GIS DAYS 2021

VPN на основе политик и VPN на основе маршрутизации. Разница в подходах

Андрей Шпаков

Руководитель отдела
технического консалтинга

ООО «С-Терра СиЭсПи»

GIS DAYS

s•terra®

План доклада

- VPN на основе политик и VPN на основе маршрутизации (Policy-based VPN vs. Route-based VPN)
- Преимущества Route-based VPN для вашей сети
- Почему Route-based VPN не используется повсеместно в сертифицированных VPN-шлюзах

GIS DAYS

s•terra®

Policy-based VPN

Правило шифрования – это описание вида откуда-куда шифруем
Из хоста или подсети «A» в хост или подсеть «B»

Реализация правил:

- Списки доступа в CLI. Удобны в плане автоматизации, легко сделать шаблон;
- Правила в GUI систем управления. Вопросы по автоматизации и удобству.

Ключевые характеристики:

- **Статичен.** Все правила шифрования зафиксированы в политике безопасности;
- **Тяжело масштабируется.** Изменение в топологии – изменение политики безопасности на каждом узле.

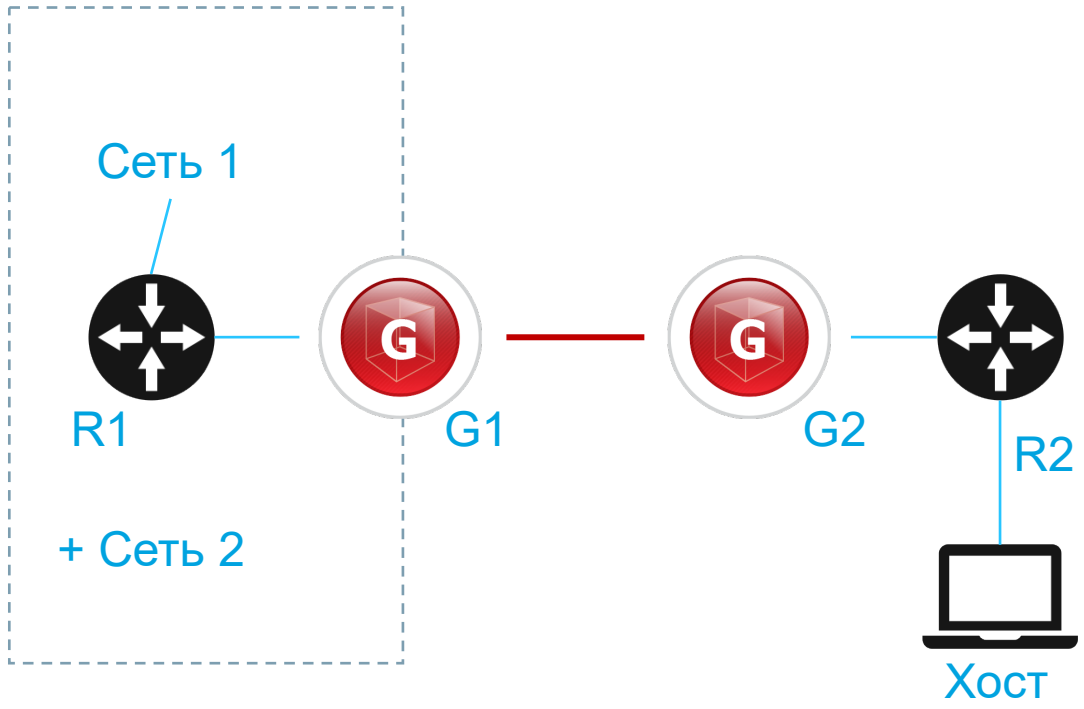
GIS DAYS

s•terra®

Route-based VPN

Параметр сравнения	Policy-based VPN	Route-based VPN
Правило шифрования	Список доступа (модель)	Наличие маршрута
Маршрутизация	Только статическая	Статическая и динамическая
Масштабирование	Сложно. Изменения на всех шлюзах в сети	Легко. Достаточно анонса нового маршрута
Сопутствующие технологии	—	GRE/VTI, динамическая маршрутизация, поддержка динамики внутри VPN
Топологии	Статичные	Динамичные

Сравнение масштабируемости двух подходов



Policy-based VPN:

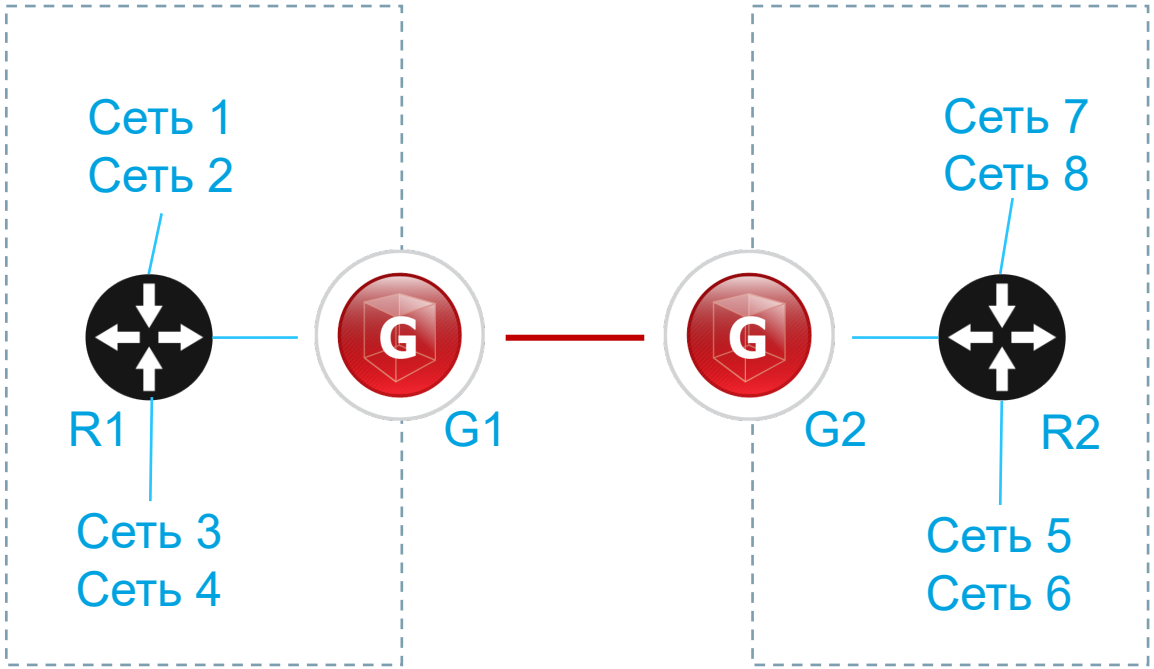
- Настроен туннель между Сеть 1 и Хост;
- Добавляется Сеть 2;
- На G1 и G2 нужно добавить новые правила:

  Сеть 2 – Хост и наоборот.

Route-based VPN:

- Настроен туннель между Сеть 1 и Хост;
- Добавляется Сеть 2;
- R1 анонсирует Сеть 2 в сторону G1 по протоколу динамической маршрутизации. Конфигурация G1 и G2 не меняется.

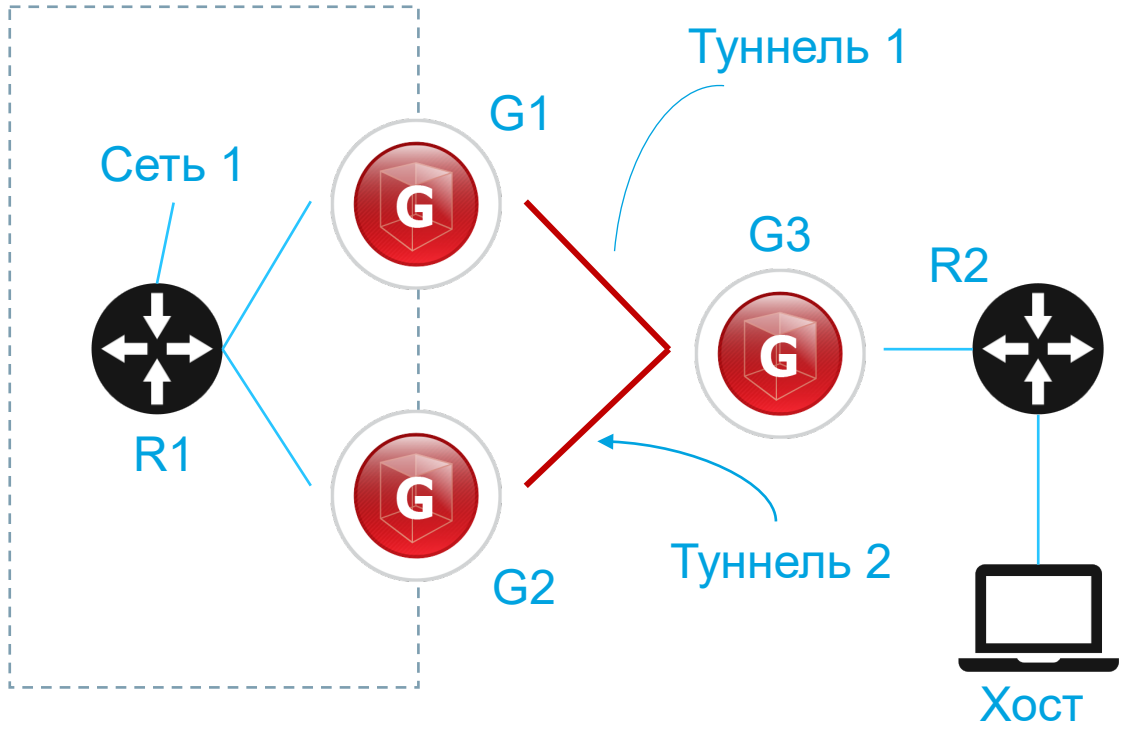
Идеальное решение для сервис провайдеров и не только



Route-based VPN:

- Изменение топологии не влечет изменение конфигурации шлюзов.
- «Трубы», которые можно не трогать. Удобно в условиях разграничения зон ответственности

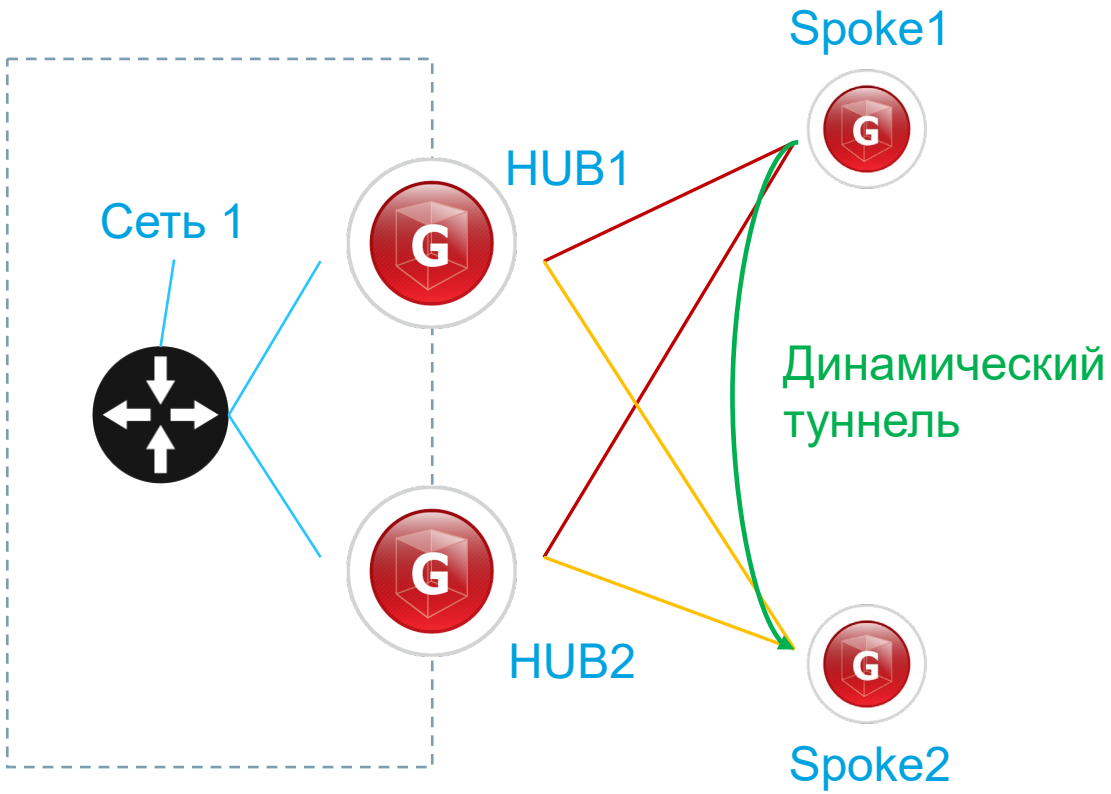
«Кластер» с переключением ~0 секунд



Route-based VPN:

- У R2 есть два маршрута до Сеть 1 через туннель 1 и туннель 2;
- Работает ECMP (балансировка трафика по сессиям);
- При выходе из строя G1, остается один маршрут через туннель 2. Переключится только половина сессий;
- Время переключения = время отработки динамики. С BFD очень быстро (0.5с).

Развитие Route-based VPN: DMVPN и аналоги для Full-Mesh



Динамический VPN:

- Венегрет из технологий (IPsec, mGRE, NHRP, динамическая маршрутизация)
- Мы указываем на Spoke только HUB1 и HUB2. Далее туннели строятся сами
- Масштабирование сети. Если добавить Spoke3, конфигурация всех других устройств не меняется;
- Туннели между Spoke динамические, существуют, когда нужны. Нет переплаты за большие ресурсы старших шлюзов;
- Конфиг Spoke – шаблон. Легко автоматизировать.
- Отказоустойчивость и балансировка нагрузки в центре средствами протокола динамической маршрутизации.

GIS DAYS

s•terra®

Причины текущего положения дел

— **Общее технологическое отставание российских производителей**
Как следствие, мало вендоров, предлагающих Route-based VPN;

— **Нет культуры стандартизации.**
Большая часть решений на рынках используют проприетарные технологии. Все проблемы решены в мировых технологиях.

— **Вендоры ограниченно поддерживают протоколы динамической маршрутизации.**
Единицы могут передать маршрутную информацию внутри VPN туннеля;

GIS DAYS

s•terra®

Причины текущего положения дел

— **Высокий порог входа.**
Для настройки требуются достаточно глубокие знания сетевых технологий;

— **Ужесточения политики регуляторов.**
Все больше нельзя, все тяжелее реализовать.

GIS DAYS

s•terra®

Спасибо за внимание!

ashpakov@s-terra.ru
+7 (499) 940 9001 доб. 133
www.s-terra.ru