция принимает все пакеты/кадры независимо от того, кому они адресованы; • 2 — false, интерфейс принимает только пакеты/кадры, адресованные этой станции; Значение объекта не влияет на прием широковещательных и многоадресных пакетов/кадров
ifAlias	string	Название интерфейса, заданное администратором
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счетчиков интерфейса

Журналы и отчеты

Журналы

Описание

Version: 5.x, 6.1.9, 7.0.1
Documentation: ☑

UserGate журналирует все события, которые происходят во время его работы, и записывает их в следующие журналы:

- **Журнал событий** — события, связанные с изменением настроек NGFW, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных NGFW.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing.
- **Журнал СОВ** — события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал АСУ ТП** — события, регистрируемые правилами контроля систем АСУ ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — поисковые запросы пользователей в популярных поисковых системах.

Управление журналами автоматизировано: журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

ПримечаниеЗаписи журнала событий никогда не ротируются.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных будут отображены в журнале событий. В случае, если подключен LogAn, то запись будет отображена в журнале событий Log Analyzer.

Журнал событий

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1
Product: NGFW

Журнал событий отображает события, связанные с изменением настроек NGFW, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал или VPN, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал веб-доступа

Version: 7.0.1
Product: NGFW
Documentation:

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL, Веб-безопасности, Captive-портала в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Категории сайтов.
- Приложение.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Тип контента (если присутствует).
- Информация.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Операционная система.
- User-agent браузер.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

ПримечаниеКогда NGFW версии 7.0.x. не интегрирован с внешним узлом LogAn, события срабатывания правил на DNS-запросы отображаются в его журнале веб-доступа. Если NGFW версии 7.0.x, подключен к LogAn версии 7.1.x, то на самом NGFW в журнале веб-доступа dns-запросы отображаться не будут. При этом на LogAn эти запросы отобразятся в отдельном журнале DNS.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал трафика

Version: 7.0.1
Product: NGFW
Documentation: ☑

Журнал трафика отображает события срабатывания правил межсетевого экрана и правил NAT, в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.
- NAT IP-адрес источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP-адрес назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов отправлено/получено.

ПримечаниеВ столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик, учтенный в момент срабатывания журналирующего правила.
Если в настройках журналирования в правиле выбрано: "Журналировать каждый пакет", то значения учтенного трафика в журнале будут кумулятивно нарастать в течение сессии.
Если в настройках журналирования в правиле выбрано: "Журналировать начало сессии", будет учтен всего один или несколько пакетов, необходимых для срабатывания этого правила.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал СОВ

Version: 7.0.1
Product: NGFW, LogAn
Documentation: ☑

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры СОВ, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Файлы Pcap.
- Узел NGFW, на котором произошло событие.
- Время.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Сигнатуры.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал АСУ ТП

Version: 6.1.9, 7.0.1
Product: NGFW, LogAn
Documentation: ☑

Журнал АСУ ТП отображает срабатывания правил автоматизированной системы управления технологическим процессом, для которых включена функция журналирования. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP-адрес источника.
- IP-адрес назначения.
- Порт назначения.
- Протокол АСУ ТП.
- Команда АСУ ТП.
- Адрес регистра.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал инспектирования SSH

Version: 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH, для которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время.
- Пользователь.
- Действие.
- Правило.
- Команда.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

История поиска

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation:

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Поиск и фильтрация данных

Version: 7.0.1
Product: NGFW
Documentation: ☑

Количество записей, регистрируемых в журналах, как правило, очень велико, и не все поля доступны в базовом режиме просмотра. NGFW предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31 будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date<='2019-03-28T20:59:59' AND statusCode=303
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date>="2019-03-13T21:00:00" AND statusCode=200
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, date < '2019-03-28T20:59:59' AND statusCode=404
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, (statusCode>200 AND statusCode<300) OR (statusCode=404)
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, несодержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, browser ~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, browser !~ "Mozilla/5.0" Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details MATCH '\"module\":\"threats\"' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, details NOT MATCH '\"module\":\"threats\"' Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

При составлении расширенного запроса NGFW показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. Список полей и их возможных значений может отличаться для каждого из журналов.

При переключении режима поиска с основного на расширенный NGFW автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме

поиска.

Экспорт журналов

Version: 5.x, 6.1.9, 7.0.1
Product: NGFW
Documentation: ☑

Функция экспортирования журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал СОВ.
- Журнал трафика.
- Журнал АСУ ТП. (в версиях 6+)
- Журнал инспектирования SSH. (в версиях 6+)

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

ПримечаниеЕсли в настройках указан Log Analyzer, то обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал событий. • Журнал веб-доступа. • Журнал СОВ. • Журнал трафика. • Журнал АСУ ТП. • Журнал инспектирования SSH. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в Приложение 3. Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog -- RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Тревога**: состояние, требующее незамедлительного вмешательства. • **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: в системе возникли ошибки. • **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками. • **Информативная**: информационные сообщения.

Наименование	Описание
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • **Сообщения пользовательские**. • **Системный сервис**. • **Безопасность/авторизация**. • **Аудит**. • **Тревога**. • **Local 0**. • **Local 1**. • **Local 2**. • **Local 3**. • **Local 4**. • **Local 5**. • **Local 6**. • **Local 7**.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки. Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.

Отчеты

Описание

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел **Отчеты** состоит из трех подразделов — **Шаблоны**, **Правила отчётов** и **Созданные отчеты**. Чтобы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета.	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет.	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет.	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе **Созданные отчеты.**

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.
ПримечаниеВ отчетах по трафику (кроме отчетов веб-доступа) используются данные из компонента Netflow. Отчеты веб-доступа по трафику используют данные из журналов (домены, URL-категории и т.п.).

Шаблоны отчетов

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией-разработчиком UserGate.

Список шаблонов отчетов, сгруппированных по категориям:

- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** — группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Сетевая активность** — группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** — группа шаблонов авторизации через SSL VPN.
- **Трафик** — группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **VPN** -- группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

Правила отчетов

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Включено	Включение/отключения отчета.
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. **Важно!** Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Для шаблонов **Подробный список всех посещенных URL** и **Подробный список всех посещенных сайтов** автоматически используется формат CSV, независимо от выбранного формата.
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задает пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.
Расписание	Выбор расписания для создания отчетов. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7 • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23" Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа.
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: • Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. • От — имя отправителя письма. • Тема письма — тема письма (subject). • Тело письма — содержимое письма. • Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки **Почтовые адреса**.

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

ПримечаниеДля того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку Запустить сейчас. Готовый отчет после создания будет доступен в разделе Созданные отчеты.

Гостевой портал

Управление гостевыми пользователями

Documentation: ☑
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1

NGFW позволяет создавать списки гостевых пользователей. Данная возможность может быть полезна для гостиниц, публичных Wi-Fi, сетей интернет, где необходимо идентифицировать пользователей и предоставить им доступ на ограниченное время.

Гостевые пользователи могут быть созданы заранее администратором системы или пользователям может быть предоставлена возможность самостоятельной регистрации в системе с подтверждением через SMS или email.

Для создания списка гостевых пользователей администратором необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать администратора гостевых пользователей (опционально).	• В разделе **Администраторы** нажать кнопку **Добавить** и создать профиль администратора, разрешающий **Гостевой портал** для чтения и записи в закладке **Разрешения для веб-консоли**. Данный профиль дает доступ в консоль управления временными пользователями. • Создать учетную запись администратора и назначить ей созданную роль. Более подробно о создании администраторов NGFW смотрите соответствующий раздел руководства.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа гостевых пользователей.	В консоли NGFW в разделе **Группы** нажать на кнопку **Добавить** и создать группу, отметив поле **Группа для гостевых пользователей.** Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Подключиться к консоли управления Гостевого портала.	В браузере перейти на адрес https://IP_NGFW:8001/ta Для авторизации необходимо использовать логин и пароль администратора устройства или администратора гостевых пользователей, созданного на шаге 1.
Шаг 4. Создать список пользователей.	В консоли нажать на кнопку **Добавить** и заполнить поля: • Количество пользователей. • Комментарий. • **Дата и время окончания** — время, когда учетная запись гостевого пользователя будет отключена. • **Длина пароля** — определяет длину пароля для создаваемого пользователя. • **Сложность пароля** — определяет сложность пароля для создаваемого пользователя. Возможны варианты: • Цифры. • Буквы + цифры. • Буквы + цифры + спецсимволы. • **Время жизни** — продолжительность времени с момента первой авторизации гостевого пользователя, по истечении которого учетная запись будет отключена. • **Группа** — созданная на шаге 2 группа, в которую будут помещены создаваемые пользователи.

Список созданных пользователей можно посмотреть в разделе **Пользователи** консоли управления временными пользователями.

Для самостоятельной регистрации пользователей в системе необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать профиль оповещения SMPP (для подтверждения через SMS) или SMTP (для подтверждения через email).	В разделе **Библиотеки → Профили оповещений** нажать кнопку **Добавить** и создать профиль оповещения SMPP или SMTP. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений.
Шаг 2. Создать группу, в которую будут помещены гостевые пользователи. Группа необходима для удобства управления политиками доступа временных пользователей.	В консоли NGFW в разделе **Группы** нажать на кнопку **Добавить** и создать группу, отметив поле **Группа для гостевых пользователей.** Более подробно о создании групп пользователей смотрите соответствующий раздел руководства.
Шаг 3. Создать профиль Captive-портала, в котором указать использование профиля оповещений, для отсылки информации о созданной учетной записи.	В разделе **Пользователи и устройства** в подразделе **Captive-профили** создать профиль, указав в нем использование созданного ранее профиля оповещения. Указать в качестве страницы авторизации шаблон **Captive portal: email auth** или **Captive portal: SMS auth,** в зависимости от способа отправки оповещения. Настроить сообщение оповещения, группу, в которую будут помещены временные пользователи, времена действия учетной записи. Более подробно о создании профилей оповещения смотрите раздел руководства Профили оповещений.
Шаг 4. Создать правило Captive-портала, которое будет использовать созданный на предыдущем шаге Captive-профиль.	В разделе **Пользователи и устройства → Captive-портал** создать правило, которое будет использовать созданный ранее Captive-профиль. Более подробно о создании правил Captive-портала смотрите раздел руководства Настройка Captive-портала.

Помощь

Помощь(Описание)

Documentation: ☑
Product: NGFW
Version: 7.0.1

Раздел предоставляет ссылки на полезные ресурсы портала технической поддержки UserGate:

Наименование	Описание
Помощь	Ссылка на актуальную версию руководства администратора.
Обучающее видео	Ссылка на список видеороликов, объясняющих настройку различных служб UserGate.
Поддержка	Ссылка на портал службы технической поддержки UserGate на сайте компании https://www.usergate.com/ru/support содержит дополнительную информацию по настройке UserGate. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.

ADMIN

ADMIN (описание)

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1

Данный раздел позволяет зарегистрированному администратору сменить свой пароль, изменить некоторые настройки профиля и выйти из системы.

Наименование	Описание
Сменить пароль	Для смены пароля необходимо указать свой текущий пароль и два раза указать новый пароль.
Предпочтения	• Количество элементов на странице — устанавливает количество строк, отображаемых в одном диалоговом окне, например, список правил межсетевого экрана. • Популярные фильтры — изменение названия или удаление фильтров различных журналов, созданных данным пользователем.
Выход	Завершение сеанса работы в веб-консоли устройства.

Приложения

Установка сертификата локального удостоверяющего центра

Documentation: ☑
Product: NGFW
Version: 6.1.9, 7.0.1, 7.1.0

Скачайте сертификат центра авторизации, который вы используете для перехвата HTTPS-трафика, как это описано в главе Управление сертификатами, и следуйте инструкциям по установке сертификата ниже в этом разделе.

Установка сертификата в браузеры Internet Explorer, Chrome в ОС Windows

Откройте папку, куда вы скачали pem-сертификат, переименуйте его в user.der и дважды нажмите на него:

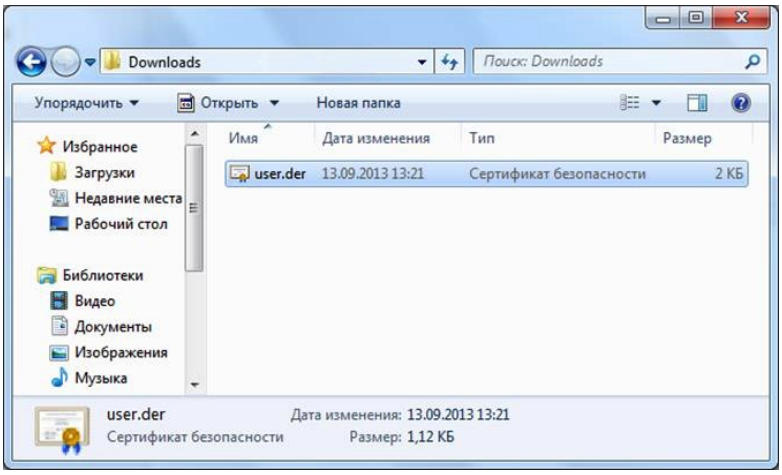


Рисунок 5 Выбор файла сертификата

Откроется информация о сертификате. Нажмите на кнопку **Установить сертификат**:

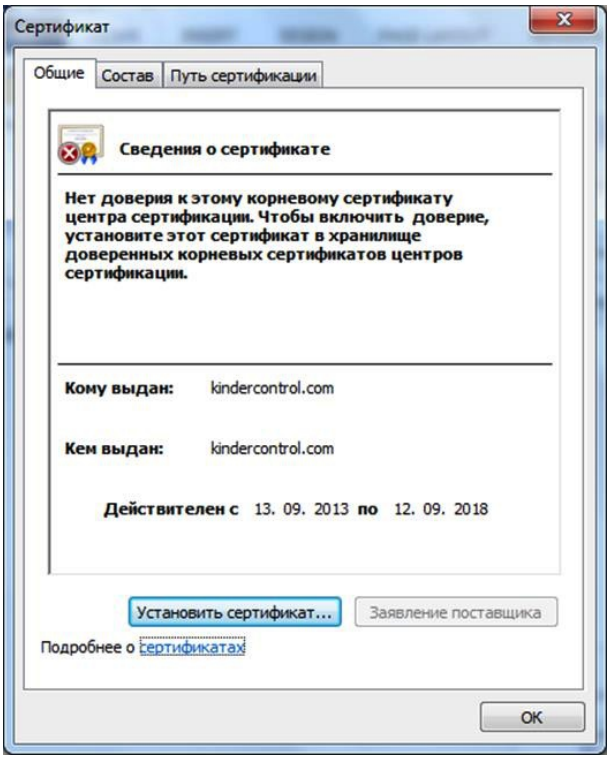


Рисунок 6 Установка сертификата

Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:

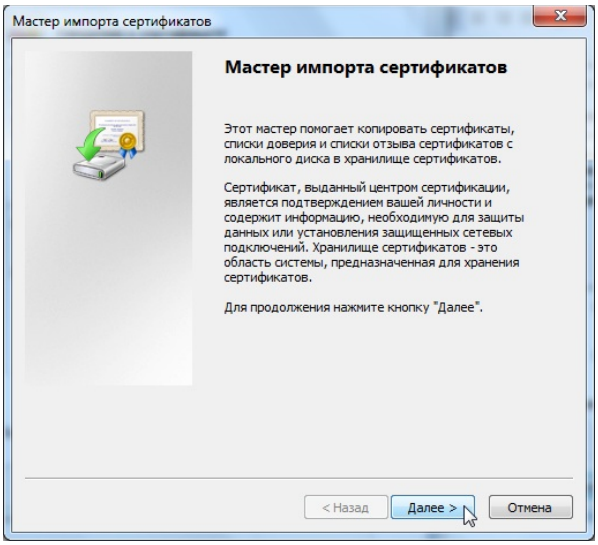


Рисунок 7 Мастер импорта сертификатов

Выберите хранилище сертификата и нажмите кнопку **Обзор**:

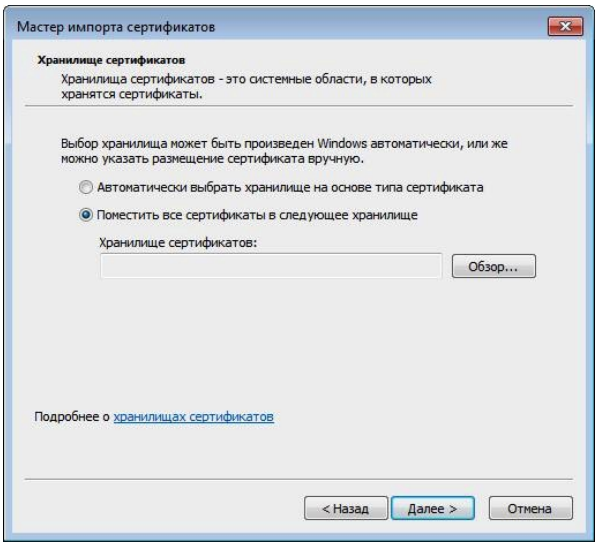


Рисунок 8 Выбор хранилища

Выберите **Доверенные корневые центры сертификации** и нажмите кнопку **ОК**:

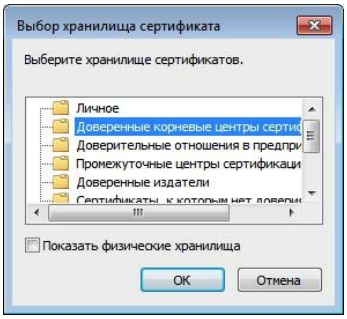


Рисунок 9 Выбор хранилища (продолжение)

Нажмите кнопку «Готово»:

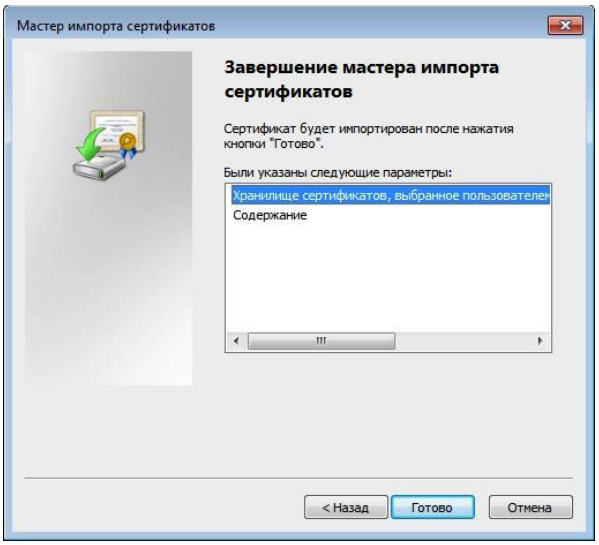


Рисунок 10 Завершение импорта

Когда появится предупреждение системы безопасности, нажмите кнопку **Да**:

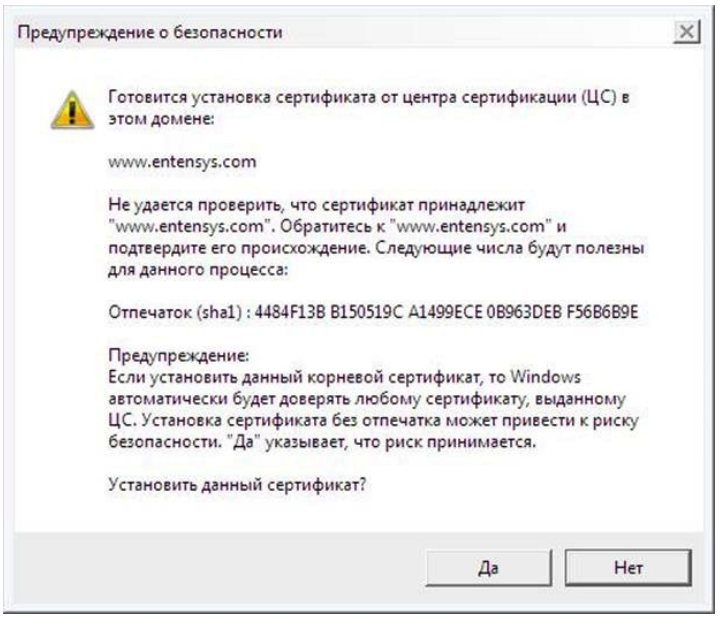


Рисунок 11 Согласие на установку сертификата

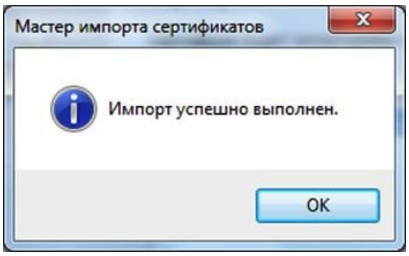


Рисунок 12 Установка завершена

Установка сертификата завершена.

Установка сертификата в браузер Safari, Chrome в ОС MacOSX

Перейдите в папку, куда вы скачали pem-сертификат и дважды нажмите на него:

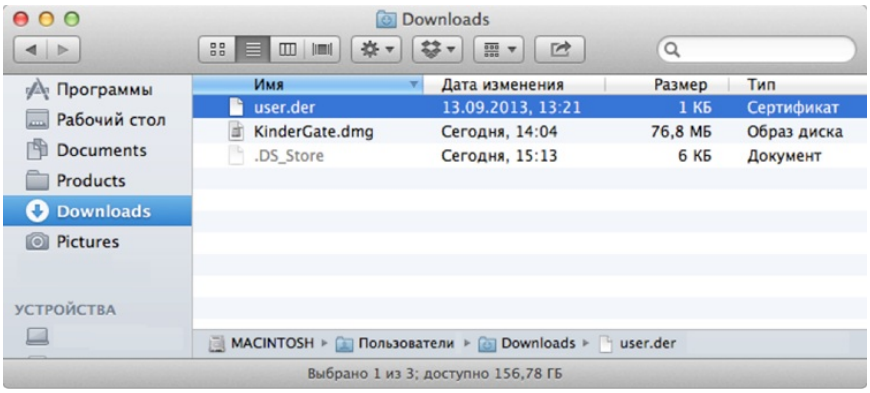


Рисунок 13 Выбор файла сертификата

Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:

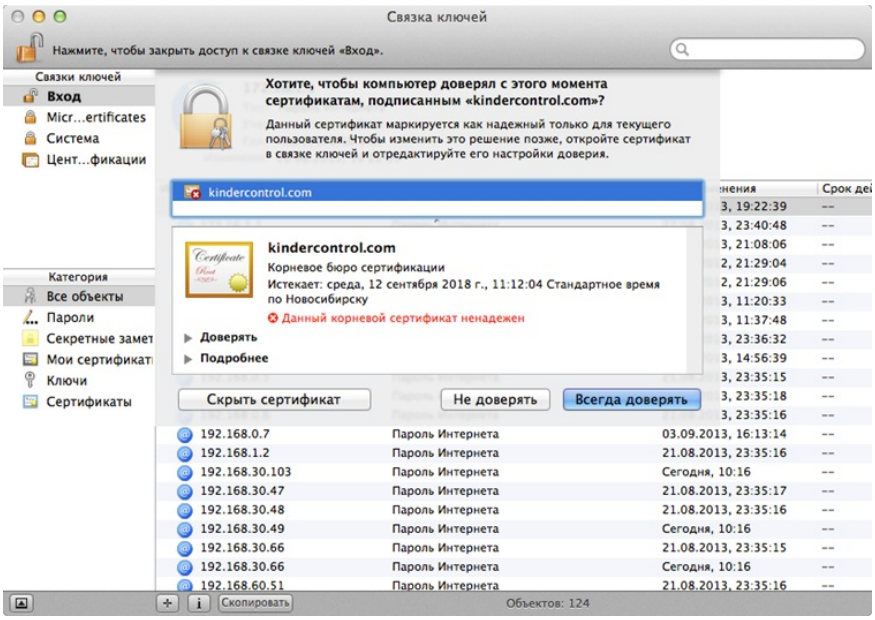


Рисунок 14 Доверие сертификату

Введите свой пароль для подтверждения данной операции:

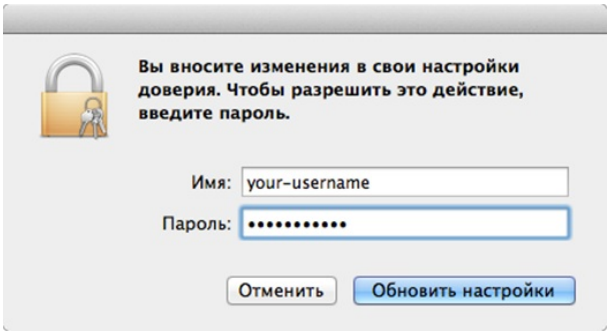


Рисунок 15 Ввод пароля

Сертификат установлен.

Установка сертификата в браузер Firefox

Установка сертификата в браузер Firefox выполняется аналогично для всех операционных систем. Рассмотрим установку на примере ОС Windows.

Откройте настройки браузера Firefox (**Инструменты → Настройки**):

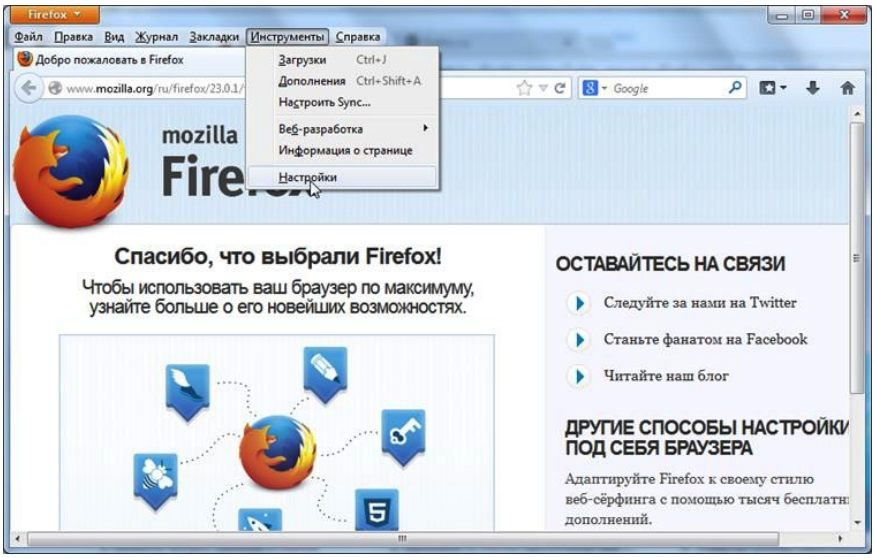


Рисунок 16 Вход в режим Настройки

Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите на кнопку **Просмотр сертификатов**:

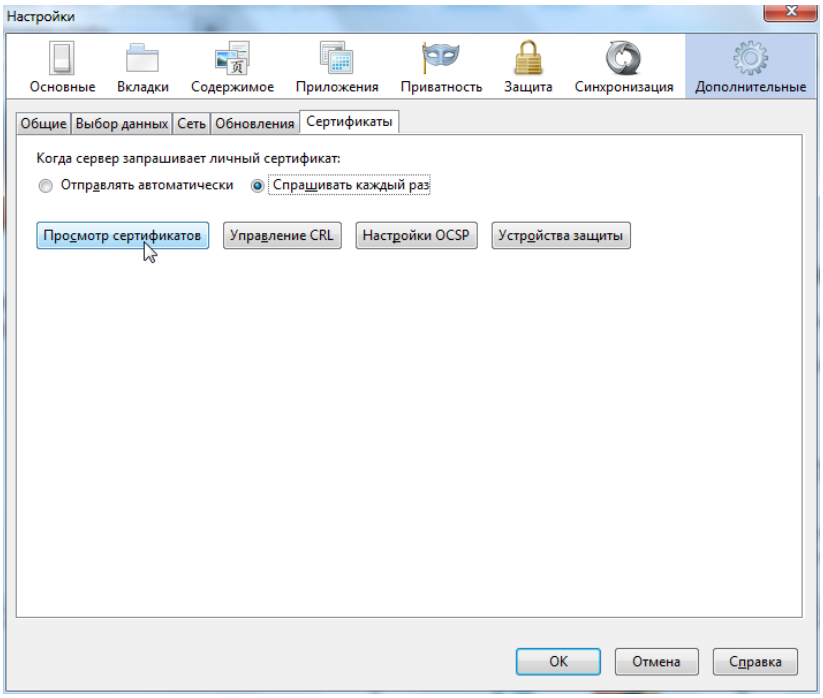


Рисунок 17 Раздел Сертификаты

Нажмите кнопку **Импортировать** и укажите путь к скачанному pem-сертификату:

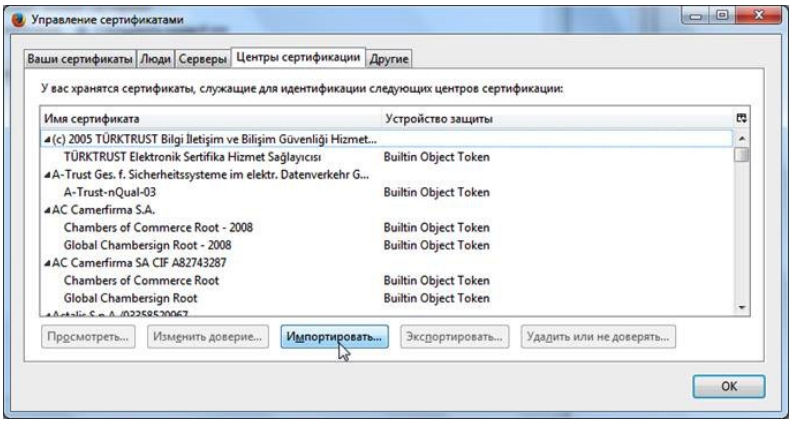


Рисунок 18 Список установленных сертификатов

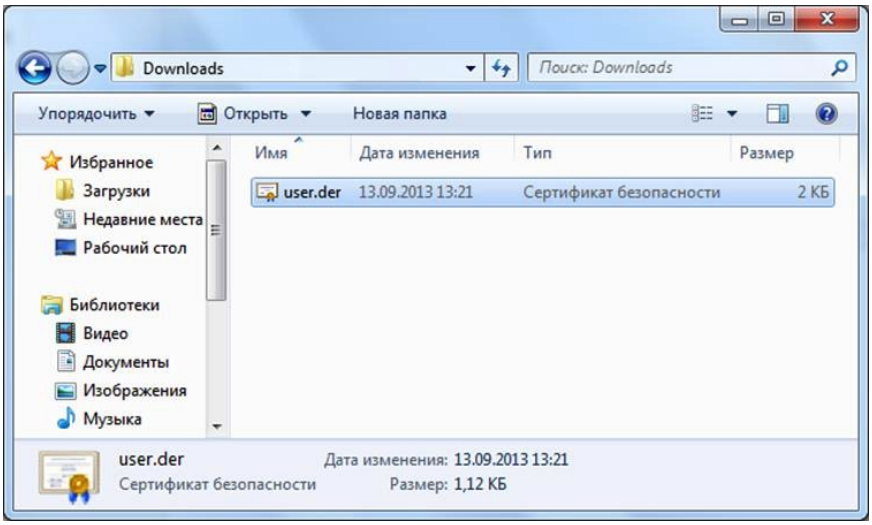


Рисунок 19 Выбор файла сертификата

Установите галочку **Доверять при идентификации веб-сайтов** и нажмите **ОК**:

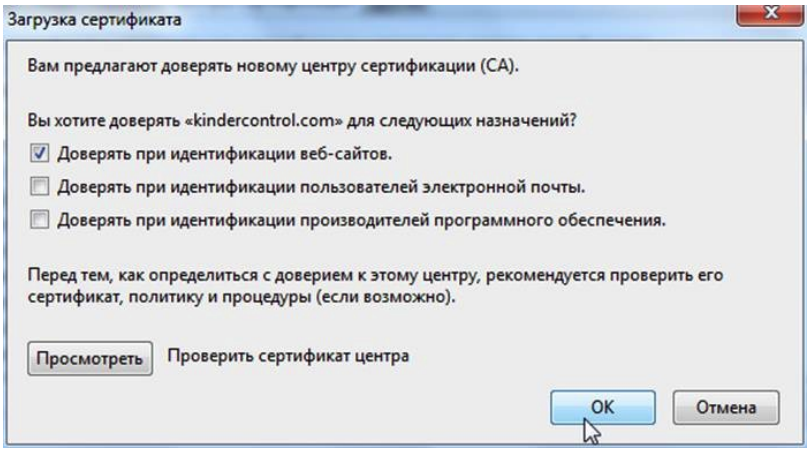


Рисунок 20 Выбор типа доверия

Установка сертификата завершена.

Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0

Documentation:
Product: NGFW
Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Peer-To-Peer	Пиринговые сети
Алкоголь. Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию	Алкоголь и табак
Баннеры и рекламные программы Баннерные сети, всплывающая реклама, рекламные программы	Реклама и всплывающие окна
Библиотеки	Искусство
Вождение и автомобили	Транспорт
Вредоносное программное обеспечение	Нелегальное ПО
Вредоносные программы	Ботнеты
	Сайты сомнительного содержания
	Вредоносное ПО
	Криптомайнеры
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечение	Поздравительные открытки
	Развлечения
	Мода и красота
	Отдых и оздоровление
	Рестораны и еда
	Спорт
	Путешествия
Здоровье и медицина	Здоровье и медицина
	Половое воспитание
Злоупотребление свободой СМИ - информация с ограниченным доступом. Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций	Оружие
Злоупотребление свободой СМИ - информация, содержащая скрытые вставки и иные технические способы воздействия на под-104№ п/п Тематическая категория Содержание скрытое воздействие сознание людей и (или) оказывающая вредное влияние на их здоровье	Сайты сомнительного содержания
Злоупотребление свободой СМИ - наркотические средства, сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Ненависть и нетерпимость
	Насилие
Злоупотребление свободой СМИ -экстремизм Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы	Ненависть и нетерпимость
	Насилие

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Знакомства	Знакомства
Информация с ограниченным доступом. Информация, составляющая государственную или иную охраняемую законом тайну	Политика
	Правительство
Информация, пропагандирующая порнографию	Порнография и насилие
Компьютерные игры	Игры
Корпоративные сайты	Бизнес
	Финансы
	Общие
	Недвижимость
Корпоративные сайты, интернет-представительства негосударственных учреждений	Некоммерческие и неправительственные организации
Личная и немодерируемая информация. Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги	Персональные сайты
	Частные IP-адреса
	Социальные сети
	Потоковое мультимедиа и загрузки
	Веб-почта
Модерируемые доски объявлений (ресурсы данной категории, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты	Социальные сети
	Чаты
Наркотические средства. Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Наркотики
Нелегальная помощь школьникам и студентам. Банки готовых рефератов, эссе, дипломных работ и пр.	Школьные мошенничества
Ненадлежащая реклама. Информация, содержащая рекламу алкогольной продукции и табачных изделий	Алкоголь и табак
Неприличный и грубый юмор. Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека	Сайты сомнительного содержания
Нижнее белье, купальники	Нудизм
Обеспечение анонимности пользователя, обход контентных фильтров. Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам	Анонимайзеры
	Переводчики
Образовательные ресурсы	Образование
Онлайн-казино и тотализаторы	Азартные игры
Отправка SMS с использованием интернет-ресурсов. Сайты, предлагающие услуги по отправке SMS-сообщений	Реклама и всплывающие окна
Платные сайты	Паркованные домены
Поиск работы, резюме, вакансии	Поиск работы
Преступления - Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию)	Преступная деятельность
Преступления-клевета, экстремизм	Преступная деятельность
	Компьютеры и технологии
	Нелегальное ПО

Программное обеспечение **Категории Министерства Образования РФ**	**Категории UserGate URL filtering 4.0**
	Информационная безопасность
Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения. Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение	Ненависть и нетерпимость
Религии и атеизм	Религиозные культы
	Религия
Система поиска изображений	Обмен картинками
	Поисковые системы и порталы
СМИ	Форумы и новостные ленты
	Новости
Табак, реклама табака, пропаганда потребления табака. Сайты, пропагандирующие потребление табака; реклама табака и изделий из него	Алкоголь и табак
Торговля и реклама	Реклама и всплывающие окна
	Покупки
Убийства, насилие	Жестокое обращение с детьми
	Насилие
Чаты	Чаты
	Сервисы мгновенных сообщений
Экстремистские материалы или экстремистская деятельность (экстремизм)	Ненависть и нетерпимость

Documentation: ☑
Version: 5.x, 6.1.9, 7.0.1

Экспорт журналов в формате CEF

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 1 — информационные. • 4 — предупреждения. • 7 — ошибки. • 10 — критичные.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	Admin
	cat	Компонент, в котором произошло событие.	console_auth
	act	Тип события.	login_successful
	src	IPv4-адрес источника.	192.168.117.254
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"name":"MIME_BUILTIN_COMPOSITE","module":"nlist_import"}

Формат журнала веб-доступа

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}

Тип поля	Название поля	Описание	Пример значения
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает было ли содержимое расшифровано.	Decrypted
	cs6	Расшифровано или нет.	true, false
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString2	Категория URL.	Computers & Technology
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения от 1 (если приложения нет) до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3

Тип поля	Название поля	Описание	Пример значения
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала СОВ

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры СОВ.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения от 2 до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	app	Протокол прикладного уровня.	HTTP
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40

Формат журнала АСУ ТП

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Название журнала.	scada
	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	1
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	app	Протокол прикладного уровня.	Modbus
	cs6Label	Поле указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	{"protocol":"modbus","pdu_severity":0,"pdu_func":"3","pdu_address":0, "mb_value":0,"mb_quantity":0,"mb_payload":"AAIAAA==", "mb_message":"response","mb_addr":0}

Формат журнала инспектирования SSH

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	**CEF:Version**	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	Usergate
	Device Product	Тип продукта.	UTM
	Device Version	Версия продукта.	6
	Source	Название журнала.	ssh

Тип поля	Название поля	Описание	Пример значения
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения от 1 (если приложения нет) до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	**rt**	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Указание на команду, передаваемую по SSH.	Command
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

Экспорт журналов в формате JSON

Описание журнала событий

Название поля	Описание	Пример значения
user	Имя пользователя.	Admin
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
ip_address	IPv4-адрес источника события.	192.168.174.134
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
attributes	Детали события в формате JSON.	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core

Название поля	Описание	Пример значения
event_component	Компонент, в котором произошло событие.	console_auth

Описание журнала веб-доступа

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
url_categories	**id**		Идентификатор категории, к которой относится URL.	39
	threat_level		Уровень угрозы категории URL.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название категории, к которой относится URL.	Social Networking
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	52
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
packets_recv			Количество байтов, переданных в направлении назначение — источник.	5
request_method			Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url			Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	2
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
media_type			Тип контента.	application/json
host			Имя хоста.	www.google.com
session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
app_protocol			Протокол прикладного уровня и его версия.	HTTP/1.1
status_code			Код ответа HTTP.	302
bytes_recv			Количество пакетов, переданных в направлении назначение — источник.	100
http_referer			URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted			Поле указывает было ли содержимое расшифровано.	true, false
reasons			Причина, по которой было создано событие, например, причина блокировки сайта.	"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]
useragent			Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника.	Trusted
	country		Страна источника трафика.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Страна назначения.	RU (отображается двухбуквенный код страны)

Название поля			Описание	Пример значения
	ip		IPv4-адрес назначения.	192.168.174.134
	port		Порт назначения.	Может принимать значения от 0 до 65535.
rule	**guid**		Уникальный идентификатор правила, срабатывание которого вызвало создание события.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name		Название правила.	Default allow
user	**guid**		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя	user_name
	groups	**guid**	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала трафика

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	100
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
packets_recv			Количество пакетов, переданных в направлении назначение — источник.	1
proto			Используемый протокол 4-го уровня.	TCP или UDP
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
action			Действие, принятое устройством в соответствии с настроенными политиками.	accept
session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
bytes_recv			Количество байтов, переданных в направлении назначение — источник.	6
signatures	**id**		Идентификатор сработавшей сигнатуры.	999999
	threat_level		Уровень угрозы сработавшей сигнатуры.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название сработавшей сигнатуры.	BlackSun Test
application	**id**		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название приложения.	Youtube
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.

Название поля			Описание	Пример значения
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
nat	**source**	**ip**	Адрес источника после переназначения (если настроены правила NAT).	192.168.117.85 (если NAT не настроен, то: **"nat":null**)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: **"nat":null**)
	destination	**ip**	Адрес назначения после переназначения (если настроены правила NAT).	64.233.164.198 (если NAT не настроен, то: **"nat":null**)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: **"nat":null**)
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила.	firewall
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
user	**guid**		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала СОВ

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	1
packets_recv		Количество пакетов, переданных в направлении назначение — источник.	1
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto		Используемый протокол 4-го уровня.	TCP или UDP
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv		Количество байтов, переданных в направлении назначение — источник.	6
action		Действие, принятое устройством в соответствии с настроенными политиками.	accept
application	**id**	Идентификатор приложения.	195
	threat_level	Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name	Название приложения.	Youtube
user	**guid**	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name	Имя пользователя.	Admin

Название поля			Описание	Пример значения
	groups	**guid**	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
signatures	**id**		Идентификатор сработавшей сигнатуры.	999999
	threat_level		Уровень угрозы сработавшей сигнатуры.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название сработавшей сигнатуры.	BlackSun Test
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.

Описание журнала АСУ ТП

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity		Критичность АСУ ТП.	1
pdu_func		Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address		Адрес регистра, с которым необходимо провести операцию.	3154
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	**pdu_varname**	Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device	Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity	Количество значений для записи (команда Read Write Register).	998
	mb_write_addr	Начальный адрес регистра для записи (команда Read Write Register).	776
	mb_value	Записываемое значение (для команд Write Single Coil, Write Single Register).	322
	mb_unit_id	Адрес устройства.	186
	mb_read_quantity	Количество значений для чтения (команда Read Write Register).	658
	mb_read_addr	Начальный адрес регистра для чтения (команда Read Write Register).	122
	mb_quantity	Количество значений для чтения.	875

Название поля			Описание	Пример значения
	mb_payload		Значения регистров (для команд Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdc24f9883
	mb_or_mask		Значение маски OR команды Mask Write Register.	1024
	mb_message		Сообщение Modbus.	exception
	mb_exception_code		Код ошибки. Актуален для типа сообщения error_response.	255
	mb_and_mask		Значение маски AND команды Mask Write Register.	121
	mb_addr		Адрес регистра.	3154
	iec104_msgtype		Тип запроса.	request, response, error_response
	iec104_ioa		Адрес объекта информации, который позволяет однозначно идентифицировать приёмной стороной тип события.	23
	iec104_cot		Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu		Адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104.	123
app_protocol			Протокол прикладного уровня.	Modbus
action			Действие, принятое устройством в соответствии с настроенными политиками.	pass
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	**zone**	**guid**	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	**guid**		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

Описание журнала инспектирования SSH

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command			Команда, передаваемая по SSH.	whoami
app_threat			Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2)
app_protocol			Протокол прикладного уровня.	SSH или SFTP
app_id			Идентификатор приложения.	195
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
		guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47

Название поля			Описание	Пример значения
source	zone	name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	FA:16:3E:65:1C:B4
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SSH Rule Example
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Опции DHCP

Documentation: ☑
Product: NGFW
Version: 7.0.1, 7.1.0

Формат значений опций соответствует RFC 2132.

Наименование	Описание
1	Маска подсети, из которой был получен адрес.
2	Разница во времени в подсети клиента относительно UTC (указывается в секундах).
3	Список IP-адресов доступных шлюзов.
6	Список DNS-серверов.
7	Список лог-серверов (MIT-LCS UDP).
9	Список LPR-серверов (RFC 1179).
13	Размер загрузочного образа для клиентов.
15	Имя домена.
16	Swap-сервер.
17	Путь корневого каталога для клиента.
18	Путь расширений BOOTP.
19	Применение пересылки IP-датаграмм.
20	Использование маршрутизации удаленного источника.
21	Политика фильтрации IP-адресов.
22	Максимальный размер датаграммы.
23	Значение TTL для IP по умолчанию.
26	Значение MTU для данного интерфейса.
27	Признак, что все подсети используют текущую конфигурацию MTU.
31	Определение использования сообщений ICMP для обнаружения маршрутизаторов.
32	Адрес, который используется для обращения к маршрутизатору.
33	Статичный список маршрутизации; состоит из пар «адрес назначения» — «адрес роутера».
34	Использование концевиков (trailers) при запросах ARP.
35	Тайм-аут кэш-памяти ARP.
36	Необходимость использования инкапсуляции данных Ethernet.
37	Значение TTL для TCP-пакетов.
38	Интервал отправки контрольных пакетов TCP (TCP keep-alive).
40	Домен NIS.
41	Список серверов NIS.
42	Список серверов времени NTP.
44	Список IP-адресов серверов NetBIOS.
45	Список IP-адресов серверов рассылки датаграмм NetBIOS.
46	Тип узла NetBIOS.
47	Область NetBIOS.

Наименование	Описание
48	IP-адреса серверов шрифтов X Windows (X Window System Font).
49	Диспетчер дисплея X Windows.
58	Время T1 - интервал времени, в течение которого клиент должен отправить запрос на обновление IP-адреса.
59	Время T2 - интервал времени (в секундах), в течение которого клиент должен отправить запрос на повторное связывание.
60	Опция используется клиентом DHCP для указания поставщика.
64	Имя домена NIS+.
65	Список серверов NIS+.
66	Имя сервера TFTP.
67	Название загрузочного файла.
68	Адреса домашних агентов (Mobile IP Home Agent).
69	Список серверов SMTP.
70	Список серверов POP3.
71	Список серверов NNTP.
74	Список серверов IRC.
77	Класс пользователя.
80	Опция позволяет получать сетевые настройки от DHCP-сервера посредством быстрого обмена двумя сообщениями вместо стандартных четырех между Requesting Router (RR) и Delegating Router (DR).
93	Архитектура системы клиента DHCP.
94	Идентификатор сетевого интерфейса клиента DHCP.
97	Идентификатор клиента на основе UUID/GUID.
119	Список поиска DNS.
120	Список серверов SIP.
121	Список бесклассовых статических маршрутов.
125	Указание информации о поставщике.
255	Конец списка опций; обязательно должен присутствовать последним.

Требования к сетевому окружению

Documentation:
Product: NGFW
Version: 7.0.1

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8001	Входящий (до веб-консоли UserGate NGFW)	Доступ к веб-интерфейсу управления устройством.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4040	Входящий (к UserGate по API)	Управление устройством UserGate по API.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверам технической поддержки. Доступ к серверам: • 93.91.171.46; • 178.154.221.222; • ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)/Входящий (от клиентов до сервера UserGate, если он используется в качестве сервера точного времени)	Синхронизация времени.
DNS	TCP/UDP	53	Входящий (от клиентов к серверу UserGate, если он выступает в качестве DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
	UDP	53	Исходящий (до серверов DNS)	
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Регистрация продуктов UserGate: доступ до сервера reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
Связь с UserGate Management Center	TCP	9712	Исходящий (от UG NGFW до UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Management Center.
		2022	Исходящий (от UG NGFW до UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Связь с UserGate Log Analyzer	TCP	9713	Входящий (от LogAn к UG NGFW)	Первоначальная установка связи и обмен ключами шифрования с сервером UserGate Log Analyzer.
		2023	Входящий (от LogAn к UG NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	TCP	Для версий 6.1.x: 1269 (передача данных на LogAn 6.1.x), 22699 (передача данных на LogAn 7.x.x) Для версий 7.0.x: 22699 (передача данных на LogAn 6.1.x), 22711 (передача данных на LogAn 7.x.x, с использованием SSL)	Исходящий (от UG NGFW к LogAn)	Передача журналов и телеметрии на сервер LogAn.
Подключение конечных устройств с установленным ПО UserGate Client (доступно начиная с версии 7.1.0)	TCP	4045	Входящий (от конечного устройства на UG NGFW)	Подключение конечных устройств и приём телеметрии для проверки комплаенса.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
Captive-портал и страница блокировки	TCP	80, 443, 8002	Входящий (от браузера клиента на UG NGFW)	Отображение страницы авторизации Captive-портала и страницы блокировки.
		8043		При активации опции "HTTPS для страницы аутентификации".
Kerberos	TCP/UDP	88	Исходящий (на сервер аутентификации Kerberos)	Аутентификация пользователей по протоколу Kerberos.

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
NTLM	TCP	445	Исходящий (на сервер аутентификации NTLM)	Аутентификация пользователей по протоколу NTLM.
RADIUS	UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
Агент терминального сервиса	UDP	1812, 1813	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимый для работы терминального агента.
Агент аутентификации для Windows	UDP	1812, 1813	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимый для работы агента аутентификации доменных пользователей, работающих на ОС Windows.
Прокси-агент	UDP	8090	Входящий (от агента на UG NGFW)	Доступ к серверу UserGate, необходимый для работы прокси-агента, предоставляющего доступ в Интернет пользователям, работающим на ОС Windows.
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
ICAP	TCP	1344	Исходящий (до серверов ICAP)	Сервис работы с серверами ICAP.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)/Входящий (UserGate выступает в качестве DHCP-сервера)	Сервис службы DHCP.
BGP	TCP	179	Исходящий (передача информации соседним BGP-маршрутизаторам)/Входящий (получение информации от соседних BGP-маршрутизаторов)	Сервис динамической маршрутизации BGP.
OSPF	89/OSPF		Исходящий (передача информации соседним OSPF-маршрутизаторам /Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамической маршрутизации OSPF.
RIP	UDP	520	Исходящий (распространение соседним маршрутизаторам RIP-маршрутов)/Входящий (получение от соседних маршрутизаторов RIP-маршрутов)	Сервис динамической маршрутизации RIP.
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.