

Table of Contents

Table of Contents	1
Маршрутизация	2
Не создается виртуальный маршрутизатор	3
Маршрутизация при использовании явного прокси	4
Не удаётся создать 2 моста L2 и L3 на одном устройстве	5
Кластер Актив-Пассив не использует виртуальный адрес для отправки трафика	6
Объединение нескольких сетей с помощью VPN site-to-site	7
Недоступны сервисы при использовании VRF	8

Не создается виртуальный маршрутизатор

Product: UserGate NGFW

Задача

Не создается виртуальный маршрутизатор

Решение

В названии VRF нельзя использовать русские буквы, заглавные буквы, а также оно не должно содержать имена интерфейсов, например port1 или tunnel1. [Подробнее...](#)

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Вопрос

При использования явного прокси будет ли явный прокси использовать для маршрутизации наружу только основной шлюз? Будут ли правила PBR учитываться в работе явного прокси?

Ответ

Правила PBR применяются к соединениям устанавливаемым через явный прокси, IP и зона источника в них также работают. Подробнее об алгоритме обработки трафика в UserGate читайте в статье [UserGate NGFW 6 packet flow](#).

Не удаётся создать 2 моста L2 и L3 на одном устройстве

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: Networking

Задача

Не удаётся создать 2 моста L2 и L3 на одном устройстве.

Решение

Это ограничения архитектуры. Мосты L2 и L3 отличаются возможностью использовать интерфейс моста L3 для исходящего трафика самого устройства и, как недостаток описанного выше, необходимостью иметь на устройстве полную таблицу маршрутизации для проходящего через мост L3 клиентского трафика; использование моста L2 требует также наличия интерфейсов L3 для связи устройства с внешними серверами.

Примечание Работа в режиме Мост ничем не отличается от работы в режиме маршрутизации трафика, но нужно учитывать, что в правилах межсетевого экрана необходимо указать одинаковые зону источника и зону назначения.

Для решения поставленной задачи, т.е. создания аналога конфигурации с мостами L2 и L3 одновременно, необходимо:

1. Создать все мосты как L3.
2. Для мостов, которые должны выполнять функции L2, создать отдельные виртуальные маршрутизаторы.
3. Каждому мосту, выполняющему функции L2, выделить по одному адресу из сетей, в разрыв которых он включен, и создать полную таблицу маршрутизации.

Примечание Схема организации связи не должна быть организована так, чтобы трафик мог проходить через устройство дважды без смены адресов/портов источника/назначения.

Кластер Актив-Пассив не использует виртуальный адрес для отправки трафика

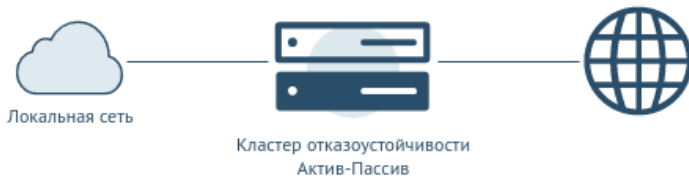
Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: Routing

Задача

Два устройства UserGate NGFW настроены на работу в кластере отказоустойчивости в режиме Актив-Пассив.



Адресация на интерфейсах, использующихся для выхода в Интернет:

- мастер-узел: IP_address1;
- резервный узел: IP_address2;
- виртуальный адрес кластерного интерфейса: IP_address3.

Необходимо произвести настройку, чтобы для отправки трафика в сеть Интернет UserGate использовал виртуальный адрес IP_address3.

Решение

Необходимо настроить правило типа NAT. Для этого перейдите в раздел **Политики сети → NAT и маршрутизация** веб-интерфейса управления, нажмите **Добавить** и укажите следующие условия:

- **Тип:** NAT;
- **SNAT IP:** виртуальный адрес IP_address3;
- **Источник:** зона локальной сети или адреса отдельных устройств, для отправки трафика которых необходимо использовать виртуальный адрес;
- **Назначение:** зона, которой принадлежат внешние интерфейсы.

Объединение нескольких сетей с помощью VPN site-to-site

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: VPN

Задача

Объединить несколько сетей с помощью VPN site-to-site.

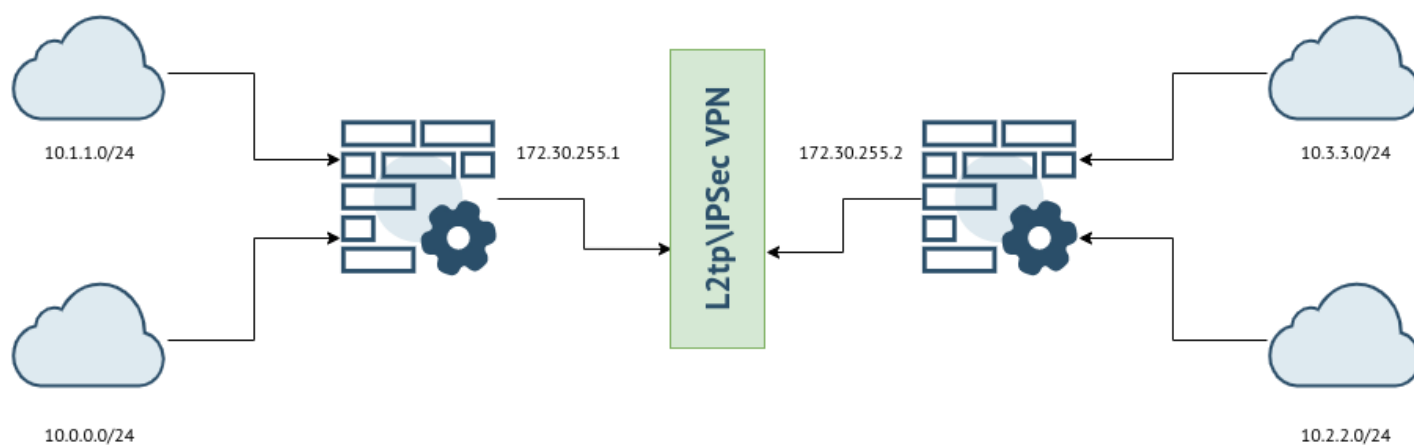
Решение

Для решения этой задачи необходимо настроить VPN туннель между граничными устройствами. В качестве таких устройств могут выступать UserGate NGFW, маршрутизаторы типа MikroTik и др.

Посмотреть настройки VPN site-to-site можно [здесь](#) или [здесь](#).

Внимание! Плохой идеей будет использование разных VPN подключений для каждой сети, при наличии единого маршрутизатора для этих сетей.

После настройки VPN туннеля необходимо будет прописать маршруты для объединяемых сетей. Например, для случая на следующей схеме:



маршруты будут выглядеть следующим образом:

На устройстве с адресом 172.30.255.1:

Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика
for10.2.2.0	unicast	10.2.2.0/24	172.30.255.2	tunnel3	0
for10.3.3.0	unicast	10.3.3.0/24	172.30.255.2	tunnel3	0

На устройстве с адресом 172.30.255.2:

Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика
for10.0.0.0	unicast	10.0.0.0/24	172.30.255.1	tunnel2	0
for10.1.1.0	unicast	10.1.1.0/24	172.30.255.1	tunnel2	0

Где: 172.30.255.1 и 172.30.255.2 - адреса VPN интерфейсов граничных устройств, имена интерфейсов взяты для примера и их нужно поменять соответственно вашей рабочей схеме сети. Метрика - отвечает за приоритет маршрута и может быть любой, в общем случае можно оставить значение 0. Номера сетей вида 10.x.x.x нужно заменить на соответствующие вашей рабочей схеме.

Недоступны сервисы при использовании VRF

Product: UserGate NGFW

Version: 6.x, 7.x

Technology: Routing

Задача

При использовании VRF некоторые сервисы становятся недоступными.

Решение

Чаще всего проблема заключается в маршрутах до искомых сервисов. Надо иметь в виду, что сервисы ПО\HW UserGate запускаются в VRF "Маршрутизаторе по-умолчанию"(Default VRF), и необходимо внимательно следить за передачей маршрутов между виртуальными маршрутизаторами. Маршруты необходимо передавать в обе стороны(прямой и обратный).

