Migration d'un tunnel de chiffrement basé sur des politiques vers un tunnel de chiffrement basé sur des routes sur ASA

Table des matières

Introduction

Ce document décrit la migration de tunnels basés sur des politiques vers des tunnels basés sur des routes sur ASA.

Conditions préalables

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Compréhension de base des concepts VPN IKEv2-IPSec.
- Connaissance du VPN IPSec sur ASA et de sa configuration.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA : code ASA version 9.8(1) ou ultérieure.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Étapes de la migration :

1. Supprimer la configuration VPN basée sur des stratégies existante
2. Configuration du profil IPSec
3. Configuration de l'interface de tunnel virtuel (VTI)
4. Configuration du routage statique ou du protocole de routage dynamique

Configurations

Tunnel basé sur des stratégies existant :

1. Configuration de l’interface :

Interface de sortie à laquelle la carte de chiffrement est liée.

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

2. Stratégie IKEv2 :

Il définit les paramètres de la phase 1 du processus de négociation IPsec.

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

3. Groupe de tunnels :

Il définit les paramètres des connexions VPN. Les groupes de tunnels sont essentiels à la configuration des VPN de site à site, car ils contiennent des informations sur l'homologue, les méthodes d'authentification et divers paramètres de connexion.

```
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 de chiffrement :

Il définit le trafic qui doit être chiffré et envoyé via le tunnel.

```
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. Proposition Crypto IPSec :

Elle définit la proposition IPsec, qui spécifie les algorithmes de chiffrement et d'intégrité pour la phase 2 de la négociation IPsec.

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

6. Configuration de crypto-carte :

Il définit la stratégie pour les connexions VPN IPsec, y compris le trafic à chiffrer, les homologues et la proposition ipsec précédemment configurée. Il est également lié à l'interface qui gère le trafic 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
```

Migration d'un tunnel basé sur des politiques vers un tunnel basé sur des routes :

1. Supprimer la configuration VPN basée sur des stratégies existante :
   Commencez par supprimer la configuration VPN basée sur des stratégies existante. Cela inclut les entrées de crypto-carte pour cet homologue, les listes de contrôle d'accès et tous les paramètres associés.

```
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. Configuration du profil IPSec :
   Définissez un profil IPsec avec la proposition IKEv2 ipsec ou le jeu de transformation existant.

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

3. Configuration de l'interface de tunnel virtuel (VTI) :
   Créez une interface de tunnel virtuel (VTI) et appliquez-lui le profil 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. Configurer le routage statique ou le protocole de routage dynamique :
   Ajoutez des routes statiques ou configurez un protocole de routage dynamique pour acheminer le trafic via l'interface du tunnel. Dans ce scénario, nous utilisons le routage statique.

   Routage statique :

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

Vérifier

Après avoir migré d'un VPN basé sur des politiques vers un VPN basé sur des routes à l'aide d'interfaces de tunnel virtuelles (VTI) sur un Cisco ASA, il est essentiel de vérifier que le tunnel fonctionne correctement. Voici quelques étapes et commandes que vous pouvez utiliser pour vérifier l'état et résoudre les problèmes si nécessaire.

1. Vérification de l'interface du tunnel
Vérifiez l'état de l'interface du tunnel pour vous assurer qu'elle est active.

<#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
```

Cette commande fournit des détails sur l'interface du tunnel, y compris son état opérationnel, son adresse IP et la source/destination du tunnel. Recherchez les indicateurs suivants :
· L'état de l'interface est up.
· L'état du protocole de ligne est activé.

2. Vérifier les associations de sécurité IPsec

Vérifiez l'état des SA IPsec pour vous assurer que le tunnel a été négocié avec succès.

<#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

Cette commande affiche l'état des SA IPsec, y compris les compteurs des paquets encapsulés et décapsulés. Vérifiez les points suivants :
· Il existe des SA actives pour le tunnel.
· Les compteurs d'encapsulation et de décapsulation s'incrémentent, indiquant un flux de trafic.

Pour plus d'informations, vous pouvez utiliser :

<#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
```

Cette commande affiche l'état des associations de sécurité IKEv2, qui sont à l'état READY (PRÊT).

3. Vérification du routage
Vérifiez la table de routage pour vous assurer que les routes pointent correctement à travers l'interface du tunnel.

<#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

Recherchez les routes qui sont routées via l'interface du tunnel.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. Vérifiez la configuration de tunnel basée sur la route de l'ASA.

2. Pour dépanner le tunnel IKEv2, vous pouvez utiliser ces débogages :

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

3. Pour dépanner le problème de trafic sur l'ASA, prenez la capture de paquets et vérifiez la configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.