Table of Contents

Table of Contents 1
Введение 2
- Безопасность сети и защита от сетевых угроз 3
  - Межсетевое экранирование 4
  - Обнаружение и предотвращение вторжений 5
  - Защита от DOS-атак и сетевого флуда 6
  - Антивирусная проверка трафика 7
  - Проверка почтового трафика 8
  - Работа с внешними системами безопасности 9
  - Управление АСУ ТП 10
  - Настройка политик безопасности при помощи сценариев 11
- Улучшение производительности и надежности интернета 12
  - Поддержка кластеризации и отказоустойчивости 13
  - FTP поверх HTTP 14
  - Поддержка нескольких провайдеров 15
  - Управление пропускной способностью 16
  - Поддержка WCCP 17
- Управление трафиком и контроль доступа в интернет 18
  - Маршрутизация трафика и публикация ресурсов 19
  - Аутентификация и авторизация пользователей 20
  - Поддержка гостевого портала 21
  - Проксирование приложений 22
- Журналы и отчеты 23
  - Журналы и отчеты(описание) 24
- Другие функции 25
  - Ролевой доступ администраторов к элементам управления UserGate NGFW 26
  - Использование оповещений 27
  - Типы интерфейсов 28
  - DNS-фильтрация 29
  - Функция балансировщика нагрузки 30
- Контент-фильтрация и контроль приложений 31
  - Интернет-фильтрация 32
  - Выборочная блокировка рекламы 33
  - Активация безопасного поиска 34
  - Блокировка приложений социальных сетей 35
  - Инжектирование кода на веб-страницы 36
  - Инспектирование SSL-трафика 37
  - VPN и веб-портал 38
- Совместимость с аппаратными платформами 39
  - Совместимость версий UserGate NGFW с аппаратными платформами 40

Введение

Безопасность сети и защита от сетевых угроз

Межсетевое экранирование

Documentation:

Version: 5.x, 6.1.9, 7.x, 7.0.1

Product: NGFW

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

Обнаружение и предотвращение вторжений

Version: 7.0.1, 6.1.9, 5.x

Documentation: ☑

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

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

Защита от DOS-атак и сетевого флуда

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

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

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

Антивирусная проверка трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation:

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

Проверка почтового трафика

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

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

Работа с внешними системами безопасности

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

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

Управление АСУ ТП

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: ☑

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

Настройка политик безопасности при помощи сценариев

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

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

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

Улучшение производительности и надежности интернета

Поддержка кластеризации и отказоустойчивости

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

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

FTP поверх HTTP

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

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

Поддержка нескольких провайдеров

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

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

Управление пропускной способностью

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

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

Поддержка WCCP

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

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

Управление трафиком и контроль доступа в интернет

Маршрутизация трафика и публикация ресурсов

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

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

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

Аутентификация и авторизация пользователей

Documentation:

Product: UserGate NGFW

Version: 6.1.9, 7.0.1

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

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

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

Поддержка гостевого портала

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

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

Проксирование приложений

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

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

Журналы и отчеты

Журналы и отчеты(описание)

Documentation:

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

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

Другие функции

Ролевой доступ администраторов к элементам управления UserGate NGFW

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

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

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

Использование оповещений

Documentation:

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

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

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

Типы интерфейсов

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

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

DNS-фильтрация

Documentation:

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

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

Функция балансировщика нагрузки

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

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

Контент-фильтрация и контроль приложений

Интернет-фильтрация

Documentation:

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

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

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

Выборочная блокировка рекламы

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

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

Активация безопасного поиска

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☑

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

Блокировка приложений социальных сетей

Product: NGFW

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Documentation: ☑

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

Инжектирование кода на веб-страницы

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation:

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

Инспектирование SSL-трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation:

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

VPN и веб-портал

Version: 5.x, 6.1.9, 7.0.1

Documentation: ☑

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

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

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

Совместимость с аппаратными платформами

Совместимость версий UserGate NGFW с аппаратными платформами

Documentation:
Product: NGFW
Version: 7.0.1

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

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

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