Настройте Виртуальные туннельные интерфейсы ASA в двойном Сценарии интернет-провайдера

Содержание

Введение

Этот документ описывает, как настроить VTI (Действительный Туннель Intrfaces) между двумя ASA (Устройства адаптивной безопасности) с использованием IKEv2 (Версия 2 обмена ключами между сетями) протокол для обеспечения безопасного подключения между двумя ответвлениями. Оба из ответвлений имеют два канала поставщика для высокого availablility и целей распределения нагрузки. Соседство Протокола BGP установлено по туннелям для обмена информацией о внутренней маршрутизации.
Эта функция представлена в версии ASA 9.8 (1). ASA реализация VTI совместим с реализацией VTI, доступной на маршрутизаторах IOS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Протокол BGP

Используемые компоненты

Сведения в этом документе основываются на межсетевых экранах ASAv, работающих 9.8 (1) 6 версий программного обеспечения.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Различия между VTI и криптокартой

- Криптокарта является функцией обработки исходящих данных интерфейса. Для передачи трафика через криптокарту базирующийся туннель трафик должен маршрутизироваться к интернет-интерфейсу направления (традиционно вызванный внешний интерфейс) и должен совпасться против крипто-ACL. С другой стороны, VTI является логическим интерфейсом. Туннель к каждому узлу VPN представлен другим VTI. Если точки маршрутизации к VTI, пакет будет зашифрован и передан к соответствующему узлу.

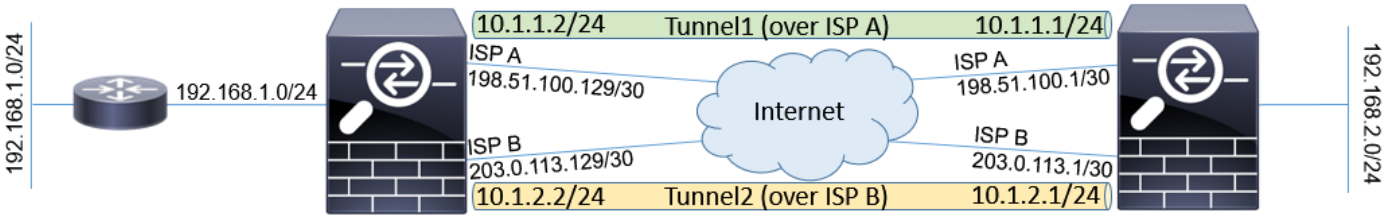
- VTI избавляет от необходимости использовать крипто-списки доступа и правила освобождения Технологии NAT.

- Список контроля доступа (ACL) криптокарты не обеспечивает перекрывающиеся записи. VTI является основанной VPN маршрута, и обычные правила маршрутизации просят трафик VPN, который упрощает конфигурацию и процессы для устранения проблем.

- Криптокарта автоматически предотвращает трафик между узлами, которые будут передаваться в открытом тексте, если туннель не работает. VTI автоматически не защищает против него. Пустые маршруты должны быть добавлены для обеспечения равной функциональности.

Настройка

Схема сети



Конфигурации

Примечание: Данный пример не подходит для сценария, где ASA является участником independed автономной системы и имеет равноправные информационные обмены BGP с сетями ISP. Это покрывает топологию, где ASA имеет два независимых канала поставщика с общими адресами от других автономных систем. В таком случае интернет-провайдер может развернуть защиту антиспуфинга, которая проверяет, не получены ли полученные пакеты от общего IP , который принадлежит другому интернет-провайдеру. В этой конфигурации надлежащие меры приняты для

предотвращения этого.

1. Общее шифрование и параметры аутентификации. Информация о рекомендуемых криптографических параметрах может быть найдена в: https://www. cisco . com/c/en/us/about/security-center/next-generation-cryptography.html

   На обоих ASA:

```
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 24
prf sha256
lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal PROP
protocol esp encryption aes-256
protocol esp integrity sha-256
```

2. Настройте Профиль IPSEC. Одна из сторон должна быть инициатором, и нужно быть респондентом согласования IKEv2:

   ASA уехал:

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
responder-only
```

   Право ASA:

```
crypto ipsec profile PROF
set ikev2 ipsec-proposal PROP
set pfs group24
```

3. Включите протокол IKEv2 на обоих интерфейсах интернет-провайдера.

   Оба ASA:

```
crypto ikev2 enable ispa
crypto ikev2 enable ispb
```

4. Настройте Предварительный общий ключ для взаимной аутентификации ASA:

   ASA уехал:

```
tunnel-group 198.51.100.1 type ipsec-l2l
tunnel-group 198.51.100.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.1 type ipsec-l2l
tunnel-group 203.0.113.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

Право ASA:

```
tunnel-group 198.51.100.129 type ipsec-l2l
tunnel-group 198.51.100.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
tunnel-group 203.0.113.129 type ipsec-l2l
tunnel-group 203.0.113.129 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

5. Настройте интерфейсы интернет-провайдера:

ASA уехал:

```
interface GigabitEthernet0/1
nameif ispa
security-level 0
ip address 198.51.100.129 255.255.255.252
!
interface GigabitEthernet0/2
nameif ispb
security-level 0
ip address 203.0.113.129 255.255.255.252
!
```

Право ASA:

```
interface GigabitEthernet0/1
nameif ispa
security-level 0
ip address 198.51.100.1 255.255.255.252
!
interface GigabitEthernet0/2
nameif ispb
security-level 0
ip address 203.0.113.1 255.255.255.252
!
```

6. Основное соединение является интернет-провайдером интерфейс. Интернет-провайдер B вторичен. Доступность основного соединения отслежена с использованием запроса Функции проверки связности ICMP ping к хосту в Интернете в данном примере, ASA используют друг друга интернет-провайдер интерфейс как назначение эхо-запроса:

ASA уехал:

```
sla monitor 1
type echo protocol ipIcmpEcho 198.51.100.1 interface ispa
!
sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1 reachability
!
route ispa 0.0.0.0 0.0.0.0 198.51.100.130 1 track 1
route ispb 0.0.0.0 0.0.0.0 203.0.113.130 10
```

Право ASA:

```
sla monitor 1
type echo protocol ipIcmpEcho 198.51.100.129 interface ispa
!
sla monitor schedule 1 life forever start-time now
!
track 1 rtr 1 reachability
```

```
!
route ispa 0.0.0.0 0.0.0.0 198.51.100.2 1 track 1
route ispb 0.0.0.0 0.0.0.0 203.0.113.2 10
```

7. Основной VTI всегда устанавливается по интернет-провайдеру A. Вторичный VTI установлен по интернет-провайдеру B. Статические маршруты к назначению туннеля необходимы. Это гарантирует, что зашифрованные пакеты уезжают от корректного физического интерфейса для предотвращения отбрасываний антиспуфинга интернет-провайдера:

   ASA уехал:
   ```
   route ispa 198.51.100.1 255.255.255.255 198.51.100.130 1
   route ispb 203.0.113.1 255.255.255.255 203.0.113.130 1
   ```
   Право ASA:
   ```
   route ispa 198.51.100.129 255.255.255.255 198.51.100.2 1
   route ispb 203.0.113.129 255.255.255.255 203.0.113.2 1
   ```
8. Конфигурация VTI:

   ASA уехал:
   ```
   interface Tunnel1
   nameif tuna
   ip address 10.1.1.2 255.255.255.0
   tunnel source interface ispa
   tunnel destination 198.51.100.1
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile PROF
   !
   interface Tunnel2
   nameif tunb
   ip address 10.1.2.2 255.255.255.0
   tunnel source interface ispb
   tunnel destination 203.0.113.1
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile PROF
   ```
   Право ASA:
   ```
   interface Tunnel1
   nameif tuna
   ip address 10.1.1.1 255.255.255.0
   tunnel source interface ispa
   tunnel destination 198.51.100.129
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile PROF
   !
   interface Tunnel2
   nameif tunb
   ip address 10.1.2.1 255.255.255.0
   tunnel source interface ispb
   tunnel destination 203.0.113.129
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile PROF
   ```

9. BGP - конфигурация. Туннель, привязанный к интернет-провайдеру A, является основным. Префиксы, объявленные по туннелю, сформированному по интернет-провайдеру B, имеют более низкую локальную-переменную-prefernce, которая делает их менее предпочтительными таблицей маршрутизации:

   ASA уехал:

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.1 remote-as 65000
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 next-hop-self
neighbor 10.1.2.1 remote-as 65000
neighbor 10.1.2.1 activate
neighbor 10.1.2.1 next-hop-self
neighbor 10.1.2.1 route-map BACKUP out
network 192.168.1.0
no auto-summary
no synchronization
exit-address-family
```

Право ASA:

```
route-map BACKUP permit 10
set local-preference 80
!
router bgp 65000
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.1.1.2 remote-as 65000
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 next-hop-self
neighbor 10.1.2.2 remote-as 65000
neighbor 10.1.2.2 activate
neighbor 10.1.2.2 next-hop-self
neighbor 10.1.2.2 route-map BACKUP out
network 192.168.2.0
no auto-summary
no synchronization
exit-address-family
```

10. (Необязательно) для объявления дополнительной сети позади левого ASA, который непосредственно не связан с нею, перераспределение статического маршрута может быть настроено:

    ASA уехал:

    ```
    route inside 192.168.10.0 255.255.255.0 192.168.1.100 1
    !
    prefix-list REDISTRIBUTE_LOCAL seq 10 permit 192.168.10.0/24
    !
    route-map REDISTRIBUTE_LOCAL permit 10
    match ip address prefix-list REDISTRIBUTE_LOCAL
    !
    router bgp 65000
    address-family ipv4 unicast
    redistribute static route-map REDISTRIBUTE_LOCAL
    ```

11. (Необязательно) трафик может быть с балансировкой нагрузки между туннелями на основе назначения пакета. В данном примере маршрут к 192.168.10.0/24 сети предпочтен по резервному туннелю (туннель интернет-провайдера B)

    ASA уехал:

    ```
    route-map BACKUP permit 5
    match ip address prefix-list REDISTRIBUTE_LOCAL
    set local-preference 200
    !
    ```

```
route-map BACKUP permit 10
set local-preference 80
```

12. Для предотвращения трафика между узлами от того, чтобы быть передаваемым в открытом тексте к Интернету, если туннели не работают Пустые маршруты должны быть добавлены. Все адреса RFC1918 были добавлены для простоты:

    Оба ASA:

```
route Null0 10.0.0.0 255.0.0.0 250
route Null0 172.16.0.0 255.240.0.0 250
route Null0 192.168.0.0 255.255.0.0 250
```

13. (Необязательно) По умолчанию процесс BGP ASA передает пакеты Keepalive один раз в 60 секунд. Если ответ на сообщение поддержки активности не получен от узла в течение 180 секунд, это объявлено мертвое. Для ускорения, обнаружение граничат со сбоем, можно настроить таймеры BGP. В данном примере пакеты Keepalive передаются каждые 10 секунд, и соседний узел объявлен вниз после 30 секунд.

```
router bgp 65000
address-family ipv4 unicast
neighbor 10.1.1.2 timers 10 30
neighbor 10.1.2.2 timers 10 30
exit-address-family
```

Проверка

Проверьте, подключен ли туннель IKEv2:

```
ASA-right(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:32538, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
836052177 198.51.100.1/500 198.51.100.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/7 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xc6623962/0x5c4a3bce

IKEv2 SAs:

Session-id:1711, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
832833529 203.0.113.1/500 203.0.113.129/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:24, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/29 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x2e3715af/0xc20e22b4
```

Проверьте статус смежного соединения BGP:

```
ASA-right(config)# show bgp summary
BGP router identifier 203.0.113.1, local AS number 65000
BGP table version is 29, main routing table version 29
3 network entries using 600 bytes of memory
5 path entries using 400 bytes of memory
5/3 BGP path/bestpath attribute entries using 1040 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2040 total bytes of memory
BGP activity 25/22 prefixes, 69/64 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.2 4 65000 6 5 29 0 0 00:00:51 2
10.1.2.2 4 65000 7 6 29 0 0 00:01:20 2
```

Проверьте маршруты, полученные от BGP. Маршруты, отмеченные">", установлены в таблице маршрутизации:

```
ASA-right(config)# show bgp

BGP table version is 29, local router ID is 203.0.113.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
*>i192.168.1.0 10.1.1.2 0 100 0 i
* i 10.1.2.2 0 80 0 i
*> 192.168.2.0 0.0.0.0 0 32768 i
* i192.168.10.0 10.1.1.2 0 100 0 ?
*>i 10.1.2.2 0 200 0 ?

Verify routing table:

ASA-right(config)# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 198.51.100.2 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.2, ispa
S 10.0.0.0 255.0.0.0 is directly connected, Null0
C 10.1.1.0 255.255.255.0 is directly connected, tuna
L 10.1.1.1 255.255.255.255 is directly connected, tuna
C 10.1.2.0 255.255.255.0 is directly connected, tunb
L 10.1.2.1 255.255.255.255 is directly connected, tunb
S 172.16.0.0 255.240.0.0 is directly connected, Null0
S 192.168.0.0 255.255.0.0 is directly connected, Null0
B 192.168.1.0 255.255.255.0 [200/0] via 10.1.1.2, 00:02:06
C 192.168.2.0 255.255.255.0 is directly connected, inside
L 192.168.2.1 255.255.255.255 is directly connected, inside
B 192.168.10.0 255.255.255.0 [200/0] via 10.1.2.2, 00:02:35
C 198.51.100.0 255.255.255.252 is directly connected, ispa
L 198.51.100.1 255.255.255.255 is directly connected, ispa
S 198.51.100.129 255.255.255.255 [1/0] via 198.51.100.2, ispa
```

```
C 203.0.113.0 255.255.255.252 is directly connected, ispb
L 203.0.113.1 255.255.255.255 is directly connected, ispb
S 203.0.113.129 255.255.255.255 [1/0] via 203.0.113.2, ispb
```

Устранение неполадок

Отладки использовали устранять неполадки протокола IKEv2:

debug crypto ikev2 протокол 4
debug crypto ikev2 платформа 4

Для получения дополнительной информации об устранении проблем протокола IKEv2: https://www. cisco . com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

Для получения дополнительной информации об устранении проблем протокола BGP: https://www. cisco . com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Дополнительные сведения

- **Правила выбора маршрута BGP:** https://www. cisco . com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- **Руководство по конфигурации BGP ASA:** https://www. cisco . com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Cisco Systems – техническая поддержка и документация