

在ASA上使用ASDM或CLI配置IKEv1 IPsec站點到站點隧道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[通過ASDM VPN嚮導配置](#)

[通過CLI配置](#)

[為ASA 8.4及更高版本配置站點B](#)

[為ASA 8.2及更低版本配置站點A](#)

[組策略](#)

[驗證](#)

[ASDM](#)

[CLI](#)

[第1階段](#)

[第2階段](#)

[疑難排解](#)

[ASA 8.4及更高版本](#)

[ASA 8.3及更低版本](#)

簡介

本文檔介紹如何在運行軟體版本9.2.x的Cisco 5515-X系列自適應安全裝置(ASA)和運行軟體版本8.2.x的Cisco 5510系列ASA之間配置網際網路金鑰交換版本1(IKEv1)IPsec站點到站點隧道。

必要條件

需求

思科建議您瞭解以下主題：

- 必須建立端到端IP連線
- 必須允許以下協定：
適用於IPsec控制平面的使用者資料包通訊協定(UDP)500和4500為IPsec資料平面封裝安全負載(ESP)IP協定50

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.2的Cisco 5510系列ASA
- 運行軟體版本9.2的Cisco 5515-X ASA

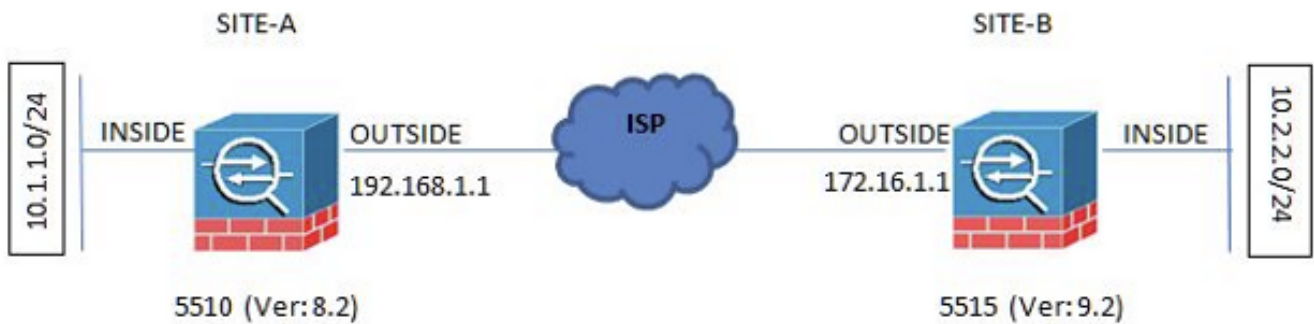
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

本節介紹如何通過自適應安全裝置管理器(ASDM)VPN嚮導或通過CLI配置站點到站點VPN隧道。

網路圖表

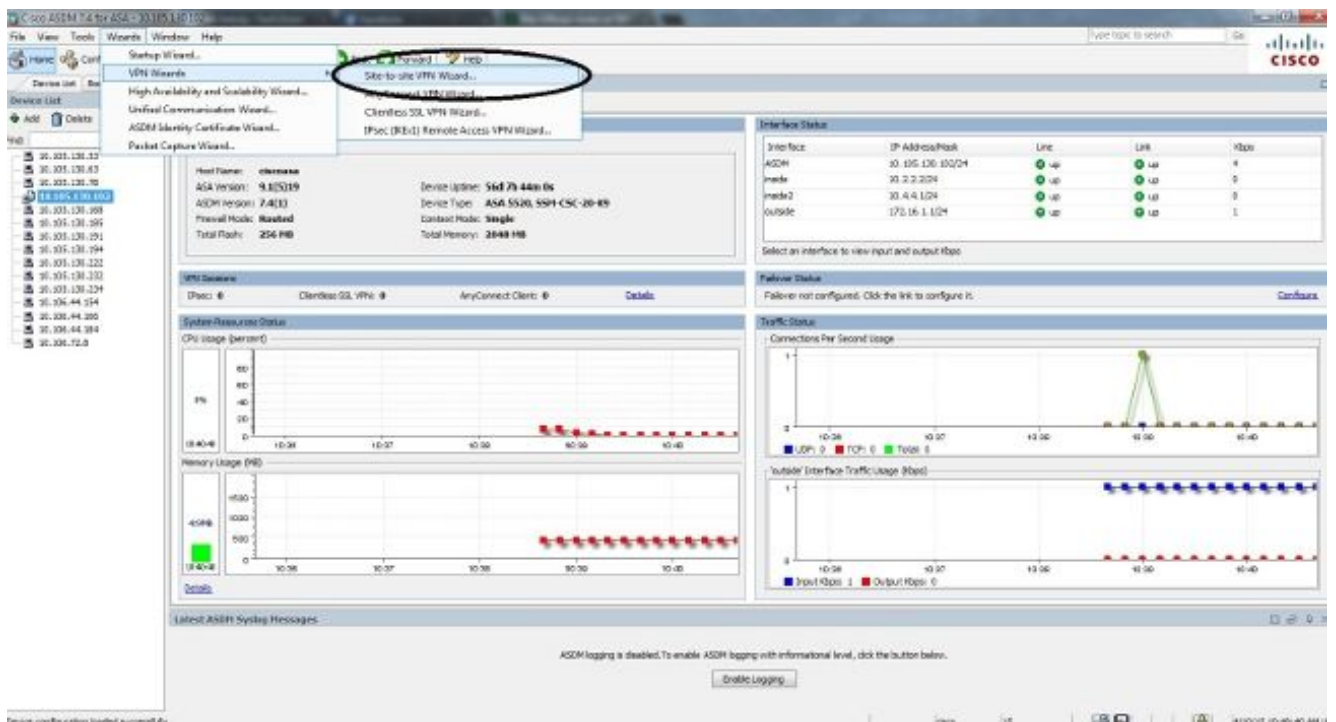
此拓撲用於本文檔中的示例：



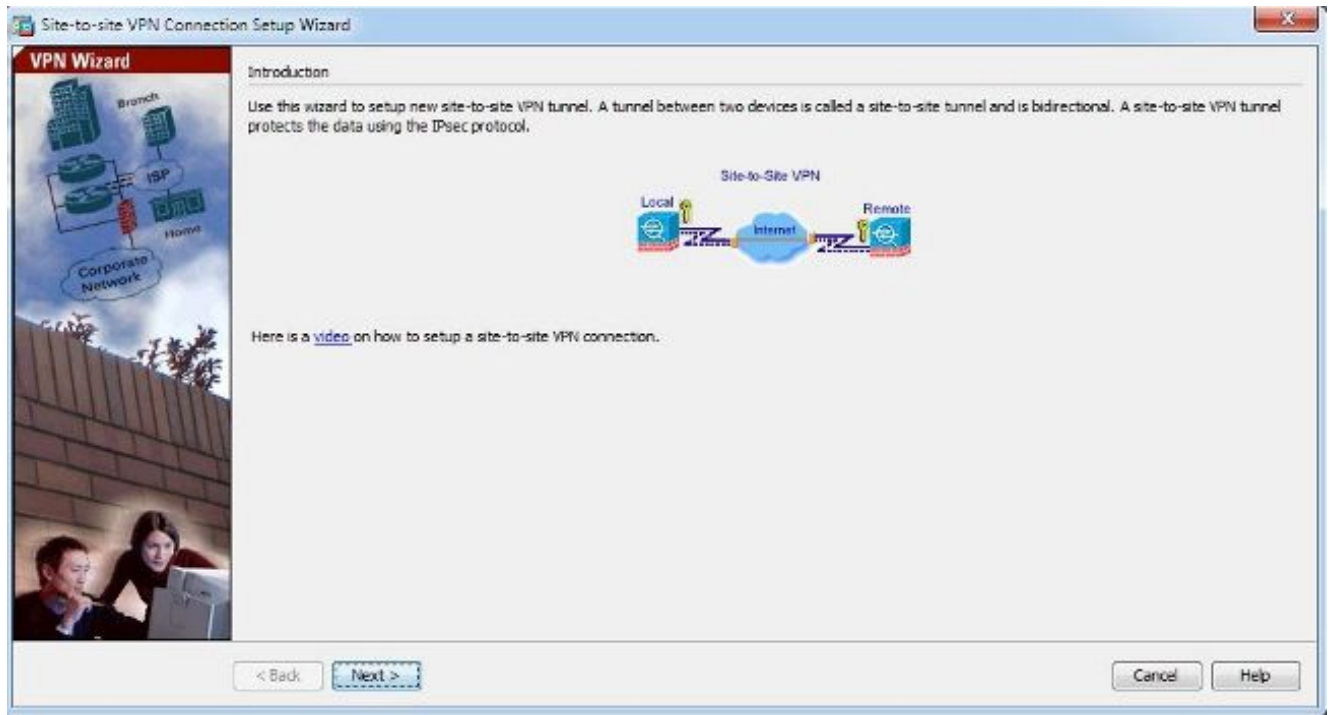
通過ASDM VPN嚮導配置

完成以下步驟，以便通過ASDM嚮導設定站點到站點VPN隧道：

1. 開啟ASDM並導航至 Wizards > VPN Wizards > Site-to-site VPN Wizard.

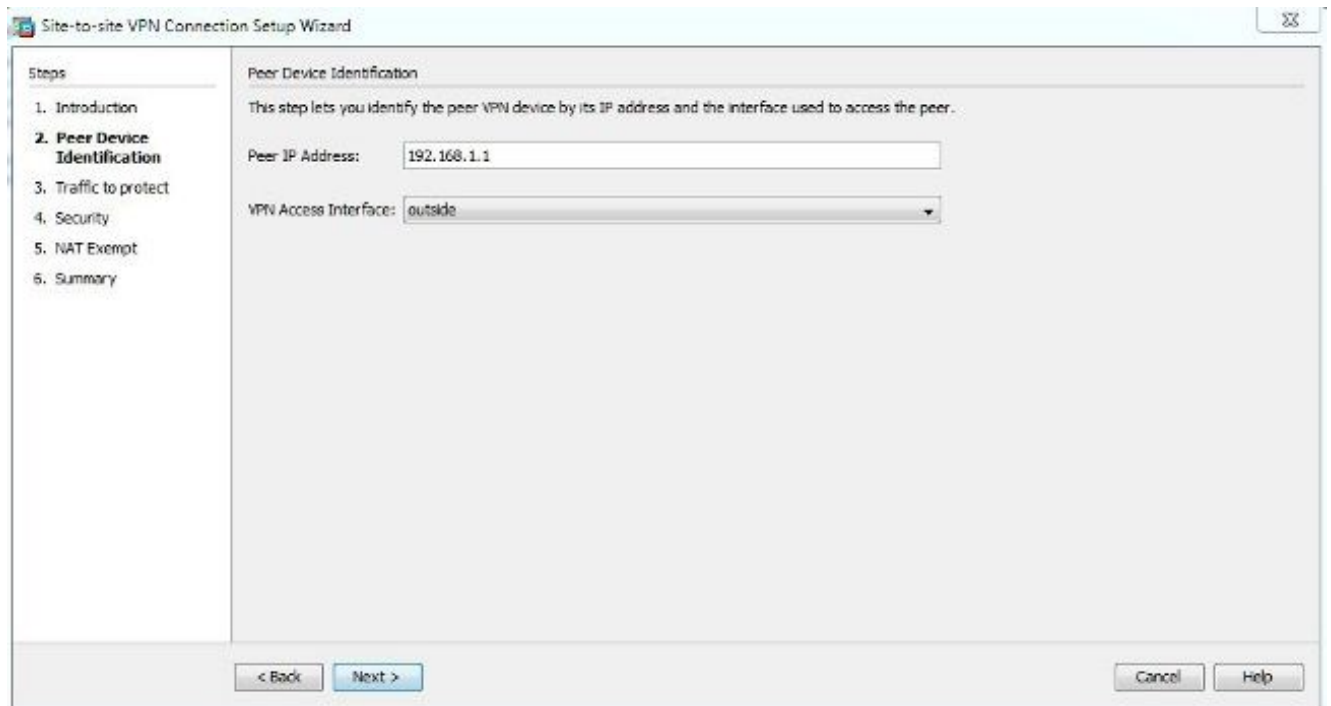


2. 按一下 Next 進入嚮導首頁後。

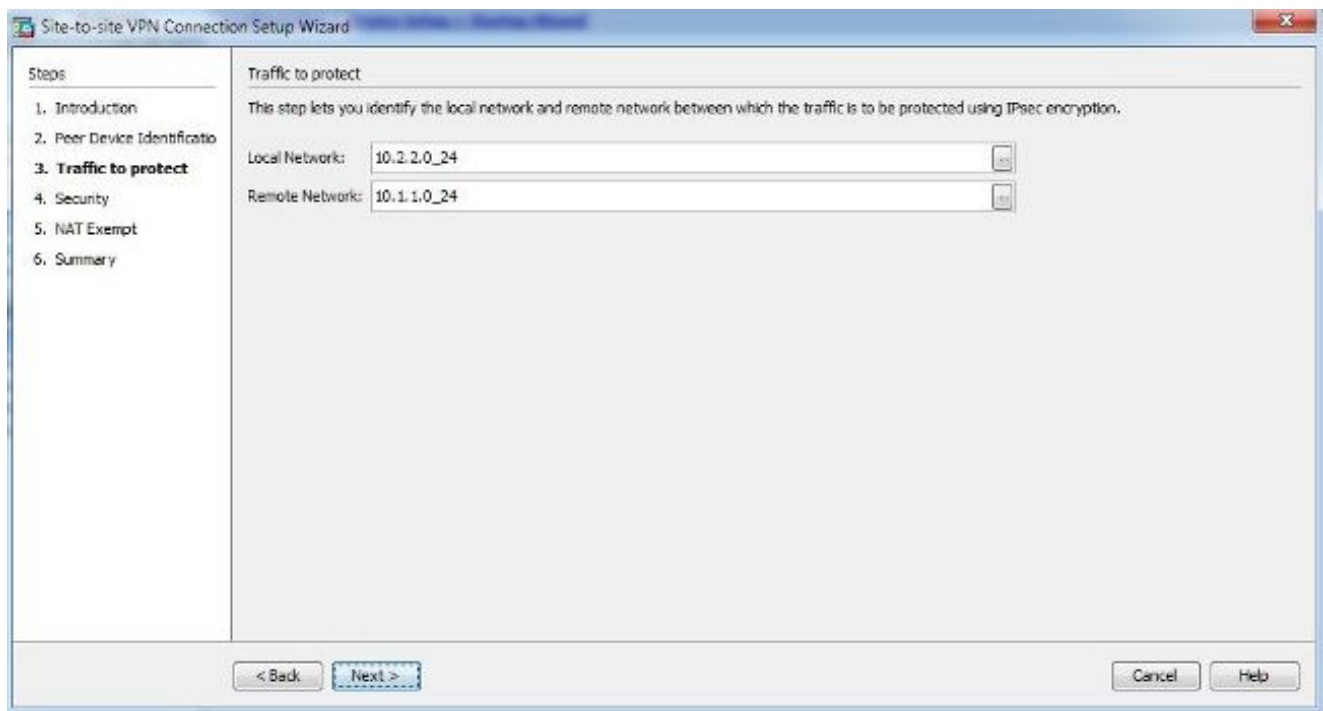


註：最新的ASDM版本提供影片連結，解釋此配置。

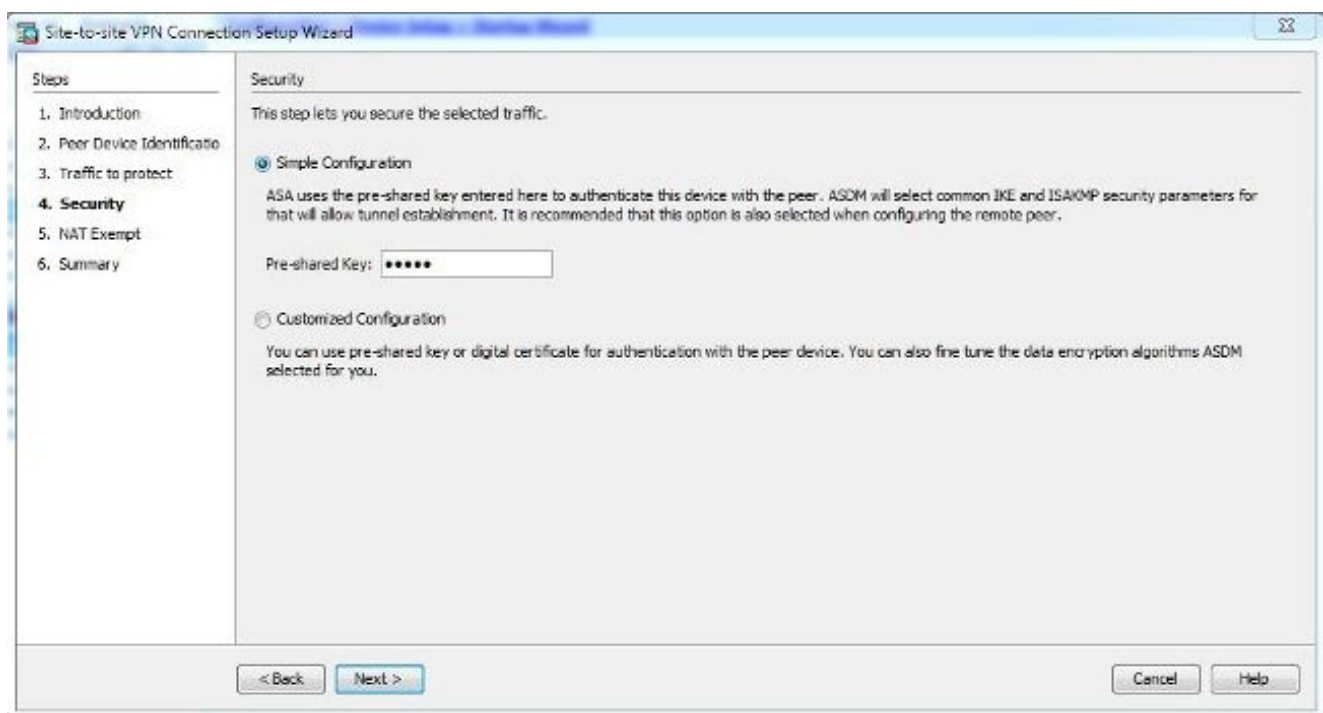
3. 配置對等IP地址。在本示例中，站點B的對等IP地址設定為192.168.1.1。如果在站點A上配置對等IP地址，則必須將其更改為172.16.1.1。還指定了可以到達遠端端的介面。按一下 Next 一旦完成。



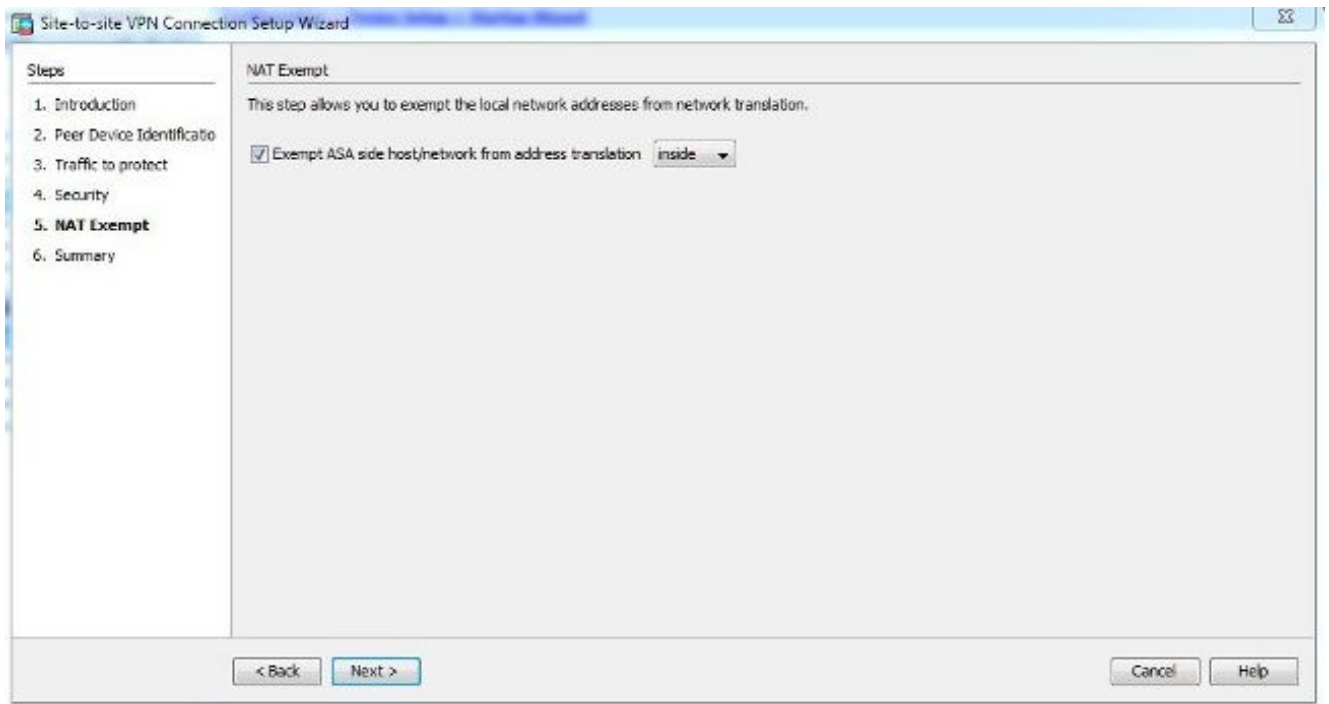
4. 配置本地和遠端網路 (流量源和目標)。此圖顯示了站點B的配置 (與站點A相反)。



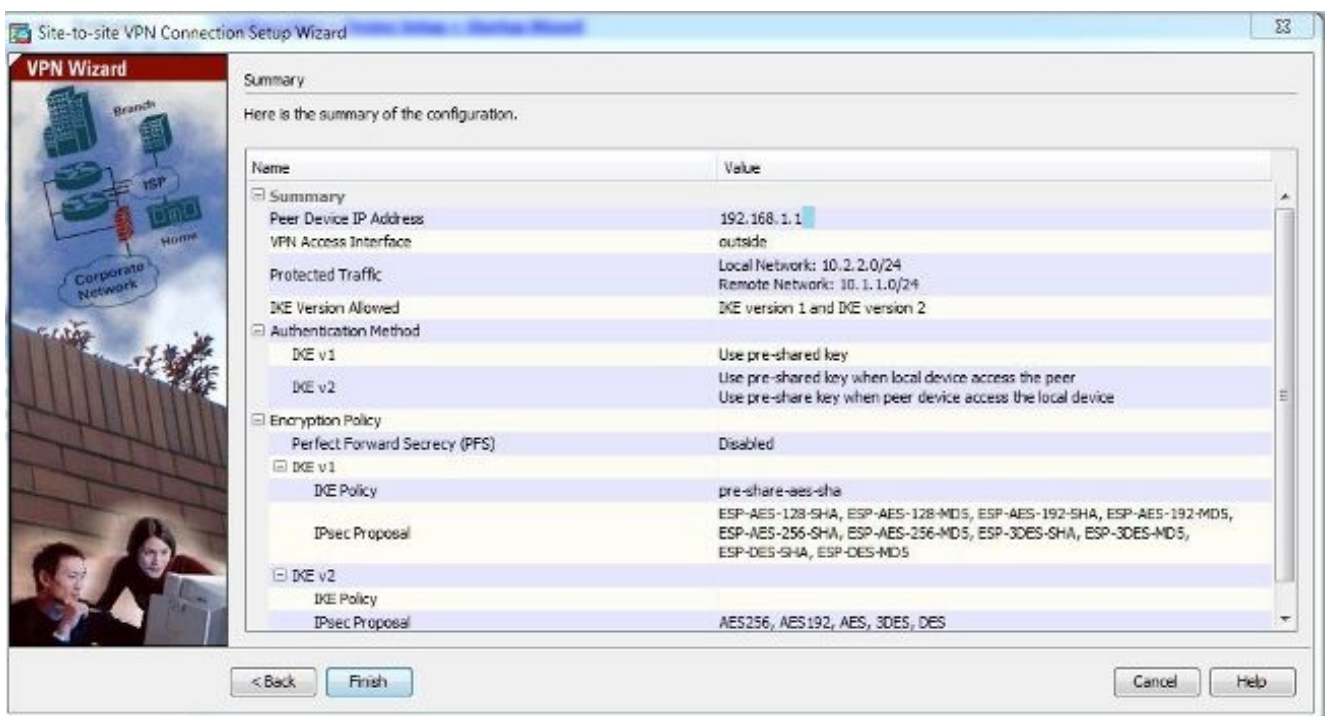
5. 在Security頁面上，配置預共用金鑰（其兩端必須匹配）。按一下 Next 一旦完成。



6. 為ASA上的流量配置源介面。ASDM根據ASA版本自動建立網路地址轉換(NAT)規則，並在最後步驟中將其與配置其餘部分一起推送。註：對於本文檔中使用的示例，「inside」是流量的來源。



7. 現在，該嚮導提供推送到ASA的配置的摘要。檢視並驗證配置設定，然後按一下 Finish。



通過CLI配置

本節介紹如何通過CLI配置IKEv1 IPsec站點到站點隧道。

為ASA 8.4及更高版本配置站點B

在ASA 8.4及更高版本中，引入了對IKEv1和Internet金鑰交換版本2(IKEv2)的支援。

提示：有關兩個版本之間差異的更多資訊，請參閱在ASA 8.4代碼思科文檔上將IKEv1遷移到IKEv2 L2L隧道配置的Swift遷移IKEv1至IKEv2的原因[遷移到IKEv2?](#)部分。

提示：有關ASA的IKEv2配置示例，請參閱[ASA和路由器之間的站點到站點IKEv2隧道配置示例Cisco](#)文檔。

第1階段(IKEv1)

完成第1階段配置的以下步驟：

1. 在CLI中輸入以下命令以在外部介面上啟用IKEv1:

```
crypto ikev1 enable outside
```

2. 建立IKEv1策略，該策略定義用於雜湊、身份驗證、Diffie-Hellman組、生存期和加密的演算法/方法：

```
crypto ikev1 policy 1
!The 1 in the above command refers to the Policy suite priority
(1 highest, 65535 lowest)
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. 在IPsec屬性下建立隧道組，並配置對等IP地址和隧道預共用金鑰：

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
! Note the IKEv1 keyword at the beginning of the pre-shared-key command.
```

階段2(IPsec)

完成第2階段配置的以下步驟：

1. 建立定義要加密和隧道化的流量的訪問清單。在本例中，感興趣的流量是來自從10.2.2.0子網到10.1.1.0的隧道的流量。如果站點之間涉及多個子網，則它可以包含多個條目。

在8.4及更高版本中，可以建立用作網路、子網、主機IP地址或多個對象的容器的對象或對象組。建立兩個具有本地和遠端子網的對象，並將它們用於加密訪問控制清單(ACL)和NAT語句。

```
object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
subnet 10.1.1.0 255.255.255.0
```

```
access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

2. 配置轉換集(TS)，其中必須包含關鍵字 IKEv1。在遠端也必須建立相同的TS。

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

3. 配置包含以下元件的加密對映：

對等IP地址包含相關流量的已定義訪問清單TS可選的完全向前保密(PFS)設定，它建立了一對新的Diffie-Hellman金鑰，用於保護資料（在第2階段啟動之前，兩端都必須啟用PFS）

4. 在外部介面上應用加密對映：

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

NAT免除

確保VPN流量不受任何其他NAT規則的約束。以下是使用的NAT規則：

```
nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

注意：使用多個子網時，您必須建立包含所有源子網和目標子網的對象組，並在NAT規則中使用它們。

```
object-group network 10.x.x.x_SOURCE
network-object 10.4.4.0 255.255.255.0
network-object 10.2.2.0 255.255.255.0
```

```
object network 10.x.x.x_DESTINATION
network-object 10.3.3.0 255.255.255.0
network-object 10.1.1.0 255.255.255.0
```

```
nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE destination
static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

完成示例配置

以下是站點B的完整配置：

crypto ikev1 enable outside

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

```
tunnel-group 192.168.1.1 type ipsec-l2l
tunnel-group 192.168.1.1 ipsec-attributes
ikev1 pre-shared-key cisco
```

!Note the IKEv1 keyword at the beginning of the pre-shared-key command.


```
object network 10.2.2.0_24
subnet 10.2.2.0 255.255.255.0
object network 10.1.1.0_24
subnet 10.1.1.0 255.255.255.0

access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24

crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 192.168.1.1
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static
10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

為ASA 8.2及更低版本配置站點A

本節介紹如何為ASA 8.2及更低版本配置站點A。

第1階段(ISAKMP)

完成第1階段配置的以下步驟：

1. 在CLI中輸入以下命令，以在外部介面上啟用網際網路安全性關聯和金鑰管理通訊協定 (ISAKMP):

```
crypto isakmp enable outside
```

註：由於不再支援多個版本的IKE (IKEv1和IKEv2)，因此使用ISAKMP來指代第1階段。

2. 建立一個ISAKMP策略，該策略定義用於構建階段1的演算法/方法。

註：在此示例配置中，關鍵字 IKEv1 從9.x版替換為 ISAKMP。

```
crypto isakmp policy 1
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
```

3. 使用預共用金鑰為對等IP地址 (外部IP地址5515) 建立隧道組：

```
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco
```

階段2(IPsec)

完成第2階段配置的以下步驟：

1. 與版本9.x中的配置類似，您必須建立擴展訪問清單以定義感興趣的流量。


```
access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
```

2. 定義包含所有可用加密和雜湊演算法的TS (提供的問題有一個問號)。確保它與另一端配置的配置相同。

```
crypto ipsec transform-set myset esp-aes esp-sha-hmac
```

3. 配置包含以下元件的加密對映：
對等IP地址包含相關流量的已定義訪問清單TS一個可選的PFS設定，該設定建立一個新的Diffie-Hellman金鑰對，用於保護資料 (兩端必須啟用PFS才能啟動階段2)
4. 在外部介面上應用加密對映：

```
crypto map outside_map 20 set peer 172.16.1.1
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside
```

NAT免除

建立一個訪問清單，定義要免除進行NAT檢查的流量。在此版本中，它類似於您為感興趣的流量定義的訪問清單：

```
access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
```

當使用多個子網時，將另一行新增到同一個訪問清單中：

```
access-list nonat line 1 extended permit ip 10.3.3.0 255.255.255.0
10.4.4.0 255.255.255.0
```

訪問清單與NAT一起使用，如下所示：

```
nat (inside) 0 access-list nonat
```

註：這裡的「inside」是指內部介面的名稱，ASA接收與訪問清單匹配的流量。

完成示例配置

以下是站點A的完整配置：

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption aes
hash sha group 2
```

```
lifetime 86400

tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 ipsec-attributes
pre-shared-key cisco

access-list 100 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0
crypto ipsec transform-set myset esp-aes esp-sha-hmac

crypto map outside_map 20 set peer
crypto map outside_map 20 match address 100
crypto map outside_map 20 set transform-set myset
crypto map outside_map 20 set pfs
crypto map outside_map interface outside

access-list nonat line 1 extended permit ip 10.1.1.0 255.255.255.0
10.2.2.0 255.255.255.0

nat (inside) 0 access-list nonat
```

組策略

組策略用於定義適用於隧道的特定設定。這些策略與隧道組結合使用。

組策略可以定義為內部，這意味著從ASA上定義的屬性中抽取屬性，也可以定義為外部，從外部伺服器查詢屬性。以下是用於定義組策略的命令：

```
group-policy SITE_A internal
```

註：您可以在組策略中定義多個屬性。有關所有可能屬性的清單，請參閱Cisco ASA 5500系列版本5.2的選定ASDM VPN配置過程的[配置組策略](#)部分。

組策略可選屬性

其 `vpn-tunnel-protocol` 屬性確定必須應用這些設定的隧道型別。在此範例中，使用IPsec:

```
vpn-tunnel-protocol ?
group-policy mode commands/options:
IPSec IP Security Protocol l2tp-ipsec L2TP using IPSec for security
svc SSL VPN Client
webvpn WebVPN

vpn-tunnel-protocol ipsec - Versions 8.2 and prior
vpn-tunnel-protocol ikev1 - Version 8.4 and later
```

您可以選擇配置隧道，使其保持空閒（無流量）且不發生故障。要配置此選項，請 `vpn-idle-timeout` 屬性值必須使用分鐘，或者可以將該值設定為 `none`，這意味著隧道永遠不會關閉。

以下是範例：

```
group-policy SITE_A attributes
vpn-idle-timeout ?
group-policy mode commands/options:
<1-35791394> Number of minutes
none IPsec VPN: Disable timeout and allow an unlimited idle period;
```

其 default-group-policy 隧道組常規屬性下的命令定義用於為已建立的隧道推送某些策略設定的組策略。未在組策略中定義的選項的預設設定取自全域性預設組策略：

```
tunnel-group 172.16.1.1 general-attributes
default-group-policy SITE_A
```

驗證

使用本節提供的資訊以驗證您的組態是否正常運作。

ASDM

要檢視來自ASDM的隧道狀態，請導航至 **Monitoring > VPN**。以下資料提供：

- 對等IP地址
- 用於建立通道的通訊協定
- 使用的加密演算法
- 隧道啟動的時間和啟動時間
- 接收和傳輸的資料包數

提示：按一下 **Refresh** 因為資料不會即時更新，所以要檢視最新的值。

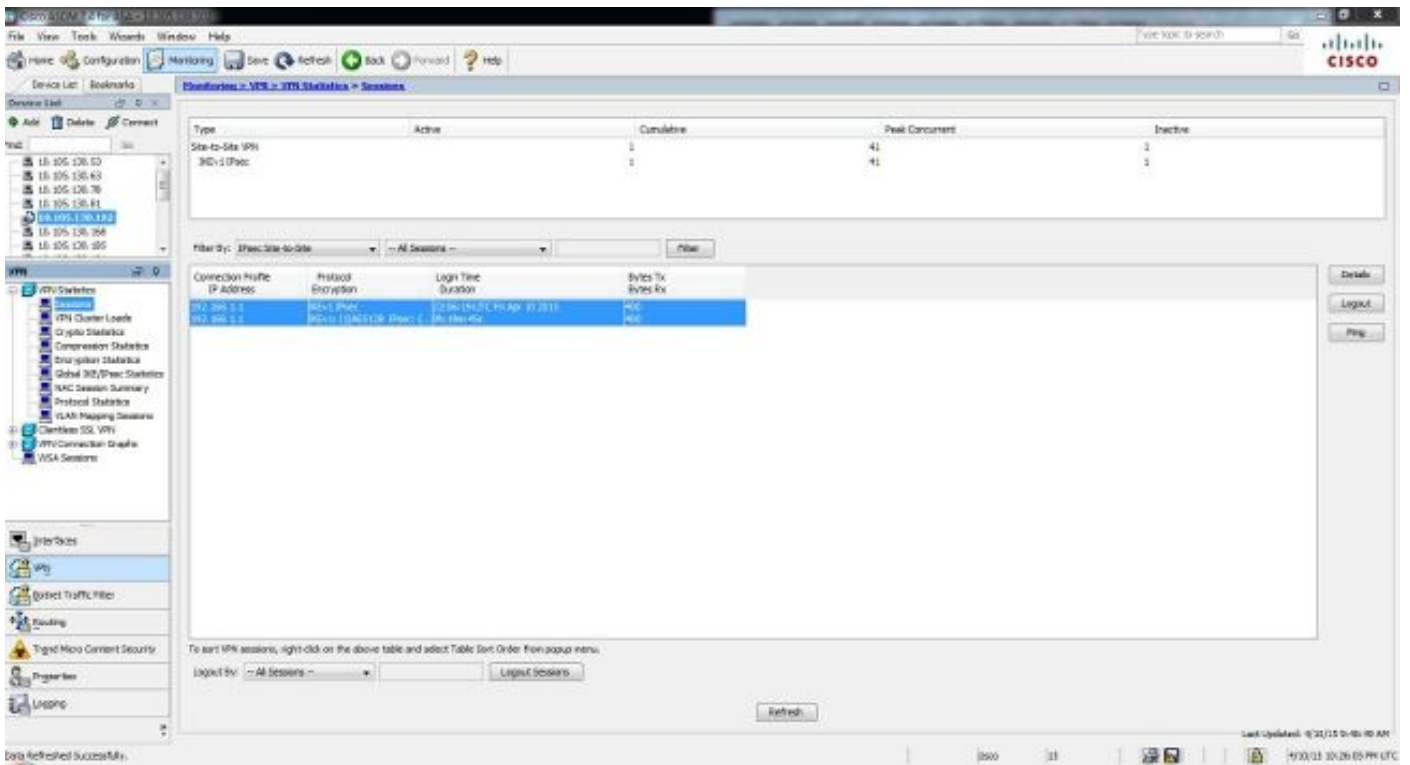
The screenshot shows the Cisco ASDM interface for monitoring VPN sessions. The main window displays a table with the following data:

Reverse Access	Site-to-Site	Overview	VPN Client	Inactive	Total	E-mail Proxy	VPN LoadBalancing	Total	Total Cumulative
0	1	1	0	0	0	0	0	1	2

Below the table, there is a section for 'Filter By: IPsec Site-to-Site' and a table of active sessions:

Connection Profile	IP Address	Protocol	Encryption	Duration	Login Time	Bytes Tx	Bytes Rx
172.16.1.1	172.16.1.1	IPsec	DES	00:00:00:00	00:00:00:00	0	0
172.16.1.1	172.16.1.1	IPsec	DES	00:00:00:00	00:00:00:00	0	0

The interface includes a 'Refresh' button at the bottom and a status bar at the very bottom that reads 'Data Refreshed Successfully' and 'Last Updated: 4/10/15 9:43:56 AM'.



CLI

本節介紹如何通過CLI驗證您的配置。

第1階段

在CLI中輸入以下命令，以在站點B(5515)端驗證階段1的組態：

```
show crypto ikev1 sa
```

```
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: 192.168.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

在CLI中輸入以下命令，以在站點A(5510)端驗證階段1的組態：

```
show crypto isakmp sa
```

```
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: 172.16.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```

第2階段

其 `show crypto ipsec sa` 命令顯示在對等體之間構建的IPsec SA。對於網路10.1.1.0和10.2.2.0之間流動的流量，在IP地址192.168.1.1和172.16.1.1之間構建加密隧道。您可以看到為入站和出站流量構建的兩個ESP SA。由於沒有AH SA，因此未使用身份驗證報頭(AH)。

在CLI中輸入以下命令，以在站點B(5515)端驗證階段2配置：

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 172.16.1.1
  local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
  current_peer: 192.168.1.1
PERMIT, flags={origin_is_acl,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
#pkts decompress failed: 0, #send errors 0, #recv errors 0
  local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas
```

在CLI中輸入以下命令，以在站點A(5510)端驗證階段2的組態：

```
interface: FastEthernet0
Crypto map tag: outside_map, local addr. 192.168.1.1
  local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  current_peer: 172.16.1.1
PERMIT, flags={origin_is_acl,}
  #pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify 20
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0,
```

```

#pkts decompress failed: 0, #send errors 0, #recv errors 0
  local crypto endpt.: 192.168.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, media mtu 1500
current outbound spi: 3D3
inbound esp sas:
spi: 0x136A010F(325714191)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3442, flow_id: 1443, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
inbound pcp sas:
outbound esp sas:
spi: 0x3D3(979)
  transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 3443, flow_id: 1444, crypto map: outside_map
  sa timing: remaining key lifetime (k/sec): (4608000/52)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas

```

疑難排解

使用本節提供的資訊對組態問題進行疑難排解。

ASA 8.4及更高版本

輸入以下debug命令可判斷通道失敗的位置：

- debug crypto ikev1 127 (第1階段)
- debug crypto ipsec 127 (第2階段)

以下是偵錯輸出的完整範例：

```

IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple: Prot=1,
saddr=10.2.2.1, sport=19038, daddr=10.1.1.1, dport=19038
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 20: matched.
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE Initiator: New Phase 1, Intf NP
Identity Ifc, IKE Peer 192.168.1.1 local Proxy Address 10.2.2.0, remote Proxy
Address 10.1.1.0, Crypto map (outside_map) Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing ISAKMP SA payload Feb 13 23:48:56 [IKEv1 DEBUG]IP =
192.168.1.1, constructing NAT-Traversal VID ver 02 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver 03 payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Traversal VID
ver RFC payload

```

Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Fragmentation VID + extended capabilities payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 172
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Oakley proposal is acceptable
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received NAT-Traversal ver 02 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Fragmentation VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, IKE Peer included IKE fragmentation capability flags: Main Mode: True Aggressive Mode: True
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing Cisco Unity VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing xauth V6 VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send IOS VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, constructing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ke payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing ISA_KE payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]?IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Cisco Unity client VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received xauth V6 VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, processing NAT-Discovery payload
!
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, computing NAT Discovery hash
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, **Connection landed on tunnel_group 192.168.1.1**
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, Generating keys for Initiator...

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing ID payload
Feb 13 23:48:56 [IKEv1 DEBUG]!Group = 192.168.1.1, IP = 192.168.1.1, constructing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Constructing IOS keep alive payload: proposal=32767/32767 sec.
!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/10 ms
ciscoasa# Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing dpd vid payload
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500 from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, ID_IPV4_ADDR ID received 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Computing hash for ISAKMP
Feb 13 23:48:56 [IKEv1 DEBUG]IP = 192.168.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec.
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, processing VID payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Received DPD VID
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Connection landed on tunnel_group 192.168.1.1
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Oakley begin quick mode
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator starting QM: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 1 COMPLETED
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, Keep-alive type for this connection: DPD
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting P1 rekey timer: 73440 seconds.
IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,
Direction: inbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got SPI from key engine: SPI = 0x03fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constucting quick mode
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing blank hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, constructing IPSec SA payload

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing IPSec nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
constructing proxy ID
**Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Transmitting Proxy Id:**
Local subnet: 10.2.2.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
IKE Initiator sending Initial Contact
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1,
IP = 192.168.1.1, constructing qm hash payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1,
IP = 192.168.1.1, IKE Initiator sending 1st QM pkt: msg id = 4c073b21
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
NOTIFY (11) + NONE (0) total length : 200
Feb 13 23:48:56 [IKEv1]IKE Receiver: Packet received on 172.16.1.1:500
from 192.168.1.1:500
Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE RECEIVED Message (msgid=4c073b21)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
total length : 172
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing hash payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing SA payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing nonce payload
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
processing ID payload
Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
loading all IPSEC SAs
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
NP encrypt rule look up for crypto map outside_map 20 matching ACL
100: returned cs_id=6ef246d0; encrypt_rule=752972d0;
tunnelFlow_rule=75ac8020
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1,
Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x6f0e03f0,
SCB: 0x75B6DD00,
Direction: outbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000002
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x1BA0C55C
IPSEC: Creating outbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x0B47D387

Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: New outbound encrypt rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false

IPSEC: Completed outbound encrypt rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: New outbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, NP encrypt rule look up for crypto map outside_map 20 matching ACL 100: returned cs_id=6ef246d0; encrypt_rule=752972d0; tunnelFlow_rule=75ac8020

Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, Security negotiation complete for LAN-to-LAN Group (192.168.1.1) Initiator, Inbound SPI = 0x03fc9db7, Outbound SPI = 0x1ba0c55c

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, oakley constructing final quick mode

Feb 13 23:48:56 [IKEv1 DECODE]Group = 192.168.1.1, IP = 192.168.1.1, IKE Initiator sending 3rd QM pkt: msg id = 4c073b21

Feb 13 23:48:56 [IKEv1]IP = 192.168.1.1, IKE_DECODE SENDING Message (msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 76

Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, IKE got a KEY_ADD msg for SA: SPI = 0x1ba0c55c

IPSEC: New embryonic SA created @ 0x75298588,
SCB: 0x75C34F18,

Direction: inbound

SPI : 0x03FC9DB7

Session ID: 0x00004000

VPIF num : 0x00000002

Tunnel type: l2l

Protocol : esp

Lifetime : 240 seconds

IPSEC: Completed host IBSA update, SPI 0x03FC9DB7
IPSEC: Creating inbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000006
SA : 0x75298588
SPI : 0x03FC9DB7
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F614
SCB : 0x0B4707C7
Channel: 0x6ef0a5c0
IPSEC: Completed inbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x00011f6c
IPSEC: Updating outbound VPN context 0x0000F614, SPI 0x1BA0C55C
Flags: 0x00000005
SA : 0x6f0e03f0
SPI : 0x1BA0C55C
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00011F6C
SCB : 0x0B47D387
Channel: 0x6ef0a5c0
IPSEC: Completed outbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0000f614
IPSEC: Completed outbound inner rule, SPI 0x1BA0C55C
Rule ID: 0x74e1c558
IPSEC: Completed outbound outer SPD rule, SPI 0x1BA0C55C
Rule ID: 0x6f0dec80
IPSEC: New inbound tunnel flow rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x03FC9DB7
Rule ID: 0x74e1b4a0
IPSEC: New inbound decrypt rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x03FC9DB7

```
Rule ID: 0x6f0de830
IPSEC: New inbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x03FC9DB7
Rule ID: 0x6f0de8d8
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Pitcher:
received KEY_UPDATE, spi 0x3fc9db7
Feb 13 23:48:56 [IKEv1 DEBUG]Group = 192.168.1.1, IP = 192.168.1.1, Starting
P2 rekey timer: 24480 seconds.
Feb 13 23:48:56 [IKEv1]Group = 192.168.1.1, IP = 192.168.1.1, PHASE 2
COMPLETED (msgid=4c073b21)
```

ASA 8.3及更低版本

輸入以下debug命令可判斷通道失敗的位置：

- debug crypto isakmp 127 (第1階段)
- debug crypto ipsec 127 (第2階段)

以下是偵錯輸出的完整範例：

```
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Oakley proposal is acceptable
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 02 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal ver 03 VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received NAT-Traversal RFC VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Fragmentation VID
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE Peer included IKE fragmentation
capability flags: Main Mode: True Aggressive Mode: True
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing IKE SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, IKE SA Proposal # 1, Transform # 1
acceptable Matches global IKE entry # 1
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ISAKMP SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Traversal VID ver
02 payload
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Fragmentation VID +
```

extended capabilities payload

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 132

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ke payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing ISA_KE payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing nonce payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Cisco Unity client VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received xauth V6 VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, processing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing ke payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing nonce payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing Cisco Unity VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing xauth V6 VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send IOS VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, constructing NAT-Discovery payload

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, computing NAT Discovery hash

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating keys for Responder...

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + NONE (0) total length : 304

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing ID payload

Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, ID_IPV4_ADDR ID received 172.16.1.1

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing hash payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Computing hash for ISAKMP

Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Processing IOS keep alive payload: proposal=32767/32767 sec.

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing VID payload

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Received DPD VID

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Connection landed on tunnel_group 172.16.1.1

Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,

constructing ID payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
Computing hash for ISAKMP
Feb 13 04:19:53 [IKEv1 DEBUG]: IP = 172.16.1.1, Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
constructing dpd vid payload
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) + NONE (0)
total length : 96
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 1 COMPLETED
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, Keep-alive type for this connection: DPD
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P1
rekey timer: 82080 seconds.
Feb 13 04:19:53 [IKEv1 DECODE]: IP = 172.16.1.1, IKE Responder starting QM: msg id =
4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NOTIFY (11) + NONE (0) total length : 200
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.2.2.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received remote IP
Proxy Subnet data in ID Payload: Address 10.2.2.0, Mask 255.255.255.0,
Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1,
processing ID payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Received local IP
Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
notify payload
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, QM IsRekeyed old sa
not found by addr
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map
check, checking map = outside_map, seq = 20...
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Static Crypto Map
check, map outside_map, seq = 20 is a successful match**
**Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Remote Peer
configured for crypto map: outside_map**
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
IPSec SA payload
**Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IPSec SA
Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20**
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0xAB5C63A8,
SCB: 0xABD54E98,
Direction: inbound
SPI : 0x1BA0C55C
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp

Lifetime : 240 seconds
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got SPI
from key engine: SPI = 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, oakley
constucting quick mode
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
blank hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec SA payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
IPSec nonce payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
proxy ID
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Transmitting
Proxy Id:
Remote subnet: 10.2.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, constructing
qm hash payload
Feb 13 04:19:53 [IKEv1 DECODE]: Group = 172.16.1.1, IP = 172.16.1.1, IKE Responder
sending 2nd QM pkt: msg id = 4c073b21
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE SENDING Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) +
ID (5) + NONE (0) total length : 172
Feb 13 04:19:53 [IKEv1]: IP = 172.16.1.1, IKE_DECODE RECEIVED Message
(msgid=4c073b21) with payloads : HDR + HASH (8) + NONE (0) total length : 52
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, processing
hash payload
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, loading all
IPSEC SAs
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt
rule look up for crypto map outside_map 20 matching ACL 100: returned
cs_id=ab9302f0; rule=ab9309b0
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Generating
Quick Mode Key!
IPSEC: New embryonic SA created @ 0xAB570B58,
SCB: 0xABD55378,
Direction: outbound
SPI : 0x03FC9DB7
Session ID: 0x00004000
VPIF num : 0x00000001
Tunnel type: l2l
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x03FC9DB7
IPSEC: Creating outbound VPN context, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: New outbound encrypt rule, SPI 0x03FC9DB7
Src addr: 10.1.1.0
Src mask: 255.255.255.0
Dst addr: 10.2.2.0
Dst mask: 255.255.255.0
Src ports

Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x03FC9DB7
Rule ID: 0xABD557B0
IPSEC: New outbound permit rule, SPI 0x03FC9DB7
Src addr: 192.168.1.1
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x03FC9DB7
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, NP encrypt rule
look up for crypto map outside_map 20 matching ACL 100: returned cs_id=ab9302f0;
rule=ab9309b0
Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, Security negotiation
complete for LAN-to-LAN Group (172.16.1.1) Responder, Inbound SPI = 0x1ba0c55c,
Outbound SPI = 0x03fc9db7
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, IKE got a
KEY_ADD msg for SA: SPI = 0x03fc9db7
IPSEC: Completed host IBSA update, SPI 0x1BA0C55C
IPSEC: Creating inbound VPN context, SPI 0x1BA0C55C
Flags: 0x00000006
SA : 0xAB5C63A8
SPI : 0x1BA0C55C
MTU : 0 bytes
VCID : 0x00000000
Peer : 0x0000F99C
SCB : 0x0150B419
Channel: 0xA7A98400
IPSEC: Completed inbound VPN context, SPI 0x1BA0C55C
VPN handle: 0x0001169C
IPSEC: Updating outbound VPN context 0x0000F99C, SPI 0x03FC9DB7
Flags: 0x00000005
SA : 0xAB570B58
SPI : 0x03FC9DB7
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x0001169C
SCB : 0x01512E71
Channel: 0xA7A98400
IPSEC: Completed outbound VPN context, SPI 0x03FC9DB7
VPN handle: 0x0000F99C
IPSEC: Completed outbound inner rule, SPI 0x03FC9DB7

Rule ID: 0xABD557B0
IPSEC: Completed outbound outer SPD rule, SPI 0x03FC9DB7
Rule ID: 0xABD55848
IPSEC: New inbound tunnel flow rule, SPI 0x1BA0C55C
Src addr: 10.2.2.0
Src mask: 255.255.255.0
Dst addr: 10.1.1.0
Dst mask: 255.255.255.0
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x1BA0C55C
Rule ID: 0xAB8D98A8
IPSEC: New inbound decrypt rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x1BA0C55C
Rule ID: 0xABD55CB0
IPSEC: New inbound permit rule, SPI 0x1BA0C55C
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.1.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x1BA0C55C
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x1BA0C55C
Rule ID: 0xABD55D48
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Pitcher: received
KEY_UPDATE, spi 0x1ba0c55c
Feb 13 04:19:53 [IKEv1 DEBUG]: Group = 172.16.1.1, IP = 172.16.1.1, Starting P2 rekey
timer: 27360 seconds.

Feb 13 04:19:53 [IKEv1]: Group = 172.16.1.1, IP = 172.16.1.1, PHASE 2 COMPLETED
(msgid=4c073b21)

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）。