Table of Contents

Table of Contents 1
Управление трафиком и контроль доступа в интернет 2
- Маршрутизация трафика и публикация ресурсов 3
- Аутентификация и авторизация пользователей 4
- Поддержка гостевого портала 5
- Проксирование приложений 6
- Перенаправление трафика на вышестоящий прокси-сервер 7

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: NGFW
Version: 7.x

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 устройстве UserGate. В Captive-портале также возможна аутентификация пользователей посредством сертификатов, использующих инфраструктуру открытых ключей (PKI).

Благодаря функциональности UserID возможна прозрачная аутентификация пользователей на выбранных устройствах UserGate. В качестве источника данных аутентификации используются журналы Active Directory, syslog и сообщения RADIUS accounting. Для этого агент UserID осуществляет запросы посредством протокола WMI на серверы AD, в сценарии с syslog осуществляет прослушивание порта syslog и сбор информации, которую присылают серверы syslog, а в сценарии с RADIUS-серверами принимает сообщения RADIUS accounting от серверов NAS. Далее информация фильтруется по событиям входа/выхода пользователей. По полученным данным происходит поиск пользователя в каталогах пользователей источника логов. Если пользователь найден, то данные для авторизации пользователя отправляются на все устройства UserGate, указанные в Профиле редистрибуции источника и производится вход пользователя 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.

Перенаправление трафика на вышестоящий прокси-сервер

Documentation:
Product: NGFW
Version: 7.1.0

С помощью функциональности Upstream proxy UserGate NGFW позволяет перенаправлять пользовательский трафик на вышестоящий прокси-сервер, благодаря чему возможно создание каскадной иерархии, когда трафик с одного прокси-сервера передается на следующий в цепочке прокси-серверов. Подобное каскадирование обычно используется для обеспечения конфиденциальности коммуникаций или для организации доступа к контенту с региональными ограничениями. Также благодаря технологии каскадирования упрощается встраивание новых региональных офисов в существующую иерархию глобальной сети компании.