Migrazione rapida della configurazione del tunnel IKEv1 a IKEv2 L2L su codice ASA 8.4

Sommario

Introduzione

In questo documento vengono fornite informazioni su IKEv2 e sul processo di migrazione da IKEv1.

Prerequisiti

Requisiti

Verificare che le appliance di sicurezza Cisco ASA eseguano IPsec con il metodo di autenticazione a chiave precondivisa (PSK) IKEv1 e che il tunnel IPsec sia in stato operativo.

Per un esempio di configurazione di un'appliance di sicurezza Cisco ASA con IPsec e metodo di autenticazione PSK IKEv1, fare riferimento a PIX/ASA 7.x e versioni successive: Esempio di configurazione del tunnel VPN da PIX a PIX.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software.

- Cisco ASA serie 5510 Security Appliance con versione 8.4.x e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Perché migrare a IKEv2?

- IKEv2 offre una migliore resilienza agli attacchi di rete. IKEv2 è in grado di mitigare un attacco DoS alla rete quando convalida l'iniziatore IPsec. Per rendere la vulnerabilità DoS difficile da sfruttare, il responder può chiedere un cookie all'iniziatore che deve assicurare al responder che questa è una connessione normale. In IKEv2, i cookie del risponditore mitigano l'attacco DoS in modo che il risponditore non mantenga uno stato dell'iniziatore IKE o non esegua un'operazione D-H a meno che l'iniziatore restituisca il cookie inviato dal risponditore. Il risponditore utilizza una quantità minima di CPU e non esegue il commit dello stato in un'associazione di protezione (SA, Security Association) fino a quando non è in grado di convalidare completamente l'iniziatore.
- IKEv2 riduce la complessità della definizione di IPsec tra prodotti VPN diversi. Aumenta l'interoperabilità e consente di utilizzare un metodo standard per i metodi di autenticazione legacy. IKEv2 fornisce un'interoperabilità IPsec perfetta tra i fornitori poiché offre tecnologie integrate quali Dead Peer Detection (DPD), NAT Traversal (NAT-T) o Initial Contact.
- IKEv2 ha un sovraccarico minore. Con un minore sovraccarico, offre una migliore latenza di configurazione della SA. In transito sono consentite più richieste, ad esempio quando un multiplo di associazioni di protezione figlio viene impostato in parallelo.
- Ritardo SA ridotto per IKEv2. In IKEv1 il ritardo nella creazione delle associazioni di protezione si amplifica man mano che il volume del pacchetto si amplifica. IKEv2 mantiene lo stesso ritardo medio quando il volume del pacchetto si amplifica. Quando il volume del pacchetto si amplifica, il tempo necessario per crittografare ed elaborare l'intestazione del pacchetto aumenta. La creazione di una nuova associazione di sicurezza richiede più tempo. L'associazione di protezione generata da IKEv2 è minore di quella generata da IKEv1. Per un pacchetto di dimensioni amplificate, il tempo necessario per creare un'associazione di protezione è quasi costante.
- Tempo di rigenerazione chiavi più veloce per IKEv2. La rigenerazione delle chiavi delle associazioni di protezione richiede più tempo di quella di IKEv2. La rigenerazione delle chiavi IKEv2 per le associazioni di protezione offre migliori prestazioni di protezione e riduce il numero di pacchetti persi durante la transizione. A causa della ridefinizione di alcuni meccanismi di IKEv1 (ad esempio il payload ToS, la scelta della durata delle SA e l'univocità SPI) in IKEv2, meno pacchetti vengono persi e duplicati in IKEv2. Pertanto, la necessità di ridefinire le SA è minore.

Nota: poiché la protezione di rete può essere forte solo come il collegamento più debole, IKEv2 non interagisce con IKEv1.

Panoramica sulla migrazione

Se la configurazione di IKEv1 o anche SSL esiste già, l'ASA semplifica il processo di migrazione. Dalla riga di comando, immettere il comando **migrate**:

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

Note importanti:

- Definizioni parole chiave:**l2l** - Converte i tunnel IKEv1 l2l correnti in IKEv2.**accesso remoto** - Converte la configurazione di accesso remoto. È possibile convertire i gruppi di tunnel IKEv1 o SSL in IKEv2.**overwrite**: se si desidera sovrascrivere una configurazione IKEv2, questa parola chiave converte la configurazione IKEv1 corrente e rimuove la configurazione IKEv2 superflua.
- Èimportante notare che IKEv2 è in grado di utilizzare sia chiavi simmetriche che asimmetriche per l'autenticazione PSK. Quando si immette il comando **migration** sull'appliance ASA, l'appliance crea automaticamente una VPN IKEv2 con una chiave PSK simmetrica.
- Dopo aver immesso il comando, le configurazioni IKEv1 correnti non vengono eliminate. Al contrario, entrambe le configurazioni IKEv1 e IKEv2 vengono eseguite in parallelo e sulla stessa mappa crittografica. È possibile eseguire questa operazione anche manualmente. Quando IKEv1 e IKEv2 vengono eseguiti in parallelo, consente a un iniziatore VPN IPsec di eseguire il fallback da IKEv2 a IKEv1 quando esiste un problema di protocollo o configurazione con IKEv2 che può causare un errore nel tentativo di connessione. Quando IKEv1 e IKEv2 vengono eseguiti in parallelo, forniscono anche un meccanismo di rollback e semplificano la migrazione.
- Quando IKEv1 e IKEv2 vengono entrambi eseguiti in parallelo, ASA utilizza un modulo denominato tunnel manager/IKE, comune sull'iniziatore, per determinare la mappa crittografica e la versione del protocollo IKE da utilizzare per una connessione. L'ASA preferisce sempre avviare IKEv2, ma in caso contrario, torna a IKEv1.
- La ridondanza di più peer non è supportata con IKEv2 sull'appliance ASA. In IKEv1, a scopo di ridondanza, è possibile avere più di un peer nella stessa mappa crittografica quando si immette il comando **set peer**. Il primo peer sarà quello primario e, in caso di errore, il secondo peer verrà attivato. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCud2276 (solo utenti registrati), ENH: Supporto di più peer per IKEv2.

Processo di migrazione

Configurazione

Nell'esempio, una VPN IKEv1 con autenticazione PSK (Pre-Shared Key) esiste sull'appliance ASA.

Nota: la configurazione mostrata qui è rilevante solo per il tunnel VPN.

Configurazione ASA con una VPN IKEv1 corrente (prima della migrazione)

```
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
```

Configurazione ASA IKEv2 (dopo la migrazione)

Nota: modifiche in grassetto corsivo.

```
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 *****
```

Verifica istituzione tunnel IKEv2

```
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
```

Verifica PSK dopo la migrazione

Per verificare la chiave PSK, è possibile eseguire questo comando nella modalità di configurazione globale:

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

Processo IKEv2 e Tunnel Manager

Come accennato in precedenza, l'ASA utilizza un modulo chiamato tunnel manager/IKE, comune sull'iniziatore, per determinare la mappa crittografica e la versione del protocollo IKE da usare per una connessione. Immettere questo comando per monitorare il modulo:

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

I comandi **debug**, **logging** e **show** sono stati raccolti quando il traffico viene passato per avviare il tunnel IKEv2. Per chiarezza, parte dell'output è stato omesso.

```
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.
```

Meccanismo di fallback da IKEv2 a IKEv1

Se IKEv1 e IKEv2 sono entrambi in parallelo, l'ASA preferisce sempre avviare IKEv2. In caso contrario, l'ASA torna a IKEv1. Questo processo viene gestito dal modulo comune Tunnel Manager/IKE. In questo esempio sull'iniziatore, l'associazione di protezione IKEv2 è stata cancellata e IKEv2 è ora intenzionalmente non configurato (la proposta IKEv2 viene rimossa) per dimostrare il meccanismo di fallback.

```
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
```

Rafforzamento IKEv2

Per garantire una maggiore sicurezza quando si usa IKEv2, si consiglia di utilizzare i seguenti comandi opzionali:

- **Richiesta cookie Crypto IKEv2**: Consente all'ASA di inviare richieste relative ai cookie ai dispositivi peer in risposta a pacchetti inizializzati da un'associazione di protezione parzialmente aperti.
- **Limite max-sa crittografia IKEv2**: Limita il numero di connessioni IKEv2 sull'appliance ASA. Per impostazione predefinita, il numero massimo di connessioni IKEv2 consentite è uguale al numero massimo di connessioni specificato dalla licenza ASA.
- **Max-in-negotiation-sa limite IKEv2 crittografia**: Limita il numero di associazioni di sicurezza IKEv2 nella negoziazione (aperte) sull'appliance ASA. Se usato insieme al comando **crypto IKEv2 cookie-challenge**, verificare che la soglia di verifica dei cookie sia inferiore a questo limite.
- Utilizzare chiavi asimmetriche. Dopo la migrazione, è possibile modificare la configurazione in modo da utilizzare chiavi asimmetriche, come illustrato di seguito:

```
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
```

Èimportante tenere presente che è necessario eseguire il mirroring della configurazione sull'altro peer per la chiave già condivisa IKEv2. Se si seleziona e si incolla la configurazione da un lato all'altro, la procedura non funzionerà.

Nota: questi comandi sono disabilitati per impostazione predefinita.

Informazioni correlate

- Documentazione e supporto tecnico