Configure las interfaces del túnel virtuales ASA en el escenario dual ISP

Contenido

Introducción

Este documento describe cómo configurar VTI (túnel virtual Intrfaces) entre dos ASA (dispositivos de seguridad adaptantes) con el uso de IKEv2 (protocolo de la versión del intercambio de claves de Internet 2) para proporcionar la conectividad segura entre dos bifurcaciones. Ambas bifurcaciones tienen dos links ISP para los altos propósitos del availablility y del Equilibrio de carga. La vecindad del Border Gateway Protocol (BGP) se establece sobre los túneles para intercambiar la información de ruteo interna.
Esta característica se introduce en la Versión de ASA 9.8(1). La implementación ASA VTI es compatible con la implementación VTI disponible en los routeres IOS.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo BGP

Componentes Utilizados

La información en este documento se basa en los Firewall de ASAv que funcionan con la versión de software 9.8(1)6.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Diferencias entre VTI y la correspondencia de criptografía

- La correspondencia de criptografía es una función de resultados de la interfaz. Para enviar el tráfico a través de la correspondencia de criptografía basó el túnel, el tráfico necesita ser ruteado a Internet que hace frente a la interfaz (tradicionalmente llamada interfaz exterior) y se debe corresponder con contra el ACL crypto. Por otra parte, VTI es una interfaz lógica. El túnel a cada par VPN es representado por un diverso VTI. Si la encaminamiento señala hacia VTI, el paquete será cifrado y enviado al par correspondiente.

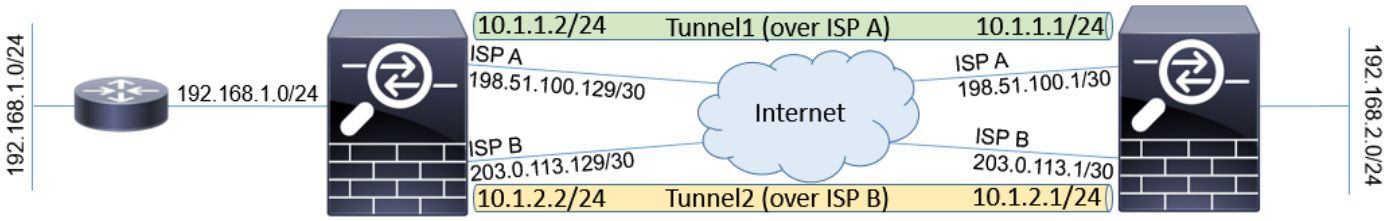
- VTI elimina la necesidad de utilizar las Listas de acceso y las reglas de exención crypto del Network Address Translation (NAT).

- La lista de control de acceso (ACL) de la correspondencia de criptografía no permite las entradas que solapan. VTI es un VPN basado ruta y las reglas de ruteo regulares solicitan el tráfico VPN, que simplifica la configuración y los procesos para resolver problemas.

- La correspondencia de criptografía previene automáticamente el tráfico entre los sitios que se enviarán en el texto claro si el túnel está abajo. VTI no protege automáticamente contra él. Las rutas nulas necesitan ser agregadas para asegurar las funciones iguales.

Configurar

Diagrama de la red



Configuraciones

Note: Este ejemplo no es conveniente para el escenario donde está un miembro del sistema autónomo independed y tiene el ASA peeringes BGP con las redes ISP. Cubre la topología donde el ASA tiene dos links independientes ISP con las direcciones públicas de los sistemas autónomos diferentes. En tal caso, el ISP puede desplegar la protección contra spoofing que verifica si los paquetes recibidos no son originados del IP del público que pertenece a otro ISP. En esta configuración, se toman las medidas apropiadas para prevenir esto.

1. Cifrado y parámetros de autenticación comunes. La información sobre los parámetros criptográficos recomendados se puede encontrar en:

https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html

En ambos 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. Configure el perfil de ipsec. Uno de los lados tiene que ser iniciador y uno necesita ser un respondedor de la negociación IKEv2:

ASA dejado:

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

La derecha ASA:

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

3. Protocolo del permiso IKEv2 en ambas interfaces ISP.

Ambos ASA:

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

4. Configure la clave previamente compartida para autenticar mutuamente los ASA:

ASA dejado:

```
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 *****
```

La derecha 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. Configure las interfaces ISP:

   ASA dejado:

```
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
!
```

   La derecha 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. El link principal es interfaz ISP A. El ISP B es secundario. La Disponibilidad del link principal se sigue con el uso de la petición del ping de ICMP a un host en Internet, en este ejemplo el uso ASA interfaz ISP A como destino del ping:

   ASA dejado:

```
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
```

   La derecha 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. El VTI primario se establece siempre sobre el ISP A. Secondary VTI se establece sobre las Static rutas ISP B. hacia el destino del túnel es necesario. Esto se asegura de que los paquetes encriptados se vayan de la interfaz física correcta para evitar los descensos contra spoofing ISP:

ASA dejado:

```
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
```

La derecha 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. Configuración VTI:

ASA dejado:

```
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
```

La derecha 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. Configuración BGP. El túnel asociado a ISP A es un primario. Los prefijos des divulgación sobre el túnel formado sobre ISP B tienen más bajo local-prefernce que lo haga preferida menos por la tabla de ruteo:

ASA dejado:

```
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
```

La derecha 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) para hacer publicidad de la red adicional detrás del ASA izquierdo que no está conectado directamente con ella, la redistribución de la Static ruta puede ser configurada:

    ASA dejado:

    ```
    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) el tráfico puede ser carga equilibrio entre los túneles basados en el destino del paquete. En este ejemplo, la ruta hacia la red 192.168.10.0/24 se prefiere sobre el túnel de reserva (el túnel ISP B)

    ASA dejado:

    ```
    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 evitar que el tráfico entre los sitios sea enviado en el texto claro a Internet si los túneles están abajo, las rutas nulas necesitan ser agregadas. Todos los direccionamientos del RFC1918 fueron agregados para la simplicidad:

    Ambos 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) por abandono, el proceso BGP ASA envía el Keepalives una vez por 60 segundos. Si la respuesta de keepalive no se recibe del par por 180 segundos, se declara absolutamente. Para acelerar el error del neigbor de la detección, usted puede configurar los temporizadores BGP. En este ejemplo, el Keepalives se envía cada 10 segundos y declaran el vecino abajo después de 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
```

Verificación

Verifique si el túnel IKEv2 está para arriba:

```
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 el estatus de la vecindad 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 las rutas recibidas del BGP. Las rutas marcadas con “>” están instaladas en la tabla de ruteo:

```
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 usados para resolver problemas el protocolo IKEv2:

protocolo 4 del debug crypto ikev2
plataforma 4 del debug crypto ikev2

Para más información sobre resolver problemas el 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 más información sobre el protocolo BGP del troubleshooting:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html#anc37

Información Relacionada

- Reglas de selección de la ruta BGP:
  https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- Guía de configuración BGP ASA:
  https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118050-config-bgp-00.html
- Soporte Técnico y Documentación - Cisco Systems