정책 기반 암호화 터널을 ASA의 경로 기반 암호화 터널로 마이그레이션

목차

소개

이 문서에서는 ASA에서 정책 기반 터널을 경로 기반 터널로 마이그레이션하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- IKEv2-IPSec VPN 개념에 대한 기본적인 이해
- ASA의 IPSec VPN 및 해당 구성에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA: ASA 코드 버전 9.8(1) 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

마이그레이션 단계:

1. 기존 정책 기반 VPN 구성 제거
2. IPSec 프로필 구성
3. VTI(가상 터널 인터페이스) 구성
4. 고정 라우팅 또는 동적 라우팅 프로토콜 구성

설정

기존 정책 기반 터널:

1. 인터페이스 구성:

암호화 맵이 바인딩된 이그레스(egress) 인터페이스.

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

2. IKEv2 정책:

IPsec 협상 프로세스의 1단계에 대한 매개변수를 정의합니다.

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

3. 터널 그룹

VPN 연결에 대한 매개변수를 정의합니다. 터널 그룹은 피어, 인증 방법 및 다양한 연결 매개변수에 대한 정보를 포함하므로 사이트 간 VPN을 구성하는 데 필수적입니다.

```
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. 암호화 ACL:

이는 터널을 통해 암호화 및 전송해야 하는 트래픽을 정의합니다.

```
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. 암호화 IPSec 제안

IPsec 제안을 정의합니다. IPsec 제안에서는 IPsec 협상의 2단계에 대한 암호화 및 무결성 알고리즘을 지정합니다.

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

6. 암호화 맵 구성:

암호화할 트래픽, 피어, 이전에 구성한 ipsec-proposal을 포함하여 IPsec VPN 연결에 대한 정책을 정의합니다. 또한 VPN 트래픽을 처리하는 인터페이스에 바인딩됩니다.

```
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
```

정책 기반 터널을 경로 기반 터널로 마이그레이션:

1. 기존 정책 기반 VPN 컨피그레이션을 제거합니다.
   먼저 기존 정책 기반 VPN 컨피그레이션을 제거합니다. 여기에는 해당 피어에 대한 암호화 맵

항목, ACL 및 관련 설정이 포함됩니다.

```
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 프로필을 구성합니다.
   기존 IKEv2 ipsec-proposal 또는 transform-set으로 IPsec 프로필을 정의합니다.

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

3. VTI(Virtual Tunnel Interface) 구성:
   VTI(Virtual Tunnel Interface)를 생성하고 여기에 IPsec 프로필을 적용합니다.

```
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. 고정 라우팅 또는 동적 라우팅 프로토콜을 구성합니다.
   고정 경로를 추가하거나 터널 인터페이스를 통해 트래픽을 라우팅하도록 동적 라우팅 프로토콜을 구성합니다. 이 시나리오에서는 고정 라우팅을 사용합니다.

   정적 라우팅:

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

다음을 확인합니다.

Cisco ASA에서 VTI(Virtual Tunnel Interface)를 사용하여 정책 기반 VPN에서 경로 기반 VPN으로 마이그레이션한 후에는 터널이 작동 중이고 올바르게 작동하는지 확인하는 것이 중요합니다. 상태를 확인하고 필요한 경우 문제를 해결하는 데 사용할 수 있는 몇 가지 단계와 명령은 다음과 같습니다.

1. 터널 인터페이스 확인

터널 인터페이스의 상태를 확인하여 가동 상태인지 확인합니다.

<#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
```

이 명령은 작동 상태, IP 주소, 터널 소스/대상을 포함하여 터널 인터페이스에 대한 세부 정보를 제공합니다. 다음 지표를 확인합니다.
· 인터페이스 상태가 up입니다.
· 회선 프로토콜 상태가 up입니다.

2. IPsec SA(Security Association) 확인

IPsec SA의 상태를 확인하여 터널이 성공적으로 협상되었는지 확인합니다.

<#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

이 명령은 캡슐화된 패킷과 캡슐화되지 않은 패킷에 대한 카운터를 포함하여 IPsec SA의 상태를 표시합니다. 다음 사항을 확인합니다.
· 터널에 대한 활성 SA가 있습니다.
· 캡슐화 및 역캡슐화 카운터가 증가하여 트래픽 흐름을 나타냅니다.

자세한 내용은 다음을 사용할 수 있습니다.

<#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
```

이 명령은 READY 상태인 IKEv2 SA의 상태를 표시합니다.

3. 라우팅 확인
라우팅 테이블에서 경로가 터널 인터페이스를 올바르게 가리키는지 확인합니다.

<#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
```

터널 인터페이스를 통해 라우팅되는 경로를 찾습니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

1. ASA의 경로 기반 터널 컨피그레이션을 확인합니다.

2. IKEv2 터널의 문제를 해결하려면 다음 디버그를 사용할 수 있습니다.

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

3. ASA에서 트래픽 문제를 해결하려면 패킷 캡처를 수행하고 컨피그레이션을 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.