ASA 8.4 코드에서 IKEv1을 IKEv2 L2L 터널 구성으로 신속하게 마이그레이션

목차

소개

이 문서에서는 IKEv2 및 IKEv1의 마이그레이션 프로세스에 대한 정보를 제공합니다.

사전 요구 사항

요구 사항

IKEv1 PSK(Pre-shared Key) 인증 방법으로 IPsec을 실행하는 Cisco ASA Security Appliance가 있는지 확인하고 IPsec 터널이 작동 상태인지 확인합니다.

IKEv1 PSK 인증 방법으로 IPsec을 실행하는 Cisco ASA Security Appliance의 컨피그레이션의 예는 PIX/ASA 7.x 이상을 참조하십시오.PIX-to-PIX VPN 터널 컨피그레이션 예.

사용되는 구성 요소

이 문서의 정보는 이러한 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- 버전 8.4.x 이상에서 실행되는 Cisco ASA 5510 Series Security Appliance

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

IKEv2로 마이그레이션해야 하는 이유

- IKEv2는 네트워크 공격 복원력을 향상시킵니다.IKEv2는 IPsec 개시자를 검증할 때 네트워크에서 DoS 공격을 완화할 수 있습니다.DoS 취약성을 익스플로잇하기 어렵게 만들기 위해 응답자는 정상적 연결임을 응답자에게 확인해야 하는 개시자에게 쿠키를 요청할 수 있습니다 .IKEv2에서 responder 쿠키는 DoS 공격을 완화하여 responder가 IKE 개시자의 상태를 유지하거나 initiator가 responder가 보낸 쿠키를 반환하지 않는 한 D-H 작업을 수행하지 않도록 합니다.응답자는 최소 CPU를 사용하며 개시자를 완전히 검증할 수 있을 때까지 SA(Security Association)에 대한 상태를 커밋하지 않습니다.
- IKEv2는 서로 다른 VPN 제품 간의 IPsec 설정의 복잡성을 줄여줍니다.상호운용성을 높이고 레거시 인증 방법을 위한 표준 방법을 허용합니다.IKEv2는 DPD(Dead Peer Detection), NAT-T(NAT Traversal) 또는 Initial Contact와 같은 내장 기술을 제공하기 때문에 벤더 간에 원활한 IPsec 상호운용성을 제공합니다.
- IKEv2는 오버헤드가 적습니다.오버헤드가 줄어들어 SA 설정 레이턴시가 개선됩니다.여러 요청이 전송 중에 허용됩니다(예: 여러 하위 SA가 병렬로 설정된 경우).
- IKEv2는 SA 지연이 감소되었습니다.IKEv1에서 SA 생성 지연은 패킷 볼륨이 증폭될 때 증폭됩니다.IKEv2는 패킷 볼륨이 증폭될 때 동일한 평균 지연을 유지합니다.패킷 볼륨이 증폭될 때 패킷 헤더의 증폭을 암호화하고 처리하는 시간이 걸립니다.새 SA 설정을 생성해야 하는 경우 더 많은 시간이 필요합니다.IKEv2에서 생성된 SA가 IKEv1에서 생성된 SA보다 작습니다. 증폭 패킷 크기의 경우 SA를 생성하는 데 걸린 시간은 거의 일정합니다.
- IKEv2는 키 재설정 시간이 더 빠릅니다.IKE v1은 IKEv2보다 SA를 다시 키화하는 데 더 많은 시간이 걸립니다. SA용 IKEv2 rekey는 보안 성능을 개선하고 전환 중에 손실된 패킷 수를 줄입니다.IKEv2에서 IKEv1의 특정 메커니즘(예: ToS 페이로드, SA 수명 선택, SPI 고유성)을 재정의하므로 IKEv2에서 손실되고 중복되는 패킷이 더 적습니다. 따라서 SA를 다시 키 지정할 필요가 없습니다.

참고: 네트워크 보안은 가장 약한 링크만큼 강력할 수 있으므로 IKEv2는 IKEv1과 상호 운용되지 않습니다.

마이그레이션 개요

IKEv1 또는 SSL이 이미 있는 경우 ASA는 마이그레이션 프로세스를 단순화합니다.명령줄에서 migrate 명령을 **입력합니다**.

```
migrate {l2l | remote-access {ikev2 | ssl} | overwrite}
```

참고 사항:

- 키워드 정의:**l2l** - 현재 IKEv1 l2l 터널을 IKEv2로 변환합니다.**원격 액세스** - 원격 액세스 컨피그레이션을 변환합니다.IKEv1 또는 SSL 터널 그룹을 IKEv2로 변환할 수 있습니다.**덮어쓰기** - 덮어쓸 IKEv2 컨피그레이션이 있는 경우 이 키워드는 현재 IKEv1 컨피그레이션을 변환하고 불필

요한 IKEv2 컨피그레이션을 제거합니다.

- IKEv2에는 PSK 인증에 대칭 및 비대칭 키를 모두 사용할 수 있는 기능이 있습니다.ASA에서 **migration** 명령을 입력하면 ASA는 대칭 PSK가 있는 IKEv2 VPN을 자동으로 생성합니다.
- 명령을 입력하면 현재 IKEv1 컨피그레이션이 삭제되지 않습니다.대신 IKEv1 및 IKEv2 컨피그레이션이 모두 동일한 암호화 맵에서 병렬로 실행됩니다.수동으로 수행할 수도 있습니다 .IKEv1 및 IKEv2가 모두 병렬로 실행되는 경우 IKEv2에 연결 시도 실패로 이어질 수 있는 프로토콜 또는 구성 문제가 있을 때 IPsec VPN 이니시에이터가 IKEv2에서 IKEv1로 폴백할 수 있습니다.IKEv1 및 IKEv2를 병렬로 실행할 때 롤백 메커니즘도 제공하고 마이그레이션을 더 쉽게 합니다.
- IKEv1 및 IKEv2가 모두 병렬로 실행되는 경우 ASA는 초기자에 공통되는 터널 관리자/IKE라는 모듈을 사용하여 연결에 사용할 암호화 맵 및 IKE 프로토콜 버전을 결정합니다.ASA는 항상 IKEv2를 시작하는 것을 선호하지만, 시작할 수 없으면 IKEv1로 돌아갑니다.
- 이중화에 사용된 여러 피어는 ASA의 IKEv2에서 지원되지 않습니다.IKEv1에서는 이중화를 위해 set peer 명령을 입력할 때 동일한 암호화 맵 아래에 둘 이상의 피어를 가질 수 있습니다.첫 번째 피어가 기본 피어가 되며, 실패하면 두 번째 피어가 시작합니다.Cisco 버그 ID CSCud22276(등록된 고객만 해당) , ENH:여러 피어가 IKEv2를 지원합니다.

마이그레이션 프로세스

구성

이 예에서는 PSK(Pre-Shared Key) 인증을 사용하는 IKEv1 VPN이 ASA에 있습니다.

참고: 여기에 표시된 컨피그레이션은 VPN 터널에만 해당됩니다.

현재 IKEv1 VPN을 사용하는 ASA 컨피그레이션(마이그레이션 전)

```
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset
crypto map vpn interface outside
crypto isakmp disconnect-notify
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3
```

ASA IKEv2 컨피그레이션(마이그레이션 후)

참고: 굵게 기울임꼴로 표시된 변경 내용.

```
ASA-2(config)# migrate l2l
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac

crypto ipsec IKEv2 ipsec-proposal goset protocol esp encryption 3des protocol esp integrity sha-
1
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset

crypto map vpn 12 set IKEv2 ipsec-proposal goset
crypto map vpn interface outside
crypto isakmp disconnect-notify

crypto IKEv2 policy 1 encryption 3des integrity sha group 5 prf sha lifetime seconds 86400
crypto IKEv2 enable outside
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3

IKEv2 remote-authentication pre-shared-key ***** IKEv2 local-authentication pre-shared-key *****
```

IKEv2 터널 설정 확인

```
ASA1# sh cry IKEv2 sa detail

IKEv2 SAs:
Session-id:12, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local                Remote     Status        Role
102061223 192.168.1.1/500  192.168.2.2/500  READY    INITIATOR
     Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,Auth verify: PSK
     Life/Active Time: 86400/100 sec
     Status Description: Negotiation done
     Local spi: 297EF9CA996102A6       Remote spi: 47088C8FB9F039AD
     Local id: 192.168.1.1
     Remote id: 192.168.2.2
      DPD configured for 10 seconds, retry 3
     NAT-T is not detected
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
         remote selector 10.20.20.0/0 - 10.20.20.255/65535
         ESP spi in/out: 0x637df131/0xb7224866

ASA1# sh crypto ipsec sa
```

```
interface: outside
   Crypto map tag: vpn, seq num: 12, local addr: 192.168.1.1
     access-list NEWARK extended permit ip 10.10.10.0 255.255.255.0
     10.20.20.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
     current_peer: 192.168.2.2
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

마이그레이션 후 PSK 확인

PSK를 확인하려면 글로벌 컨피그레이션 모드에서 이 명령을 실행할 수 있습니다.

```
more system: running-config | beg tunnel-group
```

IKEv2 및 터널 관리자 프로세스

앞에서 언급한 대로, ASA는 Initiator에서 공통적으로 사용되는 터널 관리자/IKE라는 모듈을 사용하여 연결에 사용할 암호화 맵 및 IKE 프로토콜 버전을 확인합니다.모듈을 모니터링하려면 다음 명령을 입력합니다.

```
debug crypto ike-common <level>
```

IKEv2 터널을 시작하기 위해 트래픽이 전달될 때 **debug**, **logging** 및 **show** 명령이 수집되었습니다 .명확성을 위해 일부 출력이 생략되었습니다.

```
ASA1(config)# logging enable
ASA1(config)# logging list IKEv2 message 750000-752999
ASA1(config)# logging console IKEv2
ASA1(config)# exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5

%ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-5-750001: Local:192.168.1.1:500 Remote:192.168.2.2:500 Username:Unknown
Received request to establish an IPsec tunnel; local traffic selector = Address Range:
10.10.10.11-10.10.10.11 Protocol: 0
Port Range: 0-65535; remote traffic selector = Address Range:
10.20.20.21-10.20.20.21 Protocol: 0 Port Range: 0-65535
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv2.  Map Tag = vpn.  Map Sequence Number = 12.
IKEv2-PLAT-3: attempting to find tunnel group for IP: 192.168.2.2
IKEv2-PLAT-3: mapped to tunnel group 192.168.2.2 using peer IP
    26%ASA-5-750006: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA UP. Reason: New Connection Established
43%ASA-5-752016: IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x0000000000000000 MID=00000000
IKEv2-PROTO-3: (12): Insert SA
IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
```

```
IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PROTO-3: (12): Verify peer's policy
IKEv2-PROTO-3: (12): Get peer authentication method
IKEv2-PROTO-3: (12): Get peer's preshared key for 192.168.2.2
IKEv2-PROTO-3: (12): Verify authentication data
IKEv2-PROTO-3: (12): Use preshared key for id 192.168.2.2, key len 5
IKEv2-PROTO-2: (12): SA created; inserting SA into database
IKEv2-PLAT-3:
CONNECTION STATUS: UP... peer: 192.168.2.2:500, phase1_id: 192.168.2.2
IKEv2-PROTO-3: (12): Initializing DPD, configured for 10 seconds
IKEv2-PLAT-3: (12) DPD Max Time will be: 10
IKEv2-PROTO-3: (12): Checking for duplicate SA
Mar 22 15:03:52 [IKE COMMON DEBUG]IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager Removed entry.
Map Tag = vpn.  Map Sequence Number = 12.
```

IKEv2에서 IKEv1 폴백 메커니즘

IKEv1 및 IKEv2를 병렬로 사용하는 경우 ASA는 항상 IKEv2를 시작하는 것을 선호합니다. ASA가 그럴 수 없는 경우 IKEv1로 돌아갑니다. 터널 관리자/IKE 공통 모듈은 이 프로세스를 관리합니다.이 니시에이터의 이 예에서는 IKEv2 SA가 지워지고 IKEv2가 의도적으로 잘못 구성됨(IKEv2 제안이 제거됨)으로 폴백 메커니즘을 시연합니다.

```
ASA1# clear  crypto  IKEv2 sa

%ASA-5-750007: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA DOWN. Reason: operator request
ASA1(config)# no crypto map vpn 12 set IKEv2 ipsec-proposal GOSET
ASA1# (config ) logging enable
ASA1# (config ) logging list IKEv2 message 750000-752999
ASA1# (config ) logging console IKEv2
ASA1# (config ) exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5
%ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-4-752010: IKEv2 Doesn't have a proposal specified
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv1.  Map Tag = vpn.  Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv2 Doesn't have a proposal specified
%ASA-5-752016: IKEv1 was successful at setting up a tunnel.  Map Tag = vpn.
Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv1 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.

ASA1(config)# sh cry IKEv2 sa
There are no IKEv2 SAs
ASA1(config)# sh cry IKEv1 sa
IKEv1 SAs:
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1   IKE Peer: 192.168.2.2
   Type    : L2L             Role    : initiator
```

```
Rekey   : no               State   : MM_ACTIVE
```

IKEv2 강화

IKEv2를 사용할 때 추가 보안을 제공하려면 다음 옵션 명령을 사용하는 것이 좋습니다.

- **Crypto IKEv2 쿠키 챌린지**:절반이 열린 SA 시작 패킷에 응답하여 ASA가 피어 디바이스에 쿠키 챌린지를 전송할 수 있도록 합니다.
- **Crypto IKEv2 limit max-sa**:ASA에서 IKEv2 연결 수를 제한합니다.기본적으로 허용되는 최대 IKEv2 연결은 ASA 라이센스에서 지정한 최대 연결 수와 같습니다.
- **Crypto IKEv2 limit max-in-negotiation-sa**:ASA에서 IKEv2 협상 중(열린) SA의 수를 제한합니다 .crypto IKEv**2 cookie-challenge** 명령과 함께 사용할 경우 cookie-challenge 임계값이 이 제한보다 낮아야 합니다.
- 비대칭 키를 사용합니다.마이그레이션 후에는 다음과 같이 비대칭 키를 사용하도록 컨피그레이션을 수정할 수 있습니다.

```
ASA-2(config)# more system:running-config
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key cisco1234
 IKEv2 remote-authentication pre-shared-key cisco1234
 IKEv2 local-authentication pre-shared-key cisco123
```

IKEv2 사전 공유 키를 위해 다른 피어에 컨피그레이션을 미러링해야 함을 인식하는 것이 중요합니다.한 쪽에서 다른 쪽으로 컨피그레이션을 선택하여 붙여넣으면 작동하지 않습니다.

참고: 이러한 명령은 기본적으로 비활성화되어 있습니다.

관련 정보

- 기술 지원 및 문서