

Table of Contents

Table of Contents	1
Настройки сети	2
Настройка UserGate с двумя интерфейсами	3
Настройка UserGate с одним интерфейсом	4
Router on a Stick	5
Создание отказоустойчивого L2 кластера	6
Настройка подключения отказоустойчивого кластера к двум провайдерам	9
Изменение настроек при использовании нескольких провайдеров	10
Прозрачный мост L2	11
Прозрачный мост L3	12
Настройка WCCP	13
Мониторинг Mirror-порта	16
Виртуальные маршрутизаторы	17
Настройка DHCP Relay и особенности работы	18
Варианты настройки BGP для кластера Актив-Пассив	19
Настройка мультикаст маршрутизации	25
Настройка статической маршрутизации	29

Настройка UserGate с двумя интерфейсами

Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW
KnowledgeBase: 

Данный способ внедрения решения UserGate является рекомендованным. В данной схеме UserGate выступает полноценным узлом в сети, реализующим функции пограничного маршрутизатора с возможностью глубокого анализа пакетов и применения политик фильтрации контента на уровнях 3-7 сетевой модели OSI.

Описываемый способ внедрения также позволяет использовать решение в качестве явного прокси для конфигурирования ПО, установленного на клиентских хостах сети.

В данной конфигурации, в малых сетях, шлюзом по умолчанию на конечных узлах сети указывается IP-адрес решения UserGate. В более сложных сетях решение выступает шлюзом по умолчанию для маршрутизаторов Core уровня.

Так как в данном сценарии UserGate маршрутизирует трафик между различными интерфейсами, вам потребуется назначить IP-адрес на каждый интерфейс.

Для настройки работы UserGate в данном режиме вам потребуется произвести следующие настройки:

- Задать IP-адреса для каждого из физически коммутированных интерфейсов.
- Задать настройки маршрутизации.
- Задать настройки Domain Name Services (DNS).

Для настройки IP-адресов, необходимо определить, какие физические интерфейсы коммутированы. Номера интерфейсов на устройстве, либо в виртуальной машине напрямую соответствуют интерфейсам в консоли администратора. Например, интерфейс "0" на устройстве, будет соотнесен с интерфейсом "port0" в консоли администратора.

Подключите интерфейс port0 UserGate к коммутатору локальной сети, к интерфейсу port1 подключите кабель от провайдера, подключите монитор и клавиатуру (в случае аппаратной платформы) и включите питание.

При первом включении UserGate подтвердите начальную инициализацию.

При наличии в локальной сети DHCP-сервера выделенный адрес интерфейса будет отображён в веб-консоли, при отсутствии DHCP-сервера задайте адрес интерфейса командой CLI-консоли (A.B.C.D/M - выделенный адрес и маска локальной сети):

- Для UserGate версий 6.1.x:

```
UTM> iface config -name port0 -ipv4 A.B.C.D/M -enabled true -mode static
```

С компьютера локальной сети откройте в браузере в веб-консоль по ссылке <https://A.B.C.D:8001/> где A.B.C.D - назначенный или выделенный адрес интерфейса UserGate.

При первом подключении к веб-консоли выберите язык, часовой пояс и задайте логин/пароль администратора (всё это можно будет позже изменить).

На вкладке **Настройки → Сеть → Интерфейсы** в свойствах интерфейса port1 задайте IP-адрес и маску и включите интерфейс. Настройте шлюз по умолчанию и DNS на вкладках **Настройки → Сеть → Шлюзы** и **Настройки → Сеть → DNS** соответственно.

Примечание Шлюз - это маршрут во внешнюю сеть, если в локальной сети есть сегменты, отделённые другими маршрутизаторами - создайте необходимые маршруты на вкладке Настройки → Сеть → Виртуальные маршрутизаторы.

При наличии двух или более шлюзов возможны 2 варианта работы:

- Балансировка трафика между шлюзами. Для этого в свойствах шлюзов необходимо 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).
- 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** необходима для проверки доступности хоста в интернет с указанной в настройках периодичностью. В случае, если хост становится недоступным, то происходит перевод всего трафика на запасные шлюзы в порядке их расположения в консоли.

Зарегистрируйте продукт: кликните по надписи "**Незарегистрированная версия**" в верхней части экрана и введите необходимую информацию.

Успешная регистрация является подтверждением правильных настроек параметров сети.

На вкладке **Настройки → Сеть → Зоны** в свойствах зоны **Trusted** на вкладке **Контроль доступа** отметьте чекбокс **Консоль администрирования**. Далее укажите зону **Trusted** в свойствах интерфейса **port0** на вкладке **Общие**.

Перейдите на вкладку **Настройки → Политики сети → Межсетевой экран** и включите предустановленное правило **Allow trusted to untrusted**.

В разделе **Настройки → Политики сети → NAT и маршрутизация** включите предустановленное правило **NAT from Trusted to Untrusted**.

Настройка параметров сети UserGate выполнена, на компьютерах пользователей вы можете указать адрес интерфейса локальной сети UserGate как HTTP-прокси (по умолчанию порт 8090) или как шлюз по умолчанию.

Настройка UserGate с одним интерфейсом

KnowledgeBase: 
Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW

Подключите интерфейс port0 UserGate к коммутатору локальной сети, подключите монитор и клавиатуру (в случае аппаратной платформы) и включите питание.

При первом включении UserGate подтвердите начальную инициализацию.

При наличии в сети DHCP-сервера выделенный адрес интерфейса будет отображён в веб-консоли, при отсутствии DHCP-сервера задайте адрес интерфейса командой CLI-консоли:

Примечание Для UserGate версий 6.1.x: UTM> iface config -name port0 -ipv4 A.B.C.D/M -enabled true -mode static

где A.B.C.D/M - выделенный адрес и маска локальной сети.

С компьютера локальной сети откройте в браузере в веб-консоль по ссылке <https://A.B.C.D:8001/>, где A.B.C.D - назначенный или выделенный адрес интерфейса UserGate.

При первом подключении к веб-консоли выберите язык, часовой пояс и задайте логин/пароль администратора (всё это можно будет позже изменить).

В веб-консоли проверьте настройки шлюза по умолчанию (**Настройки → Сеть → Шлюзы**) и DNS и (**Настройки → Сеть → DNS**), при необходимости задайте.

Примечание Шлюз - это маршрут во внешнюю сеть, если в локальной сети есть сегменты, отделённые другими маршрутизаторами - создайте необходимые маршруты на странице Настройки → Сеть → Виртуальный маршрутизатор. Если адрес интерфейса был назначен по DHCP - в свойствах интерфейса port0 (Настройки → Сеть → Интерфейсы) измените режим с DHCP на Статический.

Зарегистрируйте продукт для чего кликните по надписи **Незарегистрированная версия** в верхней части экрана и введите необходимую информацию.

Успешная регистрация является подтверждением правильных настроек параметров сети.

На вкладке **Настройки → Сеть → Зоны** откройте свойства зоны **Trusted** и отметьте чекбокс **Консоль администрирования** на вкладке **Контроль доступа**. Далее во вкладке **Настройки → Сеть → Интерфейсы** в свойствах интерфейса port0 выберите зону **Trusted**.

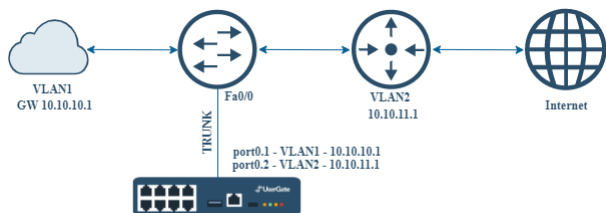
Перейдите в раздел **Настройки → Политики сети → Межсетевой экран**. В свойствах предустановленного правила **Allow trusted to untrusted** во вкладке **Назначение** отключите чекбокс **Untrusted** и включите правило.

В разделе **Настройки → Политики сети → NAT и маршрутизация** в свойствах предустановленного правила **NAT from Trusted to Untrusted** измените зону назначения с **Untrusted** на **Trusted** и включите правило.

Настройка параметров сети UserGate выполнена, для фильтрации трафика пользователей вы можете указать адрес UserGate как HTTP-прокси (по умолчанию порт 8090) или как шлюз по умолчанию.

Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW
KnowledgeBase:

Router-on-a-stick — это термин, часто используемый для описания настройки, которая состоит из маршрутизатора (в нашем случае — устройства UserGate) и коммутатора, подключенных с помощью одного канала Ethernet, настроенного как TRUNK-канал. В этой настройке порты коммутатора принадлежат различным VLAN, и UserGate выполняет всю маршрутизацию между различными сетями/VLAN. Иными словами, на единственном порту UserGate настраиваются подинтерфейсы, которые принадлежат разным VLAN и имеют разные IP адреса. По сути, это соответствует способу внедрения UserGate с двумя интерфейсами, описанному выше, только в качестве интерфейсов используются саб-интерфейсы.



Для конфигурации данной архитектуры произведите следующие настройки.

1. В разделе **Сеть → Интерфейсы** веб-консоли администратора нажмите на кнопку **Добавить** и из выпадающего меню выберите **Добавить VLAN**.
2. В свойствах VLAN-интерфейса в пункте **Тип интерфейса** установите значение **Layer 3**.
3. Укажите корректный номер VLAN в пункте **Тег VLAN**.
4. Выберите интерфейс, который вы скоммутировали для работы.
5. В пункте **Зона** укажите зону, к которой будет принадлежать создаваемый виртуальный интерфейс.
6. Во вкладке **Сеть** укажите режим назначения IP-адреса на интерфейс - **DHCP** или **Статический**. Если выбран статический режим, то укажите сетевые параметры вручную.
7. Активируйте интерфейс, включив чекбокс **Включено**.

The first screenshot shows the 'Свойства VLAN-интерфейса' (VLAN Interface Properties) window. The 'Общие' (General) tab is selected. The 'Включено' (Enabled) checkbox is checked. The 'Название' (Name) field is 'port0.1'. The 'Описание' (Description) field is empty. The 'Тип интерфейса' (Interface Type) is set to 'Layer 3'. The 'Тег VLAN' (VLAN Tag) is set to '1'. The 'Имя узла' (Node Name) is 'utmcore@pretalereean'. The 'Интерфейс' (Interface) is set to 'port0'. The 'Зона' (Zone) is set to 'Зона не установлена' (Zone not set). The 'Профиль netflow' (Netflow Profile) is 'Не выбран' (Not selected). The 'Сохранить' (Save) and 'Отмена' (Cancel) buttons are at the bottom.

The second screenshot shows the 'Свойства VLAN-интерфейса' (VLAN Interface Properties) window. The 'Сеть' (Network) tab is selected. The 'Режим' (Mode) is set to 'Статический' (Static). The 'MAC-адрес' (MAC Address) field is empty. The 'MTU' is set to '1500'. The 'IP интерфейс' (IP Interface) table shows the following configuration:

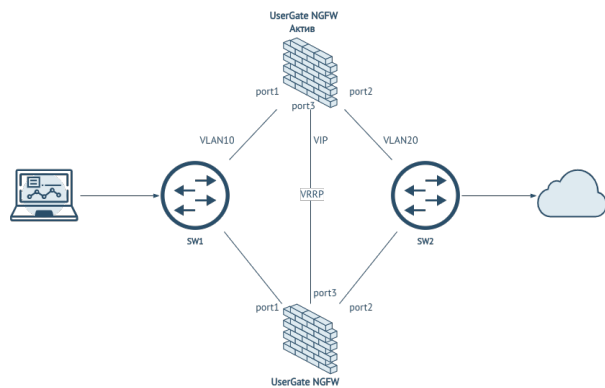
IP интерфейс	Маска
10.10.10.1	255.255.255.0

The 'Сохранить' (Save) and 'Отмена' (Cancel) buttons are at the bottom.

Повторите описанные действия для других виртуальных интерфейсов.

UserGate поддерживает работу кластера отказоустойчивости на канальном уровне сетевой модели OSI (L2). Отказоустойчивый L2 кластер работает в режиме Актив-Пассив, при котором один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а другой — в качестве резервного. В случае сбоя активного узла резервный становится активным и начинает обрабатывать трафик. Поддержка синхронизации пользовательских сессий обеспечивает прозрачное для пользователей переключение трафика с одного узла на другой.

Рассмотрим работу отказоустойчивого L2 кластера на следующем примере:



Трафик транслируется через мост активного узла кластера. На резервном узле передача транзитного трафика блокируется. На всех узлах кластера выполняется мониторинг состояния интерфейсов моста и проверка доступности работающих сетевых сервисов (DNS-сервер, HTTP-сервер).

Для создания отказоустойчивого L2 кластера на UserGate NGFW необходимо:

1. Создать кластер конфигурации.
2. Создать L2 мост на интерфейсах узлов кластера.
3. Настроить кластер отказоустойчивости.

Создание кластера конфигурации

Состояние узлов кластера конфигурации можно увидеть в разделе **UserGate → Управление устройством → Кластер конфигурации**.

Клuster конфигурации				
✎ Редактировать ✖ Удалить узел Генерировать секретный код ↺				
Имя узла ↑	Идентификатор узла	Лицензия	Статус	IP-адрес
utmcore@forprostaome	node_2	Лицензия активна	Узел доступен	192.168.100.6
utmcore@thihealetero	node_1	Лицензия активна	Узел доступен	192.168.100.5

1. В веб-консоли администратора в разделе **Сеть → Интерфейсы** нажать кнопку **Добавить** и из выпадающего меню выбрать **Добавить мост**.
2. В открывшемся окне в пункте **Тип интерфейса** установить значение **Layer 2**. В пункте **Зона** указать зону, которой будет принадлежать создаваемый мост. В пункте **Интерфейсы моста** выбрать два интерфейса, которые коммутировались для работы в данном режиме:

Свойства

Общие

Дополнительно

Сеть

DHCP-релей

Включено:

☒

Название:

bridge1

Описание:

Тип интерфейса:

Layer 2

Имя узла:

utmcore@thihealetero

Зона:

Trusted

Профиль netflow:

Не выбран

☒ Интерфейсы моста

Интерфейс:

port1

Интерфейс:

port2

☐ Интерфейсы байпас моста

Пары интерфейсов:

Нет

3. При успешном создании L2 моста в разделе **Интерфейсы** появится новый тип интерфейса **Сетевой мост**:

	Сетевой мост	bridge1	Без адреса	Нет	08:00:27:28:62:a8	 Trusted	—	—	 port1  port2	100 Mb/s	Layer 2
--	--------------	---------	------------	-----	-------------------	---	---	---	--	----------	---------

Настройка кластера отказоустойчивости

Создать кластер отказоустойчивости в режиме Актив-Пассив. Для этого необходимо выполнить следующие настройки:

1. В разделе **UserGate → Управление устройством → Кластеры отказоустойчивости** нажать кнопку **Добавить**. Выбрать режим работы кластера **Актив-Пассив**, поставить флажок **Включено** в пункте **Синхронизировать сессии**:

Свойства кластера отказоустойчивости

ОбщиеУзлыВиртуальные IP

Включено:

☒

Название:

L2 cluster

Описание:

Режим кластера:

Актив-Пассив

Синхронизировать сессии:

☒ Включено

Мультикаст идентификатор

0

Идентификатор виртуального маршрутизатора (VRID):

1

Сохранить

Отмена

2. Выбрать узлы, которые войдут в кластер отказоустойчивости:

Свойства кластера отказоустойчивости

ОбщиеУзлыВиртуальные IP

Можно добавить до 4-х узлов в кластер отказоустойчивости. Каждый узел может быть использован только в одном кластере. Узел с ролью Мастер принимает на себя весь трафик в режиме кластера Актив-Пассив, или управляет распределением трафика на все узлы в режиме Актив-Актив

Узел

Доступные узлы

☒ utmcore@forprostaome

☒ utmcore@thihealetero

Сохранить

Отмена

3. Добавить виртуальный IP-адрес на выделенный кластерный интерфейс между узлами:

Свойства кластера отказоустойчивости

ОбщиеУзлыВиртуальные IP

Добавить

Редактировать

Удалить

IP-адрес

Интерфейс

Сохранить

Отмена

Свойства виртуального IP

Виртуальный IP:

92.168.100.10

Маска:

255.255.255.0

Интерфейсы

utmcore@forprostaome:

port3

utmcore@thihealetero:

port3

Сохранить

Отмена

Свойства кластера отказоустойчивости

Общие

Узлы

Виртуальные IP

Добавить

Редактировать

Удалить

IP-адрес	Интерфейс
192.168.100.10/24	utmcore@thihealetero: port3 utmcore@forprostaome: port3

Сохранить

Отмена

4. Состояние узлов кластера можно определить по цвету индикатора около названия узла UserGate в разделе **UserGate → Управление устройством → Кластеры отказоустойчивости** :

- **Красный**: нет связи с соседними узлами конфигурации.
- **Жёлтый**: кластер отказоустойчивости не запущен на узле.
- Отсутствие индикатора напротив названия узла говорит о доступности узла кластера.

Кластеры отказоустойчивости

Включить

Отключить

Назначить мастером

Название	Узлы	Виртуальные IP
L2 cluster	utmcore@thihealetero ★ utmcore@forprostaome	192.168.100.10/24

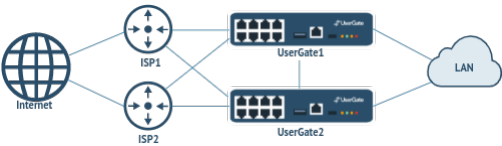
Создание отказоустойчивого L2 кластера завершено.

Настройка подключения отказоустойчивого кластера к двум провайдерам

Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW
KnowledgeBase:

UserGate поддерживает настройку кластера отказоустойчивости для обеспечения бесперебойной работы сети. Кластер отказоустойчивости может работать в двух режимах **Актив-Актив** и **Актив-Пассив**. Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другое.

Концептуальная схема подключения будет выглядеть следующим образом:



В данной схеме, устройства UserGate настроены в режиме отказоустойчивого кластера по схеме Актив-Пассив. В данном режиме один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные - в качестве резервных. На каждом из узлов кластера выбраны сетевые интерфейсы, которым администратор назначил виртуальные IP-адреса. Между этими интерфейсами происходит обмен сообщениями - VRRP-объявления, с помощью которых узлы обмениваются информацией о своём состоянии.

При переходе роли Мастер-узла на резервный сервер происходит перенос всех виртуальных IP-адресов всех кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети, например, главный узел выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в Интернет, и доступ в Интернет отсутствует через все имеющиеся шлюзы.
- Сбой в работе ПО UserGate.

Подробнее о работе кластера читайте в UserGate. Руководство администратора.

Для конфигурации автоматического переключения хостов на резервного оператора связи необходимо настроить несколько шлюзов - в данном примере два. При этом один из шлюзов необходимо указать как шлюз по умолчанию (зелёная/красная точка - индикатор доступности адреса).

Шлюзы							
Добавить Редактировать Удалить Копировать Установить по умолчанию Включить Показать Все Отключить							
Название	IP шлюза	В...	Балансировка	Виртуальный м...	Интерфейс	MAC	Пр...
Узел кластера: utm@a (текущий узел)							
10.10.10.11 (По умолчанию)	10.10.10.11	1	Отключено	Виртуальный ...	port3	00:0c:29:56:0b:39	static
192.168.117.85	192.168.117.1	1	Отключено	Виртуальный ...	port2	44:67:47:9a:53:6f	static
Узел кластера: utm@b							
10.10.10.11 (По умолчанию)	10.10.10.11	1	Отключено	Виртуальный ...	port3	00:0c:29:56:0b:39	static
192.168.117.242	192.168.117.1	1	Отключено	Виртуальный ...	bond1	44:67:47:9a:53:6f	static

Далее нужно включить функцию **Проверка сети** (нажав на одноимённую кнопку) и указать узел в интернете, доступность которого система будет периодически проверять.

Свойства проверки сети

Включено:

Частота проверки: 10 (В секундах, допустимые зн

Процент неудачных запросов: 70 (%; допустимые значения: 1

Добавить Редактировать Удалить

IP-адрес

8.8.8.8

Сохранить Отмена

Когда ресурс перестанет быть доступным, система переключится на следующий в списке шлюз и будет использовать его по умолчанию.

На следующем рисунке, обратите внимание, что основной шлюз по умолчанию стал недоступен (зелёная/красная точка - индикатор доступности адреса):

Шлюзы							
Добавить Редактировать Удалить Копировать Установить по умолчанию Включить Показать Все							
Название	IP шлюза	В...	Балансировка	Виртуальный мар...	Интерфейс	MAC	Прото...
Узел кластера: utm@a (текущий узел)							
10.10.10.11 (По умолчанию)	10.10.10.11	1	Отключено	Виртуальный мар...	port3	00:0c:29:56:0b:39	static
192.168.117.85	192.168.117.1	1	Отключено	Виртуальный мар...	port2	44:67:47:9a:53:6f	static
Узел кластера: utm@b							
10.10.10.11 (По умолчанию)	10.10.10.11	1	Отключено	Виртуальный мар...	port3	00:0c:29:56:0b:39	static
192.168.117.242	192.168.117.1	1	Отключено	Виртуальный мар...	bond1	44:67:47:9a:53:6f	static

Кластер переключился на запасной шлюз:

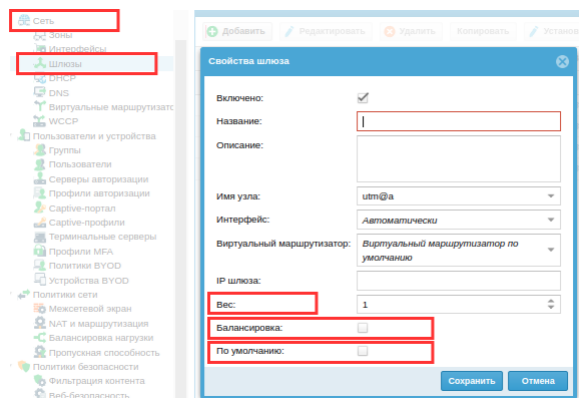
```
oksa@ubuntu:~$ traceroute 8.8.8.8
17: [LOCALHOST]
1: 10.0.0.1 0.369ms
1: 10.0.0.1 0.257ms
2: 192.168.117.1 5.528ms
3: 192.168.11.0 1.775ms
```

Изменение настроек при использовании нескольких провайдеров

Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW
KnowledgeBase:

Для подключения UserGate к сети Интернет возможно использование нескольких провайдеров. В такой ситуации необходимо указать несколько шлюзов (подробнее смотрите в [UserGate 6. Руководство администратора](#)).

При использовании нескольких провайдеров с помощью приоритетов можно настроить резервирование интернет-каналов или режим балансировки. Сделать это можно при указании шлюзов в разделе **Сеть → Шлюзы**, включив чекбоксы **Балансировка** или чекбокс **По умолчанию**.



Если при настройке шлюзов в свойствах нескольких из них включить чекбокс **По умолчанию**, то шлюзом по умолчанию будет назначен последний выбранный шлюз.

При включении режима балансировки необходимо указать вес шлюза: больший вес шлюза соответствует большей доле трафика, которая идет через шлюз. При распределении трафика между шлюзами с разными весами происходит:

1. Вычисление хэша от адресов источника и назначения.
2. 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 $n1/w1 = n2/w2$.

При использовании режима балансировки включение чекбокса **По умолчанию** не оказывает влияния на работу шлюзов, т.е. если одновременно включить чекбоксы **Балансировка** и **По умолчанию**, то шлюзы будут работать в режиме балансировки в соответствии с указанными весами.

Version: 5.x, 6.1.8, 6.1.9
Product: UserGate NGFW
KnowledgeBase:

Внимание! Функционал DNS-фильтрации и мост L2 в текущей версии несовместимы - при включении DNS-фильтрации DNS-запросы через мост проходить перестают.

Сетевой мост работает на канальном уровне сетевой модели OSI (L2). При получении из сети кадра он сверяет его MAC-адрес назначения и, если он не принадлежит данному сегменту, передает (транспирует) кадр дальше; если кадр принадлежит данному сегменту, мост ничего не делает.

Интерфейс мост можно использовать в UserGate аналогично обычному интерфейсу. Кроме этого, через мост можно настроить фильтрацию передаваемого контента 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:



При выборе режима Layer 2 создаваемому мосту не нужно назначать IP-адрес и прописывать маршруты и шлюзы для его корректной работы. В данном режиме мост работает на уровне MAC-адресов, транспируя пакет из одного сегмента в другой. В этом случае невозможно использовать правила ACU ТП и защиты почтового трафика; контентная фильтрации в этом режиме работает.

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 UserGate) 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.

Чтобы сконфигурировать UserGate, в режиме L2 прозрачного моста произведите следующие настройки.

1. В веб-консоли администратора перейдите во вкладку **Сеть → Интерфейсы**.
2. Нажмите на кнопку **Добавить** и из выпадающего меню выберите **Добавить мост**.
3. В открывшемся окне в пункте **Тип интерфейса** установите значение **Layer 2**.
4. В пункте **Зона** укажите зону, которой будет принадлежать создаваемый мост.
5. В разделе **Интерфейсы моста** выберите два интерфейса, которые вы сконфигурировали для работы в данном режиме.

Если ваше оборудование поддерживает режим работы Байпас моста, в разделе **Интерфейсы байпас моста**, выберите соответствующие интерфейсы

Активируйте мост, включив чекбокс **Включено**.

Прозрачный мост L3

Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW
KnowledgeBase:

При выборе режима Layer 3 создаваемому мосту необходимо назначить IP-адрес и указать маршруты в сети, подключенные к интерфейсам моста.



В данном режиме могут быть использованы все механизмы фильтрации, доступные в UserGate.

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 UserGate) 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.

Чтобы сконфигурировать UserGate в режиме L3 прозрачного моста, произведите следующие настройки.

1. В главной консоли перейдите на вкладку **Сеть → Интерфейсы**.
2. Далее, нажав на кнопку **Добавить**, выберите **Добавить мост**.
3. В открывшемся окне установите значение **Layer 3** в пункте **Тип интерфейса**.
4. Также укажите зону, которой будет принадлежать создаваемый мост.
5. В разделе **Интерфейсы моста** выберите два интерфейса, которые вы сконмутировали для работы в данном режиме.
6. Если ваше оборудование поддерживает режим работы Байпас-моста, в разделе **Интерфейсы байпас моста**, выберите соответствующие интерфейсы
7. Во вкладке **Сеть**, выберите предпочитаемый метод назначения сетевых параметров для моста - **DHCP** или **Статический**. При выборе статического режима, задайте сетевые параметры вручную.

The image shows two screenshots of the UserGate configuration interface. The left screenshot shows the 'Свойства' (Properties) window for a bridge, with the 'Сеть' (Network) tab selected. The 'Включено' (Enabled) checkbox is checked. The 'Тип интерфейса' (Interface type) is set to 'Layer 3'. The 'Зона' (Zone) is set to 'Trusted'. The 'Интерфейсы моста' (Bridge interfaces) section shows 'port1' and 'port2' selected. The right screenshot shows the 'Свойства' window with the 'Сеть' tab selected, and the 'Режим' (Mode) set to 'Статический' (Static). A 'IP интерфейса' (Interface IP) dialog box is open, showing the IP address '10.10.10.10' and the mask '255.255.255.0'.

Активируйте мост, отметив чекбокс **Включено**.

Настройка WCCP

Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW
KnowledgeBase: 

WCCP (Web Cache Communication Protocol) - протокол, разработанный компанией Cisco и предназначенный для перенаправления трафика в режиме реального времени. Поддержка протокола WCCP позволяет использовать UserGate в инфраструктуре с WCCP-серверами (UserGate может выступать только в качестве WCCP-клиента).

Когда устройство UserGate не находится в физическом пути клиентов и серверов, оно должно полагаться на внешнее устройство—либо коммутатор уровня 4 (L4), либо маршрутизатор с поддержкой WCCP, для перенаправления пакетов к нему для прозрачного проксирования. Этот тип развертывания известен как развертывание виртуально в разрыв. WCCP рекомендуется использовать для схемы виртуально в разрыв, поскольку он обеспечивает следующие преимущества:

Масштабируемость и балансировка нагрузки — трафик может быть автоматически распределен на несколько устройств UserGate. Если один UserGate отключается, трафик автоматически перераспределяется между другими устройствами UserGate в группе.

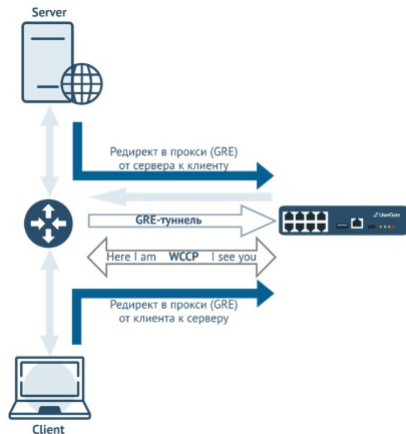
Безопасность — вы можете защитить группу служб WCCP паролем, чтобы к ней могли присоединиться только авторизованные устройства. Кроме того, можно настроить списки управления доступом (ACL) на маршрутизаторе, чтобы ограничить доступ только к определенным устройствам UserGate.

Отказоустойчивость — в случае отсутствия устройств UserGate, доступных для перенаправления трафика, маршрутизатор перенаправляет трафик на исходный адрес назначения.

Гибкость — вы точно контролируете, какой трафик перенаправлять и как его перенаправлять. Вы можете перенаправить весь трафик, входящий или исходящий из интерфейса маршрутизатора; вы можете фильтровать трафик с помощью ACL или вы можете определить конкретный протокол и порты для перенаправления.

В развертываниях прозрачных прокси клиент не знает, что он взаимодействует с UserGate, а не с конечным сервером (КС). Таким образом, пакет от клиента адресован КС. Маршрутизатор проверяет трафик на интерфейсах с поддержкой WCCP (входящий или исходящий в зависимости от конфигурации) и определяет, следует ли перенаправлять его на основе правил, согласованных маршрутизатором и устройствами UserGate.

Далее будет рассмотрена настройка перенаправления трафика по протоколу WCCP между оборудованием Cisco и UserGate.



На оборудовании Cisco необходимо настроить перенаправление на UserGate клиентских http/https запросов и ответов сервера. Настройка маршрутизатора Cisco производится в соответствии со следующим алгоритмом.

Создать два списка доступа. Список wccp_to_inet разрешает трафик из сети с компьютерами пользователей в любые сети. Список wccp_to_lan разрешает любой трафик в сеть с компьютерами пользователей.

```
ip access-list extended wccp_to_inet
permit ip <PC_network_IP> <PC_network_wildcard_mask> any

ip access-list extended wccp_to_lan
permit ip any <PC_network_IP> <PC_network_wildcard_mask>
```

```
ip wccp 80 redirect-list wccp_to_inet password <Password>
ip wccp 90 redirect-list wccp_to_lan password <Password>
```

#Настройка интерфейса, смотрящего в сторону UTM

```
interface GigabitEthernet2/0
ip wccp redirect exclude in
```

#Настройка интерфейса, смотрящего в Интернет

```
interface FastEthernet0/0
ip wccp 90 redirect in
```

#Настройка интерфейса, смотрящего в сторону клиента

```
interface GigabitEthernet1/0
ip wccp 80 redirect in
```

На UserGate необходимо настроить сервисные группы для редиректа клиентских запросов и ответов сервера, использующие GRE (Generic Routing Encapsulation) туннель и порты 80 и 443. При включении WCCP создаётся туннель GRE, который не отображается в списке интерфейсов и не имеет зоны. Правила NAT для перенаправления трафика не используются. Настройка UserGate произведена следующим образом.

В разделе **Сеть → WCCP** свойствах сервисной группы WCCP для перенаправления запросов пользователей на сервер необходимо указать следующие значения параметров:

- **Сервисная группа:** 80.
- **Приоритет:** 240.
- **Способ перенаправления трафика:** GRE.
- **Способ возврата трафика:** GRE.
- **Маршрутизатор WCCP:** 192.168.55.100.
- **Порт для перенаправления:** 80, 443.
- **Протокол:** TCP.
- **Хэш:** IP источника.

Свойства сервисной группы WCCP

Общие Маршрутизаторы WCCP Способ назначения

Включено: ☒

Название: Client-Server

Описание:

Пароль: *****

Способ перенаправления трафика: GRE

Способ возврата трафика: GRE

Сервисная группа: 80

Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу

Приоритет: 240

Порты для перенаправления: 80, 443

Порты для перенаправления через запятую, т.е. 80, 443

☐ Порт источника

Протокол: TCP

Сохранить Отмена

Свойства сервисной группы WCCP

Общие Маршрутизаторы WCCP Способ назначения

Маршрутизаторы WCCP

добавить редактировать удалить

Название списка	Владелец
IP 192.168.55.100	

Создать и добавить новый объект

Сохранить Отмена

Свойства сервисной группы WCCP

Общие Маршрутизаторы WCCP Способ назначения

Хэш

Хэш: ☒ IP источника ☐ Порт источника ☐ IP назначения ☐ Порт назначения

Альтернативный хэш: ☐ IP источника ☐ Порт источника ☐ IP назначения ☐ Порт назначения

Маска

Схема маскирования: IP источника

Значение маски:

Маска может быть длиной 16 бит для схемы маскирования по порту, и 32 бита для схемы маскирования по IP-адресу. Укажите значение в шестнадцатичном формате, например: EFEF

Сохранить Отмена

В свойствах сервисной группы WCCP для перенаправления ответов сервера в клиентскую сеть необходимо указать следующие значения параметров:

- Сервисная группа: 90
- Приоритет: 240
- Способ перенаправления трафика: GRE.
- Способ возврата трафика: GRE.
- Маршрутизатор WCCP: 192.168.55.100
- Порт для перенаправления: 80, 443
- Протокол: TCP.
- Порт источника: True
- Хэш: IP назначения.

Свойства сервисной группы WCCP

Общие Маршрутизаторы WCCP Способ назначения

Включено: ☒

Название: Server-Client

Описание:

Пароль: *****

Способ перенаправления трафика: GRE

Способ возврата трафика: GRE

Сервисная группа: 90

Числовой идентификатор сервисной группы. Идентификатор сервисной группы должен быть одинаков на всех устройствах, входящих в группу

Приоритет: 240

Порты для перенаправления: 80, 443

Порты для перенаправления через запятую, т.е. 80, 443

☒ Порт источника

Протокол: TCP

Сохранить Отмена

Свойства сервисной группы WCCP

Общие Маршрутизаторы WCCP **Способ назначения**

☒ Хэш

Хэш: ☐ IP источника ☐ Порт источника ☒ IP назначения ☐ Порт назначения

Альтернативный хэш: ☐ IP источника ☐ Порт источника ☐ IP назначения ☐ Порт назначения

☐ Маска

Схема маскирования: IP источника

Значение маски:

Маска может быть длиной 16 бит для схемы маскирования по порту, и 32 для схемы маскирования по IP-адресу. Укажите значение в шестнадцатичном формате, например: EFEF

Сохранить Отмена

Свойства сервисной группы WCCP

Общие Маршрутизаторы WCCP **Способ назначения**

☒ Хэш

Хэш: ☐ IP источника ☐ Порт источника ☒ IP назначения ☐ Порт назначения

Альтернативный хэш: ☐ IP источника ☐ Порт источника ☐ IP назначения ☐ Порт назначения

☐ Маска

Схема маскирования: IP источника

Значение маски:

Маска может быть длиной 16 бит для схемы маскирования по порту, и 32 для схемы маскирования по IP-адресу. Укажите значение в шестнадцатичном формате, например: EFEF

Сохранить Отмена

Установление соединения происходит следующим образом.

1. Инициатором является WCCP-клиент, в данном случае UserGate. Он посылает сообщение «Я здесь», которое говорит о том, что UserGate готов принять пакеты.
2. Cisco подтверждает получение сообщения «Я здесь», отвечая «Я тебя вижу». Сообщение также содержит сообщение о настройках, в частности, поле «Receive ID».
3. UserGate в ответ посылает ещё одно сообщение «Я здесь», в котором содержится поле «Receive ID», со значением, совпадающим с полученным от Cisco. Так UserGate подтверждает готовность работы с маршрутизатором Cisco.
4. После получения сообщения маршрутизатор отправляет запросы, попадающие под условия на UserGate.

Пакеты пользователей, подходящие под условия IP-адреса источника и портов назначения и пакеты от сервера, попадающие под условия IP-адреса назначения и портов источника заворачиваются в GRE туннель; остальные запросы проходят через физические интерфейсы. Все запросы попадают под правила контентной фильтрации и межсетевого экрана: в правилах UserGate не нужно указывать зону, т.к., как было сказано ранее, GRE туннель не имеет зоны.

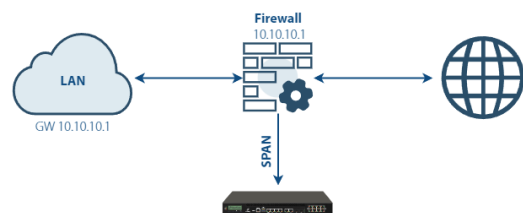
Во вкладке **Дашборд** можно увидеть статистику по этому интерфейсу. Чтобы удалить GRE туннель необходимо выключить WCCP правило.

Поиск неисправностей можно проводить с использованием трафика WCCP на UserGate или оборудовании Cisco и логов на оборудовании Cisco.

Логи с маршрутизатора Cisco выводятся в syslog сервер. Для просмотра используйте следующие команды:

- Для отображения информации о важных событиях, связанных с WCCP-протоколом:
debug ip wccp events
- Для отображения информации о всех пакетах, принятых или отправленных роутером по протоколу WCCP:
debug ip wccp packets
- Для отображения общей информации о WCCP (где 80 и 90 - сервисные группы):
sh ip wccp 80
sh ip wccp 90

KnowledgeBase: ☒
Version: 6.1.8, 6.1.9, 5.x
Product: UserGate NGFW



В конфигурации, представленной выше, устройство UserGate получает копию трафика с какого-либо сетевого оборудования, обладающего возможностью отправить копию трафика на один из своих портов. В данной конфигурации, UserGate может выполнять роль COB (система обнаружения вторжений) и L7.

Для настройки вашего сетевого оборудования в режиме Mirror-порта, обратитесь к соответствующей документации.

Чтобы сконфигурировать UserGate, в режиме COB на Mirror-порте, произведите следующие настройки:

- В главной консоли перейдите в раздел **Сеть → Интерфейсы**.
- Выберите интерфейс и, нажав на кнопку **Редактировать** откройте свойства интерфейса. На вкладке **Общие**, в пункте **Тип интерфейса**, установите значение **Mirror**.
- Активируйте интерфейс, отметив чекбокс **Включено**.

Конфигурация зоны, для этого порта значения не имеет.

Настройка DHCP Relay и особенности работы

Product: NGFW
Version: 5.x, 6.x, 7.x
Technology: Networking

В обычном состоянии сервер DHCP может обслуживать только один широковещательный сегмент сети, это связано со спецификой его работы. Но в некоторых случаях необходимо распространить работу DHCP сервера на другой широковещательный сегмент. В этом случае необходимо использовать DHCP Relay. Рассмотрим один из таких вариантов:

Для настройки DHCP Relay необходимо в свойствах порта port0.301, на вкладке **DHCP-релей** указать адрес DHCP-сервера (192.168.1.2) и адрес UserGate NGFW из vlan 301 (192.168.2.1). Установить флажок **Включено**.

ПримечаниеПри использовании поля Адрес UserGate, unicast-пакеты будут отправлены на DHCP-сервер с этого *src.ip*, также этот адрес будет указан как *relay agent ip address*.

После этого все запросы типа DHCP-Discover и DHCP-Request будут пересылаться из vlan301 в vlan300, а ответы DHCP сервера будут пересылаться из vlan300 в vlan301.

ПримечаниеВ настройках DHCP Relay адрес должен быть из сетей, которые назначены на интерфейс, иначе DHCP Relay не будет иметь информации, куда должен быть отправлен DHCP-Offer.

Важно!Необходимо, чтобы у DHCP-сервера шлюзом по умолчанию был UserGate NGFW, либо был прописан маршрут в сеть vlan301 с UserGate NGFW в качестве шлюза к этой сети. DHCP-сервер в ответ должен отправить unicast-запрос, с адресом назначения DHCP Relay, для этого ему и нужен маршрут.

ПримечаниеНомера vlan на схеме и в статье взяты для примера и могут быть любыми в диапазоне 1 — 4094

ПримечаниеЕсли настроен кластер отказоустойчивости, работающий в режиме «активный — пассивный», и необходимо использовать отказоустойчивый DHCP Relay, для корректной передачи DHCP-пакетов между клиентом и сервером на каждом узле кластера в окне свойств соответствующего интерфейса на вкладке «DHCP-релей» в поле «Адрес UserGate» нужно указать кластерный виртуальный IP-адрес.

Product: UserGate NGFW
Version: 6.1.8, 6.1.9

В данном разделе рассматривается пример настройки подключения к провайдеру по BGP при использовании кластера Актив-Пассив.

Настройка отказоустойчивого кластера

UserGate поддерживает настройку кластера отказоустойчивости для обеспечения бесперебойной работы сети. Кластер отказоустойчивости может работать в двух режимах Актив-Актив и Актив-Пассив. Оба режима поддерживают синхронизацию пользовательских сессий, что обеспечивает прозрачное для пользователей переключение трафика с одного узла на другие.

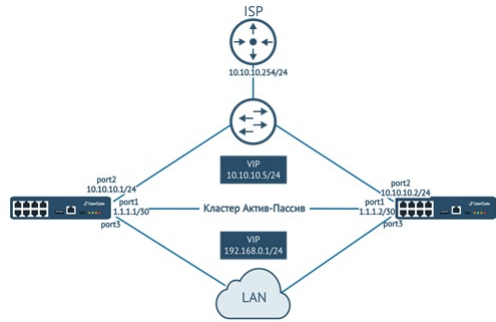
В данной схеме, устройства UserGate настроены в режиме отказоустойчивого кластера по схеме Актив-Пассив. В данном режиме один из серверов выступает в роли Мастер-узла, обрабатывающего трафик, а остальные - в качестве резервных. На каждом из узлов кластера выбраны сетевые интерфейсы, которым администратор назначил виртуальные IP-адреса. Между этими интерфейсами происходит обмен сообщениями - VRRP-объявления, с помощью которых узлы обмениваются информацией о своём состоянии.

При переходе роли мастер-узла на резервный сервер происходит перенос всех виртуальных IP-адресов всех кластерных интерфейсов. Безусловный переход роли происходит при следующих событиях:

- Запасной сервер не получает подтверждения о том, что главный узел находится в сети, например, главный узел выключен или отсутствует сетевая доступность узлов.
- На узле настроена проверка доступа в Интернет, и доступ в Интернет отсутствует через все имеющиеся шлюзы.
- Сбой в работе ПО UserGate.

Подробнее о работе кластера читайте в [UserGate 6. Руководство администратора](#).

Принципиальная схема сети будет выглядеть следующим образом:



Как видно, схема содержит два устройства UserGate, подключённых к коммутатору через интерфейс **port2**; интерфейсы **port1** используются для создания кластера; к интерфейсам **port3** подключена локальная сеть (LAN). Для интерфейсов **port2** и **port3** использованы виртуальные интерфейсы, полученные по протоколу VRRP.

Настройка UserGate.

Считается, что кластер в режиме Актив-Пассив уже настроен; в данном примере рассмотрена настройка BGP.

BGP (Border Gateway Protocol) - динамический протокол маршрутизации, относится к классу протоколов маршрутизации внешнего шлюза (англ. EGP - Exterior 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 внутрисетевой 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 (подробнее о BGP читайте в [UserGate 6. Руководство администратора](#)).

1. Перейдите в раздел **Сеть → Виртуальные маршрутизаторы** нажмите **Добавить** и выберите **BGP**. Далее задайте параметры пиринга. Во вкладке **BGP-маршрутизатор**:
 - Чекбокс **Включено**.
 - **Идентификатор маршрутизатора**: 10.10.10.1
 - **Номер автономной системы (AS)**: 65001

Во вкладке **Сети** укажите IP-адрес белой подсети.

Во вкладке **Routemaps** нажмите **Добавить** и укажите следующие параметры:

- **Название**.
- **Описание** (опционально).
- **Действие**: Разрешить.
- **Сравнивать по**: IP.
- **Установить next hop**: 10.10.10.5 (виртуальный IP-адрес в сторону провайдера).

Далее в свойствах route-map перейдите во вкладку **IP-адреса** и укажите IP-адрес белой подсети.

Остальные параметры можно оставить без изменений. Данная настройка необходима для передачи провайдеру информации об узле (мастер-узле), на который необходимо отправлять пакеты для нашей сети.

Сохраните настройки route-map и перейдите во вкладку **BGP-соседи** свойств виртуального маршрутизатора. Нажмите **Добавить** и во вкладке **Общие** укажите необходимые данные:

- Чекбокс **Включено**.
- **Host**: 10.10.10.254 (необходимо указать IP-адрес интерфейса оборудования провайдера).
- **Удалённая ASN**: номер AS провайдера.

Далее перейдите во вкладку **Route-maps** и отметьте чекбокс **out** созданного ранее route-map. Сохраните настройки BGP-маршрутизатора.

2. Перейдите в раздел **Сеть** → **Зоны**. В свойствах зоны интерфейса port2 во вкладке **Контроль доступа** отметьте чекбокс **BGP**.

Далее, аналогично, необходимо настроить второе устройство UserGate. После настройки UserGate со стороны маршрутизатора провайдера можно просмотреть краткую информацию о BGP и таблицу маршрутизации с использованием следующих команд:

```
Router#sh bgp summ
<вывод пропущен...>
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 4 65001 29 32 3 0 0 00:25:27 1
10.10.10.2 4 65001 29 33 3 0 0 00:25:29 1

Router#sh ip ro bgp
<вывод пропущен...>
<ваша белая подсеть>/28 is subnetted, 1 subnets
B <ваша белая подсеть> [20/10] via 10.10.10.5, 00:26:04
```

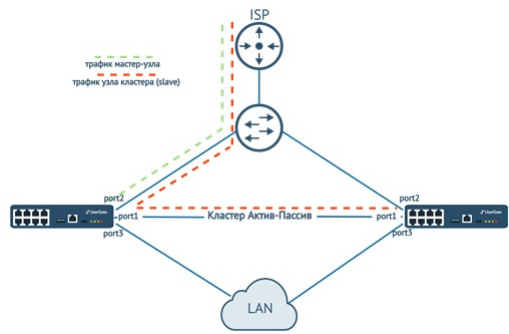
Адрес 10.10.10.5 является виртуальным и всегда находится на узле кластера, назначенном мастером.

Настройка доступа в интернет на кластерах узла

Примечание Т.к. маршрутизатор провайдера видит маршруты только до мастер-узла, другие узлы кластера UserGate не будут иметь выхода в сеть Интернет. Доступ в Интернет необходим на всех узлах UserGate для периодической проверки лицензий и скачивания различных обновлений. Далее представлены 2 варианта сетевых настроек, которые с помощью которых можно настроить доступ в Интернет на узлах кластера.

Первый вариант

предполагает использование мастер-узла (master) для проксирования доступа в Интернет для других узлов кластера (slave).



ПримечаниеСетевые настройки являются уникальными для каждого узла кластера и не синхронизируются, т.е. каждый узел кластера настраивается индивидуально.

Для настройки перейдите в раздел **Сеть → Шлюзы** и добавьте второй шлюз с IP-адресом кластерного интерфейса соседнего узла (т.е. на узле А добавьте адрес узла В; на узле В - адрес узла А). Далее необходимо включить **Проверка сети** (для этого необходимо нажать на одноимённую кнопку). В открывшемся окне:

- Отметьте чекбокс **Включено**.
- Укажите проверочный хост в Интернете (узлы кластера будут проверять доступность хоста, посылая ICMP-пакеты).

Свойства проверки сети

Включено:

☒

Частота проверки:

10

(В секундах, допустимые значения: 10-300)

Процент неудачных запросов:

70

(%, допустимые значения: 1-100)

Добавить

Редактировать

Удалить

IP-адрес

8.8.8.8

Сохранить

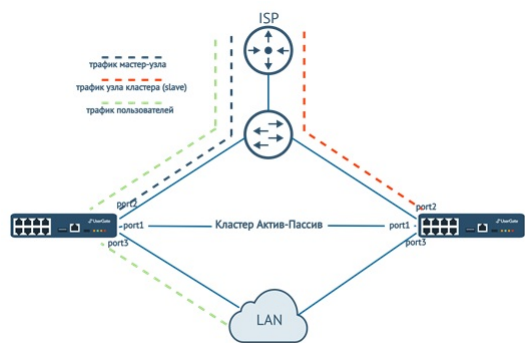
Отмена

ПримечаниеДанное решение предполагает использование белых адресов на внешних интерфейсах всех узлов кластера, чтобы проверка сети проходила даже при отсутствии виртуального адреса.

При такой настройке узел кластера (slave) будет производить проверку доступности тестового адреса в Интернете. Т.к. напрямую ответы от удалённого хоста доходить до узла не будут, узел переключит шлюз по умолчанию на следующий указанный в списке шлюз, т.е. на адрес кластерного интерфейса мастер-узла. Так узел сможет проверять лицензию и наличие доступных обновлений. Также для работы такой схемы необходима корректная настройка правил межсетевого экрана - мастер-узел не должен блокировать трафик от другого узла кластера.

Второй вариант

позволяет работать с кластерами, содержащими более двух узлов, но требует несколько адресов в стыковочной сети и белых адресов. В данном способе будут опубликованы BGP-маршруты на маршрутизаторы провайдера, специфичные для всех узлов кластера. Т.е. удаленному маршрутизатору будут указаны пути до всех устройств кластера напрямую и, дополнительно, путь для виртуального адреса, который всегда будет находиться на мастер-узле и на который будет возвращаться ответный трафик пользователей, а также который будет использоваться в случае публикации сервисов.



Таким образом, трафик, сгенерированный на самих устройствах, будет маршрутизироваться обратно на эти устройства, а трафик, сгенерированный в пользовательском сегменте и проходящий через кластер, будет маршрутизироваться на виртуальный IP-адрес, который всегда находится на мастер-узле.

Необходимо настроить правила NAT и соответствующие им BGP routemaps. Ниже представлена таблица правил NAT серых адресов в белые.

Зона источника	Серый IP-адрес источника	Зона назначения	Белый IP-адрес
Trusted	Any	Untrusted	WhiteIP 1
Any	10.10.10.1	Untrusted	WhiteIP 2
Any	10.10.10.2	Untrusted	WhiteIP 3

Для настройки правил NAT необходимо перейти в раздел **Политики сети → NAT и маршрутизация**. Правила NAT настроены таким образом, что если трафик сгенерирован в условной зоне Trusted (т.е. пользовательский трафик), то локальные адреса преобразуются в виртуальный белый IP-адрес; если зона источника трафика неизвестна (Unknown) и IP-адрес источника трафика равен IP-адресу интерфейса UserGate, то адрес будет преобразован в один из белых IP-адресов согласно таблице выше.

ПримечаниеПорядок правил NAT в списке важен, т.к. исполнение правил происходит сверху вниз и срабатывает первое правило, удовлетворяющее всем заданным условиям.

Указать зону Unknown невозможно, поэтому для срабатывания правил не нужно указывать зону (Any).

Для создания правила NAT, применяемого к пользовательскому трафику, необходимо во вкладке **Общие** указать:

- Чекбокс **Включено**.
- Название** (для примера: NAT for users traffic).
- Описание** (опционально).
- Тип**: NAT.
- SNAT IP (внешний адрес)**: белый IP-адрес.

Свойства правила

Общие Источники Пользователи Назначение Сервис Порт-форвардинг DMZ Network mapping

Включено: ☒

Название: NAT for users traffic

Описание:

Тип: NAT

Шлюз: Пожалуйста, выберите шлюз

Сценарий: Не использовать сценарий

SNAT IP (внешний адрес): WhiteIP1

Журналирование: Нет

Включить лимит журналирования: ☐

Журналирование создаст дополнительную нагрузку на сервер. Не рекомендуется включать журналирование без установки лимитов на большой объем трафика

Ограничить число событий, записываемых в журнал: 3 / час

Максимальное количество пакетов, журналируемых на событие: 5

NAT — Преобразование сетевых адресов. Обычно используется для разрешения доступа из локальной сети в интернет
 DNAT — Перенаправляет трафик на указанный IP-адрес. Обычно используется для публикации внутренних ресурсов в интернет
 Policy-based routing — Позволяет маршрутизировать IP-пакеты на основе расширенной информации, например, сервисов, MAC-адресов или серверов (IP-адресов)
 SNAT IP — Адрес, на который будет заменен адрес источника для трафика NAT
 Порт-форвардинг — Так же, как и DNAT, обычно используется для публикации внутренних ресурсов в интернет, но способен изменять номер порта публикуемого сервиса
 Network mapping — Позволяет произвести замену IP-адресов источника или назначения одной сети на другую сеть

Сохранить Отмена

Во вкладке **Источники**:

- **Зона источника:** Trusted.

Свойства правила

Общие Источники Пользователи Назначение Сервис Порт-форвардинг DMZ Network mapping

Зона источника

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☐ Tunnel inspection zone

☐ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес источника

Добавить Редактировать

Название списка	Владелец
-----------------	----------

Создать и добавить новый объект

☐ Инвертировать

Сохранить Отмена

Во вкладке **Назначение**:

- **Зона назначения:** Untrusted.

Свойства правила

Общие Источники Пользователи Назначение Сервис Порт-форвардинг DMZ Network mapping

Зона назначения

☐ Cluster

☐ DMZ

☐ Management

☐ Trusted

☒ Untrusted

☐ Tunnel inspection zone

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес назначения

Добавить Редактировать

Название списка	Владелец
-----------------	----------

Создать и добавить новый объект

☐ Инвертировать

Сохранить Отмена

Настройка правила NAT в случае, если зона источника трафика неизвестна (Unkown) и IP-адрес источника трафика равен IP-адресу интерфейса UserGate. Во вкладке **Общие** укажите:

- Чекбокс **Включено**.
- **Название** (для примера: origin UserGate1).
- **Описание** (опционально).
- **Тип**: NAT.
- **SNAT IP (внешний адрес)**: белый IP-адрес.

Свойства правила

Общие

Источники

Пользователи

Назначение

Сервис

Порт-форвардинг

DNAT

Network mapping

Включено:

☒

Название:

origin UserGate1

Описание:

Тип:

NAT

Шлюз:

Пожалуйста, выберите шлюз

Сценарий:

Не использовать сценарии

SNAT IP (внешний адрес):

WhiteIP 2

Журналирование:

Нет

Включить лимит журналирования:

☐

Ограничить число событий, записываемых в журнал:

3 / час

Максимальное количество пакетов, журналируемых на событие:

5

Журналирование создаст дополнительную нагрузку на сервер. Не рекомендуется включать журналирование без установки лимитов на большом объеме трафика

NAT — Преобразование сетевых адресов. Обычно используется для разрешения доступа из локальной сети в интернет

DNAT — Перенаправляет трафик на указанный IP-адрес. Обычно используется для публикации внутренних ресурсов в интернет

Policy-based routing — Позволяет маршрутизировать IP-пакеты на основе расширенной информации, например, сервисов, MAC-адресов или серверов (IP-адресов)

SNAT IP — Адрес, на который будет заменен адрес источника для трафика NAT

Порт-форвардинг — Так же, как и DNAT, обычно используется для публикации внутренних ресурсов в интернет, но способен изменять номер порта публикуемого сервиса

Network mapping — Позволяет произвести замену IP-адресов источника или назначения одной сети на другую сеть

Сохранить

Отмена

Во вкладке **Источники**:

- Адрес источника**: список с IP-адресом интерфейса UserGate (список IP-адресов может быть создан в разделе **Библиотеки → IP-адреса** или в свойствах правил нажатием на **Создать и добавить новый объект**).

Свойства правила

Общие

Источники

Пользователи

Назначение

Сервис

Порт-форвардинг

DNAT

Network mapping

Зона источника

☐ Cluster

☐ DMZ

☐ Management

☐ Trusted

☐ Tunnel inspection zone

☐ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес источника

Добавить

Редактировать

Название списка

Владелец

10.10.10.1

вы

Создать и добавить новый объект

☐ Инвертировать

Сохранить

Отмена

Во вкладке **Назначение**:

- Зона назначения**: Untrusted.

Свойства правила

Общие

Источники

Пользователи

Назначение

Сервис

Порт-форвардинг

DNAT

Network mapping

Зона назначения

☐ Cluster

☐ DMZ

☐ Management

☐ Trusted

☒ Tunnel inspection zone

☒ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инвертировать

Адрес назначения

Добавить

Редактировать

Название списка

Владелец

Создать и добавить новый объект

☐ Инвертировать

Сохранить

Отмена

#	Тип	С...	Название	Зона ист...	Адрес исто...	П...	Зона назначения	Адр...	Сер...	DN...	Шл...	С...	Не...
1	NAT	(...)	NAT for users traffic	Trusted	люб/люб	---	Untrusted	люб/люб	люб/люб	---	---	---	---
2	NAT	(...)	origin UserGate1	люб/люб	10.10.10.1	---	Untrusted	люб/люб	люб/люб	---	---	---	---
3	NAT	(...)	origin UserGate2	люб/люб	10.10.10.2	---	Untrusted	люб/люб	люб/люб	---	---	---	---

Далее необходимо опубликовать отдельные IP-адреса.

Перейдите в раздел **Сеть → Виртуальные маршрутизаторы** и настройте BGP-маршрутизатор (настройка аналогична представленной выше).

Во вкладке **Сети** свойств виртуального маршрутизатора укажите белые IP-адреса (WhiteIP 1, WhiteIP 2, WhiteIP 3).

Во вкладке **Routemaps** укажите следующие карты

Свойства виртуального маршрутизатора

BGP

BGP-маршрутизатор

Сети

Routemaps

Фильтры

BGP-соседи

Добавить

Редактировать

Удалить

Название	Действие	Условия
directly_to_10.1	Разрешить	White IP 2/32:0:0
directly_to_10.2	Разрешить	White IP 3/32:0:0
to_VIP_10.5	Разрешить	White IP 1/32:0:0

Наверх

Выше

Ниже

Вниз

Сохранить

Отмена

Далее включите созданные карты в настройках BGP-соседей, активировав чекбокс **out**.

Свойства соседа

Общие

Аутентификация

Фильтры BGP-соседей

Routemaps

in	out	Название	Действие
☐	☒	directly_to_10.1	permit
☐	☒	directly_to_10.2	permit
☐	☒	to_VIP_10.5	permit

Route maps используются для модификации маршрутизирующей информации, которая передается между доменами

Сохранить

Отмена

После настройки UserGate со стороны маршрутизатора провайдера можно просмотреть BGP-маршруты:

```
Router#sh ip ro bg
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
<вывод пропущен...>
Gateway of last resort is 192.168.2.1 to network 0.0.0.0
<ваша белая подсеть>/32 is subnetted, 3 subnets
B White ip.2 [20/10] via 10.10.10.1, 00:10:47
B White ip.3 [20/10] via 10.10.10.2, 00:10:47
B White ip.1 [20/10] via 10.10.10.5, 00:10:47
```

В результате настроек трафик с NAT IP-адреса, используемого для пользовательского трафика будет отправляться на виртуальный IP-адрес 10.10.10.2.

Настройка мультикаст маршрутизации

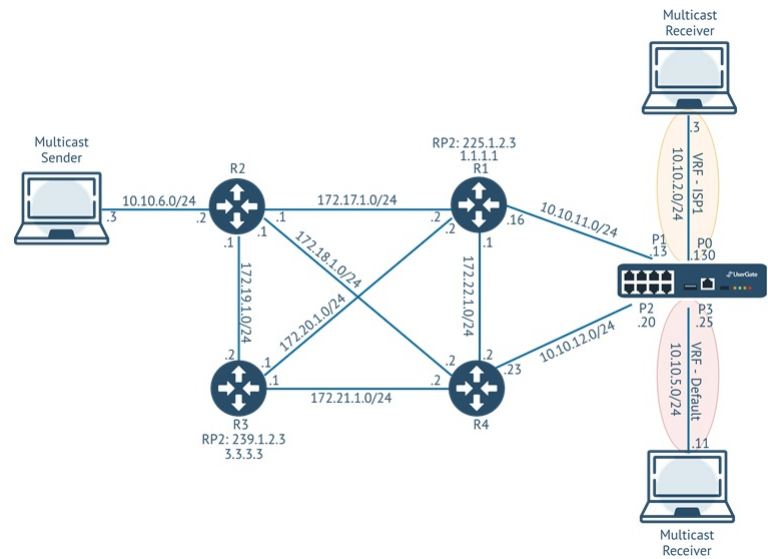
KnowledgeBase:
Product: UserGate NGFW
Version: 6.1.8, 6.1.9

Мультикаст (multicast) - технология широковещательной передачи данных, которая позволяет организовывать одновременную многоадресную рассылку и потоковую передачу данных в режиме реального времени.

Технология IP мультикастинга позволяет существенно сократить объем передаваемого трафика, тем самым обеспечивая рациональное использование пропускной способности, экономию вычислительных возможностей сервера и снижение нагрузки на сеть. Технология является особенно эффективной для доставки голосового и видео трафика, т.к. позволяет доставлять единый поток информации к тысячам потребителей.

Мультикаст маршрутизация позволяет доставлять трафик к группе хостов - мультикаст-группе, которая идентифицируется групповым адресом. Хосты (получатели), которые хотят получать данный трафик должны присоединиться к соответствующей мультикаст-группе по протоколу IGMP (Internet Group Management Protocol). Подробнее о технологии читайте в [UserGate 6. Руководство администратора](#).

По представленной схеме произведём настройку мультикаст маршрутизации по протоколу маршрутизации многоадресных сообщений PIM-SM (Protocol Independent Multicast Sparse Mode) протокола с использованием протокола динамической маршрутизации OSPF для unicast пакетов.



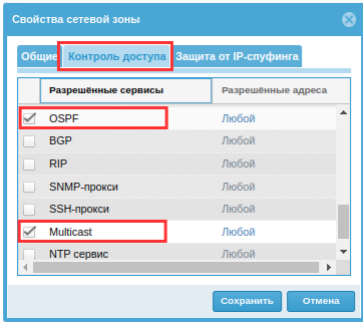
Сначала происходит установка соседства между маршрутизаторами путём отправки Hello сообщений (сообщение отправляется всем соседям, кроме того, от кого был получен данный пакет). Остальные мультикаст маршрутизаторы повторяют данный процесс. Путь, который прошёл мультикаст пакет от источника до конечных получателей, образует дерево, которое называется — source-based distribution tree, shortest-path tree (SPT), source tree.

При запуске на сервере приложения с поддержки мультивещания, оно посылает в сеть уведомление, что соответствующая группа доступна для присоединения. Клиент, который хочет присоединиться к группе, посылает об этом уведомление. Все промежуточные маршрутизаторы записывают, что за соответствующим маршрутом есть клиент соответствующей мультикаст-группы.

После получения данных об отправителе и получателе трафика на роутерах формируются таблицы мультикаст маршрутизации. Для обеспечения актуальности информации о источнике и получателе трафика используется точки rendezvous Rendezvous Point — RP благодаря которым происходит связность источника с приемниками трафика. Запрос роутерами мультикастового трафика выполняется с помощью сообщения PIM Join. В начале весь мультикаст трафик идёт через RP, но после определения более короткого пути трафик пойдёт по нему.

Настройка UserGate.

- 1. В разделе **Сеть → Зоны** во вкладке **Контроль доступа** необходимо разрешить OSPF и Multicast.



- 2. Произвести настройку виртуальных маршрутизаторов в разделе **Сеть → Виртуальные маршрутизаторы**.

Настройка Default VRF.

- OSPF:
- Идентификатор маршрутизатора: 10.10.12.20.
 - Redistribute: connected.
 - Интерфейсы: port 2, port 3.
 - Области: area 1.

- Мультикаст маршрутизатор:
- Port 2: отключить чекбокс IGMP.
 - Port 3: включить чекбокс IGMP.

Настройка ISP1.

- OSPF:
- Идентификатор маршрутизатора: 10.10.11.13.
 - Redistribute: connected.
 - Интерфейсы: port 0, port 1.
 - Области: area 1.

- Мультикаст маршрутизатор:
- Port 0: включить чекбокс IGMP.
 - Port 1: отключить чекбокс IGMP.
 - IP-адрес Rendezvous points: 1.1.1.1.

- 3. В разделе **Политики сети → Межсетевой экран** настроить разрешающее правило, указав IP-адреса назначения 225.1.2.3 и 239.1.2.3.

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Включено: ☒

Название: Allow RP

Описание:

Действие: Разрешить

Отбросить и:

Сценарий: Не использовать сценарии

Журналирование: Нет

Включить лимит журналирования:

Ограничить число событий, записываемых в журнал:

Максимальное количество пакетов, журналируемых на событие:

Применить правило к: Все пакеты

Вставить: Вниз списка правил

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Зона назначения:

Адрес назначения:

Редактирование списка IP-адресов

Название списка: RP

Описание: Нет

URL обновления: Нет

IP-адреса:

225.1.2.3

239.1.2.3

Страница 1 из 1

Найти:

Закрыть

Настройка маршрутизаторов Cisco.

Далее будут представлены настройки маршрутизаторов R1, R2, R3 и R4.

Для маршрутизатора R1 с использованием следующей команды включить мультикаст маршрутизацию.

```
ip multicast-routing
```

Далее необходимо создать логический Loopback Interface с адресом 1.1.1.1 и настроить режим PIM-SM.

```
interface Loopback1
ip address 1.1.1.1 255.255.255.255
ip pim sparse-mode
```

С использованием следующих команд производится настройка интерфейсов Fast Ethernet 1/0, Fast Ethernet 1/1, Fast Ethernet 2/0 и Fast Ethernet2/1: им присваиваются соответствующие IP-адреса, настраивается использование режима PIM-SM и автоматическое согласование скорости и дуплексного режима.

```
interface FastEthernet1/0
ip address 10.10.11.16 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet1/1
ip address 172.17.1.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/0
ip address 172.22.1.1 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/1
ip address 172.20.1.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
```

Далее необходимо настроить протокол OSPF на маршрутизаторе, чтобы роутеры могли постоянно обмениваться информацией про известные маршруты и состояние соединений (где 1 — это идентификатор процесса для маршрутизатора):

```
router ospf 1
router-id 1.1.1.1
```

Также можно включить журналирование протокола и перераспределение маршрутизатором всех подключённых сетей:

```
log-adjacency-changes
redistribute connected subnets
```

Далее указываются сети, которые маршрутизатор будет транслировать в другие сети:

```
network 10.10.11.0 0.0.0.255 area 1
network 172.17.1.0 0.0.0.255 area 1
network 172.20.1.0 0.0.0.255 area 1
network 172.22.1.0 0.0.0.255 area 1
```

Далее задаются RP и указываются их IP-адреса:

```
ip pim rp-address 1.1.1.1 RP1
ip pim rp-address 3.3.3.3 RP2
```

С использованием следующих команд создаются именованные списки доступа, которые разрешают трафик с адресов 225.1.2.3 (RP1) и 239.1.2.3 (RP2).

```
ip access-list standard RP1
permit 225.1.2.3
```

```
ip access-list standard RP2>
permit 239.1.2.3
```

Настройка маршрутизаторов R2, R3 и R4 производится аналогично.

Конфигурация R2:

```
ip multicast-routing>
interface Loopback1
ip address 2.2.2.2 255.255.255.255>
ip pim sparse-mode
interface FastEthernet1/0
ip address 172.17.1.1 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet1/1
ip address 172.19.1.1 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/0
ip address 172.18.1.1 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/1
ip address 10.10.6.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
redistribute connected subnets
network 172.17.1.0 0.0.0.255 area 1
network 172.18.1.0 0.0.0.255 area 1
network 172.19.1.0 0.0.0.255 area 1
ip pim rp-address 1.1.1.1 RP1
ip pim rp-address 3.3.3.3 RP2
ip access-list standard RP1
permit 225.1.2.3
ip access-list standard RP2
permit 239.1.2.3
```

Конфигурация R3:

```
nip multicast-routing
interface Loopback1
ip address 3.3.3.3 255.255.255.255
ip pim sparse-mode
interface FastEthernet1/0
ip address 172.21.1.1 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet1/1
ip address 172.19.1.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/0
ip address 172.20.1.1 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/1
no ip address
ip pim sparse-mode
duplex auto
speed auto
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
redistribute connected subnets
network 172.19.1.0 0.0.0.255 area 1
network 172.20.1.0 0.0.0.255 area 1
network 172.21.1.0 0.0.0.255 area 1
ip pim rp-address 1.1.1.1 RP1
ip pim rp-address 3.3.3.3 RP2
ip access-list standard RP1
permit 225.1.2.3
ip access-list standard RP2
permit 239.1.2.3
```

Конфигурация R4:

```
ip multicast-routing
interface Loopback1
ip address 4.4.4.4 255.255.255.255
ip pim sparse-mode
interface FastEthernet1/0
ip address 172.22.1.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet1/1
ip address 172.21.1.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/0
ip address 172.18.1.2 255.255.255.0
ip pim sparse-mode
duplex auto
speed auto
interface FastEthernet2/1
ip address 10.10.12.23 255.255.255.0
ip pim sparse-mode
ip igmp query-interval 125
duplex auto
speed auto
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
redistribute connected subnets
network 10.10.12.0 0.0.0.255 area 1
network 172.18.1.0 0.0.0.255 area 1
network 172.21.1.0 0.0.0.255 area 1
network 172.22.1.0 0.0.0.255 area 1
ip pim rp-address 1.1.1.1 RP1
ip pim rp-address 3.3.3.3 RP2
ip access-list standard RP1
permit 225.1.2.3
ip access-list standard RP2
permit 239.1.2.3
```

Если клиент больше не хочет получать мультикаст трафик, то ему необходимо отправить запрос на отсоединение от группы: сообщение PIM Prune.

Выявление ошибок мультикаст маршрутизации на оборудовании Cisco.

С использованием команды show ip pim neighbor

на оборудовании Cisco можно посмотреть список соседних мультикаст маршрутизаторов.

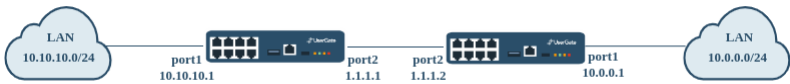
```
R1#sh ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority, S - State Refresh Capable
Neighbor Interface Uptime/Expires Ver DR
Address Prio/Mode
10.10.11.13 FastEthernet1/0 1d22h/00:01:28 v2 1 /
172.17.1.1 FastEthernet1/1 1d22h/00:01:23 v2 1 / S P
172.22.1.2 FastEthernet2/0 1d22h/00:01:35 v2 1 / DR S P
172.20.1.1 FastEthernet2/1 1d22h/00:01:15 v2 1 / S P
```

Команда show ip mroute отобразит мультикаст маршрут.

```
R1#sh ip mroute 225.1.2.3
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected, L - Local, P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running, A - Candidate for MSDP Adv
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 225.1.2.3), 1d22h/00:03:03, RP 1.1.1.1, flags: S - есть отправитель трафика
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
FastEthernet1/0, Forward/Sparse, 00:01:01/00:03:03
FastEthernet1/1, Forward/Sparse, 01:06:06/00:02:51
(10.10.6.3, 225.1.2.3), 1d22h/00:03:22, flags: T - есть получатель трафика
Incoming interface: FastEthernet1/1, RPF nbr 172.17.1.1
Outgoing interface list:
FastEthernet1/0, Forward/Sparse, 00:00:30/00:03:03
```

Настройка статической маршрутизации

KnowledgeBase: 
Product: UserGate NGFW
Version: 6.1.8, 6.1.9



Необходимо настроить статическую маршрутизацию между подсетями с IP-адресами 10.10.10.0/24 и 10.0.0.0/24.

Для добавления статического маршрута перейдите в раздел **Сеть → Виртуальный маршрутизаторы**. Далее можно создать виртуальный маршрутизатор или использовать маршрутизатор, созданный по умолчанию (виртуальный маршрутизатор по умолчанию).

Чтобы создать виртуальный маршрутизатор нажмите Добавить. Во вкладке Общие свойств виртуального маршрутизатора задайте:

- **Название** виртуального маршрутизатора.
- **Описание** (опционально).
- **Имя узла**: если узел входит в состав кластера, выберите узел, на котором будет создан виртуальный маршрутизатор.

Перейдите во вкладку **Интерфейсы** и выберите интерфейсы, которые необходимо добавить в виртуальный маршрутизатор (интерфейсы, добавленные в другие виртуальные маршрутизаторы, не могут быть добавлены; интерфейс может принадлежать только одному виртуальному маршрутизатору):

Дальнейшая настройка UserGate не зависит от того, какой виртуальный маршрутизатор используется (виртуальный маршрутизатор по умолчанию или созданный вами).

Откройте свойства маршрутизатора и выберите **Статические маршруты**.

Далее нажмите **Добавить** и заполните необходимые поля:

- Отметьте чекбокс **Включено**.
- **Название** статического маршрута.
- **Описание** (опционально).
- **Тип маршрута**: выберите необходимый тип маршрута:
 - **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).
- **Адрес назначения**: укажите IP-адрес сети назначения маршрута (в примере 10.0.0.0/24).
- **Шлюз**: укажите IP-адрес шлюза, через который будет доступна указанная ранее подсеть. Указанный IP-адрес должен быть доступен с сервера UserGate (в примере: 1.1.1.2).
- **Интерфейс**: укажите интерфейс, через который будет добавлен маршрут. Можно оставить значение **Автоматически**, тогда UserGate самостоятельно определит интерфейс исходя из сетевых настроек.
- **Метрика**: если маршрутов в данную сеть несколько, то задайте метрику маршрута: чем меньше метрика, тем приоритетней маршрут.

Свойства маршрута

Включено: ☒

Название: to 10.0.0.0/24

Описание:

Тип: unicast

Адрес назначения: 10.0.0.0/24

Шлюз: 1.1.1.2

Интерфейс: Автоматически

Метрика: 0

Сохранить Отмена

Аналогично, добавьте маршрут на другом узле UserGate, изменив **Адрес назначения** (на 10.10.10.0/24) и **Шлюз** (на 1.1.1.1).

Свойства маршрута

Включено: ☒

Название: to 10.10.10.0/24

Описание:

Тип: unicast

Адрес назначения: 10.10.10.0/24

Шлюз: 1.1.1.1

Интерфейс: Автоматически

Метрика: 0

Сохранить Отмена

Просмотр добавленных маршрутов доступен во вкладке **Диагностика и мониторинг** в разделе **Мониторинг** → **Маршруты**.

На первом узле (для настройки использовался виртуальный маршрутизатор по умолчанию):

Узел: utmcore@leaerointale Виртуальный маршрутизатор:

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
F - PBR, f - OpenFabric,
> - selected route, * - FIB route, q - queued route, r - rejected route

VRF default

VRF default:

K>* 0.0.0.0/0 [0/0] via 192.168.117.1, port0, 05:53:57

K>* 10.0.0.0/24 [0/0] via 1.1.1.2, port2, 01:40:22

На втором узле (для настройки использовался виртуальный маршрутизатор по умолчанию):

Узел: utmcore@b Виртуальный маршрутизатор:

Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
F - PBR, f - OpenFabric,
> - selected route, * - FIB route, q - queued route, r - rejected route

VRF default

VRF default:

K>* 0.0.0.0/0 [0/0] via 192.168.117.1, port0, 05:31:52

K>* 10.10.10.0/24 [0/0] via 1.1.1.1, port2, 01:35:29

Как видно из рисунков, представленных выше, UserGate самостоятельно определил интерфейс, через который был добавлен маршрут.

Проверка корректности настройки статической маршрутизации между подсетями производилась с помощью утилиты ping (вкладка **Диагностика и мониторинг** раздел **Сеть** → **Ping**):

Ping

Настройка ping

Ping host: 10.0.0.1 TTL: 30 Интерфейс: 10.10.10.1 (port1) Старт Сброс

Счётчик: 6 ☐ Показывать временные метки ☐ Не резолвить имена

Выход ответа

PING 10.0.0.1 (10.0.0.1) from 10.10.10.1 : 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.548 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.284 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.439 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.424 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.416 ms

--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4077ms
rtt min/avg/max/mdev = 0.284/0.422/0.548/0.084 ms

Для прохождения трафика между локальными сетями необходимо настроить правило межсетевого экрана. Для этого перейдите в раздел **Политики сети** → **Межсетевой экран**, нажмите **Добавить** и укажите во вкладке **Общие**:

- **Название** правила межсетевого экрана.
- **Действие**: Разрешить.

Во вкладке **Источник** укажите зону источника **Trusted**; во вкладке **Назначение** - зону **Untrusted**.

Можно использовать правило, созданное по умолчанию, **Allow trusted to Untrusted**.

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Включено: ☒

Название: Allow trusted to untrusted

Описание: Firewall rule which allows traffic from Trusted zone to Untrusted zone. This is an example rule which can be changed or deleted if necessary.

Действие: ☒ Разрешить

Отбросить и: Не выбран

Сценарий: Не использовать сценарии

Журналирование: Нет

Включить лимит журналирования: ☒

Ограничить число событий, записываемых в журнал: 3 / час

Максимальное количество пакетов, журналируемых на событие: 5

Применить правило к: Все пакеты

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Исходная зона

☐ Cluster

☐ DMZ

☐ Management

☒ Trusted

☐ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инvertировать

Адрес источника

Добавить Редактировать

Владелец

Создать и добавить новый объект

☐ Инvertировать

Сохранить Отмена

Свойства правила межсетевого экрана

Общие Источники Пользователи Назначение Сервис Приложения Время

Зона назначения

☐ Cluster

☐ DMZ

☐ Management

☐ Trusted

☒ Untrusted

☐ VPN for remote access

☐ VPN for Site-to-Site

Если зоны не выбраны, то подразумевается "любая зона"

Создать и добавить новый объект

☐ Инvertировать

Адрес назначения

Добавить Редактировать

Владелец

Создать и добавить новый объект

☐ Инvertировать

Сохранить Отмена

Если необходимо разрешить прохождение трафика между виртуальными маршрутизаторами, то необходимо в статических маршрутах виртуального маршрутизатора добавить маршрут, указав сеть назначения и интерфейс устройства UserGate, через который данная сеть доступна.

Для примера создадим виртуальный маршрутизатор **test** и добавим интерфейс port3, к которому подключена LAN с IP-адресом 10.10.0.0/24.



Чтобы разрешить трафик между двумя виртуальными маршрутизаторами, необходимо создать маршруты со следующими параметрами.

В виртуальном маршрутизаторе по умолчанию:

- **Адрес назначения:** укажите IP-адрес сети назначения (в примере 10.10.0.0/24).
- **Шлюз:** шлюз не указывается.
- **Интерфейс:** укажите интерфейс, через который будет добавлен маршрут (в примере **port3**).

Свойства маршрута

Включено: ☒

Название: to test

Описание:

Тип: unicast

Адрес назначения: 10.10.0.0/24

Шлюз:

Интерфейс: port3

Метрика: 0

Сохранить

Отмена

В виртуальном маршрутизаторе **test**:

- **Адрес назначения**: укажите IP-адрес сети назначения (в примере 10.10.10.0/24).
- **Шлюз**: шлюз не указывается.
- **Интерфейс** укажите интерфейс, через который будет добавлен маршрут (в примере **port1**).

Свойства маршрута

Включено: ☒

Название: to 10.10.10.0/24

Описание:

Тип: unicast

Адрес назначения: 10.10.10.0/24

Шлюз:

Интерфейс: port1

Метрика: 0

Сохранить

Отмена

В разделе **Политики сети** → **Межсетевой экран** необходимо настроить правило, разрешающее трафик из зоны интерфейса **port1** в зону интерфейса **port3** (в примере из зоны **Trusted** в зону **Trusted**).

Проверка прохождения трафика между устройствами локальных сетей 10.10.10.0/24 и 10.10.0.0/24:

```
S ping 10.10.0.7 -c 4
PING 10.10.0.7 (10.10.0.7) 56(84) bytes of data.
64 bytes from 10.10.0.7: icmp_seq=1 ttl=63 time=0.748 ms
64 bytes from 10.10.0.7: icmp_seq=2 ttl=64 time=0.505 ms
64 bytes from 10.10.0.7: icmp_seq=3 ttl=64 time=0.459 ms
64 bytes from 10.10.0.7: icmp_seq=4 ttl=64 time=0.558 ms

--- 10.10.0.7 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt: min/avg/max/mdev = 0.459/0.567/0.748/0.169 ms
```

