在 ASA 和 Cisco IOS 路由器之間設定站點對站點 IPSec IKEv1 通道

目錄

簡介

本文檔介紹如何通過Cisco ASA與運行Cisco IOS®軟體的路由器之間的CLI配置站點到站點（LAN到LAN）IKEv1通道。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS
- 思科調適型安全裝置(ASA)
- 一般IPSec概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 5512-X系列ASA(運行軟體版本9.4(1))
- 運行Cisco IOS軟體版本15.4(3)M2的Cisco 1941系列整合服務路由器(ISR)

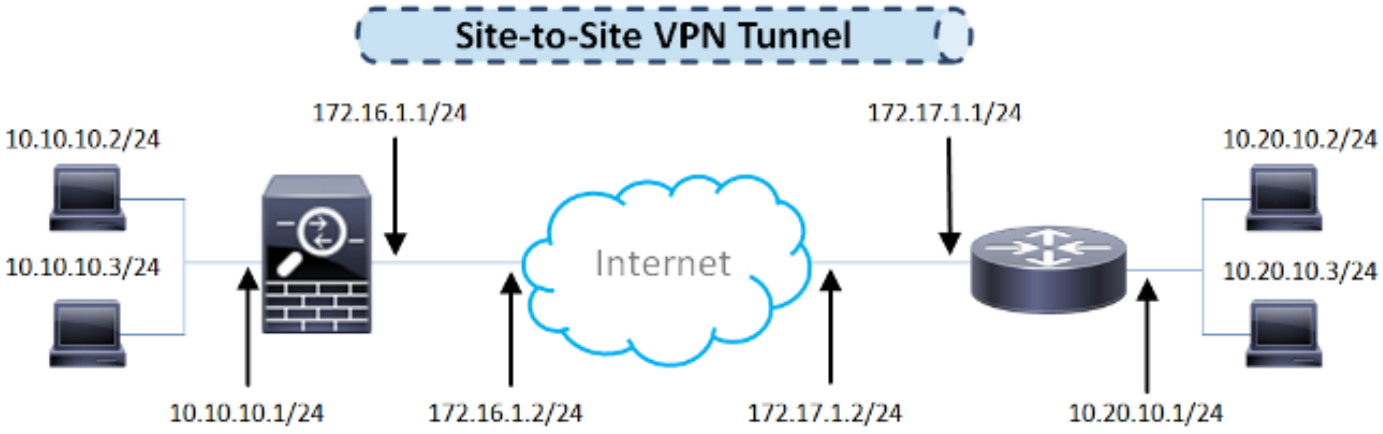
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

本節介紹如何完成ASA和Cisco IOS路由器CLI配置。

網路圖表

本檔案中的資訊使用以下網路設定：



ASA配置

配置ASA介面

如果未配置ASA介面，請確保至少配置IP地址、介面名稱和安全級別：

```
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
```

註：確保同時連線到內部和外部網路，尤其是連線到用於建立站點到站點VPN隧道的遠端對等裝置。您可以使用ping驗證基本連線。

配置IKEv1策略並在外部介面上啟用IKEv1

要為IPSec Internet金鑰交換版本1(IKEv1)連線配置Internet安全關聯和金鑰管理協定(ISAKMP)策略，請輸入 crypto ikev1 policy
指令:

<#root>

crypto ikev1 policy 10

```
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

注意：當來自兩個對等體的兩個策略包含相同的身份驗證、加密、雜湊和Diffie-Hellman引數值時，存在IKEv1策略匹配。對於IKEv1，遠端對等體策略還必須在發起方傳送的策略中指定小於或等於生存期的生存期。如果生存期不同，則ASA使用較短的生存期。

注意：如果沒有為給定的策略引數指定值，則應用預設值。

必須在終止VPN隧道的介面上啟用IKEv1。通常，這是外部（或公共）介面。要啟用IKEv1，請輸入 crypto ikev1 enable
命令在全域性配置模式下：

<#root>

crypto ikev1 enable outside

配置隧道組（LAN到LAN連線配置檔案）

對於LAN到LAN隧道，連線配置檔案型別為 ipsec-l2l .要配置IKEv1預共用金鑰，請輸入 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
```

為相關的VPN流量配置ACL

ASA使用訪問控制清單(ACL)來區分必須使用IPSec加密保護的流量和不需要保護的流量。它保護與permit Application Control Engine(ACE)匹配的出站資料包，並確保與permit ACE匹配的入站資料包具有保護。

<#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：用於VPN流量的ACL在網路地址轉換(NAT)之後使用源和目標IP地址。

注意：用於VPN流量的ACL必須在兩個VPN對等體上映象。

注意：如果需要向受保護流量新增新子網，只需將子網/主機新增到各自的對象組，並在遠端VPN對等體上完成映象更改。

配置NAT免除

註：本節中介紹的配置是可選的。

通常情況下，不能對VPN流量執行NAT。要免除該流量，您必須建立身份NAT規則。身份NAT規則只是將地址轉換為同一地址。

```
<#root>

nat (inside,outside) source static

local-network local-network

 destination static

remote-network remote-network

 no-proxy-arp route-lookup
```

配置IKEv1轉換集

IKEv1轉換集是安全協定和演算法的組合，用於定義ASA保護資料的方式。在IPSec安全關聯(SA)協商期間，對等體必須標識兩個對等體相同的轉換集或提議。然後，ASA應用匹配的轉換集或提議，以便建立一個SA，保護該加密對映的訪問清單中的資料流。

要配置IKEv1轉換集，請輸入 crypto ipsec ikev1 transform-set 指令:

```
<#root>

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

設定密碼編譯對應並將其套用到介面

加密對映定義要在IPSec SA中協商的IPSec策略，包括：

- 訪問清單，用於標識IPSec連線允許和保護的資料包
- 對等體識別
- IPSec流量的本地地址
- IKEv1轉換集

以下是範例：

```
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
```

接著您可以對介面套用密碼編譯對應：

<#root>

crypto map outside_map interface outside

ASA最終配置

以下是ASA的最終配置：

```
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
```

Cisco IOS路由器CLI配置

配置介面

如果尚未配置Cisco IOS路由器介面，則必須至少配置LAN和WAN介面。以下是範例：

```
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
```

確保同時連線到內部和外部網路，尤其是連線到用於建立站點到站點VPN隧道的遠端對等裝置。您可以使用ping驗證基本連線。

配置ISAKMP(IKEv1)策略

要為IKEv1連線配置ISAKMP策略，請輸入 crypto isakmp policy 命令。 以下是範例：

```
<#root>

crypto isakmp policy 10

 encr aes
 authentication pre-share
 group 2
```

注意：可以在參與IPSec的每個對等體上配置多個IKE策略。當IKE協商開始時，它會嘗試查詢在兩個對等體上配置的公共策略，並且從遠端對等體上指定的最高優先順序策略開始。

配置加密ISAKMP金鑰

要配置預共用身份驗證金鑰，請輸入 crypto isakmp key 命令在全域性配置模式下：

<#root>

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

為相關的VPN流量配置ACL

使用擴展訪問清單或命名訪問清單來指定必須通過加密保護的流量。以下是範例：

```
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：用於VPN流量的ACL在NAT之後使用源和目標IP地址。

注意：用於VPN流量的ACL必須在兩個VPN對等體上映象。

配置NAT免除

註：本節中介紹的配置是可選的。

通常情況下，不能對VPN流量執行NAT。如果使用NAT過載，則必須使用路由對映，以免除轉換所關注的VPN流量。請注意，在路由對映中使用的訪問清單中，必須拒絕所關注的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
```

配置轉換集

要定義IPSec轉換集（安全協定和演算法的可接受組合），請輸入 crypto ipsec transform-set 命令。以下是範例：

<#root>

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

 mode tunnel
```

設定密碼編譯對應並將其套用到介面

若要建立或修改加密對映條目並進入加密對映配置模式，請輸入crypto map全域性配置命令。為了完成加密對映條目，必須至少定義以下幾個方面：

- 必須定義可將受保護流量轉發到的IPsec對等路由器。以下是可以建立SA的對等路由器。要在加密對映條目中指定IPSec對等體，請輸入 set peer 指令。
- 必須定義可與受保護流量一起使用的轉換集。要指定可與加密對映條目一起使用的轉換集，請輸入 set transform-set 指令。
- 必須定義必須保護的流量。要為加密對映條目指定擴展訪問清單，請輸入 match address 指令。

以下是範例：

<#root>

```
crypto map outside_map 10 ipsec-isakmp

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

最後一步是將之前定義的加密對映集應用到介面。若要應用此功能，請輸入 crypto map interface configuration命令：

<#root>

```
interface GigabitEthernet0/0
```

crypto map outside_map

Cisco IOS最終配置

下面是最終的Cisco 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
```

驗證

在驗證隧道是否已啟動並且是否傳遞流量之前，必須確保將相關流量傳送到ASA或Cisco IOS路由器。

> 注意：在ASA上，可以使用與感興趣的流量匹配的Packet Tracer工具來啟動IPSec隧道(例如 packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed 例如)。

第1階段驗證

要驗證ASA上的IKEv1第1階段是否已啟動，請輸入show crypto isakmp sa 命令。預期輸出將看到 MM_ACTIVE 狀態:

<#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#
```

要驗證Cisco IOS上的IKEv1第1階段是否已啟動，請輸入 show crypto isakmp sa 指令。預期輸出將看到 ACTIVE 狀態:

<#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           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

第2階段驗證

要驗證ASA上的IKEv1第2階段是否已啟動，請輸入 show crypto ipsec sa 指令。預期輸出是檢視入站和出站安全引數索引(SPI)。如果流量通過隧道，您必須看到封裝/解除封裝計數器的增量。

注意：對於每個ACL條目，都會建立一個單獨的入站/出站SA，這會導致 show crypto ipsec sa 命令輸出（取決於加密ACL中ACE條目的數量）。

以下是範例：

```
<#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: 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#
```

要驗證Cisco IOS上的IKEv1第2階段是否已啟動，請輸入 show crypto ipsec sa 指令。預期輸出是同時檢視入站和出站SPI。如果流量通過隧道，您必須看到封裝/解除封裝計數器的增量。

以下是範例：

```
<#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: 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#
```

第1階段和第2階段驗證

本節介紹可以在ASA或Cisco IOS上使用的命令，以驗證第1階段和第2階段的詳細資訊。

輸入 show vpn-sessiondb 命令進行驗證：

<#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)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#
```

輸入 show crypto session 命令，以便驗證：

<#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 2015 drop 0 life (KB/Sec) 4449870/3383
        Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

註：使用之前，請參閱有關Debug命令和IP安全性故障排除的重要資訊 — 瞭解和使用debug命令Cisco文檔 debug 指令。

IPSec LAN到LAN檢查器工具

要自動驗證ASA和Cisco IOS之間的IPSec LAN到LAN配置是否有效，可以使用IPSec LAN到LAN檢查工具。該工具設計為接受 show tech 或 show running-config ASA或Cisco IOS路由器的命令。它會檢查配置並嘗試檢測是否配置了基於加密對映的LAN到LAN IPSec隧道。如果配置成功，則會對配置執行多點檢查，並突出顯示要協商的隧道的所有配置錯誤和設定。

ASA調試

若要對ASA防火牆上的IPSec IKEv1通道協商進行故障排除，可以使用以下命令 debug 指令：

<#root>

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

注意：如果ASA上的VPN隧道數量很大，則 debug crypto condition peer A.B.C.D 在啟用調試之前，必須使用command命令以限制調試輸出只包括指定的對等體。

Cisco IOS路由器調試

若要對Cisco IOS路由器上的IPSec IKEv1通道交涉進行疑難排解，可以使用以下debug命令：

<#root>

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

注意：如果Cisco IOS上的VPN隧道數量很大，則 debug crypto condition peer ipv4 A.B.C.D 必須在啟用調試之前使用，以便將調試輸出限製為僅包括指定的對等體。

提示：有關如何對站點到站點VPN進行故障排除的詳細資訊，請參閱最常見的L2L和遠端訪問IPSec VPN故障排除解決方案Cisco文檔。

參考資料

- 有關Debug命令的重要資訊
- IP安全性疑難排解 — 瞭解和使用debug命令
- 最常見的L2L和遠端訪問IPSec VPN故障排除解決方案
- IPSec LAN到LAN檢查器
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。