Настройте Безопасный сеанс eBGP с IPsec VTI

Содержание

Введение

Этот документ описывает, как защитить отношения соседей внешнего протокола пограничного шлюза (eBGP) с использованием интерфейса виртуальных туннелей IPsec (VTI) наряду с физическими интерфейсами (нетуннель) для трафика плоскости данных. Преимущества этой конфигурации включают:

- Завершенная конфиденциальность Соседнего BGP узел открывает сеанс с конфиденциальностью данных, антивоспроизведением, подлинностью и целостностью.
- Трафик плоскости данных не ограничен к издержкам Максимального размера передаваемого блока данных (MTU) туннельного интерфейса. Клиенты могут передать стандартные пакеты MTU (1500 байтов) без влияний производительности или фрагментации.
- Меньше издержек на маршрутизаторах оконечная точки начиная с шифрования/дешифрования Индекса политики безопасности (SPI) ограничено трафиком уровня управления BGP.

Преимущество этой конфигурации - то, что плоскость данных не ограничена к ограничению туннелируемого интерфейса. Дизайном трафиком плоскости данных не является защищенный IPsec.

Внесенный Чарльз Стизза, специалист службы технической поддержки Cisco.

Предварительные условия

Требования

Корпорация Cisco рекомендует ознакомиться со следующими темами:

- конфигурация eBGP и основные принципы проверки
- Политика BGP, Бухгалтерская (PA) манипулирование с помощью route-map
- Основной Протокол ISAKMP и функции политики IPsec

Используемые компоненты

Сведения в этом документе основываются на Cisco IOS? Выпуск ПО 15.3 (1.3) T, но другие поддерживаемые версии работает. Так как Конфигурация IPSec является криптографической функцией, гарантируйте, что ваша версия кода содержит этот набор функций.

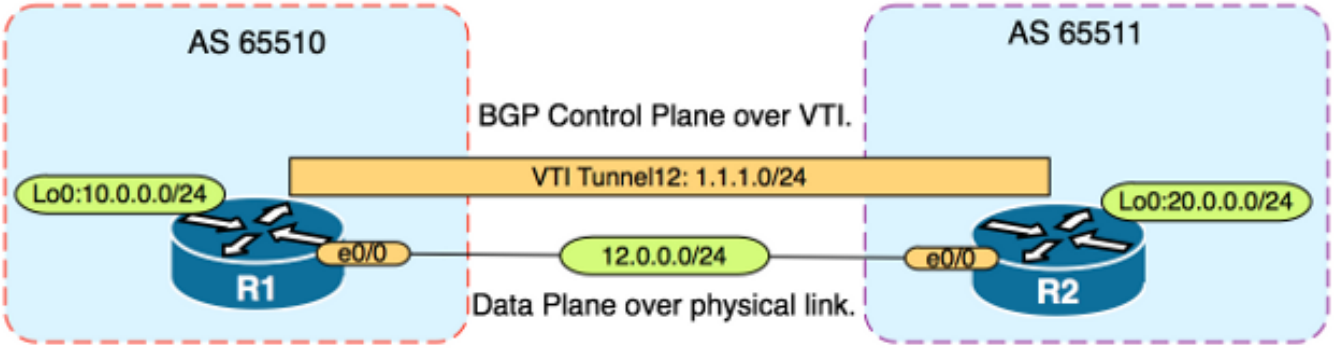
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

> **Внимание. :** Пример конфигурации в этом документе использует скромные алгоритмы шифра, которые могли бы или не могли бы подойти для вашей среды. См. Описание технологических решений Шифрования Следующего поколения для обсуждения относительной безопасности различных наборов шифров и размеров ключа.

Настройка

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети



Конфигурации

Выполните следующие действия:

1. Настройте параметры фазы 1 Протокола IKE на R1 и R2 с предварительным общим ключом на R1:**Примечание:** Никогда не используйте номера группы DH 1, 2 или 5, так как их считают нижними. Если возможное применение группа DH с Эллиптической кривой Cryptopgraphy (ECC), такой как группы 19, 20 или 24. Расширенный стандарт шифрования (AES) и Защищенный алгоритм хэширования 256 (SHA256) нужно считать выше Стандарта шифрования данных (DES) / 3DES и алгоритм представления сообщения в краткой форме 5 (MD5) / SHA1 соответственно. Никогда не используйте пароль "Cisco" в производственной среде.**Конфигурация R1**
```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
R1(config-isakmp)exit

R1(config)#crypto isakmp key CISCO address 12.0.0.2
```
Конфигурация R2
```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```
2. Настройте шифрование пароля уровня 6 для предварительного общего ключа в NVRAM на R1 и R2. Если маршрутизатор поставился под угрозу, это уменьшает вероятность предварительного общего ключа, сохраненного в открытом тексте от того, чтобы быть считанным:
```
R1(config)#key config-key password-encrypt CISCOCISCO

R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```
Примечание: Как только шифрование пароля уровня 6 включено, активная конфигурация больше не показывает версию открытого текста предварительного общего ключа:
```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```
3. Настройте параметры фазы 2 IKE на R1 и R2:**Конфигурация R1**
```
R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
R1(ipsec-profile)#set pfs group19
```
Конфигурация R2
```
R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET

R2(ipsec-profile)#set pfs group19
```
Примечание: Установка безопасной пересылки (Perfect

Forward Secrecy, PFS) является дополнительной, но улучшает силу VPN, так как это вызывает новую генерацию симметричного ключа в установлении SA фазы 2 IKE.

4. Настройте туннельные интерфейсы на R1 и R2 и безопасный с Профилем IPSEC:**Конфигурация R1**
```
R1(config)#interface tunnel 12

R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0

R1(config-if)#tunnel mode ipsec ipv4

R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```
Конфигурация R2
```
R2(config)#interface tunnel 12

R2(config-if)#ip address 1.1.1.2 255.255.255.0

R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```
5. Настройте BGP на R1 и R2 и объявите сети loopback0 в BGP:**R1 Configuraton**
```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```
Конфигурация R2
```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.2 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```
6. Настройте route-map на R1 и R2 для ручного изменения IP-адреса следующего перехода так, чтобы это указало к физическому интерфейсу а не туннелю. Необходимо применить этот route-map на входящее направление.**Конфигурация R1**
```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```
Конфигурация R2
```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10
```

```
R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end

R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Проверьте, что и фаза 1 IKE и фаза 2 IKE завершили. Протокол линии связи в Виртуальном туннельном интерфейсе (VTI) не изменяется на, пока фаза 2 IKE не завершила:

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

Обратите внимание на то, что до приложения route-map, IP-адрес следующего перехода указывает к IP-адресу Соседнего BGP узел, который является туннельным интерфейсом:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

Когда трафик использует туннель, MTU ограничен к туннельному MTU:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
```

```
Success rate is 0 percent (0/5)

R1#show interfaces tunnel 12 | inc transport|line

Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

После применения route-map IP-адрес изменен на физический интерфейс R2, не туннель:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

Сделайте пересадку на самолет данных для использования физического следующего перехода в противоположность стандартному MTU размера разрешений туннеля:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.