# Schnelle Migration von IKEv1 zu IKEv2 L2L-Tunnelkonfiguration auf ASA 8.4-Code

## Inhalt



# Einführung

Dieses Dokument enthält Informationen über IKEv2 und den Migrationsprozess von IKEv1.

# Voraussetzungen

## Anforderungen

Stellen Sie sicher, dass Sie über eine Cisco ASA Security Appliance verfügen, die IPsec mit der Authentifizierungsmethode IKEv1 Pre-shared Key (PSK) ausführt, und stellen Sie sicher, dass sich der IPsec-Tunnel im Betriebszustand befindet.

Ein Beispiel für die Konfiguration einer Cisco ASA Security Appliance, die IPsec mit der IKEv1 PSK-Authentifizierungsmethode ausführt, finden Sie unter PIX/ASA 7.x und höher: Konfigurationsbeispiel eines PIX-zu-PIX-VPN-Tunnels.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf diesen Hardware- und Softwareversionen.

- Cisco Security Appliance der Serie ASA 5510, ausgeführt mit Version 8.4.x und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

## Gründe für die Migration zu IKEv2

- IKEv2 bietet eine bessere Ausfallsicherheit für Netzwerkangriffe. IKEv2 kann einen DoS-Angriff auf das Netzwerk bei der Validierung des IPsec-Initiators mindern. Um die Ausnutzung der DoS-Schwachstelle zu erschweren, kann der Befragte einen Cookie für den Initiator anfordern, der dem Befragten versichern muss, dass es sich um eine normale Verbindung handelt. In IKEv2 minimieren die Responder-Cookies den DoS-Angriff, sodass der Responder keinen Zustand des IKE-Initiators behält oder keinen D-H-Vorgang ausführt, es sei denn, der Initiator gibt das vom Responder gesendete Cookie zurück. Der Responder verwendet eine minimale CPU und gibt keinen Zustand an eine Security Association (SA) weiter, bis er den Initiator vollständig validieren kann.
- IKEv2 reduziert die Komplexität bei der IPsec-Einrichtung zwischen verschiedenen VPN-Produkten. Sie erhöht die Interoperabilität und ermöglicht auch eine Standardmethode für Legacy-Authentifizierungsmethoden. IKEv2 bietet eine nahtlose IPsec-Interoperabilität zwischen Anbietern, da es integrierte Technologien wie Dead Peer Detection (DPD), NAT Traversal (NAT-T) oder Initial Contact anbietet.
- IKEv2 hat weniger Overhead. Mit weniger Overhead bietet sie eine verbesserte Latenz bei der SA-Einrichtung. Bei der Übertragung sind mehrere Anforderungen zulässig (z. B. wenn mehrere untergeordnete SAs parallel eingerichtet werden).
- IKEv2 verfügt über eine reduzierte SA-Verzögerung. In IKEv1 verstärkt sich die Verzögerung der SA-Erstellung, wenn das Paketvolumen zunimmt. IKEv2 behält die gleiche durchschnittliche Verzögerung bei einer Steigerung des Paketvolumens bei. Wenn das Paketvolumen zunimmt, nimmt die Zeit zur Verschlüsselung und Verarbeitung des Paket-Headers zu. Wenn eine neue SA-Einrichtung erstellt werden soll, ist mehr Zeit erforderlich. Die von IKEv2 generierte SA ist kleiner als die von IKEv1 generierte SA. Bei einer verstärkten Paketgröße dauert die Erstellung einer SA fast konstant.
- IKEv2 bietet eine schnellere Wiederverwendungszeit. IKE v1 benötigt mehr Zeit, um SAs neu zu starten als IKEv2. IKEv2-Schlüssel für SA bietet eine verbesserte Sicherheitsleistung und reduziert die Anzahl der während der Übergangsphase verlorenen Pakete. Aufgrund der Neudefinition bestimmter Mechanismen von IKEv1 (z. B. ToS-Payload, Auswahl der SA-Lebensdauer und SPI-Einzigartigkeit) in IKEv2 gehen weniger Pakete verloren und dupliziert in IKEv2. Daher müssen die SAs weniger neu ausgewählt werden.

**Hinweis:** Da die Netzwerksicherheit nur so stark wie die schwächste Verbindung sein kann, ist IKEv2 nicht mit IKEv1 kompatibel.

## Übersicht zur Migration

Wenn Ihre IKEv1- oder sogar SSL-Konfiguration bereits vorhanden ist, vereinfacht die ASA den Migrationsprozess. Geben Sie in der Befehlszeile den Befehl **migrieren ein**:

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

Dinge:

- Schlüsselwortdefinitionen:**l2l** - Diese wandelt aktuelle IKEv1 l2l-Tunnel in IKEv2 um.**Remote-Zugriff** - Konvertiert die Konfiguration für den Remote-Zugriff. Sie können entweder die Gruppen IKEv1 oder SSL-Tunnel in IKEv2 umwandeln.**overwrite** - Wenn Sie über eine IKEv2-Konfiguration verfügen, die Sie überschreiben möchten, konvertiert dieses Schlüsselwort die aktuelle IKEv1-Konfiguration und entfernt die überflüssige IKEv2-Konfiguration.
- Es ist zu beachten, dass IKEv2 sowohl symmetrische als auch asymmetrische Schlüssel für die PSK-Authentifizierung verwenden kann. Wenn der **Migrationsbefehl** auf der ASA eingegeben wird, erstellt die ASA automatisch ein IKEv2-VPN mit einem symmetrischen PSK.
- Nach Eingabe des Befehls werden die aktuellen IKEv1-Konfigurationen nicht gelöscht. Stattdessen werden die Konfigurationen IKEv1 und IKEv2 parallel und auf derselben Crypto Map ausgeführt. Dies können Sie auch manuell durchführen. Wenn sowohl IKEv1 als auch IKEv2 parallel ausgeführt werden, kann ein IPsec-VPN-Initiator von IKEv2 auf IKEv1 zurückfallen, wenn ein Protokoll- oder Konfigurationsproblem mit IKEv2 vorliegt, das zu einem Verbindungsfehler führen kann. Wenn sowohl IKEv1 als auch IKEv2 parallel ausgeführt werden, wird ein Rollback-Mechanismus bereitgestellt und die Migration vereinfacht.
- Wenn IKEv1 und IKEv2 parallel ausgeführt werden, verwendet die ASA ein Modul namens "Tunnel Manager/IKE common" im Initiator, um die Kryptoübersicht und die Version des IKE-Protokolls für eine Verbindung zu bestimmen. Die ASA zieht es immer vor, IKEv2 zu initiieren. Ist dies jedoch nicht der Fall, fällt IKEv1 zurück.
- Für Redundanz verwendete Peers werden von IKEv2 auf der ASA nicht unterstützt. In IKEv1 kann aus Redundanzgründen bei der Eingabe des Befehls **set peer** unter derselben Crypto Map mehr als ein Peer vorhanden sein. Der erste Peer ist der primäre Peer, und bei einem Ausfall tritt der zweite Peer ein. Weitere Informationen finden Sie unter Cisco Bug ID CSCud2276 (nur registrierte Kunden), ENH: Unterstützung mehrerer Peers für IKEv2.

# Migrationsprozess

## Konfiguration

In diesem Beispiel existiert IKEv1-VPN, das Pre-Shared Key (PSK)-Authentifizierung verwendet, auf der ASA.

**Hinweis:** Die hier gezeigte Konfiguration ist nur für den VPN-Tunnel relevant.

### ASA-Konfiguration mit aktuellem IKEv1-VPN (vor der Migration)

```
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-Konfiguration (nach der Migration)

**Hinweis:** Änderungen sind kursiv markiert.

```
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-Tunnelaufbau - Verifizierung

```
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-Verifizierung nach der Migration

Zur Verifizierung Ihres PSK können Sie diesen Befehl im globalen Konfigurationsmodus ausführen:

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

# IKEv2 und Tunnel Manager-Prozess

Wie bereits erwähnt, verwendet die ASA ein Modul mit dem Namen Tunnel-Manager/IKE, das im Initiator üblich ist, um die Kryptoübersicht und die für eine Verbindung zu verwendende Version des IKE-Protokolls zu bestimmen. Geben Sie den folgenden Befehl ein, um das Modul zu überwachen:

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

Die Befehle **debug**, **logging** und **show** wurden erfasst, wenn der Datenverkehr zum Initiieren des IKEv2-Tunnels übergeben wurde. Aus Gründen der Übersichtlichkeit wurde ein Teil der Ausgabe weggelassen.

```
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.
```

## Fallback-Mechanismus IKEv2 zu IKEv1

Bei paralleler Verwendung von IKEv1 und IKEv2 zieht die ASA stets die Initiierung von IKEv2 vor. Wenn die ASA dies nicht kann, wird sie auf IKEv1 zurückgesetzt. Dieser Prozess wird vom Tunnelmanager/IKE Common Module verwaltet. In diesem Beispiel wurde die IKEv2 SA im Initiator gelöscht, und IKEv2 ist nun absichtlich falsch konfiguriert (der IKEv2-Vorschlag wird entfernt), um den Rückfallmechanismus zu veranschaulichen.

```
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 Harden

Um bei Verwendung von IKEv2 zusätzliche Sicherheit zu bieten, werden folgende optionale Befehle dringend empfohlen:

- **Crypto IKEv2 Cookie-Challenge**: Ermöglicht der ASA das Senden von Cookie-Herausforderungen an Peer-Geräte als Reaktion auf Pakete, die von der SA initiiert wurden und halb geöffnet sind.
- **Max-sa-Limit für Krypto IKEv2**: Schränkt die Anzahl der IKEv2-Verbindungen auf der ASA ein. Standardmäßig entspricht die maximal zulässige IKEv2-Verbindung der in der ASA-Lizenz angegebenen Anzahl von Verbindungen.
- **Verschlüsselung IKEv2 begrenzt die maximale In-Negotiation-sa**: Begrenzt die Anzahl der IKEv2 in-Negotiation (offene) SAs auf der ASA. Bei Verwendung des Befehls **crypto IKEv2 cookie-Challenge** muss sichergestellt werden, dass der Grenzwert für Cookie-Challenge unter diesem Grenzwert liegt.
- Verwenden Sie asymmetrische Schlüssel. Nach der Migration kann die Konfiguration so geändert werden, dass sie asymmetrische Schlüssel wie folgt verwendet:

```
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
```

Es ist wichtig zu erkennen, dass die Konfiguration für den IKEv2-Pre-Shared-Key auf dem anderen Peer gespiegelt werden muss. Dies funktioniert nicht, wenn Sie die Konfiguration von einer Seite zur anderen auswählen und einfügen.

**Hinweis:** Diese Befehle sind standardmäßig deaktiviert.

## Zugehörige Informationen

- Technischer Support und Dokumentation