Configurar interfaces de túnel virtuais ASA na encenação dupla ISP

Índice

Introdução

Este documento descreve como configurar VTI (túnel virtual Intrfaces) entre dois ASA (ferramentas de segurança adaptáveis) com uso (versão 2 do intercâmbio de chave de Internet) do protocolo IKEv2 fornecer uma conectividade segura entre dois ramos. Ambos os ramos têm dois links ISP para finalidades altas do availablility e do Balanceamento de carga. O neighborship do Border Gateway Protocol (BGP) é estabelecido sobre os túneis a fim trocar a informação de roteamento interna.
Esta característica é introduzida na versão ASA 9.8(1). A aplicação ASA VTI é compatível com a aplicação VTI disponível em IOS Router.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolo BGP

Componentes Utilizados

A informação neste documento é baseada nos Firewall de ASAv que executam a versão de software 9.8(1)6.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Diferenças entre VTI e crypto map

- O crypto map é uns recursos de emissor da relação. A fim enviar o tráfego através do túnel baseado em mapas cripto, o tráfego precisa de ser distribuído ao Internet que enfrenta a relação (chamada tradicionalmente interface externa) e deve ser combinado contra o ACL cripto. Por outro lado, VTI é uma interface lógica. O túnel a cada par VPN é representado por um VTI diferente. Se o roteamento aponta para VTI, o pacote estará cifrado e enviado ao par correspondente.

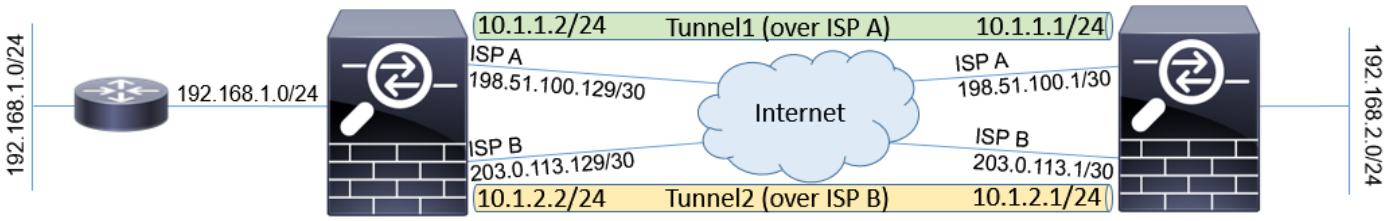
- VTI elimina a necessidade de usar regras criptos das Listas de acesso e da isenção do Network Address Translation (NAT).

- O Access Control List do crypto map (ACL) não permite entradas de sobreposição. VTI é um VPN baseado rota e as regras de roteamento regulares aplicam-se para o tráfego VPN, que simplifica a configuração e os processos para pesquisar defeitos.

- O crypto map impede automaticamente o tráfego entre os locais a ser enviados no texto não criptografado se o túnel está para baixo. VTI não protege automaticamente contra ele. As rotas nulas precisam de ser adicionadas para assegurar a funcionalidade igual.

Configurar

Diagrama de Rede



Configurações

Note: Este exemplo não é apropriado para a encenação onde o ASA é um membro do sistema autônomo independed e tem peerings BGP com redes ISP. Cobre a topologia onde o ASA tem dois links independentes ISP com os endereços públicos dos sistemas diferente autônomo. Em tal caso, o ISP pode distribuir a proteção anti-falsificação que verifica se os pacotes recebidos não são originado do IP do público que pertence a um outro ISP. Nesta configuração, as medidas apropriadas são tomadas impedir isto.

1. Criptografia e parâmetros de autenticação comuns. A informação sobre parâmetros criptograficamente recomendados pode ser encontrada em: https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

Em ambos os 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. Configurar o perfil IPSec. Um dos lados tem que ser iniciador e um precisa de ser um que responde da negociação IKEv2:

   ASA deixado:

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

   Direito ASA:

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

3. Permita o protocolo IKEv2 em ambas as relações ISP.

   Ambos os ASA:

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

4. Configurar a chave pré-compartilhada para autenticar mutuamente os ASA:

   ASA deixado:

```
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 *****
```

   Direito 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. Configurar as relações ISP:

   ASA deixado:
```
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
!
```
   Direito 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. O link principal é relação ISP A. O ISP B é secundário. A Disponibilidade do link principal é seguida com uso do pedido do ping ICMP a um host no Internet, neste exemplo o uso ASA relação ISP A como o destino do sibilo:

   ASA deixado:
```
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
```
   Direito 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. O VTI preliminar é estabelecido sempre sobre o ISP A. Secundário VTI é estabelecido sobre rotas estáticas ISP B. para o destino de túnel é precisado. Isto assegura-se de que os pacotes criptografado saam da interface física correta para evitar gotas anti-falsificação ISP:

   ASA deixado:

```
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
```

Direito 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. Configuração VTI:

ASA deixado:

```
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
```

Direito 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. Configuração de BGP. O túnel associado com o ISP A é um preliminar. Os prefixos anunciados sobre o túnel formado sobre ISP B têm mais baixo local-prefernce que o faz preferido menos pela tabela de roteamento:

ASA deixado:

```
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
```

Direito 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. (Opcional) a fim anunciar a rede adicional atrás do ASA esquerdo que não lhe é conectado diretamente, a redistribuição da rota estática pode ser configurada:

    ASA deixado:

    ```
    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. (Opcional) o tráfego pode ser carga equilibrada entre os túneis baseados no destino do pacote. Neste exemplo, a rota para a rede 192.168.10.0/24 é preferida sobre o túnel alternativo (o túnel ISP B)

    ASA deixado:

    ```
    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. Para impedir que o tráfego entre locais esteja enviado no texto não criptografado ao Internet se os túneis estão para baixo, as rotas nulas precisam de ser adicionadas. Todos os endereços do RFC1918 foram adicionados para a simplicidade:

    Ambos os 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. (Opcional) à revelia, o processo BGP ASA envia o Keepalives uma vez por 60 segundos. Se a

resposta de keepalive não é recebida do par por 180 segundos, declara-se absolutamente. A fim acelerar a falha do neigbor da detecção, você pode configurar temporizadores BGP. Neste exemplo, o Keepalives é enviado os segundos cada 10 e o vizinho é declarado para baixo após 30 segundos.

```
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
```

Verificar

Verifique se o túnel IKEv2 está acima:

```
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
```

Verifique o estado da vizinhança de 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
```

Verifique as rotas recebidas do BGP. As rotas identificadas por meio de “>” são instaladas na tabela de roteamento:

```
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
```

Troubleshooting

Debugs usou-se para pesquisar defeitos o protocolo IKEv2:

protocolo 4 do debug crypto ikev2
plataforma 4 do debug crypto ikev2

Para obter mais informações sobre de pesquisar defeitos o protocolo IKEv2: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debugs.html

Para obter mais informações sobre do protocolo BGP do Troubleshooting: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Informações Relacionadas

- Regras de seleção da rota de BGP: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- Guia de configuração de BGP ASA: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Suporte Técnico e Documentação - Cisco Systems