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

目录

简介

本文档介绍如何通过Cisco ASA和运行Cisco IOS XE软件的路由器之间的CLI配置站点到站点IKEv1隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科IOS XE
- 思科自适应安全设备(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ciscosoftware 9.20(2)2版的Cisco ASAv
- 运行Cisco IOS XE软件版本17.03.03的Cisco CSRv

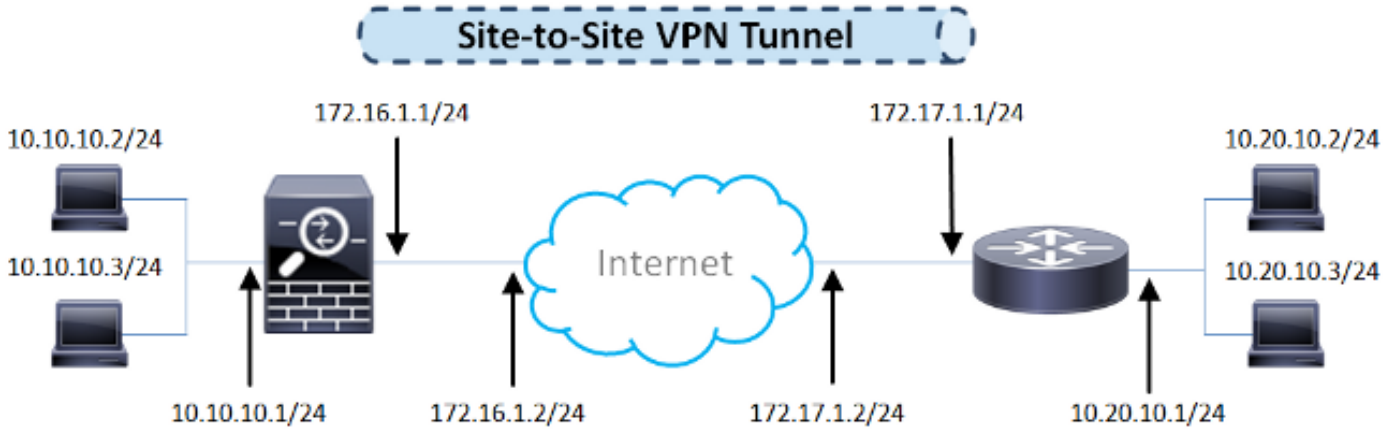
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

本节介绍如何完成ASA和Cisco IOS XE路由器CLI配置。

网络图

本文档中的信息使用以下网络设置：



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、接口名称和安全等级：

```
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：确保同时存在与内部和外部网络的连接，尤其是与用于建立站点到站点VPN隧道的远程对等体的连接。可以使用ping命令验证基本连通性。

配置IKEv1策略并在外部接口上启用IKEv1

要为IPSec Internet Key Exchange版本1 (IKEv1)连接配置互联网安全连接和密钥管理协议(ISAKMP)策略，请输入crypto ikev1 policy
命令：

<#root>

crypto ikev1 policy 10

```
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 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，远程对等体策略还必须指定小于或等于发起方发送的策略中的生存期的生存期。如果生存时间不同，则ASA使用较短的生存时间。

注意：如果没有为给定的策略参数指定值，则会应用默认值。

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
命令：

<#root>

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
```

为相关的VPN流量配置ACL

ASA使用访问控制列表(ACL)来区分必须通过IPSec加密保护的流量与不需要保护的流量。它保护与permit Application Control Engine (ACE)匹配的出站数据包，并确保与permit ACE匹配的入站数据包具有保护。

<#root>

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：用于VPN流量的ACL在网络地址转换(NAT)之后使用源和目标IP地址。

注意：用于VPN流量的ACL必须镜像到两个VPN对等体上。

注意：如果需要向受保护流量添加新子网，只需将子网/主机添加到各自的对象组并完成远程VPN对等体上的镜像更改。

配置NAT免除

注意：本节中介绍的配置是可选的。

通常，不能对VPN流量执行NAT。要免除该流量，您必须创建身份NAT规则。身份NAT规则仅将地址转换为同一地址。

```
<#root>

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，对等体必须识别对两个对等体都相同的转换集或提议。然后，ASA应用匹配的转换集或提议，以创建保护该加密映射的访问列表中的数据流的SA。

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

```
<#root>

crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
```

配置加密映射并将其应用到接口

加密映射定义要在IPSec SA中协商的IPSec策略，包括：

- 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
- 完全向前保密（可选）

例如：

```
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-AES256-SHA
```

然后，您可以将加密映射应用到接口：

<#root>

```
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 ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
!
crypto ikev1 enable outside
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 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-AES256-SHA
crypto map outside_map interface outside
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
!
```

Cisco IOS XE路由器CLI配置

配置接口

如果尚未配置Cisco IOS XE路由器接口，则必须至少配置LAN和WAN接口。例如：

```
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
```

确保同时连接到内部和外部网络，尤其是用于建立站点到站点VPN隧道的远程对等体。可以使用ping命令验证基本连通性。

配置ISAKMP (IKEv1)策略

要配置用于IKEv1连接的ISAKMP策略，请在全局配置模式下输入crypto isakmp policy 命令。 例如：

<#root>

crypto isakmp policy 10

```
 encryption aes 256
 hash sha
 authentication pre-share
 group 14
```

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公共策略，并且从远程对等体上指定的优先级最高的策略开始。

配置加密ISAKMP密钥

要配置预共享身份验证密钥，请在全局配置模式下输入crypto isakmp key命令：

<#root>

crypto isakmp key cisco123 address 172.16.1.1

为相关的VPN流量配置ACL

使用扩展或命名访问列表以指定必须通过加密保护的流量。例如：

```
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后使用源和目标IP地址。

注意：用于VPN流量的ACL必须镜像到两个VPN对等体上。

配置NAT免除

注意：本节中介绍的配置是可选的。

通常，不能对VPN流量执行NAT。如果使用NAT过载，则必须使用路由映射，以使所关注的VPN流量免于转换。请注意，在路由映射中使用的访问列表中，必须拒绝相关的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。例如：

```
<#root>

crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac

 mode tunnel
```

配置加密映射并将其应用到接口

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，至少必须定义以下几个方面：

- 必须定义可向其转发受保护流量的IPsec对等体。这些是可以建立SA的对等设备。要在加密映射条目中指定IPSec对等体，请输入set peer命令。
- 必须定义可与受保护流量一起使用的转换集。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。
- 必须定义必须保护的流量。要为加密映射条目指定扩展访问列表，请输入match address命令。

例如：

<#root>

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

```
 set peer 172.16.1.1
 set transform-set ESP-AES256-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：

<#root>

```
interface GigabitEthernet0/0
```

```
crypto map outside_map
```

Cisco IOS XE最终配置

下面是最终的Cisco IOS XE路由器CLI配置：

```
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES256-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以及是否传递流量之前，必须确保将相关流量发送到ASA或Cisco IOS XE路由器。

注意：在ASA上，匹配感兴趣流量的Packet Tracer工具可用于启动IPSec隧道(例如packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed)。

第1阶段验证

要验证ASA上的IKEv1阶段1是否已启动，请输入show crypto isakmp sa命令。预期输出是显示MM_ACTIVE状态：

<#root>

```
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Cisco IOS XE上的IKEv1阶段1是否已启动，请输入show crypto isakmp sa命令。预期输出是显示ACTIVE状态：

```
<#root>

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           2003 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

第2阶段验证

要验证ASA上的IKEv1第2阶段是否已启用，请输入show crypto ipsec sa命令。预期输出是查看入站和出站安全参数索引(SPI)。如果流量通过隧道，您必须看到封装/解码计数器递增。

注意：对于每个ACL条目，都会创建一个单独的入站/出站SA，这可能会导致长show crypto ipsec sa命令输出（具体取决于加密ACL中的ACE条目数）。

例如：

```
<#root>

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: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
```

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 989, #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: 5397114D
current inbound spi : 9B592959

inbound esp sas:
spi: 0x9B592959 (2606311769)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFD7FF

outbound esp sas:
spi: 0x5397114D (1402409293)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa#
```

要验证Cisco IOS XE上的IKEv1阶段2是否已启动，请输入show crypto ipsec sa命令。预期输出是查看入站和出站SPI。如果流量通过隧道，您必须看到封装/解码计数器递增。

例如：

<#root>

```
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: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet3
current outbound spi: 0x9B592959(2606311769)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x5397114D(1402409293)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607857/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x9B592959(2606311769)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607901/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Router#
```

第1和第2阶段验证

本节介绍可在ASA或Cisco IOS XE上用于验证第1阶段和第2阶段详细信息的命令。

在ASA上输入show vpn-sessiondb命令进行验证：

<#root>

```
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)AES256  IPsec: (1)AES256
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 98900               Bytes Rx     : 134504
Login Time   : 06:15:52 UTC Fri Sep 6 2024
Duration     : 0h:15m: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   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 84093 Seconds
  D/H Group    : 14
  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   : AES256                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     : 98900                 Bytes Rx     : 134504
  Pkts Tx      : 989                   Pkts Rx      : 989

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Cisco IOS XE上输入show crypto session命令进行验证：

<#root>

```
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 989 drop 0 life (KB/Sec) 4449870/3383
        Outbound: #pkts enc'ed 989 drop 0 life (KB/Sec) 4449868/3383

Router#
```

故障排除

本部分提供可用于对配置进行故障排除的信息。

> 注意：使用debug命令之前，请参阅有关debug命令的重要信息和IP安全故障排除-了解和使用debug命令 Cisco文档。

IPSec LAN-to-LAN检查器工具

为了自动验证ASA和Cisco IOS XE之间的IPSec LAN到LAN配置是否有效，您可以使用IPSec LAN到LAN检查器工具。该工具的设计使其能够接受来自ASA或Cisco IOS XE路由器的show tech或show running-config命令。它会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，则执行配置的多点检查，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：

<#root>

```
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，则必须使用debug crypto condition peer A.B.C.D命令才能启用调试，以便将调试输出限制为仅包括指定的对等体。

Cisco IOS XE路由器调试

为了对Cisco IOS XE路由器上的IPSec IKEv1隧道协商进行故障排除，可以使用以下debug命令：

<#root>

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

注意：如果Cisco IOS XE上的VPN隧道数量很大，则debug crypto condition peer ipv4 A.B.C.D必须在启用调试之前使用，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-to-LAN检查器(IPSec LAN-to-LAN Checker)
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。