在ASA上將基於策略的加密隧道遷移到基於路由的加密隧道

目錄

簡介

本文檔介紹如何在ASA上將基於策略的隧道遷移至基於路由的隧道。

必要條件

需求

思科建議您瞭解以下主題：

- 對IKEv2-IPSec VPN概念有基礎瞭解。
- 瞭解ASA上的IPSec VPN及其配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA：ASA代碼版本9.8(1)或更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

遷移步驟：

1. 刪除現有的基於策略的VPN配置
2. 配置IPSec配置檔案
3. 設定虛擬通道介面(VTI)
4. 配置靜態路由或動態路由協定

組態

現有基於策略的隧道：

1. 介面配置：

繫結加密對映的出口介面。

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

2. IKEv2策略：

它定義了IPSec協商過程的第1階段的引數。

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

3. 隧道組：

它定義VPN連線的引數。隧道組對於配置站點到站點VPN至關重要，因為它們包含有關對等體、身份驗證方法和各種連線引數的資訊。

```
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. 加密ACL：

它定義了必須透過隧道加密和傳送的流量。

```
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. 加密IPSec提議：

它定義了IPsec方案，該方案指定IPsec協商第2階段的加密和完整性演算法。

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

6. 加密對映配置：

它定義IPSec VPN連線的策略，包括要加密的流量、對等體以及之前配置的ipsec提議。它還繫結到處理VPN流量的介面。

```
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
```

將基於策略的隧道遷移到基於路由的隧道：

1. 刪除現有的基於策略的VPN配置：
   首先，刪除現有的基於策略的VPN配置。其中包括該對等體的加密對映條目、ACL以及任何相關設定。

```
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. 配置IPSec配置檔案：
使用現有IKEv2 ipsec-proposal或transform-set定義IPsec配置檔案。

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

3. 設定虛擬通道介面(VTI)：
建立虛擬隧道介面(VTI)並將IPSec配置檔案應用於該介面。

```
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. 配置靜態路由或動態路由協定：
增加靜態路由或配置動態路由協定以透過隧道介面路由流量。在此場景中，我們使用的是靜態路由。

靜態路由：

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

驗證

使用Cisco ASA上的虛擬隧道介面(VTI)從基於策略的VPN遷移到基於路由的VPN後，驗證隧道是否啟動並正常運行至關重要。以下是幾個步驟和命令，您可以使用這些命令來驗證狀態並在必要時進行故障排除。

1. 檢驗隧道介面
檢查通道介面的狀態，以確保其為up狀態。

```
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
```

此命令提供有關隧道介面的詳細資訊，包括其運行狀態、IP地址和隧道源/目標。尋找下列指標：
· 介面狀態為up。
· 線路協定狀態為up。

2. 驗證IPsec安全關聯(SA)

檢查IPSec SA的狀態，確保已成功協商隧道。

```
<#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

此命令顯示IPsec SA的狀態，包括封裝和解封資料包的計數器。確保：
· 通道具有活動的SA。
· 封裝和解除封裝計數器增加，表示流量傳輸。

如需更多詳細資訊，您可以使用：

<#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
```

此命令顯示IKEv2 SA的狀態，它處於READY狀態。

3. 檢驗路由
檢查路由表以確保路由正確指向隧道介面。

<#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
```

查詢透過隧道介面路由的路由。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 檢驗ASA的基於路由的隧道配置。

2. 要排除IKEv2隧道的故障，可以使用以下調試：

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

3. 要排除ASA上的流量問題，請捕獲資料包並檢查配置。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。