PIX/ASA 7.x以上：PIX到PIX VPN隧道配置示例

目录

简介

本文介绍使用 Cisco 自适应安全设备管理器 (ASDM) 在两个 PIX 防火墙之间配置 VPN 隧道的过程。ASDM 是基于应用程序的配置工具，用于帮助您通过 GUI 来设置、配置和监控 PIX 防火墙。PIX 防火墙被放置在两个不同的站点。

可以使用 IPsec 形成隧道。IPsec 是在 IPsec 对等体之间提供数据机密性、数据完整性和数据原始身份验证的开放标准组合。

注意： 在 PIX 7.1 及更高版本中，**sysopt connection permit-ipsec** 命令已更改为 sysopt connection permit-vpn。此命令允许通过 VPN 隧道进入安全设备并随后被解密的数据流绕过接口访问列表。组策略和每用户授权访问列表仍然适用于数据流。要禁用此功能，请使用此命令的 **no** 形式。在 CLI 配置中，此命令不可见。

要了解有关 Cisco PIX 安全设备运行软件版本 6.x 的相同方案的详细信息，请参阅 PIX 6.x：简单的 PIX 到 PIX VPN 隧道配置示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息指定此对等体将启动第一个专用交换以确定要连接到的相应对等体。

- Cisco PIX 500 系列安全设备（已安装版本 7.x 及更高版本）
- ASDM 版本 5.x 及更高版本

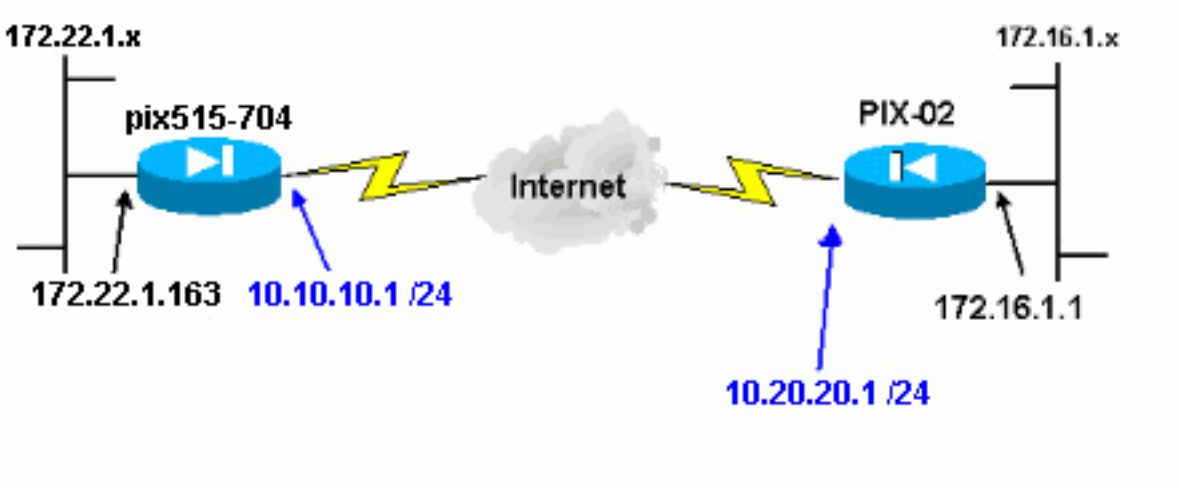
注意： 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

注意： ASA 5500 系列版本 7.x/8.x 运行 PIX 版本 7.x/8.x 中可以看到的同一软件。本文档中的配置适用于这两个产品系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

IPsec 协商可分为五个步骤，并且包括两个 Internet 密钥交换 (IKE) 阶段。

1. IPsec 隧道由相关数据流启动。如果数据流在 IPsec 对等体之间传输，则它会被认为是相关数据流。
2. 在 IKE 第 1 阶段中，IPsec 对等体对建立的 IKE 安全关联 (SA) 策略进行协商。对等体经过身份验证后，会使用 Internet 安全关联和密钥管理协议 (ISAKMP) 创建安全隧道。
3. 在 IKE 第 2 阶段中，IPsec 对等体使用经身份验证的安全隧道对 IPsec SA 转换进行协商。共享策略的协商决定建立 IPsec 隧道的方式。
4. 根据 IPsec 转换集中配置的 IPsec 参数，将在 IPsec 对等体之间创建 IPsec 隧道并传输数据。
5. 如果删除了 IPsec SA，或者 IPsec SA 的生存时间到期，则 IPsec 隧道将终止。**注意：** 如果

两个 IKE 阶段中的 SA 在对等体上不匹配，则两个 PIX 之间的 IPsec 协商将失败。

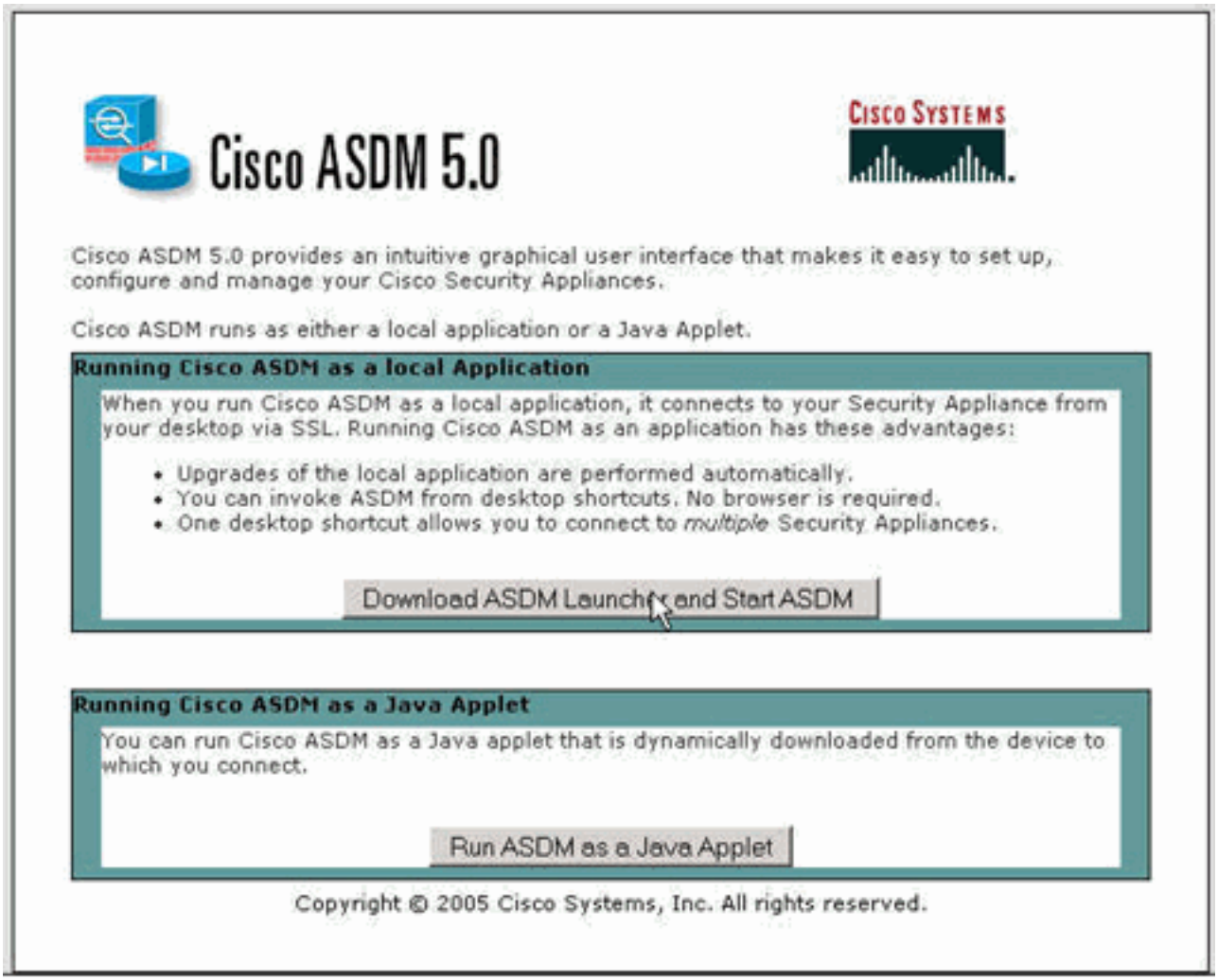
配置

- ASDM 配置
- PIX CLI 配置

ASDM 配置

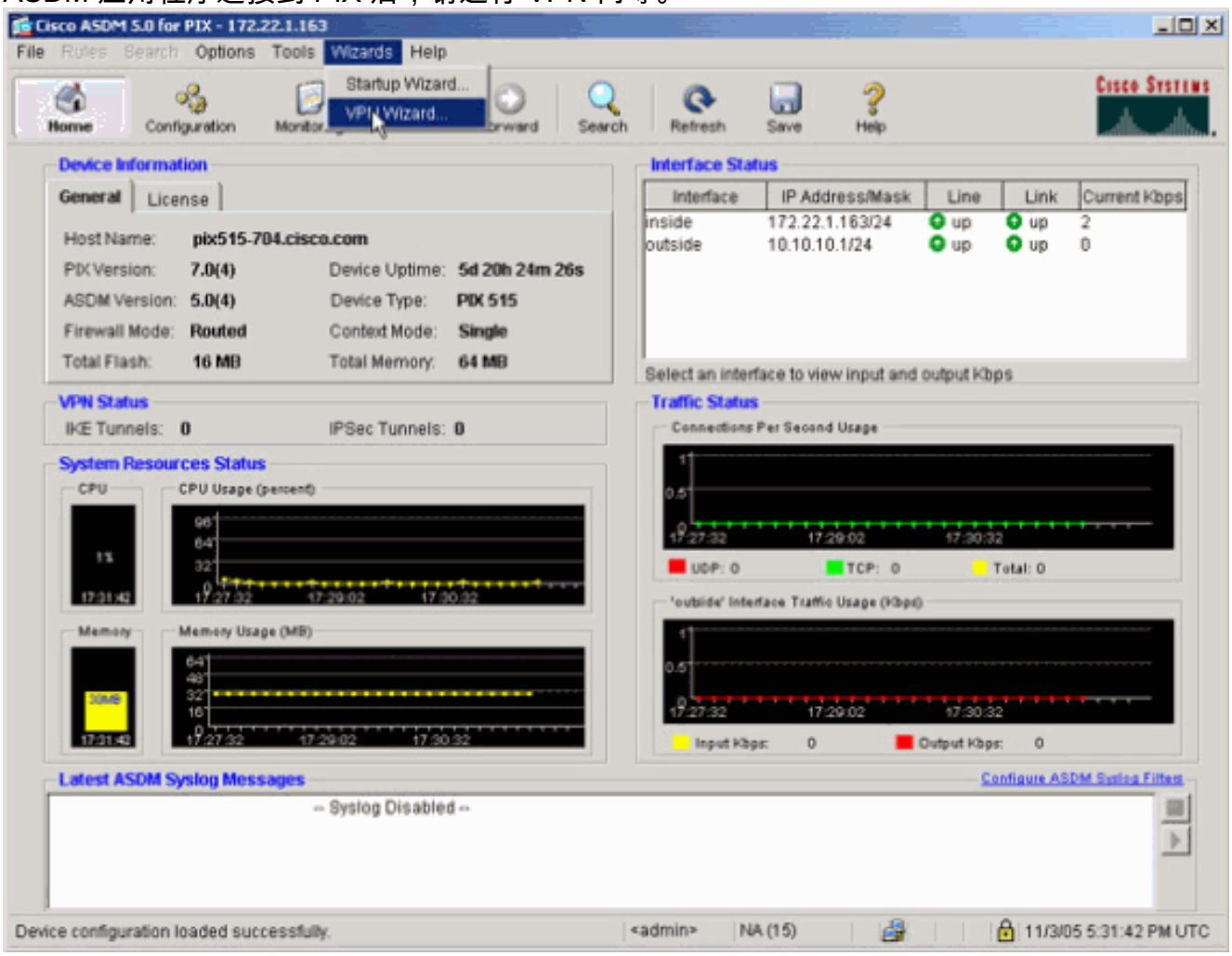
完成这些步骤：

1. 打开浏览器并键入 **https:// <Inside_IP_Address_of_PIX>** 以访问 PIX 上的 ASDM。请确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空。PIX 显示此窗口以允许下载 ASDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。

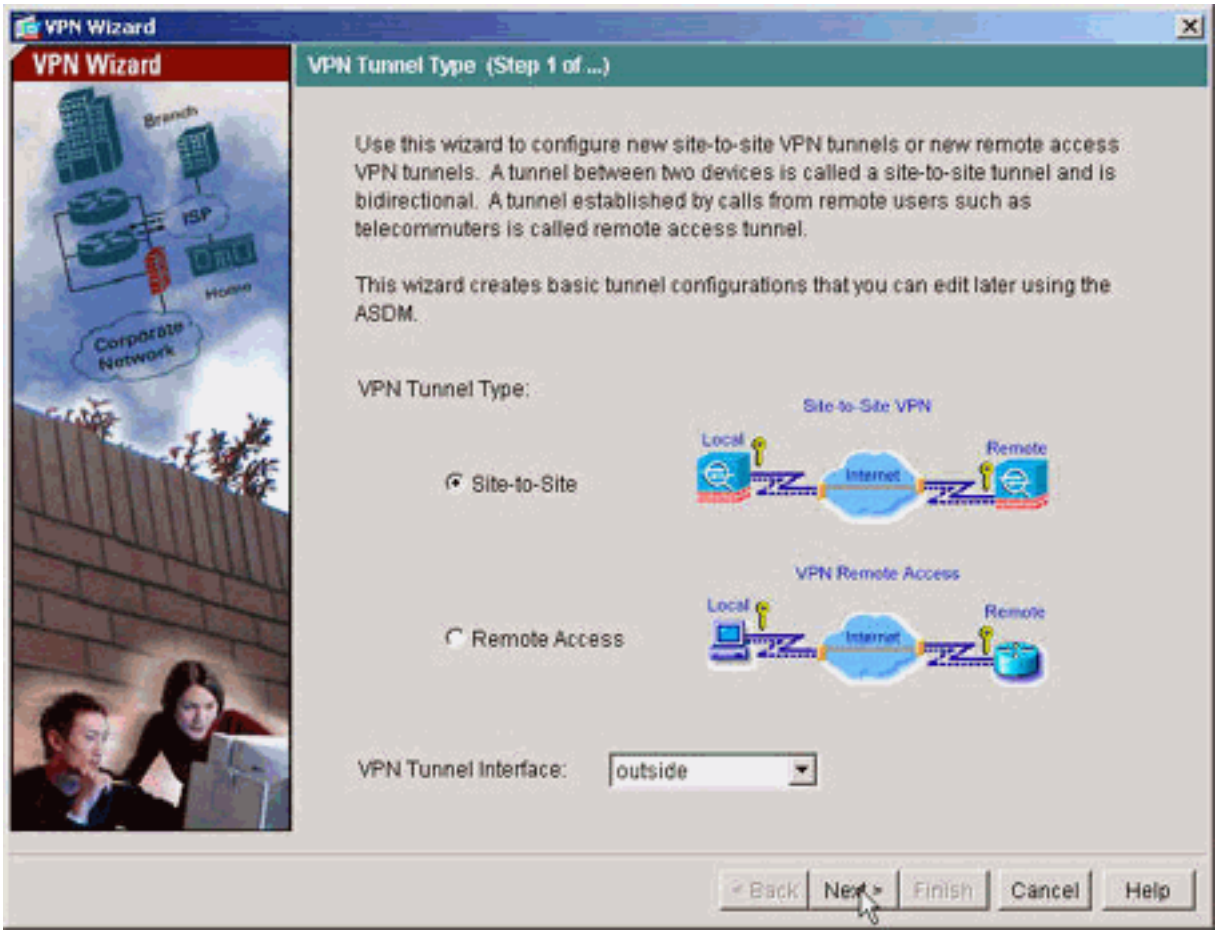


2. 单击 **Download ASDM Launcher and Start ASDM** 以下载 ASDM 应用程序的安装程序。
3. 下载 ASDM 启动程序后，按照提示安装软件并运行 Cisco ASDM 启动程序。
4. 输入使用 **http -** 命令配置的接口的 IP 地址，以及用户名和口令（如果已指定）。此示例使用默认空白用户名和口令。

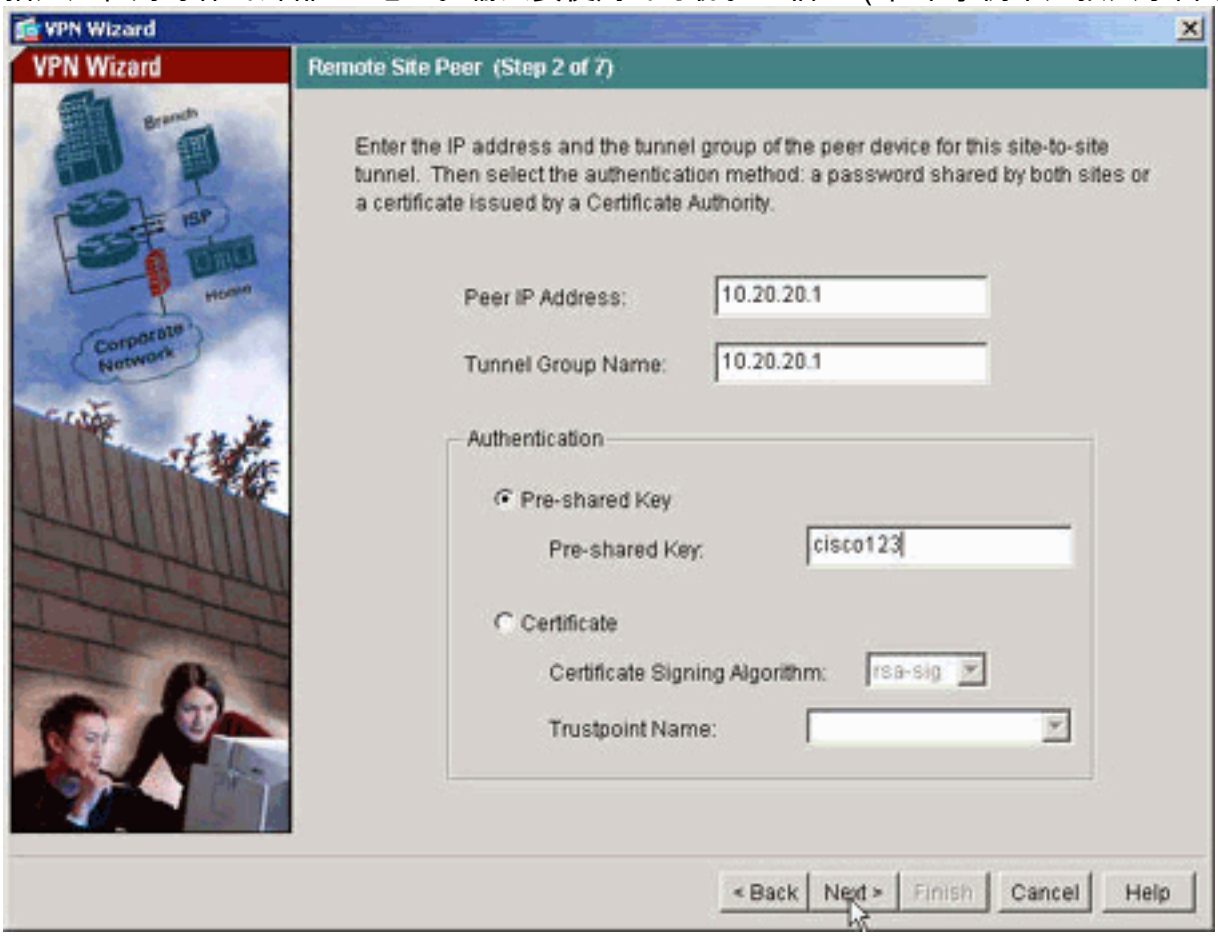
5. ASDM 应用程序连接到 PIX 后，请运行 VPN 向导。



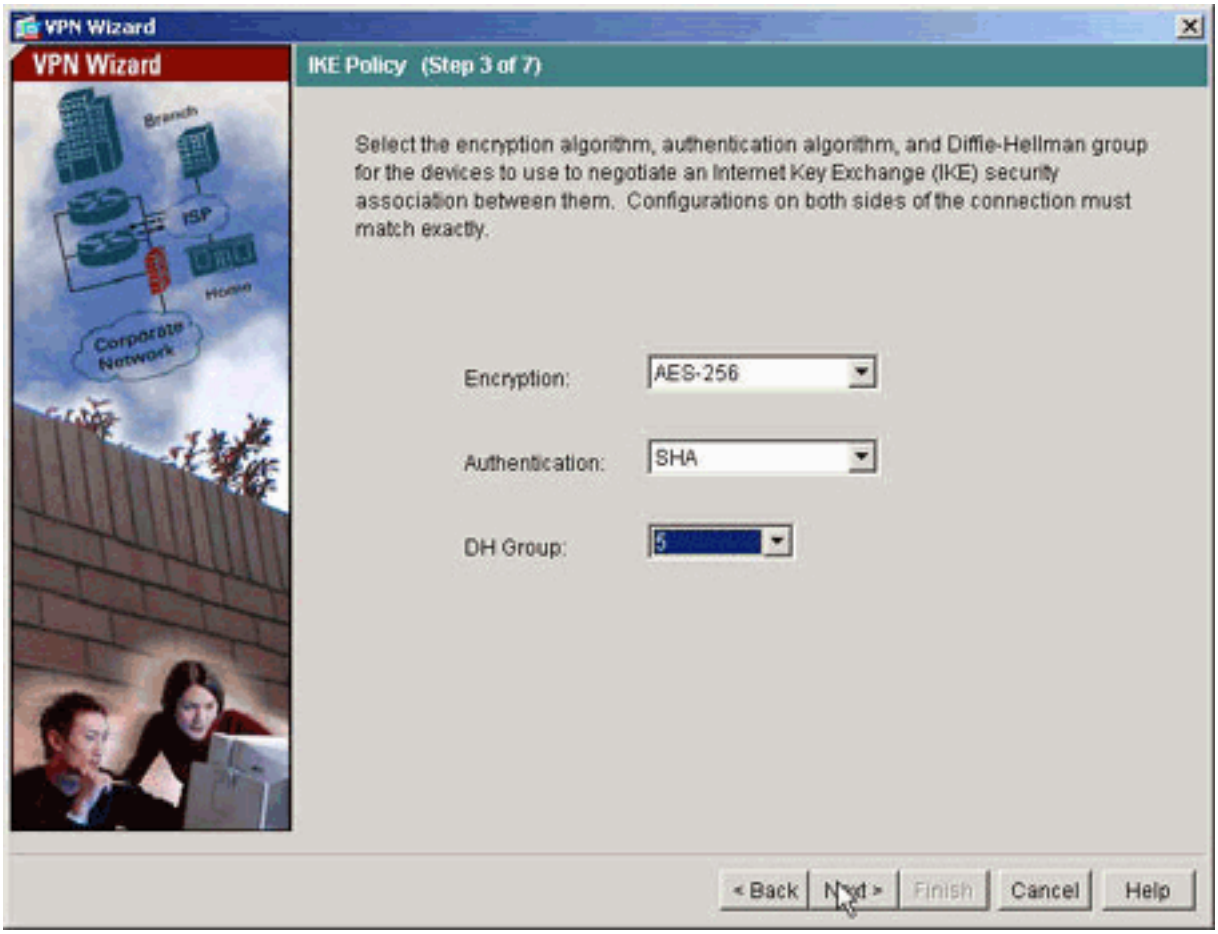
6. 选择 Site-to-Site VPN 隧道类型。



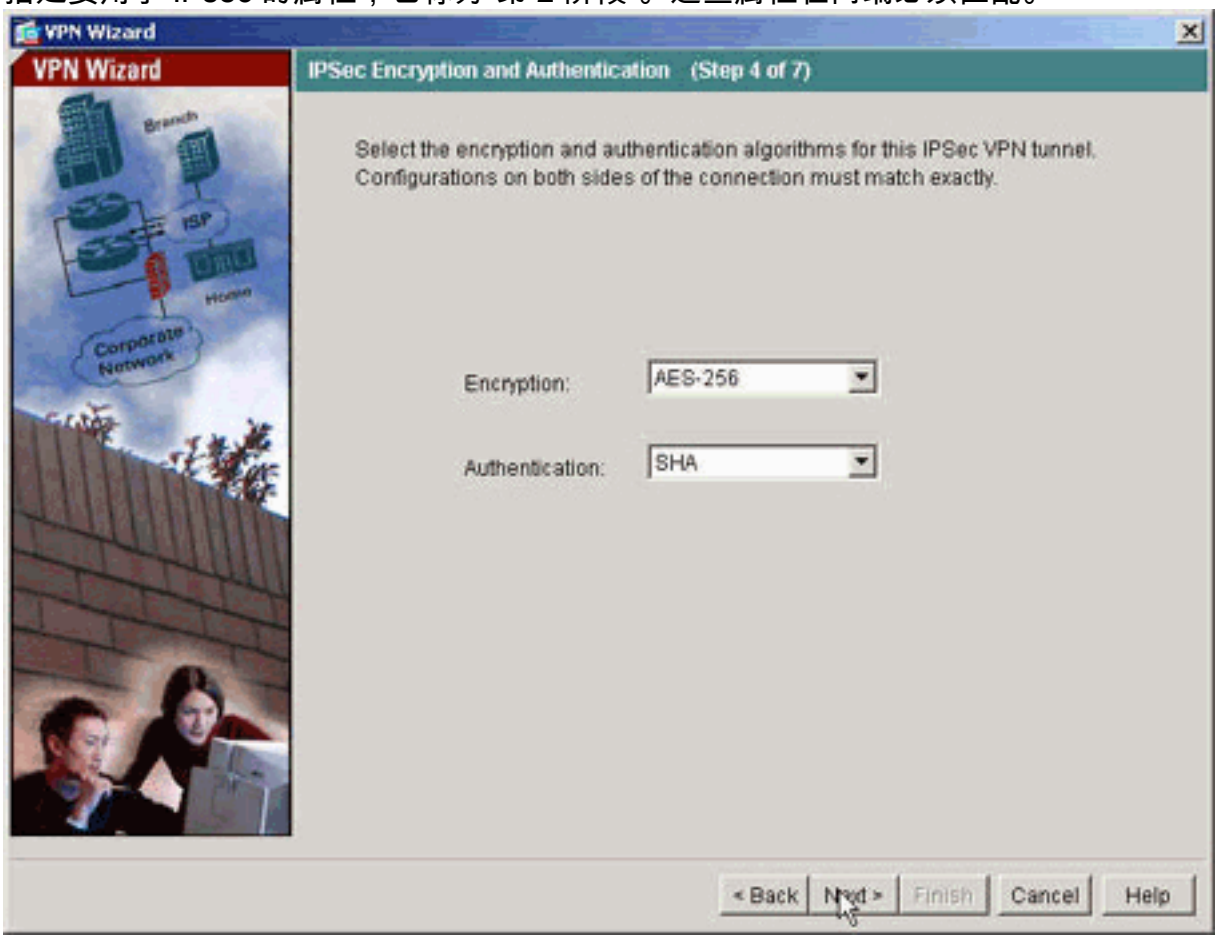
7. 指定远程对等体的外部 IP 地址。输入要使用的身份验证信息（在本示例中是预共享密钥）。



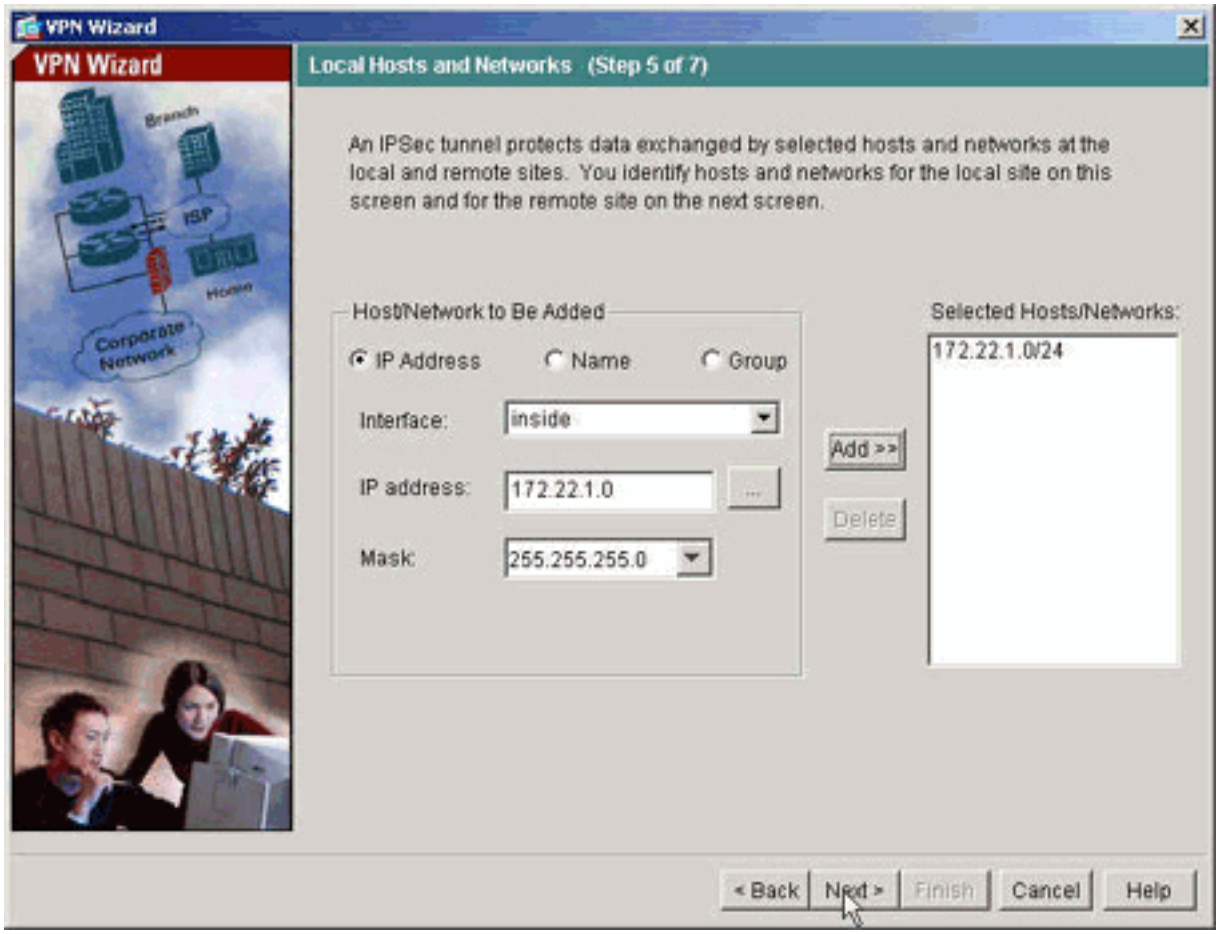
8. 指定要用于 IKE 的属性，也称为“第 1 阶段”。这些属性在隧道两端必须是相同的。



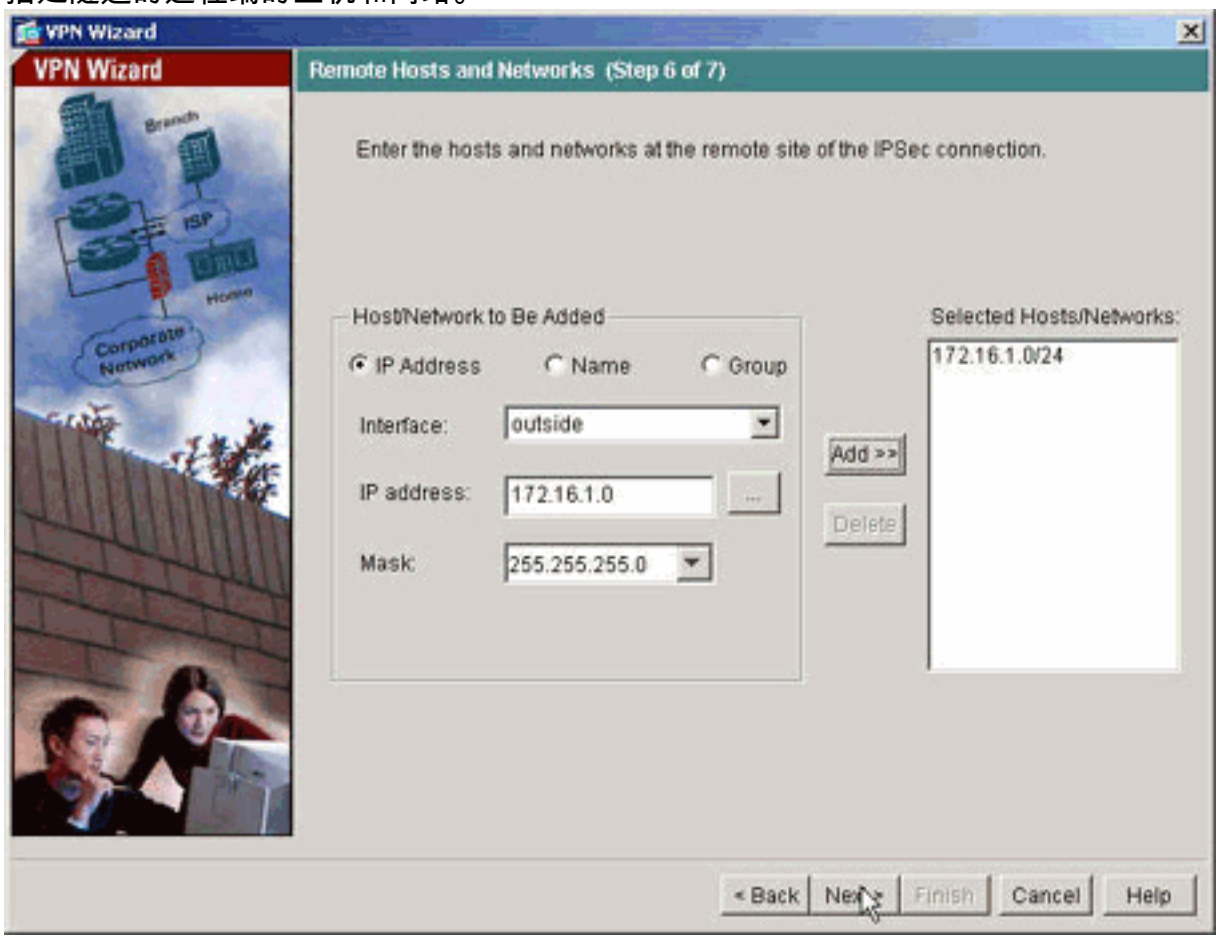
9. 指定要用于 IPsec 的属性，也称为“第 2 阶段”。这些属性在两端必须匹配。



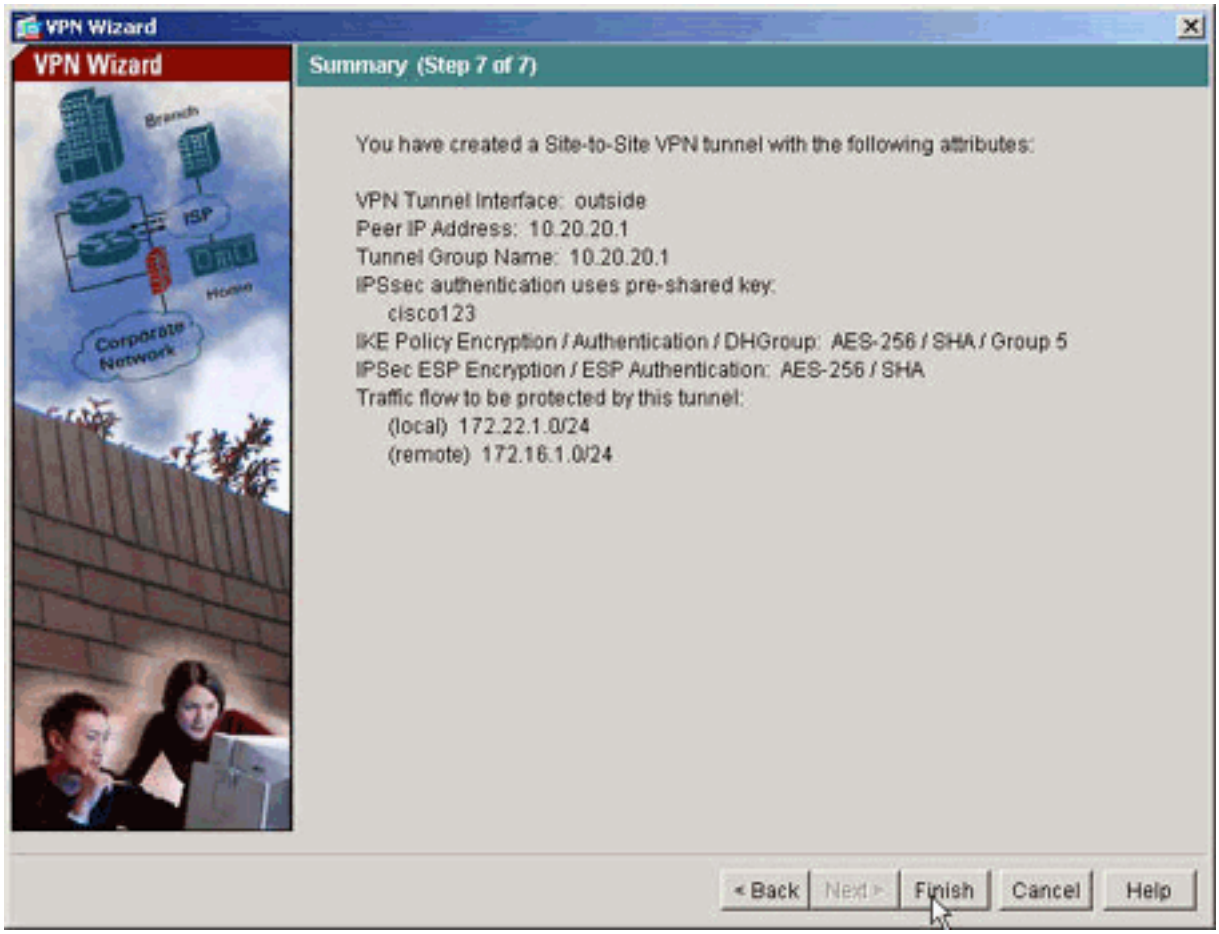
10. 指定应允许其数据流通过 VPN 隧道的主机。在此步骤中，指定 pix515-704 的本地主机。



11. 指定隧道的远程端的主机和网络。



12. 此概要中显示了通过 VPN 向导定义的属性。仔细检查配置，如果您确保设置正确，请单击 **Finish**。



PIX CLI 配置

pix515-704

```
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 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-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_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 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

```
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#
```

备用站点到站点隧道

要为此加密映射条目指定备用站点到站点功能的连接类型，请在全局配置模式下使用 **crypto map set connection-type** 命令。请使用此命令的 no 形式以返回到默认设置。

语法：

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

- **answer-only** - 用于指定此对等体在初始专用交换期间最初只对入站 IKE 连接做出响应，以确定要连接到的相应对等体。
- **bidirectional** - 用于指定此对等体可根据此加密映射条目接受和发起连接。这是所有站点到站点连接的默认连接类型。
- **originate-only** - 用于指定此对等体将发起第一个专用交换以确定要连接到的相应对等体。

crypto map set connection-type 命令为备用 LAN 到 LAN 功能指定连接类型。它允许在连接的一端指定多个备用对等体。此功能仅在以下平台之间工作：

- 两台 Cisco ASA 5500 系列安全设备
- Cisco ASA 5500 系列安全设备和 Cisco VPN 3000 集中器
- Cisco ASA 5500 系列安全设备和运行 Cisco PIX 安全设备软件版本 7.0 或更高版本的安全设备

要配置备用 LAN 到 LAN 连接，Cisco 建议您使用 originate-only 关键字将连接的一端配置为“只发起”，并使用 answer-only 关键字将具有多个备用对等体的一端配置为“只应答”。在“只发起”端上，请使用 **crypto map set peer** 命令对对等体的优先级进行排序。“只发起”安全设备尝试与列表中的第一个对等体协商。如果该对等体不响应，则安全设备会按照顺序与列表中的下一个对等体协商，直到对等体做出响应或在列表中不再有对等体。

用这种方式配置后，“只发起”对等体最初将尝试建立一条专用隧道，并与对等体协商。然后，任一个对等体都可建立一个正常的 LAN 到 LAN 的连接，并且来自任一端的数据都可发起隧道连接。

注意： 如果在一个加密条目中为 VPN 配置了多个对等 IP 地址，则一旦主对等体断开，将使用备用对等 IP 建立该 VPN。不过，一旦主对等体恢复，该 VPN 不会抢占主 IP 地址。必须手动删除现有 SA 才能重新启动 VPN 协商以将它切换到主 IP 地址。作为结论，站点到站点隧道不支持 VPN 抢占。

支持的备用 LAN 到 LAN 连接类型

远程端	中心端
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

示例

此示例（在全局配置模式下输入）配置 **crypto map mymap**，并将连接类型设置为 *originate-only*。

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

清除安全关联 (SA)

在 PIX 的特权模式下，使用以下命令：

- **clear [crypto] ipsec sa** - 删除活动 IPsec SA。关键字 **crypto** 是可选的。
- **clear [crypto] isakmp sa** - 删除活动 IKE SA。关键字 **crypto** 是可选的。

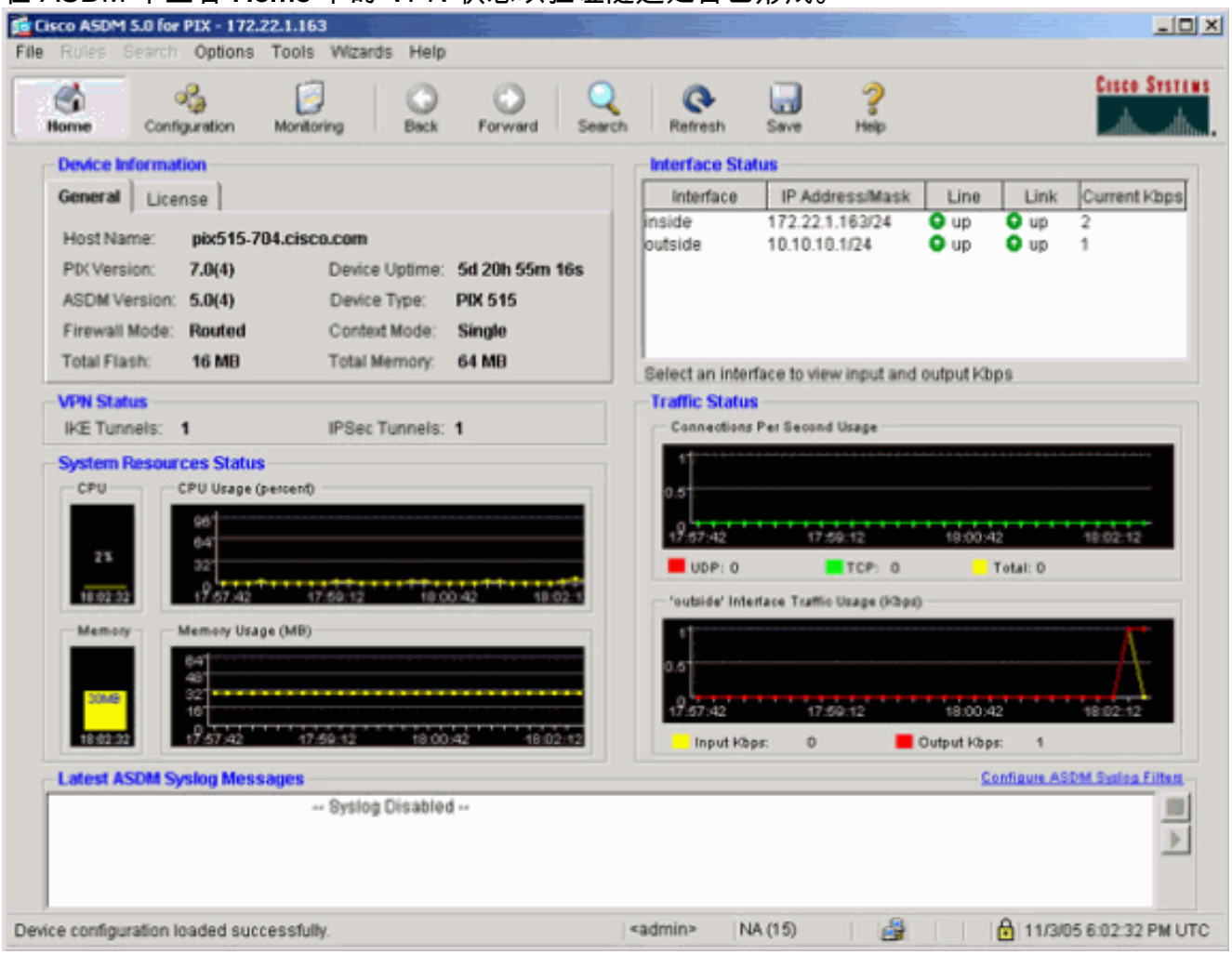
验证

使用本部分可确认配置能否正常运行。

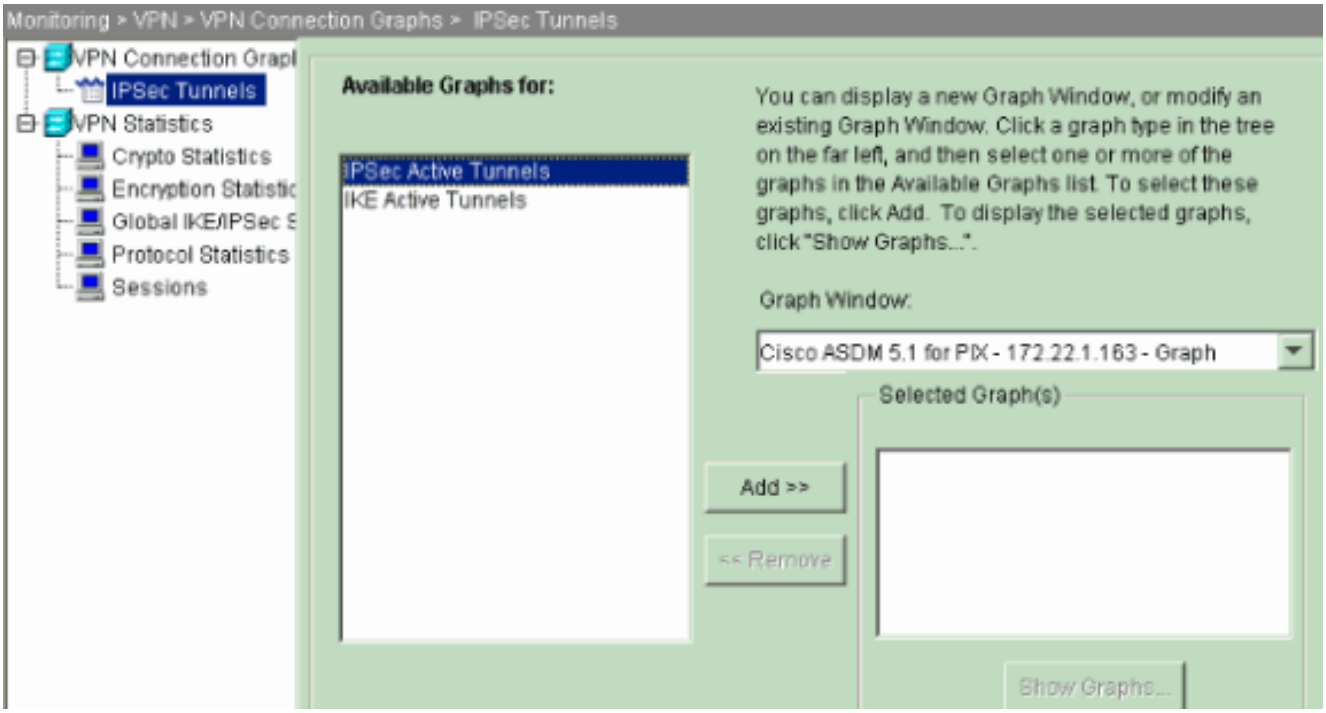
命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

如果有流向对等体的相关数据流，则将在 pix515-704 和 PIX-02 之间建立隧道。

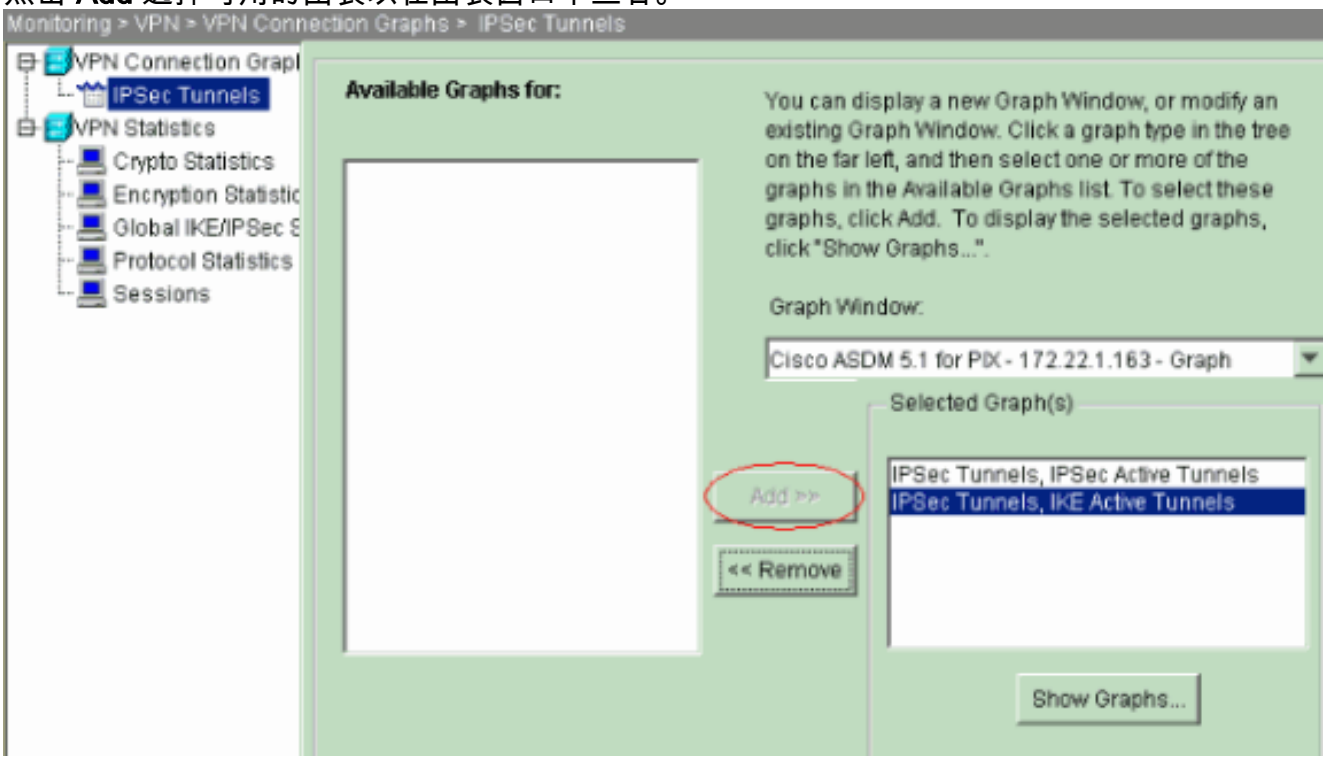
1. 在 ASDM 中查看 **Home** 下的 VPN 状态以验证隧道是否已形成。



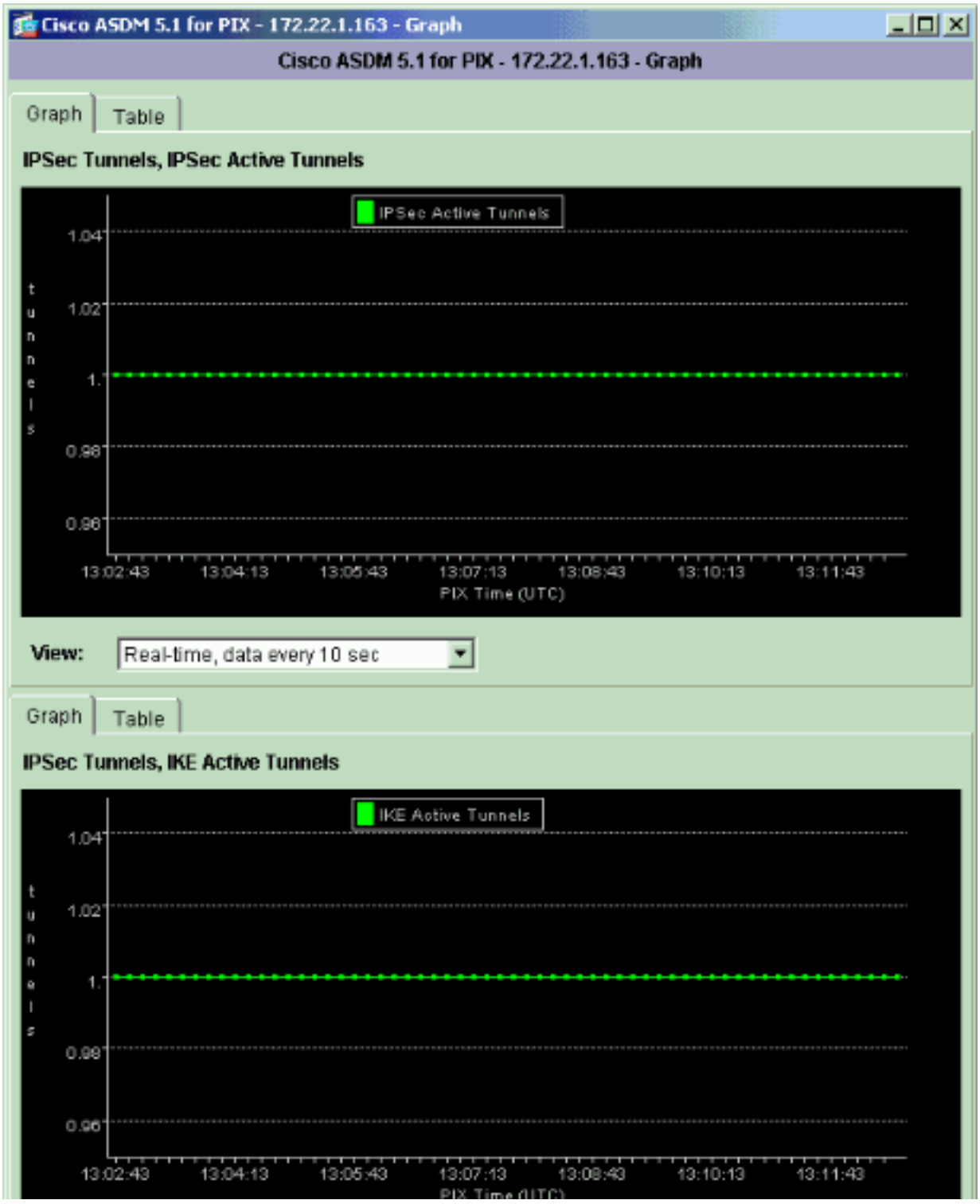
2. 选择 **Monitoring> VPN > VPN Connection Graphs > IPSec Tunnels** 以验证有关建立隧道的详细资料。



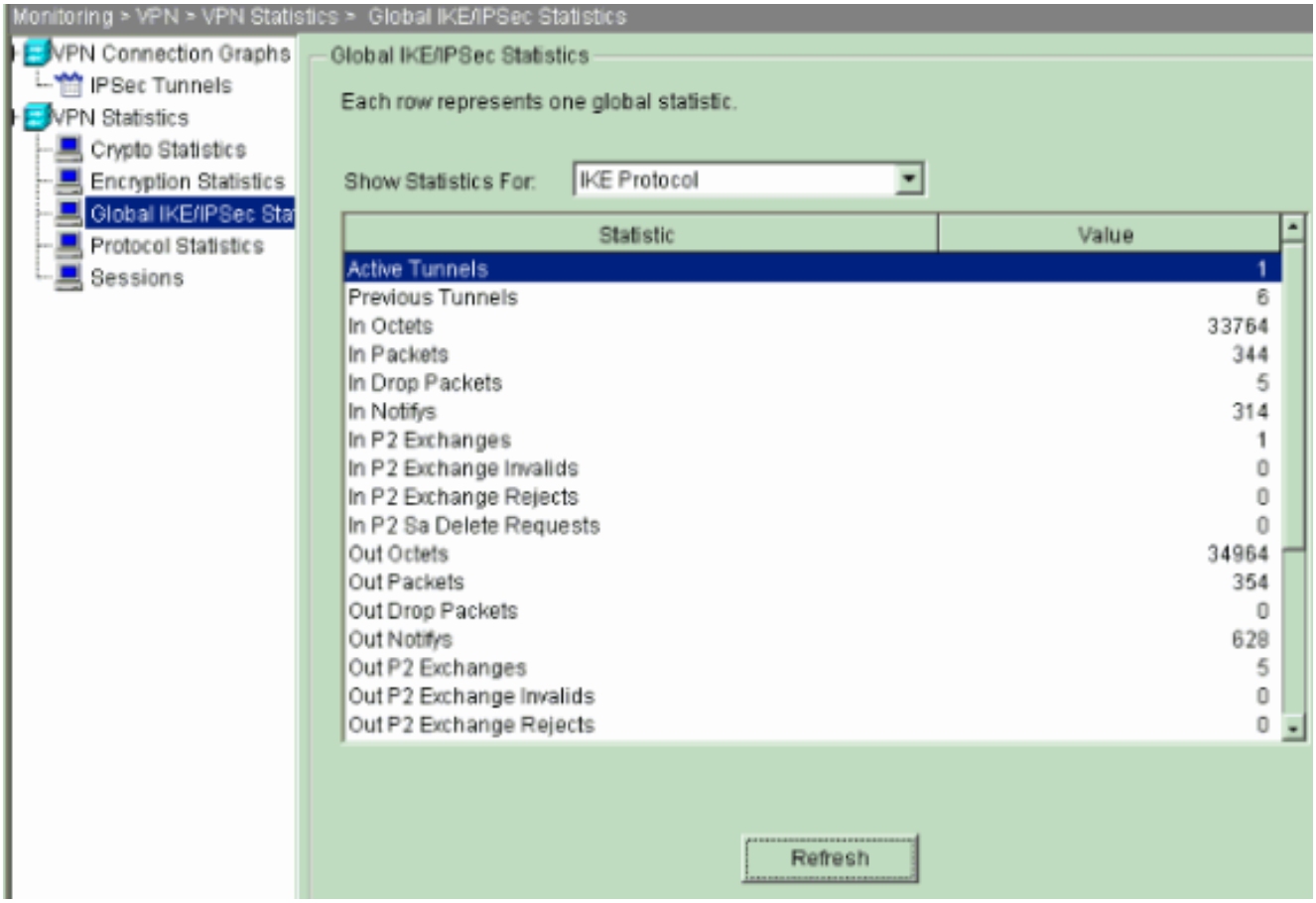
3. 点击 **Add** 选择可用的图表以在图表窗口中查看。



4. 单击 **Show Graphs** 以查看 IKE 和 IPsec 活动隧道图。



5. 选择 **Monitoring> VPN > VPN Statistics > Global IKE/IPSec Statistics** 以了解有关 VPN 隧道的统计信息。



还可以使用 CLI 验证隧道是否已形成。发出 **show crypto isakmp sa** 命令可检查隧道是否已形成，发出 **show crypto ipsec sa** 命令可观察已执行了封装、加密等操作的数据包的数量。

pix515-704

```
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

```
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
```

故障排除

PFS

在 IPsec 协商中，完全转发保密 (PFS) 可确保每个新的加密密钥与任何先前密钥不相关。请在两个隧道对等体上同时启用或禁用 PFS，否则不会在 PIX/ASA 中建立 L2L IPsec 隧道。

默认情况下 PFS 处于禁用状态。要启用 PFS，请在组策略配置模式下使用 **pfs** 命令并指定 enable 关键字。要禁用 PFS，请输入 **disable** 关键字。

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

要从正在运行的配置中删除 PFS 属性，请输入此命令的 **no** 形式。一个组策略可以从另一个组策略继承 PFS 的值。请输入此命令的 no 形式，以防止继承值。

```
hostname(config-group-policy)#no pfs
```

Management-Access

本部分提供的信息可用于对配置进行故障排除。

除非在全局配置模式下配置 management-access 命令，否则无法从隧道的另一端对 PIX 的内部接口执行 ping 操作。

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

debug 命令

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

debug crypto isakmp - 显示有关 IPsec 连接的调试信息，并显示由于两端不兼容而被拒绝的第一组属性。

debug crypto isakmp

```
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 - 显示有关 IPsec 连接的调试信息。

debug crypto ipsec

```
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
```

相关信息

- 在防火墙之间使用 PDM 创建冗余隧道
- Cisco PIX 防火墙软件
- Cisco 自适应安全设备管理器
- Cisco ASA 5500 系列自适应安全设备
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems