Configuración de las Interfaces de Túnel Virtuales ASA en el Escenario ISP Dual

Contenido

Introducción

Este documento describe cómo configurar VTI (Virtual Tunnel Interfaces) entre dos ASA (Adaptive Security Appliances) con el uso del protocolo IKEv2 (Internet Key Exchange versión 2) para proporcionar conectividad segura entre dos sucursales. Ambas sucursales tienen dos links ISP para fines de alta disponibilidad y balanceo de carga. La vecindad del protocolo de gateway fronterizo (BGP) se establece sobre los túneles para intercambiar información de routing interna. Esta función se introduce en ASA versión 9.8(1). La implementación de ASA VTI es compatible con la implementación de VTI disponible en los routers IOS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- protocolo BGP

Componentes Utilizados

La información de este documento se basa en firewalls ASAv que ejecutan la versión de software 9.8(1)6.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diferencias entre VTI y Crypto Map

- El mapa criptográfico es una función de salida de la interfaz. Para enviar el tráfico a través de un túnel basado en mapa criptográfico, el tráfico debe enrutarse a la interfaz de cara a Internet (tradicionalmente llamada interfaz externa) y debe compararse con la ACL criptográfica. Por otra parte, VTI es una interfaz lógica. El túnel a cada par VPN se representa mediante un VTI diferente. Si el ruteo apunta hacia VTI, el paquete se cifrará y se enviará al par correspondiente.

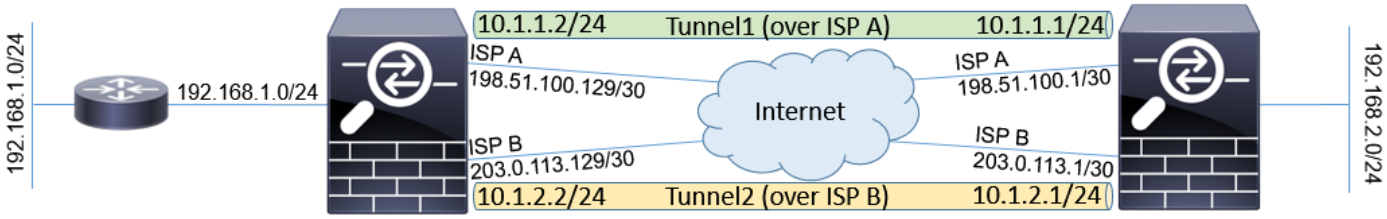
- VTI elimina la necesidad de utilizar listas de acceso criptográfico y reglas de exención de traducción de direcciones de red (NAT).

- La lista de control de acceso (ACL) de mapa criptográfico no permite entradas superpuestas. VTI es una VPN basada en ruta y se aplican reglas de ruteo regulares para el tráfico VPN, lo que simplifica la configuración y los procesos para resolver problemas.

- El mapa criptográfico evita automáticamente que el tráfico entre sitios se envíe en texto sin formato si el túnel está inactivo. VTI no se protege automáticamente contra ella. Se deben agregar rutas nulas para garantizar la misma funcionalidad.

Configurar

Diagrama de la red



Configuraciones

Nota: Este ejemplo no es adecuado para el escenario en el que ASA es miembro de un sistema autónomo independiente y tiene pares BGP con redes ISP. Abarca la topología donde ASA tiene dos links ISP independientes con direcciones públicas de diferentes sistemas autónomos. En tal caso, el ISP puede implementar una protección anti-simulación que verifique si los paquetes recibidos no se originan en IP pública que pertenece a otro ISP. En esta configuración, se toman las medidas adecuadas para evitar esto.

1. Parámetros comunes de cifrado y autenticación. Puede encontrar información sobre los parámetros criptográficos recomendados 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 IPsec. Uno de los lados debe ser el iniciador y uno debe ser el respondedor de la negociación IKEv2:

   ASA izquierda:

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

   ASA derecha:

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

3. Habilite el protocolo 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 izquierda:

```
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 *****
```

   ASA derecha:

```
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 izquierda:
```
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
!
```
   ASA derecha:
```
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 una interfaz ISP A. El ISP B es secundario. Se realiza un seguimiento de la disponibilidad del link principal con el uso de la solicitud de ping ICMP a un host en Internet. En este ejemplo, los ASA se utilizan entre sí una interfaz ISP A como destino de ping:

   ASA izquierda:
```
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
```
   ASA derecha:
```
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. La VTI principal siempre se establece sobre el ISP A. La VTI secundaria se establece sobre el ISP B. Se necesitan rutas estáticas hacia el destino del túnel. Esto asegura que los paquetes cifrados salgan de la interfaz física correcta para evitar las caídas ISP anti-suplantación:

   ASA izquierda:
```
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
```

ASA derecha:

```
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 de VTI:

ASA izquierda:

```
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
```

ASA derecha:

```
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 de BGP. El túnel asociado con el ISP A es un primario. Los prefijos anunciados sobre el túnel formado sobre el ISP B tienen menor preferencia local, lo que los hace menos preferidos por la tabla de ruteo:

ASA izquierda:

```
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
```

ASA derecha:

```
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 anunciar la red adicional detrás del ASA izquierdo que no está conectado directamente a él, se puede configurar la redistribución de ruta estática:

    ASA izquierda:

    ```
    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 se puede equilibrar de carga entre los túneles según el destino del paquete. En este ejemplo, se prefiere la ruta hacia la red 192.168.10.0/24 en lugar del túnel de respaldo (túnel ISP B)

    ASA izquierda:

    ```
    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 sitios se envíe en texto sin formato a Internet si los túneles están inactivos, se deben agregar rutas nulas. Todas las direcciones RFC1918 se agregaron para simplificar:

    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) De forma predeterminada, el proceso BGP ASA envía señales de mantenimiento una vez por 60 segundos. Si la respuesta de keepalive no se recibe del par durante 180

segundos, se declara como muerta. Para acelerar la falla del vecino de detección, puede configurar los temporizadores BGP. En este ejemplo, las señales de mantenimiento se envían cada 10 segundos y el vecino se declara inactivo 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 activo:

```
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 estado de 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 de BGP. Las rutas marcadas con ">" se instalan 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
```

Troubleshoot

Depuraciones utilizadas para resolver problemas del protocolo IKEv2:

debug crypto ikev2 protocol 4
debug crypto ikev2 platform 4

Para obtener más información sobre la resolución de problemas del 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 obtener más información sobre la resolución de problemas del protocolo BGP: 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 ruta BGP: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html
- Guía de configuración de ASA BGP: 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