在 ASA 和 Cisco IOS 路由器之间配置站点间 IPSec IKEv1 隧道

目录

简介

本文档介绍如何通过CLI在Cisco自适应安全设备(ASA)和运行Cisco IOS®软件的路由器之间配置站点到站点（LAN到LAN）IPSec互联网密钥交换版本1(IKEv1)隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS
- Cisco ASA
- 一般IPSec概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本9.4(1)的Cisco 5512-X系列ASA
- 运行Cisco IOS软件版本15.4(3)M2的Cisco 1941系列集成多业务路由器(ISR)

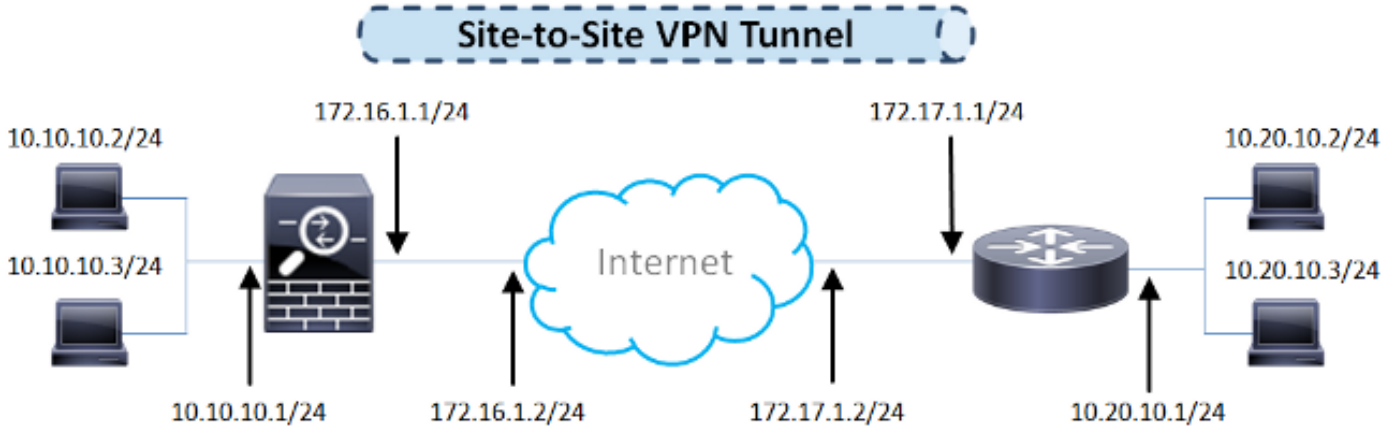
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本节介绍如何完成ASA和IOS路由器CLI配置。

网络图

本文档中的信息使用此网络设置：



ASA 配置

配置ASA接口

如果未配置ASA接口，请确保至少配置IP地址、接口名称和安全级别：

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

> **注意**：确保与内部网络和外部网络，特别是与远程对等体的连接，以便建立站点到站点VPN隧道。您可以使用ping命令检验基本连通性。

在外部接口上配置IKEv1策略并启用IKEv1

要为IKEv1连接配置互联网安全关联和密钥管理协议(ISAKMP)策略，请输入**crypto ikev1 policy <priority>命**令：

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **注意**：当来自两个对等体的两个策略包含相同的身份验证、加密、哈希和Diffie-Hellman参数值时，存在IKEv1策略匹配。对于IKEv1，远程对等策略还必须指定小于或等于发起方发送的策略中生存期的生存期。如果寿命不同，则ASA使用较短的寿命。

> **注**：如果未为给定策略参数指定值，则应用默认值。

必须在终止VPN隧道的接口上启用IKEv1。通常，这是外部(或公共)接口。要启用IKEv1，请在全局配置模式下输入**crypto ikev1 enable**<interface-name>命令：

```
crypto ikev1 enable outside
```

配置隧道组（LAN到LAN连接配置文件）

对于LAN到LAN隧道，连接配置文件类型为**ipsec-l2l**。要配置IKEv1预共享密钥，请进入*tunnel-group ipsec-attributes配置*模式：

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

为感兴趣的VPN流量配置ACL

ASA使用访问控制列表(ACL)将应使用IPSec加密保护的流量与不需要保护的流量区分开来。它保护与允许应用控制引擎(ACE)匹配的出站数据包，并确保与允许ACE匹配的入站数据包具有保护。

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

注意：VPN流量的ACL在网络地址转换(NAT)后使用源IP地址和目的IP地址。

注意：VPN流量的ACL必须在两个VPN对等体上镜像。

注意：如果需要向受保护的流量添加新子网，只需将子网/主机添加到相应的对象组，并在远程VPN对等体上完成镜像更改。

配置NAT免除

注意：本节中介绍的配置是可选的。

通常，不应对VPN流量执行NAT。要免除该流量，必须创建身份NAT规则。身份NAT规则只是将地址转换为同一地址。

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

配置IKEv1转换集

IKEv1转换集是定义ASA保护数据方式的安全协议和算法的组合。在IPSec安全关联(SA)协商期间，对等体必须标识两个对等体相同的转换集或提议。然后，ASA应用匹配的转换集或提议，以创建SA，保护该加密映射访问列表中的数据流。

要配置IKEv1转换集，请输入**crypto ipsec ikev1 transform-set**命令：

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

配置加密映射并将其应用于接口

加密映射定义要在IPSec SA中协商的IPSec策略，包括：

- 一个访问列表，用于标识IPSec连接允许和保护的数据包
- 对等体标识
- IPSec流量的本地地址
- IKEv1转换集

示例如下：

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
```

然后，可以将加密映射应用到接口：

```
crypto map outside_map interface outside
```

ASA最终配置

以下是ASA的最终配置：

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
```

```
static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
crypto map outside_map interface outside
```

IOS路由器CLI配置

配置接口

如果尚未配置IOS路由器接口，则至少应配置LAN和WAN接口。示例如下：

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
no shutdown
```

确保与内部网络和外部网络，特别是与远程对等体的连接，以便建立站点到站点VPN隧道。您可以使用ping命令检验基本连通性。

配置ISAKMP(IKEv1)策略

要为IKEv1连接配置ISAKMP策略，请在全局配置模式下输入**crypto isakmp policy <priority>**命令。以下是一个示例：

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

> **注意：**您可以在参与IPSec的每个对等体上配置多个IKE策略。当IKE协商开始时，它会尝试查找在两个对等体上配置的通用策略，并从在远程对等体上指定的最高优先级策略开始。

配置加密ISAKMP密钥

要配置预共享*的身*份验证密钥，请在全**局配置**模式下输入crypto isakmp key命令：

```
crypto isakmp key cisco123 address 172.16.1.1
```

为感兴趣的VPN流量配置ACL

使用扩展或命名访问列表指定应受加密保护的流量。示例如下：

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

注意：VPN流量的ACL在NAT后使用源IP地址和目的IP地址。

注意：VPN流量的ACL必须在两个VPN对等体上镜像。

配置NAT免除

注意：本节中介绍的配置是可选的。

通常，不应对VPN流量执行NAT。如果使用NAT过载，则应使用路由映射，以免转换所关注的VPN流量。请注意，在路由映射中使用的访问列表中，应拒绝所关注的VPN流量。

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

配置转换集

要定义IPSec转换集（安全协议和算法的可接受组合），请在全局配置模式下输入**crypto ipsec transform-set**命令。示例如下：

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

配置加密映射并将其应用于接口

要创建或修改加密映射条目并进入加密映射配置模式，请输入**crypto map** 全局配置命令。要完成加密映射条目，必须至少定义以下方面：

- 必须定义可将受保护流量转发到的IPsec对等体。这些是可以与其建立SA的对等体。要在加密映射条目中指定IPSec对等体，请输入**set peer**命令。
- 必须定义可用于受保护流量的转换集。要指定可与加密映射条目一起使用的转换集，请输入**set transform-set命**令。
- 必须定义应受保护的流量。要为加密映射条目指定扩展访问列表，请输入**match address**命令。

示例如下：

```
crypto map outside_map 10 ipsec-isakmp
```

```
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

最后一步是将之前定义的加密映射集应用到接口。要应用此命令，请输入crypto map 接口配置命令：

```
interface GigabitEthernet0/0
crypto map outside_map
```

IOS最终配置

以下是最终的IOS路由器CLI配置：

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

验证

在验证隧道是否已启用并且已通过流量之前，必须确保所关注的流量发送到ASA或IOS路由器。

注意：在ASA上，可以使用与所关注流量匹配的packet-tracer工具来启动IPSec隧道(例如，详细的tcp 10.10.10.10 12345 10.20.10.10 80中的packet-tracer输入)。

第1阶段验证

要验证ASA上的IKEv1第1阶段是否处于启用状态，请输入**show crypto isakmp sa命**令。预期输出将显示**MM_ACTIVE状**态：

```
ciscoasa# show crypto isakmp 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: 172.17.1.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

要验证IOS上的IKEv1第1阶段是否处于启用状态，请输入**show crypto isakmp sa** 命令。预期输出将显示“活动”状态：

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

第2阶段验证

要验证ASA上的IKEv1第2阶段是否处于启用状态，请输入**show crypto ipsec sa命**令。预期输出将同时显示入站和出站安全参数索引(SPI)。 如果流量通过隧道，您应看到encaps/decaps计数器增加。

注意：对于每个ACL条目，都会创建单独的入站/出站SA，这可能导致长的**show crypto ipsec sa**命令输出（取决于加密ACL中ACE条目的数量）。

示例如下：

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
   Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

      access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
```

```
     current_peer: 172.17.1.1


      #pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
      #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 8A9FE619
     current inbound spi : D8639BD0

    inbound esp sas:
      spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

要验证IOS上的IKEv1第2阶段是否处于启用状态，请输入**show crypto ipsec sa**命令。预期输出将同时显示入站和出站SPI。如果流量通过隧道，您应看到encaps/decaps计数器增加。

示例如下：

```
Router#show crypto ipsec sa peer 172.16.1.1

interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
    #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
```

```
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

     outbound esp sas:
      spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

阶段1和2验证

本节介绍可在ASA或IOS上使用的命令，以验证第1阶段和第2阶段的详细信息。

在ASA上输入show vpn-sessiondb命令进行验证：

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                     IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
```

```
 Tunnel ID    : 2.1
 UDP Src Port : 500                    UDP Dst Port : 500
 IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
 Encryption   : AES128                 Hashing      : SHA1
 Rekey Int (T): 86400 Seconds          Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 Filter Name  :

IPsec:
 Tunnel ID    : 2.2
 Local Addr   : 10.10.10.0/255.255.255.0/0/0
 Remote Addr  : 10.20.10.0/255.255.255.0/0/0
 Encryption   : AES128                 Hashing      : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds           Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes             Idle TO Left : 26 Minutes
 Bytes Tx     : 100500                 Bytes Rx     : 101400
 Pkts Tx      : 1005                   Pkts Rx      : 1014

NAC:
 Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
 SQ Int (T)   : 0 Seconds              EoU Age(T)   : 309 Seconds
 Hold Left (T): 0 Seconds              Posture Token:
 Redirect URL :

ciscoasa#
```

在IOS上输入show crypto session命令进行验证：

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 172.16.1.1
     Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

故障排除

本节提供可用于排除配置故障的信息。

> **注：**在使用debug命令之前，请参阅有关Debug命令和IP安全故障排除 — 了解和使用debug命令的重要信息Cisco文档。

IPSec LAN到LAN检查器工具

为了自动验证ASA和IOS之间的IPSec LAN到LAN配置是否有效，可使用IPSec LAN-to-LAN Checker工具。该工具的设计目的是从ASA或IOS路由器接受show tech或show running-config命令。它检查配置并尝试检测是否配置了基于加密映射的LAN到LAN IPSec隧道。如果已配置，它将对配置执行多点检查，并突出显示要协商的隧道的所有配置错误和设置。

ASA调试

要排除ASA防火墙上的IPSec IKEv1隧道协商故障，可以使用以下debug命令：

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

> **注意：如果ASA上的VPN隧道数量很大，则在启用调试之前应使用debug crypto condition peer A.B.C.D** 命令，以便将调试输出限制为仅包括指定的对等体。

IOS路由器调试

要排除IOS路由器上的IPSec IKEv1隧道协商故障，可以使用以下debug命令：

```
debug crypto ipsec
debug crypto isakmp
```

> **注意：如果IOS上的VPN隧道数量很大，则在启用调试之前应使用debug crypto condition peer ipv4 A.B.C.D**，以便将调试输出限制为仅包括指定的对等体。

> **提示：**有关如何对站点到站点VPN进行故障排除的详细信息，请参阅最常见的L2L和远程访问IPSec VPN故障排除解决方案Cisco文档。

参考

- 关于 Debug 命令的重要信息
- IP安全故障排除-了解和使用debug命令
- 最常见的L2L和远程访问IPSec VPN故障排除解决方案
- IPSec LAN到LAN检查器
- 技术支持和文档 - Cisco Systems