

Table of Contents

Table of Contents	1
Описание функций	2
Основные функции UserGate	3
Зеркалирование дешифрованного SSL трафика (Decryption Mirroring)	7

Основные функции UserGate

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

UserGate представляет собой универсальный интернет-шлюз безопасности, объединяющий в себе межсетевой экран, маршрутизацию, шлюзовой антивирус, систему обнаружения и предотвращения вторжений (COB), VPN-сервер, систему контентной фильтрации, модуль мониторинга и статистики и многие другие функции. Продукт позволяет управлять сетью компании, оптимизировать используемый ею трафик и эффективно предотвращать интернет-угрозы.

Безопасность сети и защита от сетевых угроз

Межсетевое экранирование

Встроенный в UserGate межсетевой экран нового поколения (NGFW - Next Generation Firewall) 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

Система обнаружения и предотвращения вторжений (COB) 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 COB-профили (наборы сигнатур, релевантных для защиты определенных сервисов) и задавать правила COB, определяющие действия для выбранного типа трафика, который будет проверяться модулем COB в соответствии с назначенными профилями.

Защита от DOS-атак и сетевого флуда

UserGate 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

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

Проверка почтового трафика

UserGate 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. UserGate также предоставляет возможность гибкой настройки фильтрации почтового трафика по группам пользователей.

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.

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.

Настройка политик безопасности при помощи сценариев

UserGate 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.

Улучшение производительности и надежности интернета

Поддержка кластеризации и отказоустойчивости

UserGate 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

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

Поддержка нескольких провайдеров

При подключении системы к нескольким провайдерам UserGate 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

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

Поддержка WCCP

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

Управление трафиком и контроль доступа в интернет

Маршрутизация трафика и публикация ресурсов

UserGate позволяет использовать как статическую, так и динамическую маршрутизацию. Динамическая маршрутизация осуществляется по протоколам OSPF и BGP, что позволяет использовать UserGate 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.

Авторизация пользователей

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

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

UserGate 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

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 UserGate не является шлюзом по умолчанию.

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.

Контент-фильтрация и контроль приложений

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. UserGate 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

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.

Активация безопасного поиска

UserGate 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

UserGate 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

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

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».

VPN и веб-портал

VPN (Virtual Private Network) служит для того, чтобы настраивать виртуальные логические сети поверх других сетей, например, интернет. UserGate 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. UserGate 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.

Журналы и отчеты

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

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

UserGate 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

UserGate 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

UserGate 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

UserGate 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.

Зеркалирование дешифрованного SSL трафика (Decryption Mirroring)

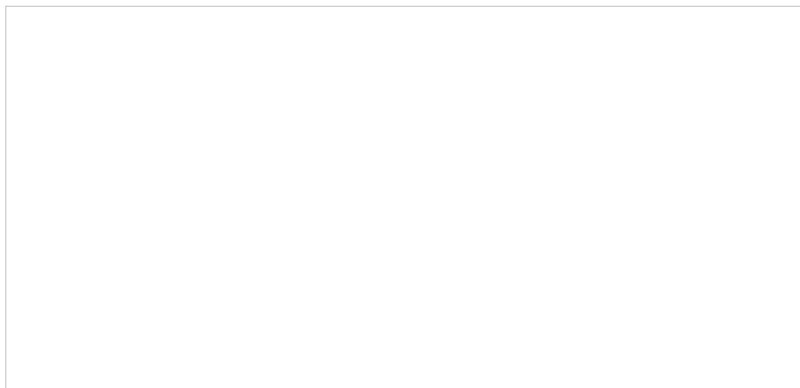
Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Функция «Расшифровать и переслать» (доступна с версии 7.0.0) предоставляет возможность передачи расшифрованного трафика SSL/TLS с брандмауэра на систему сбора и обработки трафика, например: Data Leak Protection(DLP), Intrusion Detection System(IDS), Intrusion Detection and Prevention Systems(IDPS), Антивирусная обработка и т. д.

Эта функция необходима организациям, которым требуется комплексный сбор данных в целях обеспечения безопасности и/или функция предотвращения утечки данных (DLP).

Схема подключения в общем случае выглядит так:



Таким образом, реализуется возможность проверки зашифрованного трафика практически любым анализатором трафика, вне зависимости поддерживает он SSL или нет.

В **UserGate NGFW** реализована возможность реализации 2х вариантов пересылки SSL трафика:

1. **L2**. Пересылка через физический порт **UserGate NGFW**.

В этом случае дешифрованный SSL-трафик отправляется устройству анализа трафика, подключенному непосредственно к физическому порту UserGate NGFW.

2. **L3-туннель**. Пересылка дешифрованного трафика через GRE-туннель.

В этом случае дешифрованный SSL-трафик отправляется устройству анализа трафика посредством GRE-туннеля.

Для настройки этой функции следует перейти в раздел "Политики безопасности-инспектирование SSL" и создать правило инспектирования SSL трафика. (подробнее см [Руководство Администратора](#)). В свойствах правила необходимо выбрать пункт "Действие-Расшифровать и переслать", после этого станет доступным поле "Профиль пересылки SSL", где необходимо выбрать или создать профиль для пересылки SSL трафика. При создании профиля пересылки SSL, доступны поля:

Наименование	Описание
Название	Название профиля пересылки SSL. (может быть любым, обязательное поле)
Описание	Описание профиля. (может быть пустым)
Тип пересылки	Тип пересылки трафика. Может быть: 1). L2 - пересылка через физический порт UG NGFW/кластера. 2). L3 - пересылка через L3 туннель
MAC-адрес назначения	Доступен при выборе значения поля Тип пересылки - L2. Позволяет указать MAC-адрес устройства-приемника зеркалированного трафика.
Пересылать на интерфейс	Доступен при выборе значения поля Тип пересылки - L2. Имя порта UG NGFW, используемого для пересылки дешифрованного SSL трафика.
GRE IP-адрес источника	Доступен при выборе значения поля Тип пересылки - L3-туннель. Позволяет указать IP-адрес источника данных в GRE-туннеле.
GRE IP-адрес назначения	Доступен при выборе значения поля Тип пересылки - L3-туннель. Позволяет указать IP-адрес назначения в GRE-туннеле.

Примечание В случае с кластерной реализацией UserGate NGFW, при выборе имени порта для L2 пересылки администратор должен

убедиться, что на всех узлах кластера существует порт с одинаковым именем (например, port1.100), и именно он будет использоваться на всех узлах кластера для пересылки дешифрованного SSL-трафика.

