

Table of Contents

Table of Contents	1
Настройка сети	2
Настройка зон	3
Настройка интерфейсов	5
Настройка шлюзов	11
Виртуальные маршрутизаторы	13

Настройка зон

Product: WAF
Version: 7.x

Зона в WAF — это логическое объединение сетевых интерфейсов. Политики безопасности WAF используют зоны интерфейсов, а не непосредственно интерфейсы. Это дает необходимую гибкость политикам безопасности.

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 WAF поставляется со следующими зонами:

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

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

ПримечаниеМожно 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 WAF начинает отбрасывать пакеты и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления — 3000 запросов в секунду, для порога отбрасывания пакетов — 6000 запросов в секунду. Рекомендуется включать защиту от флуда на всех интерфейсах. Необходимо увеличить пороговое значение отбрасывания пакетов для протокола UDP, если через интерфейсы зоны 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.

Наименование	Описание
Шаг 3. Настроить параметры контроля доступа зоны (опционально).	Указать предоставляемые WAF 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 WAF. • SNMP — доступ к WAF по протоколу SNMP (UDP 161). • Консоль администрирования — доступ к веб-консоли управления (TCP 8001). • CLI по SSH — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • Reverse-прокси — сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. Более подробно смотрите раздел Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси. • SNMP-прокси — сервис используется для построения распределённой системы мониторинга (позволяет регулировать нагрузку и организовывать мониторинг распределённой сетевой инфраструктуры). • NTP сервис — разрешает доступ к сервису точного времени, запущенному на сервере WAF. • API XML RPC поверх HTTPS — разрешает доступ к API поверх HTTPS (TCP 4443). Доступен в версии 7.4.1 и выше. Подробнее о требованиях сетевой доступности читайте в приложении 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. С помощью флажка 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.
Шаг 5. Настроить параметры ограничения сессий (опционально).	Ограничение количества одновременных подключений с одного IP-адреса — это мера безопасности, которая ограничивает количество активных соединений сети, исходящих от одного и того же IP-адреса. Это делается по нескольким причинам: • Защита от атак: злоумышленники могут использовать большое количество одновременных подключений с одного IP-адреса для проведения DDoS-атак (распределенные атаки, целью которых является отказ системы в обслуживании). Ограничение количества подключений помогает снизить риск таких атак, уменьшая нагрузку на сеть или сервер. • Предотвращение злоупотреблений: некоторые пользователи могут пытаться злоупотреблять ресурсами, путем создания множества одновременных подключений. Ограничение подключений помогает предотвратить избыточное использование ресурсов и поддерживать равномерное распределение нагрузки. • Сохранение доступности: предотвращение ситуаций, когда один пользователь занимает все доступные ресурсы, оставляя мало места для других пользователей. Введение ограничений способствует поддержанию доступности ресурсов для всех пользователей. • Управление ресурсами: более эффективное управление сетевыми и серверными ресурсами, обеспечивая более стабильную и предсказуемую производительность. Для ограничения количества одновременных подключений с одного IP-адреса необходимо: 1. Поставить флажок Включить ограничение сессий на IP-адрес. 2. Указать максимально возможное количество сессий с одного адреса. 3. Добавить список IP-адресов, для которых данное ограничение не будет действовать. Подробнее о создании списка смотрите в разделе IP-адреса.

Настройка интерфейсов

Product: WAF
Version: 7.x

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, 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.
- Назначить Алиас/Псевдоним — дополнительное идентификационное наименование интерфейса. Параметр является опциональным и используется для работы с SNMP.
- Изменить физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
- Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:
 - VLAN.
 - Бонд.
 - Мост.
 - Loopback.

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, 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	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow .
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. Важно! Значение параметра не может содержать символы кириллицы.

Наименование	Описание
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии ПО 7.3.0 и выше).

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 WAF, 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 .
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. Важно! Значение параметра не может содержать символы кириллицы.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.

Наименование	Описание
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. • 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 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)	Задаёт 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 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.

Наименование	Описание
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. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии ПО 7.3.0 и выше).

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 данному сегменту, передает (транслирует) кадр дальше; если кадр принадлежит данному сегменту, мост ничего не делает.

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

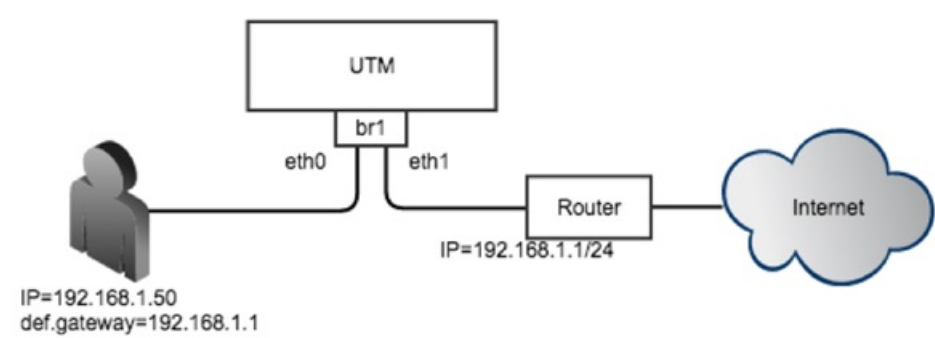


Рисунок 4 Использование моста

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

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.

Внимание! Функциональность 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 WAF.

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

- Электропитание ПАК WAF отключено.
- Система внутренней диагностики обнаружила проблему в работе ПО WAF. Тайм-аут срабатывания при обнаружении проблемы — 10 секунд.

Управление работой байпас-реле сетевых портов возможно через интерфейс PMC (подробнее читайте в статье [Команды управления платформой](#)).

Подробнее о сетевых интерфейсах, поддерживающих режим байпас, смотрите в руководствах по эксплуатации на модели [ПАК WAF](#).

С помощью кнопки **Добавить мост** администратор может объединить несколько физических интерфейсов в новый тип интерфейса — мост. Необходимо указать следующие параметры:

Наименование	Описание
--------------	----------

Наименование	Описание
Включено	Включает интерфейс мост.
Название	Название интерфейса.
Имя узла	Узел кластера WAF, 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 .
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. Важно! Значение параметра не может содержать символы кириллицы.
Интерфейсы моста	Два интерфейса, которые будут использованы для построения моста.
Интерфейсы байпас моста	Пара интерфейсов, которые можно использовать для построения байпас моста. Требуется поддержка оборудования ПАК WAF.
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. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии ПО 7.3.0 и выше).

Интерфейс loopback

Для создания loopback-интерфейса необходимо в разделе **Сеть → Интерфейсы** нажать кнопку **Добавить** и выбрать **Добавить loopback-интерфейс**. Далее необходимо задать следующие параметры:

Параметр	Описание
Включено	Включает интерфейс.
Название	Название интерфейса в виде loopbackN, где N — целое число.
Описание	Опциональное описание интерфейса.
Имя узла	Выбор узла кластера WAF, на котором создается интерфейс.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Layer 2.
Зона	Зона, к которой принадлежит интерфейс.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow .

Параметр	Описание
Профиль LLDP	Профиль LLDP для отправки данных по протоколу Link Layer Discovery Protocol (LLDP).
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. Важно! Значение параметра не может содержать символы кириллицы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно в версии ПО 7.3.0 и выше).

Настройка шлюзов

Product: WAF

Version: 7.x

Для подключения UserGate WAF к интернету необходимо указать IP-адрес шлюза. Если для подключения к интернету используется несколько провайдеров, необходимо указать несколько шлюзов. Если несколько узлов объединены в кластер конфигурации, настраивать шлюзы необходимо для каждого из узлов.

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

Добавление шлюза

Чтобы добавить шлюз:

1. В разделе **Настройки → Сеть → Шлюзы** нажмите **Добавить**.
2. В окне **Свойства шлюза** укажите его параметры: название, имя узла UserGate WAF, сетевой интерфейс (по умолчанию назначается автоматически), виртуальный маршрутизатор и IP-адрес шлюза.

ПримечаниеПодробнее о виртуальных маршрутизаторах — в разделе «[Виртуальные маршрутизаторы](#)».

3. Установите флажок **Включено** и сохраните изменения.

Настройка балансировки

Если для UserGate WAF настроены несколько шлюзов для подключения к интернету, вы можете распределять исходящий трафик между шлюзами и таким образом управлять нагрузкой на них. При балансировке трафик в интернет распределяется с учетом весов шлюзов: чем больше вес, тем большая доля трафика идет через шлюз.

Например, если для балансировки настроены два шлюза, сессии будут распределяться между ними по формуле $n1/w1 = n2/w2$, где:

- **n1, n2** — сессии, проходящие через шлюзы;
- **w1, w2** — веса шлюзов.

Чтобы настроить балансировку трафика между шлюзами:

1. В разделе **Настройки → Сеть → Шлюзы** выберите шлюз, который будут участвовать в балансировке, и нажмите **Редактировать**.
2. В окне **Свойства шлюза** укажите вес шлюза, установите флажок **Балансировка** и сохраните изменения.
3. Выполните настройку других шлюзов, участвующих в балансировке.

Исходящий трафик будет распределяться между шлюзами в соответствии с указанными весами.

Настройка проверки сети

В UserGate WAF предусмотрена проверка доступности шлюзов. По индикаторам на странице **Шлюзы** можно отслеживать, доступен ли шлюз (зеленый индикатор) или нет (красный индикатор). По умолчанию шлюз считается доступным, если UserGate WAF может получить его MAC-адрес с помощью ARP-запроса. Но доступность шлюза не означает наличие доступа в интернет. Чтобы проверить подключение шлюза к интернету, вы можете включить дополнительную проверку сети.

Проверка сети может быть полезна в следующих случаях:

- Если доступ к интернету предоставляют несколько провайдеров и добавлено несколько шлюзов, вы можете настроить отказоустойчивое соединение с интернетом. Для этого один из шлюзов назначается шлюзом по умолчанию. Если в результате проверки сети будет обнаружено, что доступ в интернет через шлюз по умолчанию отсутствует, трафик будет переведен на запасные шлюзы в порядке их расположения в веб-консоли (смена порядка сортировки в процессе текущей сессии не влияет на процесс выбора шлюза).
- Если настроен кластер отказоустойчивости, проверку сети можно использовать для диагностики узлов кластера. Подробнее об этом — в разделе «[Диагностика узлов кластера отказоустойчивости](#)».

В процессе проверки сети UserGate WAF с заданной периодичностью отправляет по пять ICMP-запросов на каждый указанный IP-адрес доступа в интернет. Доступность шлюза в этом случае определяется по порогу неудачных ICMP-запросов. Проверка считается успешной, если общее количество неудачных ICMP-запросов, отправленных на все указанные IP-адреса в рамках заданного интервала, не превышает этот порог.

Чем ниже порог, тем строже критерий доступности. Например:

- При пороге в 10% шлюз недоступен, если не прошел хотя бы один запрос.
- При 100% шлюз недоступен, только если не прошли все запросы.

Чтобы настроить проверку сети:

1. В разделе **Настройки → Сеть → Шлюзы** нажмите **Проверка сети**.
2. В окне **Свойства проверки сети** установите флажок **Включено**.
3. Нажмите кнопку **Добавить** и укажите IP-адреса для проверки доступа в интернет.

Примечание По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8).

4. В поле **Частота проверки** укажите в секундах, с какой периодичностью UserGate WAF будет отправлять ICMP-запросы на указанные IP-адреса.
5. В поле **Процент неудачных запросов** задайте порог неудачных ICMP-запросов и сохраните изменения.

Индикаторы доступности шлюзов теперь будут отражать результаты проверки сети.

Виртуальные маршрутизаторы

Product: WAF
Version: 7.x

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.

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:
 - DNS.
 - Авторизация.
 - Любой сетевой трафик, генерируемый самим устройством — проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS сообщений, SNMP трапов и т.п.
- 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 WAF. 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.

Примечание! При создании виртуального маршрутизатора его имя не должно содержать заглавных букв, и должно иметь длину не менее трех символов.

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, 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 .

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.

Наименование	Описание
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.	Возможно 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 WAF.
Шаг 6. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , то WAF сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 7. Указать метрику.	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько.

