

Table of Contents

Table of Contents	1
О UserGate DCFW	2
Общие сведения	3
Функциональные возможности	4
Алгоритм обработки трафика	5

Общие сведения

Product: DCFW

Version: 8.x

UserGate Data Center Firewall (DCFw) — высокопроизводительный межсетевой экран для защиты крупных корпоративных сетей и центров обработки данных, способный работать с сотнями тысяч правил без линейного падения производительности благодаря использованию механизма поиска правил по множеству критериев собственной разработки.

UserGate DCFw поставляется в виде программно-аппаратного комплекса (ПАК) либо в виде образа виртуальной машины, предназначенного для развертывания в виртуальной среде.

Функциональные возможности

Product: DCFW

Version: 8.x

Операционная система UGOS 8.0 для DCFW обладает широким набором функциональностей, необходимых для межсетевого экрана нового поколения.

Сетевые функции включают в себя статическую и динамическую маршрутизацию, поддержку VLAN, технологий балансировки и управления качеством обслуживания, фильтрацию на уровнях L3-L7, различные типы трансляции адресов, поддержку VPN-туннелей.

Поддерживаются различные механизмы аутентификации пользователей: Captive-портал, NTLM, при этом учетные записи могут поступать из различных источников — LDAP, Active directory, FreeIPA, TACACS+, RADIUS, SAML IDP. Аутентификация SAML IDP, 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.

Поддерживается идентификация приложений и система обнаружения вторжений. Система обнаружения 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 собственные сигнатуры для защиты определенных сервисов и включать их в профили наряду с сигнатурами, поставляемыми UserGate. Профили интегрируются в правила межсетевого экрана. При срабатывании сигнатур такого профиля будет произведено действие, настроенное в сигнатурах и произведена соответствующая запись в системных журналах.

UserGate DCFW поддерживает два 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: «активный-активный» и «активный-пассивный». Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другие.

UserGate DCFW 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). Система позволяет создавать профили оповещений, уведомляющие пользователей об определенных событиях по протоколам SMTP (email) и SMPP (SMS).

Благодаря интеграции с UserGate Management Center, поддерживается функция централизованного управления развернутыми системами DCFW. Администратор может выполнять мониторинг управляемых устройств, применять необходимые настройки, создавать политики, применяемые к группам устройств для обеспечения безопасности корпоративной сети.

Documentation: ☒

Product: DCFW

Version: 8.x

В UserGate DCFW реализован векторный межсетевой экран (VFW), использующий механизм VEGA (Vector Engine for Generic Access control) для высокоэффективного поиска правил доступа по множеству критериев.

Принцип работы векторного межсетевого экрана

Процесс определения разрешающего правила доступа в VFW разделен на две стадии:

1. Офлайн-стадия — подготовка поисковой матрицы на основании текущего набора правил доступа.
2. Онлайн-стадия — быстрый выбор подходящего правила доступа для входящего пакета с использованием предварительно вычисленной поисковой матрицы.

При создании или изменении правил доступа в системе (например, правил межсетевого экрана) специальный сервис VFW инициирует офлайн-стадию механизма VEGA. Рассчитанная поисковая матрица переносится в драйвер VFW для управления трафиком, работающий на уровне ядра операционной системы UGOS. Обновление поисковой матрицы в драйвере выполняется без дополнительных задержек и не влияет на производительность обработки трафика.

Во время онлайн-стадии поиск разрешающего правила выполняется по параметрам сетевого пакета, которые используются как координаты в рассчитанной поисковой матрице. Такой подход обеспечивает минимальное время поиска, практически не зависящее от общего количества правил.

Логически обработка сетевого трафика в VFW разделена на три фазы:

- Фаза 1 — прием входящих сетевых пакетов для транзитной передачи в сеть или для доставки локальным сервисам на самом DCFW.
- Фаза 2 — обработка пакетов, поступающих из локальных сервисов DCFW, для последующей передачи в сеть.
- Фаза 3 — завершающая обработка трафика, выполняемая перед его отправкой в сеть после внутренней маршрутизации.

Реализация VFW в версии DCFW 8.0 имеет следующие характеристики масштабируемости:

- Максимальное количество правил: 130 000 (суммарно для правил FW, NAT, PBR).
- Максимальное количество уникальных IPv4-адресов и подсетей, задействованных в правилах: 16 000 000.

Порядок обработки пакетов

Обобщенно порядок обработки пакетов в UserGate DCFW можно представить с помощью следующей логической диаграммы.

Пакеты, пришедшие на сетевой интерфейс UserGate DCFW, сначала обрабатываются правилами первичной фильтрации, предназначенными для защиты от IP-спуфинга. На этом этапе возможен немедленный сброс пакетов при срабатывании условий защиты.

На этапе VFW phase 1 выполняется фильтрация входящего трафика на основе сетевых параметров пакетов до уровня L4 — IP-адресов и портов источника и назначения, а также зоны входящего интерфейса. Поскольку маршрут дальнейшей передачи и исходящий интерфейс на этом этапе еще не определены, решения о блокировке или разрешении принимаются только для тех пакетов, для которых не требуется информация об исходящей зоне.

Ранняя проверка входящего трафика позволяет сразу отбрасывать нежелательные пакеты, которые могут быть однозначно идентифицированы межсетевым экраном, избегая их передачи в модуль маршрутизации и другие компоненты системы. Например, если правила межсетевого экрана запрещают трафик от определенного IP-адреса источника, такие пакеты оптимально блокировать на начальной стадии, снижая нагрузку на последующие модули обработки.

Если входящий пакет относится к трафику VPN-туннеля, выполняется его распаковка и дешифрация. В случае ошибки при дешифрации пакет немедленно отбрасывается.

При выполнении условий правил трансляции NAT (DNAT/PF), выполняется замена IP-адреса пакета или порта назначения.

Механизм управления соединениями проверяет, принадлежит ли пакет уже существующей сессии. Если пакет первый в потоке, создается новый контекст с ключевой информацией о сессии: адресах, портах, протоколах, интерфейсах. Если пакет принадлежит уже установленной сессии, обновляется ее состояние (таймеры, статистика, параметры протокола) и пакет передается далее по уже определенному пути обработки.

Пакет может быть отфильтрован на основе контекстных данных сессии, если ранее в этой сессии сработали сигнатуры COV или L7-идентификации, и в контексте сессии был установлен флаг принудительного сброса пакетов.

После завершения анализа пакета UserGate DCFW определяет, должен ли пакет быть обработан по стандартной таблице маршрутизации или же к нему следует применить правила PBR. Если соответствующие правила определены, маршрут будет выбираться согласно PBR.

На этапе маршрутизации выполняется сопоставление адреса назначения пакета с доступными маршрутами и выбирается дальнейший путь его обработки:

- передача локальным сервисам (например, для обновления компонентов системы, загрузки библиотек, доступа к веб-консоли и т. д.);
- направление во внешние интерфейсы для отправки в сеть (транзитный трафик).

На этапе маршрутизации пакет может быть отброшен в следующих случаях:

- в таблице маршрутизации отсутствует маршрут к сети назначения;
- к адресу назначения применен статический маршрут типа Blackhole или Unreachable.

Трафик, направленный локальным сервисам, передается соответствующим внутренним модулям UserGate DCFW.

Для транзитного трафика устанавливаются параметры пропускной способности в соответствии с заданными правилами Shaper.

При совпадении условий правил трансляции NAT (SNAT) выполняется замена исходящего IP-адреса или порта пакета.

Механизм управления соединениями обновляет записи сессии с учетом трансляции адресов правилами SNAT, таймеры и статистику соединения.

На этапе VFW phase 3 выполняется финальная проверка трафика на соответствие сетевым политикам. К этому моменту доступна полная информация о пакете, включая выбранный маршрут и исходящий интерфейс. Цель этого шага — подтвердить номер выбранного правила и определить необходимость выполнения дополнительных проверок для исходящего трафика и исходящей зоны.

После определения разрешающего правила доступа трафик при необходимости проходит дополнительную обработку с использованием контентных профилей, указанных в этом правиле:

- Пакеты анализируются с помощью сигнатур профилей безопасности COB и профилей приложений.
- При срабатывании сигнатур выполняются действия, предусмотренное соответствующим профилем.
- По результатам срабатывания обновляются флаги в контексте сессии.
- Если в профиле COB совпадений не обнаружено, трафик передается дальше без изменений.
- В профиле приложений также определяются действия для трафика, который не удалось идентифицировать.

При наличии соответствующих правил в модуле VPN encryption пакеты подвергаются инкапсуляции и шифрованию перед отправкой через VPN-туннель.

После завершения обработки пакеты передаются в исходящий интерфейс.

Трафик, генерируемый локальными сервисами UserGate DCFW, фильтруется правилами VFW phase 2, затем проверяется на соответствие правилам трансляции NAT (DNAT/PF) и далее обрабатывается по той же логической цепочке, что и транзитные пакеты.

Функция быстрой обработки сетевых пакетов FastPath

UserGate DCFW поддерживает функцию быстрой обработки сетевых пакетов FastPath: если сессия уже установлена и остальные пакеты сессии не требуют проверки и специальной обработки (например, дополнительного сканирования механизмами проверки COB/L7), то их можно сразу перенаправлять со входного интерфейса в выходной, выполнив необходимые соответствующие преобразования (трансляцию адресов, портов и т. д.).

Функция FastPath активирована по умолчанию. При записи трафика FastPath автоматически выключается.

Статус функции FastPath можно проверить в интерфейсе командной строки с помощью команды:

```
Admin@nodename# show settings fastpath
```

```
enabled    : on
```

Отключить функцию можно с помощью команды:

```
Admin@nodename# set settings fastpath enabled
```

```
+ on      Enable
```

```
+ off     Disable
```

