Migration eines richtlinienbasierten Krypto-Tunnels zu einem routenbasierten Krypto-Tunnel auf der ASA

Inhalt

Einleitung

Dieses Dokument beschreibt die Migration von richtlinienbasierten Tunneln zu routenbasierten Tunneln auf der ASA.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- Grundlegendes Verständnis der IKEv2-IPSec-VPN-Konzepte
- Kenntnisse über IPSec VPN auf ASA und deren Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ASA: ASA Code Version 9.8(1) oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Schritte für die Migration:

1. Vorhandene richtlinienbasierte VPN-Konfiguration entfernen
2. Konfigurieren des IPSec-Profils
3. Konfigurieren der Virtual Tunnel Interface (VTI)
4. Konfigurieren von statischem Routing oder von dynamischem Routing-Protokoll

Konfigurationen

Vorhandener richtlinienbasierter Tunnel:

1. Schnittstellenkonfiguration:

Ausgangsschnittstelle, an die die Crypto Map gebunden ist.

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

2. IKEv2-Richtlinie:

Es definiert die Parameter für Phase 1 des IPsec-Aushandlungsprozesses.

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

3. Tunnelgruppe:

Sie definiert Parameter für VPN-Verbindungen. Tunnelgruppen sind für die Konfiguration von Site-to-Site-VPNs unerlässlich, da sie Informationen über den Peer, Authentifizierungsmethoden und verschiedene Verbindungsparameter enthalten.

```
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. Verschlüsselungs-ACL:

Er definiert den Datenverkehr, der verschlüsselt und durch den Tunnel gesendet werden muss.

```
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. Crypto IPSec-Angebot:

Es definiert den IPsec-Vorschlag, der die Verschlüsselungs- und Integritätsalgorithmen für Phase 2 der IPsec-Aushandlung spezifiziert.

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

6. Konfiguration der Kryptografiezuordnung:

Sie definiert die Richtlinie für IPsec-VPN-Verbindungen, einschließlich des zu verschlüsselnden Datenverkehrs, der Peers und des zuvor konfigurierten ipsec-Proposal. Sie ist außerdem an die Schnittstelle gebunden, die den VPN-Datenverkehr verarbeitet.

```
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 eines richtlinienbasierten Tunnels zu einem routenbasierten Tunnel:

1. Entfernen Sie die vorhandene richtlinienbasierte VPN-Konfiguration:
   Entfernen Sie zunächst die vorhandene richtlinienbasierte VPN-Konfiguration. Dies umfasst die Crypto Map-Einträge für diesen Peer, ACLs und alle zugehörigen Einstellungen.

```
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. IPSec-Profil konfigurieren:
   Definieren Sie ein IPsec-Profil mit dem vorhandenen IKEv2 ipsec-Vorschlag oder Transformationssatz.

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

3. Virtual Tunnel Interface (VTI) konfigurieren:
   Erstellen Sie eine Virtual Tunnel Interface (VTI), und wenden Sie das IPsec-Profil darauf an.

```
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. Konfigurieren von statischem oder dynamischem Routing-Protokoll:
   Fügen Sie statische Routen hinzu, oder konfigurieren Sie ein dynamisches Routing-Protokoll, um den Datenverkehr über die Tunnelschnittstelle weiterzuleiten. In diesem Szenario wird statisches Routing verwendet.

   Statisches Routing:

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

Überprüfung

Nach der Migration von einem richtlinienbasierten VPN zu einem routenbasierten VPN mithilfe von Virtual Tunnel Interfaces (VTIs) auf einer Cisco ASA muss unbedingt überprüft werden, ob der Tunnel betriebsbereit ist und ordnungsgemäß funktioniert. Im Folgenden finden Sie eine Reihe von Schritten und Befehlen, mit denen Sie den Status überprüfen und ggf. eine Fehlerbehebung durchführen können.

1. Überprüfen der Tunnelschnittstelle

Überprüfen Sie den Status der Tunnelschnittstelle, um sicherzustellen, dass sie aktiv ist.

<#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
```

Dieser Befehl liefert Details zur Tunnelschnittstelle, einschließlich Betriebsstatus, IP-Adresse und Tunnelquelle/-ziel. Achten Sie auf folgende Indikatoren:

- Der Schnittstellenstatus ist aktiv.
- Der Status des Leitungsprotokolls ist aktiv.

2. Überprüfen von IPsec-Sicherheitszuordnungen (SAs)

Überprüfen Sie den Status der IPsec-SAs, um sicherzustellen, dass der Tunnel erfolgreich ausgehandelt wurde.

<#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

Dieser Befehl zeigt den Status der IPsec-SAs an, einschließlich der Zähler für gekapselte und entkapselte Pakete. Stellen Sie Folgendes sicher:

- Es gibt aktive SAs für den Tunnel.
- Die Zähler für Kapselung und Entkapselung werden inkrementiert und zeigen den Datenverkehrsfluss an.

Weitere Informationen finden Sie unter:

<#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
```

Dieser Befehl zeigt den Status der IKEv2-SAs an, die sich im READY-Status befinden.

3. Routing überprüfen

Überprüfen Sie die Routing-Tabelle, um sicherzustellen, dass die Routen korrekt durch die Tunnelschnittstelle zeigen.

<#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
```

Suchen Sie nach Routen, die durch die Tunnelschnittstelle geroutet werden.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

1. Überprüfen der routenbasierten Tunnelkonfiguration der ASA

2. Sie können die folgenden Fehlerbehebungen für den IKEv2-Tunnel durchführen:

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

3. Um das Datenverkehrsproblem auf der ASA zu beheben, nehmen Sie die Paketerfassung, und überprüfen Sie die Konfiguration.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.