UserGate

NGFW 6.1.x Руководство администратора

Оглавление

ВВЕДЕНИЕ

БЕЗОПАСНОСТЬ СЕТИ И ЗАЩИТА ОТ СЕТЕВЫХ УГРОЗ

Настройка политик безопасности при помощи сценариев

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 приоритезировать сценарии для скорейшей реакции на критичные угрозы.

Управление АСУ ТП

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.

Работа с внешними системами безопасности

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.

Проверка почтового трафика

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.

Антивирусная проверка трафика

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

Защита от DOS-атак и сетевого флуда

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.

Обнаружение и предотвращение вторжений

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.

Межсетевое экранирование

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.

УЛУЧШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ И НАДЕЖНОСТИ ИНТЕРНЕТА

Поддержка WCCP

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

Управление пропускной способностью

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

Поддержка нескольких провайдеров

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.

FTP поверх HTTP

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

Поддержка кластеризации и отказоустойчивости

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.

УПРАВЛЕНИЕ ТРАФИКОМ И КОНТРОЛЬ ДОСТУПА В ИНТЕРНЕТ

Поддержка политики BYOD

Концепция BYOD (Bring Your Own Device) продолжает набирать популярность, ставя перед системами безопасности новые задачи. UserGate позволяет настроить гибкие политики доступа в сеть для различных групп пользователей

и типов устройств, а также ограничить количество устройств, используемых одним пользователем.

Проксирование приложений

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.

Поддержка гостевого портала

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.

Аутентификация и авторизация пользователей

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.

Маршрутизация трафика и публикация ресурсов

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.

КОНТЕНТ-ФИЛЬТРАЦИЯ И КОНТРОЛЬ ПРИЛОЖЕНИЙ

VPN и веб-портал

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.

Инспектирование SSL-трафика

Платформа UserGate 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».

Инжектирование кода на веб-страницы

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.

Блокировка приложений социальных сетей

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.

Активация безопасного поиска

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.

Выборочная блокировка рекламы

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

Интернет-фильтрация

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.

ЖУРНАЛЫ И ОТЧЕТЫ

Журналы и отчеты(описание)

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

Функция балансировщика нагрузки

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, а также для балансировки трафика, пересылаемого на внешние серверы или ферму ICAP-серверов.

DNS-фильтрация

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.

Типы интерфейсов

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.

Использование оповещений

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).

Ролевой доступ администраторов к элементам управления UserGate NGFW

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.

ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

Описание

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

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

- Сервер регистрации - reg2.entensys.com, порты TCP 80, 443.
- Сервер обновления списков и ПО UserGate - static.entensys.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.

Развертывание виртуального образа

UserGate 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.

> **Примечание**
>
> **Для 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**

Наименование	Описание
	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 12Gb и добавьте по 1Gb на каждые 100 пользователей.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины	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.
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 и первоначальная настройка

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 UserGate укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. **Статический IP-адрес** Включить UserGate. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли UserGate по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGate_IP_address:8001.
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.
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.	

Наименование	Описание
	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 продукт UserGate.	Для регистрации продукта ввести ПИН-код и заполнить форму. Для активации системы необходим доступ UserGate в Интернет. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate.
Шаг 9. Создать правила NAT.	В разделе **NAT и Маршрутизация** создать необходимые правила NAT. Для доступа в интернет пользователей сети **Tr usted** 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 UserGate 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.

Наименование	Описание
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 UserGate готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

ЛИЦЕНЗИРОВАНИЕ

Лицензирование (Описание)

Внимание!

Лицензионные ключи версий 6 и 7 *несовместимы*! Перед обновлением до версии 7, необходимо запросить у менеджера ключ для 7-й версии.

NGFW может быть лицензирован:

- по количеству одновременных подключений;
- по параметрам производительности платформы;

Лицензирование по количеству одновременных подключений

Емкость системы ограничивается лицензированным количеством одновременно подключенных устройств, включая пользователей терминальных серверов, за исключением устройств, чей трафик проходит через NGFW с использованием правил публикации DNAT, Reverse-прокси, веб-портала, защиты почтового трафика.

Например, 100-пользовательская лицензия разрешает подключение к сети одновременно 100 устройствам с уникальными IP-адресами. 101 и следующие устройства не смогут получить доступ к сети. Количество учетных записей пользователей в системе не ограничивается.

Лицензирование по параметрам производительности платформы

UserGate может лицензироваться без ограничения по количеству одновременно подключенных устройств. Работа системы ограничивается только производительностью приобретенной платформы и зависит от:

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

Новые пользовательские сессии не блокируются, происходит естественная деградация производительности при увеличении обрабатываемого трафика.

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.**

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.

Наименование	Описание
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.

Лицензия на NGFW дает право бессрочного пользования продуктом.

НАСТРОЙКА УСТРОЙСТВА

Общие настройки

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.

Наименование	Описание
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.

Наименование	Описание
	• **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

Наименование	Описание
	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.

Наименование	Описание
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.**
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**.

Наименование	Описание
	• **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.

Наименование	Описание
	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

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

- **Кластеризация.**
- **Настройки диагностики.**
- **Операции с сервером.**
- **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 UserGate.
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.

Наименование	Описание
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 серверу UserGate 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 сервера UserGate. • **Выключить** - выключение сервера UserGate.
Обновления	Выбор канала обновлений ПО UserGate • **Стабильные** - проверка наличия стабильных обновлений ПО. • **Бета** - проверка наличия экспериментальных обновлений.

Команда UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UserGate 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 UserGate.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния UserGate, 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 UserGate будет перезагружен.

Экспорт и импорт настроек

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

Примечание

Экспорт настроек является кластерной функцией, т.е. экспортируется конфигурация всех узлов кластера. При импорте конфигурации будет предложен выбор нужного узла кластера для восстановления.

Примечание

Экспорт/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.

Примечание

В 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
Шаг 1. Экспорт настроек	В разделе **Управление устройством** нажать на ссылку **Экспорт и импорт настроек → 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 узла UserGate 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.

Примечание

Для 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

Наименование	Описание
	выражение "*/2" в поле "часы" будет означать "каждые два часа.

Кластеризация и отказоустойчивость

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.

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	

Наименование	Описание
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.
	В веб-консоли второго узла кластера в разделе **Сеть → Интерфейсы** необходимо назначить каждому интерфейсу

Наименование	Описание
Шаг 6. Назначить зоны интерфейсам второго узла.	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.

> **Примечание**
>
> **Режим 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, 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.

Примечание

Если 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.

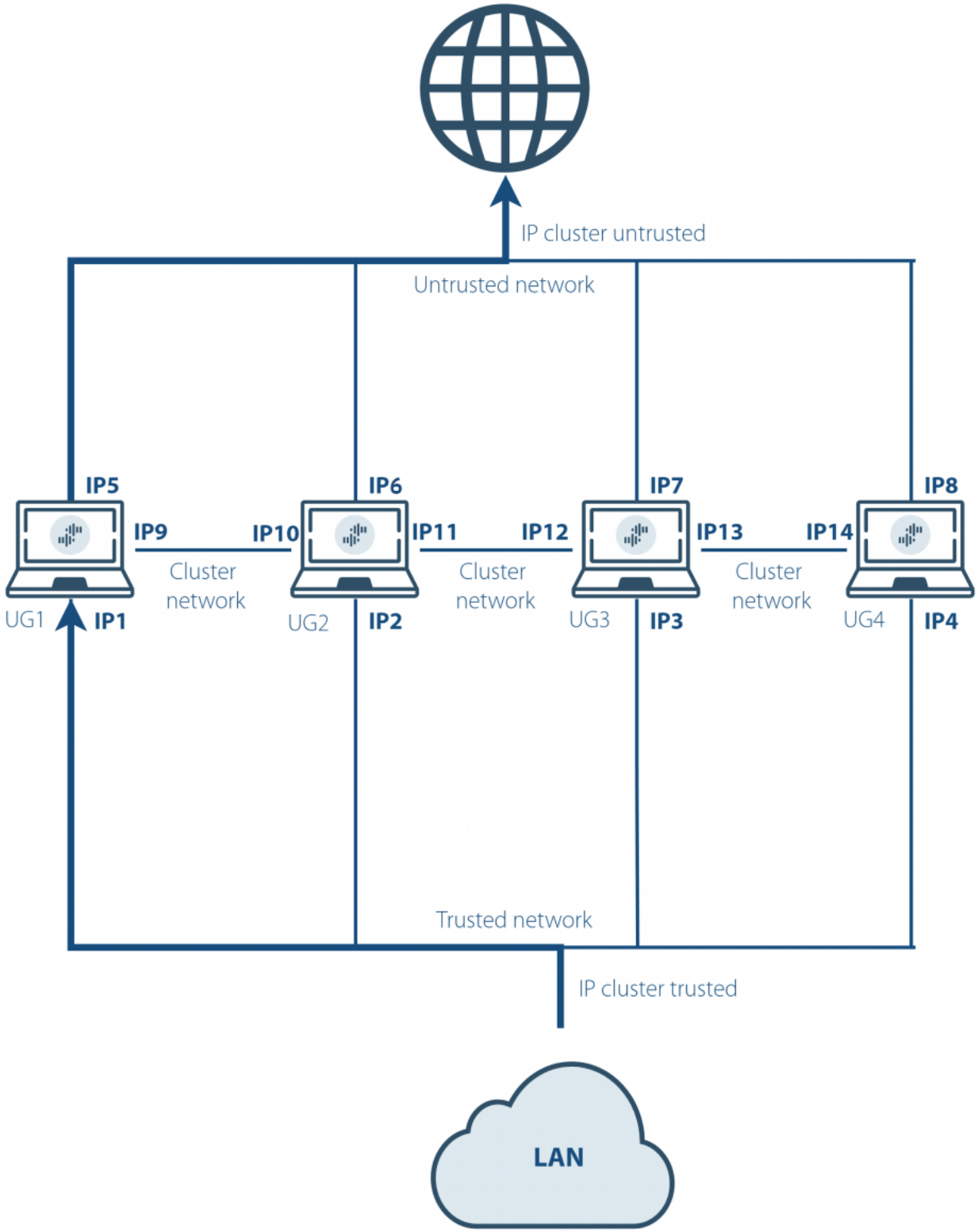
Примечание

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. 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.

> **Примечание**
>
> **Режим 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, 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.

> **Примечание**
>
> **Если 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.**

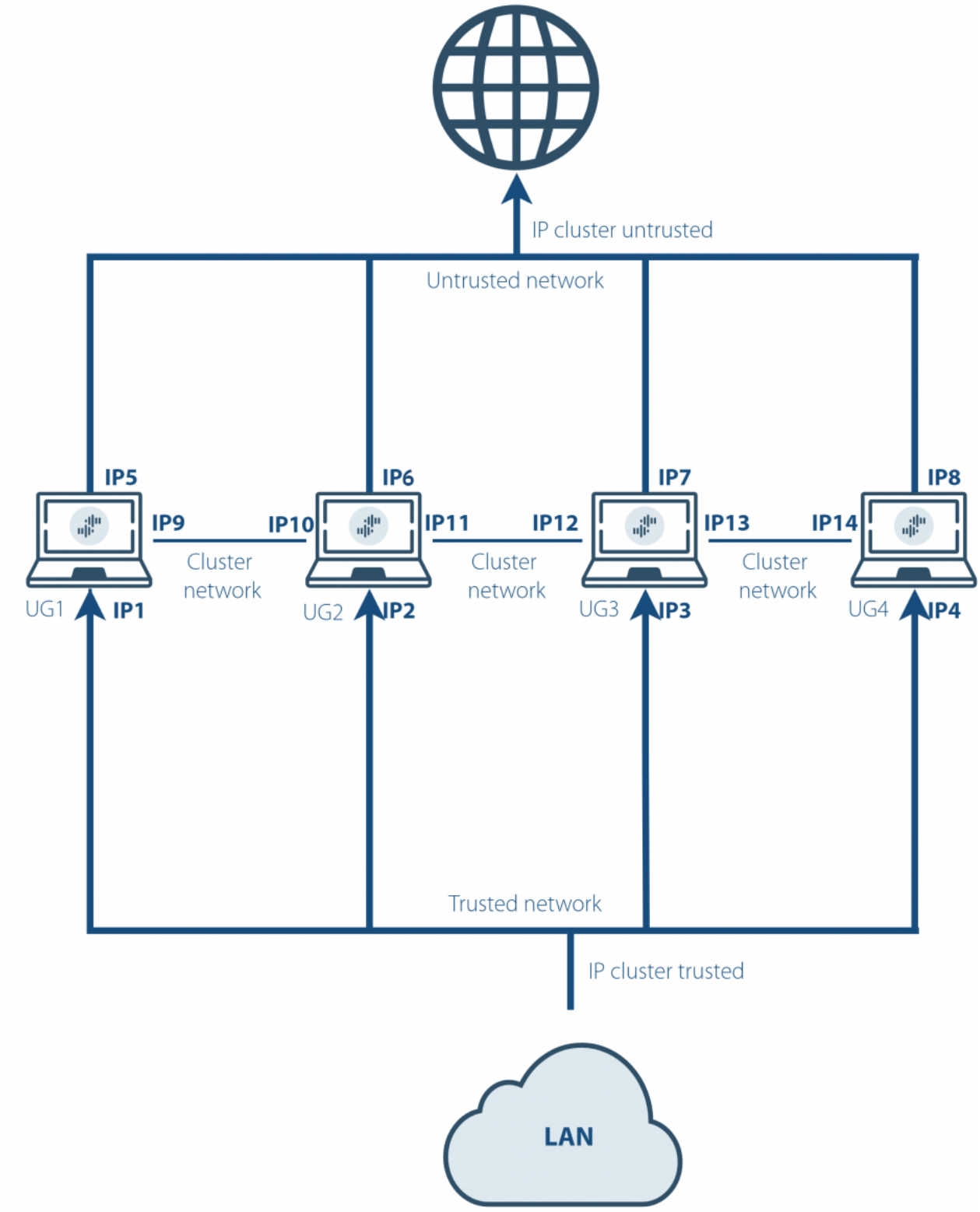
Примечание

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

Примечание

Для 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.

Наименование	Описание
	• **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

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.

> **Примечание**
>
> **При 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.

Наименование	Описание
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.

Наименование	Описание
	• **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.

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

> **Примечание**
>
> **Не 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:

Наименование	Описание

	`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	Добавить подписанные сертификаты администраторов (admin.p12 в нашем примере) в ОС (или в браузер Firefox, если он используется для доступа к консоли), с которой

Наименование	Описание
будут авторизоваться в веб-консоль.	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**.

Примечание

Переключить 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

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

Наименование	Описание
	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.

Наименование	Описание
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

Наименование	Описание
	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.

Примечание

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

Примечание

В целях безопасности NGFW не разрешает экспорт приватных ключей сертификатов.

Примечание

Пользователи 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:

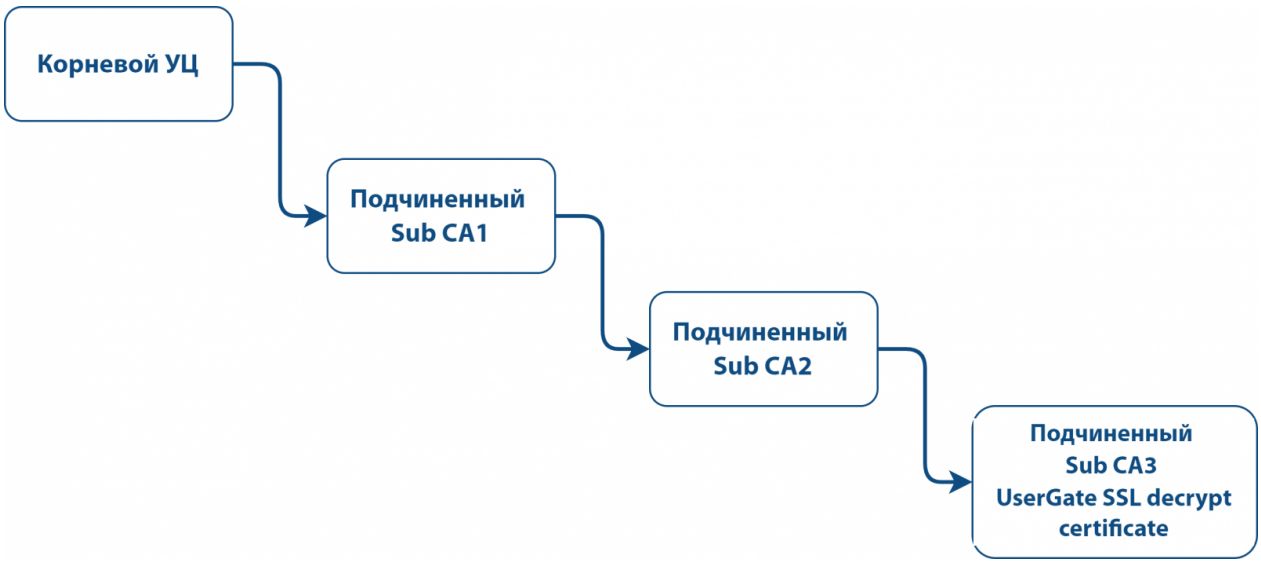
Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку **Импорт**.
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • **Название** — название сертификата, под которым он будет отображен в списке сертификатов. • **Описание** — описание сертификата. • **Файл сертификата**: загрузите файл, содержащий данные сертификата. • **Приватный ключ**: загрузите файл, содержащий приватный ключ сертификата.

Наименование	Описание
	• **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.

Примечание

NGFW 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.

Наименование	Описание
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)**.

Интерфейс командной строки (CLI)

UserGate позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, или CLI (command line interface). С помощью CLI администратор может выполнить ряд диагностирующих команд, таких, как ping, nslookup, traceroute, осуществить настройку сетевых интерфейсов и зон, а также перезагрузить или выключить 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 UserGate), через последовательный порт или с помощью SSH по сети.

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к UserGate.	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 UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к UserGate.	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate.
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 UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm.

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.
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 UserGate, 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@IPUserGate -p 2200
Шаг 3. Войти в CLI.	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UserGate не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm.

После успешного входа в CLI можно посмотреть список возможных команд с помощью команды **help**. Для подробного описания любой команды необходимо использовать синтаксис

```
help command
```

Например, для получения подробной справки по использованию команды настройки сетевого интерфейса iface необходимо выполнить

```
help iface
```

Полный список команд:

Наименование	Описание
help	Показывает список доступных команд.
exit **quit** **Ctrl+D**	Выйти из CLI.
cache ldap-clear	Очистка кэша LDAP-записей.
code-change-control	Набор команд для просмотра и настройки параметров защиты исполняемого кода продукта от потенциального несанкционированного изменения. Проверка целостности исполняемого кода происходит каждый раз после загрузки UserGate. **code-change-control show** - показывает текущий режим работы. По умолчанию отслеживание несанкционированных изменений исполняемого кода отключено. **code-change-control set log** - активирует режим отслеживания несанкционированных изменений исполняемого кода. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания. **code-change-control set block** - активирует режим отслеживания несанкционированных изменений исполняемого кода. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для возможности отключения созданного правила межсетевого экрана необходимо отключить отслеживание несанкционированных изменений.

Наименование	Описание
	code-change-control set off - отключает режим отслеживания несанкционированных изменений исполняемого кода. Требует указания пароля, который был задан при активации режима отслеживания исполняемого кода.
config-change-control	Набор команд для просмотра и настройки параметров защиты конфигурации (настроек) продукта от изменения. 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. Проверка целостности конфигурации происходит каждые несколько минут после загрузки UserGate. **config-change-control show** - показывает текущий режим работы. По умолчанию отслеживание изменений конфигурации отключено. **config-change-control set log** - активирует режим отслеживания изменений конфигурации. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий. Требует задания пароля, который потребуется в случае изменения режима отслеживания. **config-change-control set block** - активирует режим отслеживания изменений конфигурации. Требует задания пароля, который потребуется в случае изменения режима отслеживания. При обнаружении изменений UserGate записывает информацию о факте изменения в журнал событий и создает блокирующее правило межсетевого экрана, запрещающее любой транзитный трафик через UserGate. Для отключения созданного правила межсетевого экрана необходимо сбросить состояние блокировки с помощью следующей команды: **config-change-control set off** - отключает режим отслеживания изменений конфигурации. Требует указания пароля, который был задан при активации режима отслеживания конфигурации.
date	Посмотреть текущее время на сервере.
device	Набор команд для изменения параметров устройства. • **device passwd** - позволяет сменить пароль пользователю, залогиненному в CLI-консоль.

Наименование	Описание
	• **device config -list** - показывает список доступных опций для настройки. • **device config -get** - посмотреть текущее значение параметра. • **device config -set** - изменить значение параметра. Список доступных параметров: • **module_l7_enabled** - включение/отключение загрузки модуля L7. По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate. • **module_idps_enabled** - включение/отключение загрузки модуля idps. По умолчанию модуль загружен. **Важно!** После изменения данного параметра требуется перезагрузка устройства UserGate. • **module_h323_enabled** - включение/отключение загрузки модуля h323; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT. По умолчанию модуль выгружен. • **fw_drop_invalid** - включение/отключение блокировки пакетов с невалидным набором параметров в полях заголовка. Включение данной опции существенно понижает производительность межсетевого экрана. Рекомендуется оставить данную настройку в выключенном состоянии. • **fw_established** - включение/отключение создания одного общего правила межсетевого экрана для обратных пакетов. • **module_sip_enabled** - включение/отключение загрузки модуля sip; модуль необходимо включать для сопоставления сигнального соединения и соединения передачи данных в случае использования NAT. По умолчанию модуль выгружен. • **module_sunrpc_enabled** - включение/отключение загрузки модуля sunrpc. 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. По умолчанию модуль выгружен. **Важно!** Модуль нужно включать для пассивного режима работы FTP. • **fastpath** - включение/отключение модуля ускоренной обработки сетевого трафика. По умолчанию данная

Наименование	Описание
	настройка включена. В случае отключения модуля ускоренной обработки сетевого трафика, модуль будет отключен при перезагрузки устройства. • **ha_auth_type** - включение подписи IPsec Authentication Header для служебных пакетов VRRP в кластере отказоустойчивости. Для включения подписи необходимо использовать команду: device config -set ha_auth_type ah Для отключения проверки: device config -set ha_auth_type pass
gateway	Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации.
iface	Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации. Следующие параметры команды iface позволяют управлять пересылкой пакетов directed broadcast, приходящих на указанный интерфейс: iface config -name port X -link-info 'bc_forwarding=1' -enabled true iface config -name port X -link-info 'bc_forwarding=1' -enabled false Следующие параметры команды iface включают механизм Proxy ARP, UserGate будет отвечать на ARP-запросы адресов, не относящихся к сети интерфейса: iface config -name port X -link-info 'proxy_arp=1' -enabled true Следующие параметры команды iface включают механизм Proxy ARP, UserGate будет отвечать на ARP-запросы адресов, относящихся к сети интерфейса: iface config -name port X -link-info 'proxy_arp_pvlan=1' -enabled true
license	Посмотреть информацию о лицензии.
netcheck	Проверить доступность стороннего HTTP/HTTPS-сервера. netcheck [-t TIMEOUT] [-d] URL Опции: -t – максимальный таймаут ожидания ответа от веб-сервера -d – запросить содержание сайта. По умолчанию запрашиваются только заголовки.

Наименование	Описание
node	Набор команд для просмотра и настройки узлов кластера. Смотрите node help для детальной информации.
nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
proxy	Набор команд для просмотра и настройки параметров прокси-сервера. Позволяет настроить такие параметры, как добавление заголовков HTTP - via и forwarded, а также настройки таймаутов на подключение к сайтам и на загрузку контента: • **add_via_enabled** – добавлять HTTP заголовок via. По умолчанию отключено. • **add_forwarded_enabled** – добавлять HTTP заголовок forwarded. По умолчанию отключено. • **add_xforwarded_enabled** - добавлять HTTP заголовок X-Forwarded-For. 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** - разрешить использование протокола HTTP PROXY 1.1 без указания параметра host. Данный режим противоречит RFC, но необходим для совместимости с некоторыми программами. По умолчанию установлено значение strict (соблюдать RFC). • **fmode_enabled** (boolean) - включает режим ускорения загрузки контента. Может быть несовместим с работой некоторых сайтов. По умолчанию отключен. • **icap_wait_timeout** - время в секундах, которое сервер UserGate ждет ответа от ICAP-сервера. Если ответ сервера не был получен в заданный промежуток времени, то в случае, если действие правила **Переслать и игнорировать**, UserGate отправит данные пользователю без модификации, если же действие правила **Переслать**, UserGate не отдаст данные пользователю. Значение по умолчанию - 10 секунд. • **smode_enabled** (boolean) – включает режим SYN Proxy. По умолчанию выключен. • **legacy_ssl_enabled** (boolean) – отключает поддержку дешифрования протокола SSL TLSv1.3. При включении данного режима UserGate поддерживает работу протоколов TLSv1.0-TLSv1.2. Если режим отключен, то

Наименование	Описание
	поддерживается работа только TLSv1.0-TLSv1.3. По умолчанию отключен. Рекомендуется не изменять значения по умолчанию. Смотрите proxy help для детальной информации.
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate.
radmin_e	Включить или отключить удаленный доступ к серверу для технической поддержки UserGate, в случаях, когда сервер UserGate завис. В случаях, когда произошла проблема с ядром UserGate, 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 UserGate. 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.
reboot	Перезагрузить сервер UserGate.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер UserGate.
telemetry	Набор команд для просмотра и настройки режима работы телеметрии. 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. Отправка телеметрии активирована по умолчанию. **telemetry show** – показать текущий режим. **telemetry set -enabled true** – активировать телеметрию. **telemetry set -enabled false** – отключить отсылку телеметрической информации.
traceroute	Выполнить трассировку соединения до определенного хоста.
usersession	Команда для сброса авторизации указанного пользователя. **usersession terminate -ipv4 IP_ADDRESS** – сбрасывает авторизацию для указанного IP_ADDRESS.

Наименование	Описание
webaccess	Набор команд для просмотра режима авторизации веб-консоли. Позволяет вернуть режим **По имени и паролю** при невозможности авторизоваться с помощью сертификатов.
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

Системные утилиты

Системные утилиты доступны администратору во время загрузки сервера UserGate 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 UserGate. 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
1. UserGate (serial console)	Загрузка UserGate с выводом диагностической информации о загрузке в последовательный порт.
2. UserGate (verbouse mode)	Загрузка UserGate с выводом диагностической информации о загрузке в консоль tty1 (монитор).
3. Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
4. Support menu (serial console)	Войти в раздел системных утилит с выводом информации в последовательный порт. При подключении через последовательный порт загрузочное меню не отображается. Для выбора раздела **Support menu** необходимо во время загрузки нажимать клавишу "**4**". Для выбора одного из пунктов меню в разделе **Support menu** необходимо нажать клавишу, соответствующую первой букве названия пункта меню, например, для выбора **Restore backup,** необходимо нажать клавишу "**R**", затем клавишу "**Ввод**".

Наименование	Описание
5. Memory test	Запуск проверки оперативной памяти устройства.

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.
Clear logs	Очистка диагностических журналов для освобождения пространства на системном разделе. Журналы UserGate не очищаются (журналы веб-доступа, трафика, событий, СОВ и т.п.).
Export logs	Выгрузка диагностических журналов на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Expand log partition	Увеличение раздела для журналов на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются.
Backup full	Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Backup system only	Создать копию системного раздела UserGate, исключая журналы (журналы веб-доступа, трафика, событий, СОВ и т.п.) на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate с внешнего USB носителя.
Update from USB	Установка обновления ПО UserGate с внешнего USB носителя. Обновление должно быть скопировано в корень съемного диска, диск должен иметь формат NTFS или FAT32. Название файла обновления должно быть в следующем формате: **update_xxxxx** (где xxxxx – номер версии).

Наименование	Описание
Refresh NIC names	Упорядочивание имен сетевых портов в необходимом порядке. Упорядочивание производится в соответствии с номером порта на шине PCI. Эту операцию необходимо выполнять после добавления сетевых портов в настроенный аплаенс UserGate, например, после установки дополнительной сетевой карты в физический аплаенс или после добавления портов в виртуальный аплаенс. Данные и настройки UserGate не сбрасываются.
Factory reset	Сброс состояния UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

НАСТРОЙКА СЕТИ

Настройка зон

Зона в UserGate - это логическое объединение сетевых интерфейсов. Политики безопасности UserGate 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 UserGate поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление UserGate.
Trusted	Зона для подключения доверенных сетей, например, LAN-сетей.
Untrusted	Зона для интерфейсов, подключенных к недоверенным сетям, например, к интернету.

Наименование	Описание
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 UserGate по VPN.
VPN for remote access	Зона, в которую помещаются все мобильные пользователи, подключаемые к UserGate по VPN.

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

> **Примечание**
>
> **Можно 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 UserGate начинает отбрасывать пакеты и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 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

Наименование	Описание
	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!** UserGate позволят произвести более гранулированную защиту от DoS атак. Для получения дополнительной информации обратитесь в раздел Защита от DoS атак. **Внимание!** Зоны и правила защиты от DoS атак работают по разному, это две независимые системы: Первыми срабатывают зоны. Они обрабатывают входящий и исходящий трафик. Правила защиты от DoS атак распространяются только на транзитный трафик. Таким образом, если идёт атака на ваш внешний IP, то надо использовать защиту на зоне. Здесь сразу отсекается паразитный трафик.
Шаг 3. Настроить параметры контроля доступа зоны (опционально).	Указать предоставляемые UserGate 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 UserGate. • **SNMP** - доступ к UserGate 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 UserGate в кластер (TCP 4369, TCP 9000-9100). • **VRRP** - сервис, необходимый для объединения нескольких узлов UserGate 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).

Наименование	Описание
	• **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. Более подробно смотрите раздел Правила АСУ ТП. • **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 сервере UserGate. Подробнее о требованиях сетевой доступности читайте в Приложение 1. 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.

Наименование	Описание
	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

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.
- 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 UserGate** 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	

Наименование	Описание
	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 UserGate** 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 UserGate, на котором будет создан бонд.
Зона	Зона, к которой принадлежит бонд.
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.

Наименование	Описание
	• **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

Наименование	Описание
	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

Наименование	Описание
	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 UserGate** 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 данной подсети, передает (транслирует) кадр дальше в тот

сегмент, которому предназначался данный кадр; если кадр принадлежит данной подсети, мост ничего не делает.

Интерфейс мост можно использовать в UserGate 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 UserGate в качестве решения, обеспечивающего контентную фильтрацию на уровне L2, выглядит следующим образом:

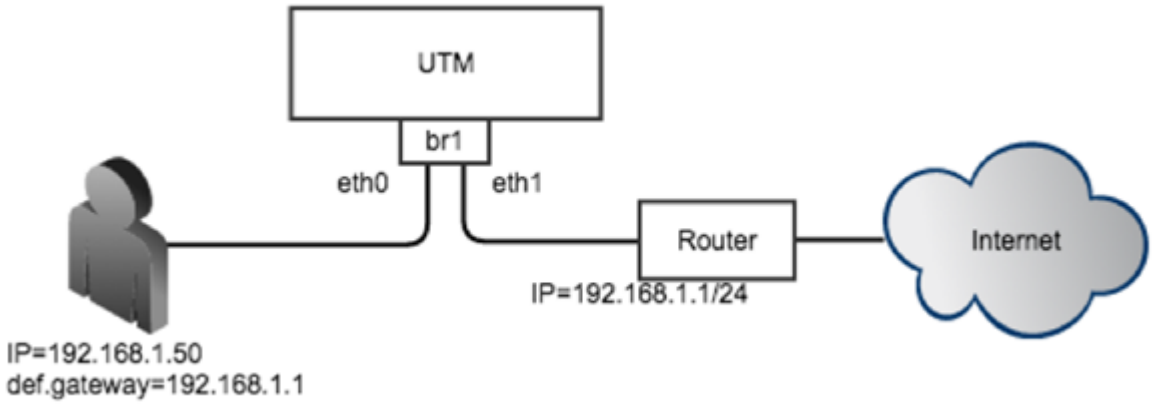


Рисунок 4 Использование моста

Примечание

Для работы виртуальной машины VMWare в данном режиме, необходимо в настройках групп портов, подключенных к мосту, перевести параметры безопасности *Promiscuous mode*, *MAC address changes*, *Forged transmits* в режим *Accept*.

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

Примечание

Одновременное использование мостов L2 и L3 на устройствах UserGate 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 UserGate.

Если мост создается в ПАК UserGate, 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 UserGate) в случаях если:

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

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

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 UserGate, 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	

Наименование	Описание
	Два интерфейса, которые будут использованы для построения моста.
Интерфейсы байпас моста	Пара интерфейсов, которые можно использовать для построения байпас моста. Требуется поддержка оборудования ПАК UserGate.
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 UserGate** 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 UserGate, на котором создать интерфейс PPPoE.
Интерфейс	Указать интерфейс, на котором будет создаваться интерфейс PPPoE.
Зона	Зона, к которой принадлежит интерфейс PPPoE.
Профиль Netflow	

Наименование	Описание
	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.
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 UserGate считает, что соединение отсутствует и разрывает его.
Использовать DNS-сервер провайдера	Если опция включена, то UserGate использует DNS-серверы, выданные провайдером.
Количество попыток подключения	Количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены.

Наименование	Описание
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 UserGate, 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:

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 серверу UserGate, 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,

Наименование	Описание
	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.

Наименование	Описание
Описание	Описание интерфейса.
Зона	Зона, к которой будет относится данный интерфейс.
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).

Сервер UserGate может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс UserGate, 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	В разделе **Сеть → Интерфейсы** в настройках конкретного сетевого интерфейса указать созданный профиль Netflow.

Наименование	Описание
необходимо собирать статистику.	

Настройка шлюзов

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**.

Наименование	Описание
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

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.

UserGate 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 UserGate 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**.

Примечание

Чтобы 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.

Примечание

Если в настройках DHCP не указывать DNS сервера, то NGFW будет отдавать в качестве DNS сервера адрес, совпадающий с адресом шлюза

Настройка DNS

Данный раздел содержит настройки сервисов DNS и DNS-прокси.

Для корректной работы продукта необходимо, чтобы NGFW мог разрешать доменные имена в IP-адреса. Укажите корректные IP-адреса серверов DNS в настройке **Системные DNS-серверы**.

Сервис DNS-прокси позволяет перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Сервис работает как в явном режиме, так и для перехвата транзитных запросов. Для явного режима необходимо разрешить доступ к сервису DNS на соответствующей зоне. Для перехвата транзитных запросов в этой зоне необходимо активировать следующие настройки в разделе DNS-прокси

Настройки DNS-прокси:

Наименование	Описание
Кэширование DNS	Включает или отключает кэширование ответов DNS. Рекомендуется оставить включенным для ускорения обслуживания клиентов.
DNS-фильтрация	Включает или отключает фильтрацию DNS-запросов. При включении DNS-фильтрации NGFW проверяет и перехватывает запросы, отправляя их дальше от своего IP-адреса. Если запрос соответствует запрещающему правилу контентной фильтрации, то он будет заблокирован. Для работы фильтрации необходимо приобрести лицензию на модуль ATP.

Наименование	Описание
	Внимание! **Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.**
Рекурсивные DNS-запросы	Разрешает или запрещает серверу осуществлять рекурсивные DNS-запросы. Рекомендуется оставить эту опцию включенной.
Максимальный TTL для DNS-записей	Устанавливает максимально возможное время жизни для записей DNS.
Лимит количества DNS-запросов в секунду на пользователя	Устанавливает ограничение на количество DNS-запросов в секунду для каждого пользователя. Запросы, превышающие данный параметр, будут отброшены. Значение по умолчанию - 100 запросов в секунду. Не рекомендуется ставить большие значения для данного параметра, поскольку DNS-флуд (DNS DoS attacks) является довольно частой причиной отказа обслуживания DNS-серверов.
Только A и AAAA DNS-записи для не идентифицированных пользователей (защита от VPN поверх DNS)	Если защита включена, то UserGate отвечает только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS.

С помощью правил DNS-прокси можно указать серверы DNS, на которые пересылаются запросы на определенные домены. Данная опция может быть полезна в случае, если внутри компании используется локальный домен, не имеющий связи с интернетом и использующийся для внутренних нужд компании, например, домен Active Directory.

Чтобы создать правило DNS-прокси, необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить правило.	Нажать на кнопку **Добавить**, задать **Название** и **Описание** (опционально).

Наименование	Описание
Шаг 2. Указать список доменов.	Задать список доменов, которые необходимо перенаправлять, например, localdomain.local. Допускается использование '*' для указания шаблона доменов.
Шаг 3. Указать DNS-серверы.	Задать список IP-адресов DNS-серверов, куда необходимо пересылать запросы на указанные домены.

Кроме этого, с помощью DNS-прокси можно задавать статические записи типа host (A-запись). Чтобы создать статическую запись, необходимо выполнить:

Наименование	Описание
Шаг 1. Добавить запись.	Нажать на кнопку **Добавить**, задать **Название** и **Описание** (опционально).
Шаг 2. Указать FQDN.	Задать **Fully Qualified Domain Name** (FQDN) статической записи, например, www.example.com.
Шаг 3. Указать IP-адреса.	Задать список IP-адресов, которые NGFW будет возвращать при запросе данного FQDN.

Виртуальные маршрутизаторы

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.

Примечание

Виртуальный 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.

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.
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.	

Наименование	Описание
	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.

Примечание

Если 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.

> **Примечание**
>
> **При 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	

Наименование	Описание
	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.
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.
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.

Наименование	Описание
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.

Наименование	Описание
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 ссылки	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.

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.

Наименование	Описание
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.

Наименование	Описание
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.

Наименование	Описание
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:

> **Внимание**
>
> **Для 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 }.

Наименование	Описание
	• 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.

Наименование	Описание
	◦ 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.

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.
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.

Наименование	Описание
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.

Наименование	Описание
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

Наименование	Описание
	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 ASM	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

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,

Наименование	Описание
	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.

Наименование	Описание
	• 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

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

> **Внимание!**
> **На версиях UserGate старше 6.1.8 этот раздел носит название *Сервера авторизации*.**

"Серверы аутентификации" - это внешние источники учетных записей пользователей(сервера аутентификации), например, LDAP-сервер, или серверы, производящие аутентификацию для UserGate, например, Radius, TACACS+, Kerberos, SAML. Система поддерживает следующие типы серверов аутентификации:

- LDAP-коннектор.
- Сервер аутентификации пользователей Radius.
- Сервер аутентификации пользователей TACACS+.
- Сервер аутентификации Kerberos.

Сервер аутентификации NTLM.

- Сервер аутентификации SAML (SSO).

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 аутентификацию 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 или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса.
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

Наименование	Описание
	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. **Примечание** **Рекомендуется загрузить keytab-файл даже в случае, если вы не планируете использовать авторизацию Kerberos. При загруженном keytab-файле UserGate использует механизм kerberos для получения списка пользователей и их групп с серверов LDAP, что очень сильно снижает нагрузку на серверы LDAP. Если у вас в организации серверы LDAP содержат большое количество объектов (более 1000 групп и пользователей) использование keytab-файла обязательно.**

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.

Примечание

Для аутентификации 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 аутентификации Radius позволяет аутентифицировать пользователей на серверах Radius, то есть UserGate выступает в роли Radius-клиента. При аутентификации через Radius-сервер UserGate 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 UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших авторизацию на сервере Radius) или **Unknown** (не прошедших аутентификацию).

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 аутентификации Radius. Более подробно о Captive-портале рассказывается в следующих главах руководства.

Сервер аутентификации пользователей TACACS+

Сервер аутентификации TACACS+ позволяет аутентифицировать пользователей на серверах TACACS+. При аутентификации через TACACS+ сервер UserGate 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 UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому в политиках фильтрации можно использовать только пользователей типа **Known** (успешно прошедших аутентификацию на сервере TACACS+) или **Unknown** (не прошедших аутентификацию).

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	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификации. По умолчанию это порт UDP 1812.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером 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 аутентифицировать 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. UserGate может быть

настроен в качестве SAML сервис-провайдера, использующего сервера SAML IDP для аутентификации клиента.

> **Внимание!**
> **Сервер SAML IDP не может предоставить свойства пользователей в UserGate 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).**

Настройка ADFS

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

Наименование	Описание
Шаг 1. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи соответствующие серверу UserGate для использования в качестве домена для auth.captive, например, utm.domain.loc. В качестве IP-адреса укажите адрес интерфейса UserGate, подключенного в сеть **Trusted**.
Шаг 2. Настроить DNS-серверы на UserGate.	В настройках UserGate 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.	Статью по настройке Microsoft ADFS можно найти на сайте Microsoft. Необходимо добавить на сервере SAML IDP запись о сервис-провайдере USERGATE, указывая созданное на шаге 1 FQDN имя. В процессе установки ADFS будет сгенерирована ссылка на xml-файл вида https://<adfs-server>/federationmetadata/2007-06/federationmetadata.xml с конфигурацией и сертификатом ADFS. Эта ссылка понадобится для настройки сервера SAML-авторизации на UserGate NGFW.
Шаг 5. Создать сервер авторизации пользователей SAML IDP.	Создать в USERGATE сервер аутентификации пользователей SAML IDP.

Настройка UserGate NGFW

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

Наименование	Описание
Шаг 1. Заполнить поле **SAML metadata URL**	**SAML metadata URL** - это путь где можно скачать xml-файл (полученный ранее при настройке ADFS) с корректной конфигурацией для сервис-провайдера (клиента) SAML. Также заполнить все необходимые поля кроме кроме **URL для метаданных SAML IDP** (оно появится после сохранения).
Шаг 2. Нажать на кнопку **Загрузить**	При этом происходит заполнение необходимых полей настройки сервера аутентификации данными, полученными из xml-файла.
Шаг 3. Нажать кнопку **Сохранить**	При этом произойдет автоматическое заполнение поля **URL для метаданных SAML IDP.**
Шаг 4. Открыть для редактирования только что созданный SAML IDP сервер.	Теперь можно скопировать автоматически сгенерированную ссылку на файл метаданных UserGate NGFW из поля **URL для метаданных SAML IDP.**
Шаг 5. Передать метаданные UserGate NGFW на сервер ADFS	С помощью данной ссылки нужно передать данные на ADFS сервер (в настройках ADFS сервера загрузить этот файл аналогично как это сделано на UserGate NGFW.).

Это предпочтительный метод настройки сервера аутентификации SAML IDP.

Описание полей Сервера авторизации доступных для заполнения:

Наименование	Описание
Включен	Включает или отключает использование данного сервера аутентификации.
Название сервера	Название сервера аутентификации.
Описание	Описание сервера аутентификации.
SAML metadata URL	URL до файла метаданных сервера ADFS, который необходимо получить. Создается при настройке ADFS.
Сертификат SAML IDP	

Наименование	Описание
	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. **Примечание** **Сертификат нужен для установки SSL\TLS соединения между ADFS и UserGate NGFW.**
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.
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 аутентификации с помощью NTLM сервер UserGate работает с контроллерами

домена, которые выполняют проверку пользователя, который получает доступ в интернет.

Сервер NTLM не может предоставить список пользователей в UserGate и, если пользователи не были заведены в UserGate предварительно (например, как локальные пользователи или получены из домена AD с помощью LDAP-коннектора), поэтому 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 UserGate не отличается от режима работы аутентификации.

Для настройки аутентификации с помощью NTLM необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. 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 2. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи, соответствующие серверу UserGate 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 UserGate, 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.

Наименование	Описание
Шаг 4. Добавить NTLM-сервер авторизации.	В разделе **Серверы авторизации** нажать на кнопку **Добавить**, выбрать **Добавить NTLM-сервер** и указать название и имя домена Windows. Для корректной работы авторизации NTLM, необходимо, чтобы указанное здесь имя домена разрешалось(resolve) в IP-адреса контроллеров домена.
Шаг 5. Создать правило Captive-портала с авторизацией NTLM.	Настроить Captive-портал для использования метода авторизации 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 UserGate в качестве адреса прокси сервера. **Примечание** **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 UserGate 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

Наименование	Описание
	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 аутентификации через Kerberos сервер UserGate работает с контроллерами домена, которые выполняют проверку пользователя, который получает 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 аутентификации Kerberos необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи, соответствующие серверу UserGate 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 UserGate, подключенного в сеть **Trusted**. **Примечание** **Для корректной работы создайте записи типа A, не используйте CNAME-записи.**
Шаг 2. Создать пользователя для сервера UserGate.	Создать пользователя в домене AD, например, kerb@domain.loc с опцией **password never expires**. Установите пароль пользователю kerb.

Наименование	Описание
	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.**
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.

Наименование	Описание
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 авторизацией 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**

Наименование	Описание
	(**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).

Критически важно!

Если браузер осуществляет запрос по https, но на NGFW дешифрование не настроено, то NGFW не в состоянии вмешаться в трафик и вставить туда требование авторизоваться по Kerberos. Для того, чтобы была возможность это сделать, в NGFW по умолчанию идёт правило *Decrypt all for unknown users*, которое включает дешифрование трафика для не авторизованных подключений.

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. Аутентификацию 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 аутентификации HTTP Basic необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать DNS-записи для сервера UserGate.	На контроллере домена создать DNS-записи, соответствующие серверу UserGate 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 UserGate, 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.

Наименование	Описание
	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 аутентификации 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 NTLM.
Шаг 5. Настроить прокси-сервер на компьютерах пользователей	На компьютерах пользователей указать обязательное использование прокси-сервера, указать IP-адрес Trusted интерфейса UserGate в качестве адреса прокси сервера.

Профили аутентификации

Внимание!

На версиях UserGate старше 6.1.8 этот раздел носит название *Профили авторизации*.

Профиль аутентификации позволяет указать набор способов и параметров аутентификации пользователей, которые в дальнейшем можно будет использовать для авторизации в различных подсистемах UserGate, 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 Captive-профиля.
Описание	Описание Captive-профиля.

Наименование	Описание
Профиль MFA	Профиль мультифакторной авторизации. Должен быть предварительно создан в разделе **Профили MFA**, если планируется использовать мультифакторную авторизацию с данным профилем аутентификации. Профиль определяет способ доставки одноразового пароля для второго метода авторизации. Более подробно о настройке профиля MFA смотрите в соответствующей главе далее. **Важно!** **Мультифакторная авторизация 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 авторизация невозможна для методов аутентификации Kerberos и NTLM.**
Время бездействия до отключения	Данный параметр определяет, через сколько секунд UserGate 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 UserGate 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 авторизации Active Directory или RADIUS. Если указано более одного метода аутентификации, то они будут использоваться в порядке, в котором они перечислены в консоли.

Наименование	Описание
	Также возможно использование встроенных механизмов авторизации, таких как: • **Локальный пользователь** - авторизация по базе данных локально заведенных пользователей. • **Принять политику** -- не требуется авторизация, но, прежде чем получить доступ в интернет, пользователь должен согласиться с политикой использования сети. Данный тип авторизации 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 с помощью Kerberos.

Настройка Captive-портала

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 веб-консоли UserGate 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 веб-консоли UserGate 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 веб-консоли UserGate 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 веб-консоли UserGate 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 UserGate для авторизации пользователей. Если клиенты используют в качестве DNS-сервера сервер UserGate, то ничего делать не надо. В противном случае необходимо прописать в качестве IP-адреса для этих доменов IP-адрес интерфейса сервера UserGate, 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.
Шаг 6. Разрешить работу сервисов Captive-портал и HTTP(S)-proxy в зоне.	В веб-консоли UserGate в разделе **Сеть → Зоны** выбрать зону источника Captive-правила с **Шага 4**, нажать кнопку **Редактировать**. В открывшемся окне перейти во вкладку **Конт**

Наименование	Описание
	роль доступа и установить флаги в пунктах **Captive-портал и страница блокировки** и **HTTP(S)-proxy**.

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 UserGate запомнит пользователя. Возможны 2 варианта: • **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. 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 сервером UserGate. Это рекомендуемое значение, устанавливаемое по умолчанию. • **Запоминать cookie**. После успешной авторизации пользователя через Captive-портал UserGate 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

Наименование	Описание
	пользователя UserGate 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.
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

Наименование	Описание
	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.

Наименование	Описание
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!** 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!** 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.

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

Примечание

Условия, 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.

Примечание

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

Примечание

При 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)

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

Наименование	Описание
	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.
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

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 авторизации** 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.

> **Примечание**
> **Имя компьютера должно состоять из букв, цифр и знака подчёркивания; использование тире не допускается.**

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 авторизации пользователей. Параметр ExcludeIP позволяет ограничить выход пользователей в Интернет с определённых IP-адресов терминального сервера (IP-адреса, с которых необходимо запретить трафик, указываются через запятую в виде **ExcludeIP=IP1,IP2**).

- **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"**.

Прокси-агент для Windows

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.

> **Примечание**
>
> **Прокси-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.

> **Примечание**
> **Прокси-агент совместим со всеми версиями ОС Windows, кроме Windows XP.**

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.

> **Примечание**
> **LocalNetwork — 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

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.

Наименование	Описание
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.

Наименование	Описание
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

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.

Наименование	Описание
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	Указанному пользователю присвоится переданный IP-адрес. Имя пользователя начнет отображаться в журналах для данного IP-адреса. Пользовательские правила начнут

Наименование	Описание
Acct-Status-Type = Start или Interim-Update.	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.

Политики BYOD

Многие компании поддерживают работу сотрудников с персональных устройств, принадлежащих самим сотрудникам. Это так называемые устройства BYOD (Bring Your Own Device). UserGate дает администратору возможность управлять BYOD устройствами, например, установив ограничения на типы разрешенных устройств, на количество устройств, с которых пользователь может получить доступ к сети одновременно, или указав конкретные устройства, с которых будет разрешен доступ в интернет.

Примечание

Управление BYOD требует наличия корректно настроенной авторизации пользователей через Captive-портал. Пользовательские устройства, не авторизованные с помощью Captive-портала, не могут управляться с помощью политик BYOD. Более подробно о Captive-портале смотрите в главе Настройка Captive-портала.

Для управления устройствами BYOD необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать правило Captive-портала.	Подробно о создании правил Captive-портала смотрите раздел Настройка Captive-портала.
Шаг 2. Создать политику BYOD.	Создать одно или несколько правил политики BYOD.

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

Если не создано ни одного правила, то разрешены все типы устройств.

Чтобы создать правило политики BYOD, необходимо нажать на кнопку **Добавить** в разделе правил **Политики BYOD** и указать необходимые параметры:

Наименование	Описание
Название	Название правила политики BYOD.
Описание	Описание правила политики BYOD.
Действие	**Разрешить**: разрешает подключение к сети устройств, удовлетворяющих условиям правила. **Запретить**: запрещает подключение к сети устройств, удовлетворяющих условиям правила.
Подтверждение администратора	Только для разрешающих правил. Если данная опция включена, то после первой успешной авторизации пользователя через Captive-портал устройство пользователя помещается в список устройств BYOD, но доступ в сеть не предоставляется до подтверждения данного устройства администратором.
Разрешено устройств всего	Только для разрешающих правил. Максимальное количество устройств, с которых пользователь может получать доступ в сеть. Если в правиле используются типы пользователей **Known**, **Unknown** или **Any**, то данный параметр не применяется.
Разрешено устройств одновременно	Только для разрешающих правил. Максимальное количество устройств, с которых пользователь одновременно может получать доступ в сеть. Если в правиле используются типы пользователей **Known**, **Unknown** или **Any**, то данный параметр не применяется.

Наименование	Описание
Пользователи и группы	Список пользователей и групп пользователей, для которых применяется данное правило политики BYOD.
Тип устройства	Тип устройств, для которых применяется данное правило политики BYOD.

Устройства, с которых пользователи подключаются в сеть, отображаются в разделе **Пользователи и устройства → Устройства BYOD**. Администратор может запретить доступ пользователя с определенного устройства, выбрав устройство в списке и нажав на кнопку **Отключить**, или разрешить доступ, нажав на кнопку **Включить**. Здесь же можно подтвердить доступ пользователя с определенного устройства в случае, если политика BYOD требует подтверждение устройства администратором.

Агент аутентификации для Windows

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 аутентификациии на все компьютеры, для которых необходимо идентифицировать пользователей. **Важно!** Агент аутентификации совместим со всеми версиями ОС Windows, кроме Windows XP. Агент аутентификации поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон,

Наименование	Описание
	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**.

Примечание

Адрес назначения "ServerIP" в настройках агента должен соответствовать адресу интерфейса на который приходят запросы агента.

Примечание

Журнал агента аутентификации можно найти здесь:

\Users\<username>\AppData\Roaming\Entensys\Entensys Auth Client\entsagent.log

ПОЛИТИКИ СЕТИ

Описание

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.

> **Примечание**
> **Правила, 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 необходимо наттирование 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

С помощью правил межсетевого экрана администратор может разрешить или запретить любой тип транзитного сетевого трафика, проходящего через UserGate. 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.

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

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

Примечание

Если не создано ни одного правила, то любой транзитный трафик через UserGate 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.

Наименование	Описание
	• **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. 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!** 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
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. 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!** 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.
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.

NAT и маршрутизация

В разделе **NAT и маршрутизация** администратор может создавать правила NAT, DNAT, Порт-форвардинга, Policy-based routing и Network mapping. UserGate 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.

Примечание

GeoIP 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**.

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

Чекбокс 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 при наттировании пакетов. Имеет смысл в случае наличия нескольких IP-адресов, назначенных интерфейсам зоны назначения. Если оставить это поле пустым, то система будет использовать произвольный 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 UserGate 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.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. 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!** 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. 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!** 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.

Примечание

Рекомендуется 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.

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

Чекбокс 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 при наттировании пакетов; если SNAT IP не указан, то адрес источника будет заменён на адрес интерфейса UserGate, 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 чекбокс **Включить SNAT**.
Журналирование	

Наименование	Описание
	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. 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!** 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 сервера UserGate, 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	

Наименование	Описание
	При включении данной опции UserGate будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.

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.

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

Чекбокс 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**.
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.

Наименование	Описание
	• **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. 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!** 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. 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!** 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 UserGate: 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.

Наименование	Описание
Включить SNAT	При включении данной опции UserGate будет изменять адрес источника в пакетах из внешней сети на свой IP-адрес.

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.

Примечание

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

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

Чекбокс 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.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. 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!** 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.

Наименование	Описание
Назначение	Зона, списки IP-адресов, списки гео IP-адресов, списки URL назначения трафика. Список URL должен включать только имена доменов. 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!** 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

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.

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.

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. 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!** 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. 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!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;

Наименование	Описание
	• 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.

Балансировка нагрузки

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 **weight**

Наименование	Описание
	ed 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.

Наименование	Описание
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.
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.

Примечание

Правила 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.

Наименование	Описание
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

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

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

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

Внимание!

Ширина полосы пропускания не является инклюзивной для пользователей указанных в правиле и распределяется на всех пользователей (указаных в правиле) в равных пропорциях.

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 приоритезации 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.

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. • **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. 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!** 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. 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!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;

Наименование	Описание
	• 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

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

С помощью правил фильтрации контента администратор может разрешить или запретить определенный контент, передаваемый по протоколам HTTP и HTTPS, если настроено инспектирование HTTPS. Более того, UserGate может блокировать HTTPS-трафик без дешифрования контента, но только в случае применения правил блокирования по категориям контентной фильтрации UserGate URL filtering или по спискам URL, в которых указаны только имена хостов. В этих случаях UserGate 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.

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

> **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**
> **Если 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

Наименование	Описание
	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 UserGate. 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. 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!** 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.

Наименование	Описание
	Список URL должен включать только имена доменов. 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!** 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.

Наименование	Описание
	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 реферер 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.

Веб-безопасность

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. UserGate 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. UserGate может блокировать приложения, не затрагивая при этом обычную функциональность социальных сетей.

В качестве условий правила могут выступать:

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

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

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

Примечание

Если 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.**

Наименование	Описание
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. 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!** 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.

Инспектирование SSL

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.

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

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

Примечание

Если 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**.
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.

Наименование	Описание
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. 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!** 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.
Адрес назначения	Списки IP-адресов назначения трафика. **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.

Наименование	Описание
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.

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

Инспектирование SSH

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.

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

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

> **Примечание**
>
> **Если 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

Наименование	Описание
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!** 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!** 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.
Время	Временной интервал, в течение которого правило активно. Можно добавить разнообразные периоды в разделе Календари.

Система обнаружения и предотвращения вторжений

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	

Наименование	Описание
	Протокол, для которого разработана данная сигнатура: • IP. • ICMP. • TCP. • UDP.
ОС	Операционная система, для которой разработана данная сигнатура.
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.

Наименование	Описание
	• 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.

Наименование	Описание
	• 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.

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).

Примечание

Правилами 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.

Примечание

Если 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. 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!** 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. 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.

Наименование	Описание
	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.

Правила АСУ ТП

С помощью правил АСУ ТП администратор может контролировать прохождение трафика автоматизированных систем управления технологическим производством (АСУ ТП) через UserGate. UserGate поддерживает контролирование следующих протоколов АСУ ТП:

- IEC 104 (ГОСТ Р МЭК 60870-5-104).
- Modbus.
- DNP3.
- MMS.
- OPC UA.

Администратору доступна возможность задать интересующие его профили АСУ ТП, в которых указать необходимый набор протоколов и команд, и использовать их в правилах.

Для начала работы с АСУ ТП необходимо:

Наименование	Описание
Шаг 1. Разрешить сервис SCADA на необходимой зоне.	В разделе **Сеть → Зоны** разрешить сервис SCADA для той зоны, со стороны которой будет инициирован трафик АСУ ТП.
Шаг 2. Создать необходимые профили АСУ ТП.	Профиль АСУ ТП - это набор элементов, каждый из которых состоит из определенной команды АСУ ТП и адреса.
Шаг 3. Создать требуемые правила АСУ ТП.	Правила АСУ ТП определяют действие для выбранного типа трафика, который будет проверяться модулем АСУ ТП в соответствии с назначенными профилями.

Для настройки профилей АСУ ТП необходимо создать профиль в разделе **Библиотеки → Профили АСУ ТП** и затем добавить в него необходимые команды. Каждая запись имеет определенные поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Записывать в журнал правил	При активации данной опции информация о срабатывание правила будет регистрироваться в соответствующем журнале статистики.
Протокол	Выберите протокол АСУ ТП.
Команда АСУ ТП	Выберите необходимую команду АСУ ТП.
Адрес АСУ ТП	Укажите адрес АСУ ТП. Можно указать целое 4-байтовое число.

Правила АСУ ТП определяют трафик, к которому применяется профиль АСУ ТП и действие, которое UserGate должен предпринять при срабатывании правила.

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

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

Для создания правила АСУ ТП необходимо нажать на кнопку **Добавить** в разделе **Политики безопасности → АСУ ТП** и заполнить поля правила.

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: • **Пропускать**: не блокировать трафик. • **Блокировать**: блокировать и записать в журнал. Дополнительно можно выбрать опцию **Записывать в журнал правил**, в этом случае факт применения правила к трафику будет записан в соответствующий журнал.
Источник	Зона, списки IP-адресов источника трафика.
Назначение	Списки IP-адресов назначения трафика.
Сервис	Сервис L4, для которого будет действовать данное правило.
Профили АСУ ТП	Список профилей АСУ ТП, созданных на предыдущем шаге.

Сценарии

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.

> **Примечание**
>
> **Сценарий 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.

Наименование	Описание
	• **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

UserGate 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 UserGate будет выступать в роли ICAP-клиента.

UserGate 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.

Для того, чтобы настроить работу UserGate 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 UserGate посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен.
Пропускать при ошибках	Если эта опция включена, то UserGate 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 Reqmod.
	• **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.

Наименование	Описание
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.
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.

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

Чекбокс 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 UserGate будет пересылать запросы.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Каждые 5 минут UserGate производит разрешение

Наименование	Описание
	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!** 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!** 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.
Сервис	Возможны варианты: • HTTP - веб-трафик. • SMTP - почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа.

Наименование	Описание
	• 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.

Защита почтового трафика

ЗАЩИТА ПОЧТОВОГО ТРАФИКА

При наличии настроенной проверки почтового трафика, UserGate 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 UserGate 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 UserGate.

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.

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

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

Примечание

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	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.

Наименование	Описание
	• **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.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. 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!** 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!** Обработка трафика происходит по следующей логике: • условия объединяются по ИЛИ, если указаны несколько списков IP-адресов и/или доменов;

Наименование	Описание
	• 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.

Проверка почтового трафика (Антиспам)

При наличии настроенной проверки почтового трафика, UserGate 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 3 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;**

- **блокировка или маркировка сообщений по результатам проверки на вирусы; требует наличия так же лицензии на Эвристический движок;**
- **маркировка сообщений по результатам проверки на спам; требует наличия так же *лицензии на Эвристический анализ*;**

> **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 UserGate 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 анализ каких-то дополнительных данных. В самих правилах можно добавлять списки адресов на вкладках envelop from / envelop 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.

Защита от DoS атак

UserGate 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 UserGate. При создании профиля необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Агрегировать	Данная настройка регулирует, будет ли UserGate 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 UserGate 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.

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

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

Внимание!

Защита от DoS атак работает только для транзитного трафика!

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.

Наименование	Описание
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.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. 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!** 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.

Наименование	Описание
	Список URL должен включать только имена доменов. 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!** 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.

Защита почтового трафика

При наличии настроенной проверки почтового трафика, UserGate 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 UserGate 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 UserGate.

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.

Наименование	Описание
Шаг 3. Создать правила защиты почтового трафика.	Создать необходимые правила защиты почтового трафика. Более подробно создание правил описано ниже в этой главе.

Примечание

При настройке правила защиты почтового трафика, если в правиле DNAT указан почтовый протокол, то он перенаправляется в модуль защиты почтового трафика. Например, если в правиле DNAT вместе с почтовым протоколом указан сервис HTTPS, то он также попадает под правило защиты почтового трафика и блокируется, а правило DNAT для порта 443 не работает. Для сервиса HTTPS должно быть выделено отдельное правило DNAT для доступа к почтовому серверу.

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.

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

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

Примечание

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	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.
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. Каждые 5 минут UserGate производит разрешение

Наименование	Описание
	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!** 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!** 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.

ГЛОБАЛЬНЫЙ ПОРТАЛ

Описание

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.

Веб-портал (SSL VPN)

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.

> **Примечание**
> **Если на целевых HTTP-ресурсах настроена аутентификация Kerberos или NTLM, то UserGate 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 UserGate, 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 авторизации	Профиль авторизации пользователей, который будет использоваться для авторизации пользователей, подключающихся к веб-порталу. Профиль авторизации задает метод авторизации, например, AD-коннектор или локальный пользователь. Также в профиле авторизации можно указать требование использовать мультифакторную авторизацию для доступа к веб-порталу. Более подробно о профилях авторизации смотрите раздел руководства Профили авторизации.
Шаблон страницы авторизации	Выбрать шаблон страницы авторизации, который будет использоваться для отображения формы для ввода логина и пароля. Создать свою страницу авторизации можно в разделе Шаблоны страниц.

Наименование	Описание
Шаблон портала	Выбрать шаблон веб-портала, который будет использоваться для отображения ресурсов, доступных через веб-портал. Создать свою страницу авторизации можно в разделе Шаблоны страниц.
Предлагать выбор домена AD/LDAP на странице авторизации	Показывать выбор домена на странице авторизации веб-портала.
Показывать CAPTCHA	При включении данной опции пользователю будет предложено ввести код, который ему будет показан на странице авторизации 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.
Авторизация пользователя по сертификату	Если выбрано, то требует предъявления пользовательского сертификата браузером. Для этого пользовательский сертификат должен быть добавлен в список сертификатов UserGate, ему должна быть назначена роль **Пользовательский сертификат** и назначен соответствующий пользователь UserGate. 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.

Наименование	Описание
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.
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.

Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси

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.

Наименование	Описание
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

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

Наименование	Описание
Включено	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Сервер reverse-прокси	Сервер reverse-прокси или балансировщик reverse-прокси, куда UserGate будет пересылать запросы.
Порт	Порт, на котором UserGate 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 UserGate, ему должна быть назначена роль **Пользовательский сертификат** и назначен соответствующий пользователь UserGate. Более подробно о пользовательских сертификатах читайте в разделе Управление сертификатами.

Наименование	Описание
Источник	Зона, списки IP-адресов, списки гео IP-адресов, списки URL источника трафика. Список URL должен включать только имена доменов. 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!** 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	Один из внешних IP-адресов сервера UserGate, 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; • 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.

Наименование	Описание
	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.

НАСТРОЙКА VPN

Описание

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 удаленного доступа клиентов (Remote access VPN)

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 вNGFW создано правило **NAT from VPN for remote access to Trusted and Untrusted**, разрешающее наттирование 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.

Наименование	Описание
	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***
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

Наименование	Описание
	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,

Наименование	Описание
	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

Наименование	Описание
	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**.
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.

Наименование	Описание
	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.

Наименование	Описание
	• **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.	

Наименование	Описание
	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.**

Наименование	Описание
	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).

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

Наименование	Описание
	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.
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 **Доб авить** 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

Наименование	Описание
	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

Наименование	Описание
	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. 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.

Наименование	Описание
	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.
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. Для создания туннеля VPN перейдите в раздел **VPN → Сети VPN**, нажмите кнопку **Добавить** и заполните следующие поля: • **Название** — название сети. • **Описание** — описание сети.

Наименование	Описание
	• **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.

Наименование	Описание
	• **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

Наименование	Описание
	разрешающее правило межсетевого экрана, указав нужную зону источника и зону назначения **VPN for Site-to-Site**.
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,

Наименование	Описание
	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,

Наименование	Описание
	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.

Наименование	Описание
	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 (для подключения к VPN-серверу NGFW) или IPsec туннель для подключения к VPN-серверу Cisco. • **Подсети для Cisco VPN** — IP адрес сети, которая будет доступна для клиентов со стороны NGFW (разрешенные подсети со стороны Cisco) и со стороны VPN-сервера Cisco (разрешенные подсети со стороны NGFW).

Наименование	Описание
	• **Имя пользователя и пароль** (только для протокола L2TP) — имя и пароль пользователя, созданного на шаге 1 при подготовке VPN-сервера.

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).

IPsec over GRE

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

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

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

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.

Наименование	Описание
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 устройства 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**.
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

Наименование	Описание
	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".

Примечание

При 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.

Сервисы

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.

IP-адреса

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 компьютеры с установленным UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
	Создать файл **list.txt** со списком адресов.

Наименование	Описание

Шаг 1. Создать файл с необходимыми IP-адресами.	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.

Наименование	Описание
	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".

Useragent браузеров

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 компьютеры с установленным 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.

Наименование	Описание
	• 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".

Типы контента

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 компьютеры с установленным

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.

Наименование	Описание
	• 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".

Списки URL

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. Более подробно о лицензии на продукт вы можете прочитать в главе 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.

Наименование	Описание
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.
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.	Смотрите раздел 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 «$»:

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

^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

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и домены 3 уровня, например: sport.yahoo.com mail.yahoo.com а также: qweryahoo.com	Блокируется весь домен и все URL этого домена и домены 3 уровня, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123 http://qwertyahoo.com/
^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 компьютеры с установленным NGFW. 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

Наименование	Описание
	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".

Календари

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

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 DCSP для QoS.	Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63.

Профили АСУ ТП

Профиль АСУ ТП - это набор элементов, каждый из которых состоит из определенной команды АСУ ТП и адреса. Профиль АСУ ТП используется в правилах АСУ ТП. Более подробно о фильтрации трафика АСУ ТП читайте в разделе Правила АСУ ТП.

Шаблоны страниц

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.

Наименование	Описание
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.

Наименование	Описание
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

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.

Измененные категории URL

Элемент библиотеки **Измененные категория URL** позволяет администратору назначить определенным сайтам категории, отличные от категорий, назначенных техническими специалистами UserGate. Такая потребность может

возникнуть в случае некорректного категорирования сайтов или в случае, если требуемый сайт не имеет назначенной ему категории. Для переопределения категории сайта необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Проверить первоначальную категорию сайта.	В разделе **Библиотеки → Измененные категории URL** ввести требуемый адрес сайта в строку проверки и нажать на кнопку **Проверить категорию**.
Шаг 2. Назначить новую категорию.	Если полученная категория не совпадает с требуемой, то необходимо нажать на кнопку **Добавить** и назначить до двух новых категорий.

После успешного изменения категории сайт будет отображаться в списке сайтов с измененными категориями. Для него также будет указаны дата изменения категории, администратор, выполнивший данное изменение, его оригинальные и новые категории.

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**.

Администратор может экспортировать списки сайтов с измененными категориями или импортировать любые списки сайтов и назначить им требуемые категории.

Приложения

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.

Наименование	Описание
Шаг 2. Добавить приложения.	Выделить созданную группу и в панели **Приложения**, нажать на кнопку **Добавить** и выбрать необходимые приложения из списка.

Почтовые адреса

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 компьютеры с установленным NGFW. 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.

Наименование	Описание
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".

Номера телефонов

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 компьютеры с установленным NGFW. 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.

Наименование	Описание
	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".

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. Более подробно о создании и использовании профилей СОВ смотрите в разделе Система обнаружения и предотвращения вторжений.

Профили оповещений

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.

Наименование	Описание
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

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	

Наименование	Описание
	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 SSL

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.

Наименование	Описание
	Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем.
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 CHACHA20 POLY1305 SHA256 • 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 DHE RSA with CHACHA20 POLY1305 SHA256 • TLS DHE RSA with DES CBC SHA • 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 ECDSA with CHACHA20 POLY1305 SHA256 • TLS ECDHE ECDSA with RC4 128 SHA • TLS ECDHE RSA with 3DES EDE CBC SHA

Наименование	Описание
	• 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 ECDHE RSA with CHACHA20 POLY1305 SHA256 • TLS ECDHE RSA with RC4 128 SHA • 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 ECDSA with RC4 128 SHA • 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 ECDH RSA with RC4 128 SHA • TLS GOST2012256 with 28147 CNT IMIT • TLS GOSTR341001 with 28147 CNT IMIT • TLS RSA PSK with 3DES EDE CBC SHA • TLS RSA PSK with AES 128 CBC SHA • TLS RSA PSK with AES 128 CBC SHA256 • TLS RSA PSK with AES 128 GCM SHA256 • TLS RSA PSK with AES 256 CBC SHA • TLS RSA PSK with AES 256 CBC SHA384 • TLS RSA PSK with AES 256 GCM SHA384 • TLS RSA PSK with RC4 128 SHA • 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

Наименование	Описание
	• TLS RSA with AES 256 CBC SHA • TLS RSA with AES 256 CBC SHA256 • TLS RSA with AES 256 GCM SHA384 • TLS RSA with DES CBC SHA • TLS RSA with RC4 128 MD5 • TLS RSA with RC4 128 SHA • TLS SRP DSS with 3DES EDE CBC SHA • TLS SRP DSS with AES 128 CBC SHA • TLS SRP DSS with AES 256 CBC SHA • TLS SRP RSA with 3DES EDE CBC SHA • TLS SRP RSA with AES 128 CBC SHA • TLS SRP RSA with AES 256 CBC SHA
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

Наименование	Описание
	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!

ДАШБОРД

Приборная панель (DashBoard)

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.

Наименование	Описание
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.

Примечание

Доступно использование выделения для более подробного ознакомления с определённой частью графика; для возвращения необходимо использовать двойной клик левой кнопкой мыши.

ГОСТЕВОЙ ПОРТАЛ

Управление гостевыми пользователями

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.

Наименование	Описание
	• 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	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.

Наименование	Описание
предыдущем шаге Captive-профиль.	

ПОМОЩЬ

Помощь(описание)

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)

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.

Наименование	Описание
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.

ДИАГНОСТИКА И МОНИТОРИНГ

Мониторинг трафика

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.

> **Примечание**
>
> **Процесс 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

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 **S** 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

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

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

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 **О становить запись.**
Шаг 4. В разделе **Файлы**, скачать полученный файл.	Скачать pcap-файл для анализа.

Запросы в белый список

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.**

Наименование	Описание
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

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.

Наименование	Описание
	• **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.

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

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.

Наименование	Описание
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

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

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.

ОПОВЕЩЕНИЯ

Оповещения

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.

Наименование	Описание
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

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, во вкладке **Контроль доступа** разрешить сервис **SNMP**.

2. Создать правило SNMP

Для настройки мониторинга с помощью SNMP необходимо создать правила SNMP. Для создания правила SNMP необходимо в разделе **SNMP** нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Название правила	Название правила.
IP-адрес сервера для трапов	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.

Наименование	Описание
Комьюнити	SNMP community — строка для идентификации сервера 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	Указывает версию 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 авторизации 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.

Наименование	Описание
События	Выбор типов параметров, доступных для мониторинга по правилу.

> **Примечание**
> **Настройки 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 настройками SNMP в UserGate.**

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

Кнопка **Скачать MIB** позволяет скачать mib-файлы с параметрами мониторинга UserGate для последующего использования их в SNMP-менеджере. UserGate выделен 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

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.

Наименование	Описание
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.
trapLowMemory	Высокая загрузка памяти.
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

Наименование	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.

Наименование	Тип данных	Описание
utmHAStatus	integer	Текущий статус узла кластера отказоустойчивости: • **0** — master-узел. • **1** — slave-узел. • **3** — fault.
utmHAStatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: • **1** — связь с узлом потеряна. • **2** — HTTP прокси-сервер недоступен. • **3** — ни один из шлюзов недоступен. • **4** — DNS-сервер недоступен. • **5** — узел 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 %.
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

Наименование	Тип данных	Описание
		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 произойдёт 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.

Наименование	Тип данных	Описание
utmPowerSupplyStatus	integer	Состояние источника питания: • **no_power_supplies**. • **0** — off. • **1** — on.
utmCSCIfName	string	Название интерфейса.
utmCSCStatus	integer	Статус сетевого адаптера: • **1** — кабель подключен. • **2** — кабель не подключен.
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается в %.
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	

Наименование	Тип данных	Описание
		Состояние первого источника питания: • **no_power_supplies**. • **on**. • **off**.
Sys_power_supply2_status	string	Состояние второго источника питания: • **no_power_supplies**. • **on**. • **off**.
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

Наименование	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, определённый в

Наименование	Тип данных	Описание
		соответствии с протоколом физического/канального уровней: • **1** — other — неизвестный тип. • **2** — regular1822 — определён в BBN Report 1822. • **3** — hdh1822 — определён в BBN Report 1822. • **4** — ddn-x25 — определён в BBN Report 1822. • **5** — определён в стандарте канального уровня сетевой модели OSI X.25. • **6** — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • **7** — iso88023-csmacd — определён в IEEE 802.3. • **8** — iso88024-tokenBus — определён в стандарте IEEE 8802.4. • **9** — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5. • **10** — iso88026-man — определён в стандарте ISO 88026 "MAN". • **11** — starLan — определён в стандарте IEEE 802.3e. • **12** — proteon-10Mbit — Proteon 10 Mbit

Наименование	Тип данных	Описание
		• **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.

Наименование	Тип данных	Описание
		• **22** — propPointToPointSerial — определён 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); определён 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.

Наименование	Тип данных	Описание
		• **29** — ultra --ULTRA Technologies. • **30** — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексирование м сигналов DS1 и DS2; также называется T3. • **31** — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • **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.
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес).
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: • **1** — up — готов для передачи пакетов. • **2** — down — не работает.

Наименование	Тип данных	Описание
		• **3** — testing — в режиме тестирования; рабочие пакеты не могут быть переданы.
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** — notPresente — 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

Наименование	Тип данных	Описание
		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.

Наименование	Тип данных	Описание
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,

Наименование	Тип данных	Описание
		которые были отброшены или не отправлены.
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта **ifInOctets** — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInUcastPkts** — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifInMulticastPkts** — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifInBroadcastPkts** — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOutOctets	counter64	Смысл одинаков со смыслом объекта **ifOutOctets** — количество байтов, переданное данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOutUcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutUcastPkts** — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.

Наименование	Тип данных	Описание
ifHCOutMulticastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutMulticastPkts** — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOutBroadcastPkts	counter64	Смысл одинаков со смыслом объекта **ifOutBroadcastPkts** — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • **1** — enabled — включено. • **2** — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • **1** — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • **2** — false — интерфейс принимает только пакеты/кадры, адресованные этой станции.

Наименование	Тип данных	Описание
		Значение объекта не влияет на приём 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 счётчиков интерфейса.

ЖУРНАЛЫ И ОТЧЕТЫ

ЖУРНАЛЫ

Описание

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.

> **Примечание**
>
> **Записи 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

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

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.

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

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.

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

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры СОВ, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Файлы Pcap.
- Узел UserGate, 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

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

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

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

Количество записей, регистрируемых в журналах, как правило, очень велико, и не все поля доступны в базовом режиме просмотра. UserGate 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,

Наименование	Описание
	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.

При составлении расширенного запроса UserGate 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 UserGate автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Экспорт журналов

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**.

> **Примечание**
>
> **Если 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.

Наименование	Описание
	• **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.
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.

Наименование	Описание
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

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.**

Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

- **Шаблоны отчетов**
- **Правила отчетов**
- **Созданные отчеты**

Шаблоны отчетов

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

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.

Наименование	Описание
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.

Наименование	Описание
	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**.

Примечание

Процесс 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.

Примечание

Для 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.

Созданные отчеты

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).

ПРИЛОЖЕНИЯ

Установка сертификата локального удостоверяющего центра

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:

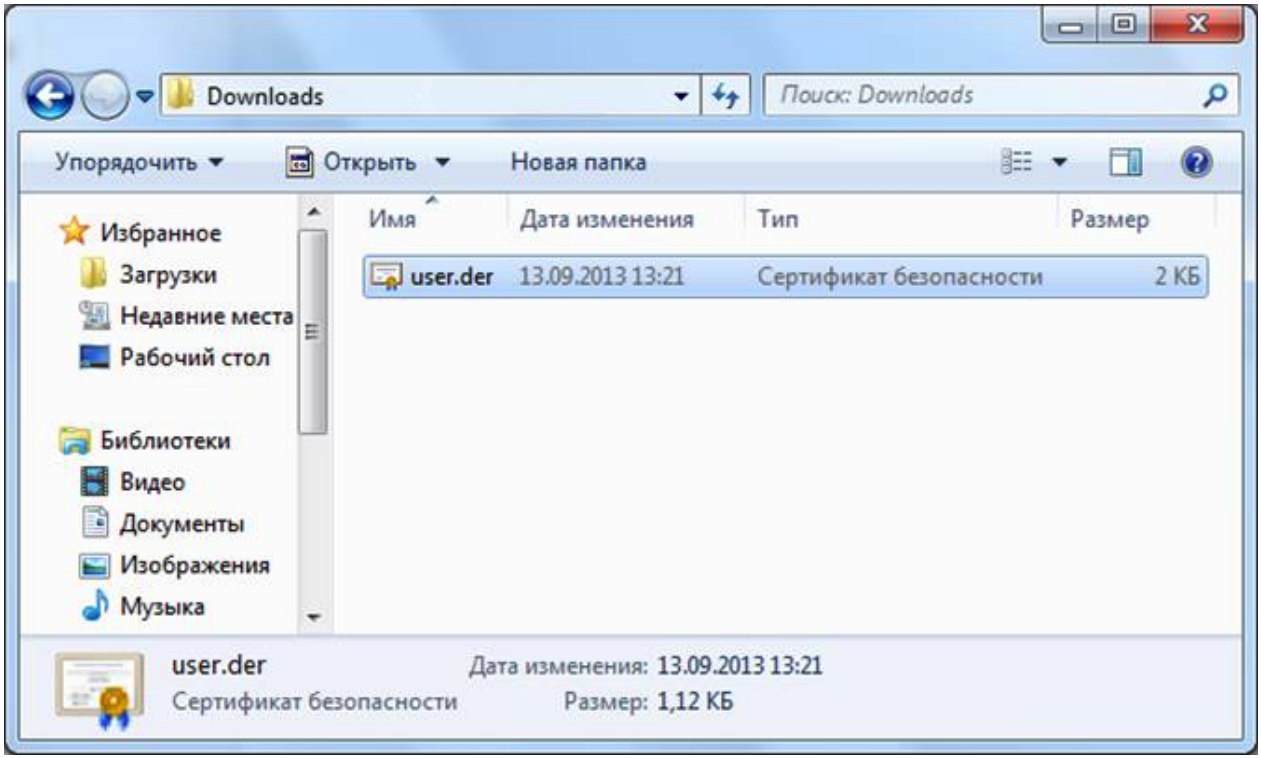


Рисунок 5 Выбор файла сертификата

Откроется информация о сертификате. Нажмите на кнопку **Установить сертификат**:

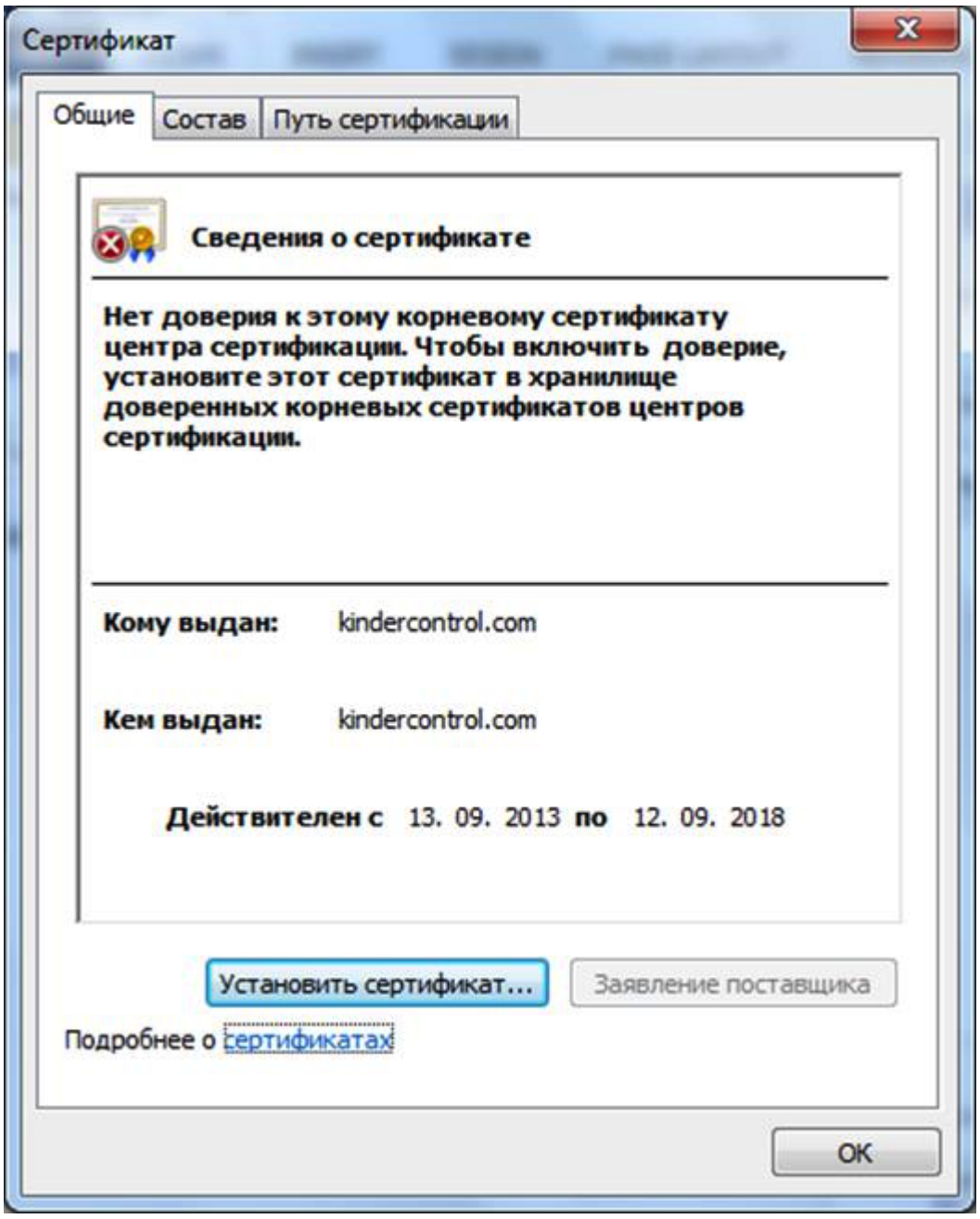


Рисунок 6 Установка сертификата

Запустится мастер импорта сертификатов. Выполните импорт, следуя всем рекомендациям, предлагаемым мастером импорта сертификатов:

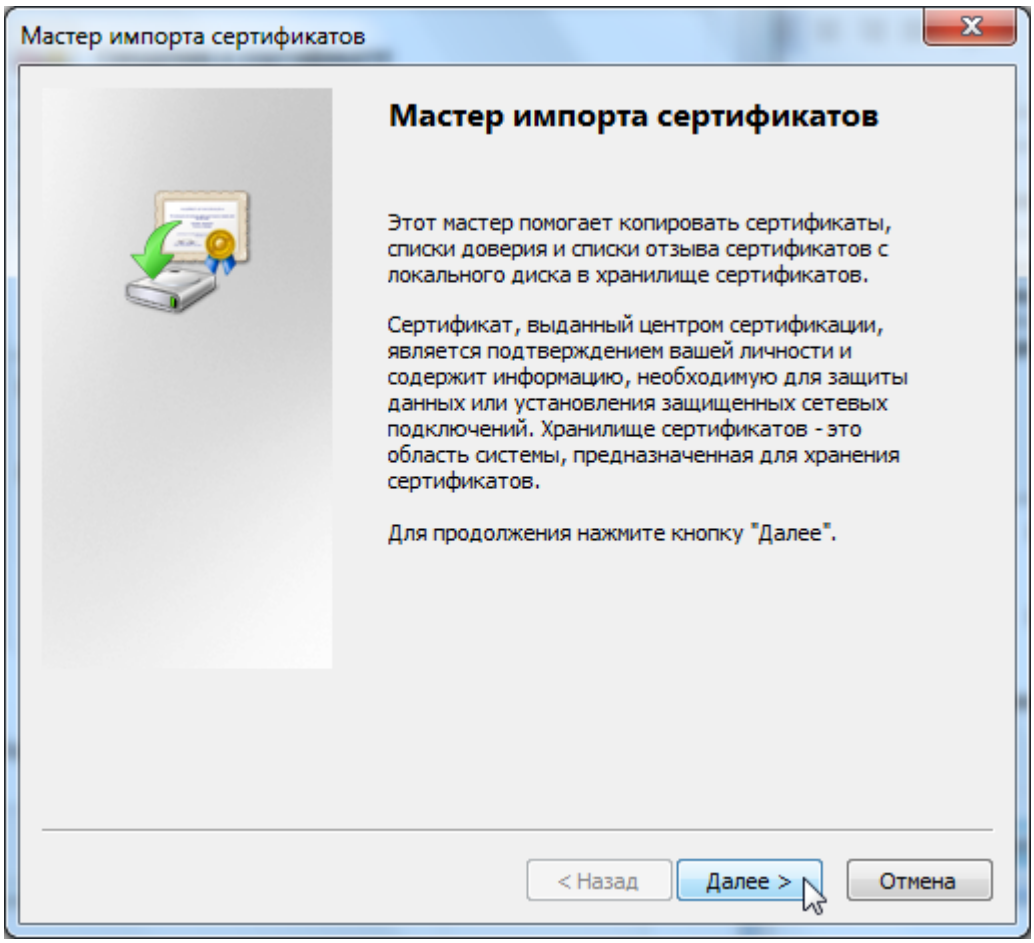


Рисунок 7 Мастер импорта сертификатов

Выберите хранилище сертификата и нажмите кнопку **Обзор**:

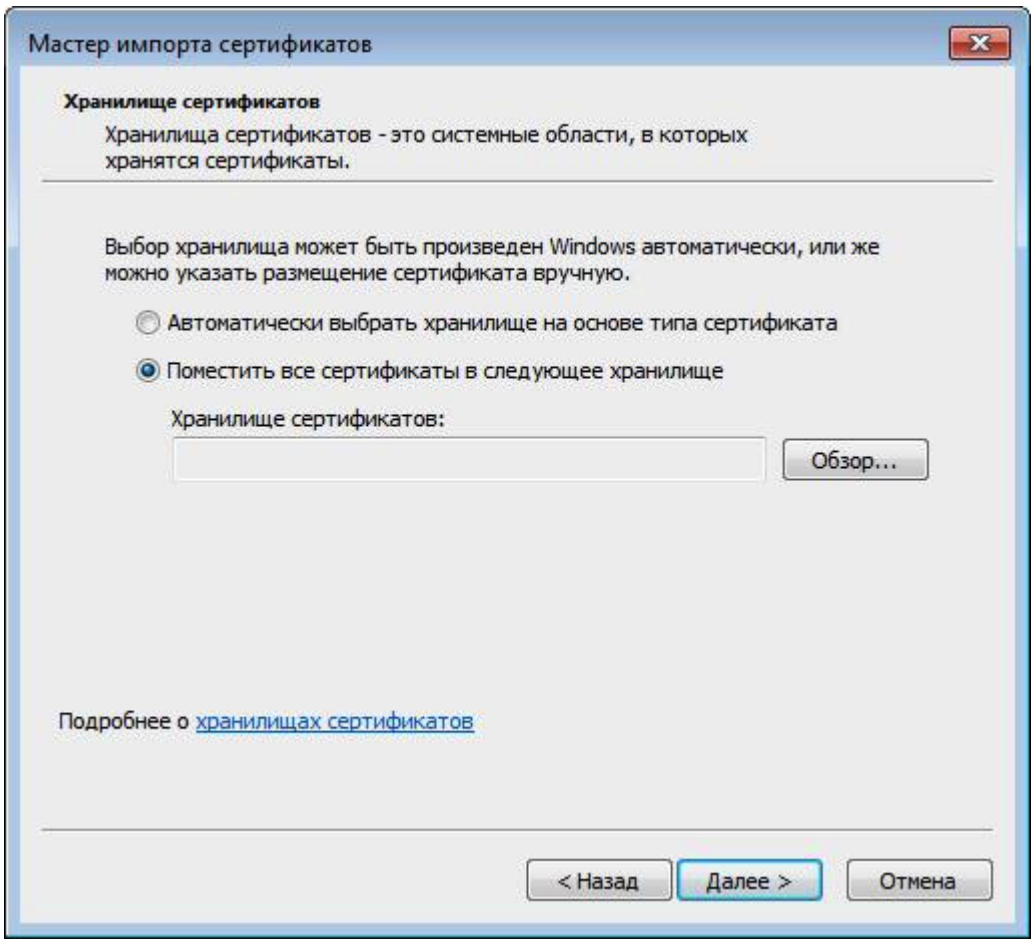


Рисунок 8 Выбор хранилища

Выберите **Доверенные корневые центры сертификации** и нажмите кнопку **ОК**:

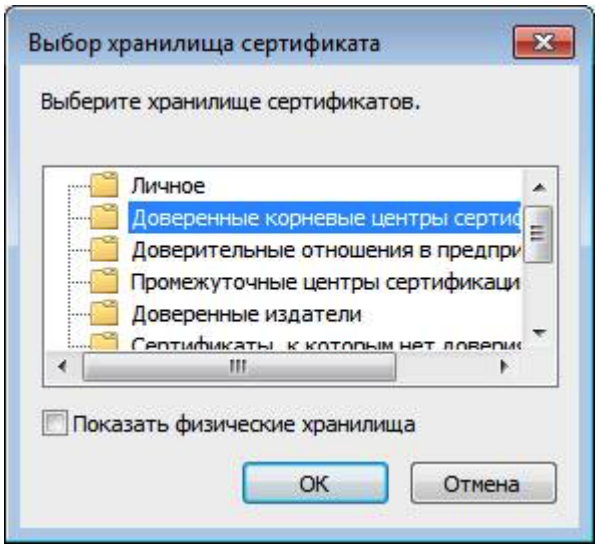


Рисунок 9 Выбор хранилища (продолжение)

Нажмите кнопку «Готово»:

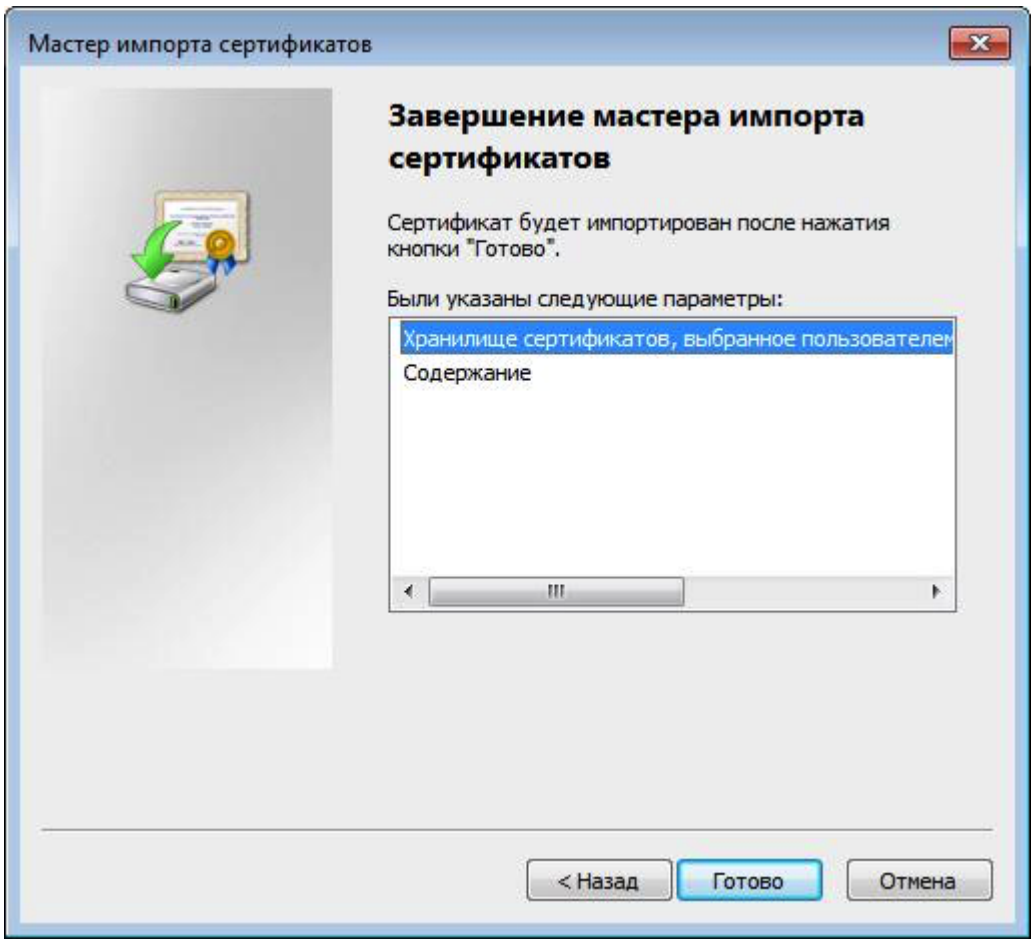


Рисунок 10 Завершение импорта

Когда появится предупреждение системы безопасности, нажмите кнопку **Да**:

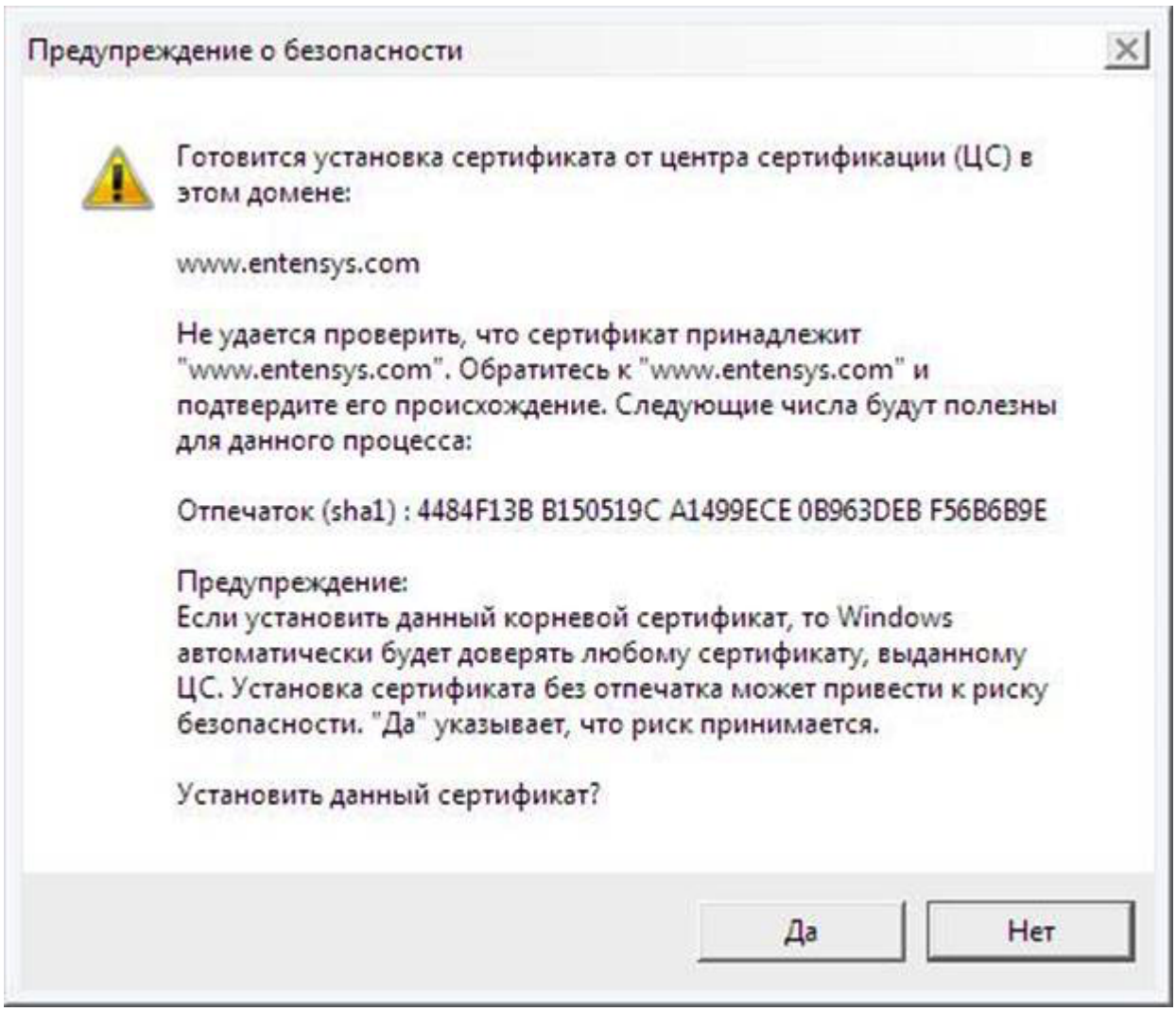


Рисунок 11 Согласие на установку сертификата

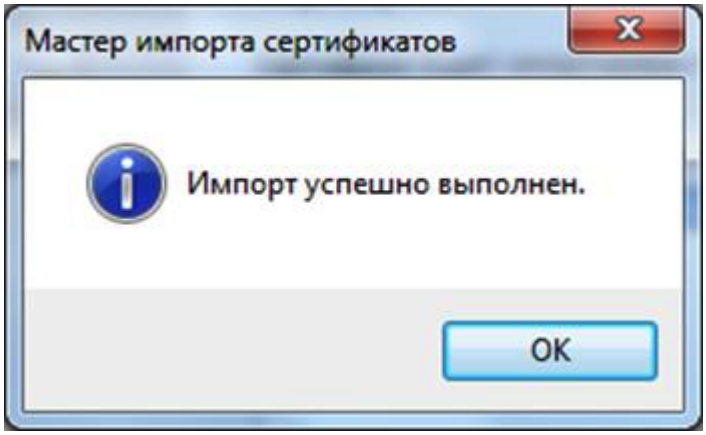


Рисунок 12 Установка завершена

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:

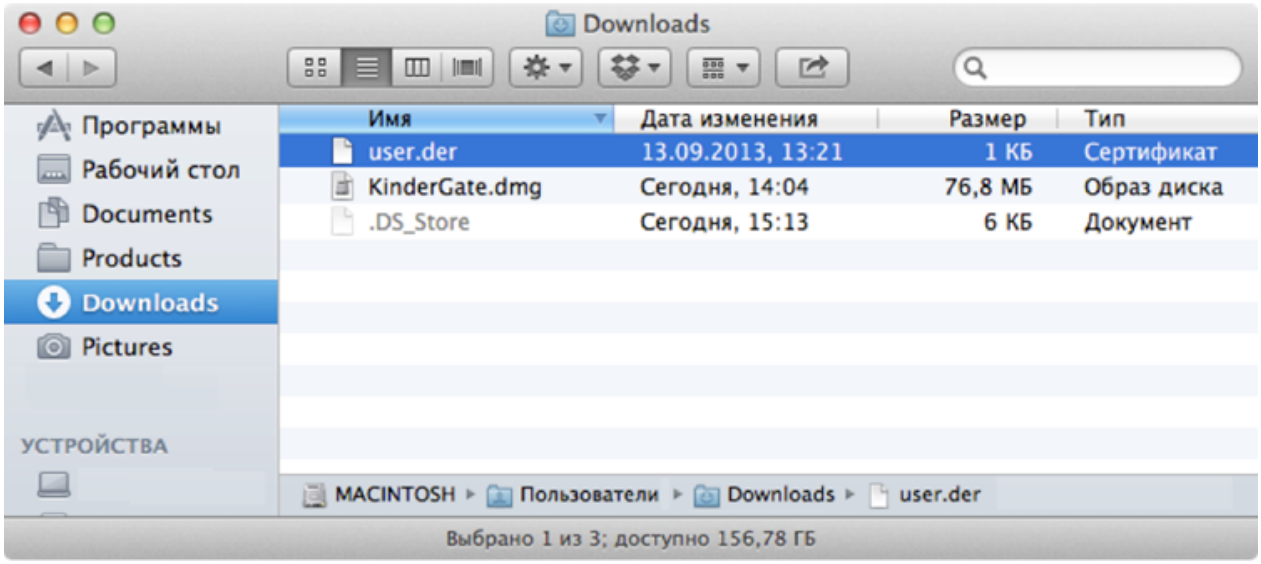


Рисунок 13 Выбор файла сертификата

Запустится программа **Связка ключей**. Выберите **Всегда доверять** данному сертификату:

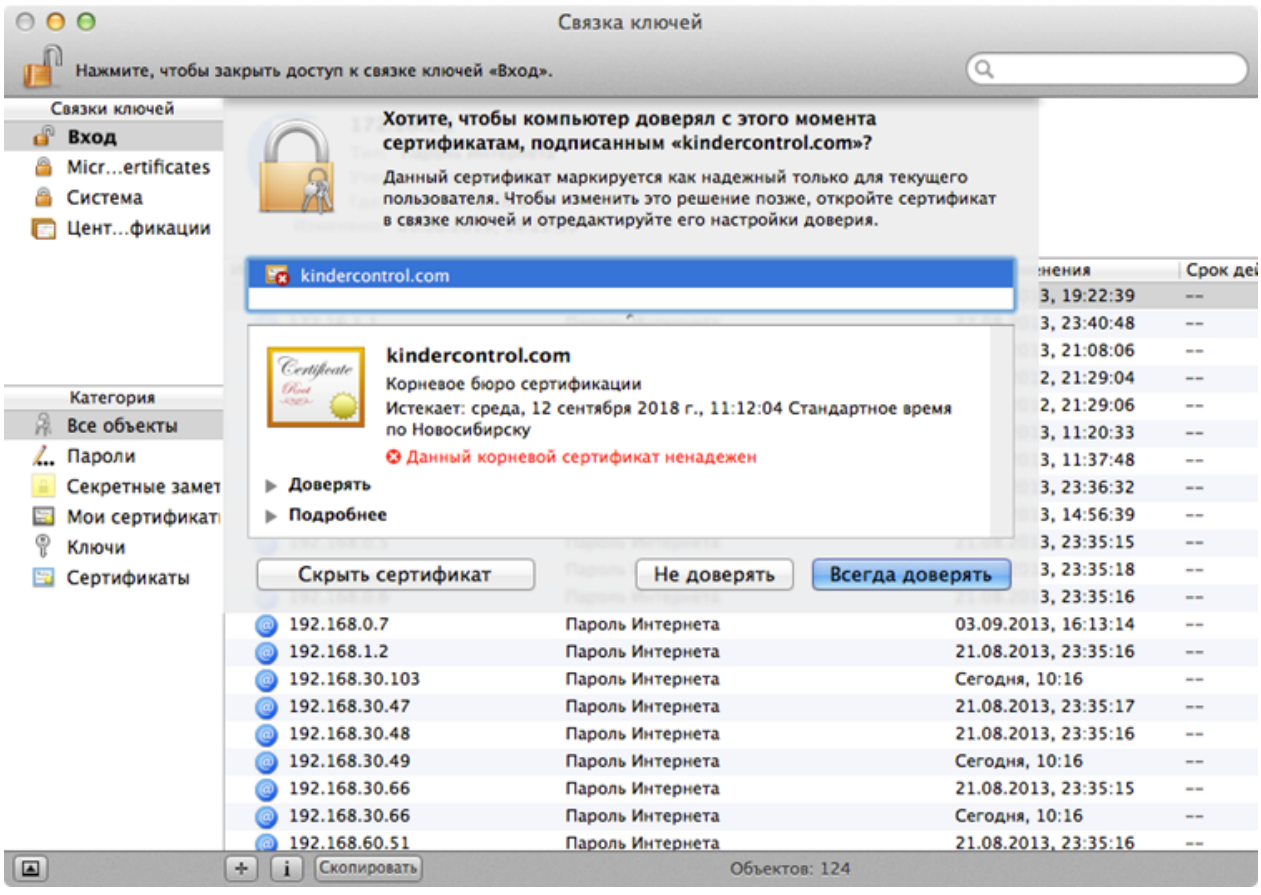


Рисунок 14 Доверие сертификату

Введите свой пароль для подтверждения данной операции:

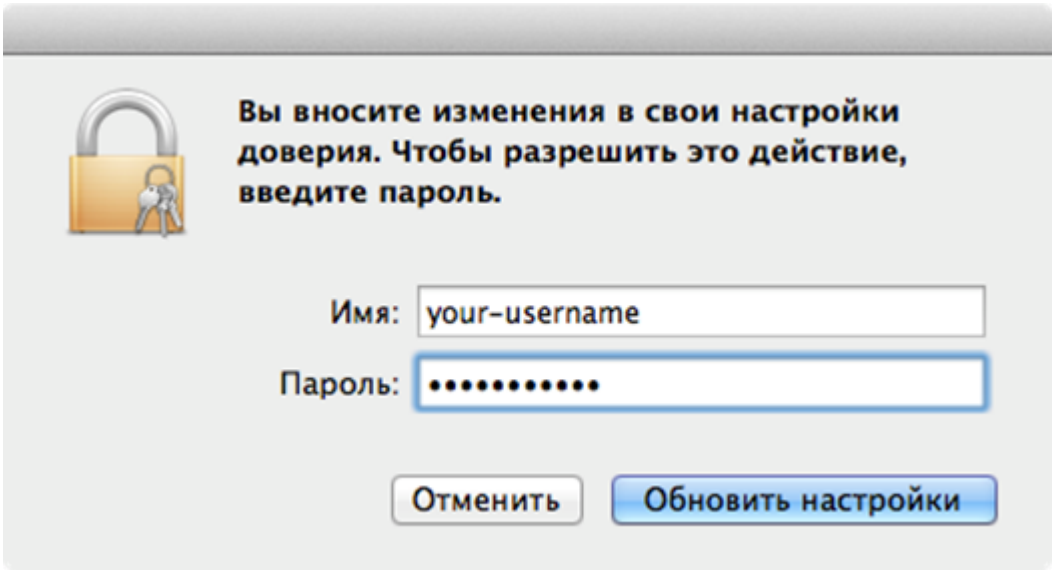


Рисунок 15 Ввод пароля

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**):

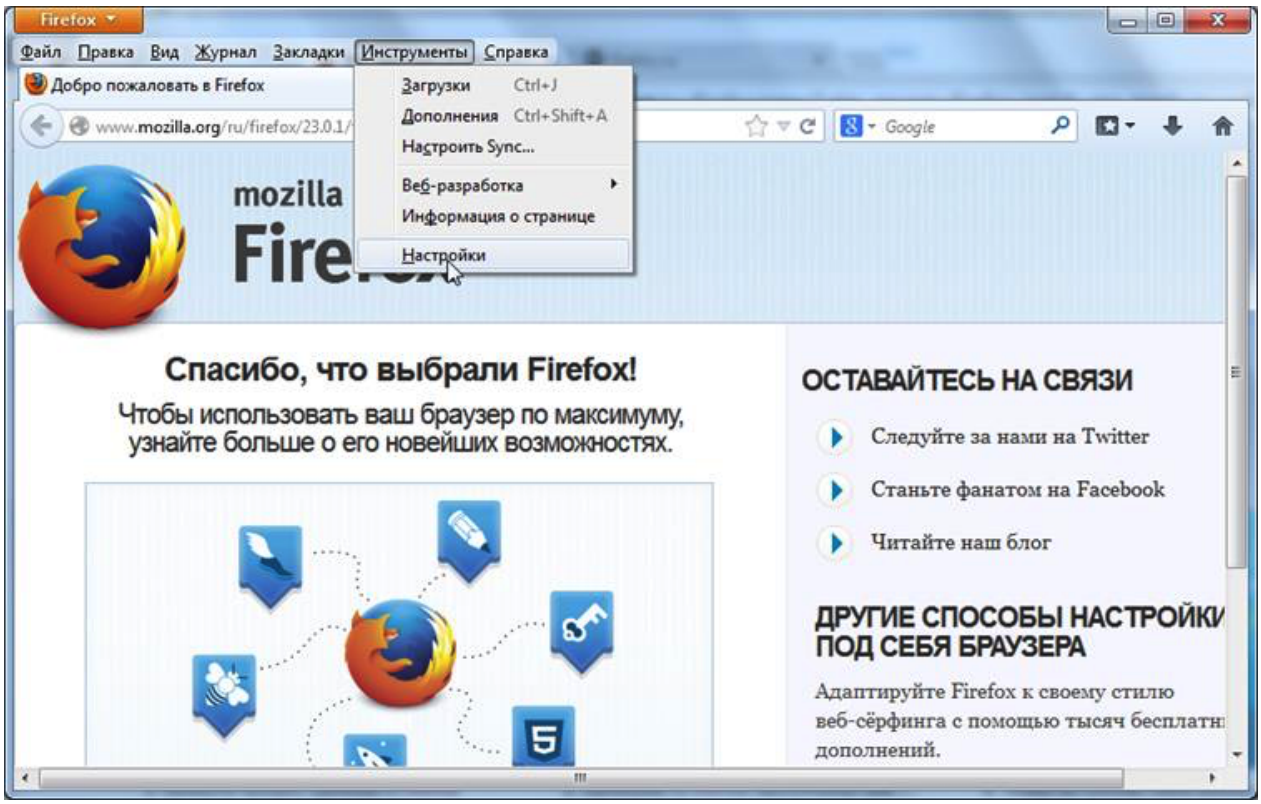


Рисунок 16 Вход в режим Настройки

Перейдите в раздел **Дополнительные** и выберите закладку **Сертификаты**. Нажмите на кнопку **Просмотр сертификатов**:

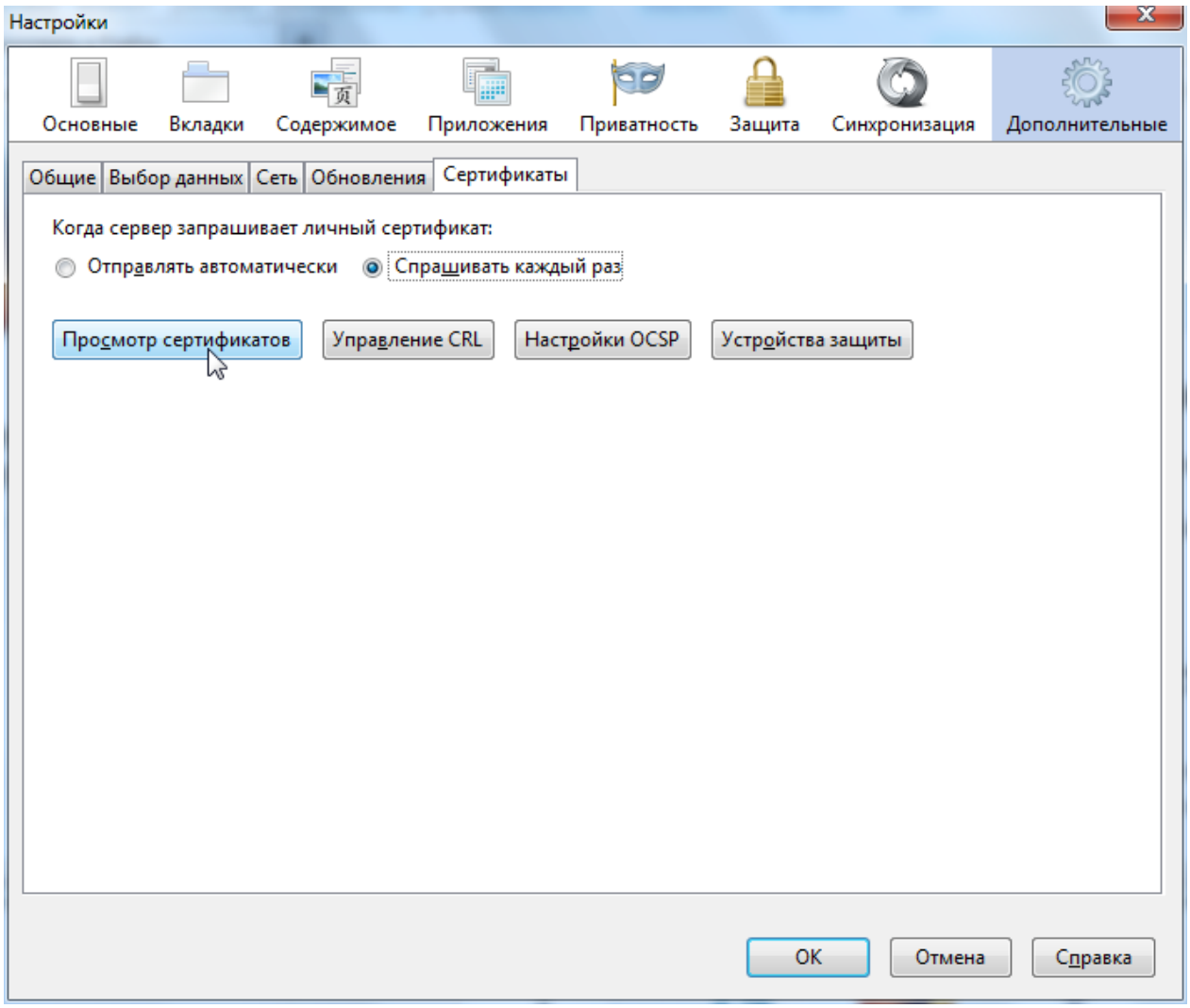


Рисунок 17 Раздел Сертификаты

Нажмите кнопку **Импортировать** и укажите путь к скачанному pem-сертификату:

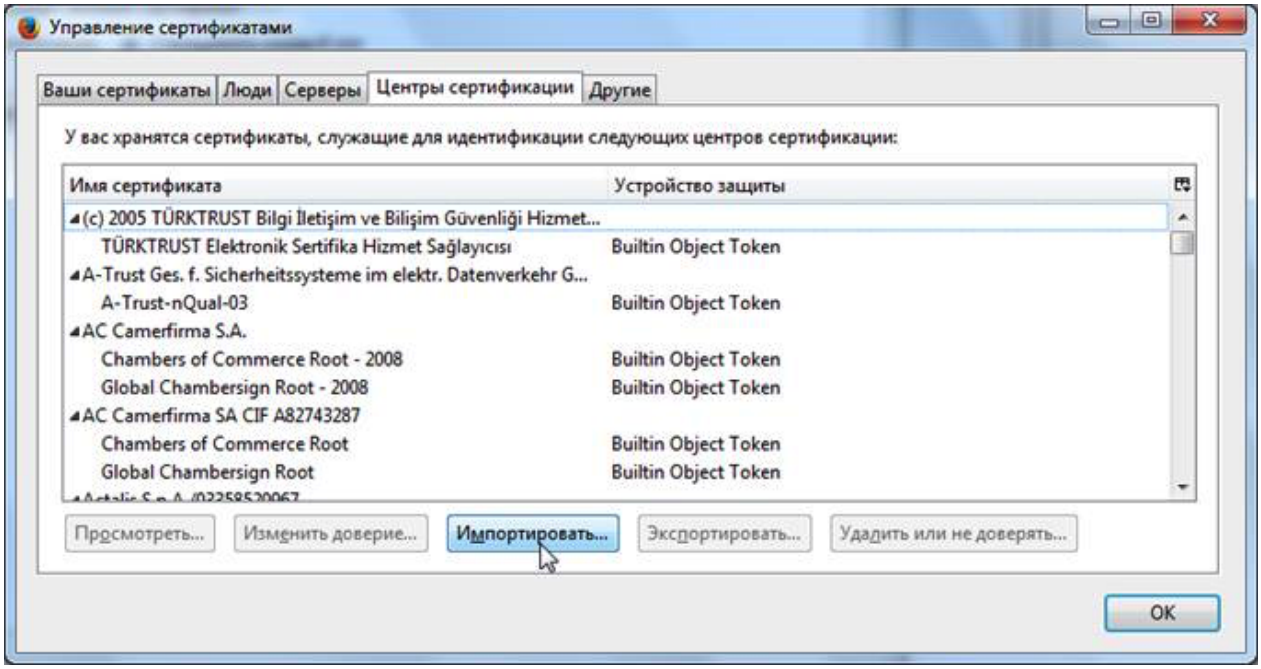


Рисунок 18 Список установленных сертификатов

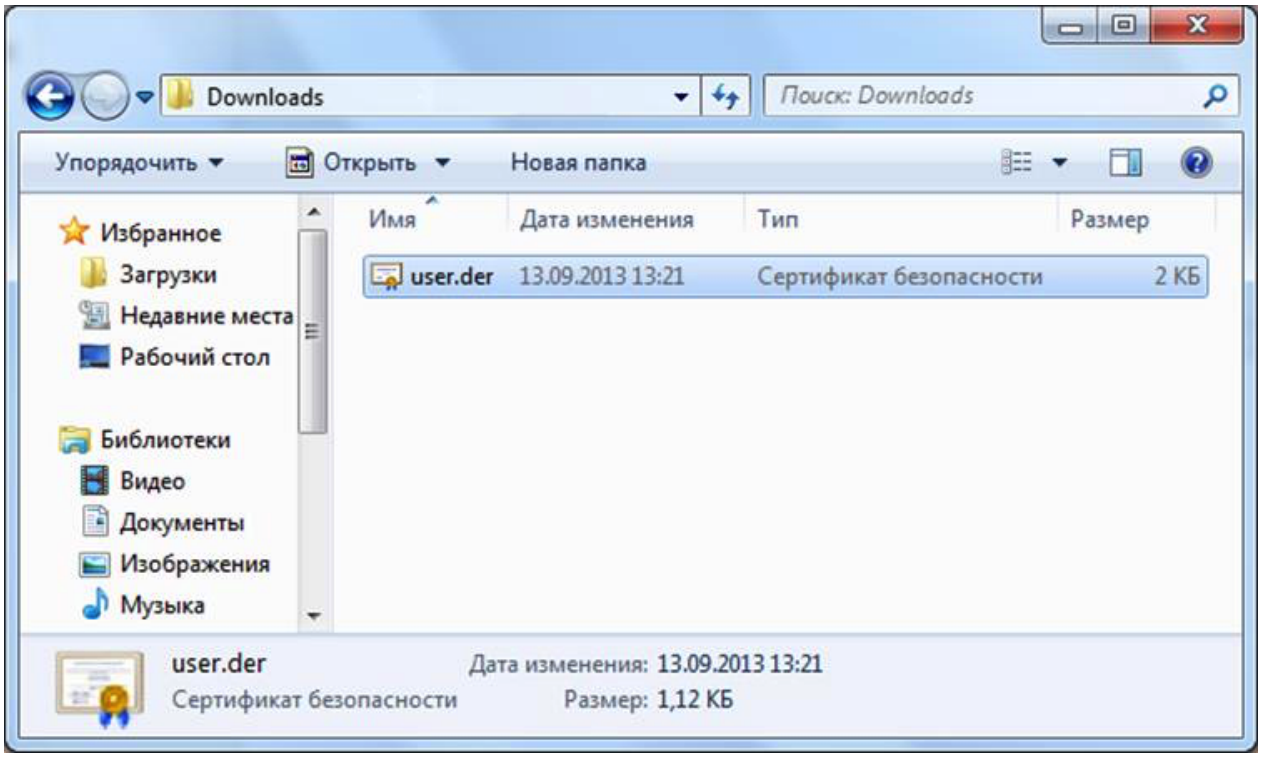


Рисунок 19 Выбор файла сертификата

Установите галочку **Доверять при идентификации веб-сайтов** и нажмите **OK**:

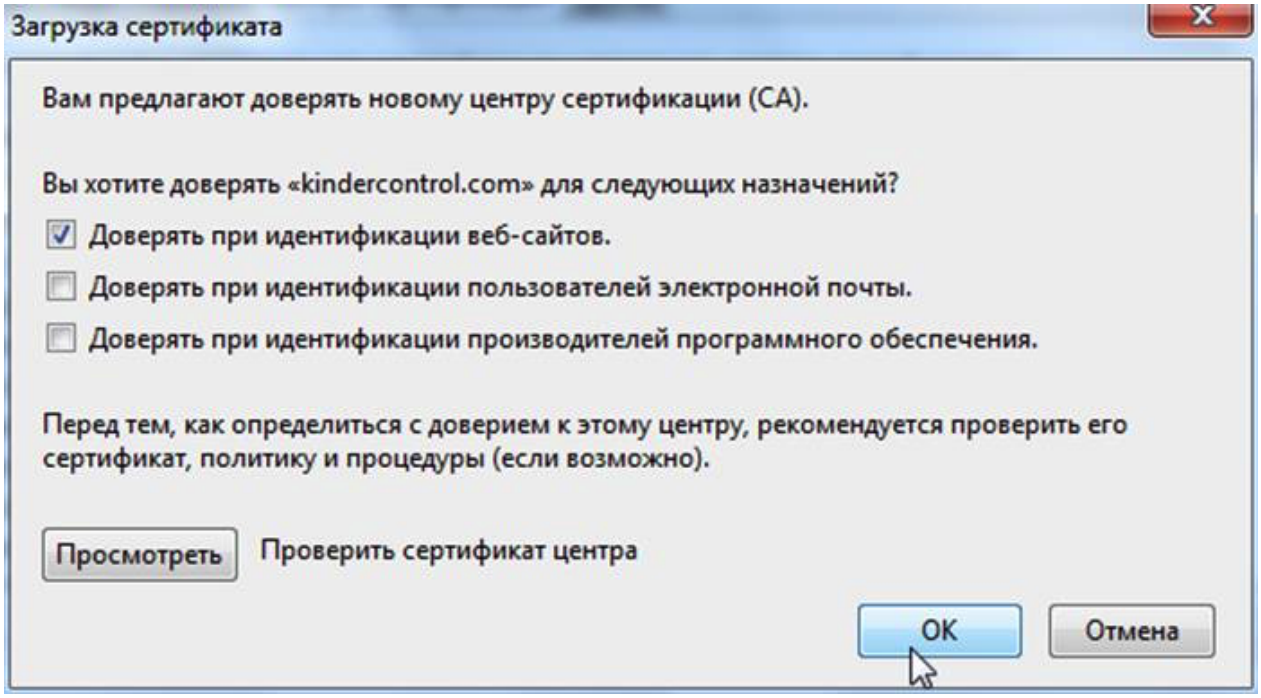


Рисунок 20 Выбор типа доверия

Установка сертификата завершена.

Таблица соответствий категорий, указанных в требованиях Министерства Образования РФ к СКФ для образовательных учреждений, с категориями UserGate URL filtering 4.0

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
	Сетевые ошибки
	Фишинг и мошенничество
	Спам-сайты
	Хакерство
Досуг и развлечение	Поздравительные открытки
	Развлечения
	Мода и красота

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
	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	Ненависть и нетерпимость

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров	Насилие
Злоупотребление свободой СМИ - экстремизм Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы	Ненависть и нетерпимость
	Насилие
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

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
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	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
продукции и табачных изделий	
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

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
Преступления-клевета, экстремизм	Преступная деятельность
Программное обеспечение	Компьютеры и технологии
	Нелегальное ПО
	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;	Алкоголь и табак

Категории Министерства Образования РФ	Категории UserGate URL filtering 4.0
реклама табака и изделий из него	
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

Описание форматов журналов

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@erstheta tica
	suser	Имя пользователя.	Admin

Тип поля	Название поля	Описание	Пример значения
	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.

Тип поля	Название поля	Описание	Пример значения
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@erstheta tica
	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}
	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.	

Тип поля	Название поля	Описание	Пример значения
			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	Decrypted

Тип поля	Название поля	Описание	Пример значения
		содержимое расшифровано.	
	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		URL Categories

Тип поля	Название поля	Описание	Пример значения
		Поле указывает на категорию запрашиваемого URL-адреса.	
	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	Packets received

Тип поля	Название поля	Описание	Пример значения
		назначение — источник.	
	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,	utmcore@erstheta tica

Тип поля	Название поля	Описание	Пример значения
		генерирующее это событие.	
	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.	

Тип поля	Название поля	Описание	Пример значения
			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	192.226.127.130 (0.0.0.0 — если нет)

Тип поля	Название поля	Описание	Пример значения
		(если настроены правила NAT).	
	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
	cn2Label	Поле используется для указания количества пакетов, переданных в	Packets received

Тип поля	Название поля	Описание	Пример значения
		направлении назначение — источник.	
	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

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	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

Тип поля	Название поля	Описание	Пример значения
	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;	231

Тип поля	Название поля	Описание	Пример значения
		данные передаются в направлении источник — назначение.	
	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

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@erstheta tica
	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

Тип поля	Название поля	Описание	Пример значения
	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
	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@erstheta tica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP

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.	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

Тип поля	Название поля	Описание	Пример значения
	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

Название поля	Описание	Пример значения
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
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.

Название поля		Описание	Пример значения
	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

Название поля			Описание	Пример значения
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)
	ip		IPv4-адрес назначения.	192.168.174.134
	port		Порт назначения.	Может принимать значения от 0 до 65535.

Название поля			Описание	Пример значения
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

Название поля			Описание	Пример значения
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

Название поля			Описание	Пример значения
	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.
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

Название поля			Описание	Пример значения
	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 COB

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		TCP или UDP

Название поля			Описание	Пример значения
			Используемый протокол 4-го уровня.	
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
	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

Название поля			Описание	Пример значения
	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

Название поля		Описание	Пример значения
	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

Название поля	Описание	Пример значения
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
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		6

Название поля			Описание	Пример значения
			Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	
	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

Название поля		Описание	Пример значения
	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
source	**zone**	**guid**	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted

Название поля			Описание	Пример значения
	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

Название поля			Описание	Пример значения
		name	Название группы, в которой состоит пользователь.	Default Group

Требования к сетевому окружению

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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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.entensys.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера static.entensys.com.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				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).

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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.
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, необходимы

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
				й 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.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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-маршрутизатор ам / Входящий (получение информации от соседних OSPF-маршрутизаторов)	Сервис динамической маршрутизации OSPF.

Сервис	Протокол	Порт	Исходящий/ Входящий	Функция
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.

Опции DHCP

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).

Наименование	Описание
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.

Наименование	Описание
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.
48	IP-адреса серверов шрифтов X Windows (X Window System Font).
49	Диспетчер дисплея X Windows.
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.
93	Архитектура системы клиента DHCP.

Наименование	Описание
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.

Описание событий, передающихся по syslog

Компонента	Событие	Описание
2fa		MFA
	profile_add_failed	Неуспешное добавление профиля MFA
	profile_added	Профиль MFA добавлен
	profile_delete_failed	Неуспешное удаление профиля MFA
	profile_deleted	Профиль MFA удалён
	profile_update_failed	Неуспешное изменение профиля MFA
	profile_updated	Профиль MFA изменён
accounts		Аккаунты и группы
	2fa_email_not_set	Не задан пользовательский email для MFA
	2fa_error_send_notify	Аутентификация MFA не может послать сообщение пользователю, проверьте настройки оповещения

Компонента	Событие	Описание
	2fa_phone_not_set	Не задан пользовательский телефон для MFA
	administrator_added	Учётная запись администратора добавлена
	administrator_deleted	Учётная запись администратора удалена
	administrator_profile_added	Профиль учётной записи администратора добавлен
	administrator_profile_deleted	Профиль учётной записи администратора удалён
	administrator_profile_updated	Профиль учётной записи администратора изменён
	administrator_unlocked	Учётная запись администратора разблокирована
	administrator_updated	Учётная запись администратора изменена
	auth_profile_add_failed	Неуспешное добавление профиля
	auth_profile_added	Профиль добавлен
	auth_profile_delete_failed	Неуспешное удаление профиля
	auth_profile_deleted	Профиль удалён
	auth_profile_fetch_failed	Неуспешное извлечение данных профиля
	auth_profile_update_failed	Неуспешное изменение профиля
	auth_profile_updated	Профиль изменён
	auth_server_add_failed	Неуспешное добавление сервера аутентификации

Компонента	Событие	Описание
	auth_server_added	Сервер аутентификации добавлен
	auth_server_deleted	Сервер аутентификации удалён
	auth_server_fetch_failed	Неуспешное извлечение данных сервера аутентификации
	auth_server_update_failed	Неуспешное изменение сервера аутентификации
	auth_server_updated	Сервер аутентификации изменён
	byod_device_deleted	Устройство BYOD удалено
	byod_device_updated	Устройство BYOD изменено
	byod_rule_add_failed	Неуспешное добавление правила BYOD
	byod_rule_added	Правило BYOD добавлено
	byod_rule_delete_failed	Неуспешное удаление правила BYOD
	byod_rule_deleted	Правило BYOD удалено
	byod_rule_move_failed	Неуспешное перемещение правила BYOD
	byod_rule_moved	Правило BYOD перемещено
	byod_rule_update_failed	Неуспешное обновление правила BYOD
	byod_rule_updated	Правило BYOD изменено
	captiveportal_profile_added	Профиль Captive-портала добавлен
	captiveportal_profile_deleted	Профиль Captive-портала удалён

Компонента	Событие	Описание
	captiveportal_profile_updated	Профиль Captive-портала изменён
	captiveportal_register_user_failed	Неуспешная регистрация пользователя через Captive-портал
	captiveportal_rule_added	Правило Captive-портала добавлено
	captiveportal_rule_deleted	Правило Captive-портала удалено
	captiveportal_rule_move_failed	Неуспешное перемещение правила Captive-портала
	captiveportal_rule_moved	Правило Captive-портала перемещено
	captiveportal_rule_updated	Правило Captive-портала изменено
	captiveportal_send_pass	Captive-портал: пароль успешно отправлен пользователю
	captiveportal_send_pass_failed	Captive-портал: ошибка отправки пароля пользователю
	ldap_server_disabled	Ошибка подключения к серверу LDAP. LDAP коннектор выключен
	ldap_server_not_responding	LDAP сервер недоступен
	ldap_server_unavailable	Сервер LDAP недоступен
	ldap_user_imported	Пользователь LDAP/AD импортирован
	ldap_user_is_missing	LDAP пользователь не найден
	ldap_users_list_failed	Неуспешная попытка отобраажения пользователей LDAP/AD

Компонента	Событие	Описание
	local_group_added	Локальная группа добавлена
	local_group_deleted	Локальная группа удалена
	local_group_updated	Локальная группа изменена
	local_user_added	Локальный пользователь добавлен
	local_user_deleted	Локальный пользователь удалён
	ta_user_added	Гостевой пользователь добавлен
	ta_user_deleted	Гостевой пользователь удалён
	ta_user_updated	Гостевой пользователь изменён
	ta_users_added_bulk	Добавлены гостевые пользователи
	ta_users_deleted_bulk	Гостевые пользователи удалены
	ta_users_updated_bulk	Гостевые пользователи изменены
	terminal_agent_add_failed	Неуспешное добавление агента терминального сервера
	terminal_agent_added	Агент терминального сервера добавлен
	terminal_agent_delete_failed	Неуспешное удаление агента терминального сервера
	terminal_agent_deleted	Агент терминального сервера удалён
	terminal_agent_update_failed	Неуспешное изменение агента терминального сервера

Компонента	Событие	Описание
	terminal_agent_updated	Агент терминального сервера изменён
	totp_code_already_init	Токен TOTP уже был успешно инициализирован
	totp_code_reset	Код TOTP сброшен
	totp_rule_added	Правило MFA добавлено
	totp_rule_deleted	Правило MFA удалено
	totp_rule_updated	Правило MFA изменено
	user_added_to_group	Пользователь добавлен в группу
	user_deleted_from_group	Пользователь удалён из группы
	user_updated	Пользователь изменён
analytics		Аналитика
	action_failed	Действие завершилось неуспешно
	action_finished	Действие завершилось
	action_rule_add_failed	Неуспешное добавление действие реагирования
	action_rule_added	Действие реагирования добавлено
	action_rule_delete_failed	Неуспешное удаление действия реагирования
	action_rule_deleted	Действие реагирования удалено
	action_rule_update_failed	Неуспешное изменение действия реагирования
	action_rule_updated	Действие реагирования обновлено

Компонента	Событие	Описание
	action_started	Действие запущено
	alert_category_add_failed	Неуспешная попытка добавления категории срабатывания
	alert_category_added	Категория срабатывания добавлена
	alert_category_delete_failed	Неуспешная попытка удаления категории срабатывания
	alert_category_deleted	Категория срабатывания удалена
	alert_category_update_failed	Неуспешная попытка изменения категории срабатывания
	alert_category_updated	Категоряи срабатывания изменена
	enrichment_setting_updated	Настройка сервисов обогащений обновлена
	enrichment_updated	Сервисы обогащений обновлены
	rule_add_failed	Неуспешное добавление правила аналитики
	rule_added	Правило аналитики добавлено
	rule_delete_failed	Неуспешное удаление правила аналитики
	rule_deleted	Правило аналитики удалено
	rule_exec_finished	Правило аналитики выполнено
	rule_exec_started	Правило аналитики запущено

Компонента	Событие	Описание
	rule_exec_stopped	Правило аналитики остановлено
	rule_import_failed	Неуспешный импорт правила аналитики
	rule_imported	Правило аналитики импортировано
	rule_update_failed	Неуспешное изменение правила аналитики
	rule_updated	Правило аналитики изменено
bandwidth		Пропускная способность
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
bgp		BGP
	filter_added	BGP-фильтр добавлен
	filter_deleted	Фильтр BGP удалён
	filter_updated	BGP фильтр обновлён
	neighbor_added	BGP-сосед добавлен
	neighbor_deleted	удалён сосед BGP
	neighbor_updated	BGP-сосед обновлён
	routemap_added	BGP-routemap добавлен
	routemap_deleted	удалён BGP routemap
	routemap_updated	BGP routemap изменён

Компонента	Событие	Описание
	router_updated	BGP-маршрутизатор обновлён
captiveportal		Captive-портал
	login_failed	Ошибка аутентификации
	login_failed_2fa_code	Неуспешная аутентификация MFA
	login_failed_anonymous	Неуспешная аутентификация через Captive-портал
	login_successful	Аутентификация успешна
cc_device		UserGate Management Center
	device_add_failed	Неуспешное добавление управляемого устройства
	device_added	Управляемое устройство добавлено
	device_check_license	Запущена проверка лицензии управляемого устройства
	device_check_license_failed	Неуспешная проверка лицензии управляемого устройства
	device_delete_failed	Неуспешное удаление управляемого устройства
	device_deleted	Управляемое устройство удалено
	device_fetch_failed	Неуспешное извлечение данных управляемого устройства
	device_reboot	Управляемое устройство перезагружено

Компонента	Событие	Описание
	device_reboot_failed	Неуспешная попытка перезагрузки управляемого устройства
	device_register	Управляемое устройство зарегистрировано
	device_register_failed	Неуспешная попытка регистрации управляемого устройства
	device_shutdown	Управляемое устройство выключено
	device_shutdown_failed	Неуспешная попытка выключения управляемого устройства
	device_update_failed	Неуспешное обновление управляемого устройства
	device_updated	Управляемое устройство изменено
	template_add_failed	Неуспешное добавление шаблона
	template_added	Шаблон добавлен
	template_delete_failed	Неуспешное удаление шаблона
	template_deleted	Шаблон удалён
	template_fetch_failed	Неуспешное извлечение данных шаблона
	template_group_add_failed	Неуспешное добавление группы шаблонов
	template_group_added	Группа шаблонов добавлена
	template_group_delete_failed	Неуспешное удаление группы шаблонов
	template_group_deleted	Группа шаблонов удалена

Компонента	Событие	Описание
	template_group_fetch_failed	Неуспешное извлечение данных группы шаблонов
	template_group_update_failed	Неуспешное извлечение данных группы шаблонов
	template_group_updated	Группа шаблонов обновлена
	template_update_failed	Неуспешное обновление шаблона
	template_updated	Шаблон обновлён
cc_device_lists_update		Обновление библиотек
	update_fetch_failed	Неуспешное удаление обновления бибиблиотек
	update_update_failed	Неуспешное изменение обновления бибиблиотек
	update_updated	Обновление библиотеки успешно изменено
cc_device_update		Обновление ПО
	update_add_failed	Неуспешная попытка добавления обновления ПО
	update_added	Обновление ПО добавлено
	update_delete_failed	Обновление ПО удалено
	update_deleted	Обновление ПО удалено
	update_fetch_failed	Неуспешная попытка удаления обновления ПО
	update_update_failed	Неуспешная попытка изменения обновления ПО
	update_updated	Обновление ПО изменено
cc_logan		LogAn сервер
	device_add_failed	Неуспешная попытка добавления LogAn сервера

Компонента	Событие	Описание
	device_added	LogAn сервер добавлен
	device_delete_failed	Неуспешная попытка удаления LogAn сервера
	device_deleted	LogAn сервер удалён
	device_fetch_failed	Неуспешная попытка извлечения данных LogAn сервера
	device_update_failed	Неуспешная попытка обновления LogAn сервера
	device_updated	LogAn сервер обновлён
certificates		Сертификаты
	client_certificate_profile_added	Профиль клиентского сертификата успешно добавлен
	client_certificate_profile_deleted	Профиль клиентского сертификата успешно удален
	client_certificate_profile_updated	Профиль клиентского сертификата успешно изменен
connectors		Коннекторы
	add_failed	Неуспешная попытка добавления коннектора
	added	Коннектор добавлен
	delete_failed	Неуспешная попытка удаления коннектора
	deleted	Коннектор удалён
	exec_failed	Неуспешная попытка выполнить команду коннектора

Компонента	Событие	Описание
	executed	Команда коннектора выполнена
	fetch_failed	Неуспешная попытка извлечения данных коннектора
	msg_send_failed	Неуспешная попытка послать сообщение на коннектор
	msg_sent	Сообщение успешно отправлено на коннектор
	restore_default	Успешный сброс коннекторов к значению по умолчанию
	restore_default_failed	Неуспешная попытка сброса коннекторов к значению по умолчанию
	update_failed	Неуспешная попытка обновления настроек коннектора
	updated	Настройки коннектора обновлены
console_auth		Консольная аутентификация
	administrator_login	Успешная аутентификация администратора
	administrator_login_failed	Неуспешная аутентификация администратора
	administrator_logout	Успешный выход администратора из системы
	administrator_logout_failed	Неуспешный выход администратора из системы
	login_failed	Ошибка аутентификации
	login_successful	Аутентификация успешна

Компонента	Событие	Описание
content_rules		Фильтрация контента
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
core		Ядро системы
	administrator_add_failed	Неуспешное добавление учётной записи администратора
	administrator_added	Учётная запись администратора добавлена
	administrator_change_password	Пароль учётной записи администратора изменён
	administrator_change_password_failed	Неуспешное изменение пароля учётной записи администратора
	administrator_delete_failed	Неуспешное удаление учётной записи администратора
	administrator_deleted	Учётная запись администратора удалена
	administrator_fetch_failed	Неуспешное извлечение данных учётной записи администратора
	administrator_login	Успешная аутентификация администратора
	administrator_login_failed	Неуспешная аутентификация администратора
	administrator_logout	Успешный выход администратора из системы

Компонента	Событие	Описание
	administrator_logout_failed	Неуспешный выход администратора из системы
	administrator_profile_add_failed	Неуспешное добавление профиля администратора
	administrator_profile_added	Профиль учётной записи администратора добавлен
	administrator_profile_delete_failed	Неуспешное удаление профиля администратора
	administrator_profile_deleted	Профиль учётной записи администратора удалён
	administrator_profile_fetch_failed	Неуспешное извлечение данных профиля администратора
	administrator_profile_update_failed	Неуспешное добавление профиля администратора
	administrator_profile_updated	Профиль учётной записи администратора изменён
	administrator_role_add_failed	Неуспешное добавление роли
	administrator_role_added	Роль добавлена
	administrator_role_delete_failed	Неуспешное удаление роли
	administrator_role_deleted	Роль удалена
	administrator_role_fetch_failed	Неуспешное извлечение данных роли
	administrator_role_update_failed	Неуспешное изменение роли
	administrator_role_updated	Роль изменена
	administrator_roles_restore_default	Успешный сброс ролевых разрешений к значению по умолчанию

Компонента	Событие	Описание
	administrator_roles_restore_default_failed	Неуспешная попытка сброса ролевых разрешений к значению по умолчанию
	administrator_terminate_session	Сессия администратора закрыта
	administrator_terminate_session_failed	Неуспешная попытка закрытия сессии администратора
	administrator_unlock	Учётная запись администратора разблокирована
	administrator_unlock_failed	Неуспешная разблокировка учётной записи администратора
	administrator_update_failed	Неуспешное изменение учётной записи администратора
	administrator_updated	Учётная запись администратора изменена
	realm_add_failed	Неуспешное добавление управляемой области
	realm_added	Управляемая область добавлена
	realm_delete_failed	Неуспешное удаление управляемой области
	realm_deleted	Управляемая область удалена
	realm_fetch_failed	Неуспешное извлечение данных управляемой области
	realm_update_failed	Неуспешное обновление управляемой области
	realm_updated	Управляемая область обновлена

Компонента	Событие	Описание
decryption_rules		Инспектирование
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
device		Устройство
	appliance_fault	Внутренняя ошибка применения конфигурации
	auth_server_update_failed	Неуспешное изменение сервера аутентификации
	backup_cancelled	Резервное копирование отменено
	backup_error	Ошибка создания резервной копии
	backup_export_rule_added	Правило резервного копирования добавлено
	backup_export_rule_deleted	Правило резервного копирования удалено
	backup_export_rule_updated	Правило резервного копирования изменено
	backup_finished	Резервное копирование успешно завершено
	backup_started	Резервное копирование запущено
	bootstrap_end	Сервер загрузился успешно
	cc_server_connection_failed	Потеряна связь с UserGate MC
	check_checksum_failed	Контрольная сумма не совпала

Компонента	Событие	Описание
	code_change_control_set	Установлена защита исполняемых файлов от изменения
	code_checksum_failed	Контрольная сумма исполняемых файлов изменена
	config_change_control_set	Установлена защита конфигурации от изменения
	config_checksum_failed	Контрольная сумма конфигурации изменена
	conntrack_table_overload	Таблица сессий заполнена на 90%
	filesystem_not_clean	Файловая система повреждена
	high_cpu_usage	Высокая загрузка процессора
	high_disk_io_utilization	Высокая загрузка ввода/вывода диска
	iface_configuration_failed	Неуспешное изменение сетевого интерфейса
	log_rotation_failed	Ошибка ротации файлов журналов
	low_memory	Высокое потребление памяти
	low_space_log_partition	Недостаточно места на разделе для журналов
	network_settings_export	Экспорт сетевых настроек
	network_settings_export_failed	Ошибка экспорта сетевых настроек
	network_settings_import	Импорт сетевых настроек
	network_settings_import_failed	Ошибка импорта сетевых настроек

Компонента	Событие	Описание
	node_info_updated	Узел обновлён
	poweroff	Инициировано выключение сервера
	reboot	Инициирована перезагрузка
	scheduled_export_complete	Экспорт завершён успешно
	scheduled_export_failed	Экспорт завершён с ошибкой
	set_log_level	Уровень журналирования изменён
	settings_export	Экспортированы настройки
	settings_export_rule_added	Правило экспорта добавлено
	settings_export_rule_deleted	Правило экспорта удалено
	settings_export_rule_updated	Правило экспорта изменено
	settings_import	Импортированы настройки
	system_logs_clear	Журналы очищены
dos		DoS
	rule_added	Правило защиты DoS добавлено
	rule_deleted	Правило защиты DoS удалено
	rule_moved	Правило защиты DoS перемещено
	rule_profile_added	Профиль защиты DoS добавлен
	rule_profile_deleted	Профиль защиты DoS удалён
	rule_profile_updated	Профиль защиты DoS изменён

Компонента	Событие	Описание
	rule_updated	Правило защиты DoS изменено
endpoint_devices_lists_update		Обновление библиотек конечного устройства
	update_fetch_failed	Неуспешная попытка удаления обновления библиотек конечного устройства
	update_update_failed	Неуспешная попытка изменения обновления библиотек конечного устройства
	update_updated	Успешное изменение библиотек конечного устройства
endpoint_devices_update		Обновление ПО конечного устройства
	update_add_failed	Неуспешная попытка добавления обновления ПО конечного устройства
	update_added	Обновление ПО конечного устройства добавлено
	update_delete_failed	Обновление ПО конечного устройства удалено
	update_deleted	Обновление ПО конечного устройства удалено
	update_fetch_failed	Неуспешная попытка удаления обновления ПО конечного устройства
	update_update_failed	Неуспешная попытка изменения обновления ПО конечного устройства
	update_updated	Обновление ПО конечного устройства изменено
ep_code		Код конечного устройства

Компонента	Событие	Описание
	endpoint_code_add_failed	Неуспешная попытка добавления кода конечного устройства
	endpoint_code_added	Код конечного устройства добавлен
	endpoint_code_delete_failed	Неуспешная попытка удаления кода конечного устройства
	endpoint_code_deleted	Код конечного устройства удалён
	endpoint_code_fetch_failed	Неуспешная попытка извлечения данных кода конечного устройства
	endpoint_code_update_failed \	Неуспешная попытка обновления кода конечного устройства
	endpoint_code_updated	Код конечного устройства обновлён
ep_compliance		Комплаенс конечного устройства
	compliance_add_failed	Неуспешная попытка добавления настроек комплаенса
	compliance_added	Добавлены настройки комплаенса
	compliance_delete_failed	Неуспешная попытка удаления настроек комплаенса
	compliance_deleted	Удалены настройки комплаенса
	compliance_fetch_failed	Неуспешная попытка извлечения данных настроек комплаенса
	compliance_update_failed	

Компонента	Событие	Описание
		Неуспешная попытка изменения настроек комплаенса
	compliance_updated	Обновлены настройки комплаенса
ep_device		Конечное устройство
	endpoint_activated	Конечное устройство активировано
	endpoint_add_failed	Неуспешная попытка добавления конечного устройства
	endpoint_added	Конечное устройство добавлено
	endpoint_deleted	Конечное устройство удалено
	endpoint_deleted_failed	Неуспешная попытка удаления конечного устройства
	endpoint_fetch_failed	Неуспешная попытка извлечения данных конечного устройства
	endpoint_sync	Синхронизация конечных устройств
	endpoint_sync_failed	Неуспешная попытка синхронизации конечного устройства
	endpoint_update_failed	Неуспешная попытка обновления конечного устройства
	endpoint_updated	Конечное устройство обновлено
ep_firewall		Межсетевой экран конечных устройств
	rule_added	Правило добавлено

Компонента	Событие	Описание
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
ep_hip_object		HIP объект
	hip_object_add_failed	Неуспешная попытка добавления HIP объекта
	hip_object_added	HIP объект добавлен
	hip_object_delete_failed	Неуспешная попытка удаления HIP объекта
	hip_object_deleted	HIP объект удален
	hip_object_fetch_failed	Неуспешная попытка извлечения данных HIP объекта
	hip_object_update_failed	Неуспешная попытка обновления HIP объекта
	hip_object_updated	HIP объект обновлен
ep_hip_profile		HIP профиль
	hip_profile_add_failed	Неуспешная попытка добавления HIP профиля
	hip_profile_added	HIP профиль добавлен
	hip_profile_delete_failed	Неуспешная попытка удаления HIP профиля
	hip_profile_deleted	HIP профиль удален
	hip_profile_fetch_failed	Неуспешная попытка извлечения данных HIP профиля
	hip_profile_update_failed	Неуспешная попытка обновления HIP профиля
	hip_profile_updated	HIP профиль обновлен

Компонента	Событие	Описание
ep_libraries		Библиотеки конечных устройств
	nlist_added	Список добавлен
	nlist_deleted	Список удалён
	nlist_exported	Список экспортирован
	nlist_import_failed	Ошибка при импорте списка
	nlist_imported	Список импортирован
	nlist_item_added	Элемент списка добавлен
	nlist_item_deleted	Элемент списка удалён
	nlist_item_updated	Элемент списка изменён
	nlist_items_deleted	Элементы списка удалены
	nlist_updated	Список изменён
	service_added	Сервис добавлен
	service_deleted	Сервис удалён
	service_updated	Сервис изменён
ep_proxy		Прокси сервер
	proxy_profile_add_failed	Неуспешная попытка добавления прокси сервера
	proxy_profile_added	Прокси сервер добавлен
	proxy_profile_delete_failed	Неуспешная попытка удаления прокси сервера
	proxy_profile_deleted	Прокси сервер удален
	proxy_profile_fetch_failed	Неуспешная попытка извлечения данных прокси сервера
	proxy_profile_update_failed	

Компонента	Событие	Описание
		Неуспешная попытка обновления данных прокси сервера
	proxy_profile_updated	Прокси сервер обновлен
ep_settings		Настройка конечного устройства
	update_failed	Неуспешная попытка обновления общих настроек конечного устройства
	updated	Общие настройки конечного устройства обновлены
ep_template		Шаблон конечного устройства
	endpoint_template_add_failed	Неуспешная попытка добавления шаблона конечного устройства
	endpoint_template_added	Шаблон конечного устройства добавлен
	endpoint_template_delete_failed	Неуспешная попытка удаления шаблона конечного устройства
	endpoint_template_deleted	Шаблон конечного устройства удалён
	endpoint_template_fetch_failed	Неуспешная попытка извлечения данных шаблона конечного устройства
	endpoint_template_update_failed\	Неуспешная попытка обновления шаблона конечного устройства
	endpoint_template_updated	Шаблон конечного устройства обновлён
ep_templates_group		Группа шаблонов конечного устройства

Компонента	Событие	Описание
	endpoint_template_group_add_failed	Неуспешная попытка добавления группы шаблонов конечного устройства
	endpoint_template_group_added	Группа шаблонов конечного устройства добавлена
	endpoint_template_group_delete_failed	Неуспешная попытка удаления группы шаблонов конечного устройства
	endpoint_template_group_deleted	Группа шаблонов конечного устройства удалена
	endpoint_template_group_fetch_failed	Неуспешная попытка извлечения данных группы шаблонов конечного устройства
	endpoint_template_group_update_failed	Неуспешная попытка обновления группы шаблонов конечного устройства
	endpoint_template_group_updated	Группа шаблонов конечного устройства обновлена
ep_vpn		VPN конечного устройства
	vpn_add_failed	Неуспешная попытка добавления VPN конечного устройства
	vpn_added	Добавлен VPN конечного устройства
	vpn_delete_failed	Неуспешная попытка удаления VPN конечного устройства
	vpn_deleted	Удален VPN конечного устройства
	vpn_fetch_failed	Неуспешная попытка извлечения данных VPN конечного устройства

Компонента	Событие	Описание
	vpn_move_failed	Неуспешная попытка перемещения VPN конечного устройства
	vpn_moved	VPN конечного устройства перемещен
	vpn_update_failed	Неуспешная попытка изменения VPN конечного устройства
	vpn_updated	VPN конечного устройства обновлен
firewall		Межсетевой экран
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
ha		Отказоустойчивость
	member_down	Узел кластера выключен
	member_up	Узел кластера доступен
	status_changed	Статус изменён
icap_rules		ICAP
	profile_added	Профиль добавлен
	profile_deleted	Профиль удалён
	profile_updated	Профиль изменён
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено

Компонента	Событие	Описание
	rule_updated	Правило изменено
idps		СОВ
	idps_build_failed	Сборка СОВ завершена неуспешно
idps_rules		СОВ
	attack_detected	Обнаружена атака
	rule_add_failed	Неуспешное добавление правила
	rule_added	Правило добавлено
	rule_delete_failed	Неуспешное удаление правила
	rule_deleted	Правило удалено
	rule_fetch_failed	Неуспешное получение информации о правиле
	rule_move_failed	Неуспешное перемещение правила
	rule_moved	Правило перемещено
	rule_update_failed	Неуспешное изменение правила
	rule_updated	Правило изменено
incident		Инциденты
	alert_added	Срабатывания добавлены в инцидент
	alert_removed	Срабатывания удалены из инцидента
	comment_added	Изменён комментарий к инциденту
	incident_added	Добавлен инцидент

Компонента	Событие	Описание
	logs_added	Логи добавлены в инцидент
	logs_removed	Логи удалены из инцидента
	observable_updated	Улики инцидента обновлены
	report_deleted	Отчёт инцидента удалён
	report_rule_added	Правило отчёта инцидента добавлено
	report_rule_deleted	Правило отчёта инцидента удалено
	report_rule_exec	Правило отчёта инцидента запущено
	report_rule_failed	Создание отчёта инцидента закончилось с ошибкой
	report_rule_finished	Создание отчёта инцидента закончилось успешно
	report_rule_started	Началось создание отчёта инцидента
	report_rule_updated	Правило отчёта инцидента изменено
	report_template_added	Шаблон отчёта инцидента добавлен
	report_template_deleted	Шаблон отчёта инцидента удалён
	report_template_updated	Шаблон отчёта инцидента изменён
	resolution_add_failed	Неуспешная попытка добавления решения инцидента
	resolution_added	Добавлено решение инцидента

Компонента	Событие	Описание
	resolution_delete_failed	Неуспешная попытка удаления решения инцидента
	resolution_deleted	Удалено решение инцидента
	resolution_fetch_failed	Неуспешная попытка извлечения данных о решении инцидента
	resolution_restore_default	Восстановлены решения инцидентов по умолчанию
	resolution_update_failed	Неуспешная попытка изменения решения инцидента
	resolution_updated	Изменено решение инцидента
	schema_added	Добавлена схема инцидента
	schema_deleted	Удалена схема инцидента
	schema_restore_default	Восстановлены схемы инцидентов по умолчанию
	schema_updated	Изменена схема инцидента
	state_add_failed	Неуспешная попытка добавления состояния инцидента
	state_added	Добавлено состояние инцидента
	state_delete_failed	Неуспешная попытка удаления состояния инцидента
	state_deleted	Удалено состояние инцидента
	state_fetch_failed	Неуспешная попытка извлечения данных о состоянии инцидента

Компонента	Событие	Описание
	state_restore_default	Восстановлены состояния инцидентов по умолчанию
	state_update_failed	Неуспешная попытка изменения состояния инцидента
	state_updated	Изменено состояние инцидента
	status_added	Изменён статус инцидента
	type_add_failed	Неуспешная попытка добавления типа инцидента
	type_added	Добавлен тип инцидента
	type_delete_failed	Неуспешная попытка удаления типа инцидента
	type_deleted	удалён тип инцидента
	type_fetch_failed	Неуспешная попытка извлечения данных о типе инцидента
	type_restore_default	Восстановлены типы инцидентов по умолчанию
	type_update_failed	Неуспешная попытка изменения типа инцидента
	type_updated	Изменён тип инцидента
ipvs		Балансировка
	server_add_failed	Неуспешное добавление сервера балансировки нагрузки
	server_added	Сервер балансировки нагрузки добавлен
	server_delete_failed	Неуспешное удаление сервера балансировки нагрузки

Компонента	Событие	Описание
	server_deleted	Сервер балансировки нагрузки удалён
	server_fetch_failed	Неуспешное извлечение данных сервера балансировки нагрузки
	server_update_failed	Неуспешное изменение сервера балансировки нагрузки
	server_updated	Сервер балансировки нагрузки изменён
libraries		Библиотеки
	ips_profile_add_failed	Неуспешная попытка добавления профиля СОВ
	ips_profile_added	Профиль СОВ успешно добавлен
	ips_profile_delete_failed	Неуспешная попытка удаления профиля СОВ
	ips_profile_deleted	Профиль СОВ успешно удален
	ips_profile_update_failed	Неуспешная попытка изменения профиля СОВ
	ips_profile_updated	Профиль СОВ успешно изменен
	ips_signature_add_failed	Неуспешная попытка добавления сигнатуры СОВ
	ips_signature_added	Сигнатура СОВ успешно добавлена
	ips_signature_delete_failed	Неуспешная попытка удаления сигнатуры СОВ
	ips_signature_deleted	Сигнатура СОВ успешно удалена

Компонента	Событие	Описание
	ips_signature_restore_settings_failed	Неуспешная попытка восстановления настроек сигнатуры СОВ
	ips_signature_restored_settings	Настройки сигнатуры СОВ восстановлены успешно
	ips_signature_update_failed	Неуспешная попытка изменения сигнатуры СОВ
	ips_signature_updated	Сигнатура СОВ успешно изменена
	l7_profile_add_failed	Неуспешная попытка добавления профиля приложения
	l7_profile_added	Профиль приложения успешно добавлен
	l7_profile_delete_failed	Неуспешная попытка удаления профиля приложения
	l7_profile_deleted	Профиль приложения успешно удален
	l7_profile_update_failed	Неуспешная попытка обновления профиля приложения
	l7_profile_updated	Профиль приложения успешно обновлен
	l7_signature_add_failed	Неуспешная попытка добавления приложения
	l7_signature_added	Приложение успешно добавлено
	l7_signature_delete_failed	Неуспешная попытка удаления приложения
	l7_signature_deleted	Приложение успешно удалено

Компонента	Событие	Описание
	l7_signature_update_failed	Неуспешная попытка обновления приложения
	l7_signature_updated	Приложение успешно обновлено
	lldp_profile_add_failed	Неуспешная попытка добавления профиля LLDP
	lldp_profile_added	Профиль LLDP добавлен
	lldp_profile_delete_failed	Неуспешная попытка удаления профиля LLDP
	lldp_profile_deleted	Профиль LLDP удален
	lldp_profile_fetch_failed	Неуспешная попытка извлечения данных профиля LLDP
	lldp_profile_update_failed	Неуспешная попытка изменения профиля LLDP
	lldp_profile_updated	Профиль LLDP изменен
	netflow_profile_add_failed	Неуспешное добавление профиля Netflow
	netflow_profile_added	Профиль Netflow добавлен
	netflow_profile_delete_failed	Неуспешное удаление профиля Netflow
	netflow_profile_deleted	Профиль Netflow удалён
	netflow_profile_fetch_failed	Неуспешное извлечение данных профиля Netflow
	netflow_profile_update_failed	Неуспешное изменение профиля Netflow
	netflow_profile_updated	Профиль Netflow изменён
	nlist_added	Список добавлен
	nlist_deleted	Список удалён

Компонента	Событие	Описание
	nlist_exported	Список экспортирован
	nlist_import_failed	Ошибка при импорте списка
	nlist_imported	Список импортирован
	nlist_item_added	Элемент списка добавлен
	nlist_item_deleted	Элемент списка удалён
	nlist_item_updated	Элемент списка изменён
	nlist_items_deleted	Элементы списка удалены
	nlist_updated	Список изменён
	resp_page_template_add_failed	Неуспешное добавление шаблона страницы блокировки
	resp_page_template_added	Шаблон страницы добавлен
	resp_page_template_delete_failed	Неуспешное удаление шаблона страницы блокировки
	resp_page_template_deleted	Шаблон страницы удалён
	resp_page_template_import_failed	Неуспешный импорт шаблона страницы блокировки
	resp_page_template_imported	Шаблон страницы импортирован
	resp_page_template_update_failed	Неуспешное изменение шаблона страницы блокировки
	resp_page_template_updated	Шаблон страницы изменён
	service_added	Сервис добавлен
	service_deleted	Сервис удалён
	service_updated	Сервис изменён

Компонента	Событие	Описание
	shaper_pool_added	Полоса пропускания добавлена
	shaper_pool_deleted	Полоса пропускания удалена
	shaper_pool_updated	Полоса пропускания изменена
	snmp_security_profile_added	Профиль безопасности SNMP добавлен
	snmp_security_profile_deleted	Профиль безопасности SNMP удален
	snmp_security_profile_updated	Неуспешная попытка удаления профиля безопасности SNMP
	ssl_forward_profile_add_failed	Неуспешное добавление профиля пересылки SSL
	ssl_forward_profile_added	Профиль пересылки SSL добавлен
	ssl_forward_profile_delete_failed	Неуспешное удаление профиля пересылки SSL
	ssl_forward_profile_deleted	Профиль пересылки SSL удалён
	ssl_forward_profile_fetch_failed	Неуспешное извлечение данных профиля пересылки SSL
	ssl_forward_profile_update_failed	Неуспешное изменение профиля пересылки SSL
	ssl_forward_profile_updated	Профиль пересылки SSL обновлён
	ssl_profile_add_failed	Неуспешное добавление профиля SSL
	ssl_profile_added	Профиль SSL добавлен

Компонента	Событие	Описание
	ssl_profile_delete_failed	Неуспешное удаление профиля SSL
	ssl_profile_deleted	Профиль SSL удалён
	ssl_profile_fetch_failed	Неуспешное извлечение данных профиля SSL
	ssl_profile_update_failed	Неуспешное изменение профиля SSL
	ssl_profile_updated	Профиль SSL изменён
license		Лицензия
	activation_failed	Ошибка активации
	activation_failed_constraints	Ошибка активации, несоответствие оборудования
	activation_started	Начало активации
	activation_successfull	Активация успешно завершилась
	check_failed	Ошибка проверки
	check_successfull	Проверка успешно завершилась
	connections_limit_reached	Достигнуто максимальное количество сессий
	remove_node	Узел кластера удалён
	status_off	Лицензия приостановлена
log_collector		Сборщик логов
	connection_failed	Ошибка подключения сборщика логов
	connection_succeeded	Сборщик логов подключен
	rsyslog_rule_add_failed	Неуспешное добавление правила syslog

Компонента	Событие	Описание
	rsyslog_rule_added	Правило syslog добавлено
	rsyslog_rule_delete_failed	Неуспешное удаление правила syslog
	rsyslog_rule_deleted	Правило syslog удалено
	rsyslog_rule_move_failed	Неуспешное перемещение правила syslog
	rsyslog_rule_moved	Правило syslog перемещено
	rsyslog_rule_updated	Правило syslog изменено
	rsyslog_rule_updated_failed	Неуспешное изменение правила syslog
	rsyslog_set_config	Конфигурация сервера syslog изменена
	rsyslog_set_config_failed	Неуспешное изменение конфигурации сервера syslog
	syslog_app_name_add_failed	Неуспешное добавление приложений syslog
	syslog_app_name_added	Приложение syslog добавлено
	syslog_app_name_delete_failed	Неуспешное удаление приложений syslog
	syslog_app_name_deleted	Приложение syslog удалено
	syslog_app_name_updated	Приложение syslog изменено
	syslog_app_name_updated_failed	Неуспешное изменение приложений syslog
logan_accounts		События LogAn
	administrator_added	Учётная запись администратора добавлена

Компонента	Событие	Описание
	administrator_deleted	Учётная запись администратора удалена
	administrator_profile_added	Профиль учётной записи администратора добавлен
	administrator_profile_delete_failed	Неуспешное удаление профиля администратора
	administrator_profile_deleted	Профиль учётной записи администратора удалён
	administrator_profile_updated	Профиль учётной записи администратора изменён
	administrator_role_add_failed	Неуспешное добавление роли
	administrator_role_added	Роль добавлена
	administrator_role_delete_failed	Неуспешное удаление роли
	administrator_role_deleted	Роль удалена
	administrator_role_fetch_failed	Неуспешное извлечение данных роли
	administrator_role_update_failed	Неуспешное изменение роли
	administrator_role_updated	Роль изменена
	administrator_updated	Учётная запись администратора изменена
	auth_server_add_failed	Неуспешное добавление сервера аутентификации
	auth_server_added	Сервер аутентификации добавлен
	auth_server_deleted	Сервер аутентификации удалён
	auth_server_update_failed	Неуспешное изменение сервера аутентификации

Компонента	Событие	Описание
	auth_server_updated	Сервер аутентификации изменён
	local_group_added	Локальная группа добавлена
	local_group_deleted	Локальная группа удалена
	local_group_updated	Локальная группа изменена
	local_user_added	Локальный пользователь добавлен
	local_user_deleted	Локальный пользователь удалён
	user_added_to_group	Пользователь добавлен в группу
	user_deleted_from_group	Пользователь удалён из группы
	user_updated	Пользователь изменён
logan_alertcategories		Категории событий LogAn
	category_add_failed	Неуспешная попытка добавления категории срабатывания
	category_added	Категория срабатывания добавлена
	category_delete_failed	Неуспешная попытка удаления категории срабатывания
	category_deleted	Категория срабатывания удалена
	category_fetch_failed	Неуспешная попытка извлечения данных о категории срабатывания
	category_updated	Категоряи срабатывания изменена
	category_updated_failed	

Компонента	Событие	Описание
		Неуспешная попытка изменения категории срабатывания
logan_devices		Устройства LogAn
	backup_export_rule_added	Правило резервного копирования добавлено
	backup_export_rule_deleted	Правило резервного копирования удалено
	backup_export_rule_updated	Правило резервного копирования изменено
	device_add_failed	Неуспешное добавлеие устройства LogAn
	device_added	Добавлено устройство LogAn
	device_check_license	Проверка лицензии LogAn
	device_check_license_failed	Неуспешная проверка лицензии LogAn
	device_delete_failed	Неуспешное удаление устройства LogAn
	device_deleted	Удалено устройство LogAn
	device_fetch_failed	Неуспешное извлечение данных об устройстве LogAn
	device_reboot	Устройство LogAn перезагружено
	device_reboot_failed	Неуспешная попытка перезагрузки устройства LogAn
	device_register	Устройство LogAn зарегистрировано
	device_register_failed	Неуспешная попытка регистрации устройства LogAn

Компонента	Событие	Описание
	device_shutdown	Устройство LogAn выключено
	device_shutdown_failed	Неуспешная попытка выключения устройства LogAn
	device_update_failed	Неуспешная попытка обновления устройства LogAn
	device_updated	Устройство LogAn обновлено
	settings_export_rule_added	Правило экспорта добавлено
	settings_export_rule_deleted	Правило экспорта удалено
	settings_export_rule_updated	Правило экспорта изменено
logan_devices_lists_update		Обновление списков LogAn
	update_fetch_failed	Неуспешное удаление обновляемого списка устройства LogAn
	update_update_failed	Неуспешное обновление обновляемого списка устройства LogAn
	update_updated	Обновляемый список устройства LogAn обновлён
logan_devices_update		Обновление LogAn
	update_add_failed	Неуспешная попытка добавления обновления для устройства LogAn
	update_added	Добавлено обновление для устройства LogAn
	update_delete_failed	Удалено обновление для устройства LogAn
	update_deleted	Удалено обновление для устройства LogAn

Компонента	Событие	Описание
	update_fetch_failed	Неуспешная попытка удаления обновления для устройства LogAn
	update_update_failed	Неуспешная попытка изменения обновления устройства LogAn
	update_updated	Обновления для устройства LogAn изменено
logan_group		Группа шаблонов LogAn
	template_group_add_failed	Неуспешное добавление группы шаблонов
	template_group_added	Группа шаблонов добавлена
	template_group_delete_failed	Неуспешное удаление группы шаблонов
	template_group_deleted	Группа шаблонов удалена
	template_group_fetch_failed	Неуспешное извлечение данных группы шаблонов
	template_group_update_failed	Неуспешное извлечение данных группы шаблонов
	template_group_updated	Группа шаблонов обновлена
logan_incident_resolutions		Решения инцидентов LogAn
	incident_resolution_add_failed	Неуспешная попытка добавления решения инцидента
	incident_resolution_added	Добавлено решение инцидента
	incident_resolution_delete_failed	Неуспешная попытка удаления решения инцидента
	incident_resolution_deleted	Удалено решение инцидента

Компонента	Событие	Описание
	incident_resolution_fetch_failed	Неуспешная попытка извлечения данных о решении инцидента
	incident_resolution_update_failed	Неуспешная попытка изменения решения инцидента
	incident_resolution_updated	Изменено решение инцидента
logan_incident_schemas		Схема инцидентов LogAn
	incident_schema_add_failed	Неуспешная попытка добавления схемы инцидентов
	incident_schema_added	Добавлена схема инцидента
	incident_schema_delete_failed	Неуспешная попытка удаления схемы инцидентов
	incident_schema_deleted	Удалена схема инцидента
	incident_schema_fetch_failed	Неуспешная попытка извлечения данных о схеме инцидентов
	incident_schema_update_failed	Неуспешная попытка изменения схемы инцидентов
	incident_schema_updated	Изменена схема инцидента
logan_incident_states		Состояния инцидентов LogAn
	incident_state_add_failed	Неуспешная попытка добавления состояния инцидента
	incident_state_added	Добавлено состояние инцидента
	incident_state_delete_failed	Неуспешная попытка удаления состояния инцидента

Компонента	Событие	Описание
	incident_state_deleted	Удалено состояние инцидента
	incident_state_fetch_failed	Неуспешная попытка извлечения данных о состоянии инцидента
	incident_state_update_failed	Неуспешная попытка изменения состояния инцидента
	incident_state_updated	Изменено состояние инцидента
logan_incident_types		Типы инцидентов LogAn
	incident_type_add_failed	Неуспешная попытка добавления типа инцидента
	incident_type_added	Добавлен тип инцидента
	incident_type_delete_failed	Неуспешная попытка удаления типа инцидента
	incident_type_deleted	удалён тип инцидента
	incident_type_fetch_failed	Неуспешная попытка извлечения данных о типе инцидента
	incident_type_update_failed	Неуспешная попытка изменения типа инцидента
	incident_type_updated	Изменён тип инцидента
logan_libraries		Библиотеки LogAn
	nlist_added	Список добавлен
	nlist_deleted	Список удалён
	nlist_exported	Список экспортирован
	nlist_import_failed	Ошибка при импорте списка
	nlist_imported	Список импортирован

Компонента	Событие	Описание
	nlist_item_added	Элемент списка добавлен
	nlist_item_deleted	Элемент списка удалён
	nlist_item_updated	Элемент списка изменён
	nlist_items_deleted	Элементы списка удалены
	nlist_updated	Список изменён
logan_log_collector		Сборщик логов LogAn
	rsyslog_rule_add_failed	Неуспешное добавление правила syslog
	rsyslog_rule_added	Правило syslog добавлено
	rsyslog_rule_delete_failed	Неуспешное удаление правила syslog
	rsyslog_rule_deleted	Правило syslog удалено
	rsyslog_rule_move_failed	Неуспешное перемещение правила syslog
	rsyslog_rule_moved	Правило syslog перемещено
	rsyslog_rule_updated	Правило syslog изменено
	rsyslog_rule_updated_failed	Неуспешное изменение правила syslog
	rsyslog_set_config	Конфигурация сервера syslog изменена
	rsyslog_set_config_failed	Неуспешное изменение конфигурации сервера syslog
	syslog_app_name_add_failed	Неуспешное добавление приложений syslog
	syslog_app_name_added	Приложение syslog добавлено
	syslog_app_name_delete_failed	Неуспешное удаление приложений syslog

Компонента	Событие	Описание
	syslog_app_name_deleted	Приложение syslog удалено
	syslog_app_name_updated	Приложение syslog изменено
	syslog_app_name_updated_failed	Неуспешное изменение приложений syslog
logan_network		Сеть LogAn
	adapter_added	Сетевой порт успешно добавлен
	bond_added	Бонд интерфейс добавлен
	default_gw_changed	Шлюз по умолчанию был изменён
	failover_update_failed	Неуспешное обновление настройки отказоустойчивости
	failover_updated	Изменена настройка отказоустойчивости
	gateway_add_failed	Неуспешное добавление сетевого шлюза
	gateway_added	Сетевой шлюз добавлен
	gateway_delete_failed	Неуспешное удаление сетевого шлюза
	gateway_deleted	Сетевой шлюз удалён
	gateway_fetch_failed	Неуспешное извлечение данных сетевого шлюза
	gateway_update_failed	Неуспешное обновление сетевого шлюза
	gateway_updated	Сетевой шлюз изменён
	iface_add_failed	Неуспешное добавление интерфейса

Компонента	Событие	Описание
	iface_delete_failed	Неуспешное удаление интерфейса
	iface_deleted	Сетевой интерфейс удалён
	iface_fetch_failed	Неуспешное извлечение данных интерфейса
	iface_update_failed	Неуспешное обновление интерфейса
	iface_updated	Сетевой интерфейс изменён
	route_add_failed	Неуспешное добавление маршрута
	route_added	Маршрут добавлен
	route_delete_failed	Неуспешное удаление маршрута
	route_deleted	Маршрут удалён
	route_fetch_failed	Неуспешное извлечение данных маршрута
	route_update_failed	Неуспешное обновление маршрута
	route_updated	Маршрут изменён
	vlan_added	VLAN добавлен
	zone_add_failed	Неуспешное добавление зоны
	zone_added	Зона добавлена
	zone_delete_failed	Неуспешное удаление зоны
	zone_deleted	Зона удалена
	zone_fetch_failed	Неуспешное извлечение данных зоны
	zone_update_failed	Неуспешное обновление зоны

Компонента	Событие	Описание
	zone_updated	Зона изменена
logan_notification		Оповещения LogAn
	smpp_profile_added	Профиль SMPP добавлен
	smpp_profile_deleted	Профиль SMPP удалён
	smpp_profile_updated	Профиль SMPP изменён
	smtp_profile_added	Профиль оповещения SMTP добавлен
	smtp_profile_deleted	Профиль оповещения SMTP удалён
	smtp_profile_updated	Профиль оповещения SMTP изменён
logan_sensors		Сенсоры LogAn
	mib_file_add_failed	Неуспешное добавление MIB файла
	mib_file_added	MIB файл добавлен
	mib_file_delete_failed	Неуспешное удаление MIB файла
	mib_file_deleted	MIB файл удалён
	snmp_sensor_add_failed	Неуспешное добавление SNMP сенсора
	snmp_sensor_added	SNMP сенсор добавлен
	snmp_sensor_delete_failed	Неуспешное удаление SNMP сенсора
	snmp_sensor_deleted	SNMP сенсор удалён
	snmp_sensor_fetch_failed	Неуспешное извлечение данных SNMP сенсора
	snmp_sensor_update_failed	Неуспешное изменение SNMP сенсора

Компонента	Событие	Описание
	snmp_sensor_updated	SNMP сенсор изменён
	utm_sensor_add_failed	Неуспешное добавление UserGate сенсора
	utm_sensor_added	UserGate сенсор добавлен
	utm_sensor_delete_failed	Неуспешное удаление UserGate сенсора
	utm_sensor_deleted	UserGate сенсор удалён
	utm_sensor_fetch_failed	Неуспешное извлечение данных UserGate сенсора
	utm_sensor_update_failed	Неуспешное изменение UserGate сенсора
	utm_sensor_updated	UserGate сенсор изменён
	wmi_sensor_add_failed	Неуспешное добавление WMI сенсора
	wmi_sensor_added	WMI сенсор добавлен
	wmi_sensor_delete_failed	Неуспешное удаление WMI сенсора
	wmi_sensor_deleted	WMI сенсор удалён
	wmi_sensor_fetch_failed	Неуспешное извлечение данных WMI сенсора
	wmi_sensor_update_failed	Неуспешное изменение WMI сенсора
	wmi_sensor_updated	WMI сенсор изменён
logan_settings		Настройки LogAn
	certificate_add	Сертификат добавлен
	certificate_add_failed	Неуспешная попытка добавления сертификата
	certificate_added	Сертификат добавлен

Компонента	Событие	Описание
	certificate_copied	Сертификат скопирован
	certificate_csr_generated	CSR создан
	certificate_deleted	Сертификат удалён
	certificate_export	Сертификат экспортирован
	certificate_generate_failed	Неуспешная попытка создания сертификата
	certificate_generated	Сертификат создан
	certificate_set_active	Сертификат активирован
	certificate_updated	Изменена роль сертификата
	update_failed	Обновление завершилось неуспешно
	updated	Обновлено
	utm_update_schedule_updated	Расписание проверки обновлений изменено
logan_template		Шаблоны LogAn
	template_add_failed	Неуспешное добавление шаблона
	template_added	Шаблон добавлен
	template_delete_failed	Неуспешное удаление шаблона
	template_deleted	Шаблон удалён
	template_fetch_failed	Неуспешное извлечение данных шаблона
	template_update_failed	Неуспешное обновление шаблона
	template_updated	Шаблон обновлён
logan_user_catalogs		Каталог пользователей LogAn

Компонента	Событие	Описание
	user_catalog_add_failed	Неуспешная попытка добавления каталога пользователей
	user_catalog_added	Каталог пользователей успешно добавлен
	user_catalog_delete_failed	Неуспешная попытка удаления каталога пользователей
	user_catalog_deleted	Каталог пользователей успешно удален
	user_catalog_fetch_failed	Неуспешная попытка извлечения данных каталога пользователей
	user_catalog_update_failed	Неуспешная попытка обновления каталога пользователей
	user_catalog_updated	Каталог пользователей успешно обновлен
logan_user_id_agent		Агент UserID LogAn
	filter_add_failed	Неуспешная попытка добавления syslog фильтра UserID агента
	filter_added	Добавлен syslog фильтр UserID агента
	filter_delete_failed	Неуспешная попытка удаления syslog фильтра UserID агента
	filter_deleted	Удален syslog фильтр UserID агента
	filter_fetch_failed	Неуспешная попытка получения syslog фильтра UserID агента
	filter_update_failed	Неуспешная попытка обновления syslog фильтра UserID агента

Компонента	Событие	Описание
	filter_updated	Изменен syslog фильтр UserID агента
	server_add_failed	Неуспешная попытка добавления сервера UserID агента
	server_added	Добавлен сервер UserID агента
	server_delete_failed	Неуспешная попытка удаления сервера UserID агента
	server_deleted	Удален сервер UserID агента
	server_fetch_failed	Неуспешная попытка получения сервера UserID агента
	server_update_failed	Неуспешная попытка изменения сервера UserID агента
	server_updated	Изменен сервер UserID агента
	set_agent_config	Настройки UserID агента успешно обновлены
	set_agent_config_failed	Неуспешная попытка обновления настроек UserID агента
	sharing_profile_add_failed	Неуспешная попытка добавления профиля редистрибуции UserID
	sharing_profile_added	Профиль редистрибуции UserID успешно добавлен
	sharing_profile_delete_failed	Неуспешная попытка удаления профиля редистрибуции UserID
	sharing_profile_deleted	Профиль редистрибуции UserID успешно удален

Компонента	Событие	Описание
	sharing_profile_fetch_failed	Неуспешная попытка получения профиля редистрибуции UserID
	sharing_profile_update_failed	Неуспешная попытка обновления профиля редистрибуции UserID
	sharing_profile_updated	Профиль редистрибуции UserID успешно обновлен
mailsecurity		Защита почтового трафика
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
nat		NAT и маршрутизация
	rule_add_failed	Неуспешное добавление правила
	rule_added	Правило добавлено
	rule_delete_failed	Неуспешное удаление правила
	rule_deleted	Правило удалено
	rule_move_failed	Неуспешное перемещение правила
	rule_moved	Правило перемещено
	rule_update_failed	Неуспешное изменение правила
	rule_updated	Правило изменено
network		Сеть
	adapter_added	Сетевой порт успешно добавлен

Компонента	Событие	Описание
	bond_added	Бонд интерфейс добавлен
	bridge_added	Мост интерфейс добавлен
	conntrack_overflow	Переполнение таблицы соединений (conntrack overflow)
	default_gw_changed	Шлюз по умолчанию был изменён
	device_cable_status_changed	Статус порта изменён
	device_driver_status	Состояние драйвера сетевой карты
	dhcp_added	DHCP сервер добавлен
	dhcp_deleted	DHCP сервер удалён
	dhcp_lease_deleted	Настройка аренды адресов DHCP сервера удалена
	dhcp_updated	DHCP сервер изменён
	dns_rule_added	Добавлено правило DNS
	dns_rule_deleted	Удалено правило DNS
	dns_rule_updated	Изменено правило DNS
	dns_static_rec_added	Статическая запись DNS добавлена
	dns_static_rec_deleted	Статическая запись DNS удалена
	dns_static_rec_updated	Статическая запись DNS изменена
	failover_update_failed	Неуспешное обновление настройки отказоустойчивости
	failover_updated	Изменена настройка отказоустойчивости

Компонента	Событие	Описание
	gateway_add_failed	Неуспешное добавление сетевого шлюза
	gateway_added	Сетевой шлюз добавлен
	gateway_delete_failed	Неуспешное удаление сетевого шлюза
	gateway_deleted	Сетевой шлюз удалён
	gateway_fetch_failed	Неуспешное извлечение данных сетевого шлюза
	gateway_update_failed	Неуспешное обновление сетевого шлюза
	gateway_updated	Сетевой шлюз изменён
	ha_cluster_added	Кластер отказоустойчивости добавлен
	ha_cluster_deleted	Кластер отказоустойчивости удалён
	ha_cluster_instance_add	Кластер отказоустойчивости добавлен
	ha_cluster_updated	Кластер отказоустойчивости изменён
	iface_add_failed	Неуспешное добавление интерфейса
	iface_delete_failed	Неуспешное удаление интерфейса
	iface_deleted	Сетевой интерфейс удалён
	iface_fetch_failed	Неуспешное извлечение данных интерфейса
	iface_update_failed	Неуспешное обновление интерфейса
	iface_updated	Сетевой интерфейс изменён

Компонента	Событие	Описание
	pcap_filter_added	Фильтр захвата пакетов добавлен
	pcap_filter_deleted	Фильтр захвата пакетов удалён
	pcap_filter_updated	Фильтр захвата пакетов изменён
	pcap_rule_added	Правило захвата пакетов добавлено
	pcap_rule_deleted	Правило захвата пакетов удалено
	pcap_rule_updated	Правило захвата пакетов изменено
	pppoe_added	Интерфейс PPPoE добавлен
	reverseproxy_profile_add_failed	Неуспешное добавление правила reverse-прокси
	reverseproxy_profile_added	Сервер reverse-прокси добавлен
	reverseproxy_profile_delete_failed	Неуспешное удаление правила reverse-прокси
	reverseproxy_profile_deleted	Сервер reverse-прокси удалён
	reverseproxy_profile_update_failed	Неуспешное обновление правила reverse-прокси
	reverseproxy_profile_updated	Сервер reverse-прокси изменён
	reverseproxy_rule_add_failed	Неуспешное добавление правила reverse-прокси
	reverseproxy_rule_added	Правило reverse-прокси добавлено
	reverseproxy_rule_delete_failed	Неуспешное удаление правила reverse-прокси

Компонента	Событие	Описание
	reverseproxy_rule_deleted	Правило reverse-прокси удалено
	reverseproxy_rule_fetch_failed	Неуспешное извлечение данных правила reverse-прокси
	reverseproxy_rule_move_failed	Неуспешное перемещение правила reverse-прокси
	reverseproxy_rule_moved	Правило reverse-прокси перемещено
	reverseproxy_rule_update_failed	Неуспешное обновление правила reverse-прокси
	reverseproxy_rule_updated	Правило reverse-прокси изменено
	route_add_failed	Неуспешное добавление маршрута
	route_added	Маршрут добавлен
	route_delete_failed	Неуспешное удаление маршрута
	route_deleted	Маршрут удалён
	route_fetch_failed	Неуспешное извлечение данных маршрута
	route_update_failed	Неуспешное обновление маршрута
	route_updated	Маршрут изменён
	scenario_rule_added	Правило сценария добавлено
	scenario_rule_deleted	Правило сценария удалено
	scenario_rule_updated	Правило сценария изменено
	tunnel_added	Туннель добавлен

Компонента	Событие	Описание
	users_overflow	Количество лицензий использовано на 90%
	virtual_router_add_failed	Неуспешное удаление вируального маршрутизатора
	virtual_router_added	Виртуальный маршрутизатор добавлен
	virtual_router_delete_failed	Неуспешное удаление вируального маршрутизатора
	virtual_router_deleted	Виртуальный маршрутизатор удалён
	virtual_router_update_failed	Неуспешное обновление вируального маршрутизатора
	virtual_router_updated	Виртуальный маршрутизатор изменён
	vlan_added	VLAN добавлен
	vpn_added	VPN адаптер добавлен
	zone_add_failed	Неуспешное добавление зоны
	zone_added	Зона добавлена
	zone_delete_failed	Неуспешное удаление зоны
	zone_deleted	Зона удалена
	zone_fetch_failed	Неуспешное извлечение данных зоны
	zone_update_failed	Неуспешное обновление зоны
	zone_updated	Зона изменена
notification		Оповещения

Компонента	Событие	Описание
	alert_rule_added	Правило оповещения добавлено
	alert_rule_deleted	Правило оповещения удалено
	alert_rule_updated	Правило оповещения изменено
	smpp_profile_added	Профиль SMPP добавлен
	smpp_profile_deleted	Профиль SMPP удалён
	smpp_profile_updated	Профиль SMPP изменён
	smtp_notification_failed	SMTP оповещение завершено с ошибкой
	smtp_profile_added	Профиль оповещения SMTP добавлен
	smtp_profile_deleted	Профиль оповещения SMTP удалён
	smtp_profile_updated	Профиль оповещения SMTP изменён
ospf		OSPF
	area_added	Область добавлена
	area_deleted	Область OSPF удалена
	area_updated	Область OSPF обновлена
	interface_added	OSPF интерфейс добавлен
	interface_deleted	OSPF интерфейс удалён
	interface_updated	OSPF интерфейс изменён
	router_updated	OSPF-маршрутизатор изменён
override_domains		Изменённые домены
	override_domain_add_failed	

Компонента	Событие	Описание
		Неуспешное добавление изменения категории домена
	override_domain_added	Для домена изменена категория
	override_domain_delete_failed	Неуспешное удаление категории домена
	override_domain_deleted	Измененная категория домена удалена
	override_domain_fetch_failed	Неуспешное извлечение данных категории домена
	override_domain_import	Импортирован файл со списком доменов
	override_domain_update	изменён домен с изменённой категорией
	override_domain_update_failed	Неуспешное изменение категории домена
pimsm		Мультикаст маршрутизатор
	interface_added	Добавлен интерфейс
	interface_deleted	удалён интерфейс
	interface_updated	изменён интерфейс
	router_updated	Изменены настройки маршрутизатора
	rpmapping_added	Добавлен rendezvous point
	rpmapping_deleted	удалён rendezvous point
	rpmapping_updated	изменён rendezvous point
proxyportal		Веб-портал
	bookmark_adde_failed	Неуспешное добавление данных закладки веб-портала

Компонента	Событие	Описание
	bookmark_added	Закладка веб-портала добавлена
	bookmark_delete_failed	Неуспешное удаление закладки Веб-портала
	bookmark_deleted	Неуспешное извлечение данных закладки Веб-портала
	bookmark_fetch_failed	Неуспешное извлечение данных закладки Веб-портала
	bookmark_move_failed	Неуспешное перемещение закладки веб-портала
	bookmark_moved	Закладка веб-портала перемещена
	bookmark_update_failed	Неуспешное обновление закладки веб-портала
	bookmark_updated	Закладка веб-портала изменена
	config_set	Настройка веб-портал изменена
	login_failed	Ошибка аутентификации
	login_failed_2fa_code	Ошибка аутентификации MFA
	login_successful	Успешная аутентификация
radius		Radius
	accounting_start	Зарегистрирован пользователь через Radius accounting
rip		RIP
	interface_added	Добавлен интерфейс
	interface_deleted	удалён интерфейс

Компонента	Событие	Описание
	interface_updated	изменён интерфейс
	router_updated	Изменены настройки маршрутизатора
safebrowsing_rules		Веб-безопасность
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
scada		SCADA
	profile_added	Профиль добавлен
	profile_deleted	Профиль удалён
	profile_updated	Профиль изменён
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
sensors		Сенсоры
	mib_file_add_failed	Неуспешное добавление MIB файла
	mib_file_added	MIB файл добавлен
	mib_file_delete_failed	Неуспешное удаление MIB файла
	mib_file_deleted	MIB файл удалён
	snmp_sensor_add_failed	Неуспешное добавление SNMP сенсора

Компонента	Событие	Описание
	snmp_sensor_added	SNMP сенсор добавлен
	snmp_sensor_delete_failed	Неуспешное удаление SNMP сенсора
	snmp_sensor_deleted	SNMP сенсор удалён
	snmp_sensor_fetch_failed	Неуспешное извлечение данных SNMP сенсора
	snmp_sensor_update_failed	Неуспешное изменение SNMP сенсора
	snmp_sensor_updated	SNMP сенсор изменён
	utm_sensor_add_failed	Неуспешное добавление UserGate сенсора
	utm_sensor_added	UserGate сенсор добавлен
	utm_sensor_delete_failed	Неуспешное удаление UserGate сенсора
	utm_sensor_deleted	UserGate сенсор удалён
	utm_sensor_fetch_failed	Неуспешное извлечение данных UserGate сенсора
	utm_sensor_offline	UserGate сенсор потерял соединение
	utm_sensor_online	UserGate сенсор подключён
	utm_sensor_update_failed	Неуспешное изменение UserGate сенсора
	utm_sensor_updated	UserGate сенсор изменён
	wmi_sensor_add_failed	Неуспешное добавление WMI сенсора
	wmi_sensor_added	WMI сенсор добавлен
	wmi_sensor_delete_failed	Неуспешное удаление WMI сенсора
	wmi_sensor_deleted	WMI сенсор удалён

Компонента	Событие	Описание
	wmi_sensor_fetch_failed	Неуспешное извлечение данных WMI сенсора
	wmi_sensor_update_failed	Неуспешное изменение WMI сенсора
	wmi_sensor_updated	WMI сенсор изменён
settings		Настройки
	antispam_updated	Конфигурация защиты почтового трафика обновлена
	batv_config_updated	Конфигурация BATV модуля защиты почты обновлена
	certificate_add	Сертификат добавлен
	certificate_add_failed	Неуспешная попытка добавления сертификата
	certificate_added	Сертификат добавлен
	certificate_copied	Сертификат скопирован
	certificate_csr_generated	CSR создан
	certificate_deleted	Сертификат удалён
	certificate_deleted_failed	Неуспешная попытка удаления сертификата
	certificate_export	Сертификат экспортирован
	certificate_generate_failed	Неуспешная попытка создания сертификата
	certificate_generated	Сертификат создан
	certificate_set_active	Сертификат активирован
	certificate_updated	Изменена роль сертификата
	conntrack_sync_config_updated	Изменена настройка синхронизации сессий

Компонента	Событие	Описание
	custom_dns_added	DNS-сервер добавлен
	custom_dns_deleted	DNS-сервер удалён
	custom_dns_updated	DNS-сервер изменён
	dashboard_tab_added	Dashboard добавлена
	dashboard_tab_deleted	Dashboard удалена
	default_dashboard_created	Создана дашборд по умолчанию
	default_incident_dashboard_created	Создана дашборд инцидентов по умолчанию
	dnsbl_config_updated	Настройка DNSBL изменена
	failover_config_updated	Изменена настройка отказоустойчивости
	fetch_failed	Параметр не найден
	idps_config_updated	Настройка СОВ изменена
	incident_dashboard_tab_added	Дэшборд инцидентов добавлена
	l7_config_updated	Конфигурация L7 обновлена
	server_time_changed	Сервер точного времени изменён
	statserver_config_updated	Настройка сервера Log Analyzer изменена
	update_failed	Обновление завершилось неуспешно
	updated	Обновлено
	utm_update_schedule_updated	Расписание проверки обновлений изменено
snmp_engine_id		SNMP Engine ID
	engine_id_updated	SNMP Engine ID

Компонента	Событие	Описание
snmp_parameters		Параметры SNMP
	parameters_add_failed	Добавление параметров SNMP завершено с ошибкой
	parameters_added	Параметры SNMP успешно добавлены
	parameters_delete_fail	Удаление параметров SNMP завершено с ошибкой
	parameters_deleted	Параметры SNMP успешно удалены
	parameters_update_fail	Обновление параметров SNMP завершено с ошибкой
	parameters_updated	Параметры SNMP успешно обновлены
snmp_rules		SNMP
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_updated	Правило изменено
	snmp_security_profile_added	Профиль безопасности SNMP добавлен
	snmp_security_profile_deleted	Профиль безопасности SNMP удален
	snmp_security_profile_updated	Неуспешная попытка удаления профиля безопасности SNMP
snmp_security_profiles		Профиль безопасности SNMP
	snmp_security_profile_added	Профиль безопасности SNMP добавлен
	snmp_security_profile_deleted	Профиль безопасности SNMP удален

Компонента	Событие	Описание
	snmp_security_profile_updated	Неуспешная попытка удаления профиля безопасности SNMP
snmp_sys_description		SNMP описание системы
	sys_description_updated	SNMP описание системы успешно обновлено
snmp_sys_location		SNMP локация системы
	sys_location_updated	SNMP локация системы успешно обновлено
snmp_sys_name		SNMP имя системы
	sys_name_updated	SNMP имя системы успешно обновлено
ssh_decryption_rules		SSH дешифрование
	rule_add_failed	Неуспешное добавление правила
	rule_added	Правило добавлено
	rule_delete_failed	Неуспешное удаление правила
	rule_deleted	Правило удалено
	rule_fetch_failed	Неуспешное извлечение данных правила
	rule_move_failed	Неуспешное перемещение правила
	rule_moved	Правило перемещено
	rule_update_failed	Неуспешное изменение правила
	rule_updated	Правило изменено
statistics		Log Analyzer
	account_added	Учётная запись добавлена

Компонента	Событие	Описание
	account_deleted	Учётная запись удалена
	log_normalization_rule_added	Правило нормализации журналов добавлено
	log_normalization_rule_deleted	Правило нормализации журналов удалено
	log_normalization_rule_updated	Правило нормализации журналов изменено
	logexport_copy_failed	Ошибка экспорт журналов
	logexport_copy_finished	Экспорт журналов завершён
	logexport_copy_started	Экспорт журналов начат
	logexport_logs_cleared	Журналы очищены
	logexport_rule_added	Правило экспорта журналов добавлено
	logexport_rule_deleted	Правило экспорта журналов удалено
	logexport_rule_updated	Правило экспорта журналов изменено
	remote_server_alarm	Оповещение удалённого сервера LogAn
	remote_server_config_set	Удалённый сервер Log Analyzer настроен
	remote_server_connected	Удалённый сервер Log Analyzer подключён
	remote_server_error	Ошибка удалённого сервера Log Analyzer
	report_deleted	Отчёт удалён
	report_rule_added	Правило отчёта добавлено
	report_rule_deleted	Правило отчёта удалено
	report_rule_exec	Правило отчёта запущено

Компонента	Событие	Описание
	report_rule_failed	Создание отчёта закончилось с ошибкой
	report_rule_finished	Создание отчёта закончилось успешно
	report_rule_started	Началось создание отчёта
	report_rule_updated	Правило отчёта изменено
	report_template_added	Шаблон отчёта добавлен
	report_template_deleted	Шаблон отчёта удалён
	report_template_updated	Шаблон отчёта изменён
	rotate_database	Ротация базы данных
	rotate_database_error	Ротация базы данных закончилась с ошибкой
tunnel_inspection_rules		Инспектирования туннелей
	rule_added	Правило добавлено
	rule_deleted	Правило удалено
	rule_moved	Правило перемещено
	rule_updated	Правило изменено
updater		Обновления
	check_version	Проверка версии
	download_failed	Скачивание закончилось неуспешно
	download_finished	Скачивание закончилось успешно
	download_started	Скачивание началось
	kavkas_finished	Обновление эвристического движка завершено

Компонента	Событие	Описание
	kavkas_started	Начато обновление эвристического движка
	offline_update_started	Начата установка автономного обновления
	security_update_apply	Установка обновления
	security_update_apply_error	Установка обновления завершилась неуспешно
	security_update_apply_ok	Установка обновления завершилась успешно
	security_update_delete	Обновление отозвано
	security_update_upload	Загрузка обновления завершилась успешно
	security_update_upload_failed	Загрузка обновления завершилась неуспешно
	up_to_date	Установлена последняя версия
	update_failed	Обновление завершилось неуспешно
	update_finished	Обновление завершилось успешно
	update_started	Обновление запущено
user_catalogs		Каталог пользователей
	user_catalog_add_failed	Неуспешная попытка добавления каталога пользователей
	user_catalog_added	Каталог пользователей успешно добавлен
	user_catalog_delete_failed	Неуспешная попытка удаления каталога пользователей

Компонента	Событие	Описание
	user_catalog_deleted	Каталог пользователей успешно удален
	user_catalog_fetch_failed	Неуспешная попытка извлечения данных каталога пользователей
	user_catalog_update_failed	Неуспешная попытка обновления каталога пользователей
	user_catalog_updated	Каталог пользователей успешно обновлен
user_id_agent		Агент UserID
	filter_add_failed	Неуспешная попытка добавления syslog фильтра UserID агента
	filter_added	Добавлен syslog фильтр UserID агента
	filter_delete_failed	Неуспешная попытка удаления syslog фильтра UserID агента
	filter_deleted	Удален syslog фильтр UserID агента
	filter_update_failed	Неуспешная попытка изменения syslog фильтра UserID агента
	filter_updated	Изменен syslog фильтр UserID агента
	server_add_failed	Неуспешная попытка добавления сервера UserID агента
	server_added	Добавлен сервер UserID агента
	server_delete_failed	Неуспешная попытка удаления сервера UserID агента

Компонента	Событие	Описание
	server_deleted	Удален сервер UserID агента
	server_update_failed	Неуспешная попытка изменения сервера UserID агента
	server_updated	Изменен сервер UserID агента
	set_agent_config	Настройки UserID агента успешно обновлены
	set_agent_config_failed	Неуспешная попытка обновления настроек UserID агента
	sharing_profile_add_failed	Неуспешная попытка добавления профиля редистрибуции UserID
	sharing_profile_added	Профиль редистрибуции UserID успешно добавлен
	sharing_profile_delete_failed	Неуспешная попытка удаления профиля редистрибуции UserID
	sharing_profile_deleted	Профиль редистрибуции UserID успешно удален
	sharing_profile_update_failed	Неуспешная попытка обновления профиля редистрибуции UserID
	sharing_profile_updated	Профиль редистрибуции UserID успешно обновлен
vpn		VPN
	auth_profile_added	Профиль аутентификации VPN добавлен
	auth_profile_deleted	Профиль аутентификации VPN удалён
	auth_profile_updated	Профиль аутентификации VPN изменён

Компонента	Событие	Описание
	client_connected	Подключён клиент VPN
	client_connecting	Подключение клиента VPN
	client_error	Ошибка клиента
	client_rule_add_failed	Неуспешное добавление клиентского правила VPN
	client_rule_added	Клиентское правило VPN добавлено
	client_rule_delete_failed	Неуспешное удаление клиентского правила VPN
	client_rule_deleted	Клиентское правило VPN удалено
	client_rule_fetch_failed	Неуспешное извлечение данных клиентского правила VPN
	client_rule_update_failed	Неуспешное обновление клиентского правила VPN
	client_rule_updated	Клиентское правило VPN изменено
	client_security_profile_added	Клиентский профиль безопасности VPN добавлен
	client_security_profile_deleted	Клиентский профиль безопасности VPN удален
	client_security_profile_updated	Клиентский профиль безопасности VPN обновлен
	client_started	Клиент запущен
	security_profile_added	Профиль безопасности VPN добавлен
	security_profile_deleted	Профиль безопасности VPN удалён
	security_profile_updated	Профиль безопасности VPN изменён

Компонента	Событие	Описание
	server_connected	Сервер VPN подключён
	server_error	Ошибка сервера
	server_rule_add_failed	Неуспешное добавление серверного правила VPN
	server_rule_added	Серверное правило VPN добавлено
	server_rule_delete_failed	Неуспешное удаление серверного правила VPN
	server_rule_deleted	Серверное правило VPN удалено
	server_rule_fetch_failed	Неуспешное извлечение данных серверного правила VPN
	server_rule_move_failed	Неуспешное перемещение серверного правила VPN
	server_rule_moved	Серверное правило VPN перемещено
	server_rule_update_failed	Неуспешное изменение серверного правила VPN
	server_rule_updated	Серверное правило VPN изменено
	server_security_profile_added	Серверный профиль безопасности VPN добавлен
	server_security_profile_deleted	Серверный профиль безопасности VPN удален
	server_security_profile_updated	Серверный профиль безопасности VPN обновлен
	server_started	VPN сервер запущен
	tunnel_added	Сеть VPN добавлена
	tunnel_deleted	Сеть VPN удалена

Компонента	Событие	Описание
	tunnel_updated	Сеть VPN изменена
	user_disconnected	Пользователь VPN отключился
	user_login_failed	Подключение пользователя к VPN не удалось
	user_login_success	Подключение пользователя к VPN прошло успешно
wccp		WCCP
	rule_add_failed	Неуспешное добавление правила
	rule_added	Правило добавлено
	rule_delete_failed	Неуспешное удаление правила
	rule_deleted	Правило удалено
	rule_fetch_failed	Неуспешное извлечение данных правила
	rule_update_failed	Неуспешное обновление правила
	rule_updated	Правило обновлено
wrdp_server		Веб-портал RDP
	authenticate_failed	Ошибка входа на сервер RDP
	connection_successful	Успешное подключение к серверу RDP
	disconnected	Отключение от сервера RDP
	get_default_template_failed	Невозможно получить шаблон RDP сервера
	host_not_found	Сервер RDP не найден
	internal_server_error	

Компонента	Событие	Описание
		Внутренняя ошибка сервера RDP
wssh_server		Веб-портал SSH
	authenticate_failed	Ошибка входа на сервер SSH
	connection_refused	Подключение к серверу SSH отклонено
	get_default_template_failed	Невозможно получить шаблон SSH сервера
	host_not_found	Сервер SSH не найден
	internal_server_error	Внутренняя ошибка сервера SSH
	login_successful	Успешная аутентификация