在ASA 8.4代碼上快速將IKEv1遷移到IKEv2 L2L隧道配置

目錄

簡介

本文檔提供有關IKEv2和從IKEv1遷移過程的資訊。

必要條件

需求

確保您擁有運行採用IKEv1預共用金鑰(PSK)身份驗證方法的IPsec的Cisco ASA安全裝置，並確保IPsec隧道處於運行狀態。

有關使用IKEv1 PSK身份驗證方法運行IPsec的Cisco ASA安全裝置的示例配置，請參閱PIX/ASA 7.x及更高版本：PIX到PIX VPN隧道配置示例。

採用元件

本檔案中的資訊是根據這些硬體和軟體版本。

- 運行版本8.4.x及更高版本的Cisco ASA 5510系列安全裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

為什麼要遷移到IKEv2?

- IKEv2提供更好的網路攻擊恢復能力。IKEv2在驗證IPsec啟動器時，可以緩解網路上的DoS攻擊。為了使DoS漏洞難以利用，響應方可以向發起方請求一個cookie，發起方必須保證這是正常連線。在IKEv2中，響應方cookie緩解DoS攻擊，使得響應方不保持IKE發起方的狀態或不執行D-H操作，除非發起方返迴響應方傳送的cookie。響應方使用最少的CPU，並且不會向安全關聯(SA)提交任何狀態，直到它完全驗證發起方。
- IKEv2降低了不同VPN產品之間的IPsec建立的複雜性。它提高了互操作性，還允許採用傳統身份驗證方法的標準方法。IKEv2在供應商之間提供了無縫IPsec互操作性，因為它提供了內建技術，如失效對等體檢測(DPD)、NAT穿越(NAT-T)或初始聯絡。
- IKEv2的開銷較低。它以較少的開銷提供了改進的SA設定延遲。在傳送過程中允許多個請求（例如，並行設定多個子SA時）。
- IKEv2具有縮短的SA延遲。在IKEv1中，SA建立的延遲會隨著資料包卷的增加而增大。資料包卷放大時，IKEv2保持相同的平均延遲。當封包卷放大時，加密和處理封包標頭的時間也會增大。建立新的SA建立時，需要更多時間。IKEv2生成的SA小於IKEv1生成的SA。對於放大的資料包大小，建立SA所需的時間幾乎保持不變。
- IKEv2具有更快的重新生成金鑰時間。與IKEv2相比，IKE v1對SA重新生成金鑰需要更多時間。IKEv2對SA重新生成金鑰提高了安全效能，並減少了轉換過程中丟失的資料包數量。由於IKEv2中對IKEv1的某些機制（如ToS負載、選擇SA生存期和SPI唯一性）進行了重新定義，因此在IKEv2中丟失和複製的資料包更少。因此，不需要對SA重新設定金鑰。

注意：由於網路安全只能與最弱鏈路一樣強，因此IKEv2不能與IKEv1互操作。

遷移概述

如果IKEv1（甚至SSL）配置已存在，ASA將簡化遷移過程。在命令列中，輸入**migrate**命令：

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

需要注意的事項：

- 關鍵字定義：**l2l** — 將當前IKEv1 l2l隧道轉換為IKEv2。**remote access** — 轉換遠端訪問配置。可以將IKEv1或SSL隧道組轉換為IKEv2。**overwrite** — 如果您具有要覆蓋的IKEv2配置，則此關鍵字將轉換當前IKEv1配置並刪除多餘的IKEv2配置。
- 必須注意的是，IKEv2能夠使用對稱和非對稱金鑰進行PSK身份驗證。在ASA上輸入**migration**命令後，ASA會自動建立具有對稱PSK的IKEv2 VPN。
- 輸入命令後，不會刪除當前的IKEv1配置。相反，IKEv1和IKEv2配置都並行運行並在同一加密對映上運行。您也可以手動執行此操作。當IKEv1和IKEv2同時運行時，這允許IPsec VPN發起程式從IKEv2回退到IKEv1，當IKEv2存在可能導致連線嘗試失敗的協定或配置問題時。當IKEv1和IKEv2並行運行時，它還提供回滾機制並簡化遷移。
- 當IKEv1和IKEv2並行運行時，ASA使用啟動器上常見的稱為隧道管理器/IKE的模組來確定用於連線的加密對映和IKE協定版本。ASA始終傾向於啟動IKEv2，但如果無法啟動，則會回退到

IKEv1。

- ASA上的IKEv2不支援用於冗餘的多個對等體。在IKEv1中，出於冗餘目的，當您輸入**set peer**命令時，同一個加密對映下可以有多個對等體。第一個對等體將成為主節點，如果它失敗，第二個對等體將啟動。請參閱Cisco錯誤ID CSCud2276(僅限註冊客戶)，增強型：支援IKEv2的多個對等體。

遷移過程

組態

在本示例中，ASA上存在使用預共用金鑰(PSK)身份驗證的IKEv1 VPN。

注意：此處顯示的配置僅與VPN隧道相關。

使用當前IKEv1 VPN的ASA配置（遷移之前）

```
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配置（遷移後）

註：以粗體斜體標籤的更改。

```
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通道建立驗證

```
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
```

遷移後的PSK驗證

若要驗證您的PSK，可以在全域性配置模式下運行此命令：

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

IKEv2和通道管理員程式

如前所述，ASA在啟動器上使用稱為隧道管理器/IKE的模組來確定用於連線的加密對映和IKE協定版本。輸入以下命令監控模組：

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

在傳遞流量以啟動IKEv2隧道時，會收集debug、logging和show命令。為清楚起見，部分輸出被省略。

```
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到IKEv1回退機制

在IKEv1和IKEv2並行的情況下，ASA始終傾向於啟動IKEv2。如果ASA無法啟動，它將回退到IKEv1。隧道管理器/IKE公共模組管理此進程。在此啟動器上的示例中，IKEv2 SA被清除，IKEv2現在故意錯誤配置（刪除IKEv2提議）以演示回退機制。

```
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
```

強化IKEv2

為了在使用IKEv2時提供額外的安全性，強烈建議使用以下可選命令：

- **Crypto IKEv2 cookie-challenge**:使ASA能夠向對等裝置傳送cookie質詢，以響應半開放SA啟動的資料包。
- **Crypto IKEv2 limit max-sa**:限制ASA上IKEv2連線的數量。預設情況下，允許的最大IKEv2連線數等於ASA許可證指定的最大連線數。
- **Crypto IKEv2 limit max-in-negotiation-sa**:限制ASA上的IKEv2協商中（開放）SA的數量。與**crypto IKEv2 cookie-challenge**命令結合使用時，請確保cookie-challenge閾值低於此限制。
- 使用非對稱金鑰。遷移後，可以修改配置以使用非對稱金鑰，如下所示：
  ```
  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
```

必須認識到，配置需要在IKEv2預共用金鑰的另一個對等體上映象。如果您從一側選擇並貼上配置到另一側，則此操作不會起作用。

注意：預設情況下禁用這些命令。

相關資訊

- **技術支援與檔案**