Migrazione del tunnel di crittografia basato su criteri al tunnel di crittografia basato su route sull'appliance ASA

Sommario

Introduzione

Questo documento descrive la migrazione dei tunnel basati su policy ai tunnel basati su routing sull'appliance ASA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei concetti della VPN con protocollo IKEv2-IPSec.
- Conoscenza della VPN IPSec sull'appliance ASA e della relativa configurazione.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA: codice ASA versione 9.8(1) o successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggi per la migrazione:

1. Rimuovi configurazione VPN basata su criteri esistente
2. Configurare il profilo IPSec
3. Configurare la VTI (Virtual Tunnel Interface)
4. Configurare il routing statico o il protocollo di routing dinamico

Configurazioni

Tunnel basato su criteri esistente:

1. Configurazione interfaccia:

Interfaccia in uscita a cui è associata la mappa crittografica.

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

2. Politica IKEv2:

Definisce i parametri per la fase 1 del processo di negoziazione IPSec.

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

3. Gruppo di tunnel:

Definisce i parametri per le connessioni VPN. I gruppi di tunnel sono essenziali per la configurazione delle VPN da sito a sito, in quanto contengono informazioni sul peer, sui metodi di autenticazione e sui vari parametri di connessione.

```
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 crittografico:

Definisce il traffico che deve essere crittografato e inviato attraverso il 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. Proposta Crypto IPSec:

Definisce la proposta IPSec, che specifica gli algoritmi di crittografia e integrità per la fase 2 della negoziazione IPSec.

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

6. Configurazione mappa crittografica:

Definisce i criteri per le connessioni VPN IPSec, inclusi il traffico da crittografare, i peer e la proposta IPSec configurata in precedenza. È inoltre associato all'interfaccia che gestisce il traffico 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
```

Migrazione del tunnel basato su criteri al tunnel basato su routing:

1. Rimuovi configurazione VPN basata su criteri esistente:
   Rimuovere innanzitutto la configurazione VPN basata su criteri esistente. Sono incluse le voci della mappa crittografica per il peer, gli ACL e le impostazioni correlate.

```
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. Configurazione profilo IPSec:
   Definire un profilo IPSec con la proposta IPSec IKEv2 o l'insieme di trasformazioni esistente.

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

3. Configurare Virtual Tunnel Interface (VTI):
   Creare una VTI (Virtual Tunnel Interface) e applicarvi il profilo 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. Configurare il routing statico o il protocollo di routing dinamico:
   Aggiungere route statiche o configurare un protocollo di routing dinamico per instradare il traffico tramite l'interfaccia del tunnel. In questo scenario, viene utilizzato il routing statico.

   Routing statico:

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

Verifica

Dopo aver eseguito la migrazione da una VPN basata su policy a una VPN basata su route con VTI (Virtual Tunnel Interfaces) su un'appliance Cisco ASA, è fondamentale verificare che il tunnel sia attivo e funzioni correttamente. Di seguito sono riportati diversi passaggi e comandi che è possibile utilizzare per verificare lo stato e, se necessario, risolvere i problemi.

1. Verifica dell'interfaccia del tunnel
Controllare lo stato dell'interfaccia del tunnel per verificare che sia attiva.

<#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
```

Questo comando fornisce dettagli sull'interfaccia del tunnel, tra cui lo stato operativo, l'indirizzo IP e l'origine/destinazione del tunnel. Cercare questi indicatori:
· Lo stato dell'interfaccia è attivo.
· Lo stato del protocollo di linea è attivo.

2. Verificare le associazioni di sicurezza IPSec

Controllare lo stato delle associazioni di protezione IPsec per verificare che la negoziazione del tunnel sia stata completata correttamente.

<#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

Con questo comando viene visualizzato lo stato delle associazioni di protezione IPsec, inclusi i contatori per i pacchetti incapsulati e decapsulati. Accertarsi che:
· Sono presenti associazioni di protezione attive per il tunnel.
· I contatori di incapsulamento e decapsulamento sono in aumento e indicano il flusso del traffico.

Per informazioni più dettagliate, è possibile utilizzare:

<#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
```

Con questo comando viene visualizzato lo stato delle associazioni di protezione IKEv2 nello stato READY.

3. Verifica del ciclo
Controllare la tabella di routing per verificare che i percorsi puntino correttamente all'interfaccia del 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

Cercare i percorsi instradati tramite l'interfaccia del tunnel.

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

1. Verificare la configurazione del tunnel ASA basata sul percorso.

2. Per risolvere i problemi del tunnel IKEv2, è possibile usare i seguenti debug:

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

3. Per risolvere il problema di traffico sull'appliance ASA, acquisire i pacchetti e controllare la configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).