ПОСТРОЕНИЕ ОТКАЗОУСТОЙЧИВЫХ КАНАЛОВ СВЯЗИ НА БАЗЕ ОБОРУДОВАНИЯ MIKROTIK

И. И. Климашевский

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель А. В. Ковалев

Достаточно часто стоит задача объединения филиалов одного предприятия в единую локальную сеть для файлообмена, построения доменной инфраструктуры, функционирования специализированного программного обеспечения. В ряде случаев интернет-провайдеры предоставляют услуги VLAN для реализации подобной задачи. Если же таковой возможности нет, то решением проблемы является построение VPN-тоннелей на собственном оборудовании. В данной работе рассмотрены два основных аспекта – построение тоннелей на основе протокола GRE с использованием шифрования IPSec и решение вопроса с отключением одного из провайдеров.

За основу возьмем оборудование производителя MikroTik, так как оно использует унифицированную систему RouterOS, имеет возможность глубокой настройки и масштабируемости. Рассмотрим ситуацию на примере двух филиалов, при необходимости схема может быть расширена. Для дополнительной надежности будем использовать по два Интернет-провайдера, имеющих внешние статические ip-адреса, со стороны каждого филиала.

Для начала рассмотрим ситуацию объединения филиалов, каждый из которых имеет одного интернет-провайдера. Предположим, что филиал № 1 имеет внешний ip-адрес 10.1.100.1/24, филиал № 2 – 10.1.200.1/24. Назначаем внутреннюю адресацию локальным сетям: для филиала № 1 – 192.168.15.0/24 (шлюз – 192.168.15.1), для филиала № 2 – 192.168.25.0/24 (шлюз – 192.168.25.1). Добавляем транспортную подсеть 172.16.30.0/30 для взаимодействия шлюзов через протокол GRE (рис. 1).

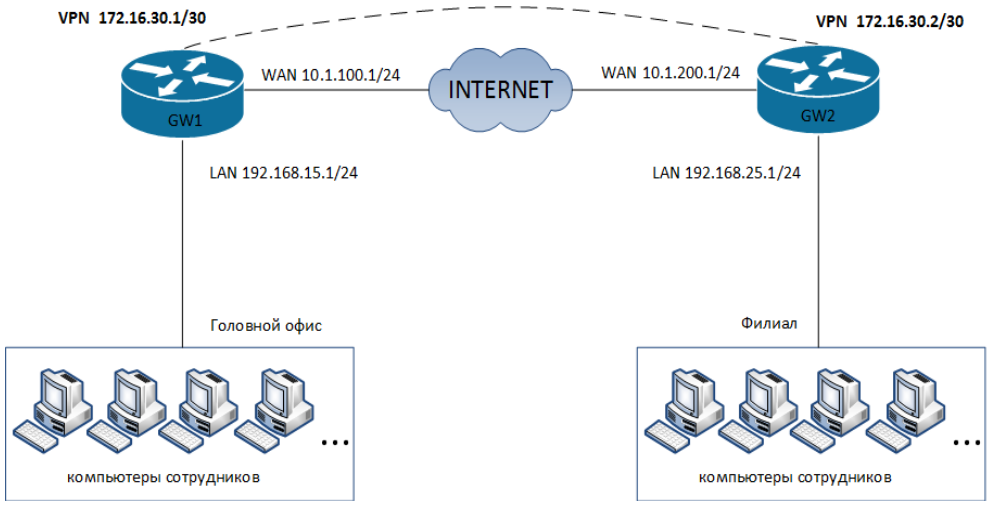

Рис. 1. IP-адресация двух филиалов, имеющих одного Интернет-провайдера с каждой стороны

Велика вероятность отказа одного из провайдеров. При таком раскладе общие ресурсы станут недоступны. С этой целью добавляем дополнительного провайдера с каждой стороны. Дополнительно просчитываем варианты отказа шлюзов на стороне любого филиала и создаем тоннели по принципу соединения «каждый с каждым». В общем виде схема будет выглядеть следующим образом (рис. 2).

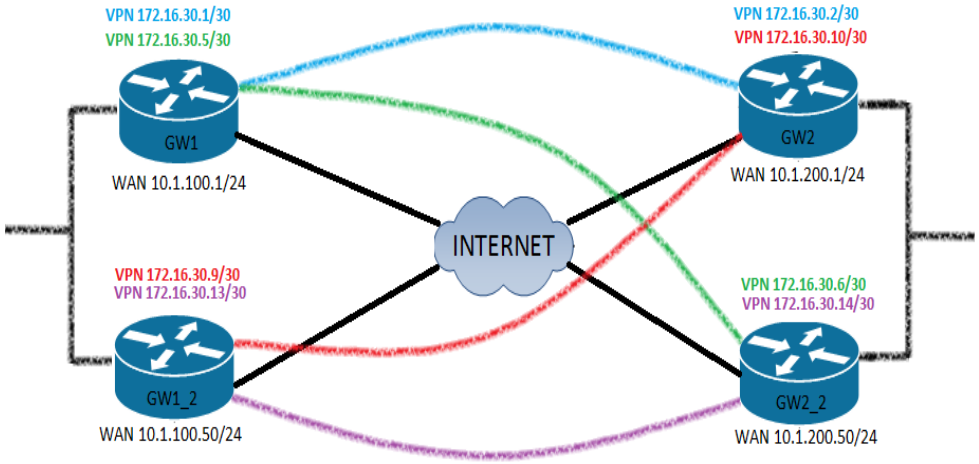

Рис. 2. Модернизация схемы связи филиалов (каждый имеет по два провайдера)

Переходим от теоретической к практической составляющей. Создаем GRE-тоннели на стороне каждого офиса. Пример приведен для одной из сторон (рис. 3, 4). Присваиваем адреса интерфейсам (рис. 5, 6). Добавление маршрутов и расстановка метрики (рис. 7, 8). Метрики маршрутов выставляем в зависимости от того, какой провайдер предоставляет более качественные услуги связи.

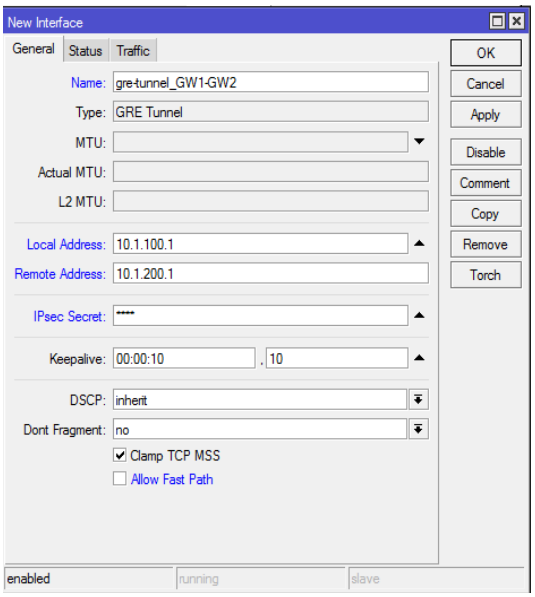

Рис. 3. Заполнение параметров GRE-тоннеля

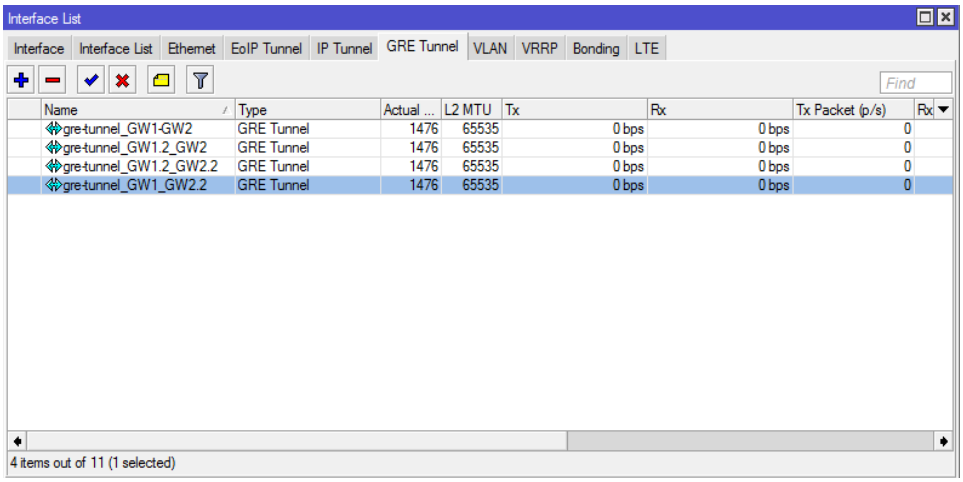

Рис. 4. Созданные тоннели на стороне первого филиала

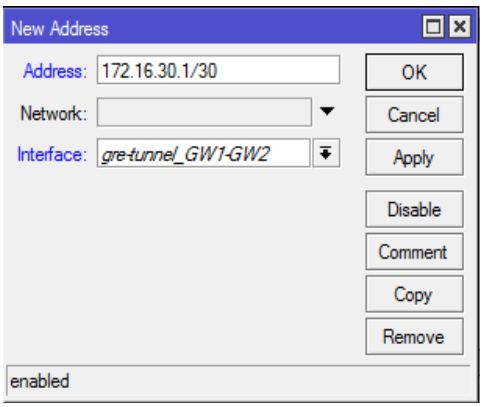

Рис. 5. Назначение ip-адреса интерфейсу транспортной сети филиала № 1

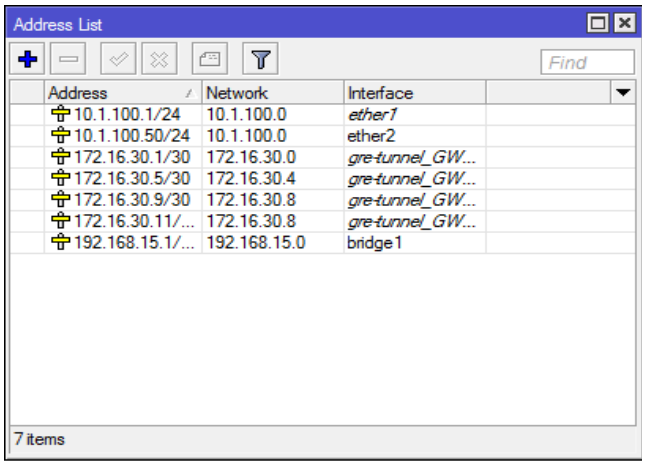

Рис. 6. IP-адреса интерфейсов со стороны первого филиала

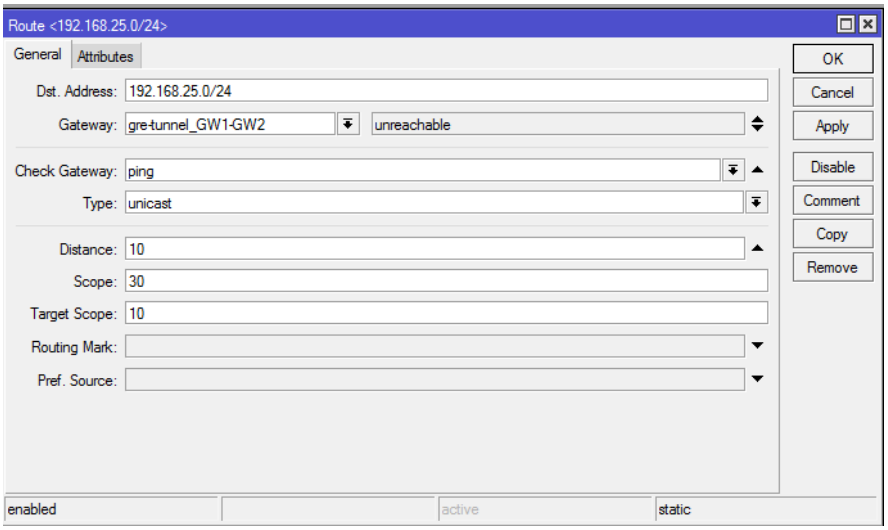

Рис. 7. Добавление маршрута для доступа к ресурсам второго филиала из подсети первого

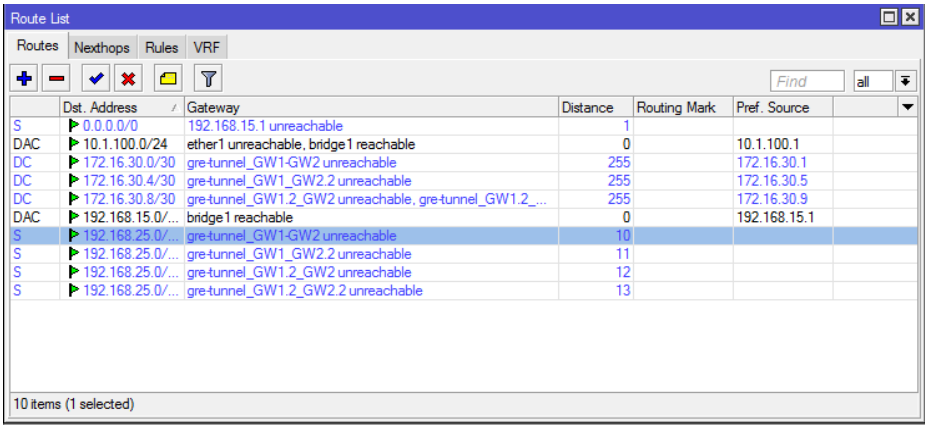

Рис. 8. Общий вид маршрутов со стороны первого филиала с различными метриками

Для того чтобы происходило переключение каналов связи, устройство должно отследить момент отсутствия доступности одного из провайдеров. Существует стандартный способ проверки, когда устройство проверяет доступность ближайшего шлюза. Данный подход имеет существенный недостаток: если модем исправен, а последующий узел нет, то устройство не произведет переключение.

Для решения данной задачи существует другой способ, основанный на встроенной утилите «Netwatch», которая будет один раз в минуту проверять доступность интернета с помощью команды ping до узла 8.8.4.4. Доступность узла будет проверяться исключительно через первый канал, для второго доступ будет всегда закрыт. Таким образом, если ping проходит – это значит, что первый канал находится в рабочем состоянии и должен быть включен, а второй канал должен быть выключен. Верно и обратное утверждение. Как только ping начнет проходить – произойдет переключение. Нужный маршрут утилита будет определять по назначенному комментарию. Пример программы для проверки доступности канала приведен на рис. 9.

```
/ip route
set comment=ISP1 [find gateway=10.1.100.1]
set comment=ISP2 [find gateway=10.1.200.1]

/ip route
add distance=1 dst-address=8.8.4.4/32 gateway=10.1.100.1

/ip firewall filter
add action=drop chain=output dst-address=8.8.4.4 out-
interface=ether2-WAN2 protocol=icmp comment="Deny 8.8.4.4 through
reserved internet-channel"

/tool netwatch
add down-script="/ip route set [find comment=\"ISP1\"] dis-
abled=yes\r\
\n/ip route set [find comment=\"ISP2\"] disabled=no" host=8.8.4.4
\
up-script="/ip route set [find comment=\"ISP1\"] disabled=no\r\
\n/ip route set [find comment=\"ISP2\"] disabled=yes"
```

Рис. 9. Программа для проверки доступности интернет-канала

Литература

1. MikroTik documentationwiki. – 2019. – Режим доступа: https://wiki.mikrotik.com/wiki/. – Дата доступа: 14.03.2019.
2. GRE (протокол). – 2015. – Режим доступа: https://ru.wikipedia.org/wiki/GRE. – Дата доступа: 26.02.2019.
3. Mikrotik. Failover. Load Balancing. – 2014. – Режим доступа: https://habr.com/ru/post/244385/. – Дата доступа: 26.02.2019.