

Table of Contents

Table of Contents	1
Настройка сети	2
Настройка зон	3
Настройка интерфейсов	5
Настройка шлюзов	12
Настройка DHCP	13
Настройка DNS	14
Виртуальные маршрутизаторы	16
WCCP	27

Настройка зон

Documentation: ☒
Version: 6.1.9, 5.x

Зона в UserGate - это логическое объединение сетевых интерфейсов. Политики безопасности UserGate используют зоны интерфейсов, а не непосредственно интерфейсы. Это дает необходимую гибкость политикам безопасности, а также существенно упрощает управление отказоустойчивым кластером. Зоны одинаковы на всех узлах кластера, то есть данная настройка является глобальной для кластера.

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 UserGate поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление UserGate.
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.
Cluster	Зона для интерфейсов, используемых для работы кластера.
VPN for Site-to-Site	Зона, в которую помещаются все клиенты типа Офис-Офис, подключаемые к UserGate по VPN.
VPN for remote access	Зона, в которую помещаются все мобильные пользователи, подключаемые к UserGate по VPN.

Администраторы UserGate 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 UserGate начинает отбрасывать пакеты и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 запросов в секунду. Рекомендуется включать защиту от флуда на всех интерфейсах, за исключением интерфейсов зоны Cluster. 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. Важно! UserGate позволяют произвести более гранулированную защиту от DoS атак. Для получения дополнительной информации обратитесь в раздел Защита от DoS атак. Внимание! Зоны и правила защиты от DoS атак работают по разному, это две независимые системы: Первыми срабатывают зоны. Они обрабатывают входящий и исходящий трафик. Правила защиты от DoS атак распространяются только на транзитный трафик. Таким образом, если идёт атака на ваш внешний IP, то надо использовать защиту на зоне. Здесь сразу отсекается паразитный трафик.

Наименование	Описание
Шаг 3. Настроить параметры контроля доступа зоны (опционально).	Указать предоставляемые UserGate 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 UserGate. • SNMP - доступ к UserGate по протоколу SNMP (UDP 161). • Captive-портал и страница блокировки - необходимы для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • XML-RPC для управления - позволяет управлять продуктом по API (TCP 4040). • Кластер - сервис, необходимый для объединения нескольких узлов UserGate в кластер (TCP 4369, TCP 9000-9100). • VRRP - сервис, необходимый для объединения нескольких узлов UserGate в отказоустойчивый кластер (IP протокол 112). • Консоль администрирования - доступ к веб-консоли управления (TCP 8001). • DNS - доступ к сервису DNS-прокси (TCP 53, UDP 53). • HTTP(S)-прокси - доступ к сервису HTTP(S)-прокси (TCP 8090). • Агент авторизации - доступ к серверу, необходимый для работы агентов авторизации Windows и терминальных серверов (UDP 1813). • SMTP(S)-прокси - сервис фильтрации SMTP-трафика от спама. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел Защита почтового трафика. • POP3(S)-прокси - сервис фильтрации POP3-трафика от спама. Необходим только при публикации почтового сервера в интернет. Более подробно смотрите раздел Защита почтового трафика. • CLI по SSH - доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • VPN - доступ к серверу для подключения к нему клиентов L2TP VPN (UDP 500, 4500). • SCADA - сервис фильтрации АСУ ТП-трафика. Необходим только при контроле АСУ ТП-трафика. Более подробно смотрите раздел Правила АСУ ТП. • Reverse-прокси - сервис, необходимый для публикации внутренних ресурсов с помощью Reverse-прокси. Более подробно смотрите раздел Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси. • Web-портал - сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. Более подробно смотрите раздел Веб-портал. • Log Analyzer - сервис для подключения к анализатору журналов Log Analyzer (TCP 2023 и 9713). • OSPF - сервис динамической маршрутизации OSPF. Более подробно смотрите раздел OSPF. • BGP - сервис динамической маршрутизации BGP. Более подробно смотрите раздел BGP. • NTP service - разрешает доступ к сервису точного времени, запущенному на сервере UserGate. Подробнее о требованиях сетевой доступности читайте в Приложение 1. 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 чекбокса 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.

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, контентной фильтрации и других правилах, 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.
- Изменить физические параметры интерфейса — MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
- Настроить работу DHCP-ретранслятора на выбранном интерфейсе. Для этого необходимо включить DHCP-ретранслятор, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция ретранслятора, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.
- Мост.
- PPPoE.
- VPN.
- Tunnel.

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, контентной фильтрации и других правилах, 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 .

Наименование	Описание
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.
DHCP-ретранслятор	Настройка работы DHCP-ретранслятора на VLAN-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

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 UserGate, 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 .
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
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.

Наименование	Описание
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.
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.
DHCP-ретранслятор	Настройка работы DHCP-ретранслятора на бонд-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

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 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 UserGate в качестве решения, обеспечивающего контентную фильтрацию на уровне L2, выглядит следующим образом:

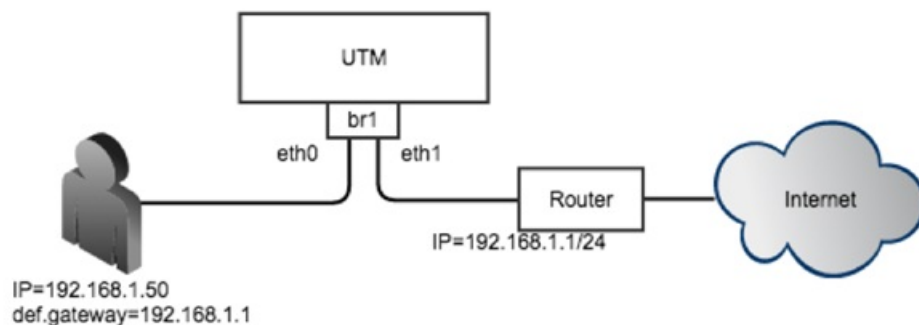


Рисунок 4 Использование моста

Примечание Для работы виртуальной машины VMWare в данном режиме, необходимо в настройках групп портов, подключенных к мосту, перевести параметры безопасности *Promiscuous mode*, *MAC address changes*, *Forged transmits* в режим *Accept*.

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

Примечание Одновременное использование мостов L2 и L3 на устройствах UserGate невозможно — это ограничения архитектуры.

В режиме 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. В этом случае невозможно использовать правила АСУ ТП, правила защиты почтового трафика и аутентификацию пользователей через captive-портал. Контентная фильтрация работает в этом режиме.

Примечание Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают.

В режиме 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 UserGate NGFW.

Если мост создается в ПАК UserGate, 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 NGFW) в случаях если:

- Электропитание ПАК UserGate отключено.
- Система внутренней диагностики обнаружила проблему в работе ПО UserGate.

Более подробно о сетевых интерфейсах, поддерживающих режим байпас смотрите в спецификации на оборудование ПАК UserGate.

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

Наименование	Описание
Включено	Включает интерфейс мост.
Название	Название интерфейса.
Имя узла	Узел кластера UserGate, 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 .
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 UserGate.
STP (Spanning Tree Protocol)	Включает использование STP для защиты сети от петель.

Наименование	Описание
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.
DHCP-ретранслятор	Настройка работы DHCP-ретранслятора на bridge-интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле Адрес UserGate IP-адрес интерфейса, на котором добавляется функция ретранслятора, и указать один или несколько серверов DHCP, куда необходимо пересылать DHCP-запросы клиентов.

Интерфейс PPPOE

PPPoE (Point-to-point protocol over Ethernet) — сетевой протокол канального уровня передачи кадров PPP через Ethernet. С помощью кнопки **Добавить**, выбрав **Добавить PPPoE**, администратор может создать PPPoE интерфейс. При создании необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает интерфейс PPPoE.
Имя узла	Узел кластера UserGate, на котором создать интерфейс PPPoE.
Интерфейс	Указать интерфейс, на котором будет создаваться интерфейс PPPoE.
Зона	Зона, к которой принадлежит интерфейс PPPoE.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow .
MTU	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet.
Логин	Имя пользователя для соединения PPPoE.
Пароль	Пароль пользователя для соединения PPPoE.
Переподключаться автоматически	Включает переподключение соединения при обрыве связи.
Тип аутентификации	Протоколы аутентификации, использующиеся в протоколе PPP: • CHAP — Challenge Handshake Authentication Protocol — протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нем. • PAP — Password Authentication Protocol — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удаленного доступа открытым текстом (без шифрования).
Интервал между попытками подключения (сек.)	Интервал времени в секундах после разрыва соединения перед повторным запуском.
Маршрут по умолчанию	Устанавливает интерфейс PPPoE в качестве маршрута по умолчанию.
Интервал проверки соединения (сек.)	Интервал проверки соединения.

Наименование	Описание
Количество неуспешных проверок	Количество неуспешных проверок соединения, после которого UserGate считает, что соединение отсутствует и разрывает его.
Использовать DNS-сервер провайдера	Если опция включена, то UserGate использует DNS-серверы, выданные провайдером.
Количество попыток подключения	Количество неуспешных попыток подключения, после которых попытки автосоединения будут прекращены.
PPPoE сервис	Имя сервиса необходимо прописывать в случае предоставления провайдером. Если имя сервиса не используется, поле необходимо оставить пустым.

Интерфейс VPN

VPN-интерфейс — это виртуальный сетевой адаптер, который будет использоваться для подключения клиентов VPN. Данный тип интерфейса является кластерным, это означает, что он будет автоматически создаваться на всех узлах UserGate, входящих в кластер конфигурации. При наличии кластера отказоустойчивости клиенты VPN будут автоматически переключаться на запасной сервер в случае обнаружения проблем с активным сервером без разрыва существующих VPN-соединений.

Внимание! Редактирование кластерного интерфейса возможно только для узла кластера cluster(даже если кластер не собран и узел всего один).

В разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить VPN**. Задайте следующие параметры:

Наименование	Описание
Название	Название интерфейса, должно быть в виде tunnelN, где N — это порядковый номер VPN-интерфейса.
Описание	Описание интерфейса.
Зона	Зона, к которой будет относиться данный интерфейс. Все клиенты, подключившиеся по VPN к серверу UserGate, будут также помещены в эту зону.
Профиль Netflow	Профиль Netflow, используемый для данного интерфейса. Не обязательный параметр.
Профиль Netflow	Профиль Netflow для отправки статистических данных на Netflow коллектор. О профилях Netflow можно прочитать в главе Профили Netflow .
Режим	Тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Если интерфейс предполагается использовать для приема VPN-подключений (Site-2-Site VPN или Remote access VPN, то необходимо использовать статический IP-адрес. Для использования интерфейса, используемого в роли клиента, необходимо выбрать Динамический режим.
MTU	Размер MTU для выбранного интерфейса.

По умолчанию в системе уже созданы 3 VPN-интерфейса:

- **tunnel1**, который рекомендовано использовать для Remote access VPN.
- **tunnel2**, который рекомендовано использовать для серверной части Site-to-Site VPN.
- **tunnel3**, который рекомендовано использовать для клиентской части Site-to-Site VPN.

Интерфейс туннель

Интерфейс туннель — это виртуальный сетевой адаптер, который может использоваться для создания соединения точка-точка через IP-сеть. Поддерживаются следующие типы туннельных интерфейсов:

- GRE — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня в IP-пакеты. Номер протокола в IP — 47.
- IPIP — это протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет. Инкапсуляция одного IP пакета в

другой IP пакет, это добавление внешнего заголовка с Source IP — точкой входа в туннель, и Destination IP — точкой выхода из туннеля.

- VXLAN — это протокол туннелирования Layer 2 Ethernet кадров в UDP-пакеты, порт 4789.

Для создания туннельного интерфейса в разделе **Сеть → Интерфейсы** нажмите кнопку **Добавить** и выберите **Добавить туннель**. Задайте следующие параметры:

Наименование	Описание
Включено	Включение или выключение данного интерфейса.
Название	Название интерфейса, должно быть в виде greN, где N — это порядковый номер туннельного интерфейса.
Описание	Описание интерфейса.
Зона	Зона, к которой будет относиться данный интерфейс.
Режим	Режим работы туннеля — GRE, IPIP, VXLAN.
MTU	Размер MTU для выбранного интерфейса.
Локальный IP	Локальный адрес point-to-point интерфейса.
Удаленный IP	Удаленный адрес point-to-point интерфейса.
IP интерфейса	IP-адрес, назначенный туннельному интерфейсу.
VXLAN ID	Идентификатор VXLAN. Только для типа туннеля VXLAN.

Настройка Netflow

Netflow — сетевой протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Анализатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчеты (часто в виде графиков).

Сервер UserGate может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс UserGate, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль Netflow.	В разделе Библиотеки → Профили Netflow нажать на кнопку Добавить и создать профиль Netflow. Подробнее о профиле Netflow смотрите раздел Профили Netflow .
Шаг 2. Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо собирать статистику.	В разделе Сеть → Интерфейсы в настройках конкретного сетевого интерфейса указать созданный профиль Netflow.

Настройка шлюзов

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: ☒

Для подключения NGFW к интернету необходимо указать IP-адрес одного или нескольких шлюзов. Если для подключения к интернету используется несколько провайдеров, то необходимо указать несколько шлюзов. Настройка шлюза уникальна для каждого из узлов кластера.

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

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок Балансировка и указать Вес каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз). При распределении трафика между шлюзами с разными весами происходит: - Вычисление хэша от адресов источника и назначения. - Выбор шлюза Трафик распределяется с учётом весов. Пусть настроены 2 шлюза: n1, n2 — сессии, проходящие через шлюзы. w1, w2 — веса шлюзов. Тогда сессии между шлюзами будут распределяться согласно $n1/w1 = n2/w2$.
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить Проверку сети, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет (с помощью ping) с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли (в случае если в текущей сессии не менялся порядок сортировки отображаемых шлюзов, смена порядка сортировки не влияет на процесс выбора шлюза). По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

Состояние шлюза (доступен — зеленый, не доступен — красный) определяется следующим образом:

Наименование	Описание
Проверка сети отключена	Шлюз считается доступным, если NGFW может получить его MAC-адрес с помощью ARP-запроса. Проверка наличия доступа в интернет через этот шлюз не производится. Если MAC-адрес шлюза не может быть определен, шлюз считается недоступным.
Проверка сети включена	Шлюз считается доступным, если: - NGFW может получить его MAC-адрес с помощью ARP-запроса. - Проверка наличия доступа в интернет через этот шлюз завершилась успешно. В противном случае шлюз считается недоступным.

Настройка DHCP

Version: 6.1.9, 5.x
Documentation: ☒

Служба DHCP (Dynamic Host Configuration Protocol) позволяет автоматизировать процесс выдачи сетевых настроек клиентам в локальной сети. В сети с DHCP-сервером каждому сетевому устройству можно динамически назначать IP-адрес, адрес шлюза, DNS.

UserGate может также выступать в качестве DHCP-релея, обеспечивая передачу DHCP-запросов от клиентов, находящихся в различных сетях, на центральный DHCP-сервер. Более подробно о настройке DHCP-релея можно посмотреть в разделе [Настройка интерфейсов](#).

В UserGate можно создать несколько диапазонов адресов для выдачи по DHCP. DHCP работает на каждом узле отказоустойчивого кластера независимо. Для обеспечения отказоустойчивости сервиса DHCP в кластере необходимо настроить DHCP на обоих узлах, указав непересекающиеся диапазоны IP-адресов.

Для создания диапазона DHCP необходимо нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного диапазона DHCP.
Узел	Узел кластера, на котором создается данный диапазон.
Интерфейс	Интерфейс сервера, на котором будут раздаваться IP-адреса из создаваемого диапазона.
Диапазон IP	Диапазон IP-адресов, выдаваемый клиентам DHCP.
Маска	Маска подсети, выдаваемая клиентам DHCP.
Время аренды	Время в секундах, на которое выдаются IP-адреса.
Домен	Название домена, выдаваемое клиентам DHCP.
Шлюз	IP-адрес шлюза, выдаваемый клиентам DHCP.
Серверы имен	IP-адрес DNS-серверов, выдаваемых клиентам DHCP.
Зарезервированные адреса	MAC-адреса и сопоставленные с ними IP-адреса.
Игнорируемые MAC	Список MAC-адресов, игнорируемых DHCP-сервером.
DHCP PXE boot	Адрес сервера и имя загрузочного файла, передаваемого на запрос PXE boot.
DHCP опции	Номер опции и ее значение (список опций доступен в Приложение 5. Опции DHCP).

Выданные IP-адреса отображаются в панели **Арендованные адреса**. Администратор может освободить любой выданный адрес, выделив адрес и нажав на кнопку **Освободить**.

Примечание Чтобы выдача адресов по DHCP работала на интерфейсе, который находится в зоне с включенной защитой от IP-спуфинга, необходимо в свойствах зоны во вкладке Защита от IP-спуфинга указать диапазоны выдаваемых IP-адресов, а также адрес 0.0.0.0.

Примечание Если в настройках DHCP не указывать DNS сервера, то NGFW будет отдавать в качестве DNS сервера адрес, совпадающий с адресом шлюза

Настройка DNS

Documentation: ☒
Version: 6.1.9, 7.0.1
Product: NGFW

В разделе **Настройки → Сеть → DNS** вы можете управлять списком системных DNS-серверов UserGate NGFW, а также настроить его работу в качестве DNS-прокси для других сетевых устройств.

Настройка системных DNS-серверов

Системные DNS-серверы необходимы для разрешения доменных имен в IP-адреса. В блоке параметров **Системные DNS-серверы** вы можете добавлять, редактировать или удалять DNS-серверы, которые использует UserGate NGFW.

Настройка сервиса DNS-прокси

Сервис DNS-прокси предназначен для обработки DNS-запросов пользователей и позволяет изменять их в соответствии с заданными правилами. Сервис поддерживает два режима работы:

- явный режим — клиенты отправляют DNS-запросы непосредственно на DNS-прокси;
- режим перехвата — DNS-прокси автоматически перехватывает транзитные DNS-запросы.

Важно!Для корректной работы DNS-прокси необходимо разрешить доступ к сервису «DNS» в параметрах контроля доступа соответствующей зоны.

Для использования сервиса DNS-прокси в режиме перехвата:

В разделе **Настройки → Сеть → DNS** в блоке **Настройка DNS-прокси** укажите значения следующих параметров.

Параметр	Описание
DNS-фильтрация	Включение или отключение фильтрации DNS-запросов. При включении функции UserGate NGFW перехватывает DNS-запросы пользователей и отправляет их от своего имени. Если запрашиваемый домен попадает под действие запрещающего правила контентной фильтрации, запрос блокируется. Для использования DNS-фильтрации требуется лицензия на модуль ATP. Важно! Функциональность DNS-фильтрации и мост L2 в текущей версии несовместимы — при включении DNS-фильтрации DNS-запросы через мост проходить перестают. Важно! Правила контентной фильтрации, использующие список IP-адресов на вкладке «Назначение» → «Адрес доставки», не обрабатываются модулем DNS-фильтрации. Обработка таких правил выполняется средствами модуля контентной фильтрации.
Кэширование DNS	Включение или отключение кэширования ответов DNS. Функция позволяет сохранять полученные DNS-ответы и использовать их при повторных запросах. Рекомендуется оставить функцию включенной, так как это уменьшает время обработки запросов и повышает скорость доступа пользователей к ресурсам
Лимит DNS-запросов в секунду на пользователя	Максимальное количество DNS-запросов, которое один пользователь может отправить за секунду. Запросы, превышающие установленный лимит, отбрасываются. Значение по умолчанию — 100 запросов в секунду. Не рекомендуется существенно увеличивать значение параметра, поскольку это может снизить эффективность защиты от DNS-флуда и других атак, направленных на отказ в обслуживании DNS-сервиса
Максимальное время жизни для DNS-записей (сек)	Максимальный период, в течение которого DNS-записи могут храниться в кэш-памяти DNS-прокси. По истечении этого времени запись считается устаревшей и должна быть обновлена посредством нового DNS-запроса
Рекурсивные DNS-запросы	Включение или отключение возможности выполнения рекурсивных DNS-запросов. Если опция включена, DNS-прокси самостоятельно запрашивает DNS-серверы для полного разрешения доменного имени. Рекомендуется оставить функцию включенной для обеспечения корректной обработки DNS-запросов
Тайм-аут (мсек)	Максимальное время ожидания ответа от DNS-сервера на один запрос. Если ответ не поступил до истечения указанного времени, запрос считается неудачным
Только А и AAAA DNS-записи для неизвестных пользователей (защита от VPN поперх DNS)	При включении параметра для пользователей, не прошедших аутентификацию, разрешаются только DNS-запросы типов А и AAAA. Запросы остальных типов отклоняются. Этот параметр позволяет ограничивать возможности DNS-туннелирования для предотвращения создания каналов передачи данных через DNS-протокол

Параметр	Описание
Число попыток	Максимальное количество повторных запросов, которые DNS-прокси может выполнить при отсутствии ответа от DNS-сервера. Если ответ не будет получен после указанного числа попыток, запрос завершится ошибкой

С помощью правил DNS-прокси можно настроить обработку запросов для отдельных доменов на определенных DNS-серверах. Такой механизм удобно использовать для разрешения внутренних доменных имен компании, например доменов Active Directory, которые не публикуются в интернете и доступны только во внутренней сети.

Для создания правила DNS-прокси:

1. В разделе **Настройки → Сеть → DNS** в блоке **DNS-прокси → Правила DNS** нажмите **Добавить**.
2. Укажите необходимые параметры:
 - На вкладке **Общие** укажите название, описание правила и его место в списке правил DNS.
 - На вкладке **Домены** укажите список доменов. Допускается использование символа «*» для указания шаблона доменов.
 - На вкладке **Серверы DNS** укажите IP-адреса DNS-серверов, на которые необходимо пересылать запросы для указанных доменов.

Вы также можете вручную задавать статические записи типа host (A-записи), которые будут использоваться сервисом DNS-прокси для фиксированного сопоставления доменных имен и IP-адресов.

Для создания статической записи:

1. В разделе **Настройки → Сеть → DNS** в блоке **DNS-прокси → Статические записи** нажмите **Добавить**.
2. Укажите необходимые параметры:
 - название и описание правила;
 - доменное имя (FQDN) статической записи (например, www.example.com);
 - список IP-адресов, которые UserGate NGFW будет возвращать при запросе указанного доменного имени.

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. Таблица маршрутизации виртуального роутера может содержать запись о маршрутах, заданных статически или полученных с помощью протоколов динамической маршрутизации — BGP, OSPF, RIP.

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:

- WCCP.
- ICAP.
- DNS.
- Авторизация.
- [Балансировка нагрузки](#).
- Любой сетевой трафик, генерируемый самим устройством — проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS сообщений, SNMP тралов и т.п.
- Действие правил NAT, DNAT, Port forwarding распространяются на все виртуальные маршрутизаторы.
- 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 NGFW. 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, VPN 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 .
Шаг 4. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации OSPF (опционально).	Настройте протокол OSPF для построения динамической карты маршрутов. Более подробно смотрите раздел руководства OSPF .

Наименование	Описание
Шаг 5. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации BGP (опционально).	Настройте протокол BGP для построения динамической карты маршрутов. Более подробно смотрите раздел руководства BGP .
Шаг 6. Добавить динамические маршруты, получаемые с помощью протокола маршрутизации RIP (опционально).	Настройте протокол RIP для построения динамической карты маршрутов. Более подробно смотрите раздел руководства RIP .
Шаг 7. Настроить мультикастинг (опционально).	Настройте параметры мультикастинга в данном виртуальном маршрутизаторе. Более подробно смотрите раздел руководства Мультикастинг .

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.
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 NGFW.
Шаг 6. Указать интерфейс.	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , то NGFW 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.

Протоколы динамической маршрутизации

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации

в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов.

Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически.

ПримечаниеЕсли в системе настроены статические шлюзы, то маршруты по умолчанию, полученные от протоколов динамической маршрутизации, игнорируются.

NGFW поддерживает работу трех протоколов маршрутизации — OSPF, BGP, RIP.

Внимание!Перед настройкой и использованием протоколов динамической маршрутизации необходимо задать соответствующие разрешения на вкладках Контроль доступа нужных зон.

OSPF

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации — вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол OSPF.

OSPF ([Open Shortest Path First](#)) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы (АС). Подробно о работе протокола OSPF читайте в соответствующей технической документации.

ПримечаниеПри работе протокола OSPF в кластере отказоустойчивости в режиме Active-Passive, узел, который обладает ролью Slave, автоматически назначает стоимость для всех своих интерфейсов и для списков редистрибуции в 2 раза выше, чем установленная на узле стоимость. Тем самым обеспечивается приоритет Master-узла в маршрутизации трафика.

Для настройки OSPF в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить OSPF-роутер.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню OSPF и настройте OSPF-роутер.

При настройке OSPF-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает использование данного OSPF-роутера.
Идентификатор роутера	IP-адрес роутера. Должен быть уникальным и задан в формате IPv4 (для удобства может совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору).
Redistribute	Распространять другим OSPF-роутерам маршруты в непосредственно подключенные к NGFW сети (connected) или статические маршруты, добавленные администратором для данного виртуального маршрутизатора (kernel).
Метрика	Установить метрику распространяемым маршрутам. Для задания метрики по-умолчанию укажите в этом поле значение 0. Метрика по-умолчанию для Мастер ноды кластера равна 20. Метрика по-умолчанию для запасной ноды равна 40.
Default originate	Оповещать другие роутеры о том, что данный роутер имеет маршрут по умолчанию.

При настройке интерфейсов OSPF укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного интерфейса.

Наименование	Описание
Интерфейс	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в данный виртуальный маршрутизатор.
Стоимость	Стоимость канала данного интерфейса. Данное значение передается в LSA (объявления о состоянии канала, link-state advertisement) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию 1.
Приоритет	Целое число от 0 до 255. Чем больше значение, тем выше шанс у маршрутизатора стать назначенным маршрутизатором (designated router) в сети для рассылки LSA. Значение 0 делает назначение для данного маршрутизатора невозможным. Значение по умолчанию 1.
Интервал hello	Время в секундах, через которое маршрутизатор посылает hello-пакеты. Это время должно быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию 10 секунд.
Интервал dead	Интервал времени в секундах, по истечении которого соседний маршрутизатор считается неработающим. Время исчисляется от момента приема последнего пакета hello от соседнего маршрутизатора. Значение по умолчанию 40 секунд.
Интервал повторения	Устанавливает временный интервал перед повторной отсылкой пакета LSA. Значение по умолчанию 5 секунд.
Задержка передачи	Устанавливает примерное время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию 1 секунда.
Аутентификация Вкл	Включает требование аутентификации каждого принимаемого роутером OSPF-сообщения. Аутентификация обычно используется для предотвращения инъекции фальшивого маршрута от нелегитимных маршрутизаторов.
Тип авторизации	Может быть: • Plain — передача ключа в открытом виде для аутентификации роутеров. Необходимо указать значение поля Ключ. • Digest — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Необходимо указать Ключ и MD5 key ID. Эти параметры должны быть идентичными на всех роутерах для нормальной работы. Значение параметра Ключ может содержать только буквы латинского алфавита, цифры и символ подчёркивания. Максимальное количество символов — 16.

При настройке области OSPF укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данной области.
Имя	Имя для данной области.
Стоимость	Стоимость LSA, анонсируемых в stub-области.
Идентификатор области	Идентификатор зоны (area ID). Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса . Идентификатор области должен совпадать для установления соседства OSPF.
Тип авторизации	Может быть: • Нет — не требовать авторизацию OSPF-пакетов. • Plain — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. • Digest — использование MD5-хеша для ключа для аутентификации OSPF-пакетов. Используется ключ, заданный в настройках интерфейсов. Идентификация на уровне интерфейсов имеет приоритет над авторизацией на уровне зоны.

Наименование	Описание
Тип области	Определяет тип области. Поддерживаются следующие типы областей: • Нормальная — обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты. • Тупиковая (Stub) — тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. • NSSA — Not-so-stubby. Зона NSSA определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться пограничный маршрутизатор (ASBR).
Не суммировать	Запрещает инъекцию суммированных маршрутов в тупиковые типы областей.
Интерфейсы	Выбор интерфейсов OSPF, на которых будет доступна данная зона.
Виртуальные линки	Специальное соединение, которое позволяет соединять, например, разорванную на части зону или присоединить зону к магистральной через другую зону. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение или как backup на случай выхода из строя основных соединений. Можно указать идентификаторы маршрутизаторов, которые доступны через данную зону.

ПримечаниеUserGate NGFW использует следующие типы сети:

- point-to-point — для интерфейсов GRE;
- point-to-multipoint — для интерфейсов VPN;
- broadcast — для физических интерфейсов, бондов и VLAN.

BGP

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол BGP.

BGP ([Border Gateway Protocol](#)) — динамический протокол маршрутизации, относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP — External Gateway Protocol). На текущий момент является основным [протоколом](#) динамической [маршрутизации](#) в [интернете](#). Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (АС), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протоколы внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие АС. Передаваемая информация включает в себя список АС, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети. Подробно о работе протокола BGP читайте в соответствующей технической документации.

Для настройки BGP в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить BGP-роутер.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню BGP и настройте BGP-роутер.
Шаг 3. Задать фильтры и Routemap (опционально) для ограничения количества получаемых маршрутов.	В разделе Фильтры нажать на кнопку Добавить и настроить параметры Routemap/фильтров. Добавить столько Routemap/фильтров, сколько необходимо для работы BGP в вашей организации.

Наименование	Описание
Шаг 4. Добавить хотя бы одного BGP-соседа (пира).	В разделе BGP-соседи нажать на кнопку Добавить и настроить параметры маршрутизатора, относящегося к соседней АС. Добавить столько соседей, сколько необходимо. Важно! Согласно требованиям RFC-8212 для каждого соседа необходимо обязательно указать входящие и исходящие фильтры. Без входящих фильтров роутер не будет принимать маршруты с данного соседа, при отсутствии исходящих фильтров роутер не будет анонсировать маршруты на данного соседа. Если интерфейсу NGFW, с которого устанавливается подключение к соседу, назначено несколько IP-адресов, то при настройке BGP-соседа, в случае отсутствия правила NAT, принудительно устанавливающего адрес источника для BGP-сессии с этим соседом, в качестве адреса NGFW необходимо указывать основной (primary) IP-адрес, т.е. адрес, который стоит первым в списке в настройках интерфейса.

При настройке BGP-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного BGP-роутера.
Идентификатор роутера	IP-адрес роутера. Должен совпадать с одним из IP-адресов, назначенным сетевым интерфейсам NGFW, относящимся к данному виртуальному маршрутизатору.
Номер автономной системы (АС)	Автономная система — это система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы задает принадлежность роутера к этой системе.
Redistribute	Позволяет распространять другим BGP-маршрутизаторам маршруты в непосредственно подключенные к NGFW-сети (connected), статические маршруты, добавленные администратором для данного виртуального маршрутизатора (kernel), или маршруты, полученные по протоколу OSPF.
Multiple path	Включает балансировку трафика на маршруты с одинаковой стоимостью.
Сети	Список сетей, относящихся к данной АС.

Для добавления BGP-соседей нажмите кнопку **Добавить** и укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного соседа.
Host	IP-адрес соседа.
Описание	Произвольное описание соседа.
Удаленная ASN	Номер автономной системы, к которой относится сосед.
Вес	Вес данных маршрутов, получаемых от данного соседа.
TTL	Максимальное количество хопов, разрешенное до этого соседа.
Allowas-in	По-умолчанию BGP маршрутизатор отбрасывает маршрут если видит в AS path собственный номер автономной системы. Эта директива позволяет маршрутизатору нарушить данное правило. Номер — указывает количество раз, которое может встречаться в AS Path номер AS BGP-соседа. Возможны значения от 0 до 10 (0 — origin).
Анонсировать себя в качестве следующего перехода (next-hop-self) для BGP	Заменять значение next-hop-self на собственный IP-адрес, если сосед является BGP.

Наименование	Описание
Multihop для eBGP	Указывает, что до этого соседа не прямое соединение (более одного хопа).
Route reflector client	Указывает, является ли этот сосед клиентом Route reflector.
Soft reconfiguration	Использовать soft reconfiguration (без разрыва соединений) для обновления конфигурации.
Default originate	Анонсировать этому соседу маршрут по умолчанию.
Аутентификация	Включает аутентификацию для данного соседа и задает пароль для аутентификации.
Фильтры BGP-соседей	Ограничивает информацию о маршрутах, получаемых от соседей или анонсируемых к ним.
Routemaps	Routemaps используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами.

Routemap позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов. Для создания routemap необходимо указать следующие параметры:

Внимание! Для анонсирования маршрутов они должны присутствовать в таблице маршрутизации!

Наименование	Описание
Название	Имя для данного routemap.
Действие	Устанавливает действие для данного routemap, может принимать значения: • Разрешить — разрешает прохождение данных, попадающих под условия routemap. • Запретить — запрещает прохождение данных, попадающих под условия routemap.
Сравнивать по	Условия применения routemap, может принимать значения: • IP. Если выбрано данное условие, то в закладке IP-адреса надо добавить все необходимые IP-адреса для данного условия. • AS путь. Если выбрано данное условие, то в закладке AS-путь надо добавить все необходимые номера автономных сетей для данного условия. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания (<u> </u>), который интерпретируется как: • Пробел. • Запятая. • Начало строки. • Конец строки. • AS set delimiter { and }. • AS confederation delimiter (and). • Community. Если выбрано данное условие, то в закладке Community надо добавить строки всех необходимых BGP community для данного условия.
Установить next hop	Установить для отфильтрованных маршрутов значение next hop в указанный IP-адрес.
Установить вес	Установить для отфильтрованных маршрутов вес в указанное значение.
Установить метрику	Установить для отфильтрованных маршрутов метрику в указанное значение.

Наименование	Описание
Установить предпочтение	Установить для отфильтрованных маршрутов предпочтение в указанное значение.
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для данного маршрута.
Community	Установить значение для BGP community для отфильтрованных маршрутов.

Фильтр позволяет фильтровать маршруты при перераспределении. При создании фильтров необходимо указать следующие параметры:

Наименование	Описание
Название	Имя для данного фильтра.
Действие	Устанавливает действие для данного фильтра, может принимать значения: - Разрешить — разрешает прохождение данных, попадающих под условия фильтра. - Запретить — запрещает прохождение данных, попадающих под условия фильтра.
Фильтровать по	Условия применения фильтра, может принимать значения: - IP. Если выбрано данное условие, то в закладке IP-адреса надо добавить все необходимые IP-адреса для данного условия. Адреса могут быть указаны в следующих форматах: 10.0.0.0/8 — только сеть 10.0.0.0/8. 10.0.0.0/8::11 — маршруты, у которых первый октет 10 и префикс от 8 до 11. 10.0.0.0/8:11:13 — маршруты, у которых первый октет 10 и префикс от 11 до 13. - AS путь. Если выбрано данное условие, то в закладке AS-путь надо добавить все необходимые номера автономных сетей для данного условия.

Пример настройки BGP для кластера NGFW приведен в статье [Варианты настройки BGP для кластера Актив-Пассив](#).

RIP

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. Маршрутизаторы общаются, используя протоколы маршрутизации. NGFW обновляет таблицу маршрутизации в ядре в соответствии с информацией, которую он получает от соседних маршрутизаторов. Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP-уровне. Ядро точно также просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: вместо добавления маршрутов вручную они добавляются и удаляются динамически. Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол RIP.

RIP ([Routing Information Protocol](#)) — протокол дистанционно-векторной маршрутизации, который оперирует транзитными участками (хоп, hop) в качестве метрики маршрутизации. Подробно о работе протокола RIP читайте в соответствующей технической документации.

Для настройки RIP в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Выбрать виртуальный маршрутизатор.	При наличии нескольких виртуальных маршрутизаторов выберите необходимый.
Шаг 2. Включить RIP-роутер.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню RIP и настройте RIP-роутер.
Шаг 3. Указать сети RIP.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню RIP и укажите сети RIP, для которых будет работать RIP протокол.
Шаг 4. Настройте интерфейсы RIP.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню RIP и произведите настройку интерфейсов RIP.

При настройке RIP-роутера необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает использование данного RIP-роутера.
Версия RIP	Определяет версию протокола RIP. Как правило используется версия протокола 2.
Метрика по умолчанию	Стоимость маршрута. Обычно метрика равна 1 и не может превышать 15.
Административное расстояние	Стоимость маршрутов, полученных с помощью протокола RIP. Значение по умолчанию для протокола RIP — 120. Используется для выбора маршрутов при наличии нескольких способов получения маршрутов (OSPF, BGP, статические).
Отправлять себя в качестве маршрута по умолчанию	Оповещать другие роутеры о том, что данный роутер имеет маршрут по умолчанию.

Маршрутизатор RIP будет слать обновления маршрутной информации только с интерфейсов, для которых заданы **сети RIP**. Необходимо указать как минимум одну сеть для корректной работы протокола. При настройке сетей RIP администратор может указать сеть в виде CIDR, например, 192.168.1.0/24, либо указать сетевой интерфейс, с которого будут отправлять обновления.

При настройке интерфейсов RIP укажите следующие параметры:

Наименование	Описание
Интерфейс	Выберите интерфейс, который будет использоваться для работы протокола RIP. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор.
Посылать версию	Укажите версию протокола RIP, которую маршрутизатор будет отсылать.
Принимать версию	Укажите версию протокола RIP, которую маршрутизатор будет принимать.
Пароль	Строка для авторизации, которая будет посылаться и приниматься в пакетах RIP. Все роутеры, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль.
Split horizon	Метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который прибыло обновление.
Poison reverse	Метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута в 16 и отсылает его соседу, от которого его получил.
Пассивный режим	Устанавливает режим работы интерфейса, при котором он принимает обновления RIP, но не отсылает их.

Параметры редистрибуции маршрутов позволяют указать какие из маршрутов необходимо отправлять соседям. Возможно задать для редистрибуции маршруты, полученные через протоколы динамической маршрутизации OSPF, BGP, а также маршруты в непосредственно подключенные к NGFW сети (connected) или маршруты, добавленные администратором в разделе **Маршруты** (kernel).

Мультикастинг

Технология IP мультикастинга позволяет существенно сократить передаваемый объем трафика, доставляя единый поток информации одновременно к тысячам и более потребителей, что особенно эффективно для доставки голосового и видео трафика. Традиционные методы доставки трафика — это unicast (доставка от точки к точке) и broadcast (широковещательная посылка трафика). Мультикастинг (multicast) позволяет доставить трафик к группе хостов (мультикаст-группа). Хосты (получатели), которые хотят получать данный трафик, должны вступить (присоединиться) к соответствующей мультикаст-группе. Для присоединения хостов к мультикаст-группе используется протокол Internet Group Management Protocol (IGMP). Мультикаст-группа идентифицируется групповым адресом. Для мультикастовых адресов выделена подсеть класса D с верхними 4 битами, установленными в 1110. Таким образом диапазон адресов для мультикаст-трансляций определен как 224.0.0.0 — 239.255.255.255.

Далее маршрутизаторы должны обеспечить эффективную доставку трафика от источника трансляции к получателям. Protocol Independent Multicast (PIM) используется на маршрутизаторах для достижения данной цели.

Маршрутизаторы в мультикастинговой среде можно разделить на First Hop Router (FHR), Rendezvous Point (RP), Last Hop Router (LHR). FHR находится ближе всего к источнику трансляции и отвечает за регистрацию источника трансляции в сети. RP является каталогом доступных мультикаст-источников для Any Source Multicast (ASM) режима. LHR находится ближе всего к приемнику мультикаст-трансляции. Клиенты (приемники трансляции) в локальных сетях, подключенных к LHR, используют протокол IGMP для регистрации себя в необходимой мультикаст-группе, посылая сообщение IGMP membership report.

NGFW может быть использован в качестве LHR для локальных сетей, подключенных к нему. Для регистрации клиентов (приемников) NGFW поддерживает протоколы IGMPv3 и IGMPv2.

Для взаимодействия с другими мультикаст-маршрутизаторами NGFW может использовать только режим работы PIM Sparse Mode (PIM-SM). Это режим, в котором мультикаст-трафик отсылается только на те приемники, которые явно запросили это. Приемники должны периодически подтверждать свое желание получать мультикаст-трафик.

NGFW поддерживает режимы работы Source Specific Multicast (SSM) и Any Source Multicast (ASM).

Режим работы Source Specific Multicast (SSM) используется, когда приемник трафика явно указывает известный ему адрес источника трансляции. В данном режиме используется следующая адресация:

rtp://<src_ip>@<group_address>:<port>

где src_ip — адрес источника трансляции, group_address — мультикастовый групповой адрес, port — порт. Например:

rtp://10.10.10.10@239.0.0.5:4344

Режим работы Any Source Multicast (ASM). В этом режиме приемник трансляции указывает мультикаст-группу, с которой хочет получать трансляцию. Для работы данного режима необходимо наличие маршрутизатора с ролью Rendezvous Point (RP). RP определяет источник трансляции для этой группы для данного приемника. После чего источник и приемник выбирают лучший сетевой путь для пересылки данного мультикаст-трафика. В данном режиме используется следующая адресация:

rtp://@<group_address>:<port>

где group_address — мультикастовый групповой адрес, port — порт. Например:

rtp://@239.0.0.5:4344

Для настройки работы NGFW в качестве LHR мультикаст-роутера необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настроить мультикаст-роутер.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню Мультикаст маршрутизатор и настройте его.
Шаг 2. Указать интерфейсы, на которых должен работать данный роутер.	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню Интерфейсы и произведите настройку интерфейсов. Будут доступны только те интерфейсы, которые относятся к данному виртуальному маршрутизатору.
Шаг 3. Задать Rendezvous points для режима ASM (опционально).	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню Rendezvous points и укажите их адреса.
Шаг 4. Установить необходимые ограничения на доступные мультикаст-группы для режима ASM (опционально).	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню Rendezvous points и укажите адреса разрешенных мультикаст-групп в закладке Разрешенные группы ASM . Если оставить этот список пустым, то будут разрешены все групповые адреса.
Шаг 5. Установить необходимые ограничения на доступные мультикаст-группы для режима SSM (опционально).	В консоли NGFW в разделе Сеть → Виртуальные маршрутизаторы выберите в меню Разрешенные группы SSM и укажите адреса разрешенных мультикаст-групп. Если оставить этот список пустым, то будут разрешены все групповые адреса.

При настройке мультикаст-роутера возможно указать следующие параметры:

Наименование	Описание
Включено	Включает или выключает мультикаст-роутер в данном виртуальном маршрутизаторе.
Использовать ECMP	Разрешает распределение трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP). Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если данная опция отключена, то весь трафик на определенный хост назначения будет пересылаться только через один из роутеров (next hop).

Наименование	Описание
Использовать ECMP rebalance	Если при включенной опции один из интерфейсов, через который отсылался трафик, отключился, то все существующие потоки будут перераспределены между оставшимися маршрутами (next hop). При отключенной опции перераспределяются только те потоки, которые передавались через отключенный интерфейс.
JOIN/PRUNE интервал	Интервал в секундах (60-600) отправки сообщений соседям PIM о мультикаст-группах, трафик которых маршрутизатор хочет принимать или более не хочет принимать.
Интервал register suppress	Интервал в секундах (5-60000), после которого маршрутизатор отправляет сообщение register suppress.
Keep-alive таймер	Интервал в секундах (31-60000), через который маршрутизатор будет посылать сообщения keeralive соседям, а также интервал, который маршрутизатор будет ждать, прежде чем будет считать соседа недоступным.

При настройке интерфейсов можно задать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного интерфейса для мультикастинга.
Интерфейс	Выберите интерфейс, который будет использоваться для работы мультикаста. Для выбора доступны только те интерфейсы, которые входят в данный виртуальный маршрутизатор.
Интервал отправки HELLO сообщений	Интервал отправки PIM HELLO сообщений в секундах (1-180). PIM Hello сообщения отправляются периодически со всех интерфейсов, для которых включена поддержка мультикастинга. Эти сообщения позволяют узнать маршрутизатору о соседних маршрутизаторах, поддерживающих мультикастинг.
Приоритет выбора DR	Приоритет при выборе Designated router (DR) от 1 до 4294967295, с помощью которого администратор может управлять процессом выбора DR для локальной сети.
Принимать IGMP	Принимать сообщения IGMP report и IGMP query на данном интерфейсе.
Использовать IGMPv2	Использовать версию IGMP v2, по умолчанию используется IGMP v3.

При настройке Rendezvous points можно указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данный RP.
Название	Название данного RP.
IP-адрес	Unicast IP-адрес данного RP.
Разрешенные группы SSM	Список разрешенных групповых адресов для any source multicast с данного RP. Любые сети из диапазона 224.0.0.0/4. Нет ограничений, если ничего не задано.

Разрешенные группы SSM — настройка мультикаст-роутера, определяющая список разрешенных групповых адресов для source specific multicast. Могут быть указаны любые сети из диапазона 232.0.0.0/8. Нет ограничений, если ничего не задано.

Исключения из SPT — настройка мультикаст-роутера, задающая список IPv4 мультикаст-групп, исключенных из переключения на shortest path tree.

WCCP

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☒

Web Cache Communication Protocol (WCCP) — разработанный компанией [Cisco](#) протокол перенаправления контента. Предоставляет механизм перенаправления потоков трафика в реальном времени, имеет встроенные масштабирование, балансировку нагрузки, отказоустойчивость. При использовании WCCP, WCCP-сервер принимает HTTP-запрос от клиентского браузера и перенаправляет его на один или несколько WCCP-клиентов. WCCP-клиент получает данные из интернет и возвращает их в браузер клиента. Доставка данных клиенту может происходить как через WCCP-сервер, так и минуя его, в соответствии с правилами маршрутизации.

NGFW может выступать в качестве WCCP-клиента. В качестве WCCP-сервера обычно выступает маршрутизатор. Для трафика, полученного через WCCP, можно применять все доступные механизмы фильтрации.

Сервисная группа WCCP — это набор серверов WCCP (роутеры, коммутаторы) и клиентов WCCP (NGFW) с общими настройками перенаправления трафика. Сервера, указанные в одной сервисной группе, должны иметь идентичные настройки.

Для настройки WCCP-клиента в NGFW необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Настройте WCCP сервер.	Произведите настройку сервера WCCP в соответствии с инструкцией на WCCP-сервер.
Шаг 2. Настроить сервисные группы WCCP.	В консоли NGFW в разделе Сеть → WCCP нажать на кнопку Добавить и создать одну или несколько сервисных групп WCCP.

При создании сервисной группы укажите следующие параметры:

Наименование	Описание
Включено	Включает или отключает данную сервисную группу.
Название	Имя сервисной группы.
Описание	Описание сервисной группы.
Сервисная группа	Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу.
Приоритет	Приоритет группы. Если несколько сервисных групп применимы к трафику на сервере WCCP, то приоритет определяет порядок, в котором сервер будет распределять трафик на клиенты WCCP.
Пароль	Пароль, необходимый для аутентификации NGFW в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP.
Способ перенаправления трафика	Определяет способ перенаправления трафика с серверов WCCP на NGFW. Возможны значения: gre — используя туннель Generic Routing Encapsulation (GRE). L2 — используя перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес NGFW. Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2. Важно! Для трафика, полученного через WCCP-туннель, в качестве IP источника NGFW будет использовать IP-адрес компьютера клиента, а зона источника не будет определена, поэтому в правилах фильтрации для зоны источника не следует явно указывать зону (оставить Any).

Наименование	Описание
Способ возврата трафика	Определяет способ перенаправления трафика с NGFW на серверы WCCP. Возможны значения: gre — используя туннель Generic Routing Encapsulation (GRE). L2 — используя перенаправление L2. В этом случае NGFW (WCCP клиент) изменяет MAC-адрес назначения в пакете на адрес роутера (WCCP сервер). Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и NGFW должны находиться в одном L2 сегменте. Не все типы серверов WCCP поддерживают работу с WCCP клиентами по L2.
Порты для перенаправления	Порты для перенаправления. Укажите здесь порты назначения трафика. При необходимости указать несколько портов, укажите их через запятую, например: 80, 442, 8080 Для перенаправления трафика на основании значений портов источника необходимо поставить флажок Порт источника. Важно! NGFW может применять фильтрацию только для перенаправленного TCP трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на NGFW с другими портами, будет отправляться в интернет без фильтрации.
Протокол	Укажите протокол — TCP или UDP.
Роутеры WCCP	Укажите IP-адреса серверов WCCP (роутеры).
Способ назначения	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. Возможны варианты: Хэш — распределение трафика на основе хэша, вычисляемому по указанным полям IP-пакета. Альтернативный хэш — если указан, то WCCP-сервер будет использовать его при превышении определенного количества пакетов, отправленных на WCCP-клиента с использованием обычного хэша. Поля IP-пакета, используемые для получения хэша, должны отличаться для вычисления основного и альтернативного хэшей. Маска — распределение трафика на основе вычисления операции AND между маской и выбранным заголовком пакета. При выборе маски проконсультируйтесь с документацией производителя сервера WCCP.

