ASA到ASA動態到靜態IKEv1/IPsec配置示例

目錄

簡介
必要條件
需求
採用元件
設定
網路圖表
ASDM配置
Central-ASA（靜態對等點）
Remote-ASA（動態對等點）
CLI組態
中央ASA（靜態對等點）配置
Remote-ASA（動態對等點）
驗證
中央ASA
Remote-ASA
疑難排解
Remote-ASA（啟動器）
Central-ASA（響應程式）
相關資訊

簡介

本文檔介紹如何使自適應安全裝置(ASA)能夠接受來自任何動態對等體（本例中為ASA）的動態IPsec站點到站點VPN連線。 如本文檔中的網路圖所示，僅當從遠端ASA端發起隧道時，才會建立IPsec隧道。由於動態IPsec配置，Central-ASA無法啟動VPN隧道。Remote-ASA的IP地址未知。

配置Central-ASA以動態接受來自萬用字元IP地址(0.0.0.0/0)和萬用字元預共用金鑰的連線。然後，按照加密訪問清單的指定，將Remote-ASA配置為加密從本地到Central-ASA子網的流量。兩端均執行網路地址轉換(NAT)免除，以繞過IPsec流量的NAT。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco ASA（5510和5520）防火牆軟體版本9.x和更新版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

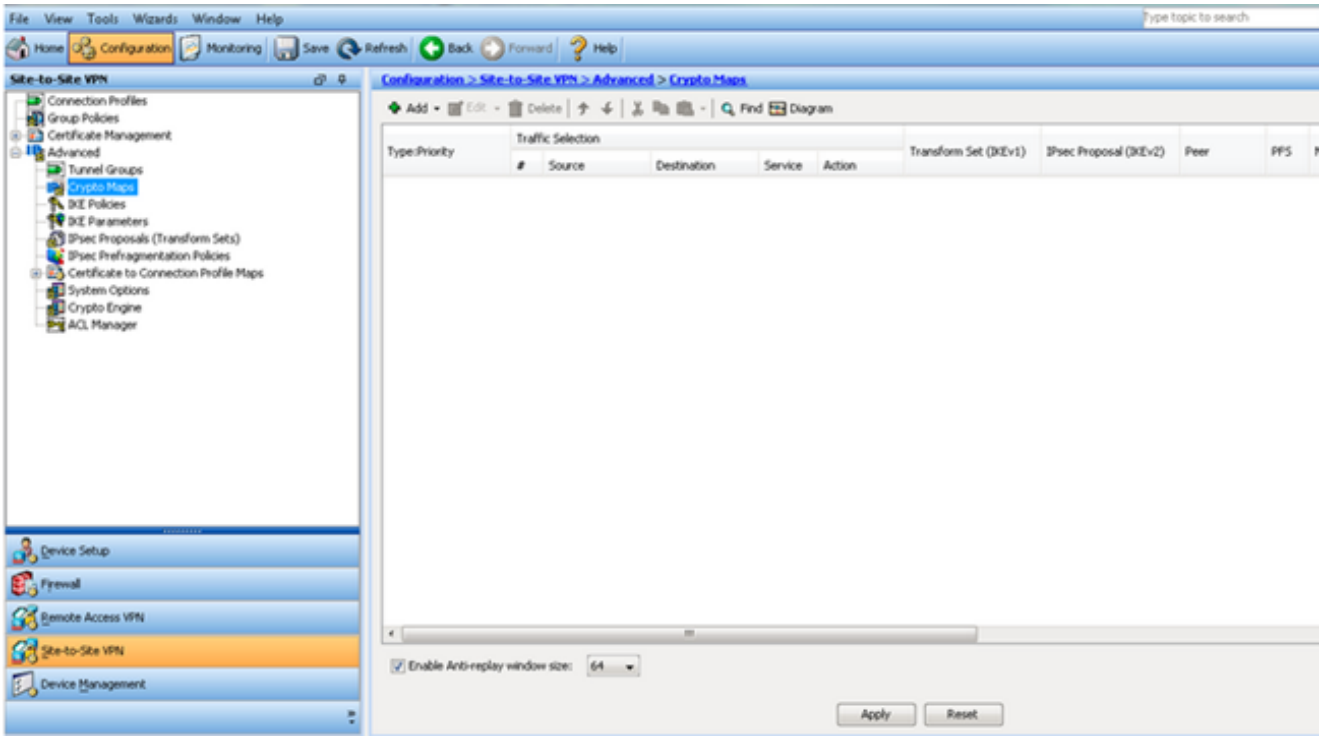
網路圖表

ASDM配置

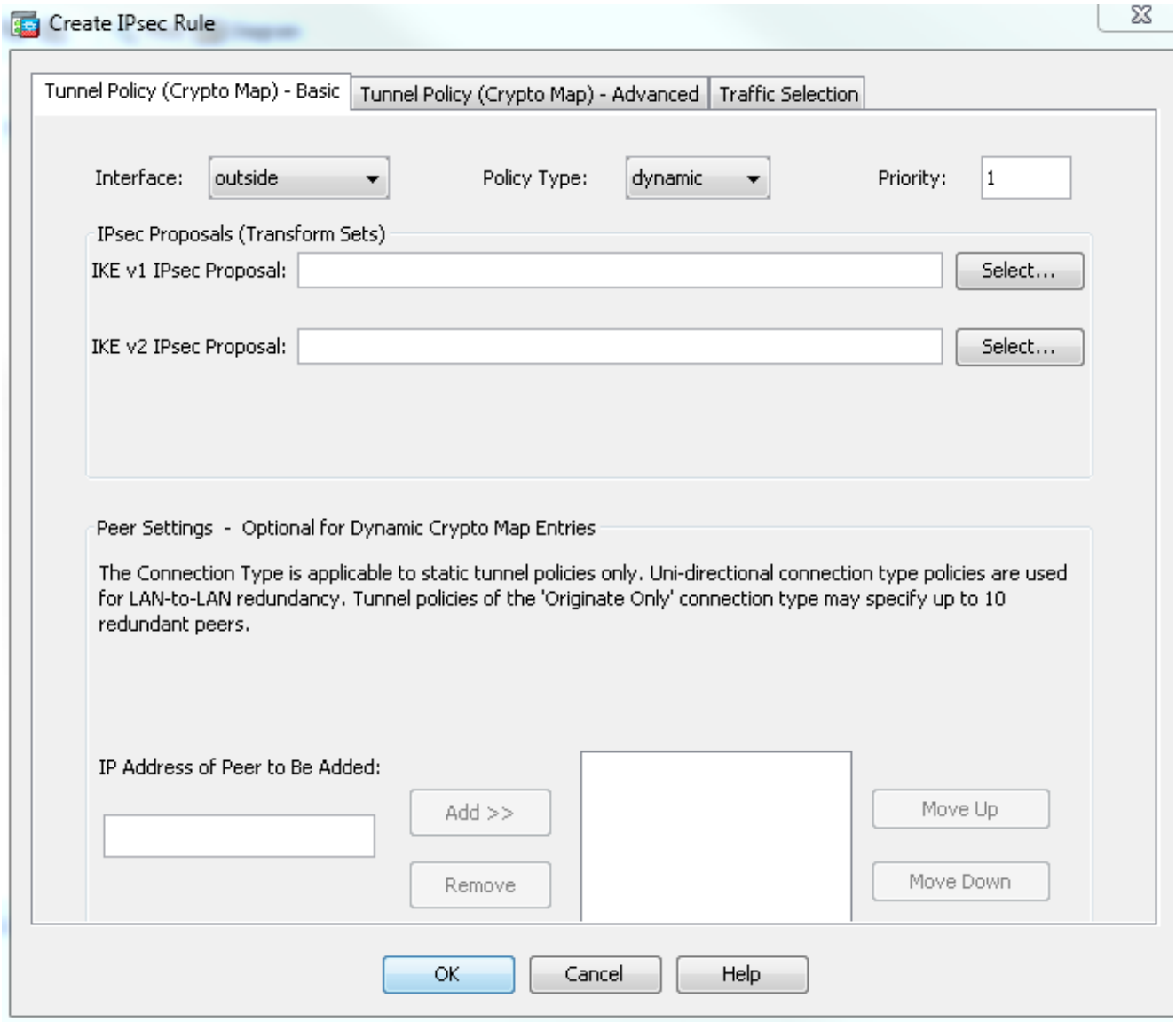
Central-ASA（靜態對等點）

在具有靜態IP地址的ASA上，設定VPN的方式使其接受來自未知對等體的動態連線，同時仍然使用IKEv1預共用金鑰對對等體進行身份驗證：

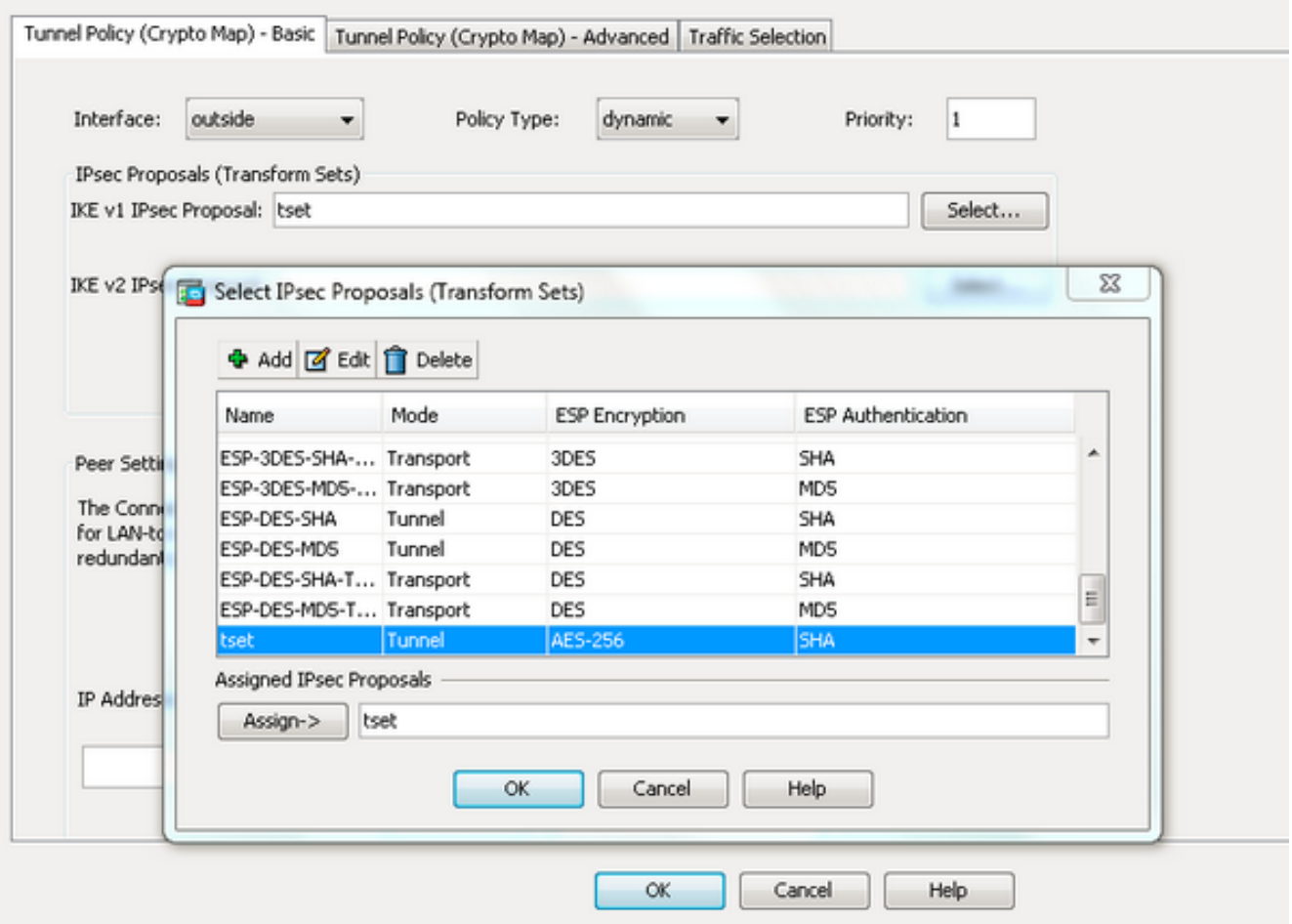
1. 選擇**Configuration > Site-to-Site VPN > Advanced > Crypto Maps**。該視窗顯示已經到位的加密對映條目清單（如果有）。 由於ASA不知道對等IP地址是什麼，為了讓ASA接受連線，請使用匹配的轉換集（IPsec建議）配置**Dynamic-map**。 按一下「**Add**」。



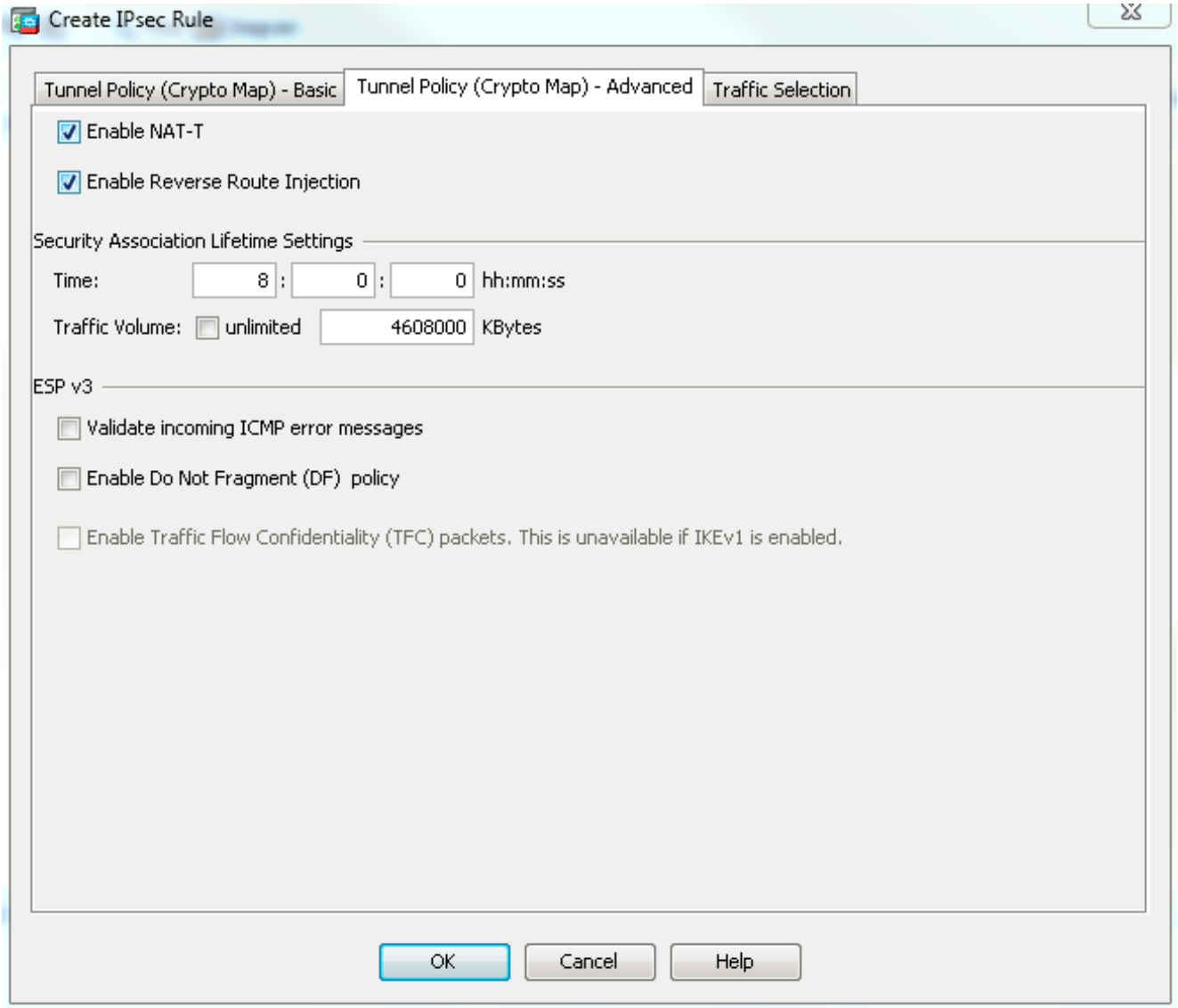
2. 在Create IPsec Rule視窗中，從Tunnel Policy(Crypto Map)- Basic頁籤，從Interface下拉選單中選擇**outside**，從**Policy Type下拉選單中選擇dynamic**。在Priority欄位中，為Dynamic-Map下存在多個條目時為此條目分配優先順序。接下來，點選IKE v1 IPsec Proposal欄位旁邊的**Select**以選擇IPsec proposal。



3. 當「選擇IPsec提議（轉換集）」對話方塊開啟時，從當前IPsec提議中進行選擇，或按一下**Add**以建立一個新提議並使用它。完成後按一下**OK**。



4. 在Tunnel Policy(Crypto Map)-Advanced頁籤中，選中**Enable NAT-T**覈取方塊（如果任一對等體位於NAT裝置後面，則必需）和**Enable Reverse Route Injection**覈取方塊。當動態對等體的VPN隧道啟動時，ASA為指向VPN介面的協商遠端VPN網路安裝動態路由。



或者，也可以從Traffic Selection頁籤為動態對等體定義相關的VPN流量，然後按一下**OK**。

Create IPsec Rule

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Action: Protect Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

Description:

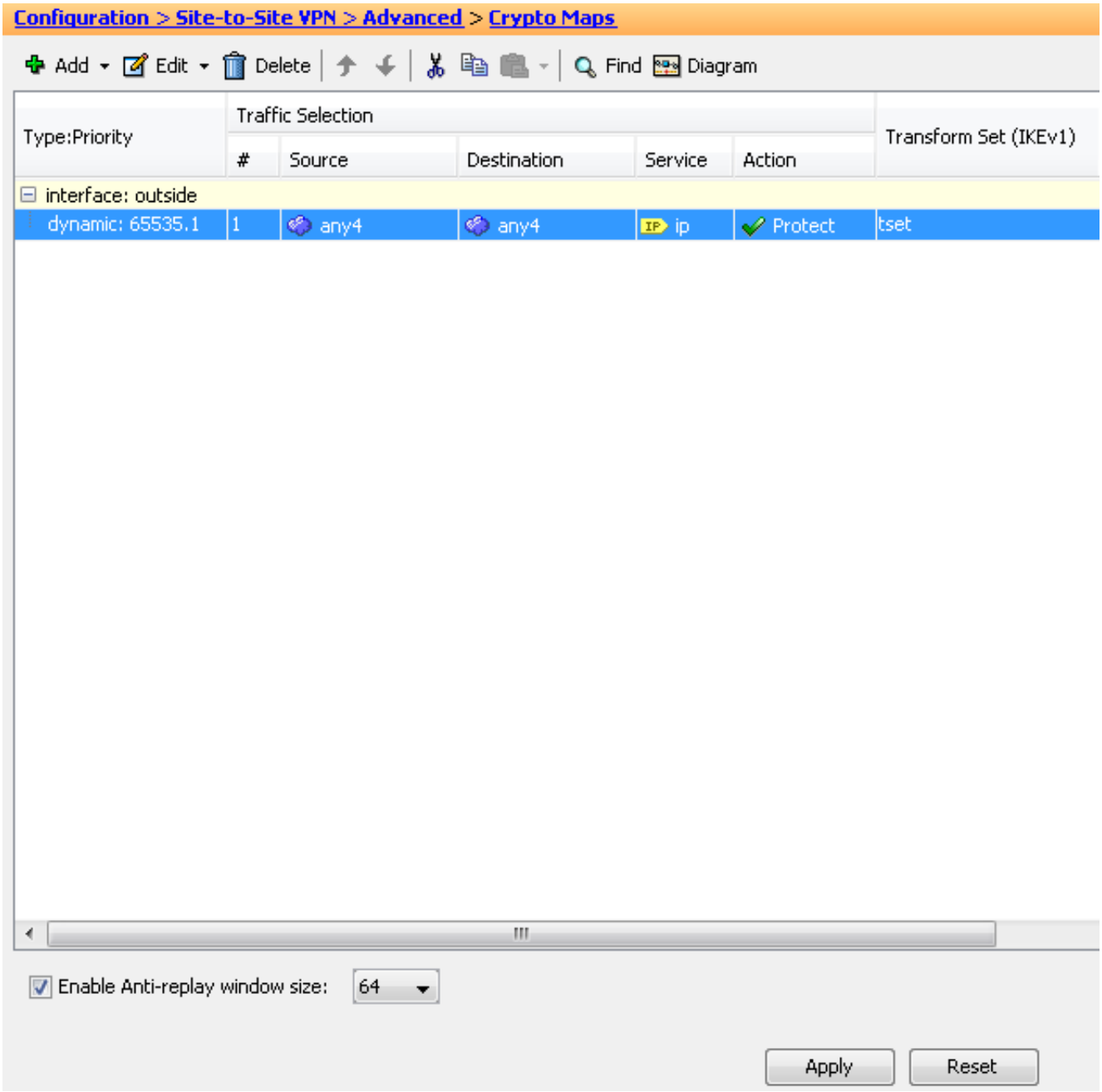
More Options

Enable Rule

Source Service: (TCP or UDP service only)

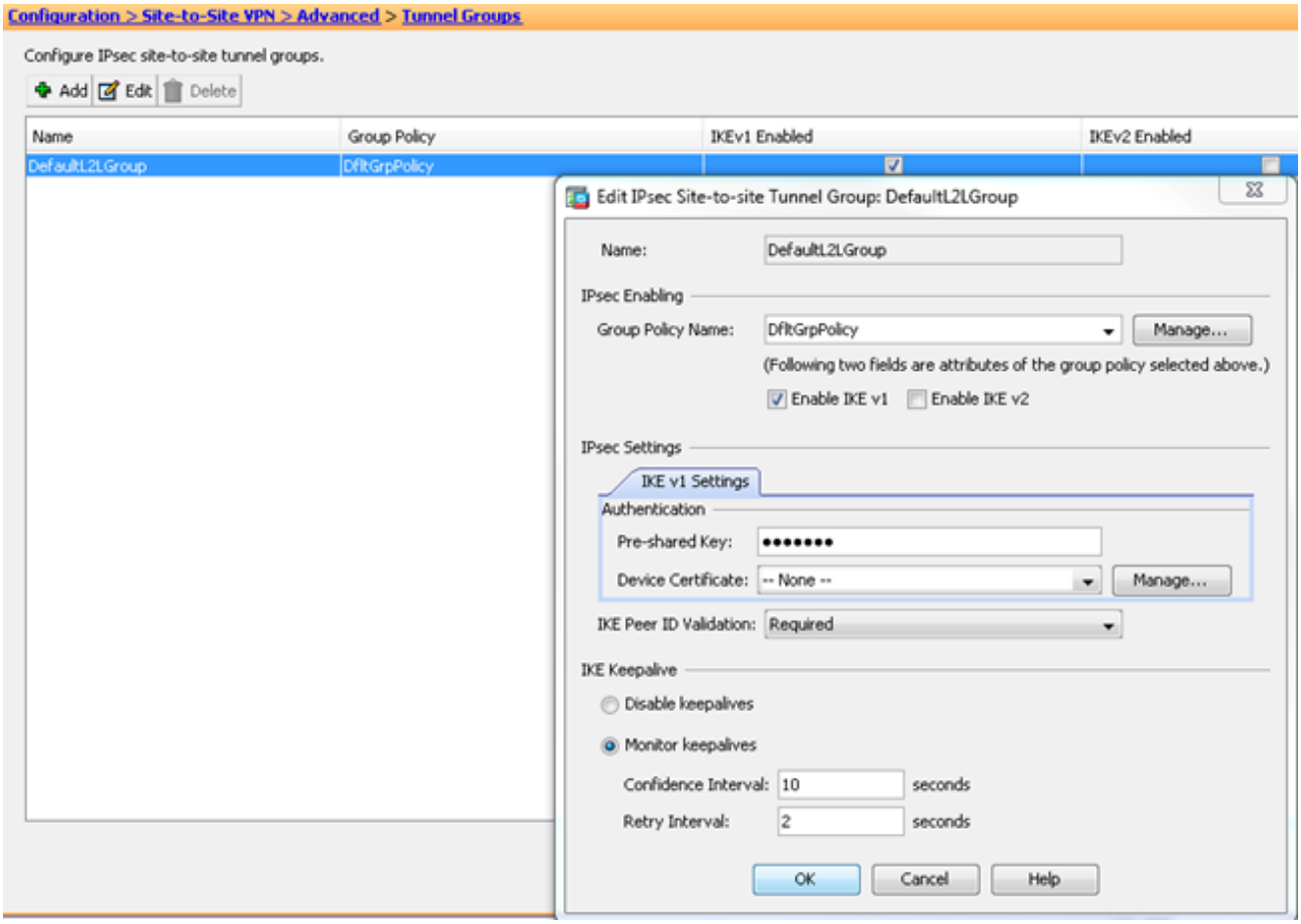
Time Range:

OK Cancel Help



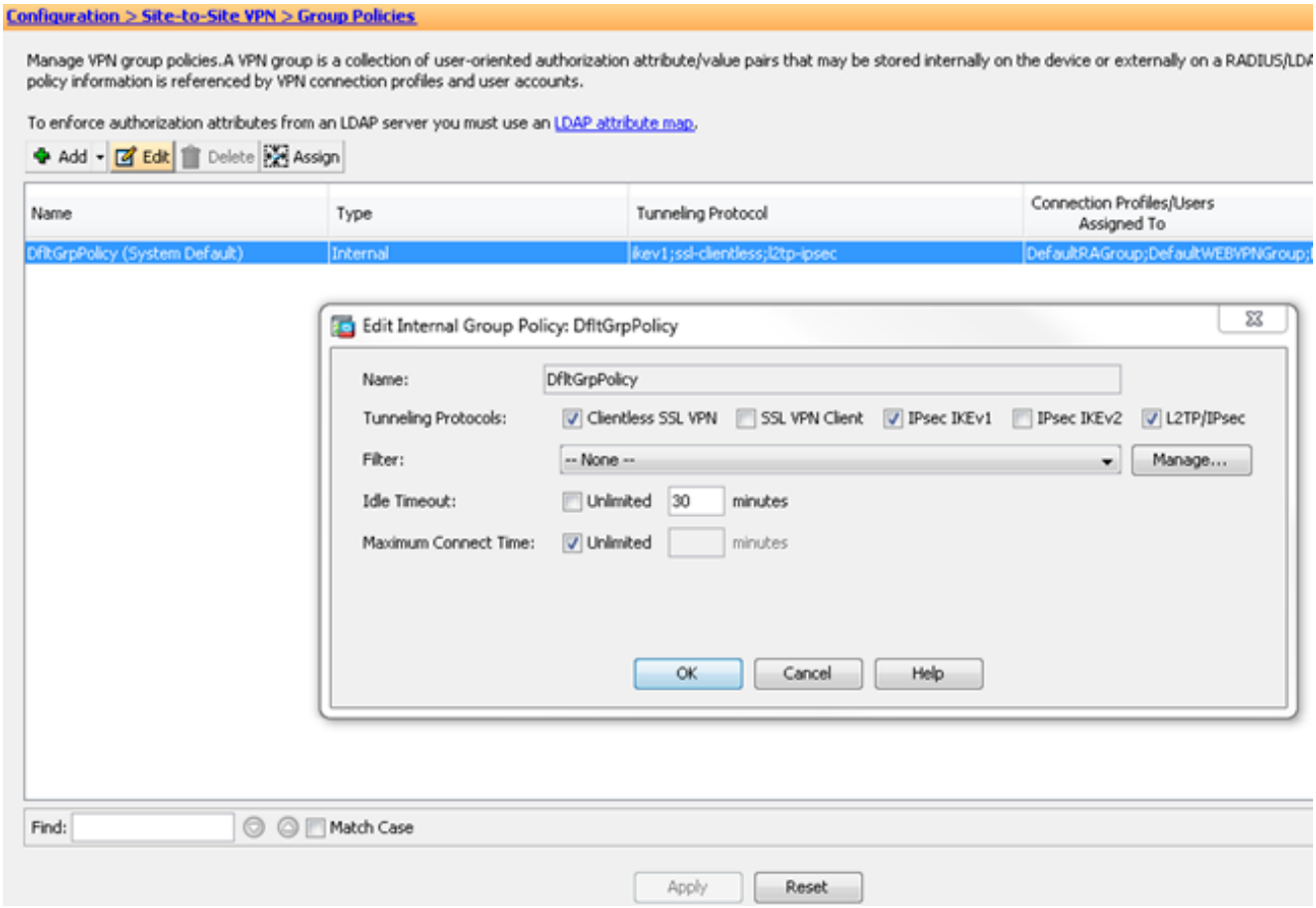
如前所述，由於ASA沒有有關遠端動態對等IP地址的任何資訊，未知連線請求將停留在預設情況下存在於ASA上的DefaultL2LGroup下。為使身份驗證成功，遠端對等體上配置的預共用金鑰（在本示例中為cisco123）需要與DefaultL2LGroup下的金鑰匹配。

5. 選擇**Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**，選擇**DefaultL2LGroup**，按一下**Edit**並配置所需的預共用金鑰。完成後按一下**OK**。

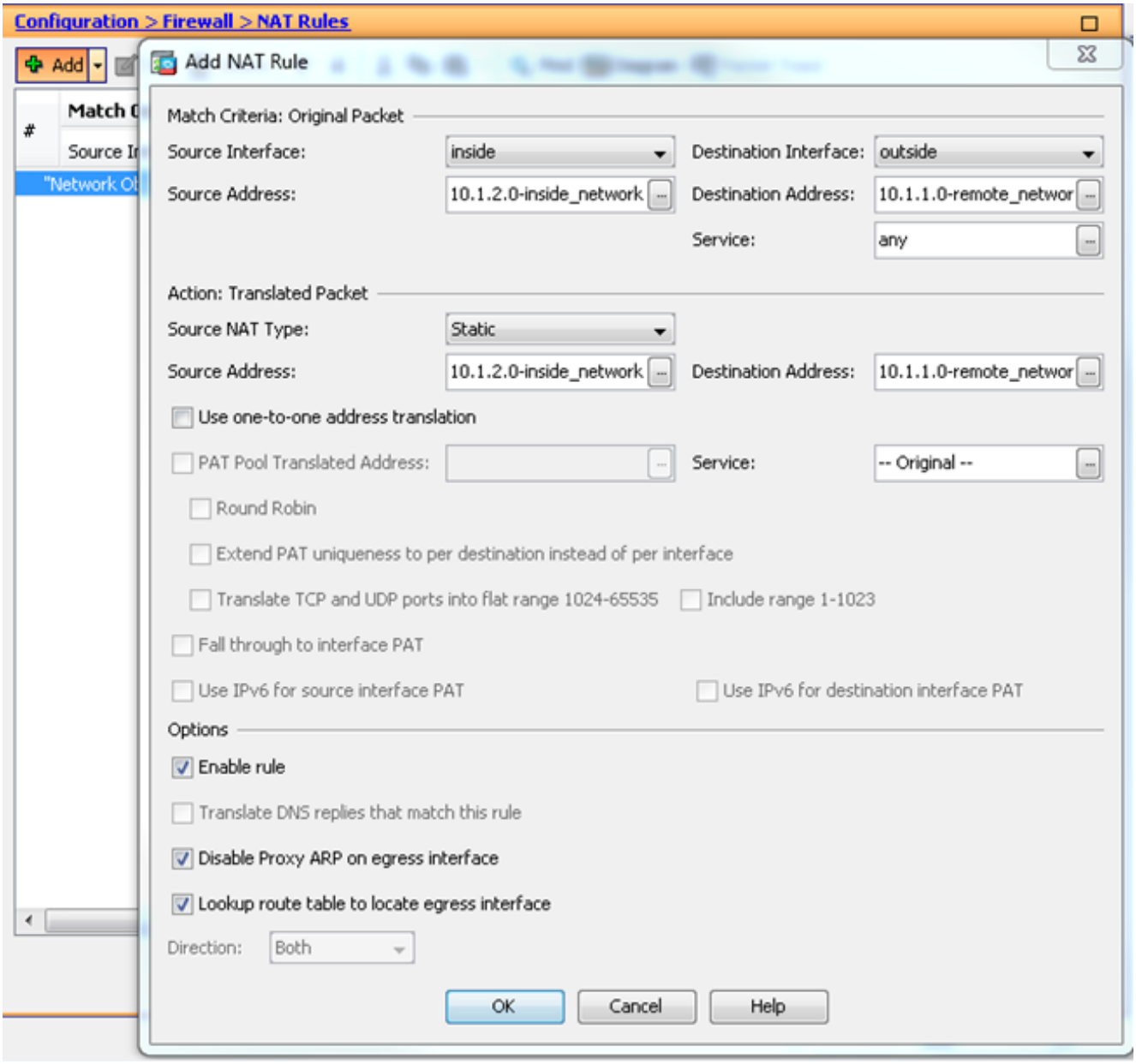


附註：這樣會在靜態對等體(Central-ASA)上建立萬用字元預共用金鑰。 知道此預共用金鑰及其匹配提議的任何裝置/對等體都可以成功建立VPN隧道並通過VPN訪問資源。請確保此預先共用的金鑰不與未知實體共用，並且不容易猜測。

6. 選擇**Configuration > Site-to-Site VPN > Group Policies**，然後選擇您選擇的組策略（本例中為預設組策略）。按一下**Edit**，然後在「編輯內部組策略」對話方塊中編輯組策略。完成後按一下**OK**。

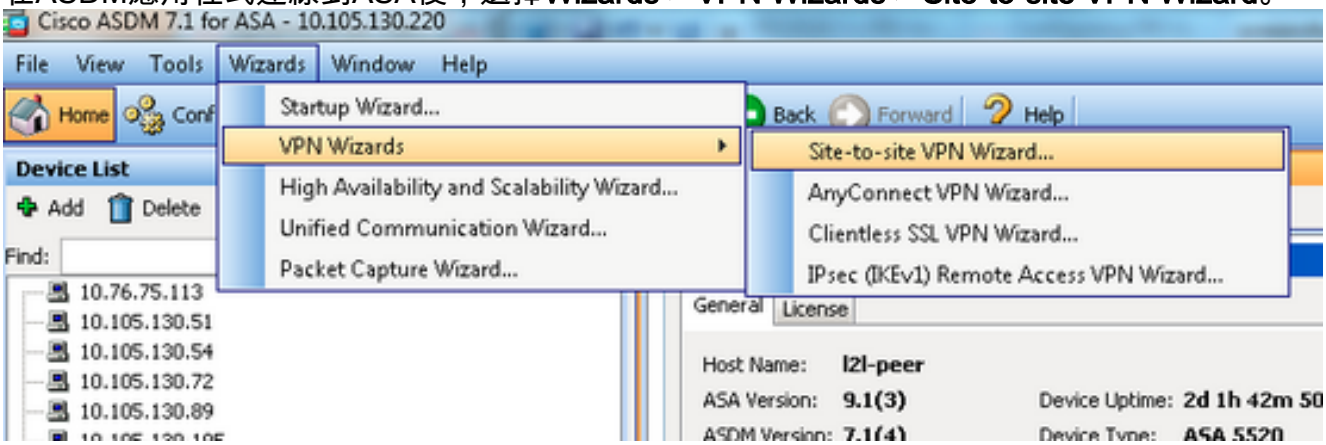


7. 選擇**Configuration > Firewall > NAT Rules**，然後在Add Nat Rule視窗中為VPN流量配置無nat（NAT免除）規則。完成後按一下**OK**。

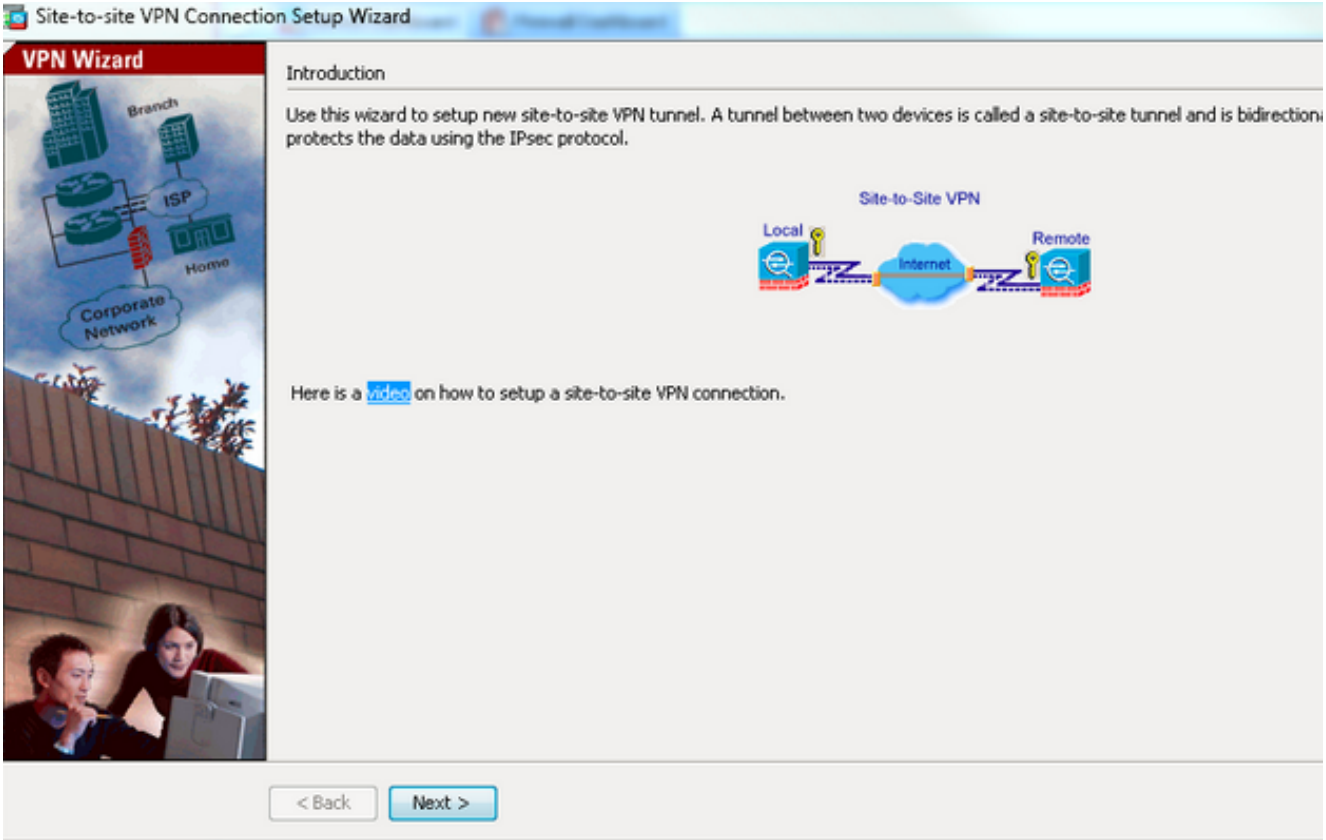


Remote-ASA（動態對等點）

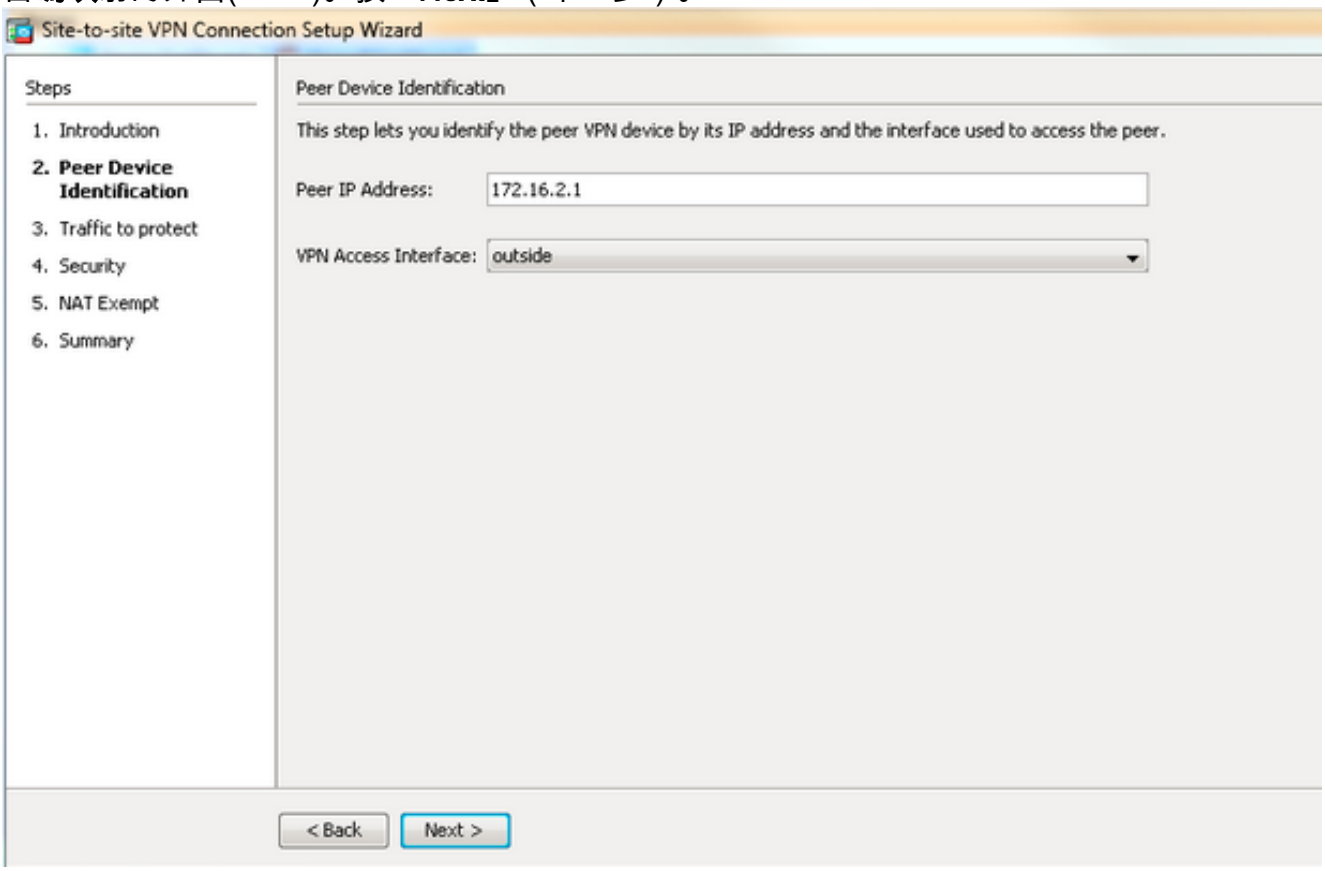
1. 在ASDM應用程式連線到ASA後，選擇**Wizards > VPN Wizards > Site-to-site VPN Wizard**。



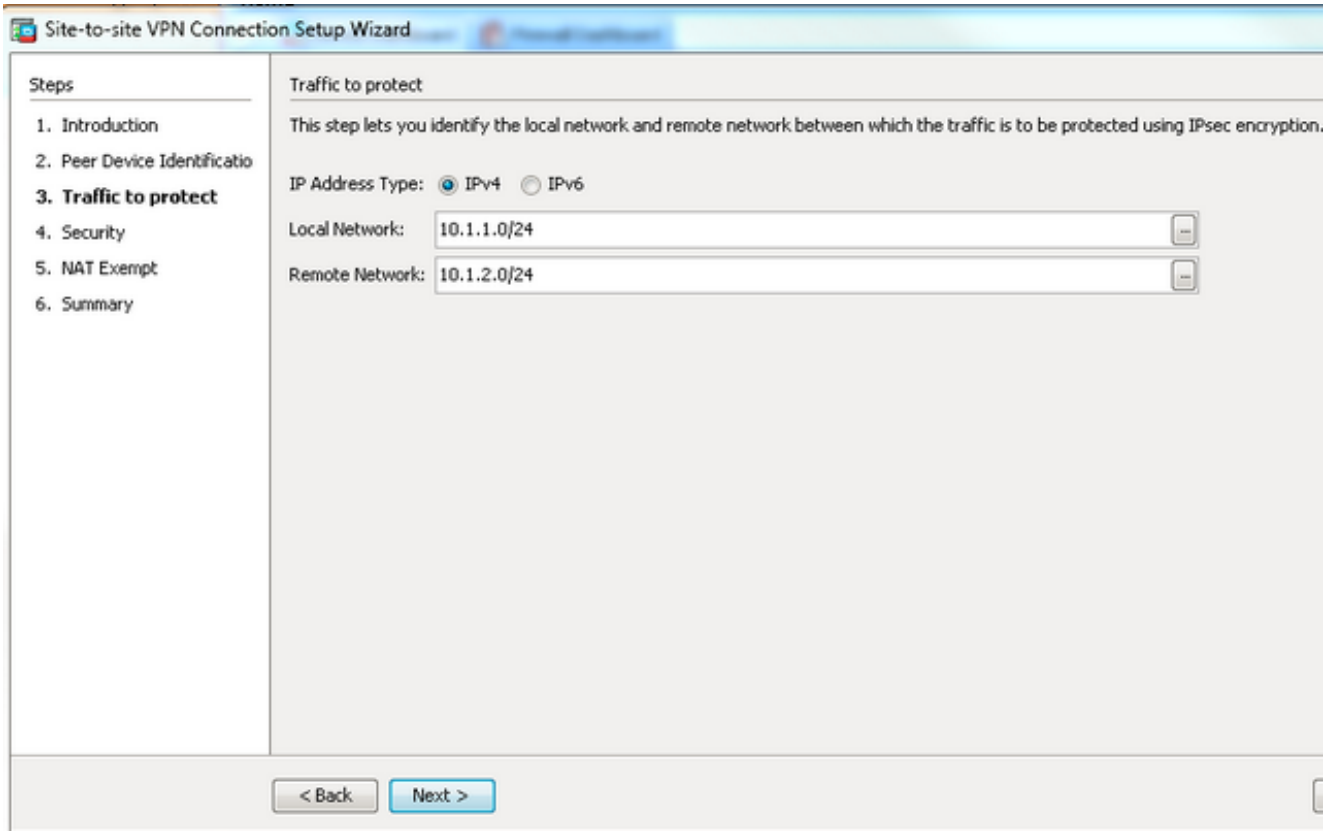
2. 按「**Next**」（下一步）。



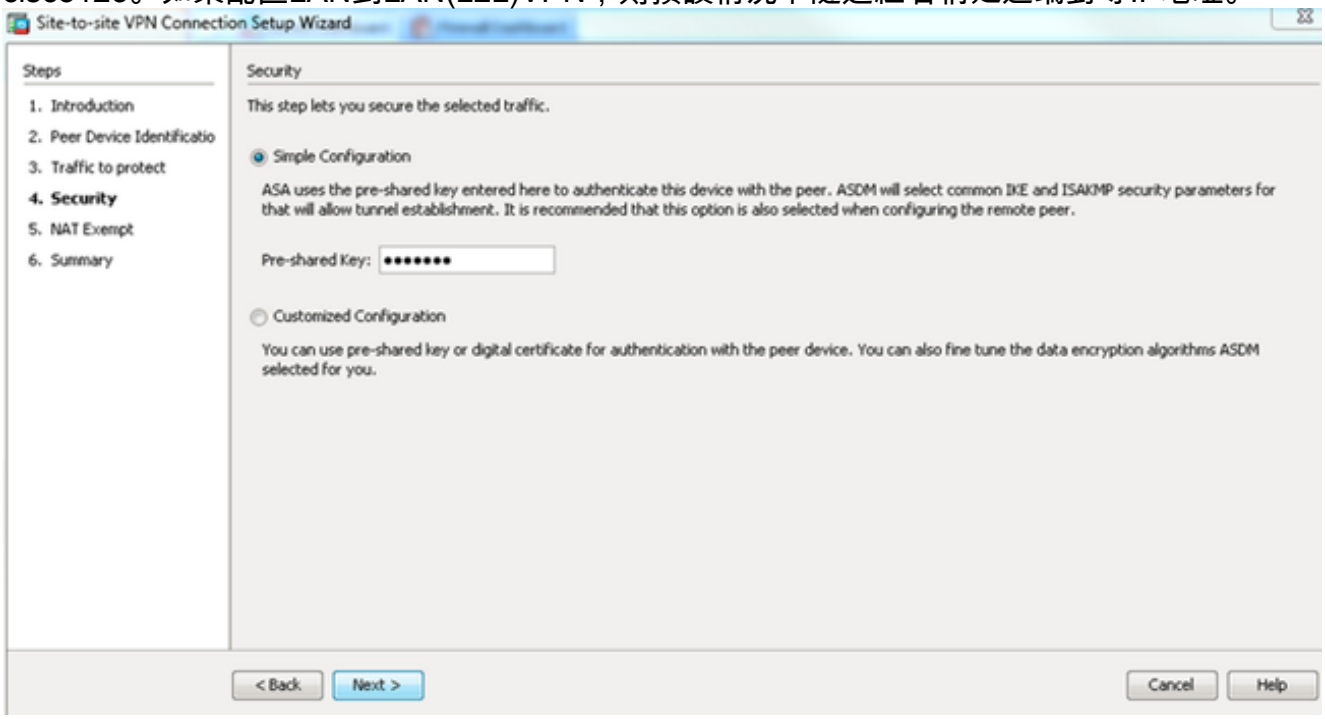
3. 從VPN Access Interface下拉選單中選擇**outside**，以指定遠端對等點的外部IP地址。選擇應用密**碼映**射的介面(WAN)。按「**Next**」（下一步）。



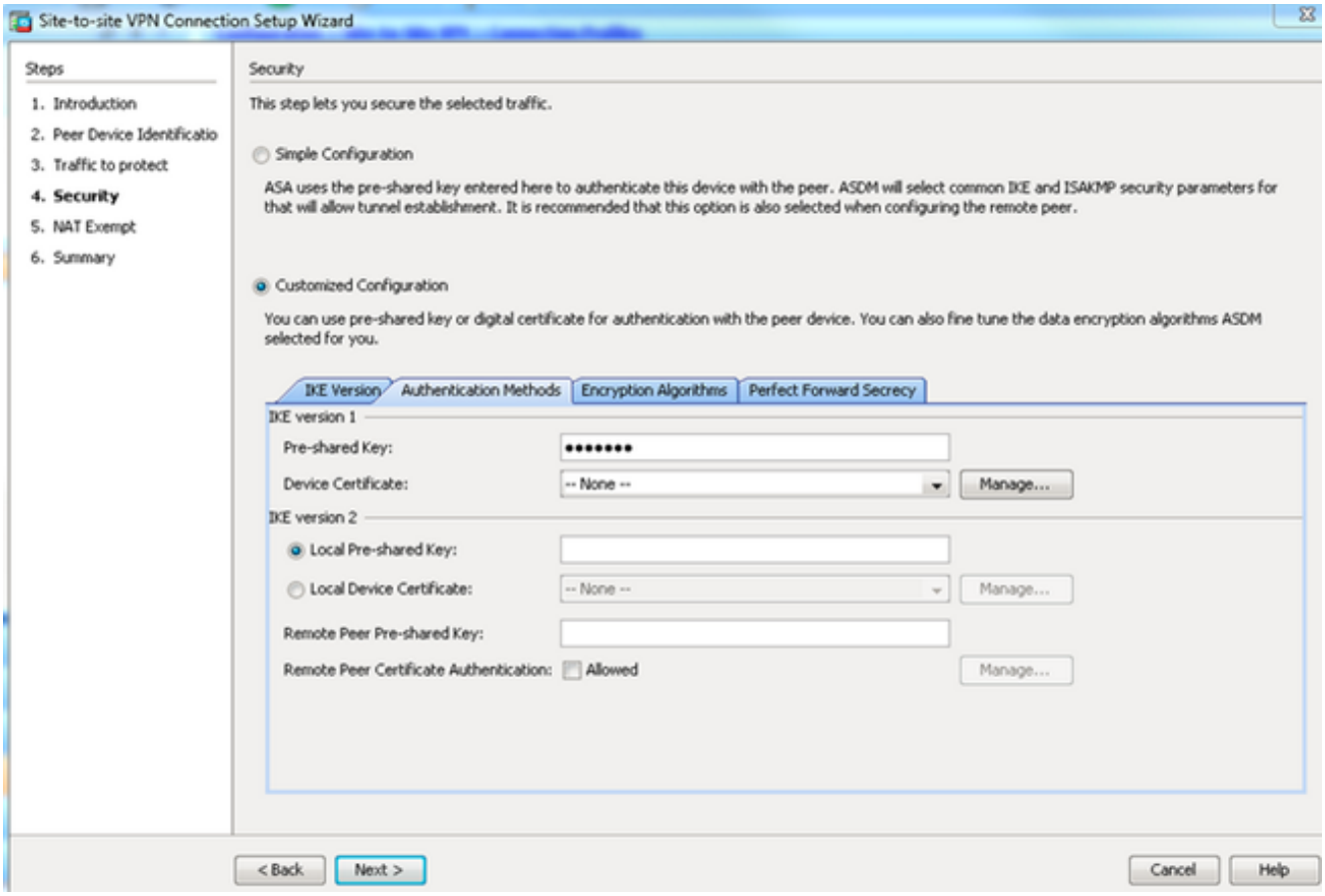
4. 指定應允許通過VPN隧道的主機/網路。在此步驟中，您需要為VPN隧道提供本地網路和遠端網路。點選Local Network和Remote Network欄位旁邊的按鈕，然後根據需要選擇地址。完成後按一下**Next**。



5. 輸入要使用的身份驗證資訊，在本例中為預共用金鑰。本示例中使用的預共用金鑰是cisco123。如果配置LAN到LAN(L2L)VPN，則預設情況下隧道組名稱是遠端對等IP地址。

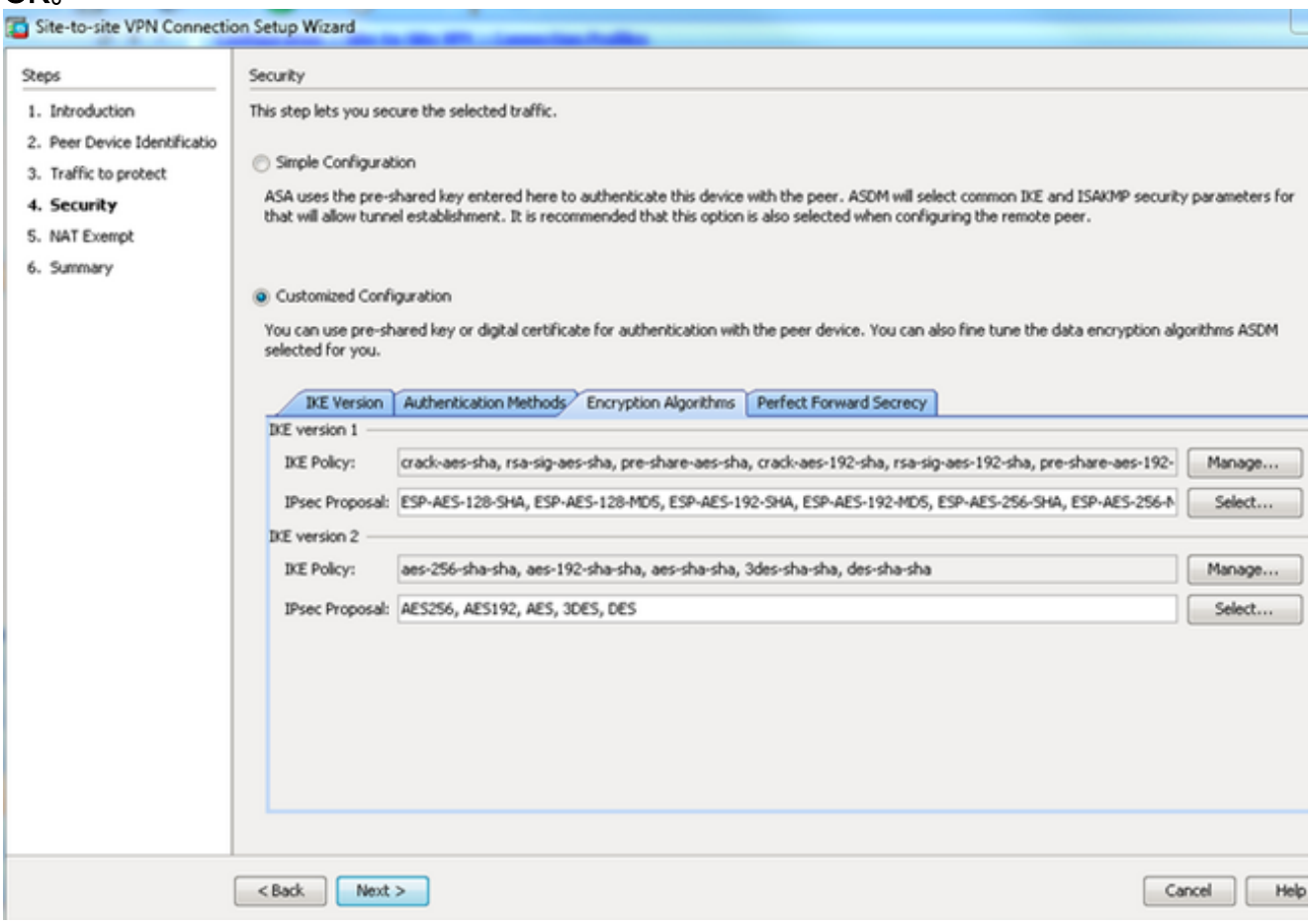


或您可以自定義配置，以包括您選擇的IKE和IPsec策略。對等體之間至少需要一個匹配策略：從Authentication Methods頁籤，在Pre-shared Key欄位中輸入IKE版本1預共用金鑰。在本例中，它是**cisco123**。

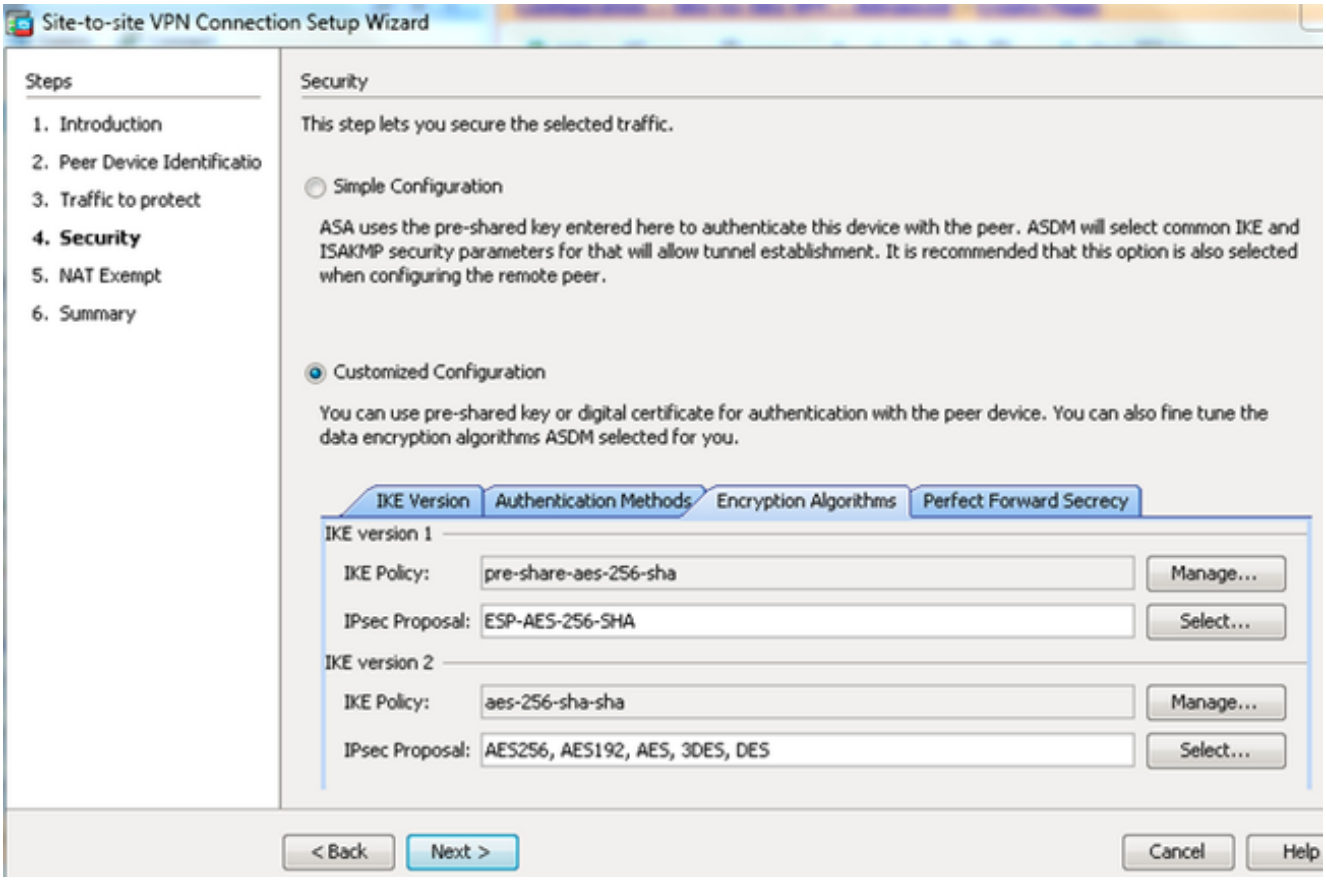


按一下**Encryption Algorithms**頁籤。

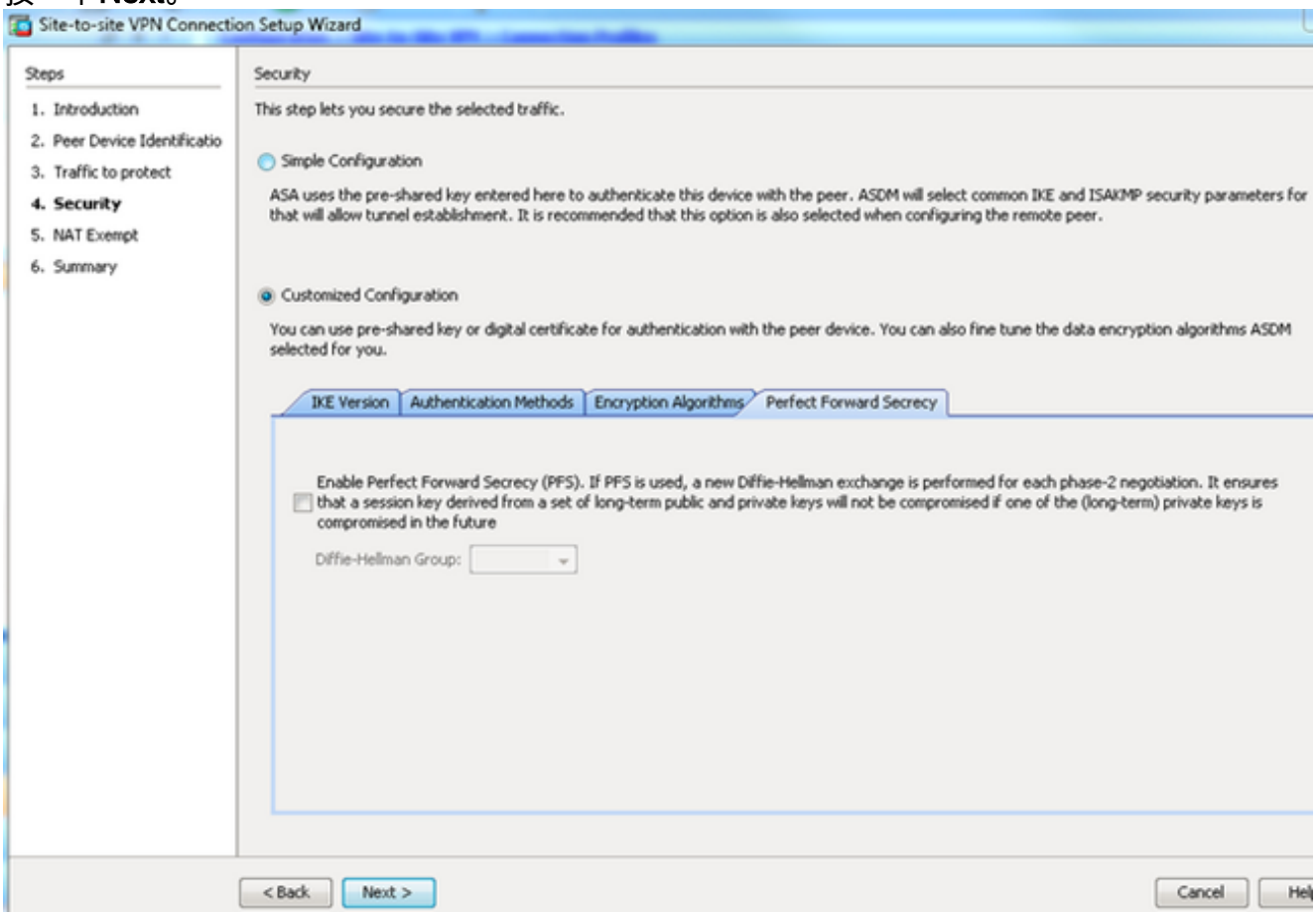
6. 點選IKE Policy欄位旁邊的**Manage**，點選**Add**並配置自定義IKE策略(phase-1)。 完成後按一下**OK**。



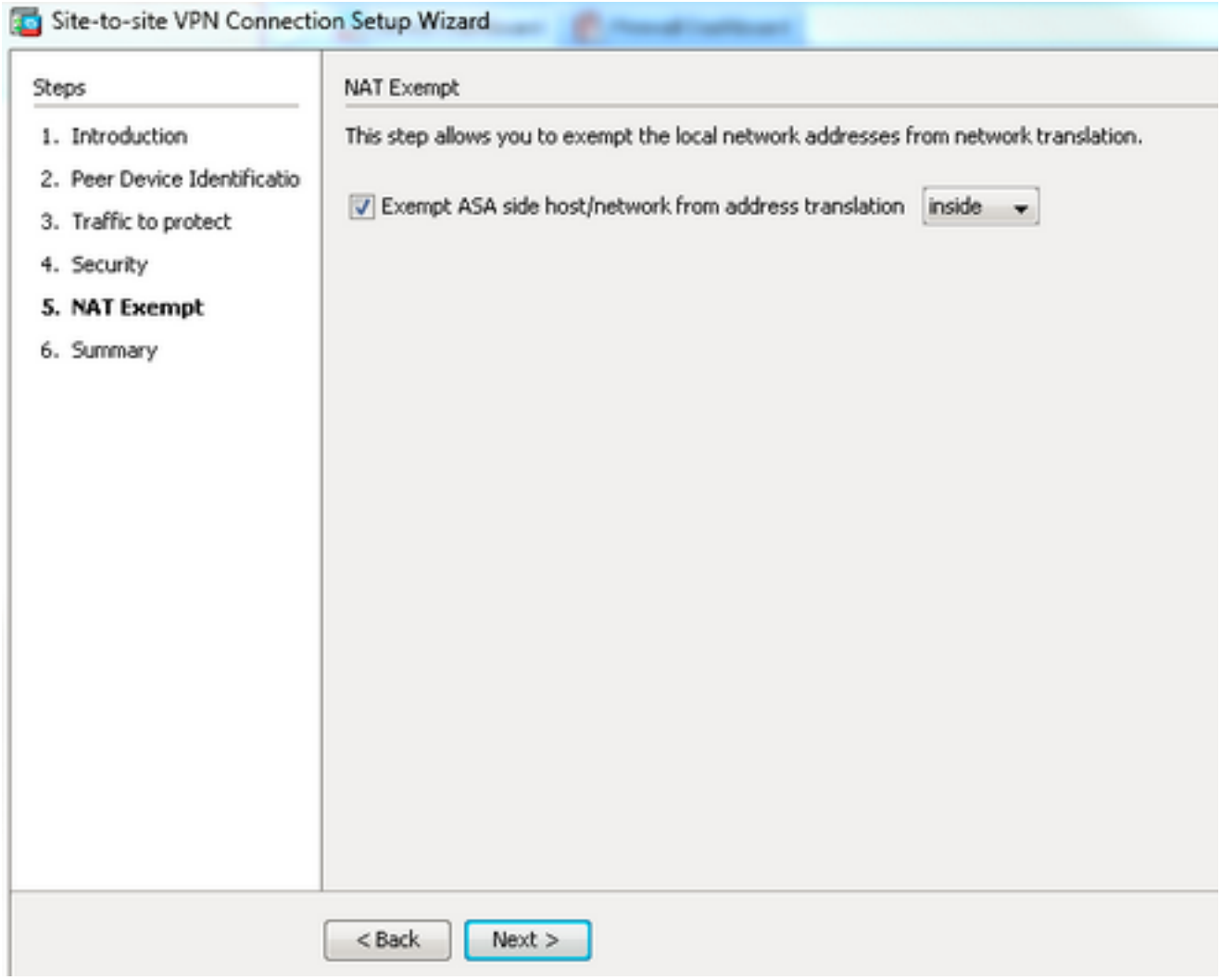
7. 按一下IPsec Proposal（IPsec建議）欄位旁邊的**Select**（選擇），然後選擇所需的IPsec Proposal（IPsec建議）。完成後按一下**Next**。



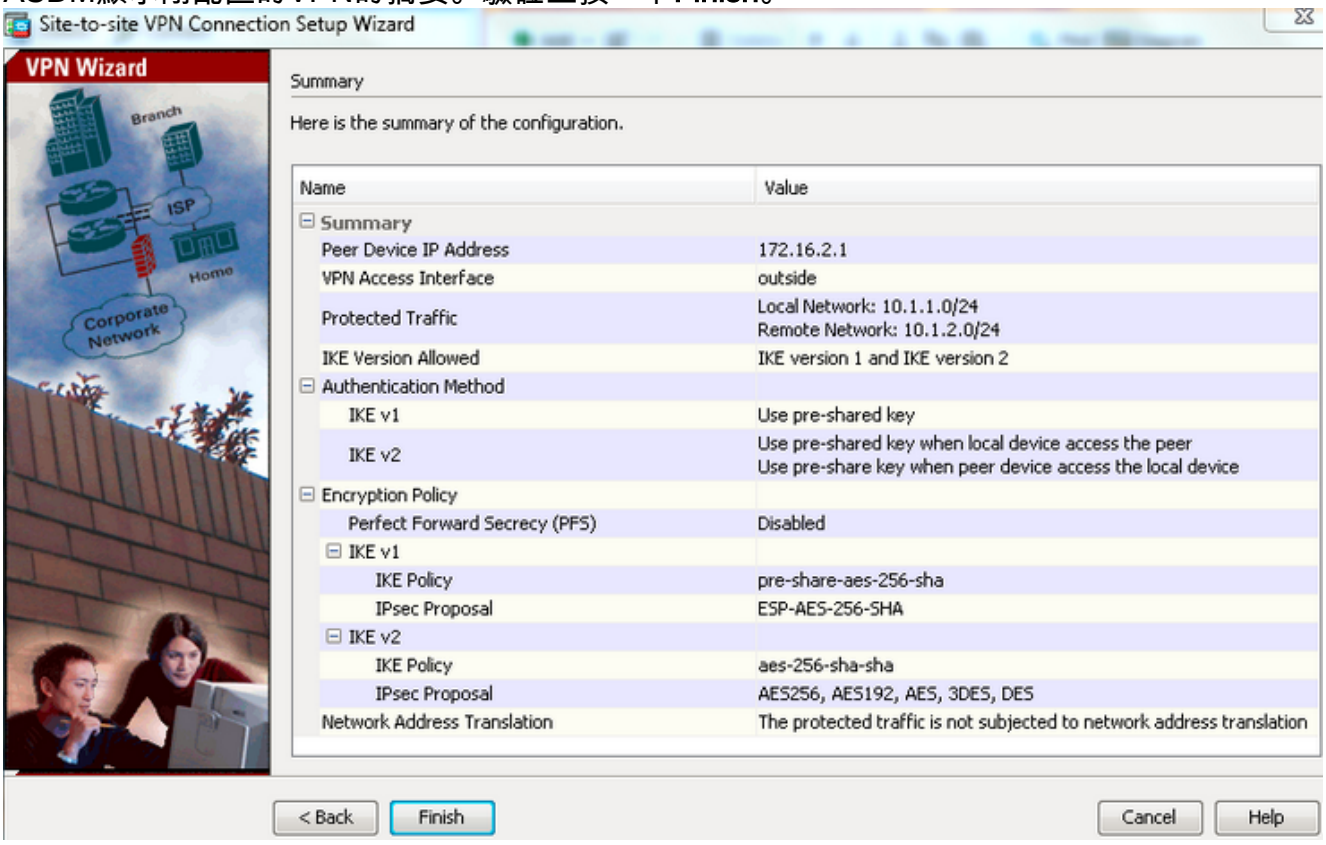
或者，您可以轉至「完全向前保密」頁籤，並選中**啟用完全向前保密**(PFS)覈取方塊。完成後按一下**Next**。



8. 選中**Exempt ASA side host/network from address translation**覈取方塊，以防止隧道流量從網路地址轉換開始。從下拉選單中選擇**local**或inside，以設定可到達本地網路的介面。按「**Next**」（下一步）。



9. ASDM顯示剛配置的VPN的摘要。驗證並按一下**Finish**。



CLI組態

中央ASA（靜態對等點）配置

1. 為VPN流量配置無NAT/NAT豁免規則，如以下示例所示：
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. 在DefaultL2LGroup下配置預共用金鑰，以便驗證任何遠端動態 — L2L對等體：
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. 定義第2階段/ISAKMP策略：
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. 定義第2階段轉換集/IPsec策略：
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. 使用以下引數配置動態對映： 所需的轉換集啟用反向路由注入(RRI)，使安全裝置能夠獲知連線的客戶端的路由資訊（可選）
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```
6. 將動態對映繫結到加密對映，應用加密對映並在外部介面上啟用ISAKMP/IKEv1:
```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

Remote-ASA（動態對等點）

1. 為VPN流量配置NAT免除規則：
```
object network 10.1.1.0-inside_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```
2. 為靜態VPN對等體和預共用金鑰配置隧道組。
```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```
3. 定義PHASE-1/ISAKMP策略：
```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. 定義第2階段轉換集/IPsec策略：
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
5. 配置定義相關VPN流量/網路的訪問清單：
```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```
6. 使用以下引數配置靜態加密對映： Crypto/VPN access-list遠端IPsec對等IP地址所需的轉換集
```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```
7. 應用加密對映並在外部介面上啟用ISAKMP/IKEv1:
```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

驗證

使用本節內容，確認組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE安全關聯(SA)。
- **show crypto ipsec sa** — 顯示所有當前IPsec SA。

本節顯示兩個ASA的驗證輸出示例。

中央ASA

```
Central-ASA#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: 172.16.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1

        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      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: 30D071C0
      current inbound spi : 38DA6E51

      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Remote-ASA

```
Remote-ASA#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: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #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.: 172.16.2.1/0
      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: 38DA6E51
      current inbound spi : 30D071C0

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 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): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 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): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

輸出直譯器工具(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

使用以下命令，如下所示：

```
clear crypto ikev1 sa <peer IP address>
Clears the Phase 1 SA for a specific peer.
```

> **注意**：clear crypto isakmp sa命令在清除所有活動VPN隧道時是入侵性的。

在PIX/ASA軟體版本8.0(3)及更高版本中，可以使用clear crypto isakmp sa *<peer ip address>命令清除單個IKE* SA。在早於8.0(3)的軟體版本中，使用vpn-sessiondb logoff tunnel-group *<tunnel-group-name>*命令可為單一通道清除IKE和IPsec SA。

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
```

```
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs
```

使用的調試：

```
debug cry condition peer <remote peer public IP>
debug cry ikev1 127
debug cry ipsec 127
```

Remote-ASA（啟動器）

輸入以下packet-tracer命令以啟動通道：

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [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=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
```

```
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Central-ASA（響應程式）

```
Jan 20 12:42:35 [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
:
.
Jan 20 12:42:35 [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
Jan 20 12:42:35 [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 (20) + NAT-D (20) + NONE (0) total length : 304
:
```

.
Jan 20 12:42:35 **[IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group DefaultL2LGroup**
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [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 (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [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
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [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
Jan 20 12:42:35 [IKEv1]**Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM**:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, **Received local IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0, Protocol 0, Port 0**Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 **[IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map check, map outside_dyn_map, seq = 1 is a successful match**
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) **Responder, Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Adding static route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0**

相關資訊

- Cisco ASA系列命令參考
- IPsec協商/IKE通訊協定支援頁面
- 要求建議 (RFC)
- 技術支援與檔案 — Cisco System