SWIFT-migratie van IKEv1 naar IKEv2 L2L-tunnelconfiguratie op ASA 8.4-code

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Conventies
Waarom migreren naar IKEv2?
Overzicht van migratie
Migratieproces
Configuratie
IKEv2-tunnelverificatie
PSK-verificatie na migratie
IKEv2- en tunnelbeheerproces
IKEv2 op IKEv1-terugvalmechanisme
Harden IKEv2
Gerelateerde informatie

Inleiding

Dit document bevat informatie over IKEv2 en het migratieproces vanaf IKEv1.

Voorwaarden

Vereisten

Zorg ervoor dat u een Cisco ASA security applicatie hebt die IPsec doorvoert met de IKEv1 Pre-Shared Key (PSK) authenticatiemethode, en zorg ervoor dat de IPsec-tunnel in de operationele status staat is.

Voor een voorbeeld van de configuratie van een Cisco ASA security applicatie die IPsec met IKEv1 PSK-detectiemethode doorvoert, raadpleegt u PIX/ASA 7.x en hoger: PIX-to-PIX VPN-tunnelconfiguratievoorbeeld.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies.

- Cisco ASA 5510 Series security applicatie die werkt met versie 8.4.x en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Waarom migreren naar IKEv2?

- IKEv2 biedt betere veerkracht van netwerkaanvallen. IKEv2 kan een DoS-aanval op het netwerk verminderen wanneer deze de IPsec-initiator bevestigt. Om DoS kwetsbaar te maken voor uitbuiting, kan de responder vragen om een koekje aan de initiator, die de responder moet verzekeren dat dit een normale verbinding is. In IKEv2 verminderen de "responder"-koekjes de DoS-aanval, zodat de responder geen staat van de IKE-initiator heeft en geen D-H-handeling uitvoert, tenzij de initiator het koekje teruggeeft dat door de responder wordt gestuurd. De responder gebruikt minimale CPU's en verbindt zich er niet toe een status te verlenen aan een Security Association (SA), totdat deze de initiator volledig kan valideren.
- IKEv2 vermindert de complexiteit in IPsec vestiging tussen verschillende VPN-producten. Het vergroot de interoperabiliteit en maakt ook een standaardmanier mogelijk voor methoden voor nationale echtheidscontrole. IKEv2 biedt een naadloze interoperabiliteit van IPsec tussen leveranciers omdat deze systemen ingebouwd zijn, zoals Dead Peer Detection (DPD), NAT Traversal (NAT-T) of Initiële contactgegevens.
- IKEv2 heeft minder overhead. Met minder overhead biedt het verbeterde SA setup-vertraging. Meervoudige verzoeken zijn toegestaan op doorreis (bijvoorbeeld wanneer een veelvoud van kinderen-SA's parallel is opgezet).
- IKEv2 heeft een lagere SA vertraging. In IKEv1 is de vertraging van de SA-aanmaak groter naarmate het pakketvolume groter wordt. IKEv2 behoudt dezelfde gemiddelde vertraging wanneer het pakketvolume wordt vergroot. Wanneer het pakketvolume wordt vergroot, wordt de tijd om de pakketheader te versleutelen en te verwerken vergroot. Wanneer er een nieuwe SA-vestiging moet worden gecreëerd, is meer tijd nodig. De SA die door IKEv2 wordt gegenereerd is minder dan die welke door IKEv1 wordt gegenereerd. Voor een versterkte pakketgrootte is de tijd die nodig is om een SA te maken vrijwel constant.
- IKEv2 heeft een snellere rektijd. IKE v1 neemt meer tijd in beslag om SA's te rekken dan IKEv2. IKEv2 rekey voor SA biedt verbeterde veiligheidsprestaties en vermindert het aantal pakketten dat verloren is gegaan in de transitie. Als gevolg van de herdefinitie van bepaalde mechanismen van IKEv1 (zoals ToS payload, keuze van SA-leven en een unieke SPI-eenheid) in IKEv2, worden minder pakketten verloren en gedupliceerd in IKEv2. Daarom is er minder behoefte om SA's te hervatten.

Opmerking: omdat de netwerkbeveiliging alleen zo sterk kan zijn als de zwakste link, werkt IKEv2 niet samen met IKEv1.

Overzicht van migratie

Als uw IKEv1- of zelfs SSL-configuratie al bestaat, maakt de ASA het migratieproces eenvoudig.

Voer in de opdrachtregel de opdracht **migreren in**:

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

Opmerkingen:

- Trefwoorddefinities:**l2l** - Hiermee worden de huidige IKEv1 l2l-tunnels naar IKEv2 geconverteerd.**toegang op afstand** - Hiermee converteert u de configuratie van de toegang op afstand. U kunt de IKEv1 of de SSL-tunnelgroepen converteren naar IKEv2.**overschrijven** - Als u een IKEv2-configuratie hebt die u wilt overschrijven, dan converteert dit sleutelwoord de huidige IKEv1-configuratie en verwijdert u de overbodige IKEv2-configuratie.
- Het is belangrijk op te merken dat IKEv2 zowel symmetrische als asymmetrische sleutels kan gebruiken voor PSK-authenticatie. Wanneer het migratiebevel op de ASA wordt ingevoerd, creëert de ASA automatisch een IKEv2 VPN met een symmetrische PSK.
- Nadat de opdracht is ingevoerd, worden de huidige IKEv1-configuraties niet verwijderd. In plaats daarvan draaien zowel IKEv1 als IKEv2 configuraties parallel en op dezelfde crypto kaart. U kunt dit ook handmatig doen. Wanneer zowel IKEv1 als IKEv2 parallel lopen, staat dit een IPsec VPN-initiator toe om van IKEv2 naar IKEv1 te fallback wanneer er een protocol- of configuratieprobleem met IKEv2 is dat kan leiden tot een poging tot het onjuist aansluiten. Wanneer IKEv1 en IKEv2 parallel lopen, biedt het ook een terugdraaiingsmechanisme en maakt het de migratie gemakkelijker.
- Wanneer zowel IKEv1 als IKEv2 parallel lopen, gebruikt ASA een module genaamd tunnelbeheerder/IKE die gebruikelijk is op de initiator om de crypto map en IKE protocol versie te bepalen die gebruikt moet worden voor een verbinding. De ASA geeft altijd de voorkeur aan het initiëren van IKEv2, maar als dat niet kan, valt het terug op IKEv1.
- Meervoudige peers gebruikt voor redundantie worden niet ondersteund met IKEv2 op de ASA. In IKEv1 kan voor redundantiedoeleinden meer dan één peer onder dezelfde crypto kaart zijn geplaatst wanneer u de **ingestelde peer** opdracht ingaat. De eerste peer zal de primaire zijn en als het mislukt, zal de tweede peer in werking treden. Raadpleeg Cisco bug-ID CSCud2276 (alleen geregistreerde klanten), ENH: Ondersteuning van meerdere peers voor IKEv2.

Migratieproces

Configuratie

In dit voorbeeld bestaat IKEv1 VPN dat pre-Shared Key (PSK) authenticatie gebruikt op de ASA.

Opmerking: de configuratie die hier wordt getoond, is alleen relevant voor de VPN-tunnel.

ASA-configuratie met een huidig IKEv1 VPN (voor migratie)

```
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-configuratie (na migratie)

Opmerking: Wijzigingen worden cursief gemarkeerd.

```
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-tunnelverificatie

```
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
```

PSK-verificatie na migratie

Om uw PSK te controleren kunt u deze opdracht in de wereldwijde configuratie-modus uitvoeren:

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

IKEv2- en tunnelbeheerproces

Zoals eerder vermeld, gebruikt de ASA een module genaamd tunnelbeheerder/IKE die gebruikelijk is op de initiator om de crypto kaart en IKE protocol versie te bepalen die gebruikt moet worden voor een verbinding. Typ deze opdracht om de module te controleren:

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

De opdrachten **debug**, **logging** en **show** werden verzameld wanneer het verkeer werd doorgegeven om de IKEv2-tunnel te openen. Voor de duidelijkheid is een deel van de productie weggelaten.

```
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.
```

IKEv2 op IKEv1-terugvalmechanisme

Met zowel IKEv1 als IKEv2 parallel geeft de ASA er altijd de voorkeur aan om IKEv2 te initiëren. Als de ASA niet kan, valt het terug naar IKEv1. De gemeenschappelijke module van de Tunnelbeheerder/IKE beheert dit proces. In dit voorbeeld voor de initiatiefnemer is de IKEv2 SA geklaard en is IKEv2 nu opzettelijk onjuist geconfigureerd (het IKEv2-voorstel wordt verwijderd) om het valterugvalmechanisme aan te tonen.

```
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
```

Harden IKEv2

Om extra beveiliging te bieden wanneer IKEv2 wordt gebruikt, worden deze optionele opdrachten sterk aanbevolen:

- **Crypto IKEv2 koekje-uitdaging**: Maakt de ASA in staat om koekjesuitdagingen naar peer apparaten te sturen in antwoord op half-open SA geïnitieerde pakketten.
- **Crypto IKEv2 limiet max-sa**: Beperkt het aantal IKEv2-verbindingen op de ASA. Standaard is de maximaal toegestane IKEv2 verbinding gelijk aan het maximale aantal verbindingen dat door de ASA licentie gespecificeerd is.
- **Crypto IKEv2 limiet max-in-onderhandeling-sa**: Beperkt het aantal IKEv2 in onderhandeling (open) SAs op de ASA. Zorg er bij gebruik in combinatie met de **crypto IKEv2** opdracht voor dat de aanroepingsdrempel lager is dan deze limiet.
- Gebruik asymmetrische toetsen. Na migratie kan de configuratie worden aangepast om asymmetrische toetsen te gebruiken, zoals hieronder wordt getoond:

```
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
```

Het is belangrijk om te realiseren dat de configuratie gespiegeld moet worden op de andere peer voor de IKEv2 pre-gedeeld sleutel. Het werkt niet als u de configuratie van de ene kant naar de andere selecteert en kleeft.

N.B.: Deze opdrachten worden standaard uitgeschakeld.

Gerelateerde informatie

- Technische ondersteuning en documentatie