在ASA 8.4代码上快速迁移IKEv1到IKEv2 L2L隧道配置

目录

简介

本文档提供有关IKEv2和从IKEv1迁移过程的信息。

先决条件

要求

确保您有使用IKEv1预共享密钥(PSK)身份验证方法运行IPsec的Cisco ASA安全设备，并确保IPsec隧道处于运行状态。

有关使用IKEv1 PSK身份验证方法运行IPsec的Cisco ASA安全设备的示例配置，请参阅PIX/ASA 7.x及更高版本：PIX 到 PIX VPN 隧道配置示例。

使用的组件

本文档中的信息基于这些硬件与软件版本。

- Cisco ASA 5510系列安全设备，运行版本为8.4.x及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

为什么迁移到IKEv2?

- IKEv2提供更好的网络攻击恢复能力。当IKEv2验证IPsec发起方时，它可以缓解网络上的DoS攻击。为了使DoS漏洞难以利用，响应方可以向必须向响应方保证这是正常连接的发起方请求cookie。在IKEv2中，响应方cookie会缓解DoS攻击，以便响应方不保留IKE发起方的状态或不执行D-H操作，除非发起方返回响应方发送的cookie。响应方使用最小的CPU，并且在完全验证发起方之前不向安全关联(SA)提交任何状态。
- IKEv2可降低不同VPN产品之间建立IPsec的复杂性。它提高了互操作性，还为传统身份验证方法提供了标准方法。IKEv2提供供应商之间的无缝IPsec互操作性，因为它提供内置技术，如失效对等体检测(DPD)、NAT穿越(NAT-T)或初始联系。
- IKEv2的开销较少。通过降低开销，可改善SA设置延迟。在传输中允许多个请求（例如，并行设置多个子SA时）。
- IKEv2的SA延迟降低。在IKEv1中，SA创建的延迟随着数据包卷的扩大而增大。当数据包卷扩大时，IKEv2保持相同的平均延迟。当数据包量增大时，加密和处理数据包报头的时间会增加。要创建新的SA建立时，需要更多时间。IKEv2生成的SA小于IKEv1生成的SA。对于放大的数据包大小，创建SA所花的时间几乎是恒定的。
- IKEv2的重新生成密钥时间更短。IKE v1比IKEv2花费更多时间对SA重新生成密钥。IKEv2对SA重新生成密钥可提高安全性能，并减少在转换中丢失的数据包数。由于在IKEv2中重定义了IKEv1的某些机制（如ToS负载、选择SA生存期和SPI唯一性），因此在IKEv2中丢失和复制的数据包较少。因此，对SA重新生成密钥的需要较少。

注意：由于网络安全性只能与最薄弱的链路一样强，因此IKEv2无法与IKEv1互操作。

迁移概述

如果IKEv1，甚至SSL，配置已存在，则ASA使迁移过程变得简单。在命令行中，输入**migrate**命令：

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

注意事项：

- 关键字定义：**l2l** — 将当前IKEv1 l2l隧道转换为IKEv2。**远程访问** — 这将转换远程访问配置。可以将IKEv1或SSL隧道组转换为IKEv2。**overwrite** — 如果您有要覆盖的IKEv2配置，则此关键字会转换当前IKEv1配置并删除多余的IKEv2配置。
- 请注意，IKEv2能够同时使用对称密钥和非对称密钥进行PSK身份验证。在ASA上输入**migration**命令时，ASA会自动创建带对称PSK的IKEv2 VPN。
- 输入命令后，不会删除当前IKEv1配置。相反，IKEv1和IKEv2配置在同一加密映射中并行运行。您也可以手动执行此操作。当IKEv1和IKEv2同时运行时，这允许IPsec VPN启动器在IKEv2存在可能导致连接尝试失败的协议或配置问题时从IKEv2回退到IKEv1。当IKEv1和IKEv2同时运行时，它还提供回滚机制并使迁移更容易。
- 当IKEv1和IKEv2同时运行时，ASA使用启动器上通用的称为隧道管理器/IKE的模块来确定用于

连接的加密映射和IKE协议版本。ASA始终首选启动IKEv2，但如果它不能，则回退到IKEv1。

- ASA上的IKEv2不支持用于冗余的多个对等体。在IKEv1中，为了实现冗余，当您输入set peer命令时，同一加密映射下可以有多个对**等体**。第一个对等体将成为主要对等体，如果它发生故障，第二个对等体将开始工作。请参阅Cisco Bug ID CSCud22276(仅注册客户)，增强版：IKEv2支持多个对等体。

迁移进程

配置

在本示例中，ASA上存在使用预共享密钥(PSK)身份验证的IKEv1 VPN。

注意：此处显示的配置仅与VPN隧道相关。

使用当前IKEv1 VPN的ASA配置（迁移前）

```
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（迁移后）

注意：以粗体斜体标记的更改。

```
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隧道建立验证

```
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
```

迁移后的PSK验证

为了验证PSK，您可以在全局配置模式下运行以下命令：

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

IKEv2和隧道管理器进程

如前所述，ASA使用发起方上通用的称为隧道管理器/IKE的模块来确定用于连接的加密映射和IKE协议版本。输入以下命令以监控模块：

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

当通过流量来启动IKEv2隧道时，会收集debug、logging和show命令。为清楚起见，部分输出已省略。

```
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回退机制

在IKEv1和IKEv2并行的情况下，ASA始终倾向于启动IKEv2。如果ASA无法启动，则会回退到IKEv1。隧道管理器/IKE通用模块管理此过程。在本示例中，在启动器上，IKEv2 SA被清除，IKEv2现在被故意错误配置（IKEv2提议被删除）以演示回退机制。

```
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
```

强化IKEv2

为了在使用IKEv2时提供额外的安全性，强烈建议使用以下可选命令：

- **加密IKEv2 cookie-challenge**:使ASA能够向对等设备发送cookie质询以响应半开SA启动的数据包。
- **加密IKEv2限制max-sa**:限制ASA上IKEv2连接的数量。默认情况下，允许的最大IKEv2连接数等于ASA许可证指定的最大连接数。
- **加密IKEv2限制max-in-negotiation-sa**:限制ASA上IKEv2协商中（打开）SA的数量。当与crypto IKEv2 cookie-challenge命**令一起使用时**，请确保cookie质询阈值低于此限制。
- 使用非对称密钥。迁移后，可以修改配置以使用非对称密钥，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
```

必须认识到，IKEv2预共享密钥的配置需要镜像到另一个对等体上。如果从一端选择配置并将其粘贴到另一端，则该配置将不起作用。

注意：这些命令默认为禁用。

相关信息

- 技术支持和文档