配置在ASA和Cisco IOS路由器之间的站点至站点IPSec IKEv1通道

目录

简介
先决条件
要求
使用的组件
配置
网络图
ASA 配置
配置ASA接口
配置IKEv1策略并且启用在外部接口的IKEv1
配置隧道组(LAN-to-LAN连接配置文件)
配置VPN流量的ACL利益
配置NAT免税
配置IKEv1转换集
配置加密映射并且应用它对接口
ASA最终配置
IOS路由器CLI配置
配置接口
配置ISAKMP (IKEv1)策略
配置crypto Isakmp key
配置VPN流量的ACL利益
配置NAT免税
配置转换集
配置加密映射并且应用它对接口
IOS最终配置
验证
阶段1验证
第2阶段验证
阶段1和2验证
故障排除
IPSec LAN对LAN检查器工具
ASA调试
IOS路由器调试
参考

简介

本文描述如何通过在思科可适应安全工具(ASA)和运行Cisco IOS软件的路由器之间的CLI配置一个站点到站点(LAN对LAN) IPSec互联网密钥交换版本1 (IKEv1)通道。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS
- Cisco ASA
- 将军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
- Cisco 1941系列集成业务路由器(ISR)该运行Cisco IOS软件版本15.4(3)M2

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

此部分描述如何完成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ASA接口没有配置，请保证您配置至少IP地址，建立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
```

Note:保证有连接对内部和外部网络，和特别是给将使用为了设立站点到站点VPN通道的远端对等体。您能使用ping为了验证基本连通性。

配置IKEv1策略并且启用在外部接口的IKEv1

为了配置IKEv1连接的互联网安全协会和密钥管理协议(ISAKMP)策略，请输入**crypto ikev1策略<priority>**命令：

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

注意： 当两个从两对等体的策略包含同样验证、加密、哈希和Diffie-Hellman参数值，IKEv1策略匹配存在。对于IKEv1，远端对等体策略必须也指定寿命小于或等于在发起者发送的策略的寿命。如果寿命不是相同的，则ASA使用更短的寿命。

注意： 如果不指定一个给的策略参数的一个值，默认值应用。

您必须启用在终止VPN通道的接口的IKEv1。一般，这是外部(或公共)接口。为了启用IKEv1，请输入**crypto ikev1 enable (event) <interface-name>** in命令全局配置模式：

```
crypto ikev1 enable outside
```

配置隧道组(LAN-to-LAN连接配置文件)

对于LAN-to-LAN隧道，连接配置文件类型是**ipsec-l2l**。为了配置IKEv1预共享密匙，请输入*隧道群ipsec属性*配置模式：

```
crypto ikev1 enable outside
```

配置VPN流量的ACL利益

ASA使用访问控制列表(ACL)为了区分应该保护与从流量的IPSec加密不要求保护的流量。它保护匹配permit应用程序控制引擎的出局信息包(ACE)并且保证匹配permit ACE请有保护的入站数据包。

```
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)以后使用源和目的IP地址。

注意：在两个VPN对等体必须反映VPN流量的ACL。

注意： 如果有需要添加每新的子网对已保护流量，请添加一子网/host到各自对象组并且完成在远程VPN对等设备的一镜像更改。

配置NAT免税

Note:在此部分描述的配置可选。

一般，不应该有在VPN流量执行的NAT。为了豁免该流量，您必须创建标识NAT规则。标识NAT规则转换对同一个地址的一个地址。

```
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

定义了方法ASA保护数据的IKEv1转换集是安全协议的组合和算法。在IPSec安全关联(SA)协商中，对等体必须识别是相同的为两个对等体的转换设置的或建议。ASA然后应用保护在访问列表的数据流该加密映射的匹配的转换设置的或建议为了创建SA。

为了配置IKEv1转换集，请输入**crypto ipsec ikev1转换集**命令：

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

配置加密映射并且应用它对接口

加密映射定义了在IPSec将协商的IPSec策略SA并且包括：

- 访问列表为了识别IPSec连接允许并且保护的数据包
- 对等体识别
- IPSec数据流的一个本地地址
- IKEv1转换集

示例如下：

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```
您能然后应用加密映射到接口：

```
crypto map outside_map interface outside
```

ASA最终配置

这是在ASA的最终配置：

```
crypto map outside_map interface outside
```

IOS路由器CLI配置

配置接口

如果IOS路由器接口没有配置，则应该配置至少LAN和广域网接口。示例如下：

```
crypto map outside_map interface outside
```
保证有连接对内部和外部网络，和特别是给将使用为了设立站点到站点VPN通道的远端对等体。您能使用ping为了验证基本连通性。

配置ISAKMP (IKEv1)策略

为了配置IKEv1连接的ISAKMP策略，请输入**crypto isakmp policy <priority>** in命令全局配置模式。 示例如下：

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

> **注意：** 您能配置在参加IPSec的每对等体的多IKE策略。当IKE协商开始时，尝试查找在两个配置对等体的一项普通政策，并且从在远端对等体指定的最高优先级的策略开始。

配置crypto Isakmp key

为了配置一*预共享*认证密钥，请输入**crypto isakmp key命令**在全局配置模式：

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

配置VPN流量的ACL利益

请使用延长或指定访问表为了指定应该由加密保护的流量。示例如下：

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

注意： VPN流量的ACL在NAT以后使用源和目的IP地址。

注意：在两个VPN对等体必须反映VPN流量的ACL。

配置NAT免税

Note:在此部分描述的配置可选。

一般，不应该有在VPN流量执行的NAT。如果使用NAT超载，则应该用于route-map为了豁免VPN流量从转换的利益。注意那在access-list用于route-map， VPN流量利益应该拒绝。

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

配置转换集

为了定义IPSec转换集(安全协议和算法的一个可接受组合)，请输入**crypto ipsec transform-set命令**在全局配置模式。示例如下：

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

配置加密映射并且应用它对接口

为了创建或修改加密映射项和输入加密映射配置模式，请输入**加密映射**全局配置命令。为了的加密映射项完成，那里是必须定义在最低的一些方面：

- 已保护流量可以转发的IPSec对等体必须定义。这些是SA可以设立的对等体。为了指定加密映射项的IPSec对等体，请输入**set peer命令**。
- 是可接受为了用在已保护流量上的转换集必须定义。为了指定能使用与加密映射项的转换集，请输入**set transform-set命令**。
- 应该保护的流量必须定义。为了指定加密映射项的一扩展访问列表，请输入**address命令的匹配**。

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
```

最后一步将应用以前定义加密映射集对接口。为了应用此，请输入**加密映射**接口配置命令：

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

IOS最终配置

这是最终IOS路由器CLI配置：

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

验证

在您验证通道是否启用和那前它通过流量，您必须保证流量利益发送往ASA或IOS路由器。

> **注意：** 在ASA，配比的数据包追踪器工具流量利益可以用于为了发起IPSec隧道(例如**数据包追踪器输入在tcp 10.10.10.10 12345 80里面**例如**被选派的**10.20.10.10)。

阶段1验证

为了验证IKEv1阶段1是否是UP在ASA，请输入**show crypto isakmp sa命令**。预期的输出是看到**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#
```

为了验证IKEv1阶段1是否是UP在IOS，请输入**show crypto isakmp sa命令**。预期的输出是看到**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

为了验证IKEv1第2阶段是否是UP在ASA，请输入**show crypto ipsec sa命令**。预期的输出是看到入站和出站安全参数索引(SPI)。如果流量穿过通道，您应该看到encaps/decap计数器增加。

> **注意**：对于每ACL条目有创建的分开的呼入/呼出的SA，也许导致一长**show crypto ipsec sa命令**输出(从属在ACE条目数量于加密ACL)。

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#
```

为了验证IKEv1第2阶段是否是UP在IOS，请输入**show crypto ipsec sa命令**。预期的输出是看到入

站和出站SPI。如果流量穿过通道，您应该看到encaps/decap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

此部分描述您在ASA或IOS能使用为了验证详细信息两个相位1和2.的命令。

输入显示vpn-sessiondb on命令验证的ASA ：

```
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#
```

输入显示crypto session命令在验证的IOS ：

```
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

此部分提供您能使用为了排除故障您的配置的信息。

> **注意：** 在您使用调试指令前，参考关于调试指令和IP安全故障排除-了解和使用debug命令Cisco文档的重要信息。

IPSec LAN对LAN检查器工具

为了自动地验证在ASA和IOS之间的IPSec LAN到LAN配置是否有效，您能使用IPSec LAN对LAN检查器工具。工具设计，以便接受**show tech**或**show running-config命令**从ASA或IOS路由器。它检查配置和尝试检测加密映射基于LAN到LAN IPSec隧道是否配置。若被设定，它执行配置的一多点检查并且突出显示任何配置错误和设置将协商的通道的。

ASA调试

为了排除故障在ASA防火墙的IPSec IKEv1隧道协商，您能使用这些调试指令：

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

> **注意：**如果VPN编号在ASA建立隧道是重大的， **a.b.c.d命令debug crypto condition的对等体**应该使用，在您使调试为了限制debug输出包括只有指定的对等体前。

IOS路由器调试

为了排除故障在IOS路由器的IPSec IKEv1隧道协商，您能使用这些调试指令：

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

> **注意：**如果VPN编号在IOS建立隧道是重大的， **debug crypto condition对等体A.B.C.D应该**使用的**ipv4，**在您使调试为了限制debug输出包括只有指定的对等体前。

> **提示**：参考最普通的L2L和排除故障解决方案Cisco文档的远程访问IPSec VPN关于如何排除故障站点到站点VPN的更多信息。

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
- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- IPSec LAN对LAN检查器
- 技术支持和文档 - Cisco Systems