ASA/PIX：有和没有 IPSec 隧道的 NTP 配置示例

目录

简介

本文档提供了使用 Network Time Protocol (NTP) 对 PIX/ASA 安全设备时钟与网络时间服务器进行同步的示例配置。ASA1 直接与网络时间服务器进行通信。ASA2 通过 IPsec 隧道向 ASA1 传送 NTP 流量，后者反过来将数据包转发给网络时间服务器。

请参阅 ASA 8.3及以上版本：有和没有IPSec隧道配置示例的NTP关于在Cisco ASA的相同配置的更多信息与版本8.3和以上。

注意： 路由器还可以用作同步 PIX/ASA 安全设备时钟的 NTP 服务器。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 必须建立端到端 IPsec 连接才能开始此 NTP 配置。
- 必须为数据加密标准 (DES) 加密（在最低加密级别）启用安全设备许可证。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco 自适应安全设备 (ASA) 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。

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。

相关产品

此配置也可用于 Cisco PIX 500 系列安全设备，这些设备运行版本 7.x 及更高版本。

注意： PIX 版本 6.2 已添加 NTP 支持。请参阅 PIX 6.2：有和没有 IPSec 隧道的 NTP 配置示例，以便在 Cisco PIX 防火墙上配置 NTP。

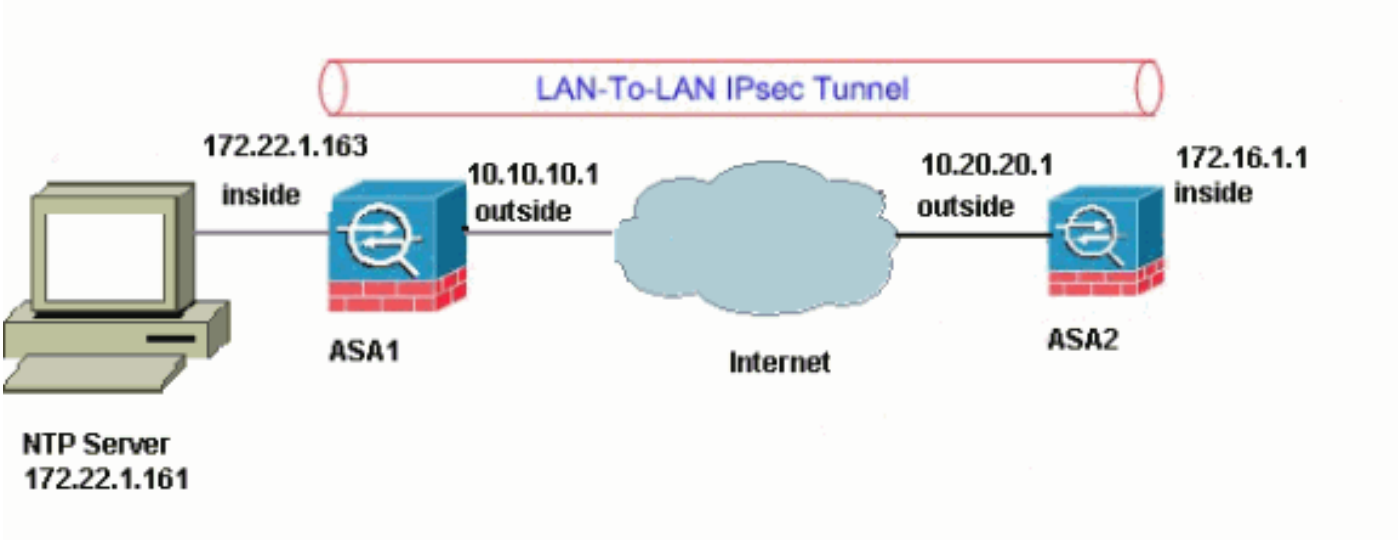
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

网络图

本文档使用此图所示的网络设置。



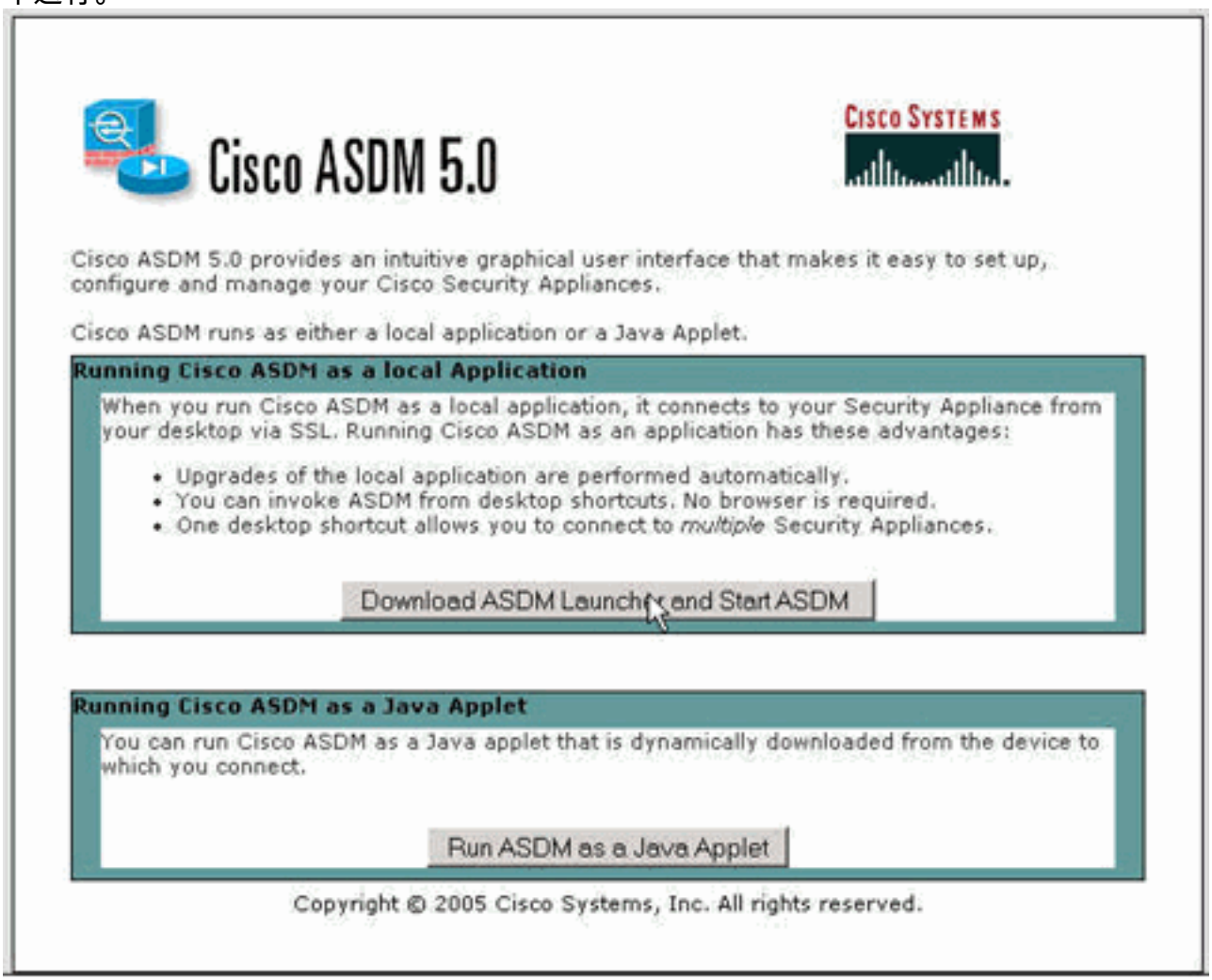
注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

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

VPN 隧道 ASDM 配置

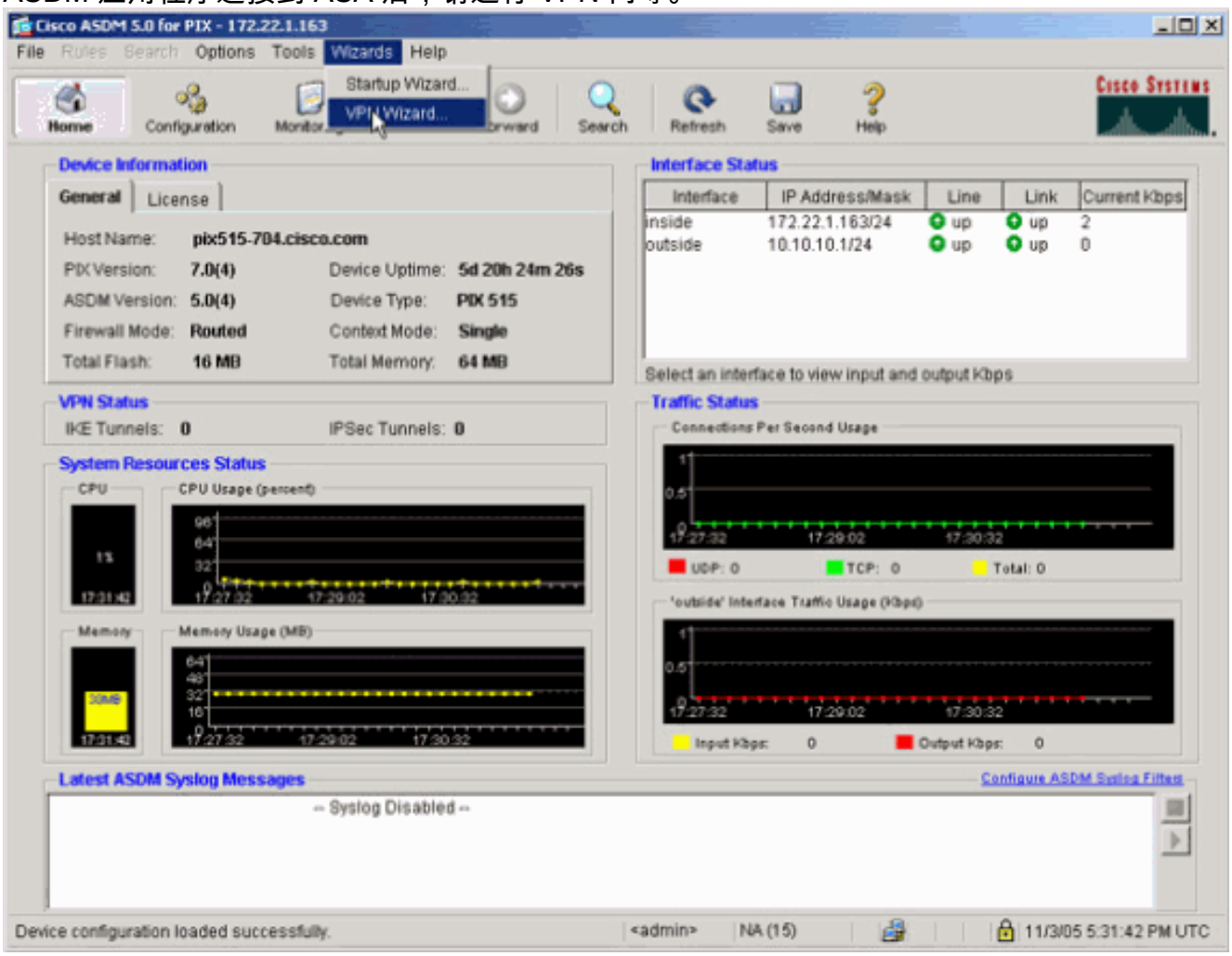
请完成以下步骤以创建 VPN 隧道：

1. 打开浏览器并键入 **https:// <Inside_IP_Address_of_ASA>** 以访问 ASA 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。ASA 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。

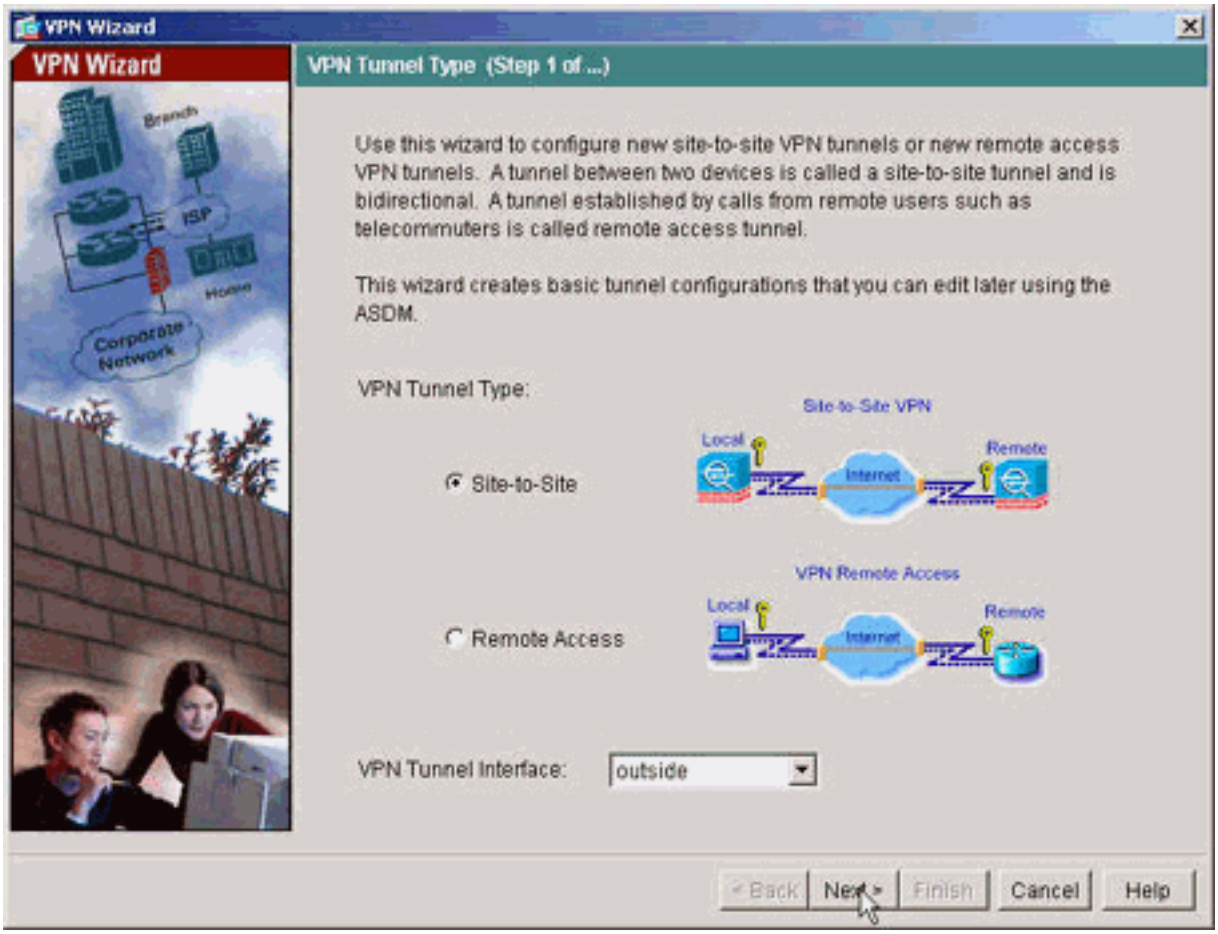


2. 单击 **Download ASDM Launcher and Start ASDM** 以下载 ASDM 应用程序的安装程序。
3. 下载 ASDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco ASDM 启动程序。
4. 输入使用 **http -** 命令配置的接口的 IP 地址，以及用户名和口令（如果已指定）。此示例使用默认空白用户名和口令。

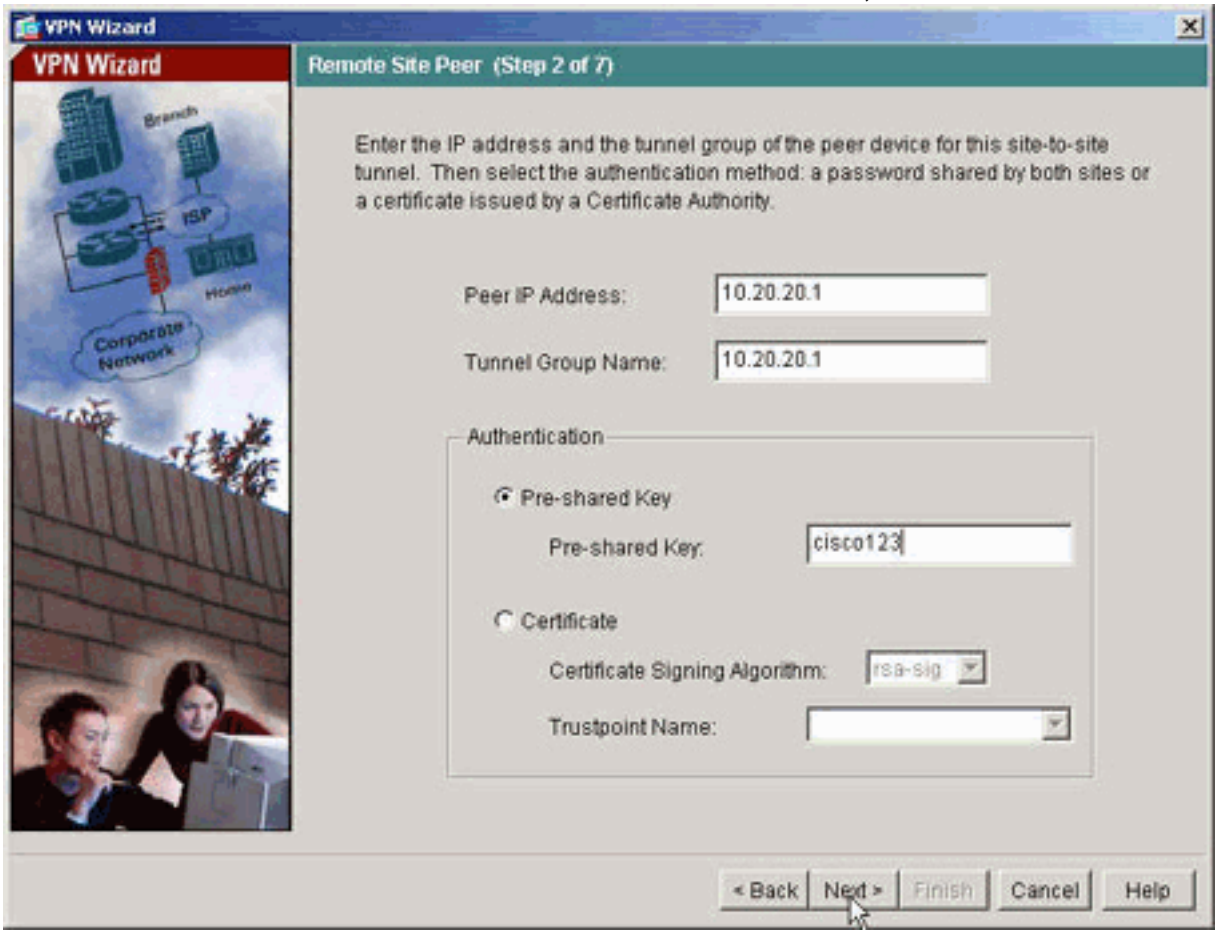
5. ASDM 应用程序连接到 ASA 后，请运行 VPN 向导。



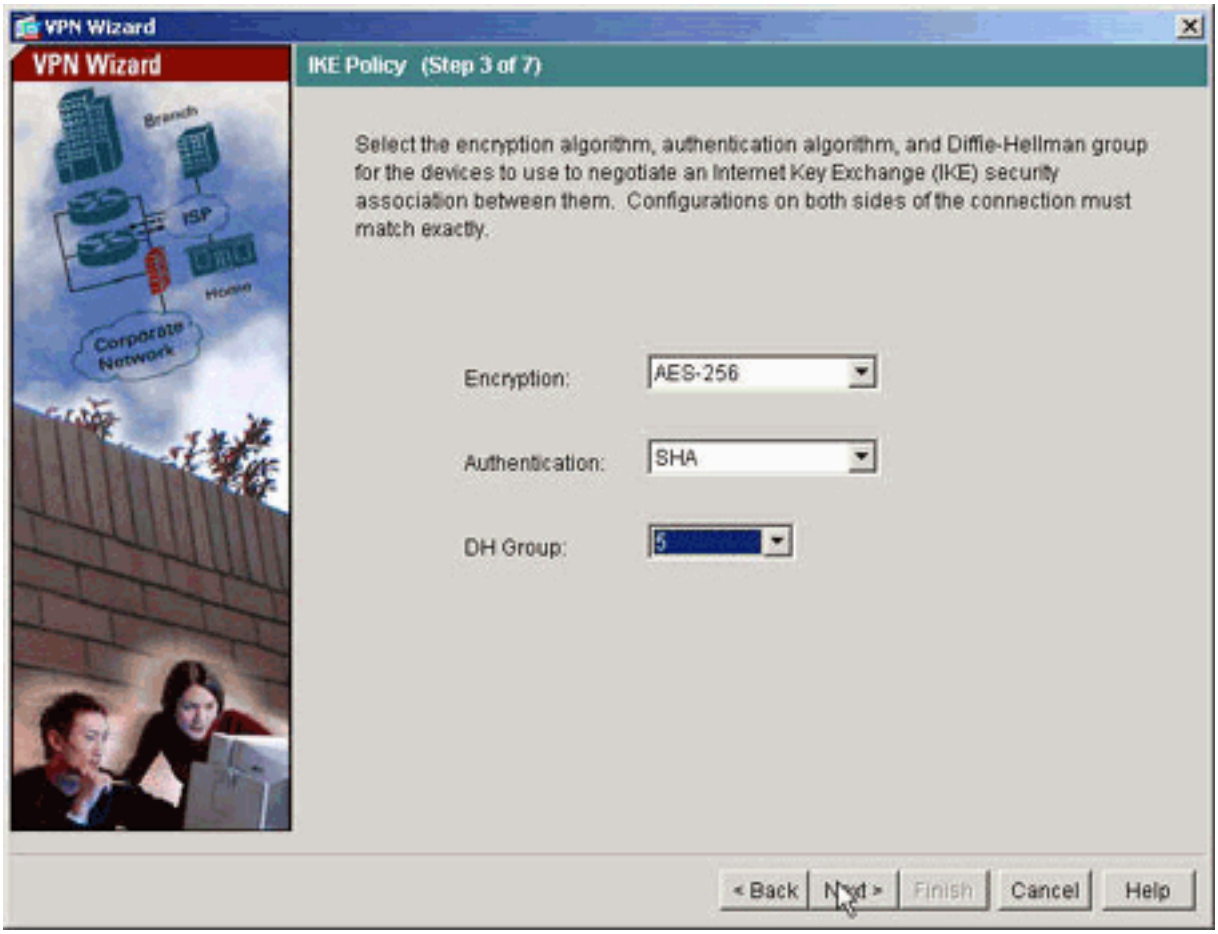
6. 选择 **Site-to-Site IPsec** VPN 隧道类型。



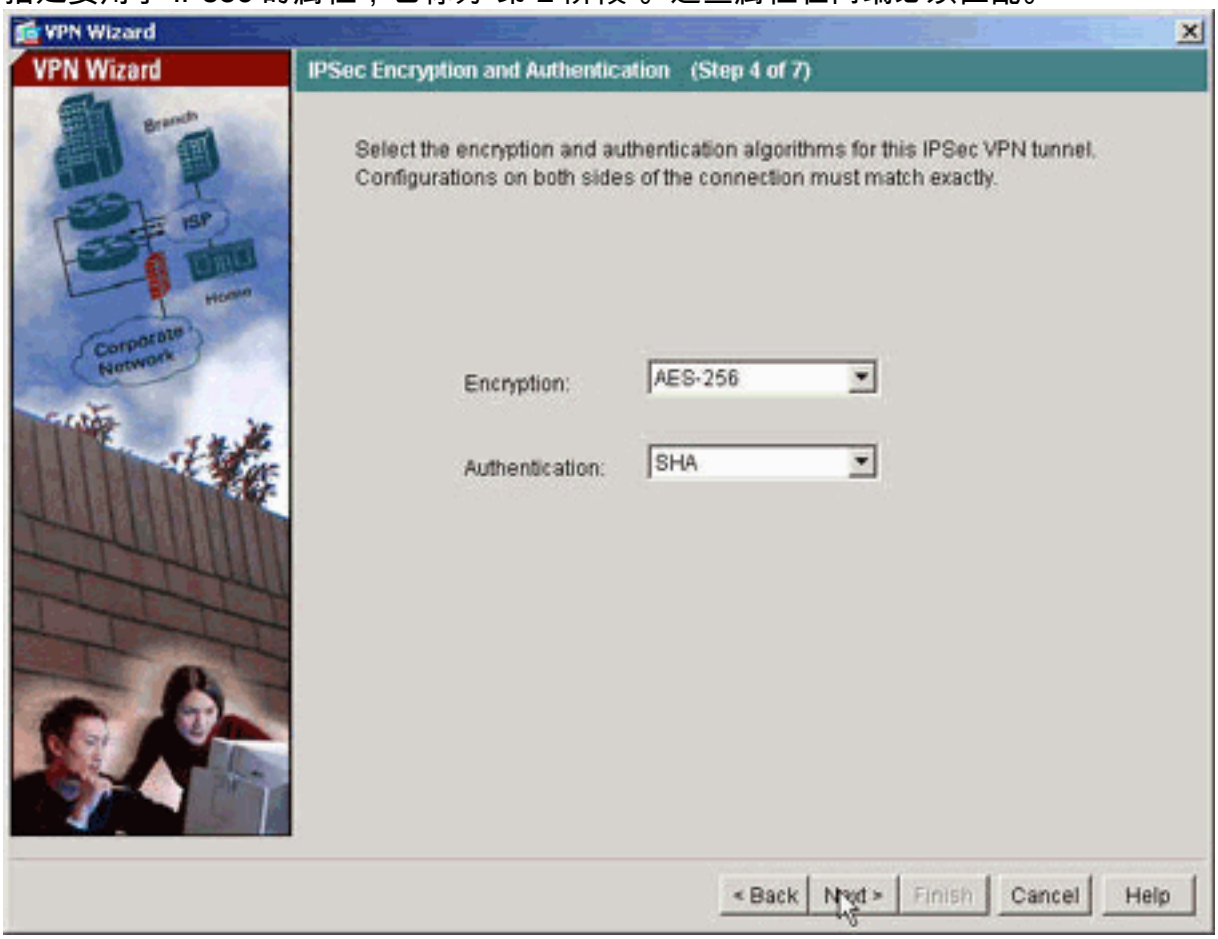
7. 指定远程对等体的外部 IP 地址。输入要使用的身份验证信息，在本示例中是预共享密钥。



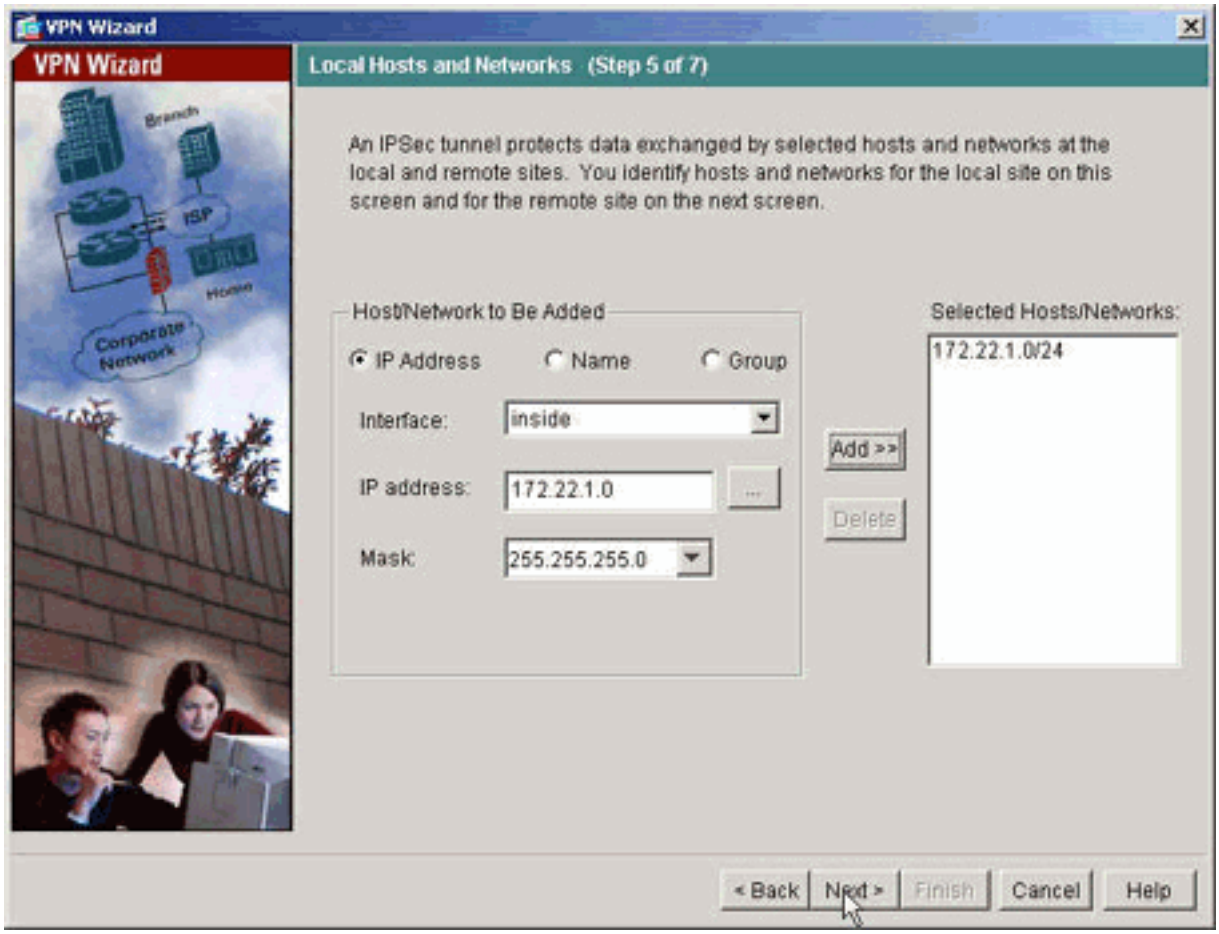
8. 指定要用于 IKE 的属性，也称为“第 1 阶段”。这些属性在隧道两端必须是相同的。



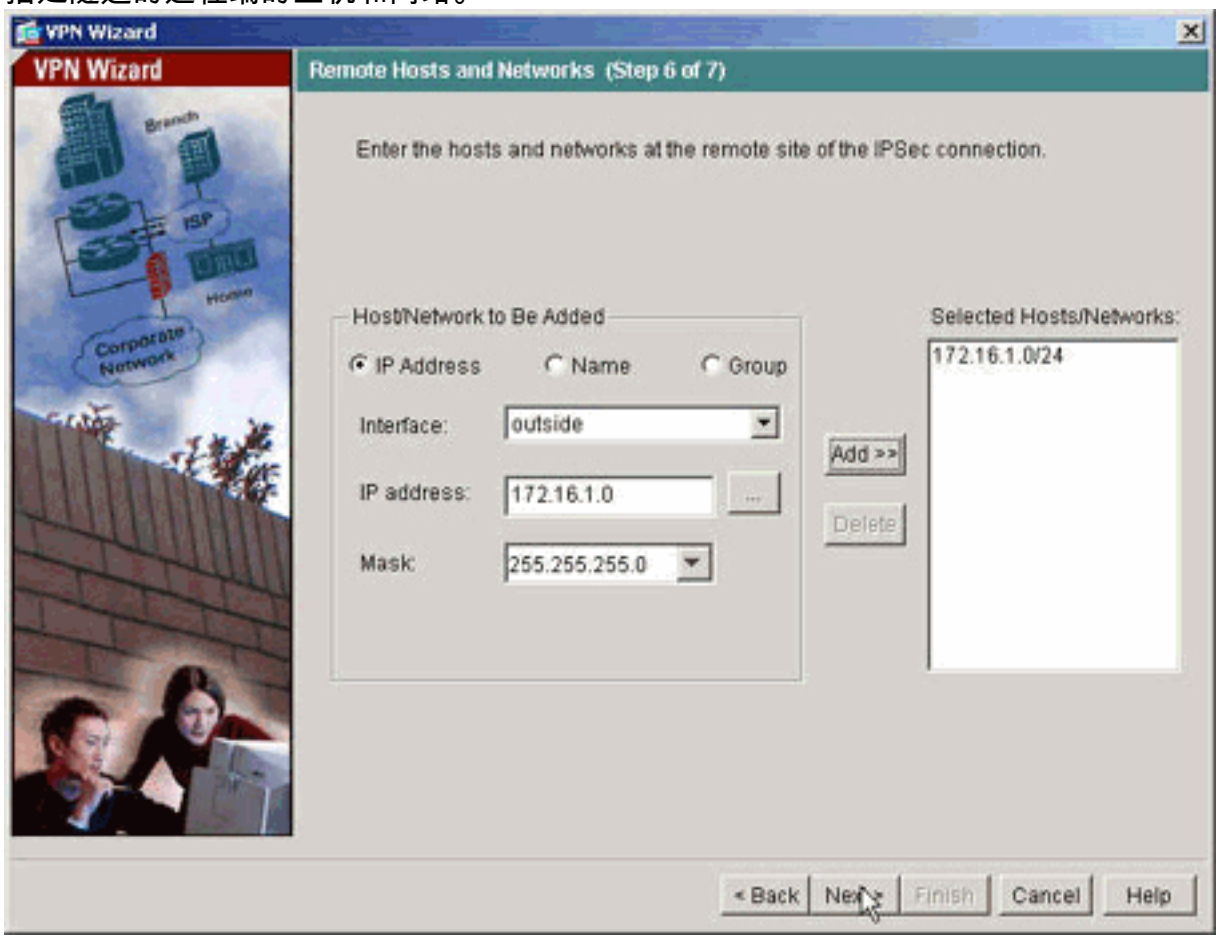
9. 指定要用于 IPsec 的属性，也称为“第 2 阶段”。这些属性在两端必须匹配。



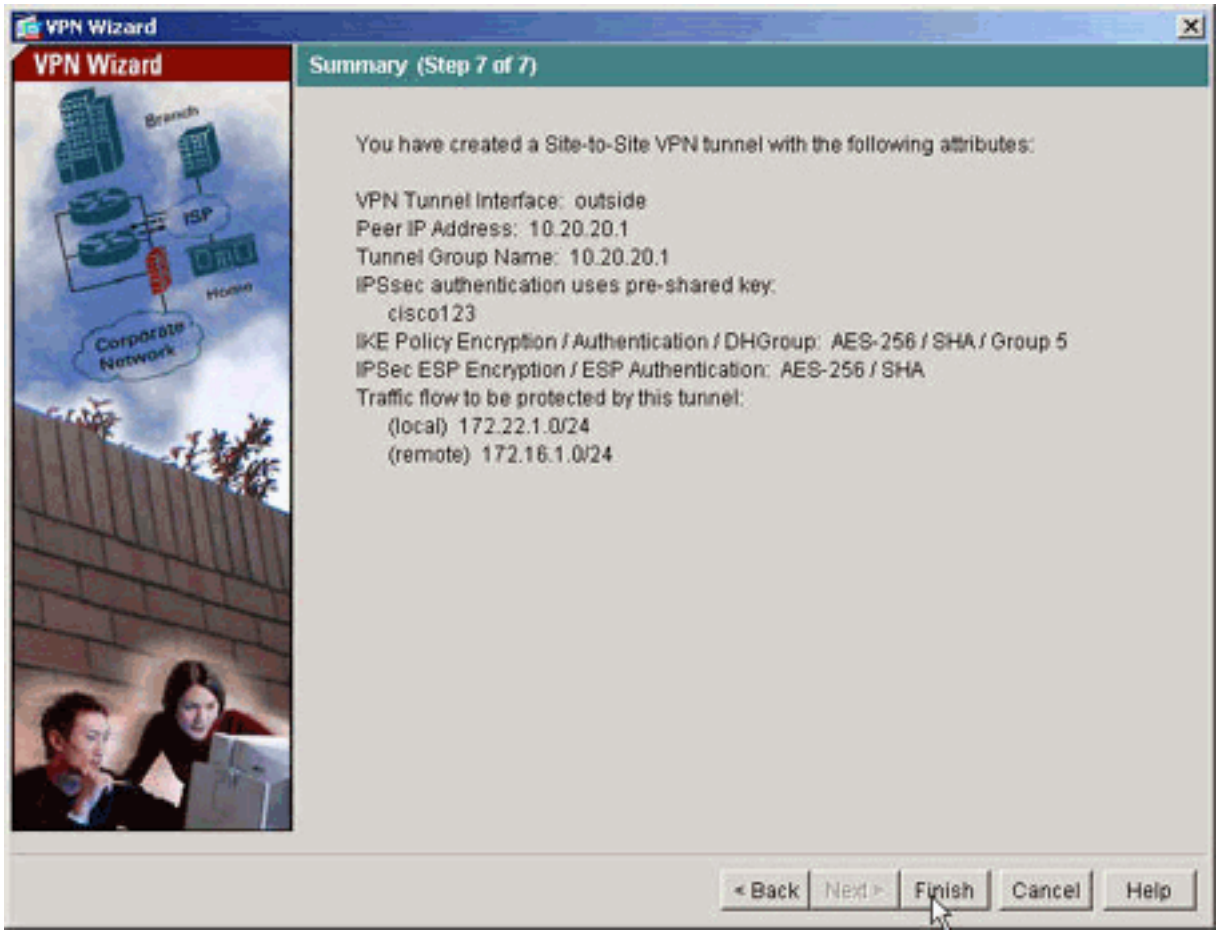
10. 指定应允许其数据流通过 VPN 隧道的主机。在此步骤中，指定 ASA1 的本地主机。



11. 指定隧道的远程端的主机和网络。

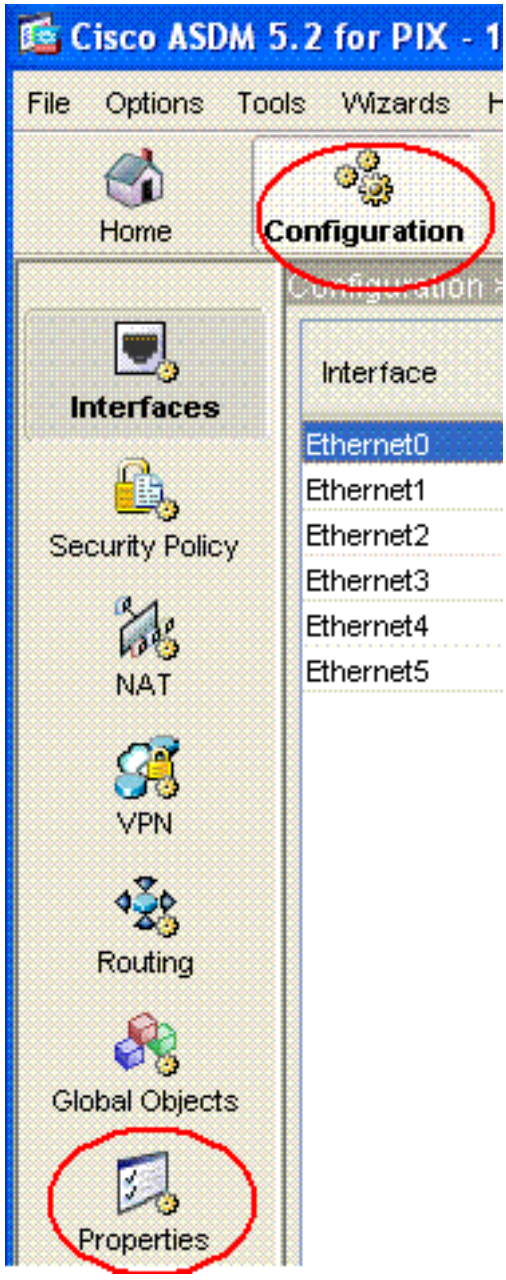


12. 此概要中显示了通过 VPN 向导定义的属性。仔细检查配置，如果您确保设置正确，请单击 **Finish**。

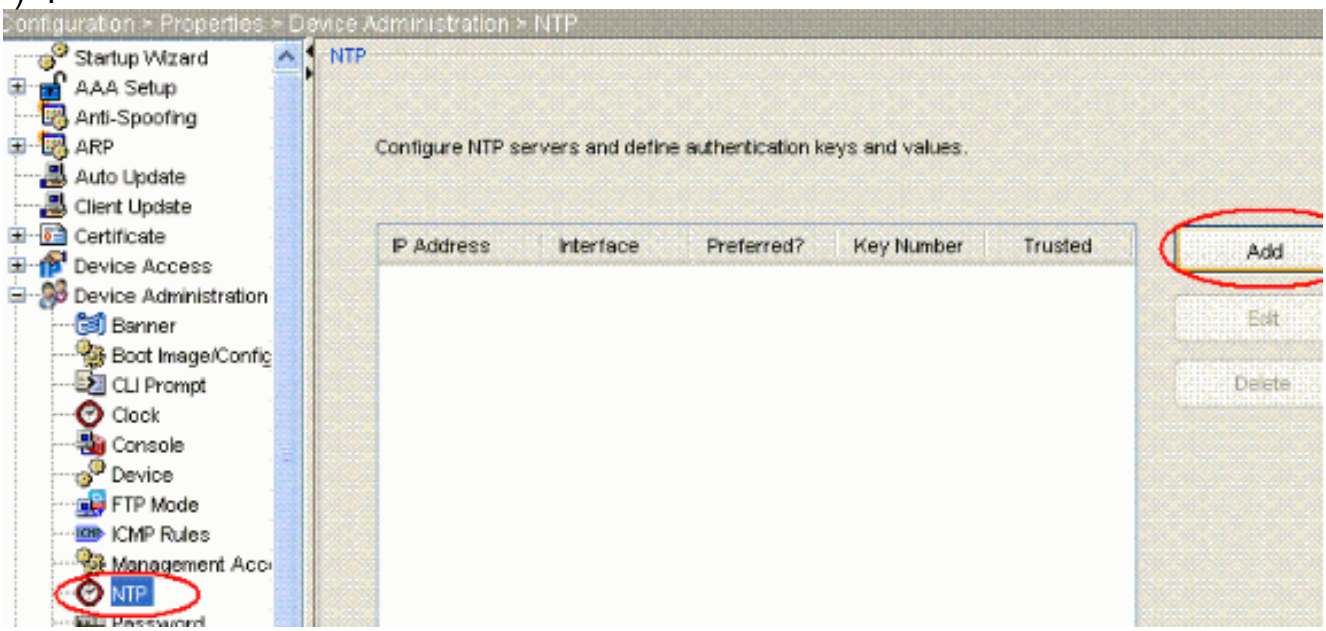


NTP ASDM 配置

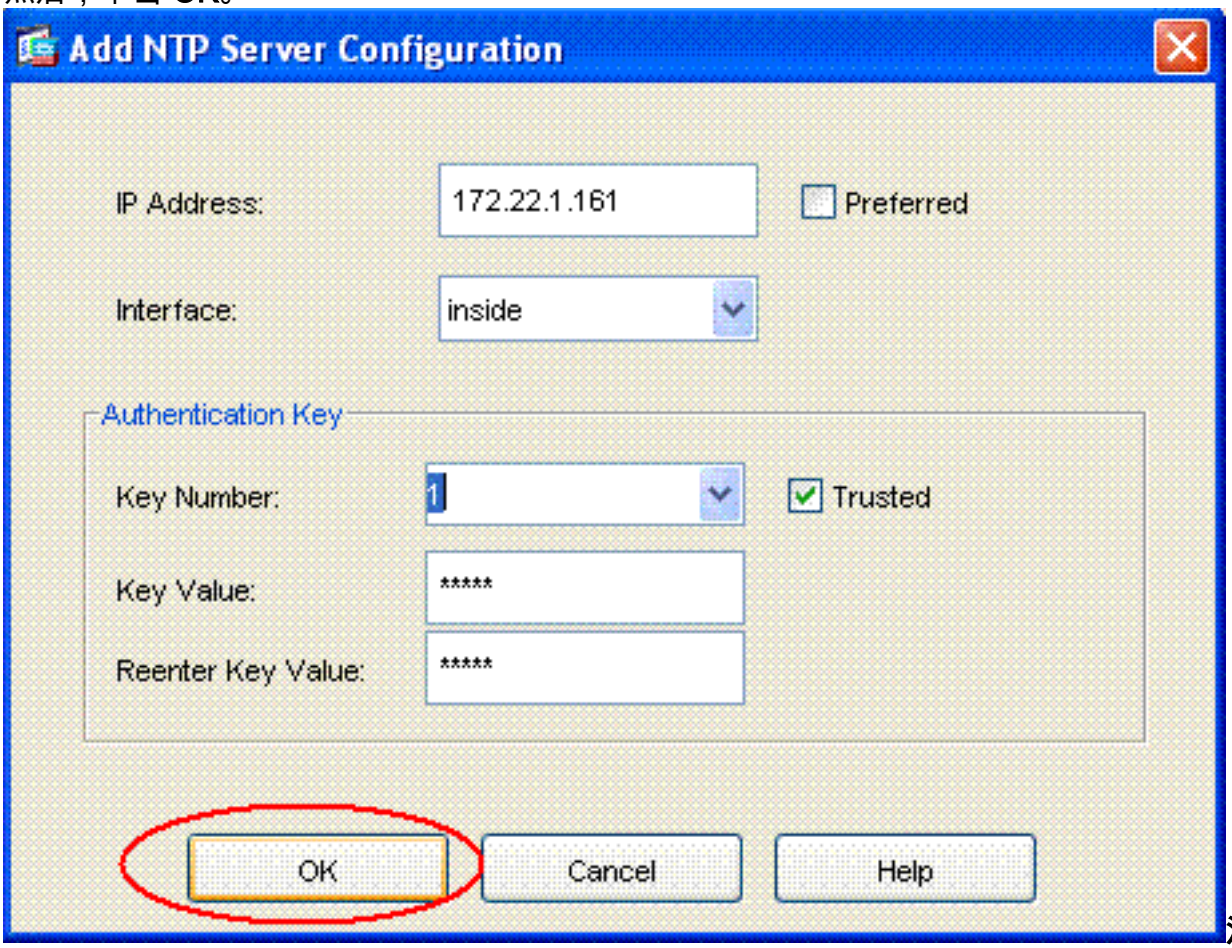
请完成以下步骤，以便在 Cisco 安全设备上配置 NTP：



1. 在 ASDM 主页中选择 **Configuration**（如图所示）：
2. 现在选择 **Properties > Device Management > NTP**，以便打开 ASDM 的 **NTP** 配置页（如图所示
   ）：



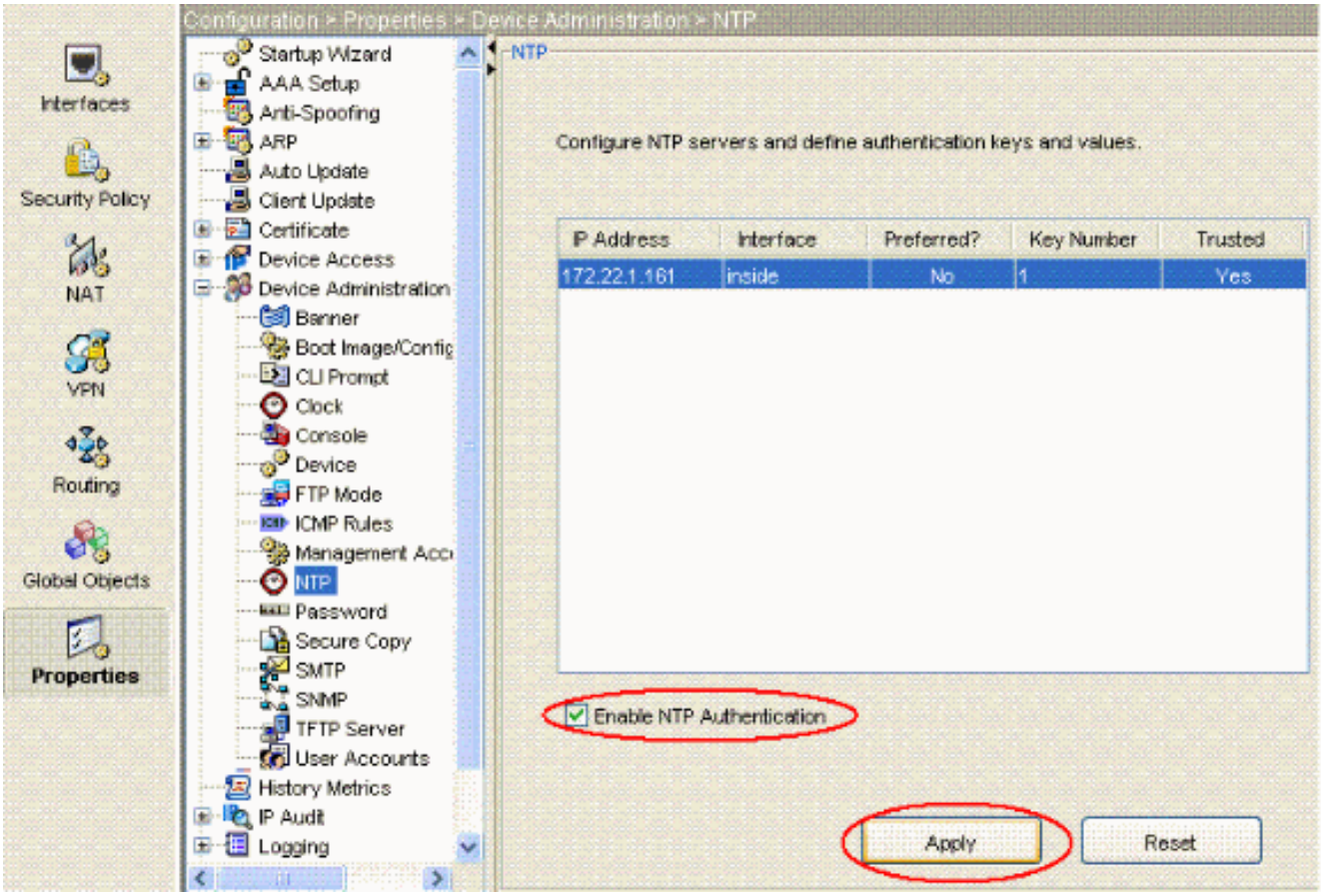
3. 单击 ADD 按钮添加 NTP 服务器，并在单击 ADD 按钮后显示的新窗口中提供所需属性，如 IP 地址、接口名称（内部或外部）以及用于身份验证的密钥编号和密钥值（如屏幕截图所示）。然后，单击 OK。



注意：应为 ASA1 选择内部接口名称，为 ASA2 选择外部接口名称。**注意**：ASA 和 NTP 服务器中的 **ntp authentication key** 应相同。CLI 中的 ASA1 和 ASA2 身份验证属性配置如下所示：

```
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. 现在单击 **Enable NTP Authentication** 复选框，然后单击 **Apply**，即可完成 NTP 配置任务。



ASA1 CLI 配置

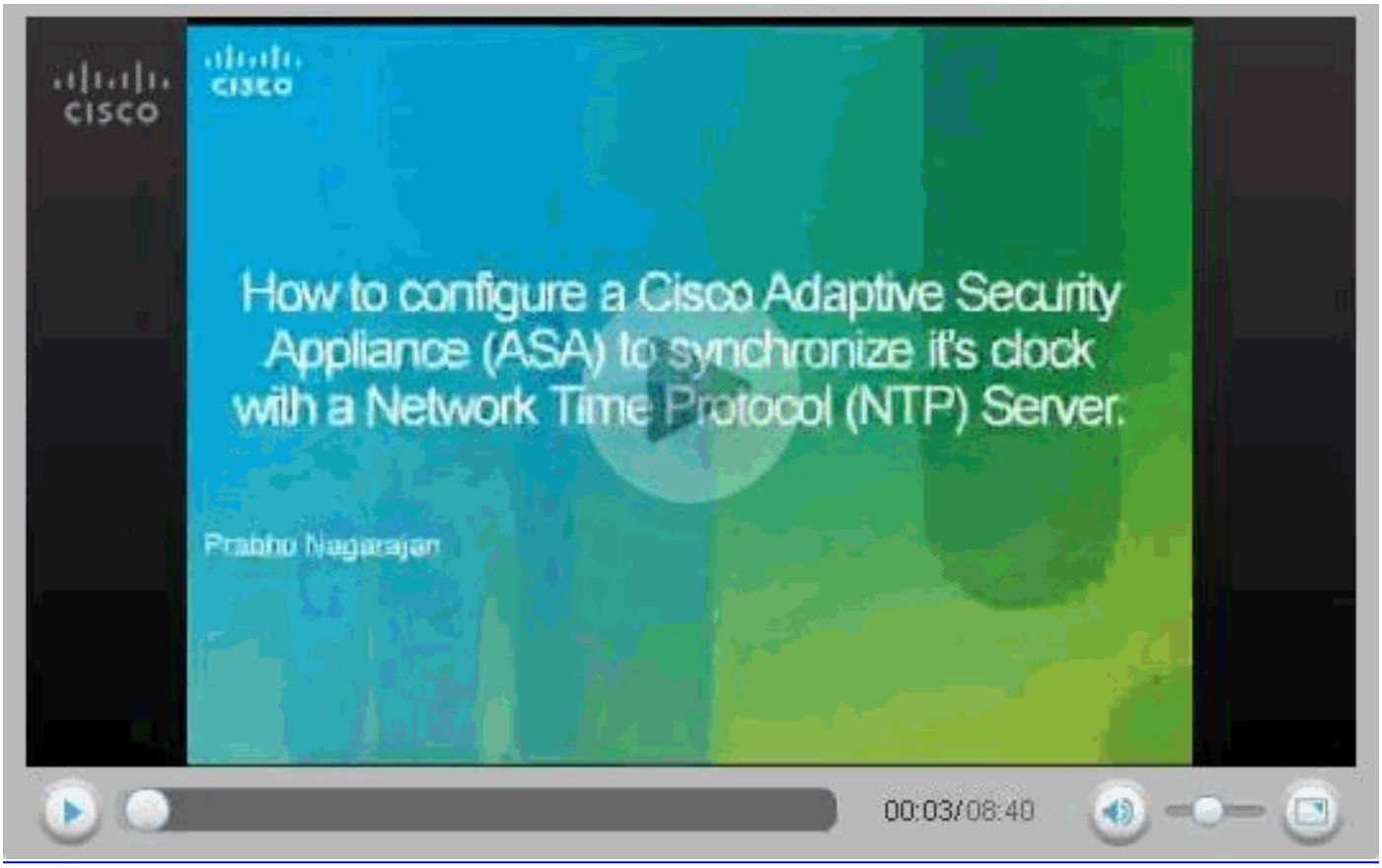
ASA1

```
ASA#show run : Saved ASA Version 7.1(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-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 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 autentication-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
```

此视频已发布到 Cisco 支持社区 ，该视频通过演示说明了将 ASA 配置为 NTP 客户端的步骤：

如何将 Cisco 自适应安全设备 (ASA) 配置为与 Network Time Protocol (NTP) 服务器同步时钟。



ASA2 CLI 配置

ASA2

```
ASA Version 7.1(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-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 !--- Define the NTP
server autentication-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#
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令，使用此工具可以查看对 show 命令输出的分析。

- show ntp status - 显示 NTP 时钟信息。`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] - 显示配置的网络时间服务器关联。`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`

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

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

- **debug ntp validity** - 显示 NTP 对等体时钟正确性。以下是密钥不匹配的 **debug** 输出：
  NTP: packet from 172.22.1.161 failed validity tests 10 Authentication failed
- **debug ntp packet** - 显示 NTP 数据包信息。当没有来自服务器的响应时，在 ASA 上只能看到 NTP xmit 数据包，而看不到 NTP rcv 数据包。
```
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)
```

相关信息

- 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
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems