ASA 8.3及更高版本：具有和不具有IPsec隧道的NTP配置示例

目錄

簡介

本文檔提供使用網路時間協定(NTP)將自適應安全裝置(ASA)時鐘與網路時間伺服器同步的示例配置。ASA1直接與網路時間伺服器通訊。ASA2通過IPsec隧道將NTP流量傳遞到ASA1,ASA1再將該資料包轉發到網路時間伺服器。

請參閱ASA/PIX:NTP with和without an IPsec Tunnel配置示例，適用於版本8.2及更低版本的Cisco ASA上的相同配置。

注意：路由器還可以用作NTP伺服器來同步ASA安全裝置時鐘。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA 8.3及更高版本
- 思科自適應安全裝置管理器(ASDM)版本6.x及更高版本

註：請參閱允許ASDM進行HTTPS訪問，以便允許ASDM配置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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

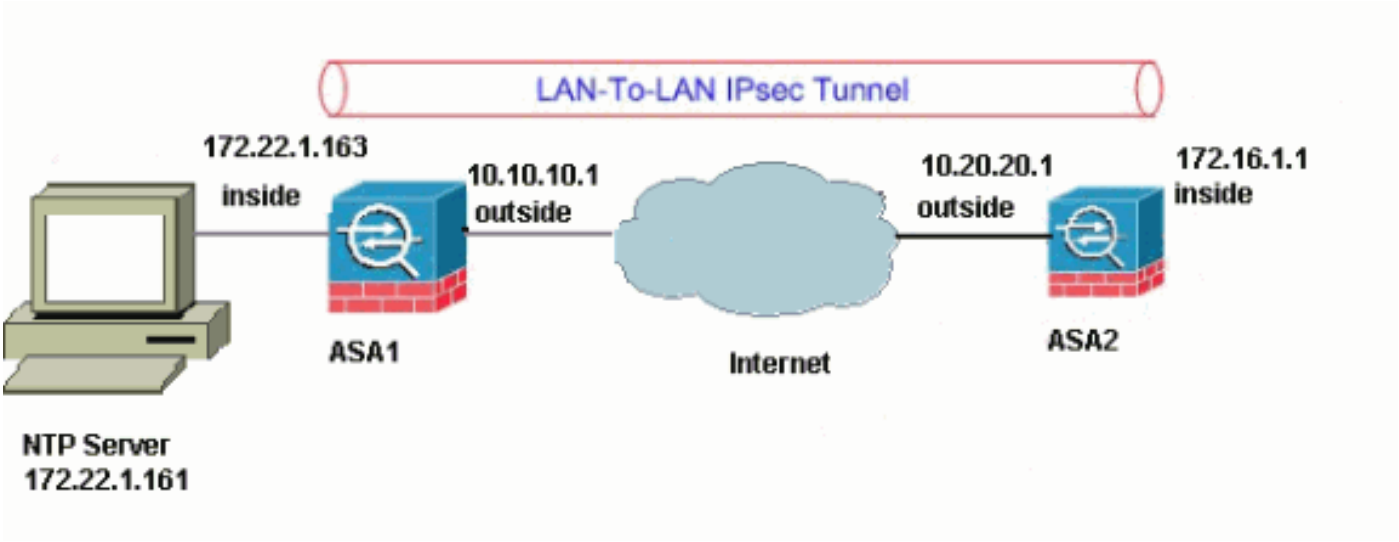
慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

組態

網路圖表

本檔案會使用以下網路設定：



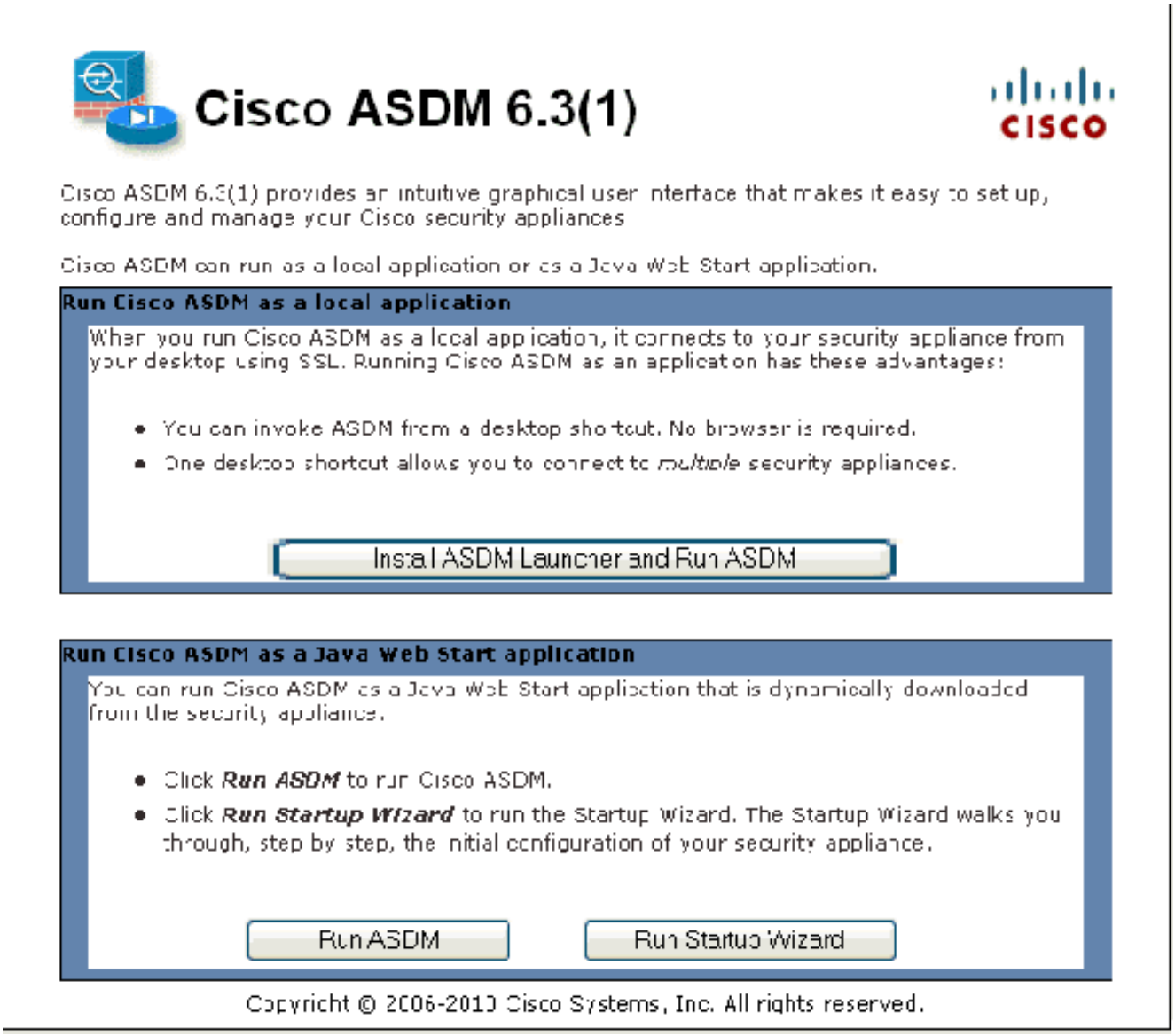
注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918 位址，已在實驗室環境中使用。

- VPN通道ASDM配置
- NTP ASDM配置
- ASA1 CLI配置
- ASA2 CLI配置

VPN通道ASDM配置

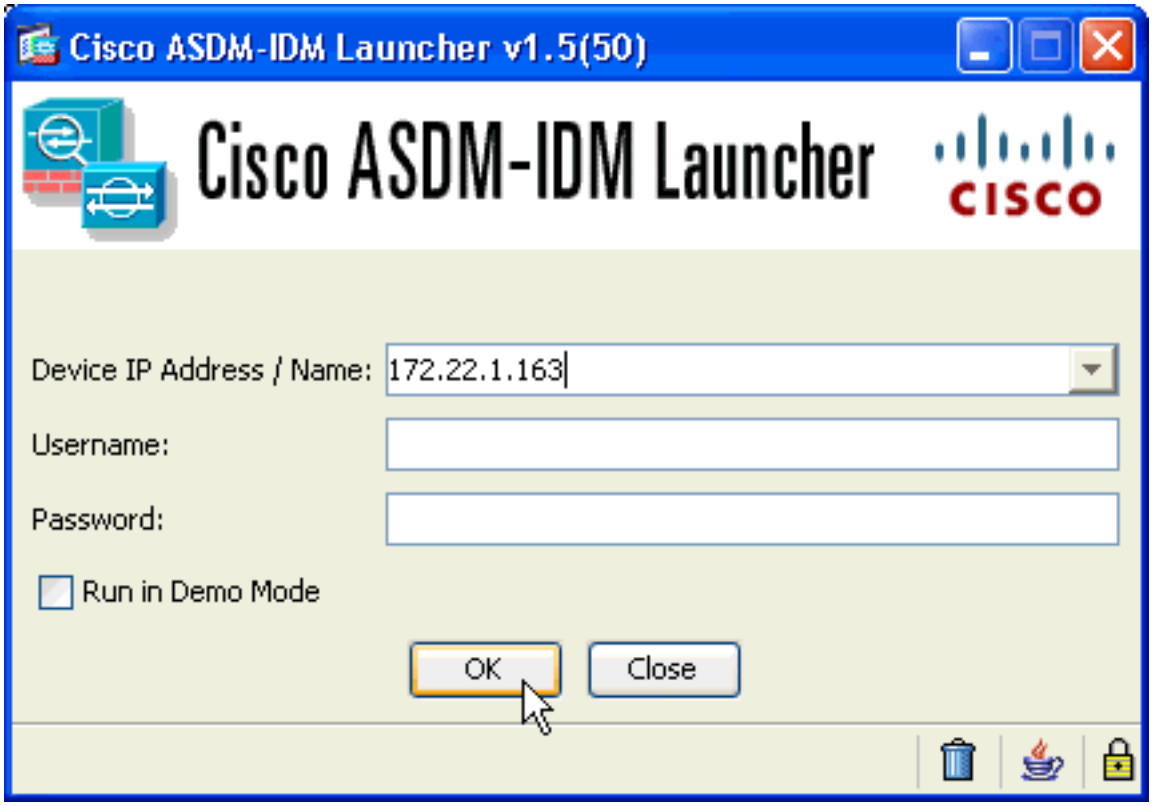
完成以下步驟以建立VPN隧道：

1. 開啟瀏覽器並鍵入**https://<Inside_IP_Address_of_ASA>**，以訪問ASA上的ASDM。請務必授權瀏覽器向您提供的與SSL證書真實性相關的任何警告。預設使用者名稱和密碼均為空。ASA顯示此視窗以允許下載ASDM應用程式。



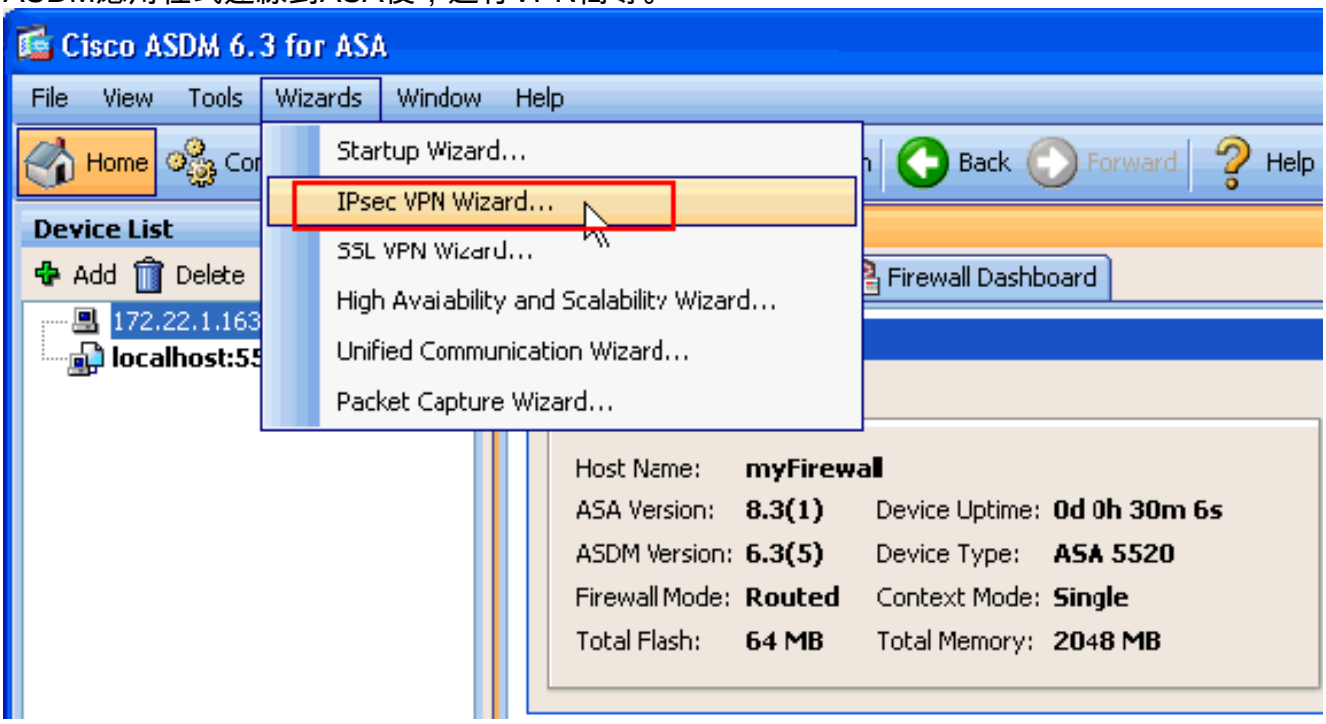
此示例將應用程式載入到本地電腦上，並且不在Java小程式中運行。

2. 按一下**Download ASDM Launcher and Start ASDM**，下載ASDM應用程式的安裝程式。
3. 下載ASDM啟動程式後，請完成提示指導的步驟，以便安裝軟體並運行Cisco ASDM啟動程式。
4. 輸入您使用**http** -命令配置的介面的IP地址，以及使用者名稱和密碼（如果已指定）。此示例使用預設空白使用者名稱和密碼

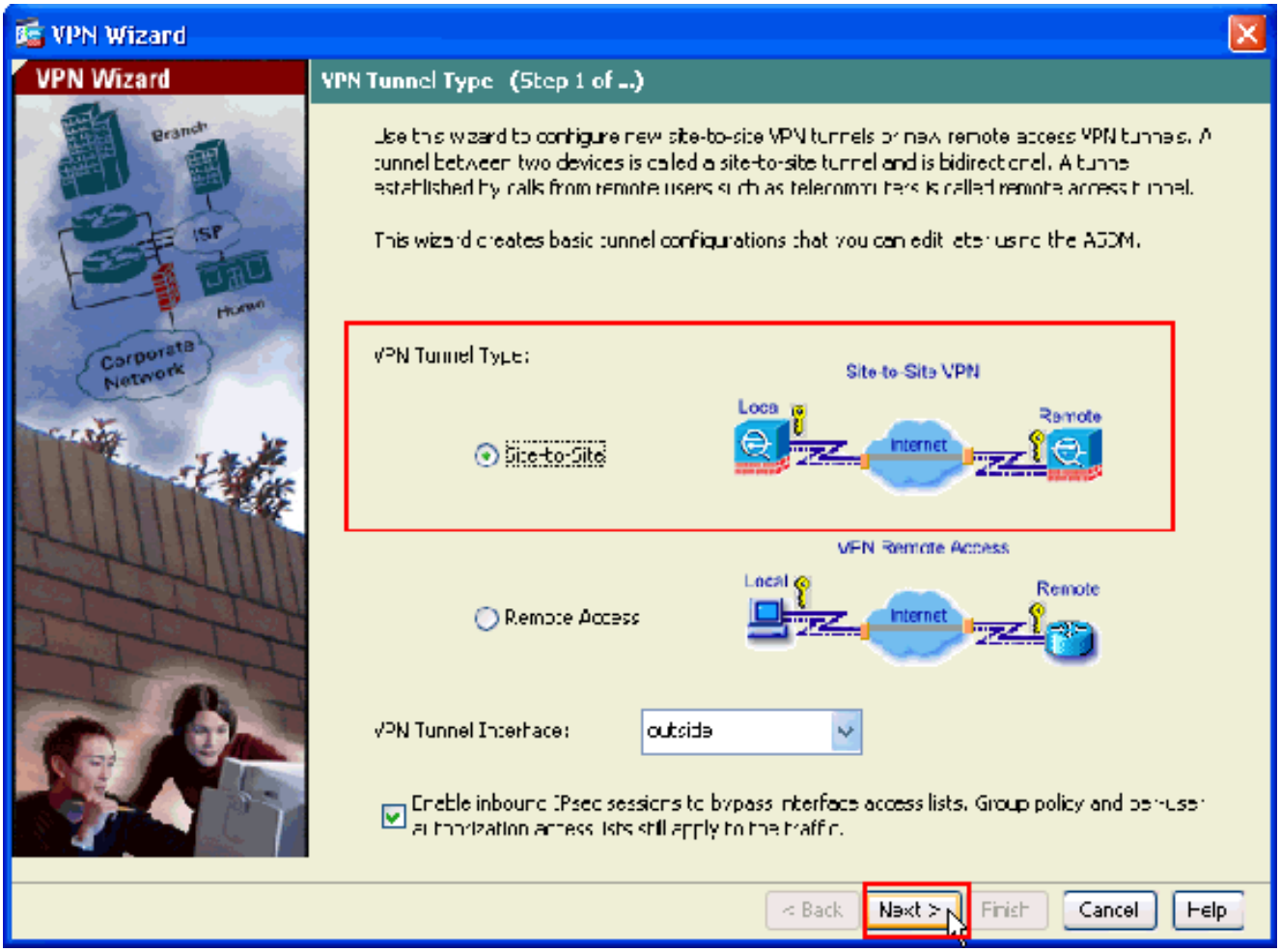


:

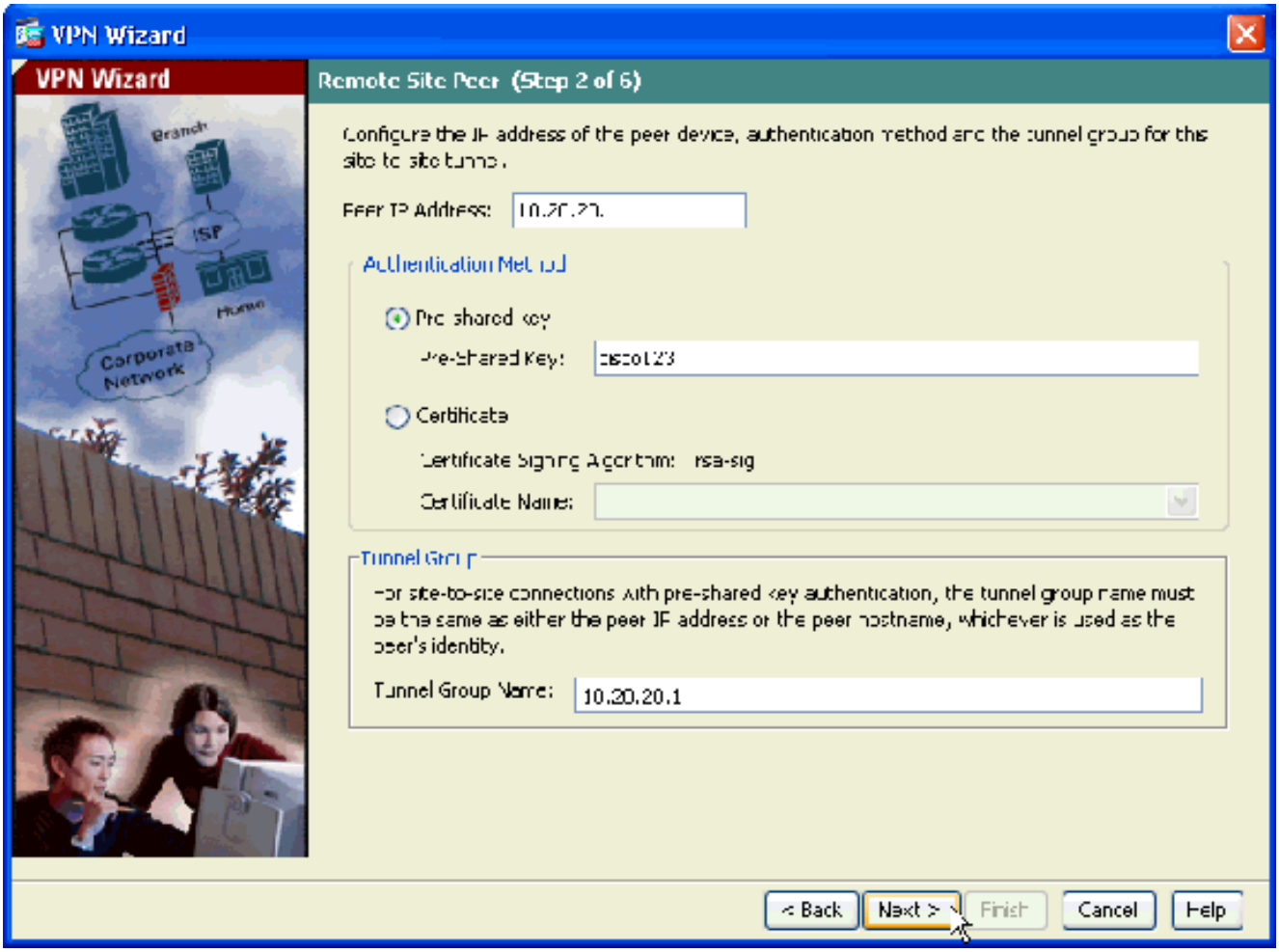
5. ASDM應用程式連線到ASA後，運行VPN嚮導。



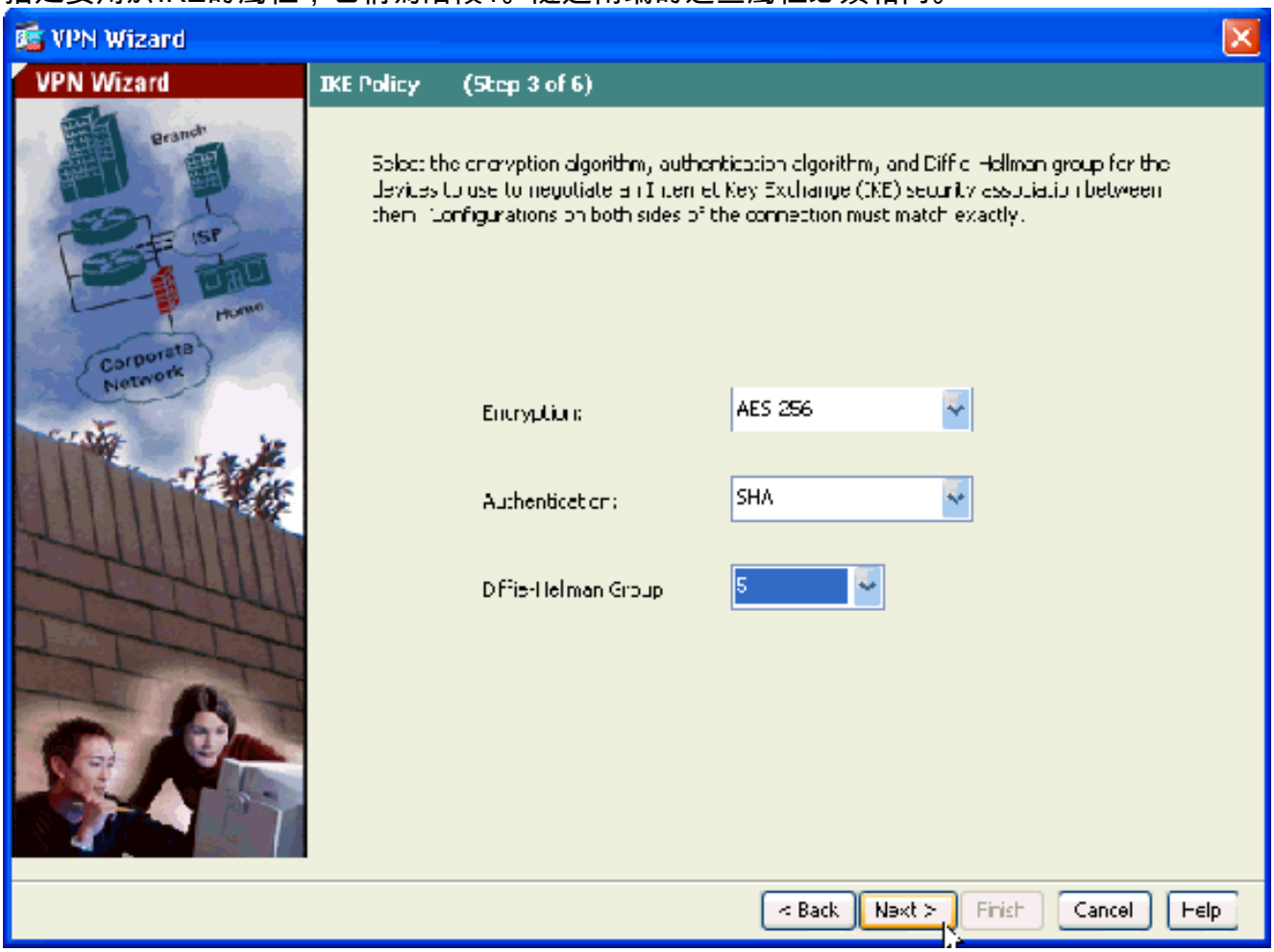
6. 為IPsec VPN隧道型別選擇**Site-to-Site**，然後按一下**Next**。



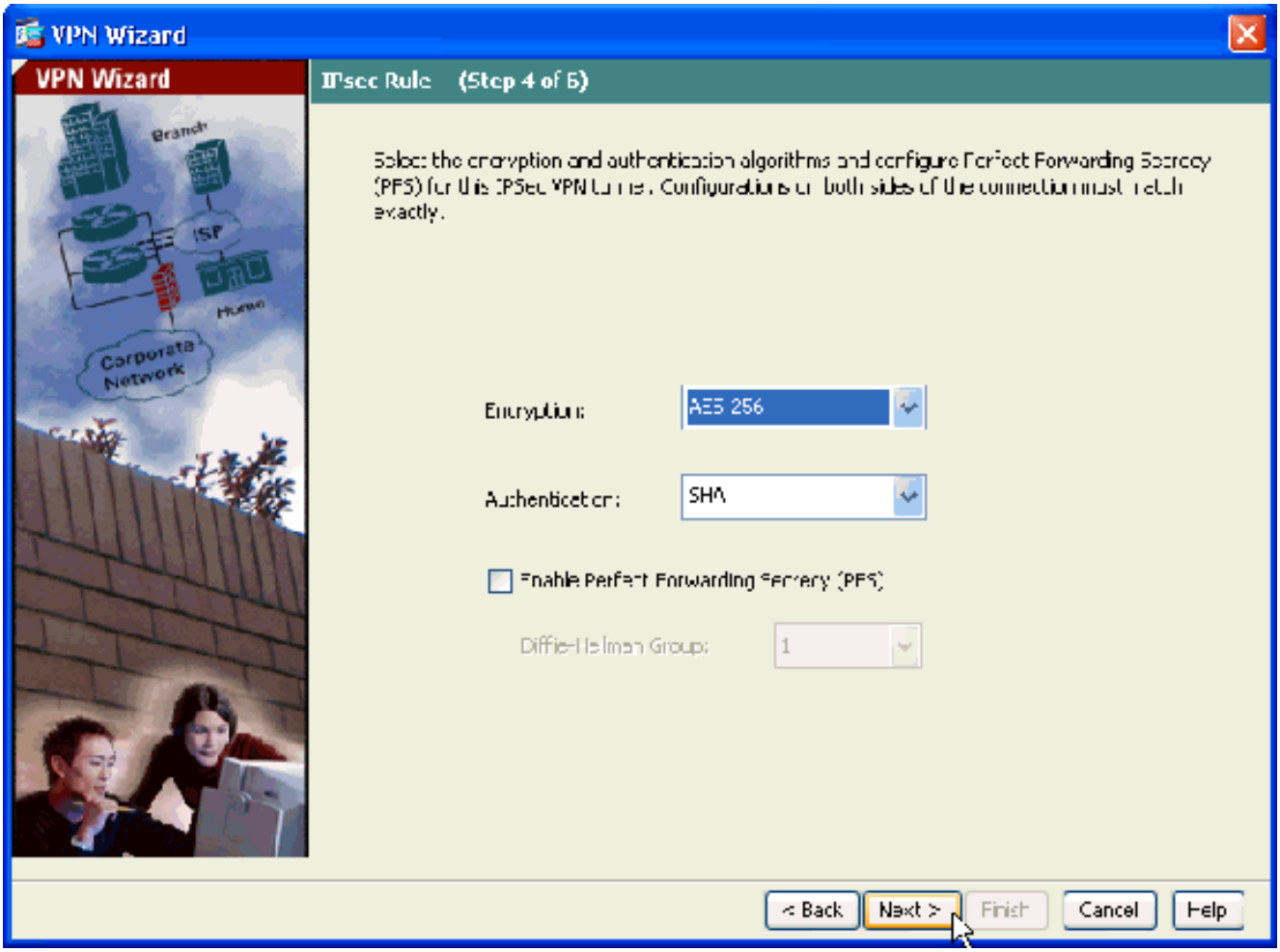
7. 指定遠端對等體的外部IP地址。輸入要使用的身份驗證資訊，即本示例中的預共用金鑰：



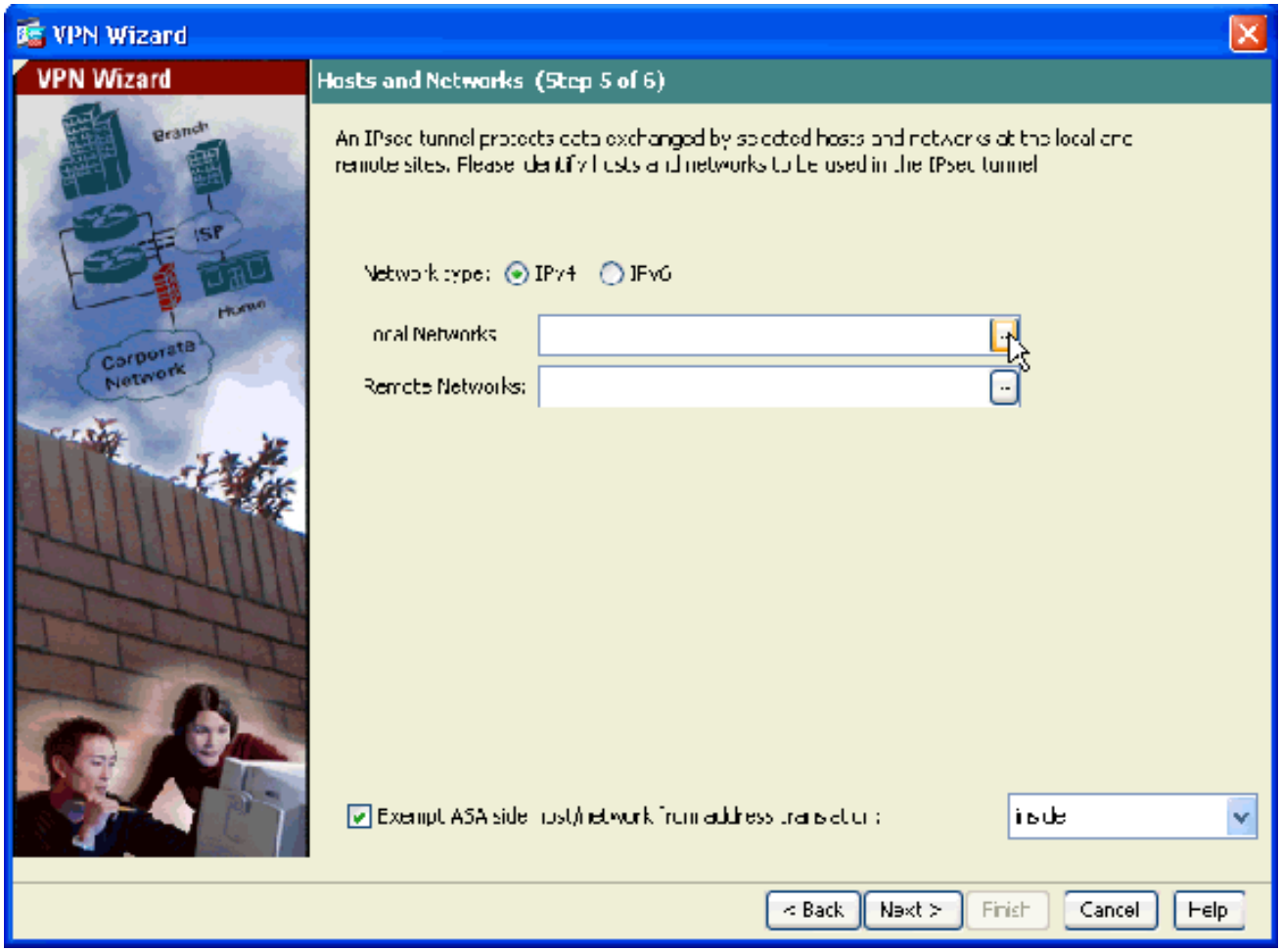
8. 指定要用於IKE的屬性，也稱為階段1。隧道兩端的這些屬性必須相同。



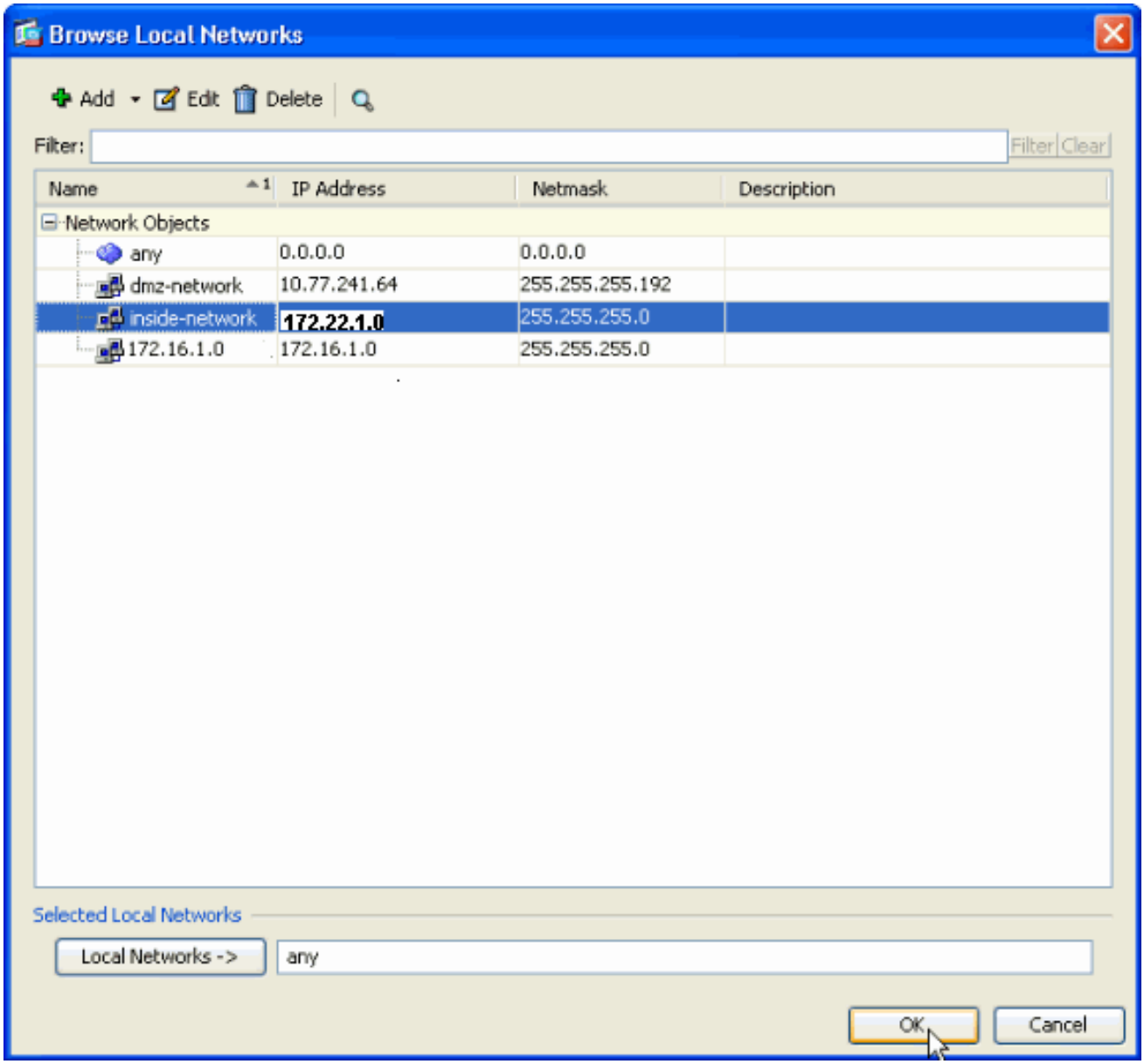
9. 指定要用於IPsec（也稱為第2階段）的屬性。這些屬性必須在兩端匹配。



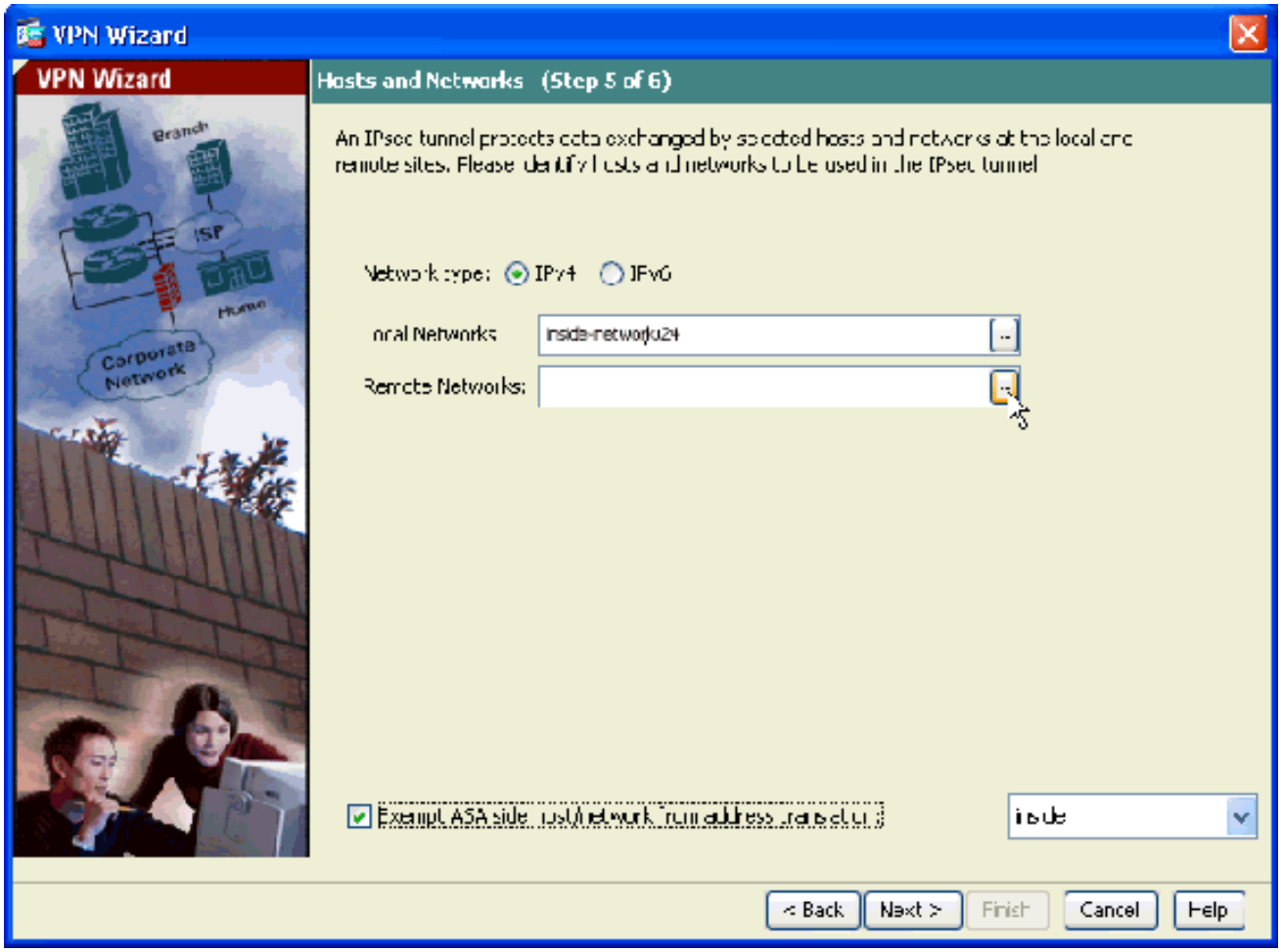
10. 指定應允許其流量通過VPN隧道的主機。在此步驟中，您必須為VPN隧道提供本地網路和遠端網路。按一下**Local Networks**旁邊的按鈕（如此處所示），從下拉選單中選擇本地網路位址
：



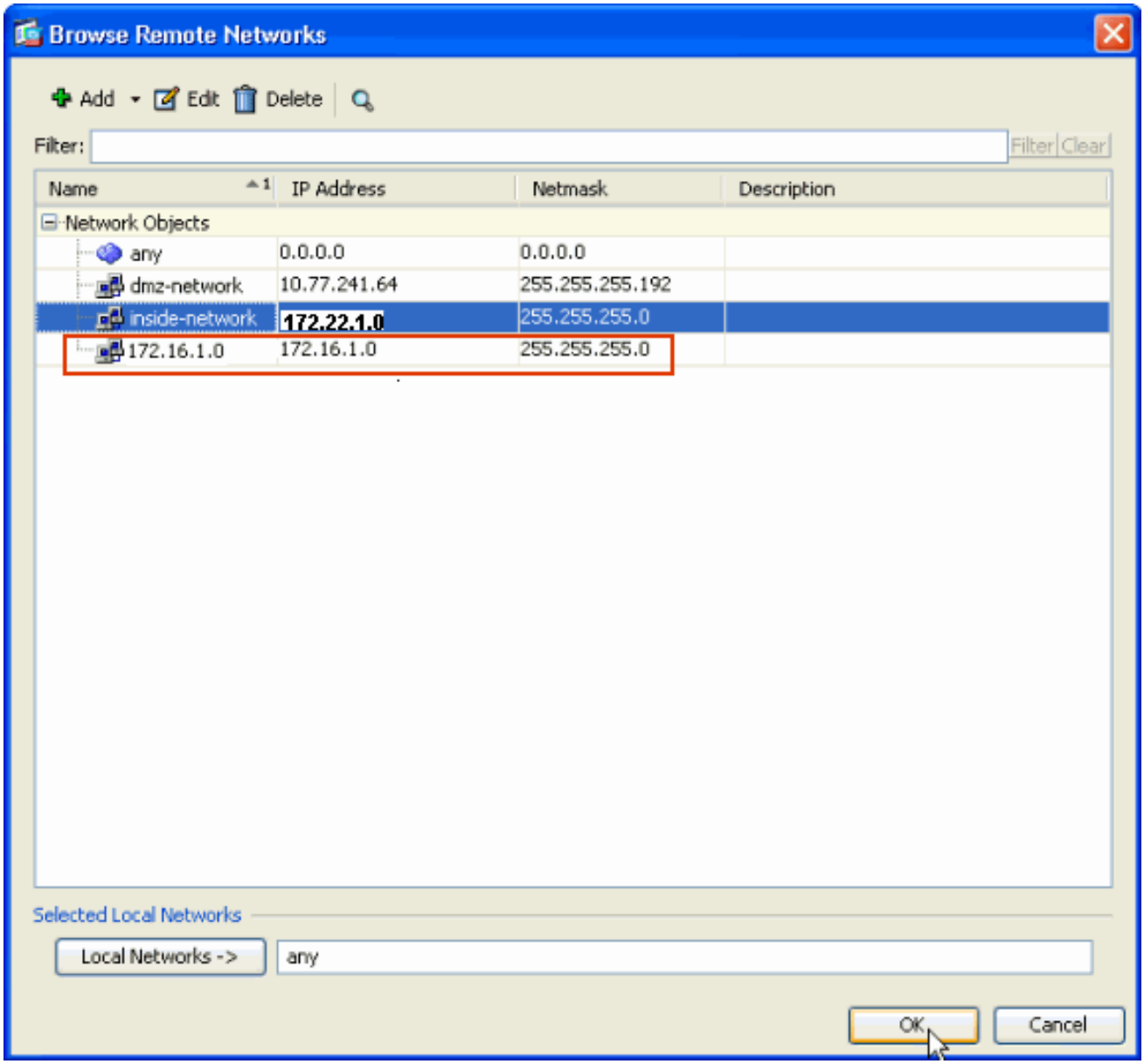
11. 選擇Local Network地址，然後按一下OK。



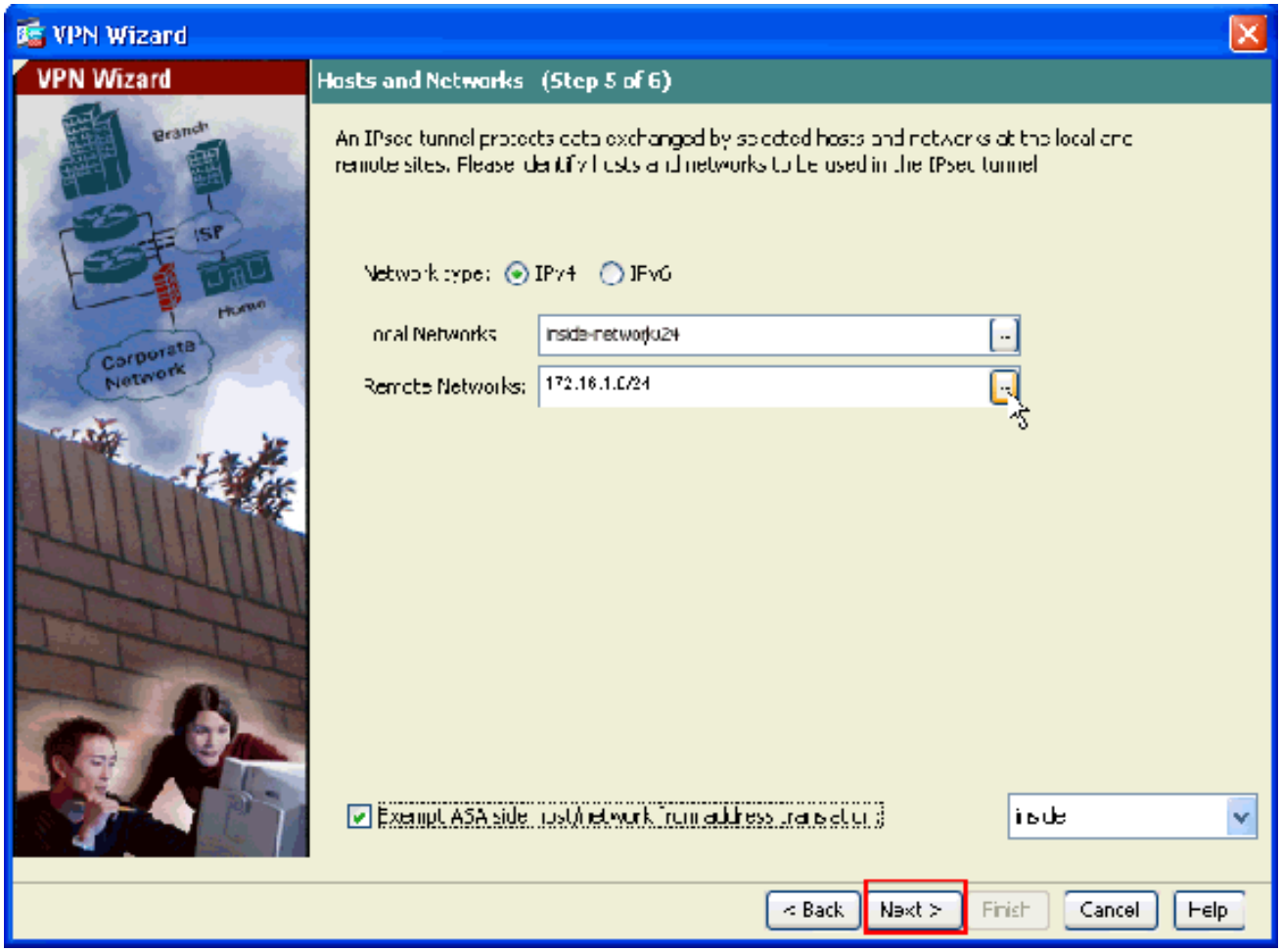
12. 按一下**Remote Networks**旁邊的按鈕，從下拉選單中選擇遠端網路地址。



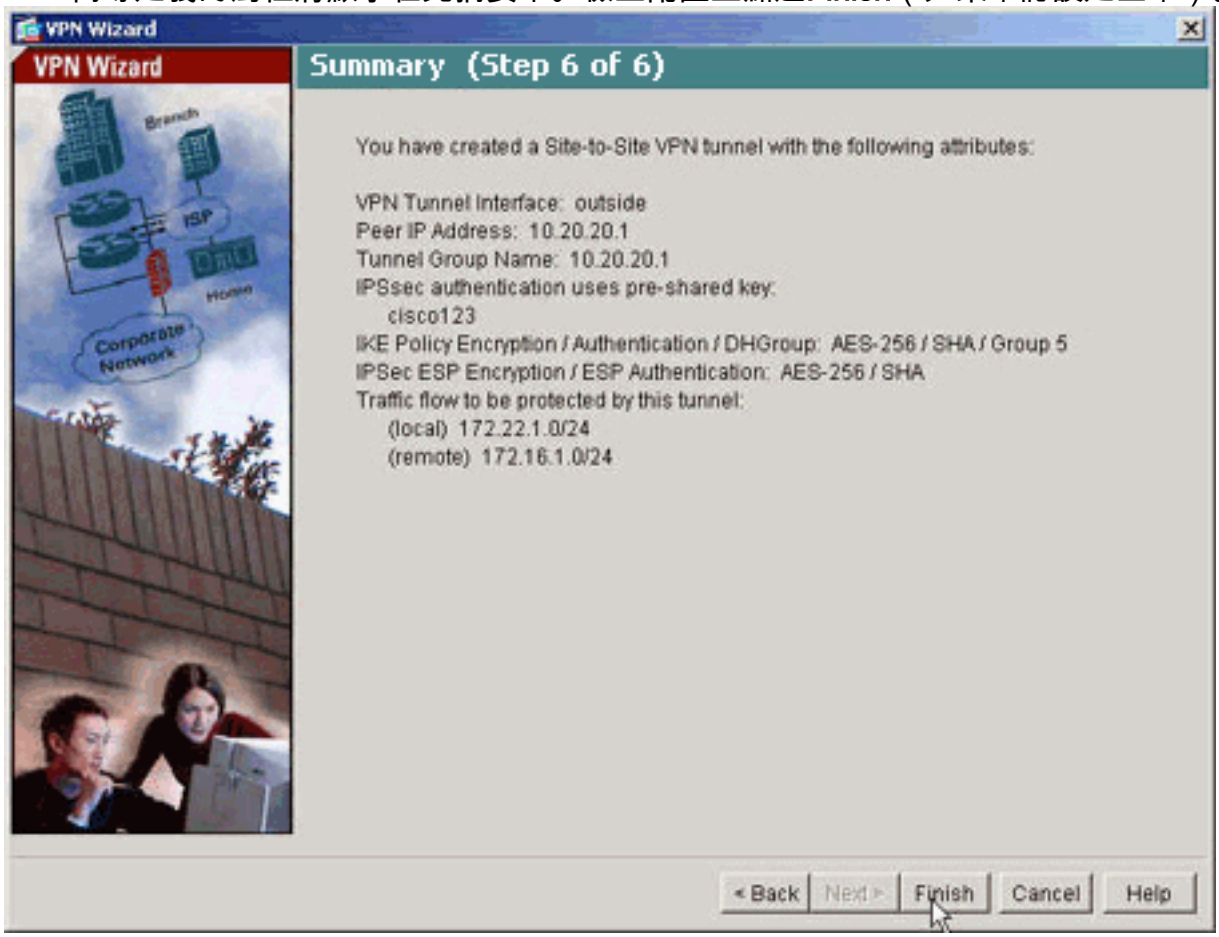
13. 選擇**Remote Network**地址，然後按一下**OK**。**注意：**如果清單中沒有遠端網路，則必須將網路新增到清單中。按一下**Add**即可完成此操作。



14. 選中**Exempt ASA side host/network from address translation**覈取方塊，以防止隧道流量進行網路地址轉換。按「**Next**」（下一步）。



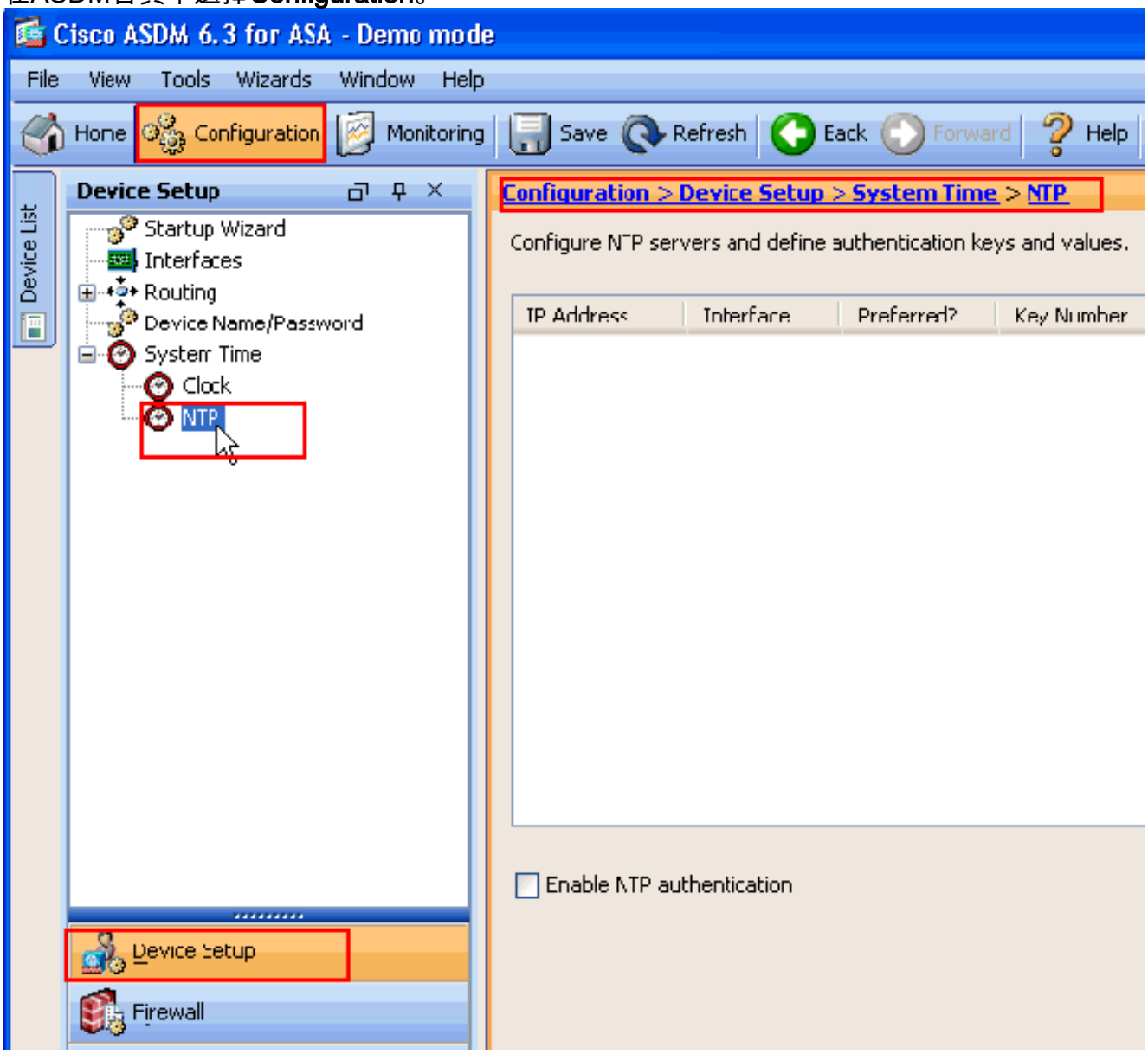
15. VPN嚮導定義的屬性將顯示在此摘要中。檢查配置並點選**Finish**（如果確認設定正確）。



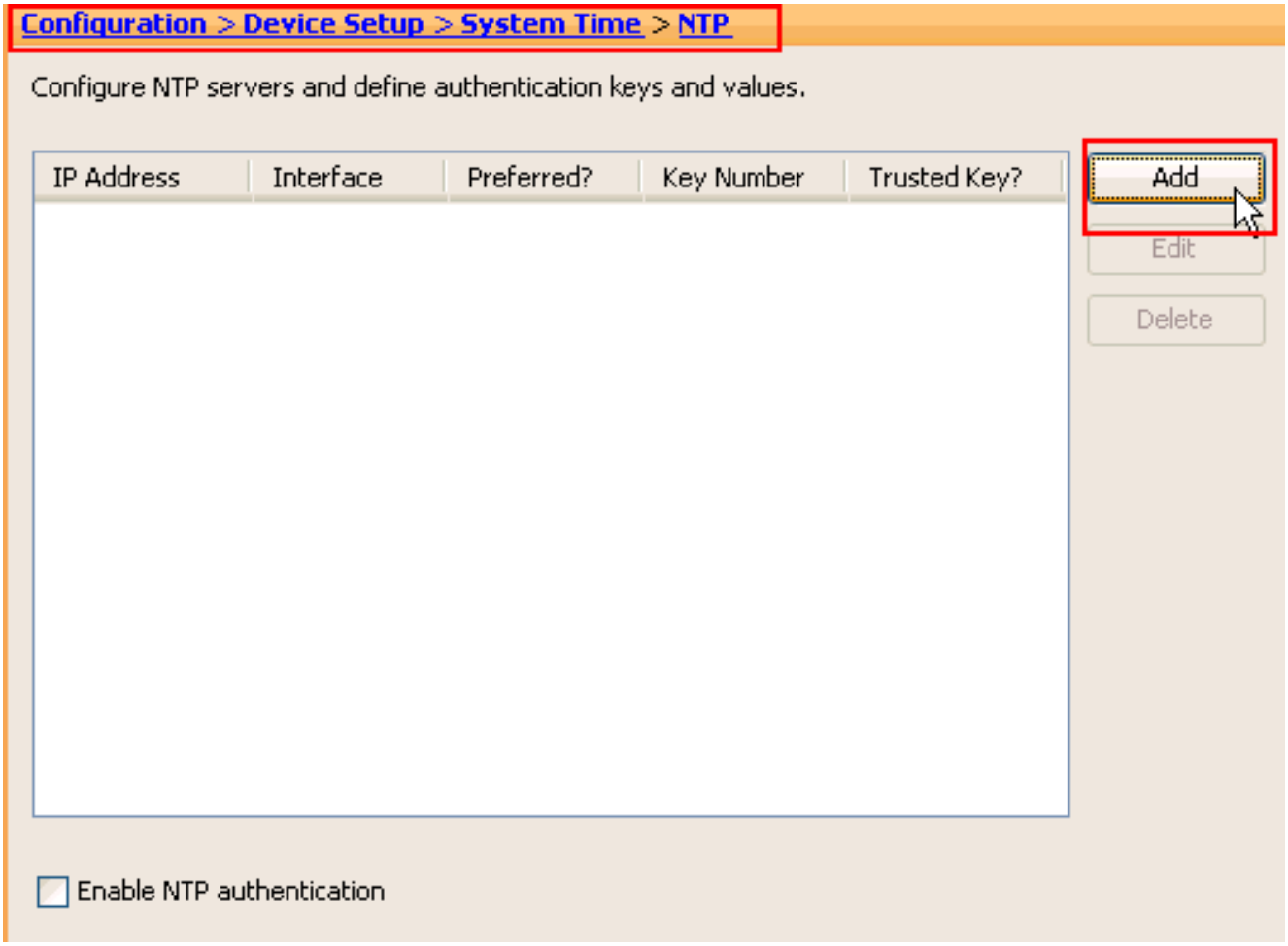
[NTP ASDM配置]

完成以下步驟，以便在思科安全裝置上配置NTP:

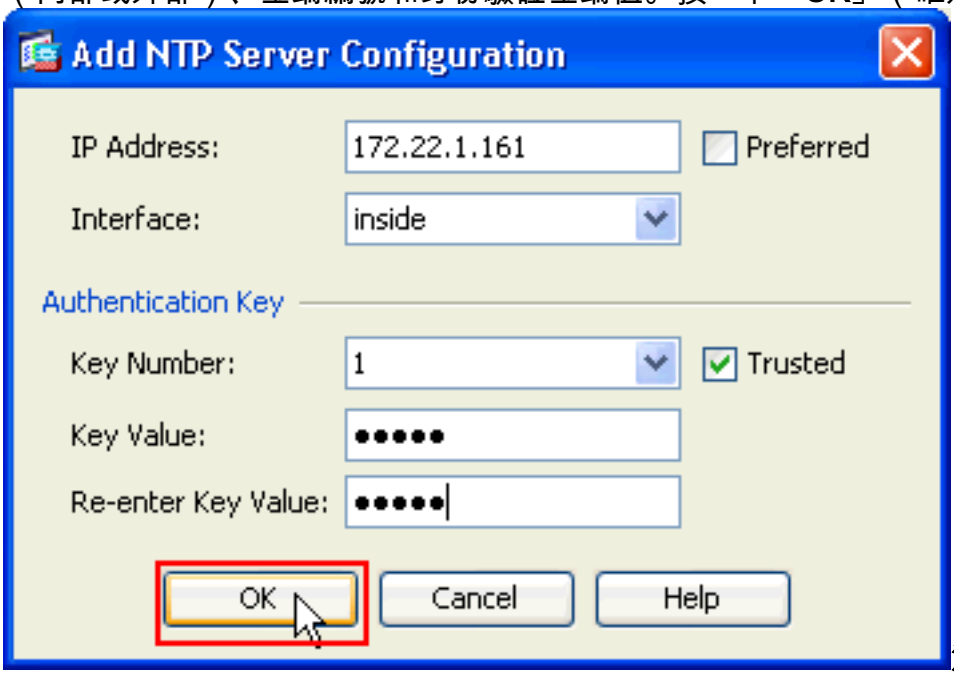
1. 在ASDM首頁中選擇**Configuration**。



2. 選擇**Device Setup > System Time > NTP**以開啟ASDM的**NTP**配置頁。



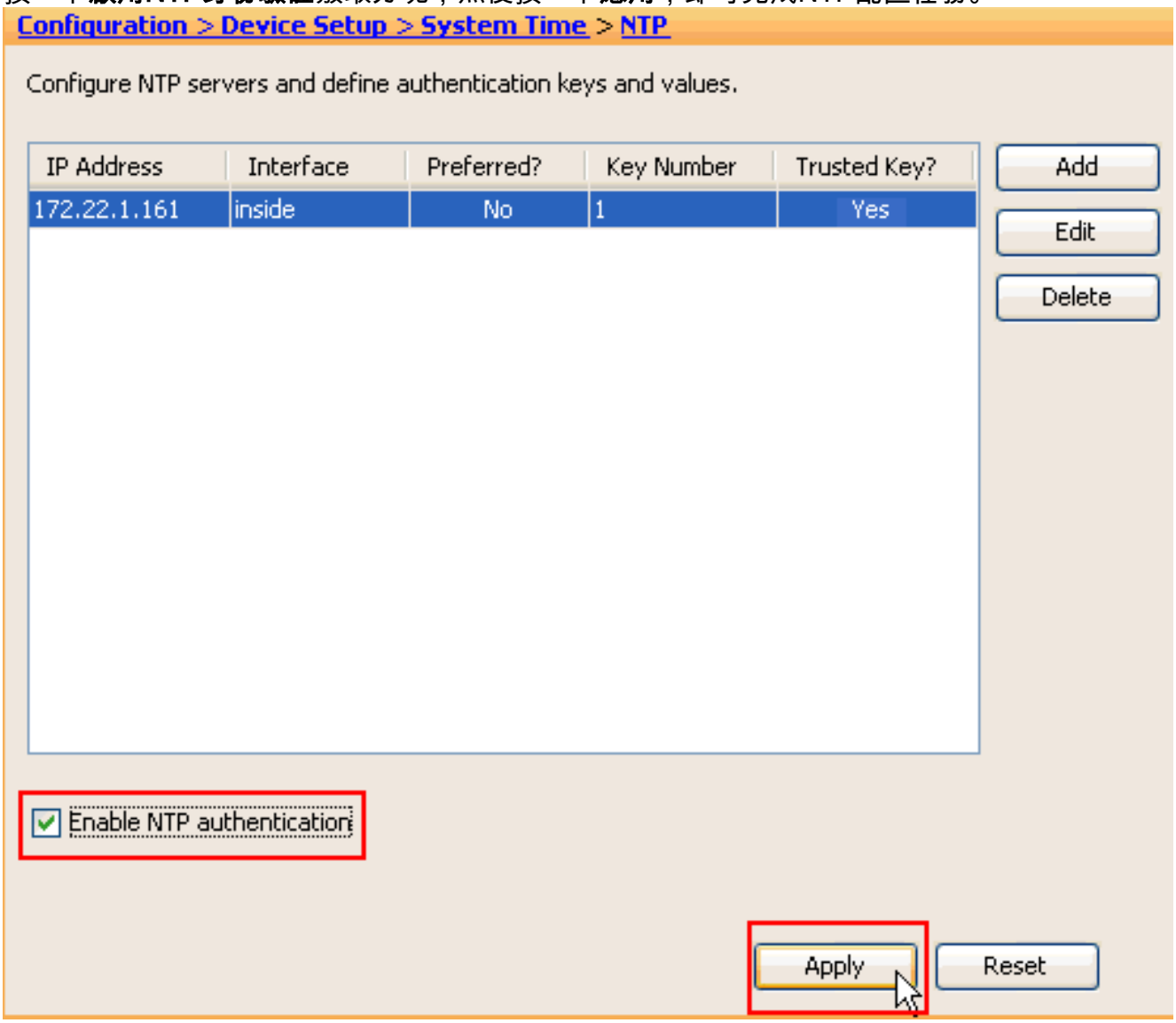
3. 點選**Add**以新增NTP伺服器，並在出現的新視窗中提供所需的屬性，例如IP地址、介面名稱（內部或外部）、金鑰編號和身份驗證金鑰值。按一下「**OK**」（確定）。



注意：對於ASA1，介面名稱應選擇為inside，對於ASA2，選擇為outside。**註**：ASA和**NTP伺服器**中的ntp身份驗證金鑰應該相同。ASA1和ASA2的CLI中的身份驗證屬性配置如下所示：

```
ASA1#ntp authentication-key 1 md5 cisco
ntp trusted-key 1
ntp server 172.22.1.161 key 1 source inside

ASA2#ntp authentication-key 1 md5 cisco
ntp trusted-key 1
ntp server 172.22.1.161 key 1 source outside
```

4. 按一下**啟用NTP身份驗證**覈取方塊，然後按一下**應用**，即可完成NTP配置任務。



ASA1 CLI配置

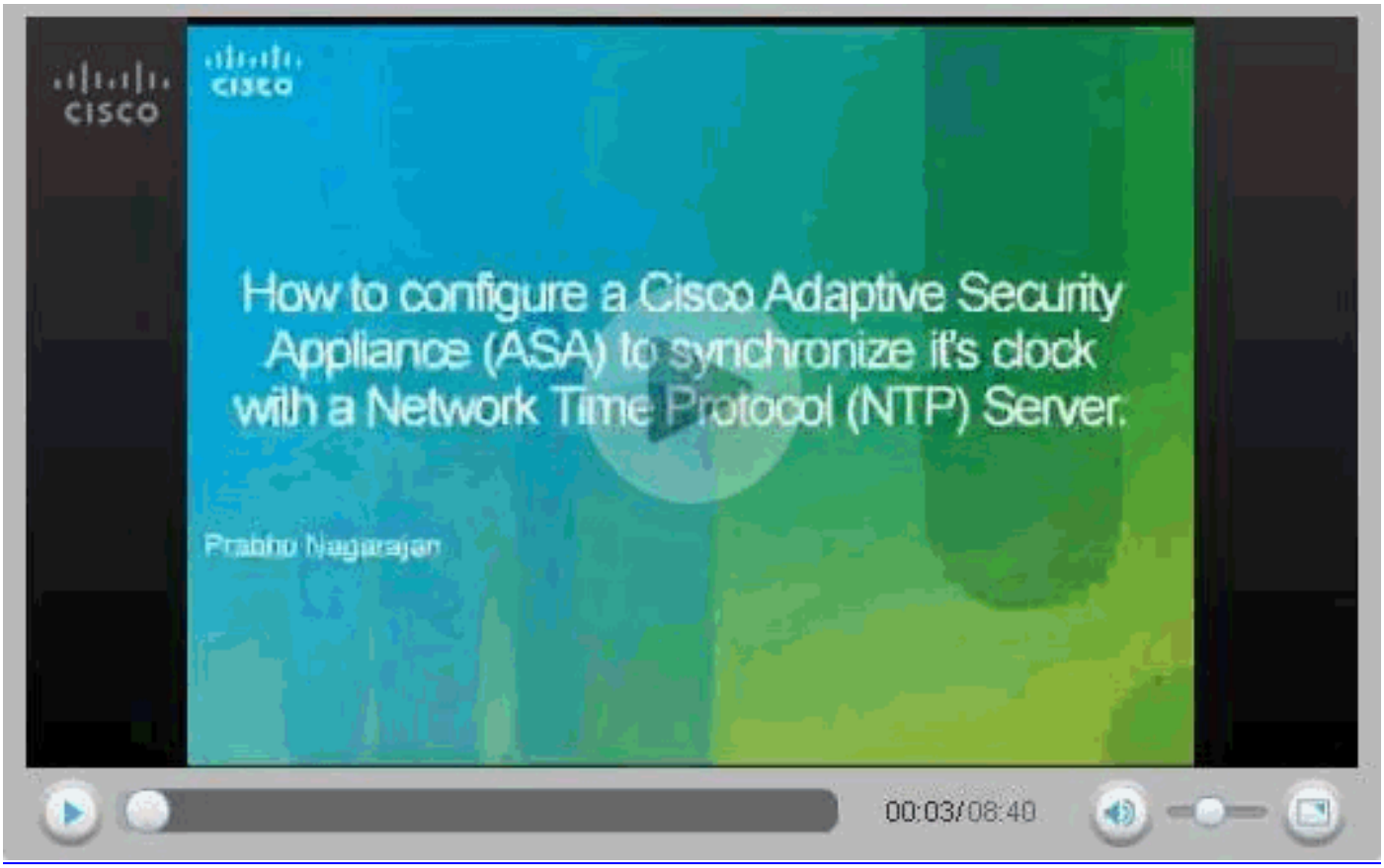
ASA1
ASA#**show run** : Saved ASA Version 8.3(1) ! hostname ASA1 domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0 nameif outside security-level 0 ip address 10.10.10.1 255.255.255.0 *!--- Configure the outside interface. !* interface Ethernet1 nameif inside security-level 100 ip address 172.22.1.163 255.255.255.0 *!--- Configure the inside* *interface. ! !-- Output suppressed !* passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server- group DefaultDNS domain-name default.domain.invalid

```
access-list inside_nat0_outbound extended permit ip
172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !---
This access list (inside_nat0_outbound) is used !---
with the nat zero command. This prevents traffic which
!--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_cryptomap_20 extended permit ip
172.22.1.0 255.255.255.0 172
.16.1.0 255.255.255.0
!--- This access list (outside_cryptomap_20) is used !--
- with the crypto map outside_map !--- to determine
which traffic should be encrypted and sent !--- across
the tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover

asdm image flash:/asdm-631.bin
!--- Enter this command to specify the location of the
ASDM image. asdm history enable arp timeout 14400 object
network obj-local subnet 172.22.1.0 255.255.255.0 object
network obj-remote subnet 172.16.1.0 255.255.255.0 nat
(inside,outside) 1 source static obj-local obj-local
destination static obj-remote obj-remote !--- NAT 0
prevents NAT for networks specified in !--- the ACL
inside_nat0_outbound.

route outside 0.0.0.0 0.0.0.0 10.10.10.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute


http server enable
!--- Enter this command in order to enable the HTTPS
server !--- for ASDM. http 172.22.1.1 255.255.255.255
inside !--- Identify the IP addresses from which the
security appliance !--- accepts HTTPS connections. no
snmp-server location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. crypto ipsec transform-set ESP-AES-
256-SHA esp-aes-256 esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 20
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
```

```
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
l2l !--- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l—IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections,
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 10.20.20.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
!--- authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
!--- Define the NTP server authentication-key,Trusted-
key !--- and the NTP server address for configuring NTP.
ntp authentication-key 1 md5 *
ntp trusted-key 1

!--- The NTP server source is to be mentioned as inside
for ASA1 ntp server 172.22.1.161 key 1 source inside
Cryptochecksum:ce7210254f4a0bd263a9072a4ccb7cf7
: end
```

發佈到思科支援社群的以下影片通過演示說明了將ASA配置為NTP客戶端的過程：

如何配置思科自適應安全裝置(ASA)以將其時鐘與網路時間協定(NTP)伺服器同步。



ASA2 CLI配置

ASA2

```
ASA Version 8.3(1)
!
hostname ASA2
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.20.20.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on ASA1.

access-list outside_cryptomap_20 extended permit ip
172.16.1.0 255.255.255.0 172
```

```
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
outside_cryptomap_20 !--- ACL on ASA1.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-631.bin
no asdm history enable
arp timeout 14400
object network obj-local
subnet 172.22.1.0 255.255.255.0

object network obj-remote
subnet 172.16.1.0 255.255.255.0


nat (inside,outside) 1 source static obj-local obj-local
destination static
obj-remote obj-remote
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256
esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-
SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
```

```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global

!--- Define the NTP server authentication-key,Trusted-
key !--- and the NTP server address for configuring NTP.
ntp authentication-key 1 md5 *
ntp trusted-key 1

!--- The NTP server source is to be mentioned as outside
for ASA2. ntp server 172.22.1.161 key 1 source outside
Cryptochecksum:d5e2ee898f5e8bd28e6f027aeed7f41b
: end
ASA#
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- show ntp status — 顯示NTP時鐘資訊。

```
ASA1#show ntp status

Clock is synchronized, stratum 2, reference is 172.22.1.161
nominal freq is 99.9984 Hz, actual freq is 99.9983 Hz, precision is 2**6
reference time is ccf22b77.f7a6e7b6 (13:28:23.967 UTC Tue Dec 16 2008)
clock offset is 34.8049 msec, root delay is 4.78 msec
root dispersion is 60.23 msec, peer dispersion is 25.41 msec
```

- show ntp associations [detail] — 顯示配置的網路時間伺服器關聯。

```
ASA1#show ntp associations detail
172.22.1.161 configured, authenticated, our_master, sane, valid, stratum 1
ref ID .LOCL., time ccf2287d.3668b946 (13:15:41.212 UTC Tue Dec 16 2008)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 7, sync dist 23.087
delay 4.52 msec, offset 9.7649 msec, dispersion 20.80
precision 2**19, version 3
org time ccf22896.f1a4fca3 (13:16:06.943 UTC Tue Dec 16 2008)
rcv time ccf22896.efb94b28 (13:16:06.936 UTC Tue Dec 16 2008)
xmt time ccf22896.ee5691dc (13:16:06.931 UTC Tue Dec 16 2008)
filtdelay =     4.52    4.68    4.61    0.00    0.00    0.00    0.00    0.00
filtoffset =    9.76    7.09    3.85    0.00    0.00    0.00    0.00    0.00
filterror =    15.63   16.60   17.58 14904.3 14904.3 14904.3 14904.3 14904.3
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug命令之前，請參閱有關Debug命令的重要資訊。

- **debug ntp validity** — 顯示NTP對等時鐘有效性。以下是金鑰不匹配的debug輸出：

```
NTP: packet from 172.22.1.161 failed validity tests 10
   Authentication failed
```

- **debug ntp packet** — 顯示NTP資料包資訊。沒有來自伺服器的響應時，在ASA上只會看到NTP xmit資料包，而沒有NTP rcv資料包。

```
ASA1# NTP: xmit packet to 172.22.1.161:
 leap 0, mode 3, version 3, stratum 2, ppoll 64
 rtdel 012b (4.562), rtdsp 0cb6 (49.652), refid ac1601a1 (172.22.1.161)
 ref ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)
 org ccf22916.f426232d (13:18:14.953 UTC Tue Dec 16 2008)
 rec ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)
 xmt ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)
NTP: rcv packet from 172.22.1.161 to 172.22.1.163 on inside:
 leap 0, mode 4, version 3, stratum 1, ppoll 64
 rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 4c4f434c (76.79.67.76)
 ref ccf2293d.366a4808 (13:18:53.212 UTC Tue Dec 16 2008)
 org ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)
 rec ccf22956.f52e480e (13:19:18.957 UTC Tue Dec 16 2008)
 xmt ccf22956.f5688c29 (13:19:18.958 UTC Tue Dec 16 2008)
 inp ccf22956.f982bcd9 (13:19:18.974 UTC Tue Dec 16 2008)
```

相關資訊

- 思科調適型資安裝置管理員
- Cisco ASA 5500系列調適型安全裝置
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems