PIX/ASA 7.x及更高版本：PIX到PIX VPN隧道配置示例

目錄

簡介

本文檔介紹使用思科自適應安全裝置管理器(ASDM)在兩個PIX防火牆之間配置VPN隧道的過程。ASDM是一種基於應用程式的配置工具，旨在幫助您使用GUI設定、配置和監控PIX防火牆。PIX防火牆位於兩個不同的站點。

使用IPsec形成隧道。IPsec是在IPsec對等體之間提供資料保密性、資料完整性和資料來源身份驗證的多種開放式標準的組合。

注意：在PIX 7.1及更高版本中，sysopt connection permit-ipsec命令已更改為sysopt connection permit-vpn。此命令允許透過VPN隧道進入安全裝置並隨後解密的流量繞過介面訪問清單。組策略和每使用者授權訪問清單仍適用於流量。要停用此功能，請使用此命令的no形式。此命令在CLI配置中不可見。

要瞭解有關Cisco PIX安全裝置運行軟體版本6.x的相同方案的詳細資訊，請參閱[PIX 6.x：簡單PIX到PIX VPN隧道配置示例](#)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊指定此對等體發起第一個專用交換以確定要連線到的相應對等體。

- Cisco PIX 500系列安全裝置，帶7.x版及更高版本
- ASDM 5.x及更高版本

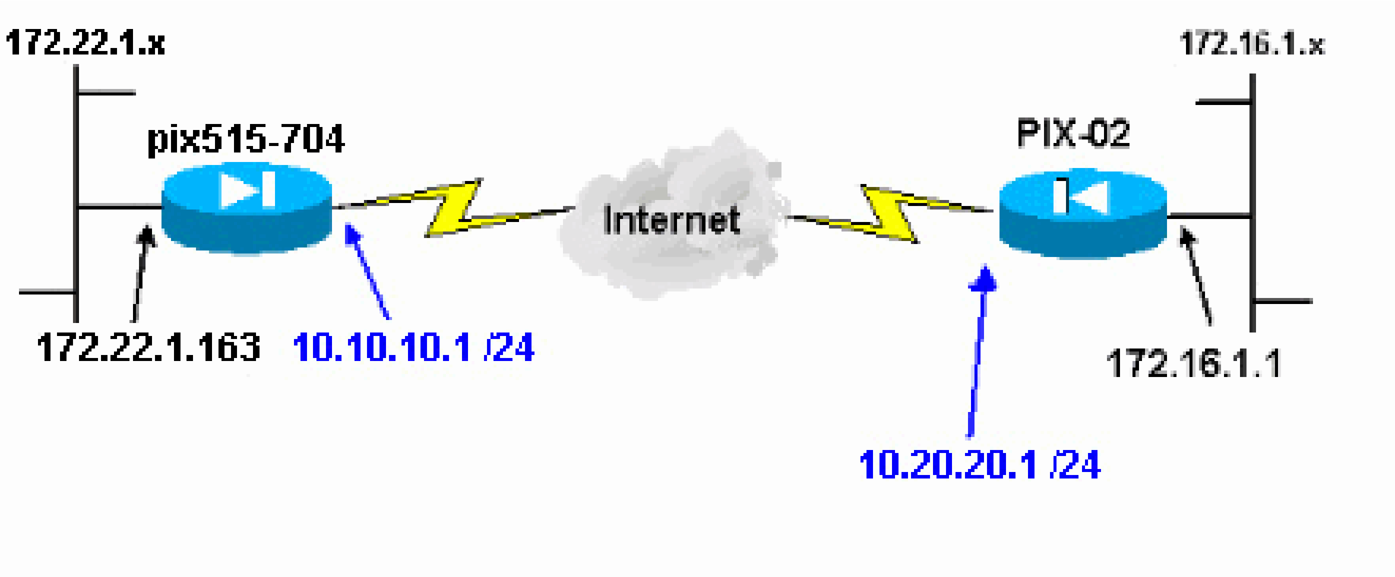
注意：要使ASDM可配置ASA，請參閱允許ASDM進行HTTPS訪問。

注意：ASA 5500系列版本7.x/8.x運行的軟體與PIX版本7.x/8.x中的軟體相同。本文檔中的配置適用於這兩種產品線。

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。

網路圖表

此文件使用以下網路設定：



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。

背景資訊

IPsec協商可分為五個步驟，包括兩個網際網路金鑰交換(IKE)階段。

1. IPsec隧道由相關流量發起。流量在IPSec對等體之間傳輸時被視為有趣。

2. 在IKE第1階段，IPSec對等體會協商已建立的IKE安全關聯(SA)策略。在對等體進行身份驗證後，會使用網際網路安全關聯和金鑰管理協定(ISAKMP)建立安全隧道。

3. 在IKE第2階段，IPSec對等體使用經過身份驗證的安全隧道來協商IPSec SA轉換。共用策略的協商確定IPSec隧道的建立方式。

4. 將建立IPSec隧道，並根據IPSec轉換集中配置的IPSec引數在IPSec對等體之間傳輸資料。

5. IPSec隧道在IPSec SA被刪除或生命期到期時終止。

   注意：如果兩個IKE階段上的SA在對等體上不匹配，則兩個PIX之間的IPsec協商失敗。

組態

- ASDM配置
- PIX CLI配置

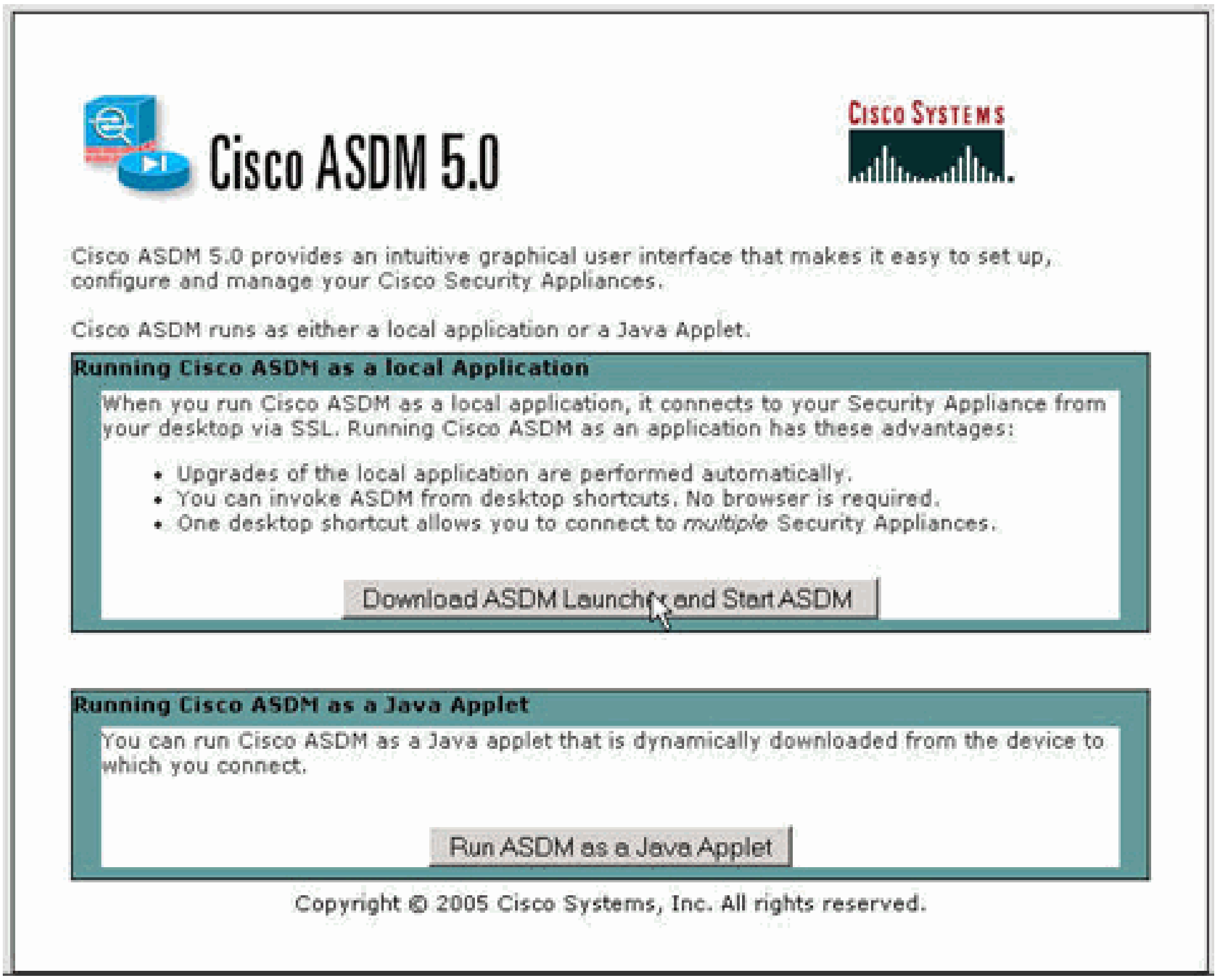
ASDM配置

請完成以下步驟：

1. 打開瀏覽器並鍵入https:// <Inside_IP_Address_of_PIX>以訪問PIX上的ASDM。

   請務必授權瀏覽器提供的與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。

   PIX顯示此窗口以允許下載ASDM應用程式。此範例會將應用程式載入本機電腦，而且不會在Java Applet中執行。



Cisco ASDM 5.0 provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or a Java Applet.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- Upgrades of the local application are performed automatically.
- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

Running Cisco ASDM as a Java Applet

You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

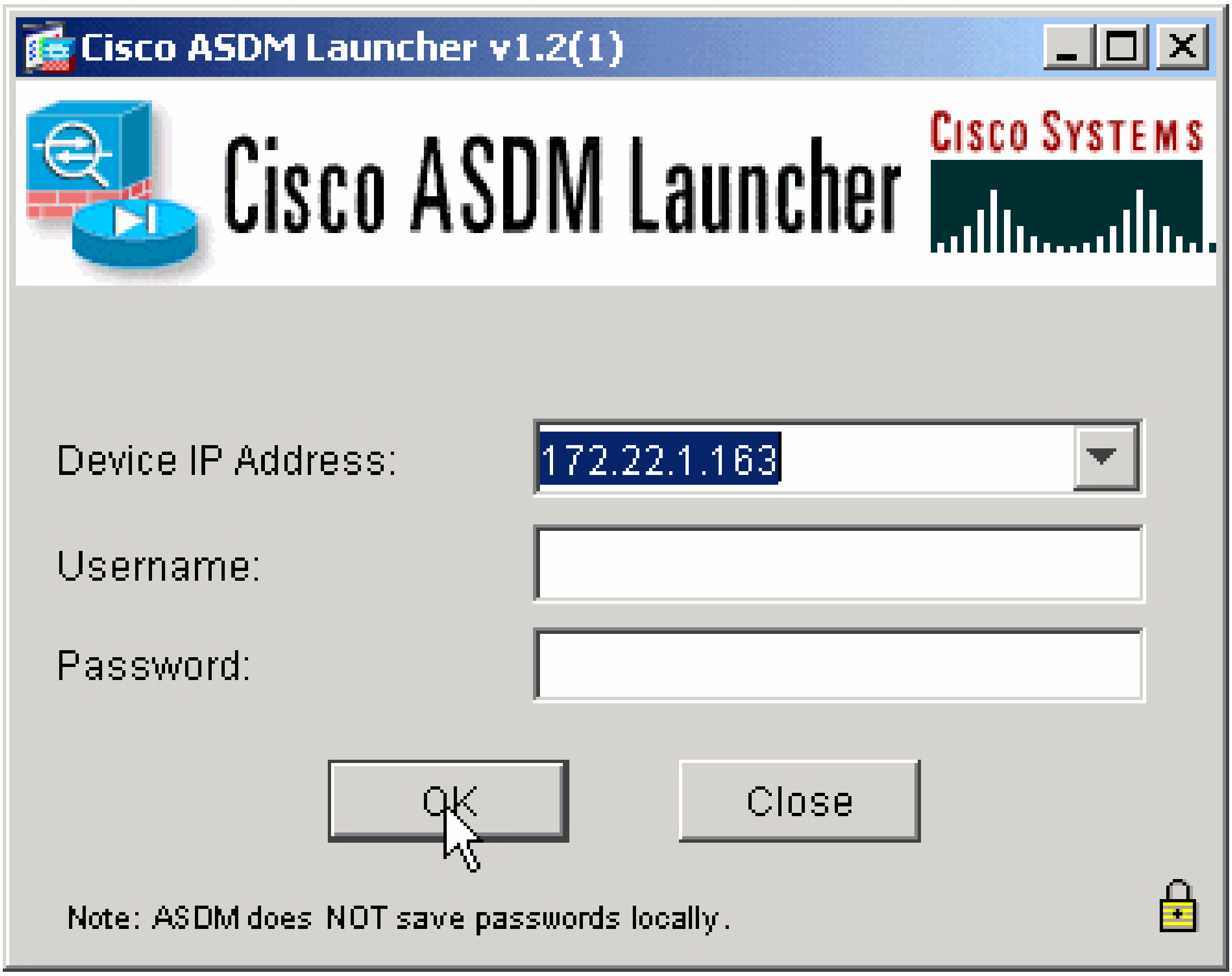
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

2. 按一下Download ASDM Launcher and Start ASDM以下載ASDM應用程式的安裝程式。

3. 下載ASDM Launcher後，請按照提示安裝軟體並運行Cisco ASDM Launcher。

4. 輸入使用http -命令配置的介面的IP地址，以及使用者名稱和口令（如果已指定）。

   此示例使用預設空白使用者名稱和密碼。



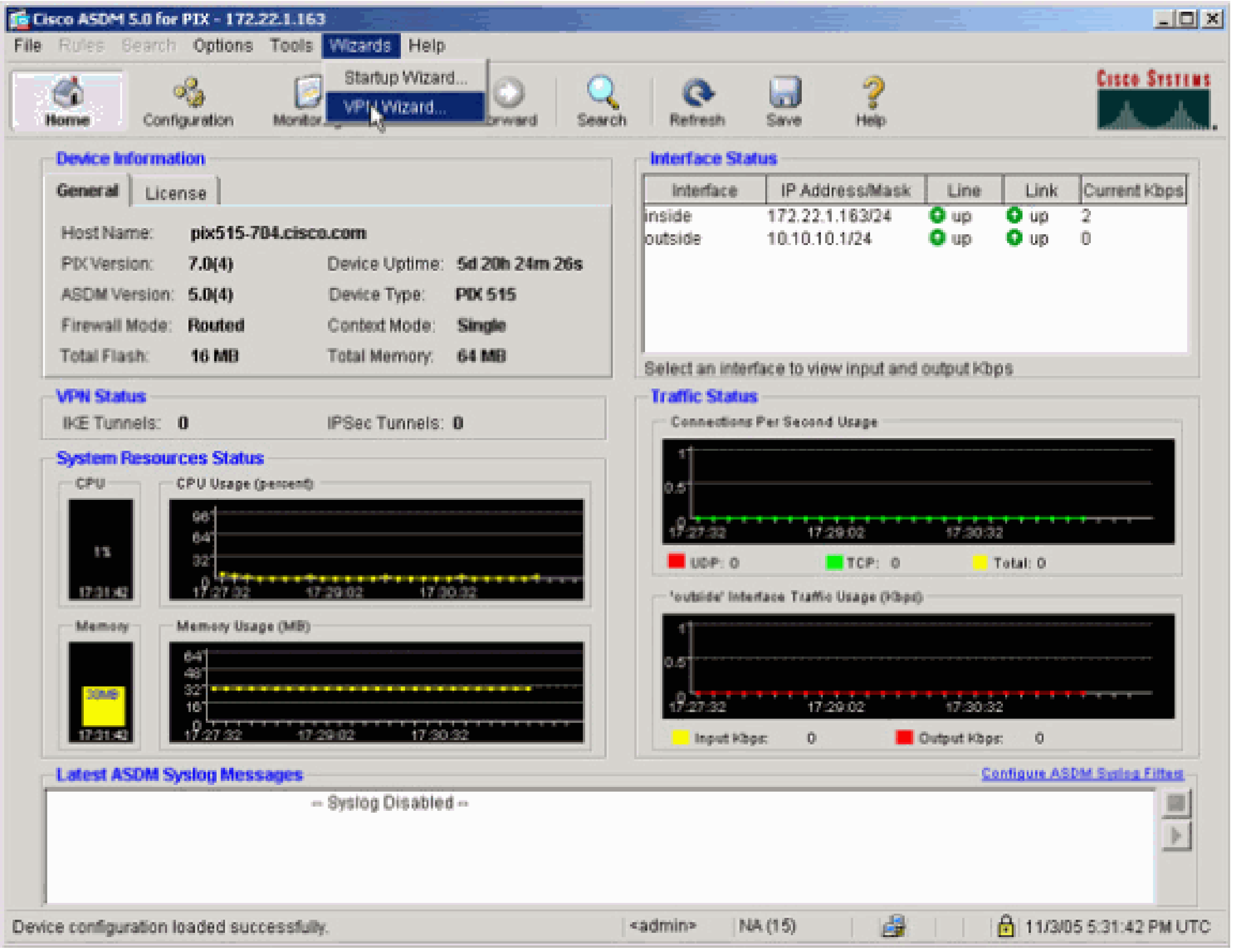
Device IP Address: 172.22.1.163

Username:

Password:

Note: ASDM does NOT save passwords locally.

5. 在ASDM應用程式連線到PIX之後，運行VPN嚮導。



Host Name: pix515-704.cisco.com

PIX Version: 7.0(4) Device Uptime: 5d 20h 24m 26s

ASDM Version: 5.0(4) Device Type: PIX 515

Firewall Mode: Routed Context Mode: Single

Total Flash: 16 MB Total Memory: 64 MB

IKE Tunnels: 0 IPSec Tunnels: 0

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.22.1.163/24	up	up	2
outside	10.10.10.1/24	up	up	0

Select an interface to view input and output Kbps

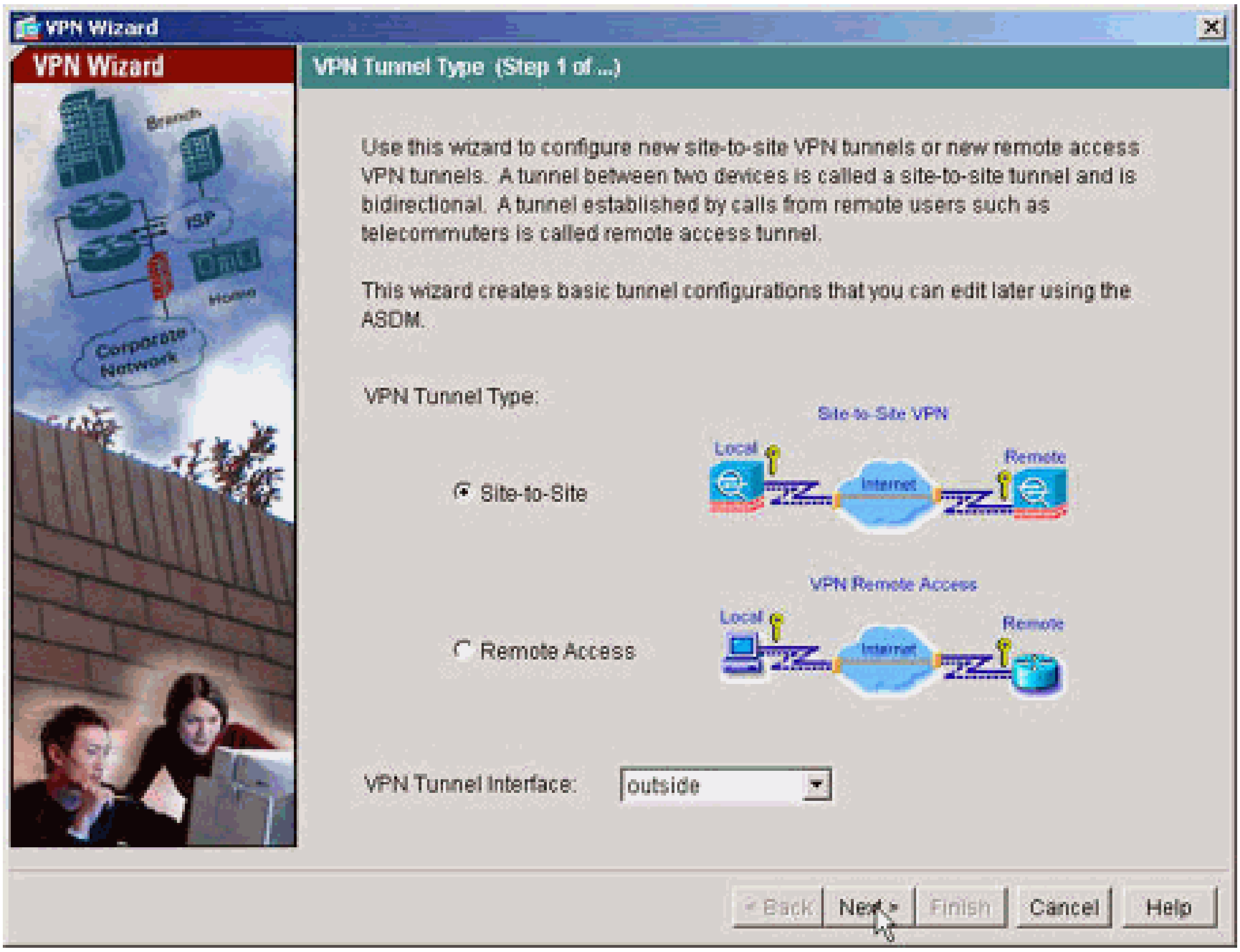
UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

-- Syslog Disabled --

Device configuration loaded successfully. <admin> NA (15) 11/3/05 5:31:42 PM UTC

6. 選擇Site-to-Site VPN隧道型別。



VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

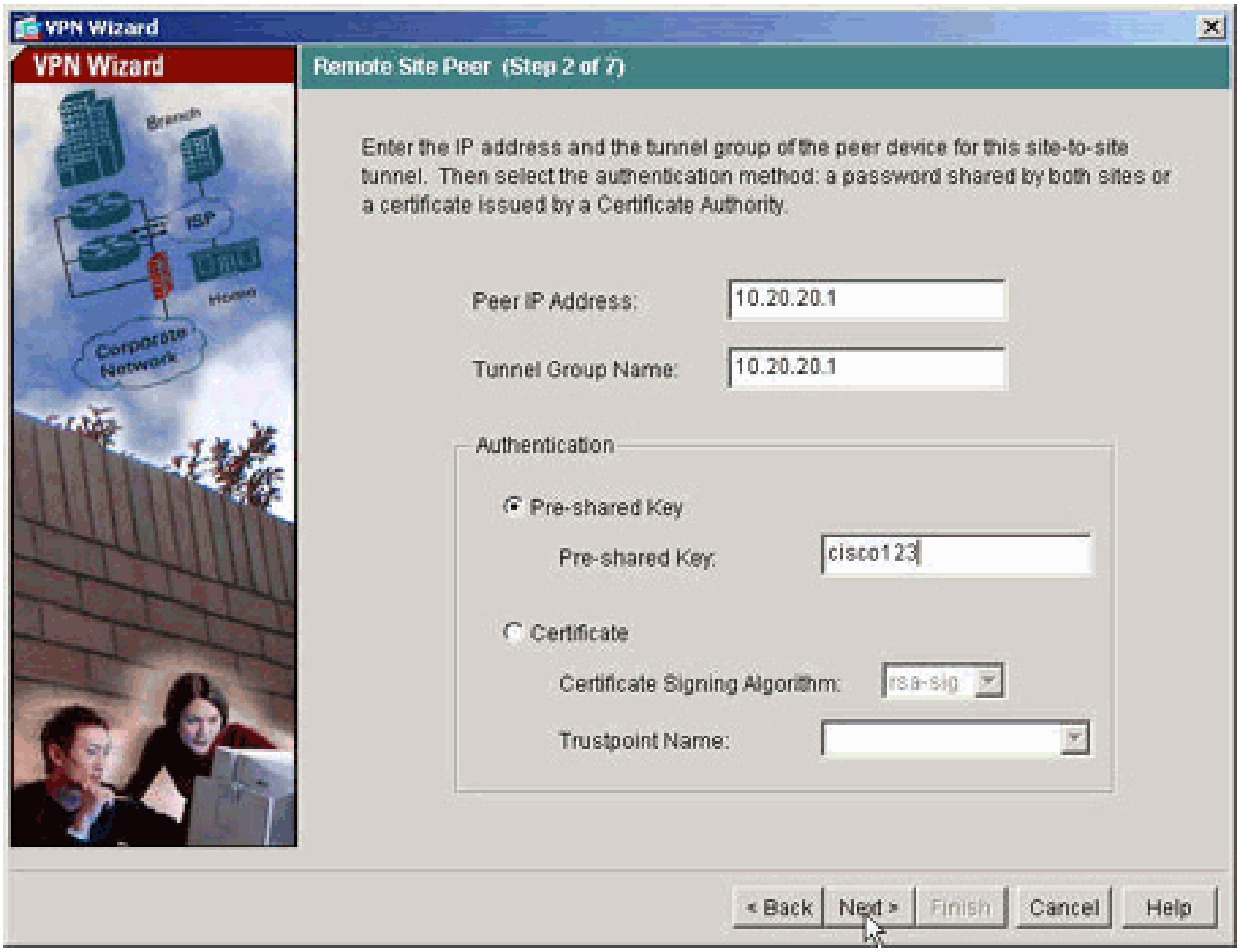
VPN Tunnel Type:

● Site-to-Site

○ Remote Access

VPN Tunnel Interface: outside

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（本示例中的預共用金鑰）。



Remote Site Peer (Step 2 of 7)

Enter the IP address and the tunnel group of the peer device for this site-to-site tunnel. Then select the authentication method: a password shared by both sites or a certificate issued by a Certificate Authority.

Peer IP Address: 10.20.20.1

Tunnel Group Name: 10.20.20.1

Authentication

● Pre-shared Key

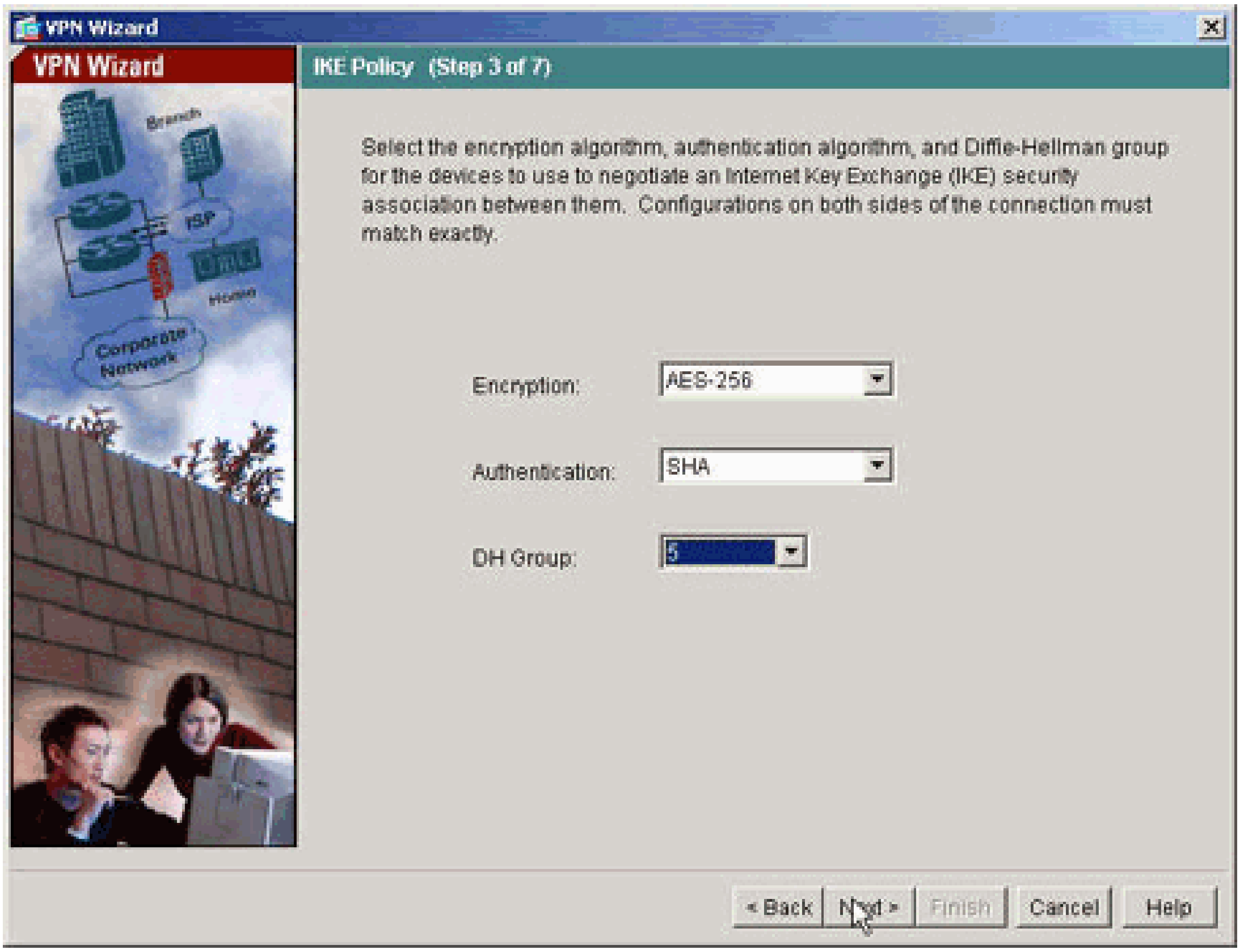
Pre-shared Key: cisco123

○ Certificate

Certificate Signing Algorithm: rsa-sig

Trustpoint Name:

8. 指定要用於IKE的屬性，也稱為「第1階段」。通道兩端的這些屬性必須相同。



IKE Policy (Step 3 of 7)

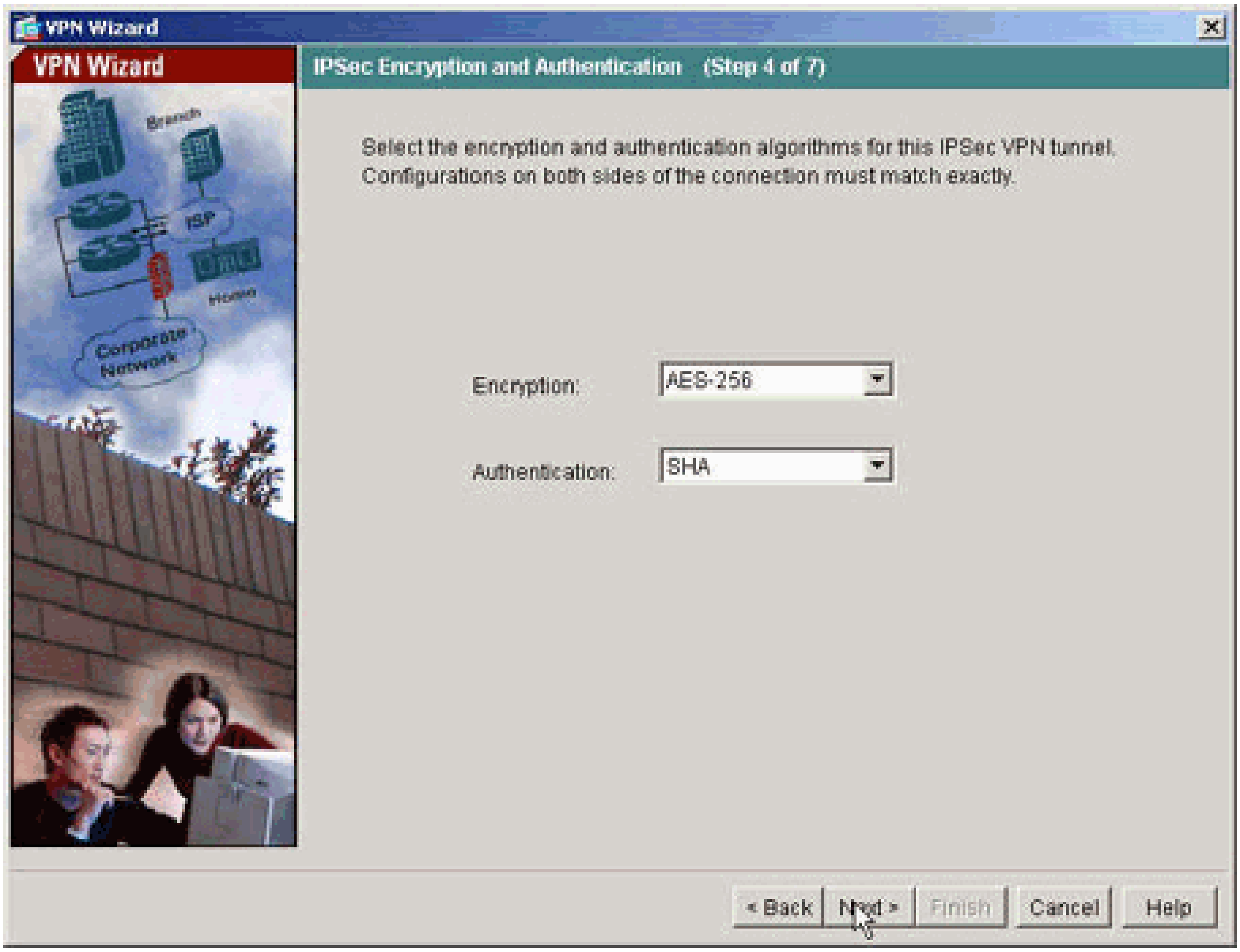
Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: AES-256

Authentication: SHA

DH Group: 5

9. 指定要用於IPsec（也稱為「階段2」）的屬性。這兩端的屬性必須相符。



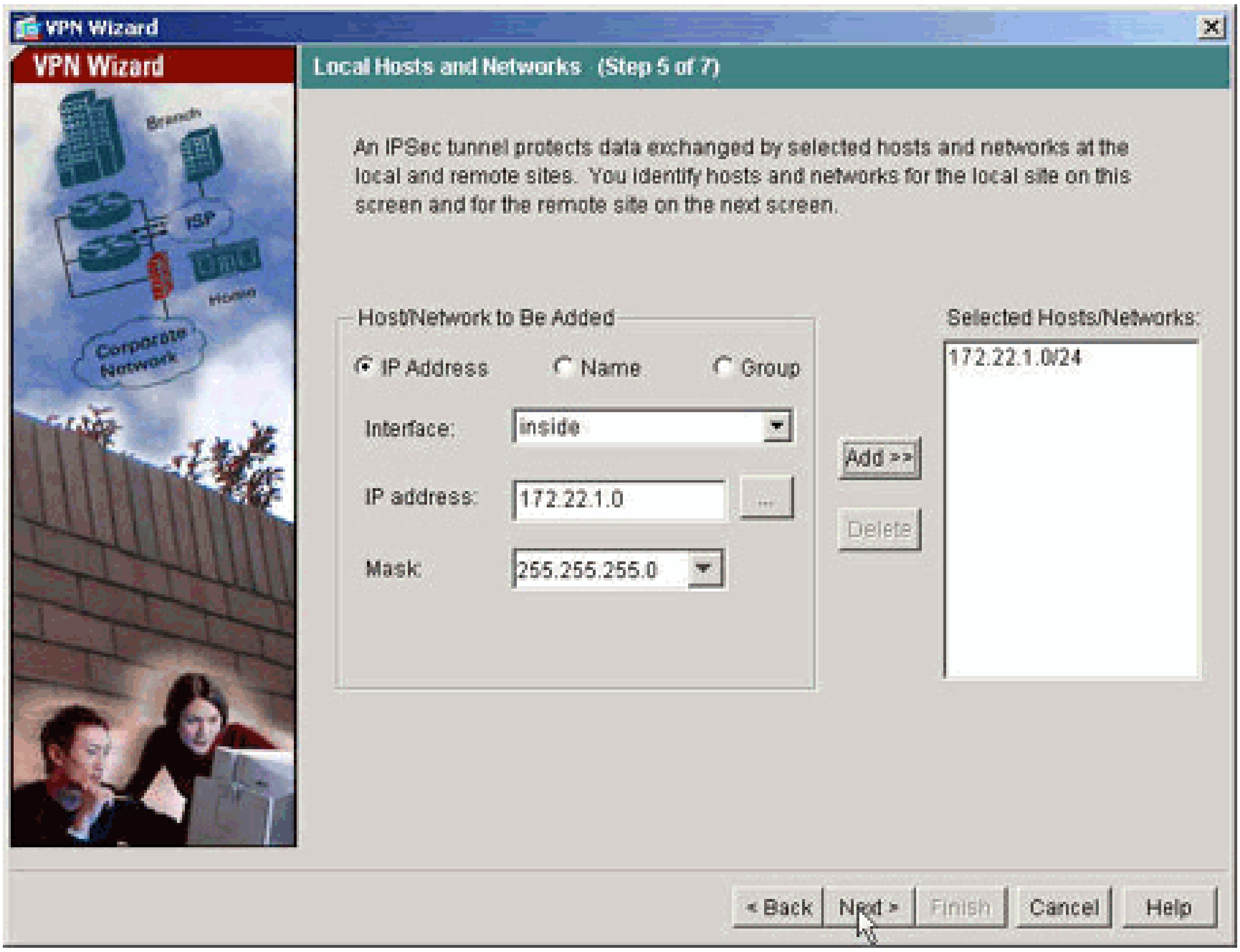
IPSec Encryption and Authentication (Step 4 of 7)

Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.

Encryption: AES-256

Authentication: SHA

10. 指定應允許其流量透過VPN隧道的主機。在此步驟中，指定了pix515-704的本地主機。



Local Hosts and Networks (Step 5 of 7)

An IPSec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. You identify hosts and networks for the local site on this screen and for the remote site on the next screen.

Host/Network to Be Added

● IP Address ○ Name ○ Group

Interface: inside

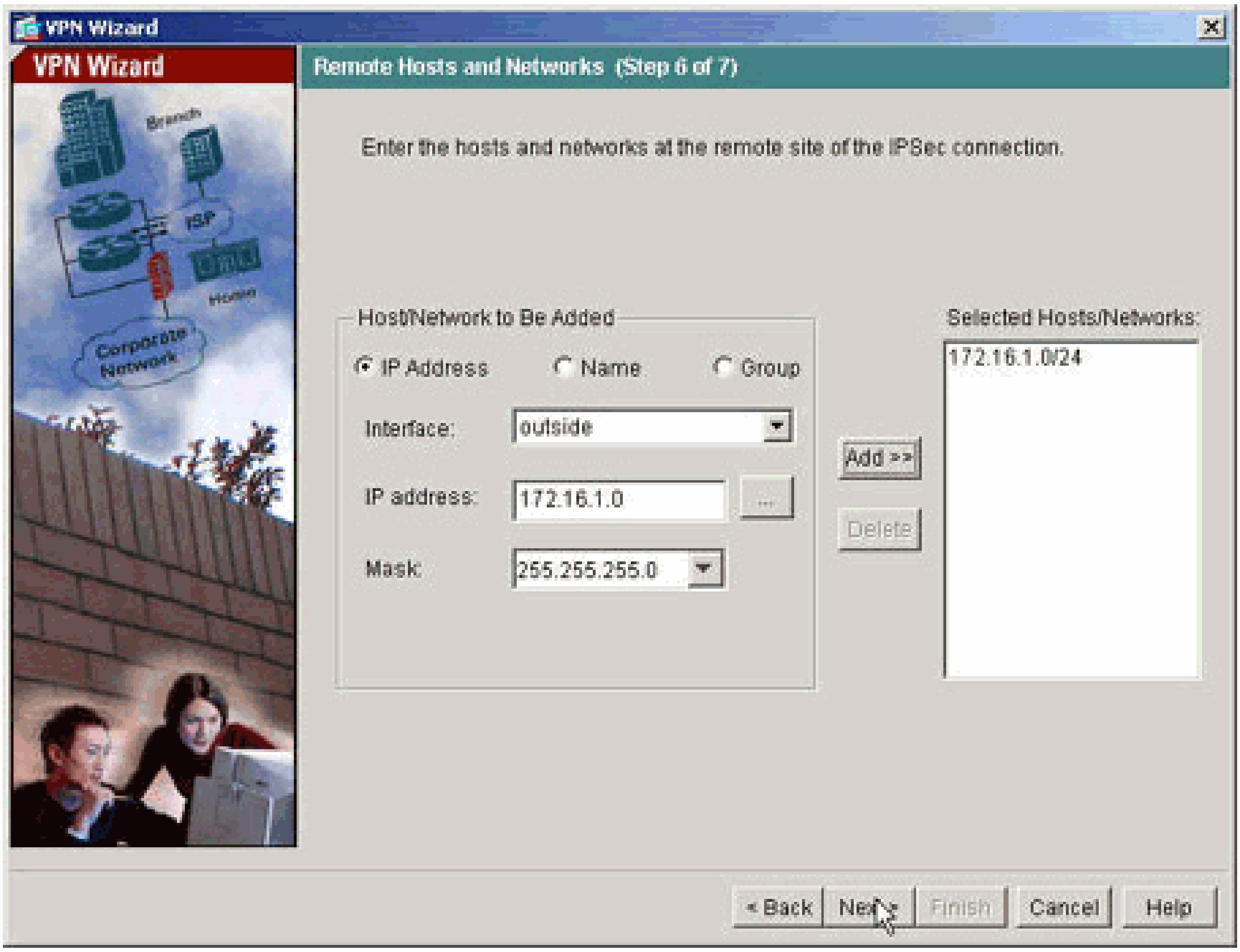
IP address: 172.22.1.0

Mask: 255.255.255.0

Selected Hosts/Networks:

172.22.1.0/24

11. 已指定通道遠端的主機和網路。



Enter the hosts and networks at the remote site of the IPSec connection.

Host/Network to Be Added

● IP Address ○ Name ○ Group

Interface: outside

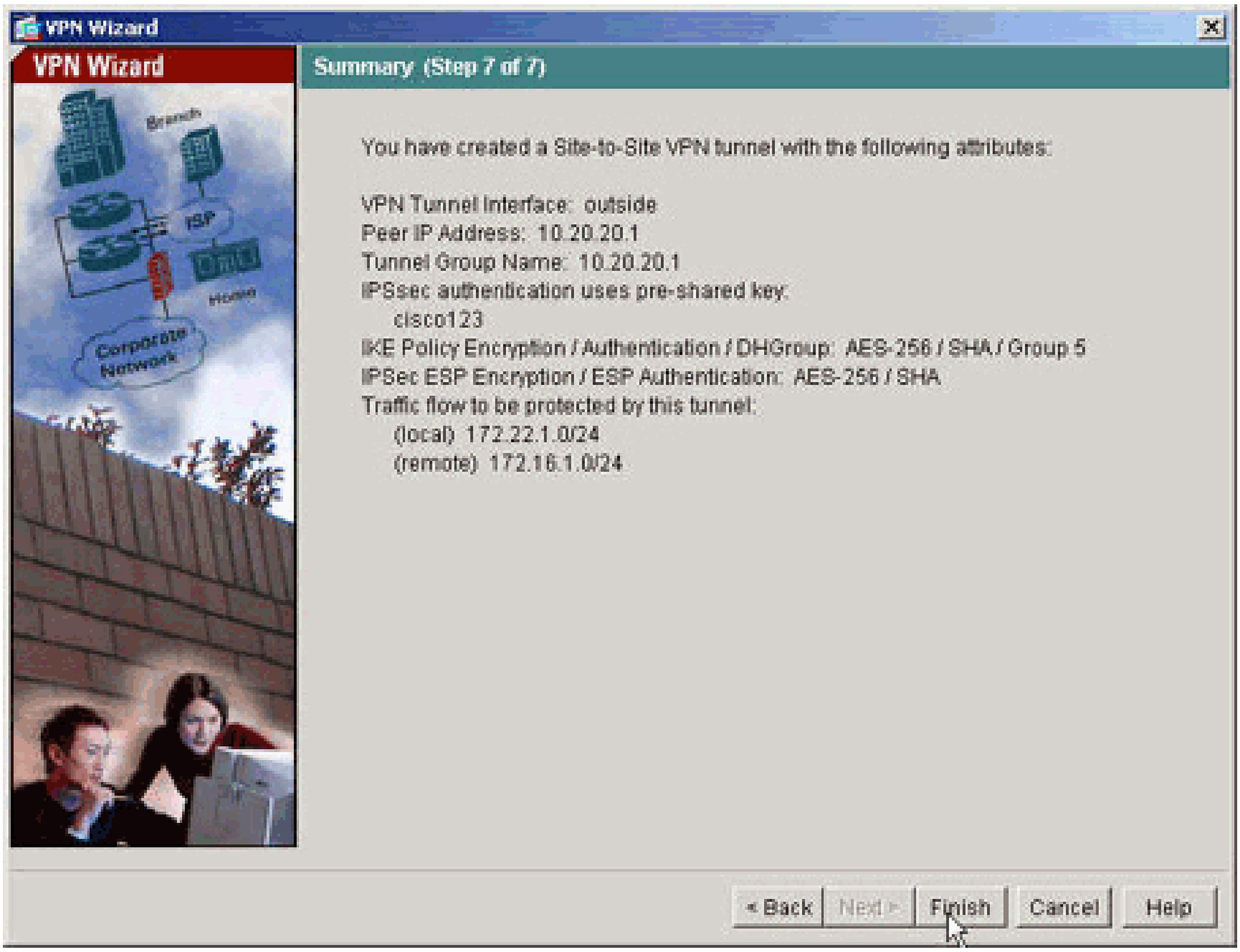
IP address: 172.16.1.0

Mask: 255.255.255.0

Selected Hosts/Networks:

172.16.1.0/24

12. VPN嚮導定義的屬性顯示在此摘要中。仔細檢查配置，如果您確保設定正確，請按一下 Finish。



Summary (Step 7 of 7)

You have created a Site-to-Site VPN tunnel with the following attributes:

VPN Tunnel Interface: outside
Peer IP Address: 10.20.20.1
Tunnel Group Name: 10.20.20.1
IPSsec authentication uses pre-shared key:
cisco123
IKE Policy Encryption / Authentication / DHGroup: AES-256 / SHA / Group 5
IPSec ESP Encryption / ESP Authentication: AES-256 / SHA
Traffic flow to be protected by this tunnel:
(local) 172.22.1.0/24
(remote) 172.16.1.0/24

PIX CLI配置

<#root>

```
pixfirewall#

show run

: Saved
PIX Version 7.1(1)
!
hostname pixfirewall
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 addres

(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 inter

(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-511.bin

!--- Enter this command to specify the location of the ASDM image.

asdm history enable
arp timeout 14400


nat (inside) 0 access-list inside_nat0_outbound
```

```
!--- 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_


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 in


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—IPse

tunnel-group

 !--- command 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
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf
: end
```

PIX-02

<#root>

```
PIX Version 7.1(1)
!
hostname pixfirewall
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 pix515-704.

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 pix515-704.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
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
Cryptochecksum:6774691244870705f858ad4e9b810874
: end
pixfirewall#
```

備用站點到站點隧道

要為此加密對映條目指定備用站點到站點功能的連線型別，請在全局配置模式下使用crypto map set connection-type命令。請使用此命令的no形式以返回到預設設定。

語法：

<#root>

crypto map *map-name seq-num set* **connection-type {answer-only | originate-only | bidirectional}**

- answer-only -用於指定此對等體在初始專用交換期間最初只對入站IKE連線做出響應，以確定要連線到的相應對等體。
- bidirectional -用於指定此對等體可根據此加密對映條目接受和發起連線。這是所有站點到站點連線的預設連線型別。
- originate-only -用於指定此對等體將發起第一個專用交換以確定要連線到的相應對等體。

crypto map set connection-type命令為備用LAN到LAN功能指定連線型別。它允許在連線的一端指定多個備份對等體。此功能僅可在以下平台之間使用：

- 兩台Cisco ASA 5500系列安全裝置
- Cisco ASA 5500系列安全裝置和Cisco VPN 3000集中器
- Cisco ASA 5500系列安全裝置和運行Cisco PIX安全裝置軟體版本7.0或更高版本的安全裝置

要配置備用LAN到LAN連線，Cisco建議您使用`originate-only`關鍵字將連線的一端配置為「只發起」，並使用`answer-only`關鍵字將具有多個備用對等體的一端配置為「只應答」。在「只發起」端上，請使用crypto map set peer命令對對等體的優先順序進行排序。僅發起安全裝置會嘗試與清單中的第一個對等裝置協商。如果該對等裝置不響應，安全裝置將沿清單向下依次工作，直到對等裝置響應或者清單中不再有對等裝置。

以此方式配置時，只發起對等體最初會嘗試建立專有隧道並與對等體協商。此後，任一對等體可以建立正常的LAN到LAN連線，並且來自任一端的資料可以啟動隧道連線。

注意：如果為加密條目配置了多個對等體IP地址的VPN，則在主對等體關閉後，將使用備用對等體IP建立VPN。但是，一旦主對等體返回，VPN就不會搶佔主IP地址。您必須手動刪除現有SA以重新啟動VPN協商，將其切換到主IP地址。如結論所述，站點到站點隧道不支援VPN搶佔。

支援的備用LAN到LAN連線型別

遠端	中心側
`Originate-Only`	`Answer-Only`
`Bi-Directional`	`Answer-Only`
`Bi-Directional`	`Bi-Directional`

範例

此示例（在全局配置模式下輸入）配置crypto map mymap，並將連線型別設定為originate-only。

```
<#root>
hostname(config)#
crypto map outside_map 20 connection-type originate-only
```

清除安全關聯(SA)

在PIX的許可權模式下，使用以下命令：

- clear [crypto] ipsec sa -刪除活動的IPsec SA。關鍵字crypto是可選的。
- clear [crypto] isakmp sa -刪除活動的IKE SA。關鍵字crypto是可選的。

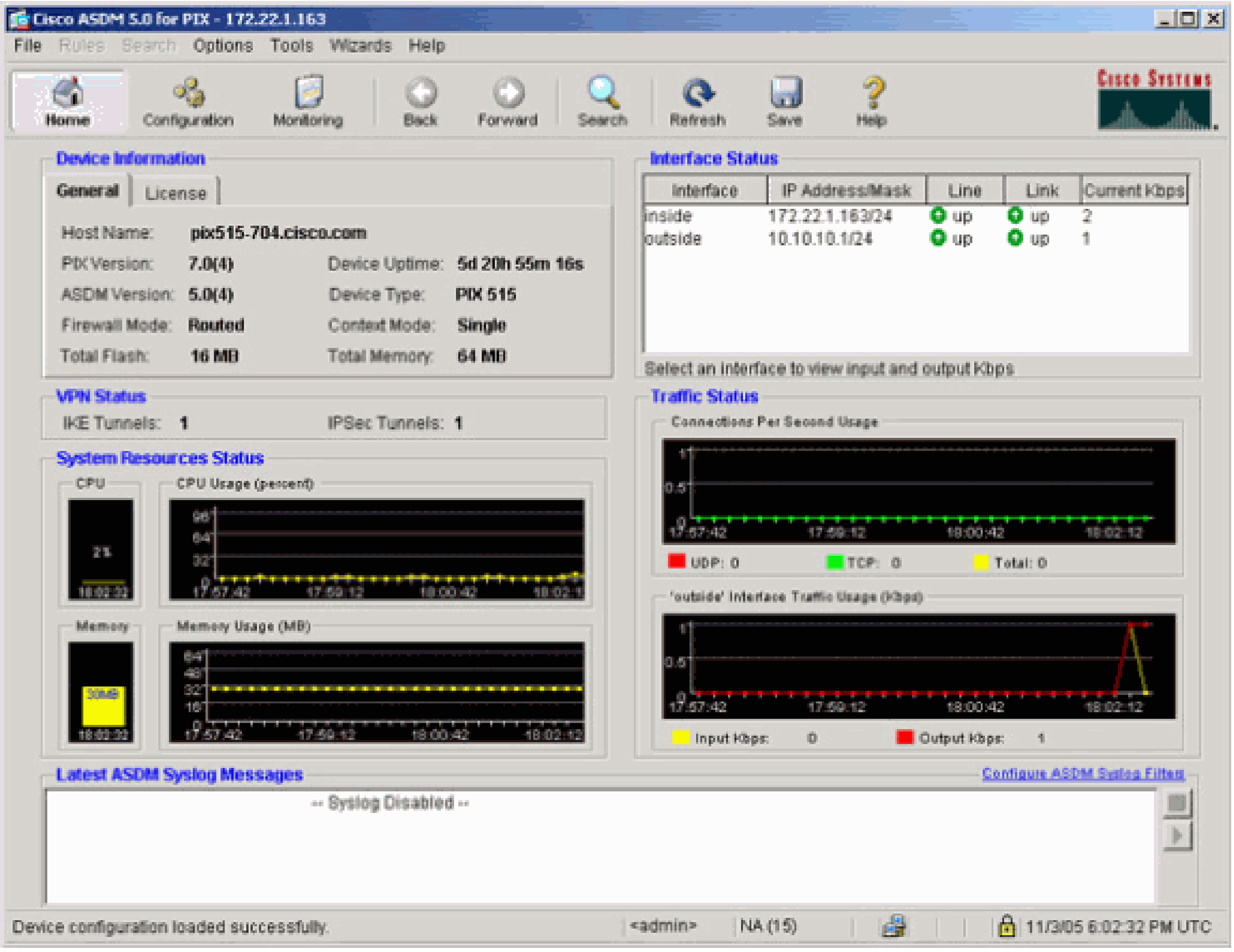
驗證

使用本節內容，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) (OIT)支援某些show指令。使用OIT檢視對show命令輸出的分析。

如果有到對等體的相關流量，則在pix515-704和PIX-02之間建立隧道。

1. 在ASDM中檢視Home下的VPN狀態以驗證隧道是否已形成。



Device Information

Host Name:	pix515-704.cisco.com		
PIX Version:	7.0(4)	Device Uptime:	5d 20h 55m 16s
ASDM Version:	5.0(4)	Device Type:	PIX 515
Firewall Mode:	Routed	Context Mode:	Single
Total Flash:	16 MB	Total Memory:	64 MB

Interface Status

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.22.1.163/24	up	up	2
outside	10.10.10.1/24	up	up	1

Select an interface to view input and output Kbps

VPN Status

IKE Tunnels: 1　　IPSec Tunnels: 1

System Resources Status

CPU: 2%　18:02:32

Memory: 30MB　18:02:32

Traffic Status

UDP: 0　TCP: 0　Total: 0

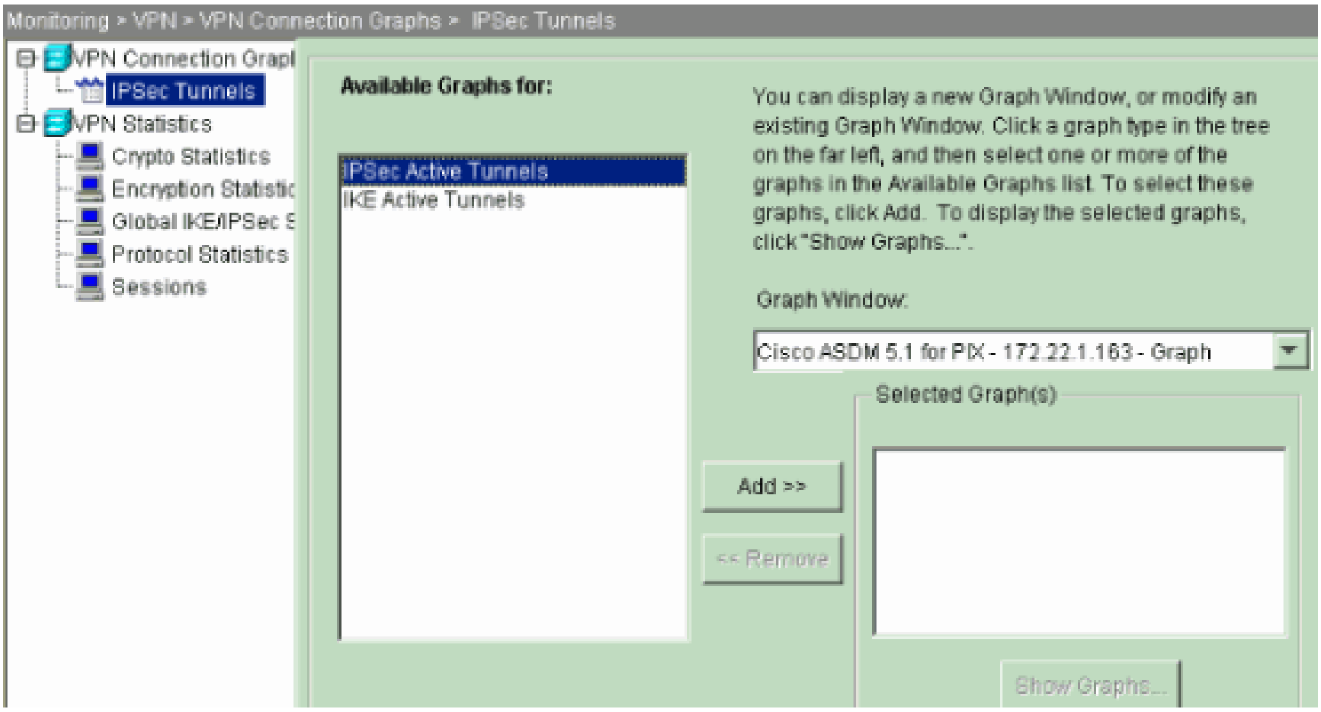
Input Kbps: 0　Output Kbps: 1

Latest ASDM Syslog Messages

-- Syslog Disabled --

Device configuration loaded successfully.　<admin>　NA (15)　11/3/05 6:02:32 PM UTC

2. 選擇Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels以驗證有關建立隧道的詳細資料。



Available Graphs for:

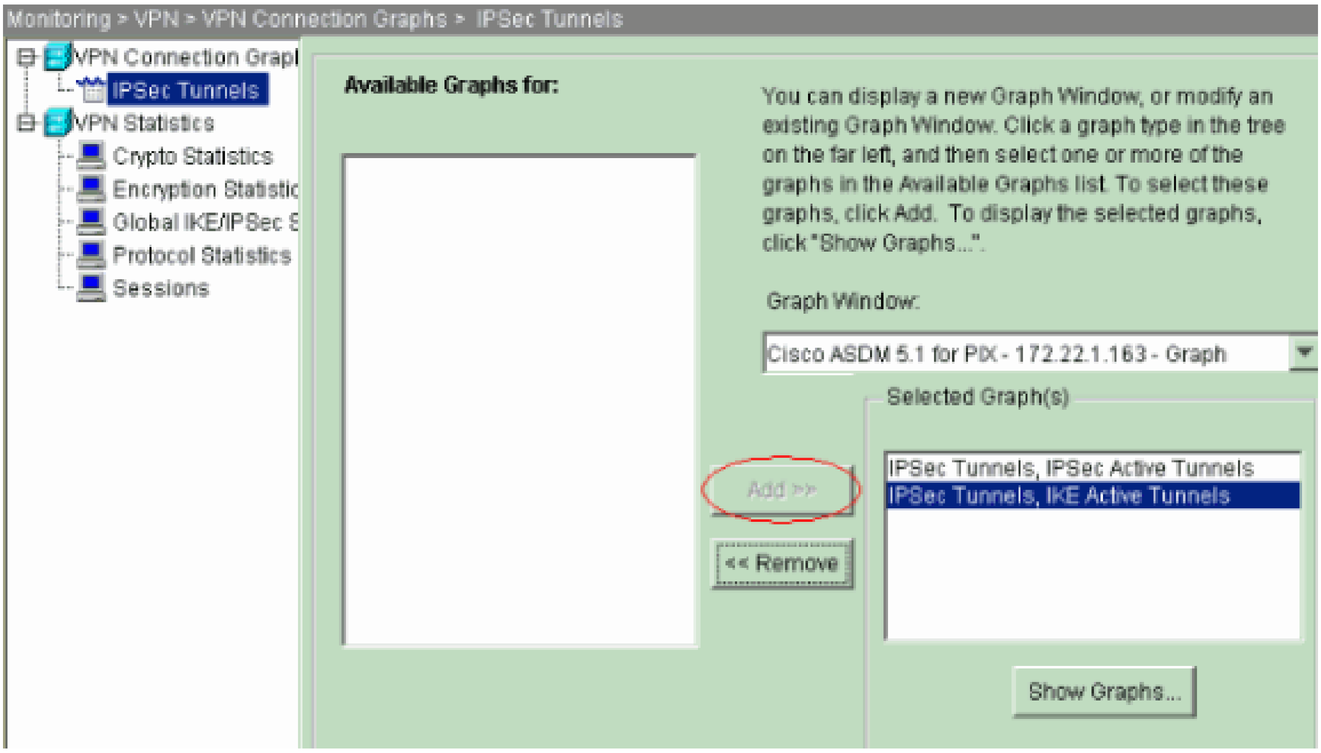
IPSec Active Tunnels
IKE Active Tunnels

You can display a new Graph Window, or modify an existing Graph Window. Click a graph type in the tree on the far left, and then select one or more of the graphs in the Available Graphs list. To select these graphs, click Add. To display the selected graphs, click "Show Graphs...".

Graph Window: Cisco ASDM 5.1 for PIX - 172.22.1.163 - Graph

Selected Graph(s)

3. 點選增加選擇可用的圖表以在圖表窗口中檢視。



Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels

You can display a new Graph Window, or modify an existing Graph Window. Click a graph type in the tree on the far left, and then select one or more of the graphs in the Available Graphs list. To select these graphs, click Add. To display the selected graphs, click "Show Graphs...".

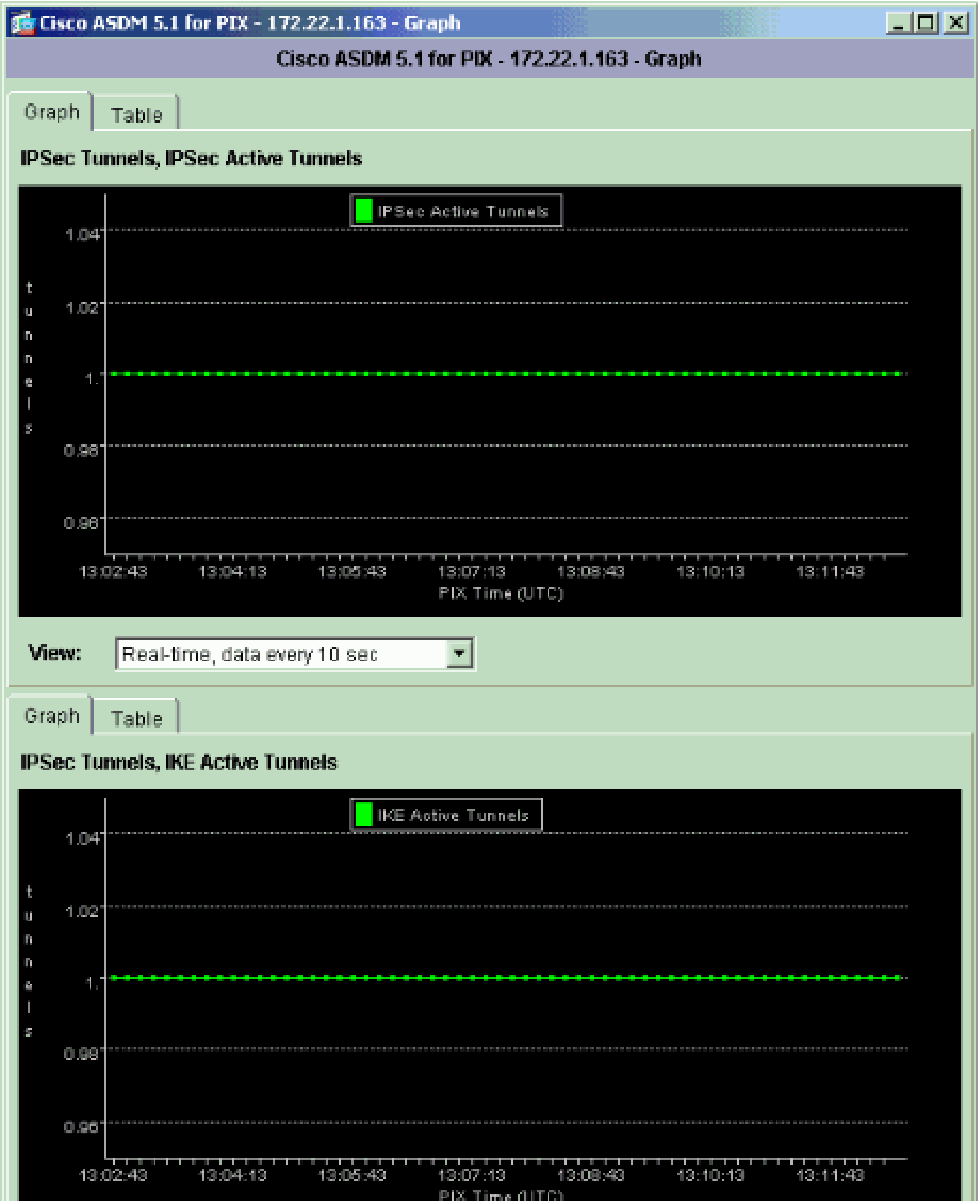
Graph Window: Cisco ASDM 5.1 for PIX - 172.22.1.163 - Graph

Selected Graph(s)

IPSec Tunnels, IPSec Active Tunnels

IPSec Tunnels, IKE Active Tunnels

4. 按一下Show Graphs以檢視IKE和IPSec活動隧道圖。



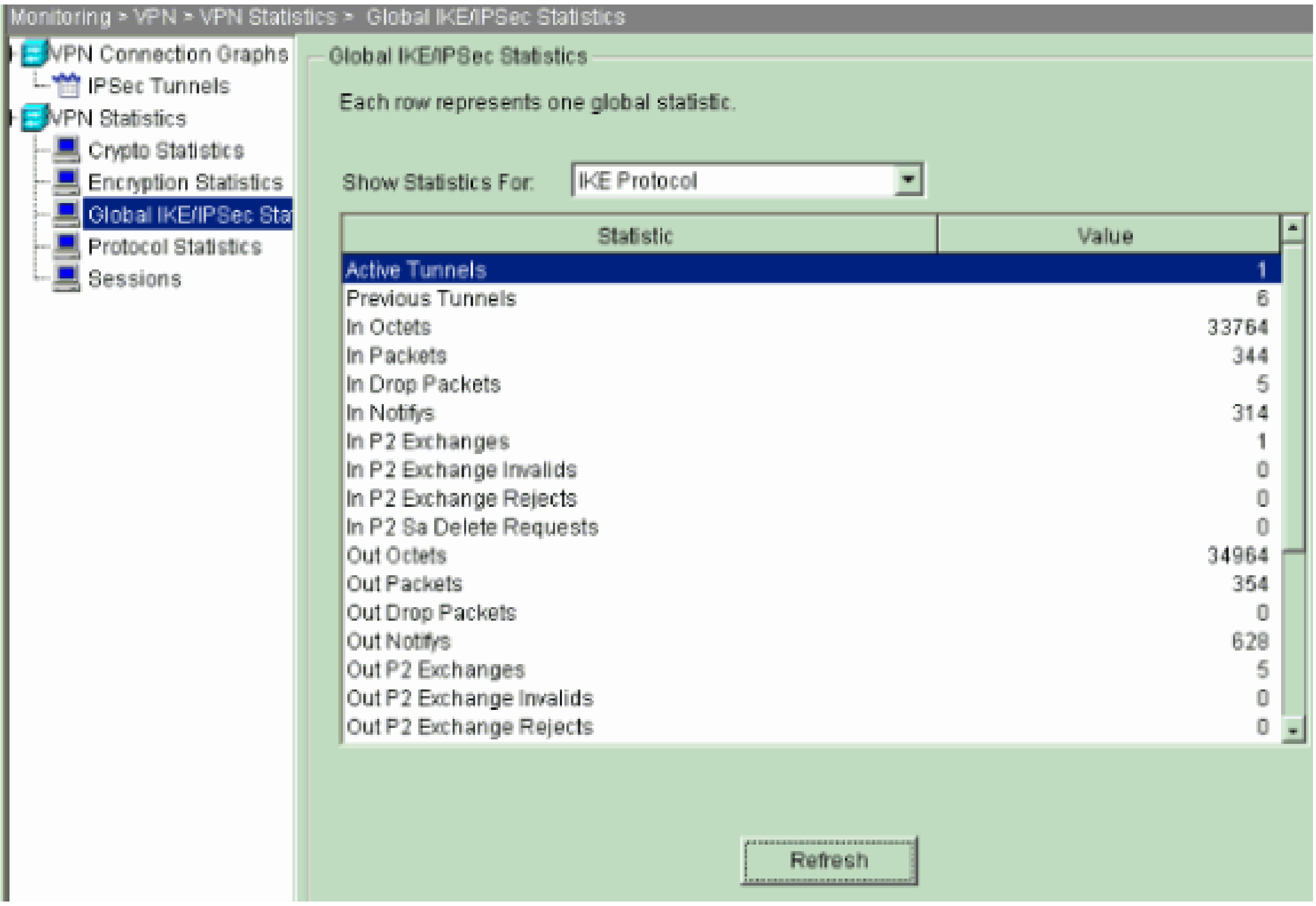
Cisco ASDM 5.1 for PIX - 172.22.1.163 - Graph

IPSec Tunnels, IPSec Active Tunnels

View: Real-time, data every 10 sec

IPSec Tunnels, IKE Active Tunnels

5. 選擇Monitoring > VPN > VPN Statistics > Global IKE/IPSec Statistics以瞭解有關VPN隧道的統計資訊。



Global IKE/IPSec Statistics

Each row represents one global statistic.

Show Statistics For: IKE Protocol

Statistic	Value
Active Tunnels	1
Previous Tunnels	6
In Octets	33764
In Packets	344
In Drop Packets	5
In Notifys	314
In P2 Exchanges	1
In P2 Exchange Invalids	0
In P2 Exchange Rejects	0
In P2 Sa Delete Requests	0
Out Octets	34964
Out Packets	354
Out Drop Packets	0
Out Notifys	628
Out P2 Exchanges	5
Out P2 Exchange Invalids	0
Out P2 Exchange Rejects	0

您還可以使用CLI驗證隧道是否已形成。發出show crypto isakmp sa命令可檢查隧道是否已形成，發出 show crypto ipsec sa命令可觀察已執行了封裝、加密等操作的資料包的數量。

pix515-704

<#root>

```
pixfirewall(config)#

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: 10.20.20.1
    Type    :

L2L

             Role    : initiator
    Rekey   : no                State   :

MM_ACTIVE
```

pix515-704

```
<#root>

pixfirewall(config)#

show crypto ipsec sa

interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 10.10.10.1

     access-list outside_cryptomap_20 permit ip 172.22.1.0
       255.255.255.0 172.16.1.0 255.255.255.0
     local ident (addr/mask/prot/port):

(172.22.1.0/255.255.255.0/0/0)

     remote ident (addr/mask/prot/port):

(172.16.1.0/255.255.255.0/0/0)

     current_peer: 10.20.20.1

      #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: 20, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.:

10.10.10.1

, remote crypto endpt.:

10.20.20.1


      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 44532974

    inbound esp sas:
      spi: 0xA87AD6FA (2826622714)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3824998/28246)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x44532974 (1146300788)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3824998/28245)
         IV size: 16 bytes
         replay detection support: Y
```

疑難排解

PFS

在IPsec協商中，完全正向保密(PFS)可確保每個新加密金鑰與之前的任何金鑰無關。啟用或停用兩個隧道對等體上的PFS，否則不會在PIX/ASA中建立L2L IPsec隧道。

PFS預設為停用。要啟用PFS，請在組策略配置模式下使用pfs命令並指定enable關鍵字。要停用PFS，請輸入disable關鍵字。

```
<#root>
hostname(config-group-policy)#
pfs {enable | disable}
```

要從正在運行的配置中刪除PFS屬性，請輸入此命令的no形式。組策略可以從其他組策略繼承PFS的值。輸入此命令的no形式，以防止繼承值。

```
<#root>
hostname(config-group-policy)#
no pfs
```

管理-訪問

本節提供的資訊可用於對組態進行疑難排解。

除非在全局配置模式下配置management-access 命令，否則無法從隧道的另一端對PIX的內部介面執行ping操作。

```
<#root>
PIX-02(config)#
management-access inside
PIX-02(config)#
show management-access
management-access inside
```

調試命令

注意：發出debug命令之前，請參閱有關Debug命令的重要資訊。

debug crypto isakmp— 顯示有關IPsec連線的調試資訊，並顯示由於兩端不相容而被拒絕的第一組屬性。

debug crypto isakmp

<#root>

```
pixfirewall(config)#

debug crypto isakmp 7

Nov 27 12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire message,
spi 0x0
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE Initiator: New Phase 1,
Intf 2, IKE Peer 10.20.20.1  local Proxy Address 172.22.1.0, remote
Proxy Address 172.16.1.0,  Crypto map (outside_map)
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ISAKMP SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Fragmentation
VID + extended capabilities payload
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
(msgid=0) with payloads : HDR +
 SA (1) + VENDOR (13) + NONE (0) total length : 148
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included
IKE fragmentation capability flags
:

Main Mode

:        True  Aggressive Mode:  True
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/
Cisco VPN3000/Cisco ASA GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) total length
 : 320
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 320
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA_KE payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA
spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA
```

```
GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys
for Initiator...
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing IOS keep alive payload: proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing dpd vid payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) +
NONE (0) total length : 119
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) +
NONE (0) total length : 96
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing IOS keep alive payload: proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Received DPD VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Oakley begin quick mode
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,

PHASE 1 COMPLETED

Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Starting phase 1 rekey timer: 73440000 (ms)
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got
SPI from key engine: SPI = 0x44ae0956
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
oakley constucting quick mode
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing blank hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing IPSec SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing IPSec nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing proxy ID
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Transmitting Proxy Id:
  Local subnet:  172.22.1.0  mask 255.255.255.0 Protocol 0  Port 0
  Remote subnet: 172.16.1.0  Mask 255.255.255.0 Protocol 0  Port 0
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing qm hash payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
(msgid=d723766b) with payloads
```

```
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) +
NONE (0) total length : 200
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message
(msgid=d723766b) with payloads
 : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
 total length : 172
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
loading all IPSEC SAs
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
Security negotiation complete for LAN-to-LAN Group (10.20.20.1)
Initiator, Inbound SPI = 0x44ae0956, Outbound SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
oakley constructing final quick mode
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
IKE got a KEY_ADD msg for SA: SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Pitcher: received KEY_UPDATE, spi 0x44ae0956
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
 Starting P2 Rekey timer to expire in 24480 seconds
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,

PHASE 2 COMPLETED

 (msgid=d723766b)
```

debug crypto ipsec -顯示有關IPsec連線的調試資訊。

debug crypto ipsec

<#root>

```
pix1(config)#

debug crypto ipsec 7


exec mode commands/options:
  <1-255>  Specify an optional debug level (default is 1)
  <cr>
pix1(config)# debug crypto ipsec 7
pix1(config)# IPSEC: New embryonic SA created @ 0x024211B0,
    SCB: 0x0240AEB0,
    Direction: inbound
    SPI      : 0x2A3E12BE
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0,
    SCB: 0x0240B710,
    Direction: outbound
    SPI      : 0xB283D32F
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xB283D32F
IPSEC: Updating outbound VPN context 0x02422618, SPI 0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: New outbound permit rule, SPI 0xB283D32F
    Src addr: 10.10.10.1
    Src mask: 255.255.255.255
    Dst addr: 10.20.20.1
    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: 0xB283D32F
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: Completed host IBSA update, SPI 0x2A3E12BE
IPSEC: Creating inbound VPN context, SPI 0x2A3E12BE
    Flags: 0x00000006
    SA   : 0x024211B0
    SPI  : 0x2A3E12BE
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x02422618
    SCB  : 0x0240AEB0
    Channel: 0x014A45B0
IPSEC: Completed inbound VPN context, SPI 0x2A3E12BE
    VPN handle: 0x0240BF80
```

```
IPSEC: Updating outbound VPN context 0x02422618, SPI 0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0240BF80
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: New inbound tunnel flow rule, SPI 0x2A3E12BE
    Src addr: 172.16.1.0
    Src mask: 255.255.255.0
    Dst addr: 172.22.1.0
    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 0x2A3E12BE
    Rule ID: 0x0240B108
IPSEC: New inbound decrypt rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    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: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x2A3E12BE
    Rule ID: 0x02406E98
IPSEC: New inbound permit rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    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: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x2A3E12BE
    Rule ID: 0x02422C78
```

相關資訊

- 使用PDM在防火牆之間建立冗餘隧道
- Cisco PIX防火牆軟體
- 思科調適型資安裝置管理員
- Cisco ASA 5500系列調適型安全裝置
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems

關於此翻譯