Migrar túnel criptográfico basado en políticas a túnel criptográfico basado en rutas en ASA

Contenido

Introducción

Este documento describe la migración de túneles basados en políticas a túneles basados en rutas en ASA.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Comprensión básica de los conceptos de IKEv2-IPSec VPN.
- Conocimiento de VPN IPSec en ASA y su configuración.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA: código ASA versión 9.8(1) o posterior.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Pasos para la migración:

1. Elimine la configuración VPN basada en políticas existente
2. Configuración del perfil IPSec
3. Configuración de la interfaz de túnel virtual (VTI)
4. Configure el ruteo estático o el protocolo de ruteo dinámico

Configuraciones

Túnel basado en políticas existente:

1. Configuración de la interfaz:

Interfaz de salida a la que está enlazado el mapa criptográfico.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
```

2. Política IKEv2:

Define los parámetros para la Fase 1 del proceso de negociación IPsec.

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

3. Grupo de túneles:

Define los parámetros para las conexiones VPN. Los grupos de túnel son esenciales para configurar VPN de sitio a sitio, ya que contienen información sobre el par, los métodos de autenticación y varios parámetros de conexión.

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

4. ACL criptográfica:

Define el tráfico que debe cifrarse y enviarse a través del túnel.

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0

access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```

5. Propuesta de IPSec criptográfica:

Define la propuesta IPSec, que especifica los algoritmos de cifrado e integridad para la Fase 2 de la negociación IPSec.

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

6. Configuración de mapa criptográfico:

Define la política para las conexiones VPN IPsec, incluyendo el tráfico que se va a cifrar, los peers y la propuesta ipsec previamente configurada. También está enlazado a la interfaz que maneja el tráfico VPN.

```
crypto map outside_map 10 match address asa-vpn
crypto map outside_map 10 set peer 10.20.20.20
crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET

crypto map outside_map interface outside
```

Migración del túnel basado en políticas al túnel basado en rutas:

1. Eliminar configuración de VPN basada en políticas existente:
   En primer lugar, elimine la configuración VPN basada en políticas existente. Esto incluye las entradas de mapa criptográfico para ese par, las ACL y cualquier configuración relacionada.

```
no crypto map outside_map 10 match address asa-vpn
no crypto map outside_map 10 set peer 10.20.20.20
no crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET
```

2. Configurar perfil IPSec:
   Defina un perfil IPsec con el conjunto de transformación o la propuesta de IPSec de IKEv2 existente.

```
crypto ipsec profile PROPOSAL_IKEV2_TSET
 set ikev2 ipsec-proposal IKEV2_TSET
```

3. Configuración de la interfaz de túnel virtual (VTI):
   Cree una interfaz de túnel virtual (VTI) y aplíquele el perfil IPsec.

```
interface Tunnel1
 nameif VPN-BRANCH
 ip address 10.1.1.2 255.255.255.252
 tunnel source interface outside
 tunnel destination 10.20.20.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROPOSAL_IKEV2_TSET
```

4. Configure el ruteo estático o el protocolo de ruteo dinámico:
   Agregue rutas estáticas o configure un protocolo de ruteo dinámico para rutear el tráfico a través de la interfaz de túnel. En esta situación, estamos utilizando el routing estático.

   Routing estático:

```
route VPN-BRANCH 172.16.10.0 255.255.255.0 10.1.1.10
```

Verificación

Después de migrar de una VPN basada en políticas a una VPN basada en rutas mediante interfaces de túnel virtual (VTI) en un Cisco ASA, es fundamental comprobar que el túnel está activo y funciona correctamente. A continuación, se indican varios pasos y comandos que puede utilizar para verificar el estado y solucionar los problemas si es necesario.

1. Verifique la interfaz del túnel
Compruebe el estado de la interfaz de túnel para asegurarse de que está activa.

<#root>

```
ciscoasa# show interface Tunnel1

Interface Tunnel1 "VPN-BRANCH", is up, line protocol is up

Hardware is Virtual Tunnel Interface
Description: IPsec VPN Tunnel to Remote Site
Internet address is
10.1.1.2/24

MTU 1500 bytes, BW 10000 Kbit/sec, DLY 500000 usec
65535 packets input, 4553623 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
65535 packets output, 4553623 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
Tunnel source 10.10.10.10, destination 10.20.20.20

Tunnel protocol/transport IPSEC/IP
Tunnel protection
IPsec profile PROPOSAL_IKEV2_TSET
```

Este comando proporciona detalles sobre la interfaz de túnel, incluyendo su estado operativo, dirección IP y origen/destino del túnel. Busque estos indicadores:
· El estado de la interfaz es activo.
· El estado del protocolo de línea es up.

2. Comprobar las asociaciones de seguridad (SA) de IPsec

Compruebe el estado de las SA de IPSec para asegurarse de que el túnel se ha negociado correctamente.

<#root>

ciscoasa# show crypto ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, seq num: 1, local addr:

10.10.10.10

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer:

10.20.20.20

#pkts encaps: 1000, #pkts encrypt: 1000, #pkts digest: 1000

#pkts decaps: 1000, #pkts decrypt: 1000, #pkts verify: 1000

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1000, #pkts compr. failed: 0, #pkts decompress failed: 0

local crypto endpt.:

10.10.10.10

/500, remote crypto endpt.:

10.20.20.20

/500
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 0xC0A80101(3232235777)
current inbound spi : 0xC0A80102(3232235778)

inbound esp sas:

spi: 0xC0A80102(3232235778)

transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: CSR:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y

Status: ACTIVE

outbound esp sas:

spi: 0xC0A80101(3232235777)

```
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: CSR:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y
```

Status: ACTIVE

Este comando muestra el estado de las SA de IPSec, incluidos los contadores de paquetes encapsulados y desencapsulados. Asegúrese de lo siguiente:
· Hay SA activos para el túnel.
· Los contadores de encapsulación y desencapsulación están aumentando, lo que indica el flujo de tráfico.

Para obtener información más detallada, puede utilizar:

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:
```

Session-id:2, Status:UP-ACTIVE

```
, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555
```

10.10.10.10/500 10.20.20.20/500 READY INITIATOR

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/259 sec
```

Este comando muestra el estado de las SA IKEv2, que se encuentran en el estado READY.

3. Verificar enrutamiento
Verifique la tabla de ruteo para asegurarse de que las rutas apunten correctamente a través de la interfaz de túnel.

<#root>

```
ciscoasa# show route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF Intra, IA - OSPF Inter, E1 - OSPF External Type 1
E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
i - IS-IS, su - IS-IS summary null, 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, H - NHRP, l - LISP
+ - replicated route, % - next hop override

S 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

C 10.1.1.0 255.255.255.0 is directly connected, Tunnel1

S 172.16.10.0 255.255.255.0 [1/0] via 10.1.1.10, Tunnel1

Busque rutas que se enrutan a través de la interfaz de túnel.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

1. Verifique la configuración de túnel basada en ruta del ASA.

2. Para resolver problemas del túnel IKEv2, puede utilizar estos debugs:

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. Para resolver el problema de tráfico en el ASA, tome la captura de paquetes y verifique la configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).