Migrar o túnel de criptografia baseado em política para o túnel de criptografia baseado em rota no ASA

Contents

Introdução

Este documento descreve a migração de túneis baseados em política para túneis baseados em rota no ASA.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Entendimento básico dos conceitos de VPN IKEv2-IPSec.
- Conhecimento da VPN IPSec no ASA e sua configuração.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASA: Código ASA versão 9.8(1) ou posterior.

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 a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapas para migração:

1. Remover a configuração de VPN baseada em política existente
2. Configurar o Perfil IPSec
3. Configurar a Interface de Túnel Virtual (VTI)
4. Configurar o Roteamento Estático ou o Protocolo de Roteamento Dinâmico

Configurações

Túnel baseado em política existente:

1. Configuração da Interface:

Interface de saída na qual o mapa de criptografia é vinculado.

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

2. Política IKEv2:

Ele define os parâmetros para a Fase 1 do processo de negociação do IPsec.

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

3. Grupo de Túneis:

Define parâmetros para conexões VPN. Os grupos de túnel são essenciais para configurar VPNs site a site, pois contêm informações sobre o peer, métodos de autenticação e vários parâmetros de conexão.

```
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 Criptografada:

Ele define o tráfego que deve ser criptografado e enviado pelo 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. Proposta Crypto IPSec:

Ele define a proposta de IPsec, que especifica os algoritmos de criptografia e integridade para a Fase 2 da negociação de IPsec.

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

6. Configuração do Mapa de Criptografia:

Ele define a política para conexões VPN IPsec, incluindo o tráfego a ser criptografado, os peers e a proposta de ipsec configurada anteriormente. Ele também está vinculado à interface que manipula o tráfego 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
```

Migração de túnel baseado em política para túnel baseado em rota:

1. Remova a configuração de VPN baseada em política existente:
   Primeiro, remova a configuração de VPN baseada em política existente. Isso inclui as entradas do mapa de criptografia para esse peer, ACLs e quaisquer configurações relacionadas.

```
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 de IPSec:
   Defina um perfil IPsec com a proposta IKEv2 ipsec ou conjunto de transformação existente.

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

3. Configurar a interface de túnel virtual (VTI):
   Crie uma Interface de Túnel Virtual (VTI) e aplique o perfil IPsec a ela.

```
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. Configurar o roteamento estático ou o protocolo de roteamento dinâmico:
   Adicione rotas estáticas ou configure um protocolo de roteamento dinâmico para rotear o tráfego através da interface do túnel. Neste cenário, estamos usando o roteamento estático.

   Roteamento estático:

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

Verificar

Depois de migrar de uma VPN baseada em políticas para uma VPN baseada em rotas usando interfaces de túnel virtual (VTIs) em um Cisco ASA, é crucial verificar se o túnel está ativo e funcionando corretamente. Aqui estão várias etapas e comandos que você pode usar para verificar o status e solucionar problemas, se necessário.

1. Verificar a interface do túnel
Verifique o status da interface do túnel para garantir que esteja ativa.

<#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
```

Esse comando fornece detalhes sobre a interface do túnel, incluindo seu status operacional, endereço IP e origem/destino do túnel. Procure estes indicadores:
· O status da interface está ativo.
· O status do protocolo de linha está ativo.

2. Verificar Associações de Segurança (SAs) IPsec

Verifique o status das SAs IPsec para garantir que o túnel tenha sido negociado com êxito.

<#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 exibe o status das SAs de IPsec, incluindo contadores para pacotes encapsulados e desencapsulados. Assegure que:
· Há SAs ativas para o túnel.
· Os contadores de encapsulamento e desencapsulamento estão aumentando, indicando o fluxo do tráfego.

Para obter informações mais detalhadas, você pode usar:

<#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
```

Esse comando mostra o status das SAs de IKEv2, que está no estado PRONTO.

3. Verificar o Roteamento
Verifique a tabela de roteamento para garantir que as rotas estejam apontando corretamente através da interface do 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
```

Procure as rotas que são roteadas através da interface do túnel.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

1. Verifique a configuração do túnel baseado em rota do ASA.

2. Para solucionar problemas do túnel IKEv2, você pode usar estas depurações:

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

3. Para solucionar o problema de tráfego no ASA, capture o pacote e verifique a configuração.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.