Table of Contents

Table of Contents 1
Настройка сети 2
- Настройка зон 3
- Настройка интерфейсов 6
- Настройка шлюзов 13
- Настройка DHCP 15
- Настройка DNS 16
- WCCP 17
- Виртуальные маршрутизаторы 19

Настройка сети

Настройка зон

Product: SWG
Version: 7.5.x

Зона в UserGate SWG — это логическое объединение сетевых интерфейсов. Политики безопасности UserGate SWG 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 SWG поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление SWG
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

Администраторы UserGate SWG 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:

Шаг	Описание
1. Создайте зону.	В разделе **Настройки → Сеть → Зоны** нажмите **Добавить** и укажите название зоны
2. Настройте параметры защиты зоны от DoS (опционально).	Укажите 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 SWG 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, 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.

Шаг	Описание
3. Настройте параметры контроля доступа зоны (опционально).	Укажите предоставляемые UserGate SWG 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 SWG. • **SNMP** — доступ к SWG по протоколу SNMP (UDP 161). • **Captive-портал** и **страница блокировки** — необходимы для показа страницы авторизации Captive-портала и страницы блокировки (TCP 80, 443, 8002). • **API XML RPC поверх HTTP** — доступ к API поверх HTTP (TCP 4040). • **Кластер** — сервис, необходимый для объединения нескольких узлов SWG в кластер (TCP 4369, TCP 9000-9100). • **VRRP** — сервис, необходимый для объединения нескольких узлов SWG 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). • **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. Подробнее — в разделе «Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси». • **Web-портал** — сервис, необходимый для публикации внутренних ресурсов с помощью SSL VPN. Подробнее — в разделе «Веб-портал». • **Log Analyzer**/**SIEM** — сервис для подключения к анализатору журналов Log Analyzer (TCP 2023 и 9713). • **OSPF** — сервис динамической маршрутизации OSPF. Подробнее — в разделе «OSPF». • **BGP** — сервис динамической маршрутизации BGP. Подробнее — в разделе «BGP». • **RIP** — сервис динамической маршрутизации «RIP». • **BFD** — сервис быстрого обнаружения сбоев в сетевом соединении. • **Multicast** — сервис мультикаста. • **NTP сервис** — разрешает доступ к сервису точного времени, запущенному на сервере SWG. • **UserID syslog коллектор** — сервис для разрешения получения информации с удалённых устройств по протоколу Syslog (по умолчанию используется порт TCP 514). • **API XML RPC поверх HTTPS** — доступ к API поверх HTTPS (TCP 4443). Подробнее о требованиях сетевой доступности — в приложении «Требования к сетевому окружению»
4. Настройте 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**

Шаг	Описание
5. Настройте 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. Активировать чекбокс **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 — в разделе «IP-адреса»

Настройка интерфейсов

Product: SWG
Version: 7.5.x

В разделе веб-консоли **Настройки → Сеть → Интерфейсы** отображаются все физические и виртуальные интерфейсы, имеющиеся в системе. Если узел является частью кластера, в разделе отображаются также интерфейсы других узлов кластера.

ПримечаниеДля модели ПАК UserGate FG в разделе веб-консоли «Настройки» ➜ «Сеть» ➜ «Интерфейсы» по умолчанию отображаются только физические сетевые интерфейсы (адаптеры). Для отображения логических интерфейсов нажмите «Типы интерфейса» в меню рабочей области раздела и выберите нужные для отображения типы интерфейсов.

В этом разделе вы можете настраивать параметры имеющихся интерфейсов или добавлять новые логические интерфейсы различных типов.

Для настройки параметров имеющегося в системе интерфейса выберите его в списке и нажмите **Редактировать**. В окне свойств интерфейса вы можете редактировать следующие параметры:

- Состояние интерфейса — включен или отключен.
- 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.
- Зона, к которой относится интерфейс.
- Профиль NetFlow для отправки статистических данных на NetFlow-коллектор.
- Профиль LLDP для отправки данных по протоколу Link Layer Discovery Protocol. Доступен только для физических сетевых интерфейсов.
- Алиас (псевдоним) — дополнительное идентификационное наименование интерфейса. Параметр является опциональным и используется для работы с SNMP.
- Физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, получаемый по DHCP.
- Параметры работы DHCP-ретранслятора. Для работы DHCP-ретранслятора его необходимо включить на вкладке **DHCP-релей**, 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.

Для добавления в систему нового логического интерфейса нажмите **Добавить** и выберите тип логического интерфейса:

- VLAN;
- бонд-интерфейс;
- мост;
- PPPoE;
- loopback.

Создание VLAN-интерфейса

Для создания VLAN-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить VLAN** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение VLAN-интерфейса
Название	Название VLAN-интерфейса. Название присваивается автоматически на основе имени физического порта и тега VLAN
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги»
Описание	Опциональное описание интерфейса
Тип интерфейса	Выбор типа 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

Параметр	Описание
Тег VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов
Имя узла	Имя узла в кластере, на котором создается данный VLAN-интерфейс
Интерфейс	Физический интерфейс, на котором создается VLAN-интерфейс
Зона	Зона, которой принадлежит VLAN-интерфейс
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 (**Режим**) — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS
DHCP-релей	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, на которые необходимо пересылать DHCP-запросы клиентов

Создание бонд-интерфейса

Вы можете объединить несколько физических интерфейсов в один логический агрегированный бонд-интерфейс с целью повышения пропускной способности или отказоустойчивости канала.

Для создания бонд-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить бонд-интерфейс** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение бонд-интерфейса
Название	Название бонд-интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги»
Имя узла	Имя узла в кластере, на котором создается данный бонд-интерфейс
Зона	Зона, которой принадлежит бонд-интерфейс
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	Интерфейс или интерфейсы, которые будут использованы для построения бонд-интерфейса

Параметр	Описание
Режим	Режим работы бонд-интерфейса должен совпадать с режимом работы интерфейса на соседнем устройстве, к которому он подключается. Доступные режимы работы: • **Round robin.** Режим применяется с целью балансировки нагрузки и обеспечения отказоустойчивости. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. • **Active backup**. Режим применяется с целью обеспечения отказоустойчивости. Активен только один сетевой интерфейс из всех объединенных интерфейсов. Переключение на резервный интерфейс происходит исключительно при отказе активного. В целях корректной работы с сетевым оборудованием MAC-адрес бонд-интерфейса анонсируется через один физический порт. • **XOR.** Режим применяется с целью балансировки нагрузки и обеспечения отказоустойчивости. Для распределения трафика между интерфейсами используется функция, которая на основе MAC-адресов источника и назначения определяет, через какой интерфейс отправить пакет. Это гарантирует, что весь трафик между одной парой устройств будет идти через один и тот же физический интерфейс, сохраняя порядок пакетов. Алгоритм распределения передачи пакетов можно уточнить с помощью политики xmit hash. • **Broadcast.** Режим применяется с целью обеспечения отказоустойчивости. Передача пакетов осуществляется на все сетевые интерфейсы. • **IEEE 802.3ad**. Режим работы, установленный по умолчанию. Поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых интерфейсов 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 политику xmit_hash. • **Adaptive transmit load balancing.** Исходящий трафик распределяется в зависимости от загруженности каждого сетевого интерфейса (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущий сетевой интерфейс. Если сетевой интерфейс выходит из строя, другой берет себе MAC-адрес вышедшего из строя интерфейса. • **Adaptive load balancing.** Основываясь на механизме предыдущего режима, дополнительно осуществляя балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых интерфейсов вовне, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевого интерфейса, участвующего в объединении. Таким образом, различные соседние устройства используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами
MII monitoring period (мсек)	Периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 (MII-мониторинг отключен)
Down delay (мсек)	Задержка (в миллисекундах) перед отключением интерфейса при обнаружении сбоя. Параметр применяется исключительно при использовании мониторинга MII (miimon). Значение задержки должно быть кратно интервалу опроса miimon, в противном случае оно будет автоматически округлено до ближайшего кратного значения. Значение по умолчанию — 0
Up delay (мсек)	Задержка (в миллисекундах) перед включением интерфейса после восстановления соединения. Параметр действует только при использовании мониторинга MII (miimon). Значение задержки должно быть кратно интервалу опроса miimon, в противном случае оно будет автоматически округлено до ближайшего кратного значения. Значение по умолчанию — 0
LACP rate	Интервал отправки LACPDU-пакетов в режиме 802.3ad. Возможные значения: • **Slow** — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • **Fast** — запрос партнера на передачу LACPDU-пакетов каждую секунду
Failover MAC	Параметр определяет, какой MAC-адрес будет использоваться виртуальным bond-интерфейсом при отказе одного из физических интерфейсов в режиме **Active-backup**. 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 интерфейсах этот MAC-адрес не устанавливается, пока они находятся в резервном режиме. MAC-адрес назначается во время обработки отказа: если резервный интерфейс становится активным, он принимает новый MAC-адрес (тот, что принадлежит бонд-интерфейсу), а старому активному интерфейсу прописывается MAC-адрес, который принадлежал текущему активному интерфейсу

Параметр	Описание
Xmit hash policy	Параметр определяет алгоритм распределения трафика между активными интерфейсами в режимах балансировки нагрузки бонд-интерфейса **XOR** или **IEEE 802.3ad**. Возможные значения: • **Layer 2** — используются только MAC-адреса для распределения трафика. При этом алгоритме трафик для конкретного узла будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с **IEEE 802.3ad**. • **Layer 2+3** — используются как MAC-адреса, так и IP-адреса. Алгоритм совместим с **IEEE 802.3ad**. • **Layer 3+4** — используются IP-адреса и протоколы транспортного уровня (TCP или UDP). 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
DHCP-релей	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 DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Создание моста (bridge-интерфейс)

Сетевой мост (L2) фильтрует трафик между сегментами сети, пересылая только те кадры, MAC-адрес назначения которых находится за пределами сегмента-отправителя.

Вы можете настроить фильтрацию передаваемого через мост контента на уровне L2 без внесения изменений в сетевую инфраструктуру компании.

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

В режиме Layer 2 создаваемому мосту не нужно назначать IP-адрес, прописывать маршруты и шлюзы для его корректной работы. В таком режиме мост работает на уровне MAC-адресов, транслируя пакет из одного сегмента в другой. В этом режиме невозможно использовать правила защиты почтового трафика.

Внимание! 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 таком режиме могут быть использованы все механизмы фильтрации, доступные в UserGate SWG.

Если мост создается на ПАК UserGate, в котором используется сетевая карта, поддерживающая режим байпас, то можно объединить два интерфейса в байпас-мост. Байпас-мост автоматически переключает два выбранных интерфейса в режим байпас (закорачивает их, пропуская весь трафик мимо SWG) в случаях, если:

- Электропитание ПАК отключено.
- Система внутренней диагностики обнаружила сбой в работе программного обеспечения. Тайм-аут срабатывания при обнаружении сбоя — 10 секунд.

Управление работой байпас-реле сетевых портов доступно через интерфейс командной строки PMC (подробнее — в разделе « Команды управления платформой» руководства PMC CLI).

Подробнее о сетевых интерфейсах, поддерживающих режим байпас, смотрите в руководствах по эксплуатации на модели ПАК UserGate.

Для создания моста:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить мост** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение интерфейса
Название	Название интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги»
Имя узла	Имя узла в кластере, на котором создается bridge-интерфейс

Параметр	Описание
Тип интерфейса	Режим работы интерфейса — Layer 3 или Layer 2
Зона	Зона, к которой принадлежит интерфейс
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 UserGate SWG
STP (Spanning Tree Protocol)	Использование алгоритма 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 размер MTU, размер MSS
DHCP-релей	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 DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Создание PPPoE-интерфейса

PPPoE (**Point-to-point protocol over Ethernet**) — сетевой протокол канального уровня передачи кадров PPP через Ethernet.

Для создания PPPoE-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить PPPoE** и настройте параметры интерфейса.

Параметры	Описание
Включено	Включение PPPoE-интерфейса
Название	Название интерфейса
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги»
Описание	Опциональное описание интерфейса
Имя узла	Имя узла в кластере, на котором создается PPPoE-интерфейс
Интерфейс	Интерфейс, на котором будет создаваться PPPoE-интерфейс
Зона	Зона, к которой принадлежит PPPoE-интерфейс
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.

Параметры	Описание
MTU	Размер MTU. По умолчанию установлено значение 1492 байт, подходящее для стандартного размера кадра Ethernet
MSS	Размер MSS. Корректные значения: 0 или число в диапазоне от 4 до значения, полученного по формуле (MTU - 40)
Логин	Имя пользователя для соединения PPPoE
Пароль	Пароль пользователя для соединения PPPoE
Переподключаться автоматически	Повторное автоматическое установление соединения при обрыве связи
Тип аутентификации	Протоколы аутентификации, использующиеся в протоколе PPP: • **CHAP** (Challenge Handshake Authentication Protocol) — протокол аутентификации с косвенным согласованием. Алгоритм проверки подлинности, предусматривающий 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 между разрывом и повторной попыткой установления соединения
Маршрут по умолчанию	Устанавливает PPPoE-интерфейс в качестве маршрута по умолчанию
Интервал проверки соединения (сек.)	Интервал проверки соединения
Количество неуспешных проверок	Количество неуспешных проверок соединения, после которых UserGate SWG считает, что соединение отсутствует, и разрывает его
Использовать DNS-сервер провайдера	Если опция включена, то UserGate SWG использует DNS-серверы, выданные провайдером
Количество попыток подключения	Количество последовательных неудачных попыток подключения, по достижении которого автоматическое восстановление соединения прекращается
PPPoE-сервис	Имя сервиса указывается, если его предоставил провайдер. Если имя сервиса не используется, поле необходимо оставить пустым

Создание loopback-интерфейса

Для создания loopback-интерфейса:

В разделе **Настройки → Сеть → Интерфейсы** нажмите **Добавить**, выберите **Добавить loopback-интерфейс** и настройте параметры интерфейса.

Параметр	Описание
Включено	Включение интерфейса
Название	Название интерфейса в виде loopbackN, где N — целое число
Теги	Указание опционального тега для маркировки интерфейса. Подробнее — в разделе « Теги»

Параметр	Описание
Описание	Опциональное описание интерфейса
Имя узла	Имя узла в кластере, на котором создается интерфейс
Тип интерфейса	Режим работы интерфейса — Layer 3 или Layer 2
Зона	Зона, которой принадлежит интерфейс.
Профиль LLDP	Профиль для отправки данных по протоколу Link Layer Discovery Protocol (LLDP). Подробнее о настройке профилей — в разделе «Профили 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
DHCP-релей	Настройка работы DHCP-ретранслятора на интерфейсе. Необходимо включить DHCP-ретранслятор, указать в поле **Адрес UserGate** IP-адрес интерфейса, на котором добавляется функция ретранслятора и указать один или несколько DHCP-серверов, на которые необходимо пересылать DHCP-запросы клиентов

Настройка шлюзов

Product: SWG
Version: 7.5.x

Для подключения UserGate SWG к интернету или к ресурсу в другой подсети компании 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 SWG, 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 SWG 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 SWG 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 SWG 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 SWG 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.

ПримечаниеПо 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 SWG 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.

Настройка DHCP

Product: SWG
Version: 7.5.x

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 SWG может также выступать в качестве DHCP-ретранслятора, обеспечивая передачу DHCP-запросов от клиентов, находящихся в различных сетях, на центральный DHCP-сервер. Подробнее о настройке DHCP-ретранслятора — в разделе «Настройка интерфейсов».

В UserGate SWG 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 разделе «Опции DHCP»).

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

ПримечаниеЧтобы 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.

Настройка DNS

Product: SWG
Version: 7.5.x

Для корректной работы устройства необходимо, чтобы UserGate SWG мог разрешать доменные имена в IP-адреса. Укажите корректные IP-адреса серверов DNS в настройке **Системные DNS-серверы**.

Сервис DNS-прокси позволяет перехватывать DNS-запросы от пользователей и изменять их в зависимости от нужд администратора. Сервис работает как в явном режиме, так и для перехвата транзитных запросов. Для явного режима необходимо разрешить доступ к сервису DNS на соответствующей зоне. Для перехвата транзитных запросов в этой зоне необходимо настроить следующие параметры в разделе DNS-прокси.

Параметр	Описание
Кэширование DNS	Включает или отключает кэширование ответов DNS. Рекомендуется оставить включенным для ускорения обслуживания клиентов
DNS-фильтрация	Включает или отключает фильтрацию DNS-запросов. При включении DNS-фильтрации SWG проверяет и перехватывает запросы, отправляя их дальше от своего IP-адреса. Если запрос соответствует запрещающему правилу контентной фильтрации, то он будет заблокирован. Для работы фильтрации необходимо приобрести лицензию 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 во вкладке Назначение ➔ Адрес доставки, не обрабатываются модулем DNS-фильтрации. Обработка таких правил выполняется средствами модуля контентной фильтрации.
Рекурсивные DNS-запросы	Разрешает или запрещает серверу осуществлять рекурсивные DNS-запросы. Рекомендуется оставить эту опцию включенной
Максимальный TTL для DNS-записей	Устанавливает максимально возможное время жизни для записей DNS
Лимит количества DNS-запросов в секунду на пользователя	Устанавливает ограничение на количество DNS-запросов в секунду для каждого пользователя. Запросы, превышающие данный параметр, будут отброшены. Значение по умолчанию - 100 запросов в секунду. Не рекомендуется ставить большие значения для данного параметра, поскольку DNS-флуд (DNS DoS attacks) является довольно частой причиной отказа обслуживания DNS-серверов
Только A и AAAA DNS-записи для не идентифицированных пользователей (защита от VPN поверх DNS)	Если защита включена, то SWG отвечает только на запросы на записи A и AAAA от неизвестных пользователей. Это позволяет эффективно блокировать попытки организации VPN поверх протокола DNS

С помощью правил DNS-прокси можно указать серверы DNS, на которые пересылаются запросы на определенные домены. Данная опция может быть полезна в случае, если внутри компании используется локальный домен, не имеющий связи с интернетом и использующийся для внутренних нужд компании, например, домен Active Directory.

Чтобы создать правило DNS-прокси:

1. В блоке **DNS-прокси** нажмите **Добавить**, задайте **Название** и **Описание** (опционально).

2. Укажите список доменов, которые необходимо перенаправлять. Например, localdomain.local. Допускается использование символа '*' для указания шаблона доменов.

3. Укажите список IP-адресов DNS-серверов, на которые необходимо пересылать запросы на указанные домены.

С помощью DNS-прокси можно задавать статические записи типа host (A-запись). Чтобы создать статическую запись:

1. В блоке **Статические записи** нажмите **Добавить**, задайте **Название** и **Описание** (опционально).

2. Укажите FQDN статической записи. Например, www.example.com.

3. Укажите список IP-адресов, которые UserGate SWG будет возвращать при запросе этого FQDN.

WCCP

Product: SWG
Version: 7.5.x

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.

SWG 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 (SWG) с общими настройками перенаправления трафика. Сервера, указанные в одной сервисной группе, должны иметь идентичные настройки.

Для настройки WCCP-клиента в SWG:

1. Настройте сервер WCCP в соответствии с его инструкцией.

2. Настройте сервисные группы WCCP. В веб-консоли UserGate SWG в разделе **Настройки → Сеть → WCCP** нажмите **Добавить** и создайте одну или несколько сервисных групп WCCP.

При создании сервисной группы укажите следующие параметры.

Параметр	Описание
Включено	Включение или отключение сервисной группы
Название	Название 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 SWG в сервисной группе. Пароль должен совпадать с паролем, указанным на серверах WCCP
Способ перенаправления трафика	Определение способа перенаправления трафика с серверов WCCP на UserGate SWG. Возможны значения: • **gre** — использовать туннель Generic Routing Encapsulation (GRE). • **L2** — использовать перенаправление L2. В этом случае роутер (WCCP сервер) изменяет MAC-адрес назначения в пакете на адрес SWG. Перенаправление L2 как правило требует меньшее количество ресурсов, чем gre, но сервер WCCP и SWG 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-адреса источника UserGate SWG будет использовать IP-адрес компьютера клиента, а зона источника не будет определена. В связи с этим, в правилах фильтрации для зоны источника не следует явно указывать зону (оставить Any).
Способ возврата трафика	Определение способа перенаправления трафика с UserGate SWG на серверы WCCP. Возможны значения: • **gre** — использовать туннель Generic Routing Encapsulation (GRE). • **L2** — использовать перенаправление L2. В этом случае UserGate SWG (WCCP-лиент) изменит MAC-адрес назначения в пакете на адрес маршрутизатора (WCCP-сервер). Перенаправление L2 как правило требует меньшее количество ресурсов, чем GRE, но сервер WCCP и UserGate SWG должны находиться в одном L2-сегменте. Не все типы серверов WCCP поддерживают работу с WCCP-клиентами по L2

Параметр	Описание
Порты для перенаправления	Порты для перенаправления. Укажите здесь порты назначения трафика. Несколько портов указываются через запятую: • 80, 442, 8080 Для перенаправления трафика на основании значений портов источника поставьте флажок **Порт источника** **Важно!** UserGate SWG может применять фильтрацию только для перенаправленного TCP-трафика с портами назначения 80, 443 (HTTP/HTTPS). Трафик, переданный на UserGate SWG с другими портами, будет отправляться в интернет без фильтрации.
Протокол	Укажите протокол — TCP или UDP
Роутеры WCCP	Укажите IP-адреса серверов WCCP
Способ назначения	При наличии в сервисной группе нескольких WCCP-клиентов способ назначения определяет распределение трафика от WCCP-серверов по WCCP-клиентам. Возможные варианты: • Хэш — распределение трафика на основе хэш-суммы, вычисленной по указанным полям IP-пакета. ◦ Альтернативный хэш — если указан, то WCCP-сервер будет использовать его при превышении определенного количества пакетов, отправленных на WCCP-клиент 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

Виртуальные маршрутизаторы

Product: SWG
Version: 7.5.x

Для изоляции трафика между логическими сегментами в крупных сетях с общей инфраструктурой применяется технология виртуальной маршрутизации (Virtual Routing and Forwarding, VRF). С помощью виртуальных маршрутизаторов можно создавать независимые группы интерфейсов, благодаря чему трафик из одной группы не попадет в другую.

Каждый виртуальный маршрутизатор имеет свою собственную таблицу маршрутизации, которая может содержать запись о маршрутах, заданных статически или полученных с помощью протоколов динамической маршрутизации.

В разных виртуальных маршрутизаторах допускается использовать одинаковые IP-сети (IP overlapping).

Интерфейсы, не вошедшие ни в один из виртуальных маршрутизаторов, автоматически назначены на виртуальный маршрутизатор, созданный в системе по умолчанию.

Виртуальные маршрутизаторы имеют следующие ограничения:

- Ряд сервисов может быть использован только в виртуальном маршрутизаторе, созданном по умолчанию:
  - WCCP;
  - ICAP;
  - DNS;
  - авторизация;
  - любой сетевой трафик, генерируемый самим устройством: проверка лицензии, скачивание обновлений, отправка журналов, отправка почтовых сообщений, SMS-сообщений, SNMP-трапов и т. п.;
  - подключение UserGate MC к UserGate SWG возможно только в случае, если порт UserGate SWG находится в виртуальном маршрутизаторе, созданном по умолчанию.
- Действие правил NAT, DNAT, Port forwarding распространяется на все виртуальные маршрутизаторы.
- Зоны являются глобальными — параметры зоны и принадлежность интерфейсов к зонам распространяются на все виртуальные маршрутизаторы.

ПримечаниеВиртуальный маршрутизатор, созданный по умолчанию, необходим для корректной работы UserGate SWG. Он используется для проверки лицензии, получения обновлений, работы DNS-служб.

Создание виртуального маршрутизатора

Чтобы создать новый виртуальный маршрутизатор:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** нажмите **Добавить** и задайте имя и описание нового виртуального маршрутизатора. Если настроен кластер, укажите имя узла, на котором создается этот виртуальный маршрутизатор.

ПримечаниеИмя виртуального маршрутизатора должно содержать минимум три символа. Могут использоваться только строчные буквы латинского алфавита или цифры; в середине и конце имени допускается использование символов «_» и «-». В качестве имени виртуального маршрутизатора нельзя использовать зарезервированные термины (prelocal, local, main, default, unspec) или префиксы (port, gre, egress, ingress, tun, tap, erspan, ppp, bond, bridge, pimreg, mgmt).

2. На вкладке **Интерфейсы** укажите интерфейсы, которые должны принадлежать новому виртуальному маршрутизатору. Интерфейсы, относящиеся к другим виртуальным маршрутизаторам, не могут быть добавлены. Любой из интерфейсов может принадлежать только одному виртуальному маршрутизатору. Допускается использовать интерфейсы всех типов — физические, виртуальные (VLAN), bond-интерфейсы, VPN-интерфейсы и другие.

Дополнительно для нового виртуального маршрутизатора вы можете настроить параметры статической и динамической маршрутизации:

1. Статические маршруты (кроме маршрута по умолчанию). Подробнее о статических маршрутах — в разделе « Статические маршруты». Маршрут по умолчанию добавляется в разделе **Настройки → Сеть → Шлюзы** . Подробнее о настройке шлюзов — в разделе «Настройка шлюзов».

2. Динамические маршруты, получаемые с помощью протокола маршрутизации OSPF. Подробнее — в разделе « OSPF».

3. Динамические маршруты, получаемые с помощью протокола маршрутизации BGP. Подробнее — в разделе « BGP».

4. Динамические маршруты, получаемые с помощью протокола маршрутизации RIP. Подробнее — в разделе « RIP».

5. Мультикастинг. Подробнее — в разделе « Мультикастинг».

Статические маршруты

С помощью статических маршрутов вы можете указать путь в сеть, доступную за определенным маршрутизатором. Маршрут применяется локально на том узле кластера и в том виртуальном маршрутизаторе, где он создается.

Для добавления статического маршрута:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **Статические маршруты** и нажмите **Добавить**. Укажите

название маршрута. Опционально можно добавить описание маршрута.

3. Выберите тип маршрута:

- **Unicast** — стандартный тип маршрута. Отправляет трафик на адреса назначения через заданный шлюз.
- **Blackhole** — трафик отбрасывается без информирования источника о том, что данные не достигли адресата.
- **Unreachable** — трафик отбрасывается. Источнику отправляется ICMP-сообщение host unreachable (тип 3, код 1).
- **Prohibit** — трафик отбрасывается. Источнику отправляется ICMP-сообщение host unreachable (тип 3, код 13).

4. Укажите адрес назначения — подсеть, на которую будет указывать маршрут, например 172.16.20.0/24.

5. Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с устройства.

6. Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, UserGate SWG сам определит интерфейс, исходя из параметров IP-адресации сетевых интерфейсов.

7. Задайте метрику маршрута. Если маршрутов в сеть несколько, то чем меньше значение метрики, тем выше приоритет маршрута.

Протоколы динамической маршрутизации

Протоколы динамической маршрутизации используются для передачи информации о том, какие сети в настоящее время подключены к каждому из маршрутизаторов. UserGate SWG обновляет таблицу маршрутизации в соответствии с информацией, которую он получает от соседних маршрутизаторов.

Динамическая маршрутизация не меняет способов, с помощью которых ядро системы осуществляет маршрутизацию на IP-уровне. Ядро так же просматривает свою таблицу маршрутизации, отыскивая маршруты к узлам, маршруты к сетям и маршруты по умолчанию. Меняется только способ помещения информации в таблицу маршрутизации: маршруты добавляются и удаляются не вручную, а динамически.

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

UserGate SWG поддерживает работу следующих динамических протоколов маршрутизации: OSPF, BGP, RIP.

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).

ПримечаниеМаршруты добавляются только в том виртуальном маршрутизаторе, в котором настроен протокол OSPF.
ПримечаниеПри работе протокола OSPF в кластере отказоустойчивости в режиме «активный — пассивный» метрики на резервных узлах для всех интерфейсов, списков перераспределения маршрутов и карт маршрутов (route map), применимых к этим спискам перераспределения, увеличиваются вдвое. Таким образом устанавливается приоритет мастер-узла в маршрутизации трафика.

Для настройки параметров OSPF в UserGate SWG:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **OSPF**.

3. Для начала настройки параметров OSPF установите флажок **Включено** и укажите идентификатор маршрутизатора. Идентификатор должен быть уникальным и задан в формате IPv4. Для удобства он может совпадать с одним из IP-адресов интерфейсов UserGate SWG, относящихся к выбранному виртуальному маршрутизатору.

4. Настройте параметры интерфейсов, на которых будет работать OSPF.

Параметр	Описание
Включено	Включение или отключение использования интерфейса
Интерфейс	Выбор одного из существующих в системе интерфейсов, на котором будет работать OSPF. Для выбора доступны только интерфейсы, входящие в выбранный виртуальный маршрутизатор
Тип сети	Тип сети для оптимизации процесса установления соседства. Доступны следующие параметры: • **Не установлен**; • **Broadcast**; • **Point-to-point**; • **Point-to-multipoint**

Параметр	Описание
Пассивный режим	Включение или отключение пассивного режима работы интерфейса, при котором через интерфейс запрещается пересылать пакеты обновления протокола маршрутизации
Стоимость	Стоимость (cost) канала интерфейса. Значение передается в объявлениях о состоянии (Link-State Advertisement, LSA) соседним маршрутизаторам и используется ими для вычисления кратчайшего маршрута. Значение по умолчанию — 1
Приоритет	Целое число от 0 до 255. Чем выше значение, тем больше вероятность того, что маршрутизатор станет назначенным (Designated Router, DR) в сети и будет рассылать LSA. Значение 0 исключает маршрутизатор из процедуры выбора DR. Значение по умолчанию — 1
Интервал hello	Интервал в секундах, через который маршрутизатор посылает hello-пакеты. Этот интервал должен быть одинаковым на всех маршрутизаторах в автономной системе. Значение по умолчанию — 10 секунд
Интервал dead	Время в секундах, по истечении которого соседний маршрутизатор считается неактивным. Время исчисляется с момента приема последнего hello-пакета от соседнего маршрутизатора. Значение по умолчанию — 40 секунд
Интервал повторения	Устанавливает интервал повторной отправки пакета LSA. Значение по умолчанию — 5 секунд
Задержка передачи	Устанавливает время, требуемое для доставки соседним маршрутизаторам обновления состояния каналов (link state). Значение по умолчанию — 1 секунда
Профиль BFD	Определяет значения параметров протокола BFD для мониторинга OSPF. Это позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF. Подробнее — в разделе «Профили BFD»
Аутентификация	Включает требование аутентификации каждого принимаемого маршрутизатором OSPF-сообщения. Аутентификация обычно используется для предотвращения внедрения ложного маршрута от нелегитимных маршрутизаторов
Тип аутентификации	Возможные значения: • **Plain** — передача ключа в открытом виде для аутентификации маршрутизаторов. Необходимо указать значение поля **Ключ**. • **Digest** — использование хеш-суммы MD5 для ключа аутентификации OSPF-пакетов. Необходимо указать **Ключ** и **MD5 key ID**. Для корректной работы эти параметры должны быть идентичными на всех маршрутизаторах. Значение параметра **Ключ** может содержать только буквы латинского алфавита, цифры и символ подчеркивания. Максимальное количество символов — 16

5. Настройте параметры областей OSPF.

Параметр	Описание
Включено	Включает или отключает использование области
Имя	Имя области
Стоимость	Стоимость (cost) маршрута по умолчанию, анонсируемая в тупиковую область (stub area). Значение по умолчанию — 1. Если тупиковая область подключена к нескольким пограничным маршрутизаторам области (Area Border Router, ABR), администратор может назначать разные стоимости маршрута по умолчанию для каждого ABR. Это позволяет управлять исходящим из области трафиком, направляя его через предпочтительный шлюз

Параметр	Описание
Идентификатор области	Идентификатор области (area ID) может быть указан в десятичном формате или в формате записи IP-адреса. Для установления соседства OSPF идентификатор области должен совпадать на соседних маршрутизаторах
Тип аутентификации	Возможные значения: • **Нет** — не требовать аутентификацию OSPF-пакетов. • **Plain** — передача ключа в открытом виде для аутентификации OSPF-пакетов. Используется ключ, заданный в параметрах интерфейсов. • **Digest** — использование MD5 хеш-суммы для ключа аутентификации OSPF-пакетов. Используется ключ, заданный в параметрах интерфейсов. Аутентификация на уровне интерфейсов имеет приоритет над аутентификацией на уровне области
Тип области	Доступные типы областей: • **Нормальная** — обычная область, которая создается по умолчанию. Эта область принимает обновления каналов, суммарные маршруты и внешние маршруты. • **Тупиковая** (stub) — тупиковая область не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других областей. Если маршрутизаторам из тупиковой области необходимо передавать информацию за границу автономной системы, они используют маршрут по умолчанию. В тупиковой области не может находиться пограничный маршрутизатор автономной системы (Autonomous System Boundary Router, ASBR). • **NSSA** — Not-so-stubby area. NSSA-область определяет дополнительный тип LSA — LSA type 7. В NSSA-области может находиться ASBR
Не суммировать	Запрещает добавление суммированных маршрутов в тупиковые типы областей
Интерфейсы	Интерфейсы OSPF, на которых будет доступна эта область
Виртуальные линки	Специальное соединение, которое позволяет соединять части областей или присоединить область через другую магистральную область. Настраивается между двумя ABR. Позволяет маршрутизаторам передать пакеты OSPF через виртуальные ссылки, инкапсулируя их в IP-пакеты. Этот механизм используется как временное решение в случае выхода из строя основных соединений. Укажите идентификаторы маршрутизаторов, которые доступны через такую область

6. Карты маршрутов (route map) позволяют фильтровать маршруты при перераспределении и изменять различные атрибуты выбранных маршрутов. На вкладке **Routemaps** указаны глобальные параметры для создания карты маршрутов.

Параметр	Описание
Название	Название карты маршрутов. Не может содержать символы кириллицы
Действие	Устанавливает действие для этой карты маршрутов. Возможные значения: • **Разрешить** — разрешает прохождение данных, отвечающих условиям карты маршрутов. • **Запретить** — запрещает прохождение данных, не отвечающих условиям карты маршрутов

Параметр	Описание
Сравнивать по	Условия применения карты маршрутов. Возможные значения: • **IP**. Если выбрано это условие, на вкладке **IP-адреса** надо добавьте все необходимые IP-адреса для этого условия с возможностью указать **le** (less or equal) и **ge** (greater or equal). Например: ◦ 10.0.0.0/8 — только сеть 10.0.0.0/8. ◦ 10.0.0.0/8::11 — маршруты с первым октетом, равным 10, и префиксом от 8 до 11. ◦ 10.0.0.0/8:11:13 — маршруты с первым октетом, равным 10, и префиксом от 11 до 13. • **AS-путь**. Если выбрано это условие, то в закладке **AS-путь** добавьте все необходимые для него номера автономных сетей. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания «_», который может интерпретироваться как: ◦ пробел; ◦ запятая; ◦ начало строки; ◦ конец строки; ◦ AS set delimiter { and }; ◦ AS confederation delimiter (and). • **Community**. Если выбрано это условие, на вкладке **Community** добавьте все необходимых для него BGP-community
Установить next hop	Установить для отфильтрованных маршрутов IP-адрес для next hop
Установить вес	Установить вес для отфильтрованных маршрутов
Установить метрику	Установить метрику для отфильтрованных маршрутов
Установить предпочтение	Установить предпочтение для отфильтрованных маршрутов
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для этого маршрута
Установить community	Установить (заменить) значение BGP-community для отфильтрованных маршрутов на указанное
Добавлять community	Установить значение BGP-community для отфильтрованных маршрутов

7. Если необходимо, на вкладке **Route redistribution** настройте перераспределения анонсируемых маршрутов из других протоколов в OSPF. Укажите следующие параметры:

- Выберите протоколы из списка:
  - **Kernel** (статические маршруты, добавленные администратором);
  - **Connected** (маршруты в непосредственно подключенные к SWG сети);
  - **RIP;**
  - **BGP.**
- Укажите для каждого выбранного протокола OSPF-метрику (0-16777214).
- При необходимости фильтрации анонсируемых маршрутов из других протоколов, укажите для каждого выбранного протокола список route map.
- Параметр **Всегда отправлять маршрут по умолчанию** позволяет анонсировать маршрут 0.0.0.0/0 даже при отсутствии его в таблице маршрутизации.

BGP

BGP (Border Gateway Protocol) — динамический протокол маршрутизации, относящийся к классу протоколов маршрутизации внешнего шлюза (Exterior Gateway Protocol, EGP). На данный 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. Маршрутизаторы используют протоколы внутридоменной маршрутизации для определения маршрутов внутри своей АС и протокол междоменной маршрутизации для определения маршрутов

доставки пакетов в другие АС. Передаваемая информация содержит список АС, к которым есть доступ через собственную систему. Выбор наилучших маршрутов осуществляет исходя из правил, принятых в сети.

Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол BGP.

Для настройки BGP в UserGate SWG:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **BGP**.

3. Для начала настройки параметров BGP поставьте флажок **Включено** и укажите в качестве идентификатора маршрутизатора IP-адрес, назначенный одному из сетевых интерфейсов UserGate SWG, относящихся к выбранному виртуальному маршрутизатору.

4. Укажите номер автономной системы. Автономная система — это группа сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации. Номер автономной системы указывает на принадлежность маршрутизатора к этой системе.

5. Укажите, какие маршруты будут распространяться в другие BGP-маршрутизаторы в порядке перераспределения (redistribution):

- **connected** — маршруты в сети, непосредственно подключенные к этому узлу;
- **kernel** — статические маршруты, добавленные администратором для выбранного виртуального маршрутизатора;
- **ospf** — маршруты, полученные по протоколу OSPF.

6, Если необходимо включить балансировку трафика для маршрутов с одинаковой стоимостью — установите флажок **Multiple path**.

7. На вкладке **Сети** добавьте сети, относящиеся к выбранной автономной системе.

ПримечаниеЕсли на вкладке «Сети» добавить сети, которых нет в таблице маршрутизации, они не будут анонсироваться.

8. На вкладке **Routemaps** настройте параметры карты маршрутов (route map) для ограничения количества получаемых маршрутов. Карта маршрутов позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов.

Параметр	Описание
Название	Название карты маршрутов. Не может содержать символы кириллицы
Действие	Устанавливает действие для этого route map: • **Разрешить** — разрешает прохождение данных, отвечающих условиям карты маршрутов. • **Запретить** — запрещает прохождение данных, не отвечающих условиям карты маршрутов
Сравнивать по	Условия применения route map: • **IP**. Если выбрано это условие, на вкладке **IP-адреса** добавьте все необходимые для него IP-адреса. • **AS-путь**. Если выбрано это условие, на вкладке **AS-путь** добавьте все необходимые для него номера автономных сетей. Допускается указывать регулярные выражения формата POSIX 1003.2, а также дополнительный символ подчеркивания «_», который может интерпретироваться как: ◦ пробел; ◦ запятая; ◦ начало строки; ◦ конец строки; ◦ AS set delimiter { and }; ◦ AS confederation delimiter (and). • **Community**. Если выбрано это условие, на вкладке **Community** добавьте строки всех необходимых для него BGP-community
Установить next hop	Установить для отфильтрованных маршрутов IP-адрес для next hop
Установить вес	Установить вес для отфильтрованных маршрутов
Установить метрику	Установить метрику для отфильтрованных маршрутов
Установить предпочтение	Установить предпочтение для отфильтрованных маршрутов

Параметр	Описание
Установить AS-prepend	Установить значение AS-prepend — список автономных систем, добавляемых для этого маршрута
Community	Установить значение BGP-community для отфильтрованных маршрутов

9. На вкладке **Фильтры** настройте параметры фильтрации при перераспределении маршрутов.

Параметр	Описание
Название	Название фильтра
Действие	Устанавливает действие для фильтра: • **Разрешить** — разрешает прохождение данных, отвечающих условиям фильтра. • **Запретить** — запрещает прохождение данных, не отвечающих условиям фильтра
Фильтровать по	Условия применения фильтра: • **IP**. Если выбрано это условие, на вкладке **IP-адреса** добавьте IP-адреса для этого 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 это условие, на вкладке **AS-путь** добавьте номера автономных систем для этого условия

10. На вкладке **BGP-соседи** нажмите **Добавить** и настройте параметры маршрутизаторов, относящихся к соседней АС.

Параметр	Описание
Включено	Включение или отключение использования BGP-соседа
Host	IP-адрес BGP-соседа
Описание	Произвольное описание BGP-соседа
Удаленная ASN	Номер автономной системы, к которой относится BGP-сосед
Вес	Вес маршрутов, получаемых от этого BGP-соседа
TTL	Максимальное количество переходов (hop), разрешенное до этого BGP-соседа
Профиль BFD	Настроить с помощью профиля BFD мониторинг BGP для возможности более быстрого обнаружения неисправностей соединений. Подробнее — в разделе «Профили BFD»
Анонсировать себя в качестве следующего перехода (next-hop-self) для BGP	Заменять значение next-hop-self на собственный IP-адрес, если сосед является BGP-соседом
Multihop для eBPGP	Указывает, что путь до этого BGP-соседа имеет больше одного перехода (hop)
Route reflector client	Указывает, является ли этот BGP-сосед клиентом Route reflector

Параметр	Описание
Soft reconfiguration	Использовать функцию soft reconfiguration (без разрыва соединений) для обновления конфигурации
Default originate	Анонсирование BGP-соседу маршрута по умолчанию
Аутентификация	Включение аутентификации для данного BGP-соседа и указание пароля для аутентификации
Фильтры BGP-соседей	Ограничение информации о маршрутах, получаемых от BGP-соседей или маршрутов, анонсируемых для BGP-соседей
Routemaps	Карты маршрутов (route maps) используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между доменами

Важно!Согласно требованиям RFC-8212 для каждого соседа необходимо указать входящие и исходящие фильтры. Без входящих фильтров маршрутизатор не будет принимать маршруты от BGP-соседа. При отсутствии исходящих фильтров маршрутизатор не будет анонсировать маршруты для BGP-соседа.

Если на интерфейсе UserGate SWG, с которого устанавливается подключение к BGP-соседу, назначено несколько IP-адресов, то при настройке BGP-соседа, при отсутствии правила NAT, принудительно устанавливающего адрес источника для BGP-сессии с этим соседом, в качестве адреса UserGate SWG необходимо указать основной (primary) IP-адрес, то есть адрес, который стоит первым в списке параметров интерфейса.

Пример настройки BGP для кластера UserGate SWG — в статье « Варианты настройки BGP для кластера Актив-Пассив ».

RIP

RIP (Routing Information Protocol) — протокол дистанционно-векторной маршрутизации, который использует параметр hop (переход) в качестве метрики маршрутизации.

Маршруты добавляются только в тот виртуальный маршрутизатор, в котором настроен протокол RIP.

Для настройки RIP в UserGate SWG:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **RIP** и установите флажок **Включено**.

3. Настройте параметры протокола RIP:

   - **Версия RIP** — определяет версию протокола RIP. Как правило используется версия 2.
   - **Метрика по умолчанию** — целочисленное значение в интервале от 1 до 15. Обычно значение метрики по умолчанию равно 1.
   - **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 маршрутизаторы о том, что этот маршрутизатор имеет маршрут по умолчанию.

4. Маршрутизатор RIP будет отправлять обновления маршрутной информации только с интерфейсов, для которых заданы **сети RIP**. На вкладке **Сети RIP** укажите 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 отправляться обновления.

5. На вкладке **Интерфейсы** добавьте интерфейсы, на которых будет работать RIP.

Параметр	Описание
Интерфейс	Выберите интерфейс, который будет использоваться для работы протокола RIP. Для выбора доступны только те интерфейсы, которые входят в выбранный виртуальный маршрутизатор
Посылать версию	Версия протокола RIP, с которой будет работать маршрутизатор при отправке сообщений
Принимать версию	Версия протокола RIP, в соответствии с которой маршрутизатор будет принимать сообщения
Пароль	Строка для авторизации, которая будет отправляться и приниматься в пакетах RIP. Все маршрутизаторы, участвующие в обмене информации по протоколу RIP, должны иметь одинаковый пароль

Параметр	Описание
Split horizon	Метод предотвращения петель маршрутизации, при котором маршрутизатор не распространяет информацию о сети через интерфейс, на который пришло обновление
Poison reverse	Метод предотвращения петель маршрутизации, при котором маршрутизатор устанавливает стоимость маршрута, равную 16, и отсылает маршрут соседу, от которого его получил
Пассивный режим	Устанавливает режим работы интерфейса, при котором он принимает обновления RIP, но не отсылает их

6. Параметры редистрибуции маршрутов позволяют указать, какие из маршрутов необходимо отправлять соседям. Вы можете задать для редистрибуции маршруты, полученные через протоколы динамической маршрутизации OSPF, BGP, а также статические маршруты в непосредственно подключенные к UserGate SWG 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 множеству потребителей. Применение этой технологии особенно эффективно для доставки голосового и видеотрафика. Традиционные методы доставки трафика — это юникаст (доставка от точки к точке) и бродкаст (широковещательная посылка трафика). Мультикаст-метод позволяет доставить трафик группе узлов (мультикаст-группа). Узлы (получатели), которые хотят получать этот трафик, должны присоединиться к соответствующей мультикаст-группе. Для присоединения узлов к мультикаст-группе используется протокол Internet Group Management Protocol (IGMP). Мультикаст-группа идентифицируется с помощью группового адреса. Для мультикастовых адресов выделена подсеть класса D со следующим диапазоном адресов для трансляций: 224.0.0.0 — 239.255.255.255.

Маршрутизаторы должны обеспечить эффективную доставку трафика от источника трансляции к получателям. Для достижения этой цели используется протокол Protocol Independent Multicast (PIM).

Маршрутизаторы в мультикастинговой среде могут иметь следующие роли:

- First Hop Router (FHR). FHR находится ближе всего к источнику трансляции и отвечает за регистрацию источника трансляции в сети.
- Rendezvous Point (RP). RP является каталогом доступных мультикаст-источников для режима Any Source Multicast (ASM).
- Last Hop Router (LHR). 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 посредством отправки сообщение IGMP membership report.

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

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

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

Режим работы SSM используется, когда приемник трафика явно указывает известный ему адрес источника трансляции. В таком 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

В режиме работы ASM приемник трансляции указывает мультикаст-группу, от которой он будет получать трансляцию. Для работы режима необходимо наличие маршрутизатора с ролью RP. RP определяет источник трансляции для группы приемника. Далее источник и приемник выбирают лучший сетевой путь для пересылки мультикаст-трафика. В этом 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 UserGate SWG в качестве LHR мультикаст-маршрутизатора:

1. В разделе **Настройки → Сеть → Виртуальные маршрутизаторы** выберите виртуальный маршрутизатор.

2. В свойствах виртуального маршрутизатора в выпадающем списке выберите **Мультикаст-маршрутизатор** и установите флажок **Включено**.

3. Настройте общие параметры мультикастинга:

- **Использовать ECMP** — распределение трафика по нескольким маршрутам по технологии Equal Cost Multi Path (ECMP). Требуется наличие нескольких маршрутов до необходимого сетевого узла. Если эта опция отключена, то весь трафик на определенный узел назначения будет пересылаться только через один из маршрутизаторов (next hop).
- **Использовать ECMP rebalance** — если при включенной опции один из интерфейсов, через который отсылался трафик, отключился, 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 для отправки сообщений PIM JOIN и PIM PRUNE для управления потоком мультикаст-трафика.

- **Интервал register suppress** — таймер в секундах, который временно запрещает маршрутизатору-источнику инкапсулировать мультикаст-трафик в пакеты PIM Register.
- **Keep-alive-таймер** — интервал в секундах (31-60 000), через который маршрутизатор будет посылать сообщения keepalive соседям. Это же значение интервала используется маршрутизатором для принятия решения о недоступности соседа.

4. На вкладке **Интерфейсы** настройте параметры интерфейсов, на которых будет работать мультикастинг.

Параметр	Описание
Включено	Включение или отключение использования интерфейса для мультикастинга
Интерфейс	Интерфейс, который будет использоваться для работы мультикастинга. Для выбора доступны только те интерфейсы, которые входят в выбранный 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. С помощью этих сообщений маршрутизатор узнает о соседних маршрутизаторах, поддерживающих мультикастинг
Приоритет выбора DR	Приоритет при выборе маршрутизатора-источника (Designated router, DR) — значение 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 этом интерфейсе
Использовать IGMPv2	Использовать IGMPv2, по умолчанию используется IGMPv3
Профиль BFD	Определяет значения параметров протокола BFD для мониторинга. Позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса. Подробнее — в разделе «Профили BFD»

5. На вкладке **Rendezvous points** укажите адреса RP для режима ASM.

Параметр	Описание
Включено	Включение или отключение RP
Название	Название RP
IP-адрес	IP-адрес RP
Разрешенные группы ASM	Список разрешенных групповых адресов для отправки any source multicast (ASM) с данного RP. Любые сети из диапазона 224.0.0.0/4. Если ничего не задано, ограничений нет

6. Если необходимо, на вкладке **Разрешенные группы SSM** установите необходимые ограничения на доступные мультикаст-группы для режима SSM. Укажите список разрешенных групповых адресов для SSM. Могут быть указаны любые сети из диапазона 232.0.0.0/8. Если ничего не задано, ограничений нет.

7. Если необходимо, на вкладке **Исключения из SPT** укажите список IPv4 мультикаст-групп, исключенных из переключения на Shortest Path Tree (SPT).