ASA/PIX： IPSec トンネルの有無による NTP の設定例

目次

概要

このドキュメントでは、ネットワーク タイム プロトコル（NTP）を使用して、PIX/ASA セキュリティ アプライアンスのクロックをネットワーク タイム サーバと同期させるための設定例を紹介します。 ASA1 はネットワーク タイム サーバと直接通信します。ASA2 は IPSec トンネルを使用して ASA1 に NTP トラフィックを送信し、ASA1 はそれらのパケットをネットワーク タイム サーバに転送します。

バージョン 8.3 以降の Cisco Adaptive Security Appliance（ASA）での ASDM を使用した同等な設定の詳細について『ASA 8.3.x 以降： IPSec トンネルがある場合とない場合の NTP の設定例』で、バージョン 8.3 以降の Cisco ASA を使用した同じ設定の詳細を参照してください。

注: ルータは、PIX/ASA セキュリティ アプライアンスのクロックを同期するための NTP サーバとしても使用できます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- この NTP の設定を開始する前に、エンドツーエンドの IPSec 接続を確立しておく必要があります。
- Data Encryption Standard（DES; データ暗号標準）の暗号化（最小限の暗号化レベル）でセキュリティ アプライアンスのライセンスを有効にする必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 7.x 以降が稼働する Cisco 適応型セキュリティ アプライアンス（ASA）
- ASDM バージョン 5.x 以降

注: ASA を ASDM で設定できるようにするには、『ASDM 用の HTTPS アクセスの許可』を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、バージョン 7.x 以降で稼働する Cisco PIX 500 シリーズ セキュリティ アプライアンスでも使用できます。

注: NTP のサポートは PIX バージョン 6.2 で追加されたものです。 Cisco PIX ファイアウォール上で NTP を設定するには、『PIX 6.2： IPSec トンネルがある場合とない場合の NTP の設定例』を参照してください。

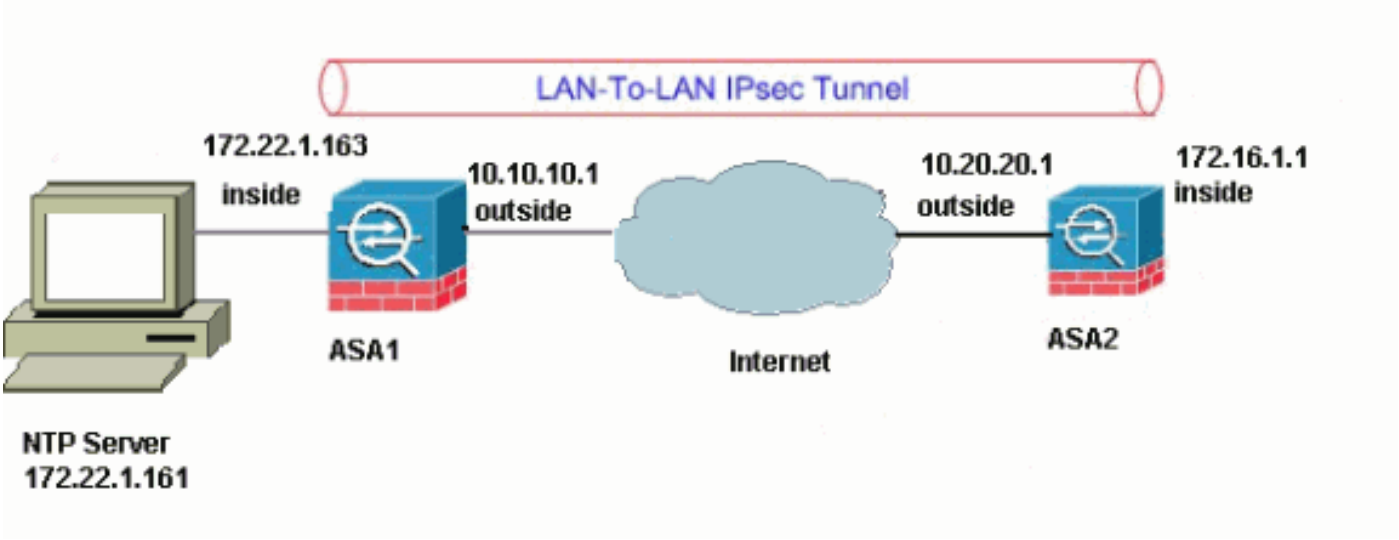
表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。

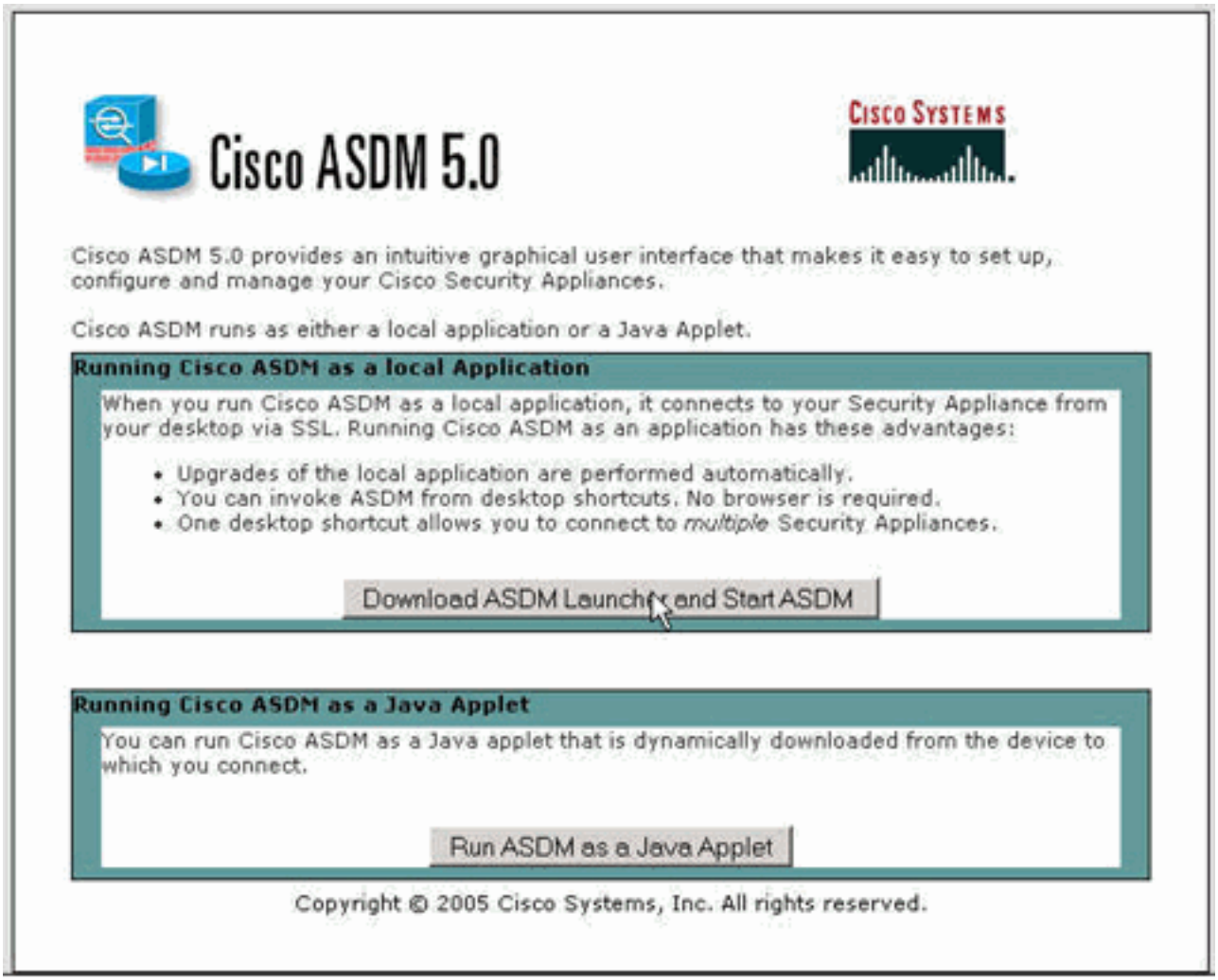


注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 のアドレスです。

VPN トンネル ASDM の設定

VPN トンネルを作成するには、以下の手順を実行します。

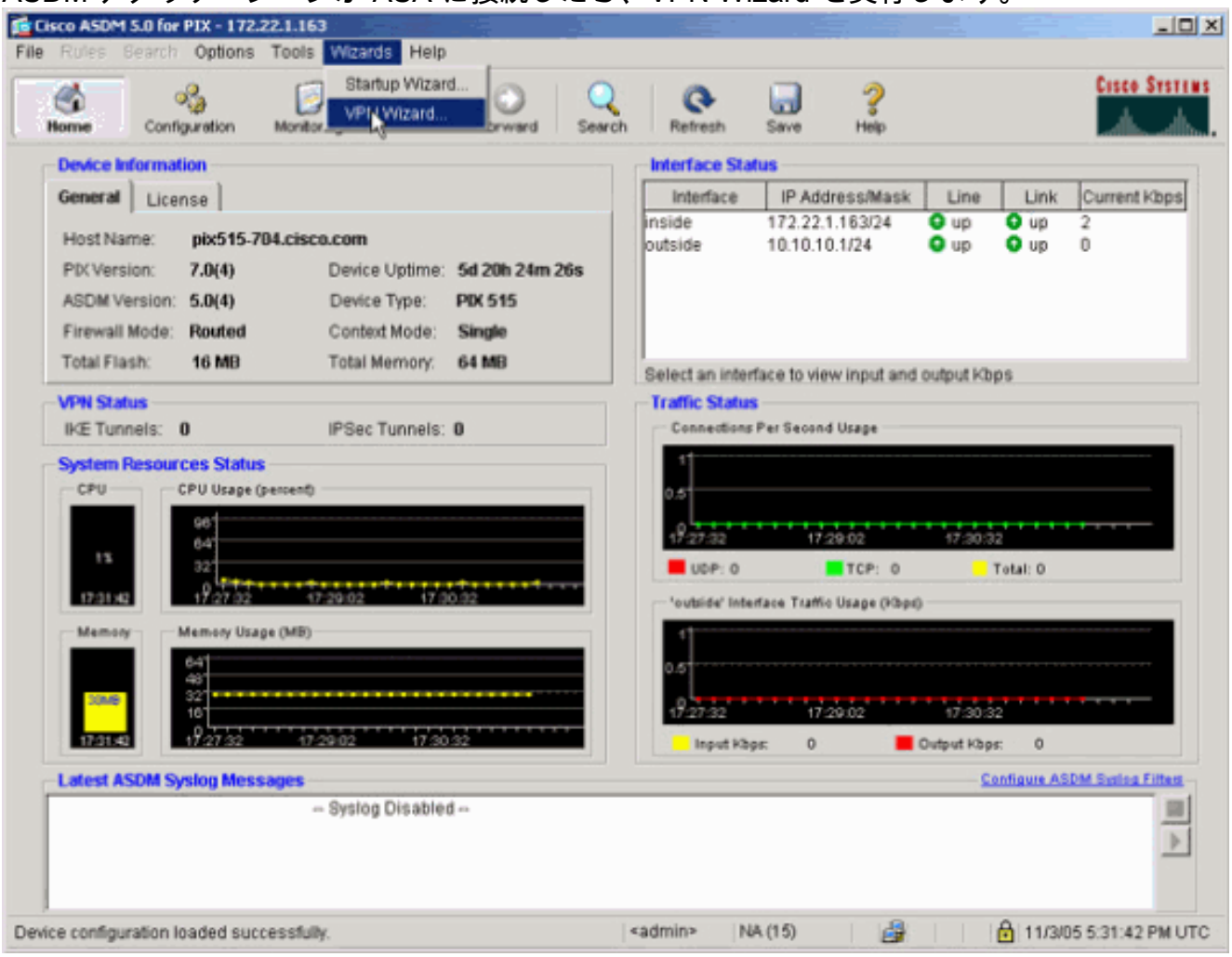
1. ブラウザを開き、**https://<Inside_IP_Address_of_ASA>** と入力して、ASA 上の ASDM にアクセスします。SSL 証明書の信憑性に関連してブラウザから出力されるすべての警告を認可します。 デフォルトのユーザ名とパスワードは、両方とも空白です。ASA がこのウィンドウを表示するのは、ASDM アプリケーションのダウンロードを許可するためです。 次の例の場合、アプリケーションはローカル コンピュータにロードされ、Java アプレットでは動作しません。



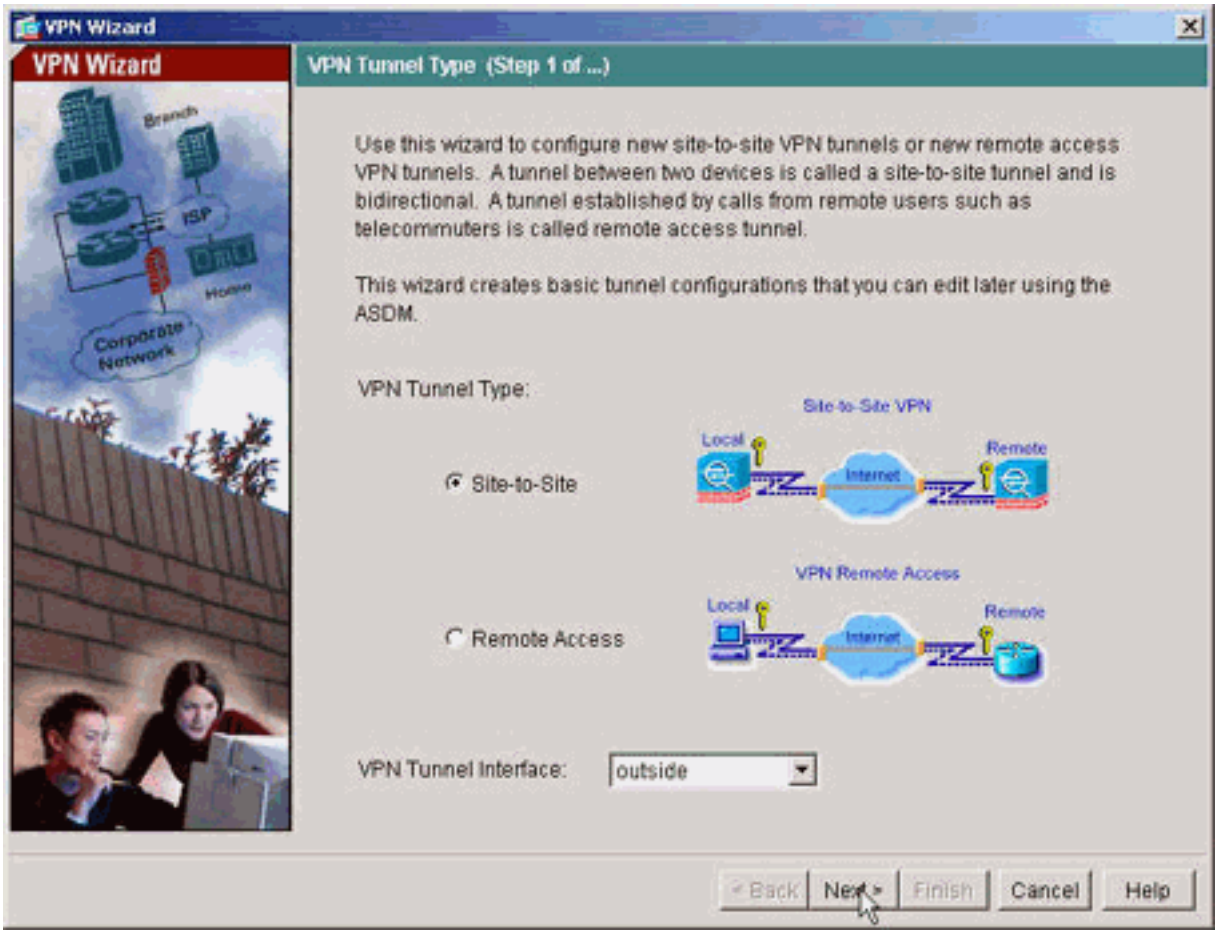
2. [Download ASDM Launcher and Start ASDM] をクリックして、ASDM アプリケーションのインストーラをダウンロードします。
3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連のステップを実行し、該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。
4. **http -** コマンドで設定したインターフェイスの IP アドレス、およびユーザ名とパスワード（指定した場合）を入力します。この例では、デフォルトの空のユーザ名とパスワードを使

用します。

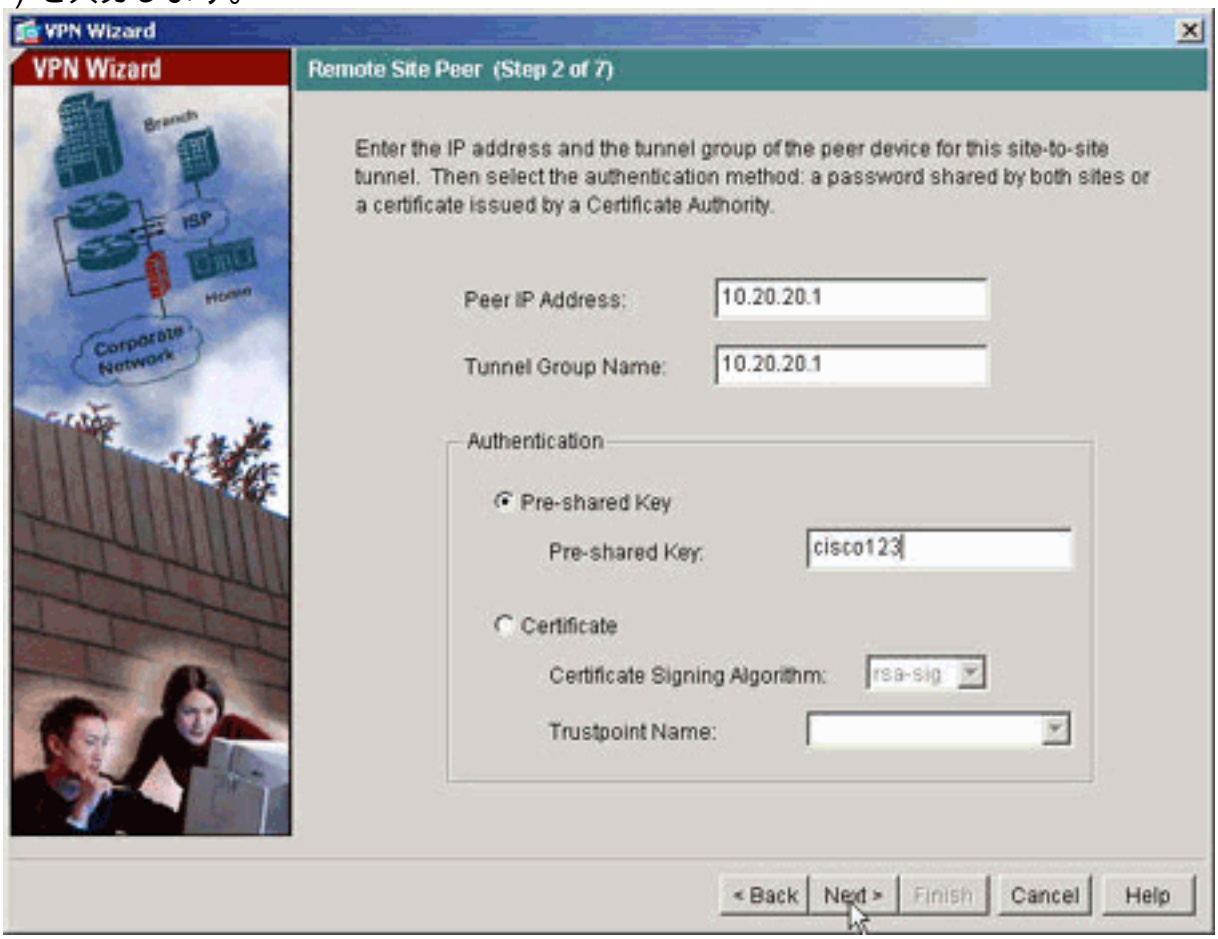
5. ASDM アプリケーションが ASA に接続したら、VPN Wizard を実行します。



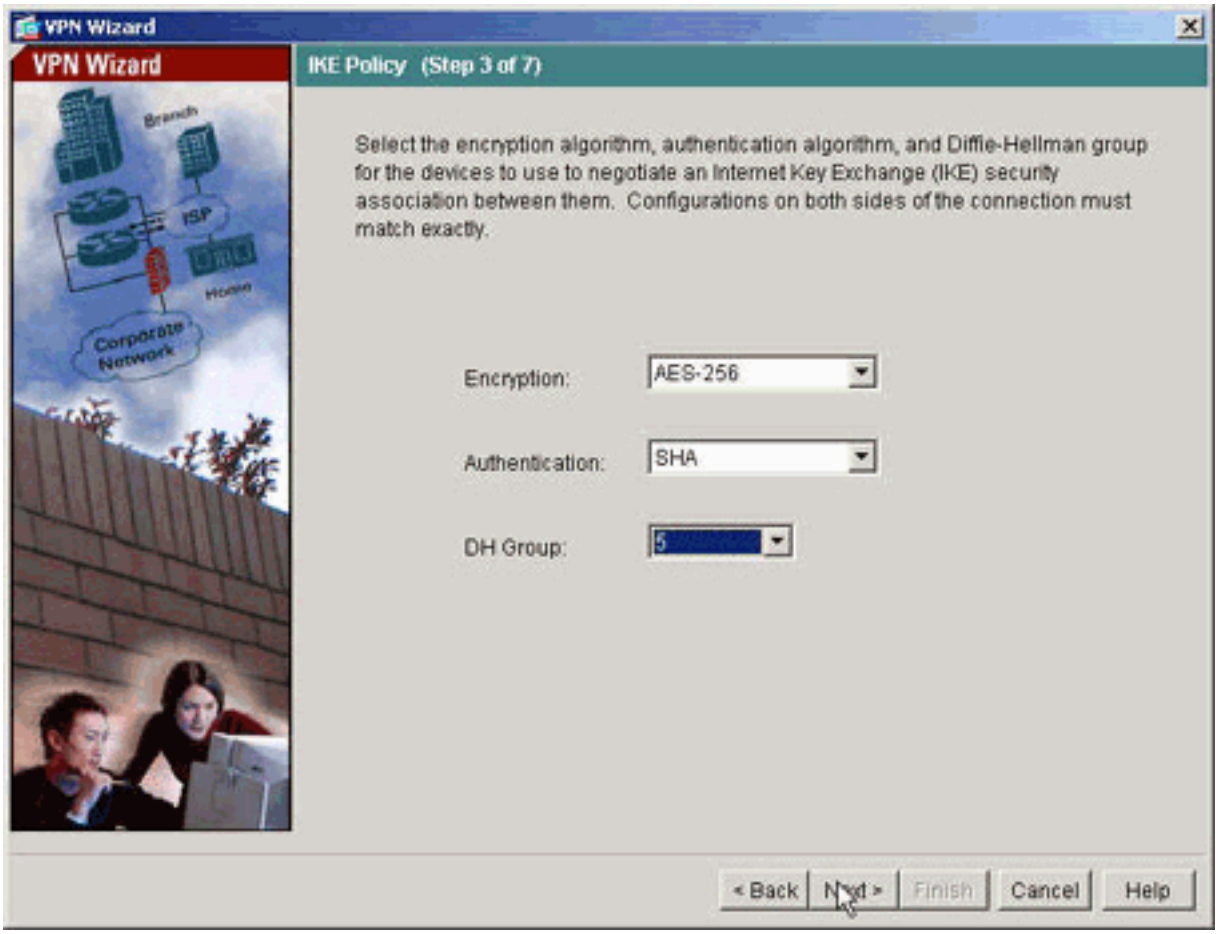
6. VPN のトンネルのタイプとして、**Site-to-Site IPsec** を選択します。



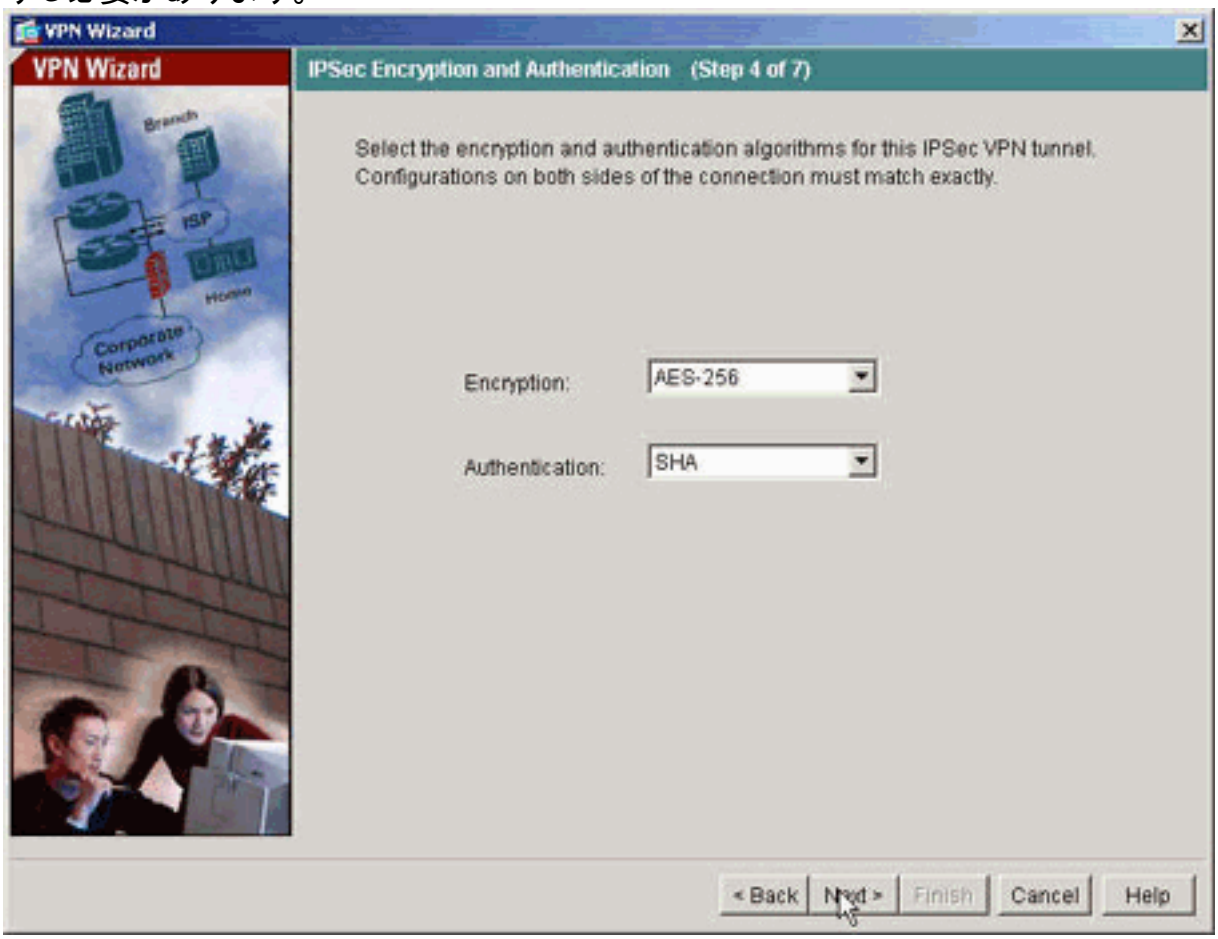
7. リモート ピアの外部 IP アドレスを指定します。 使用する認証情報 (今の場合は事前共有鍵) を入力します。



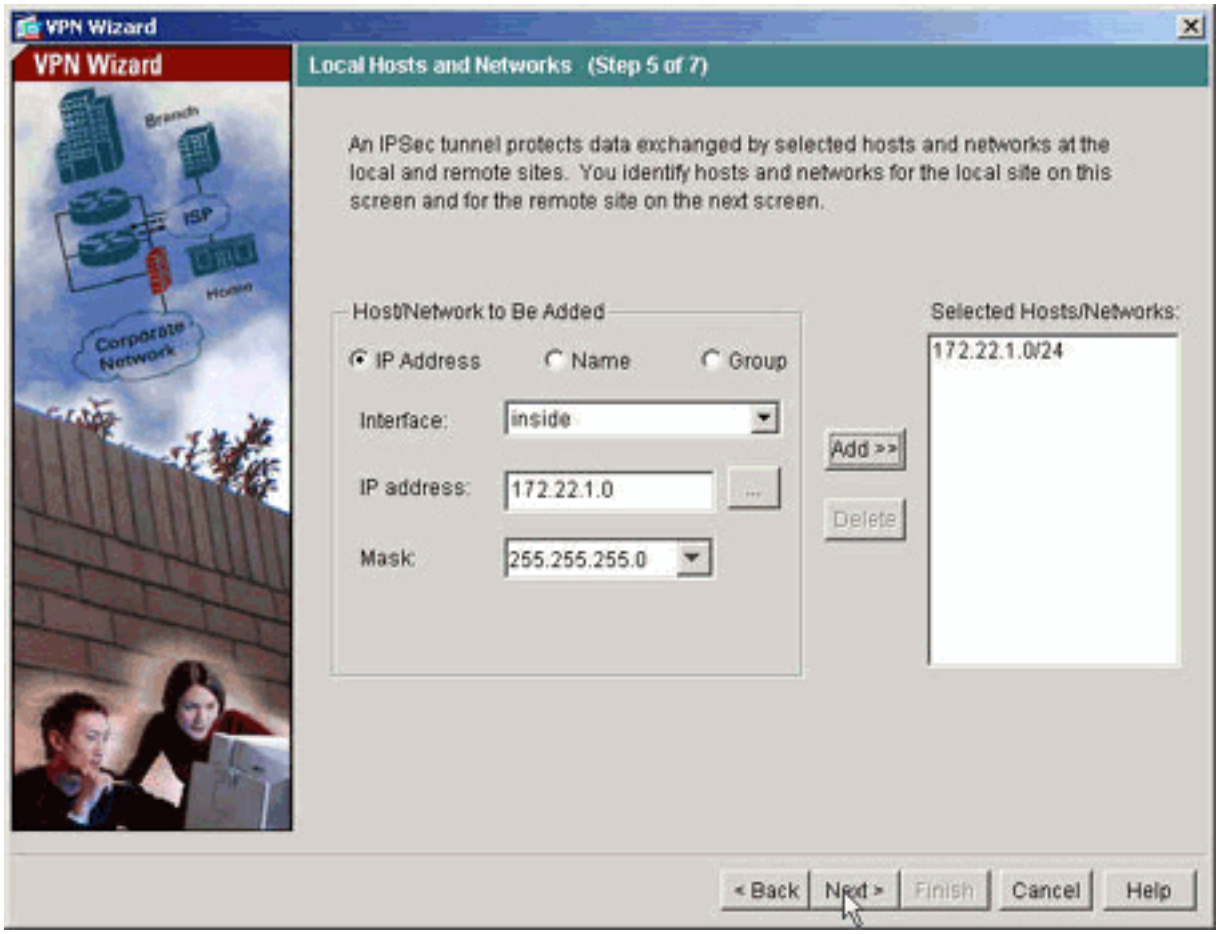
8. IKE (フェーズ 1 ともいう) で使用する属性を指定します。 これらの属性は、トンネルの両側で同じにする必要があります。



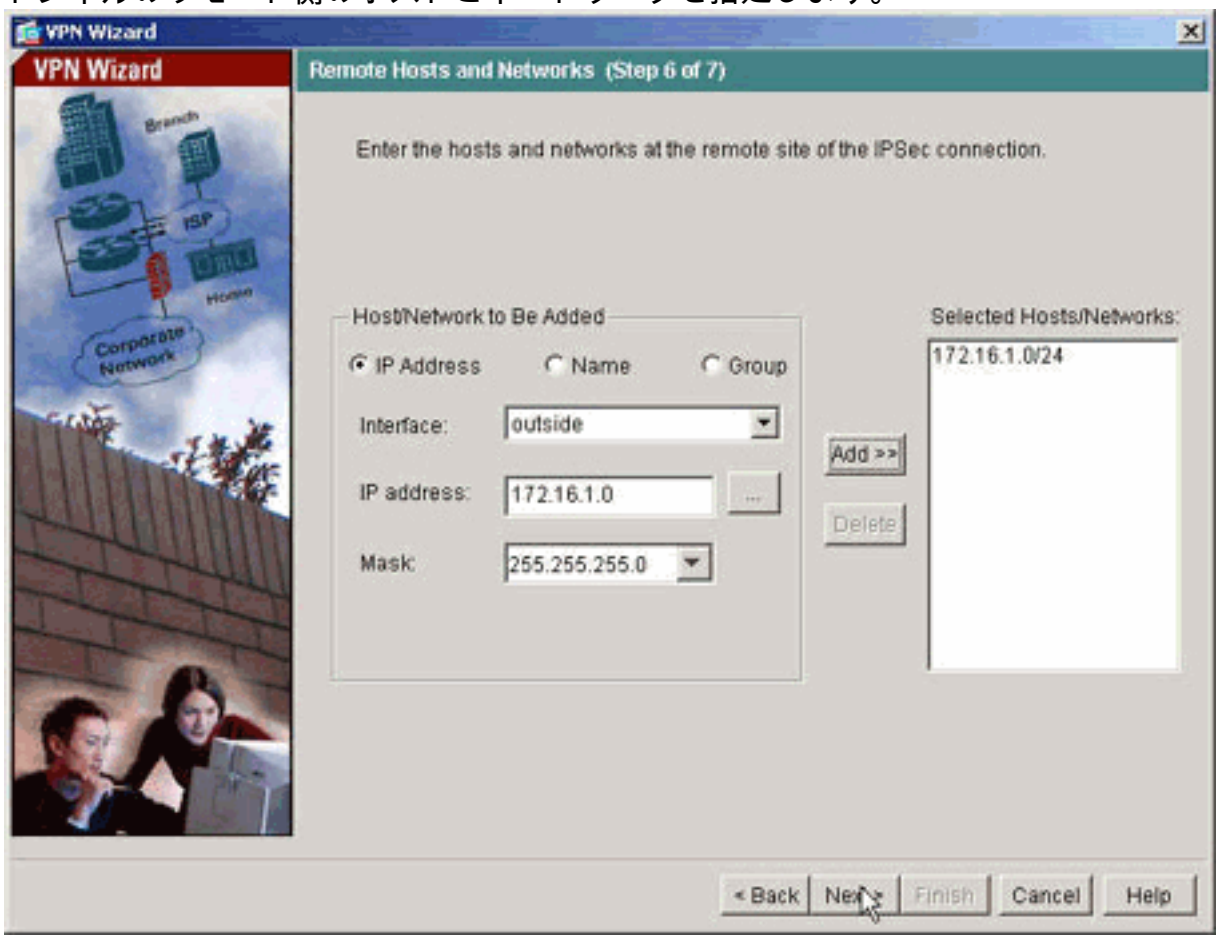
9. IPsec（フェーズ 2 ともいう）で使用する属性を指定します。 これらの属性は、両側で一致する必要があります。



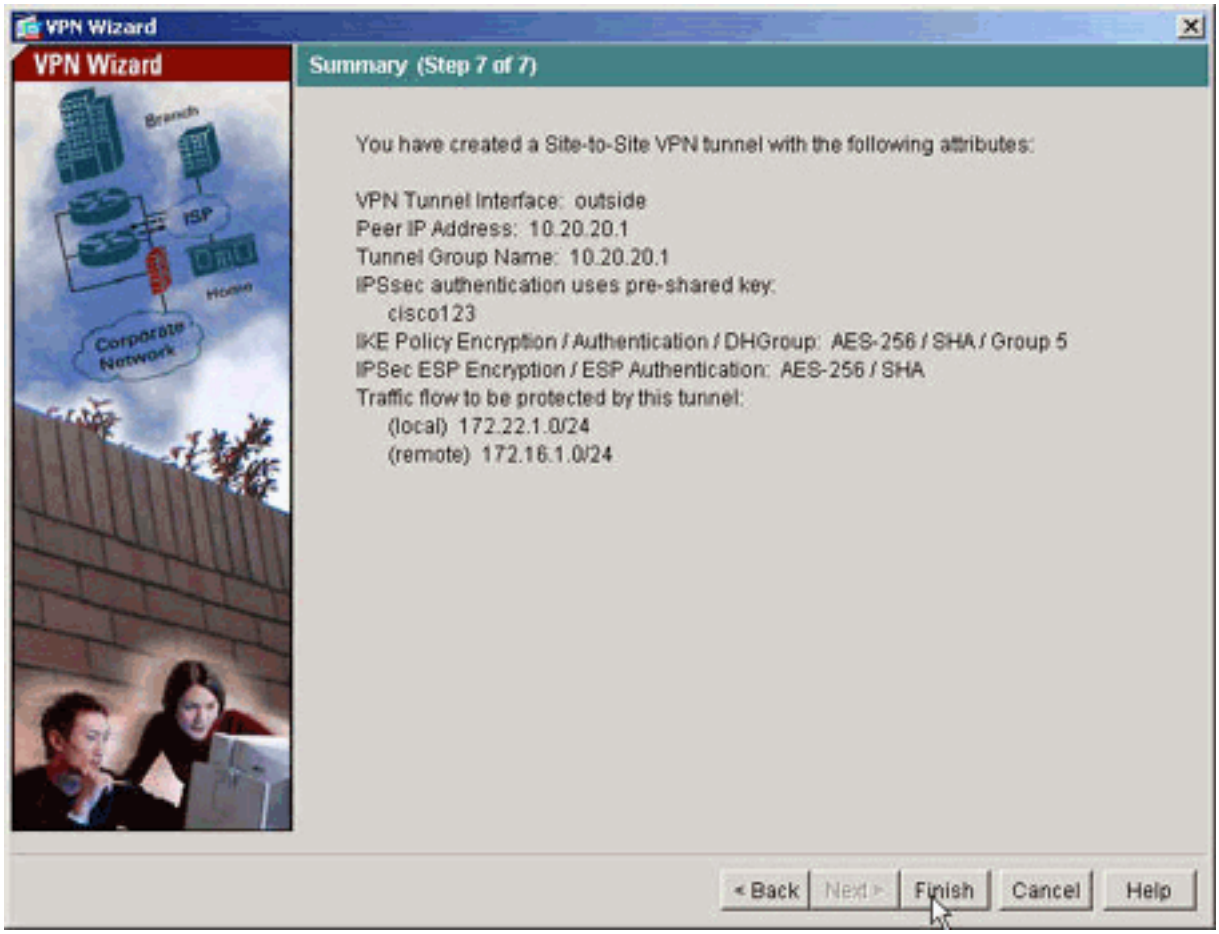
10. VPN トンネルを通過できるようなトラフィックのホストを指定します。 この手順では、ASA1 にローカルなホストを指定します。



11. トンネルのリモート側のホストとネットワークを指定します。



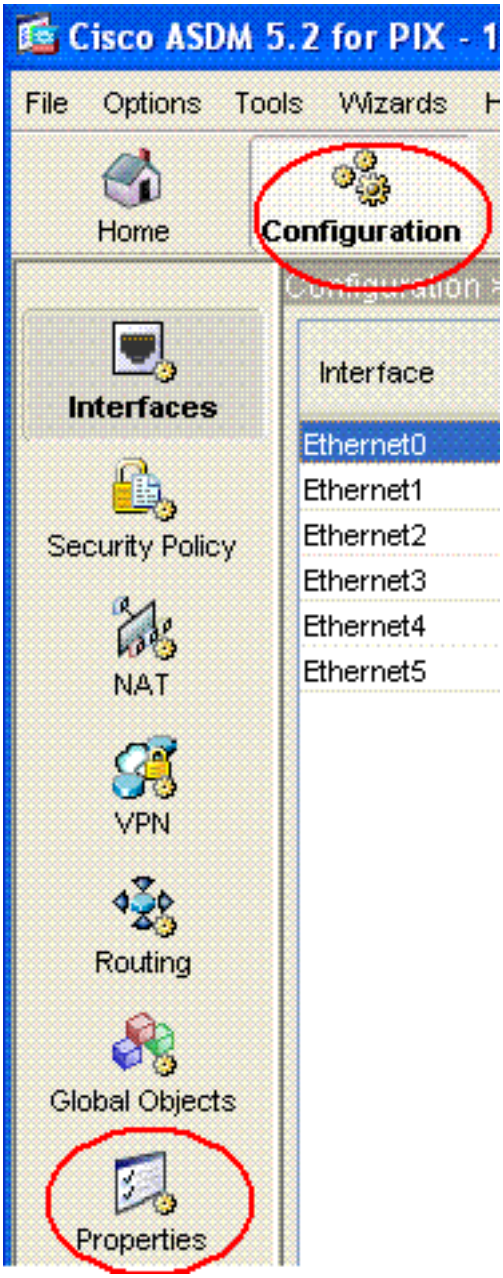
12. VPN Wizardによって定義された属性が、次の要約画面に表示されます。. 設定を再確認し、設定が正しいことを確認したら [Finish] をクリックします。



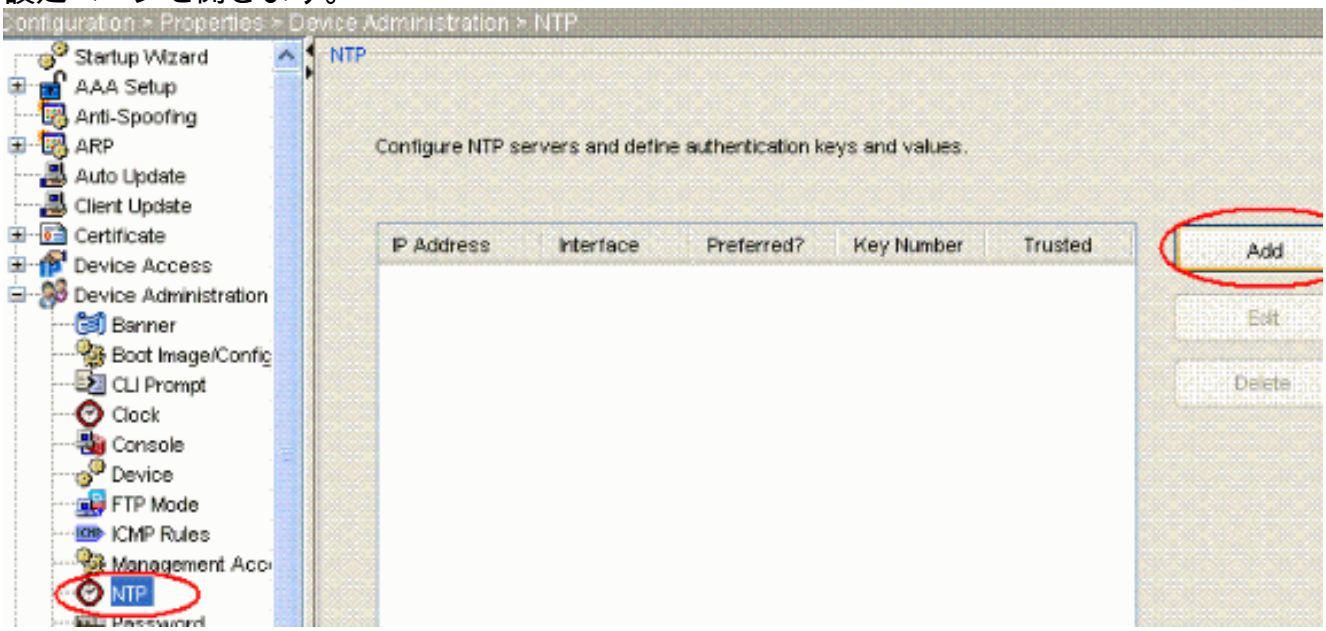
NTP ASDM の設定

Cisco セキュリティ アプライアンスで NTP を設定するには、以下の手順を実行してください。

1. 次に示すように、ASDM のホームページで [Configuration] を選択します。

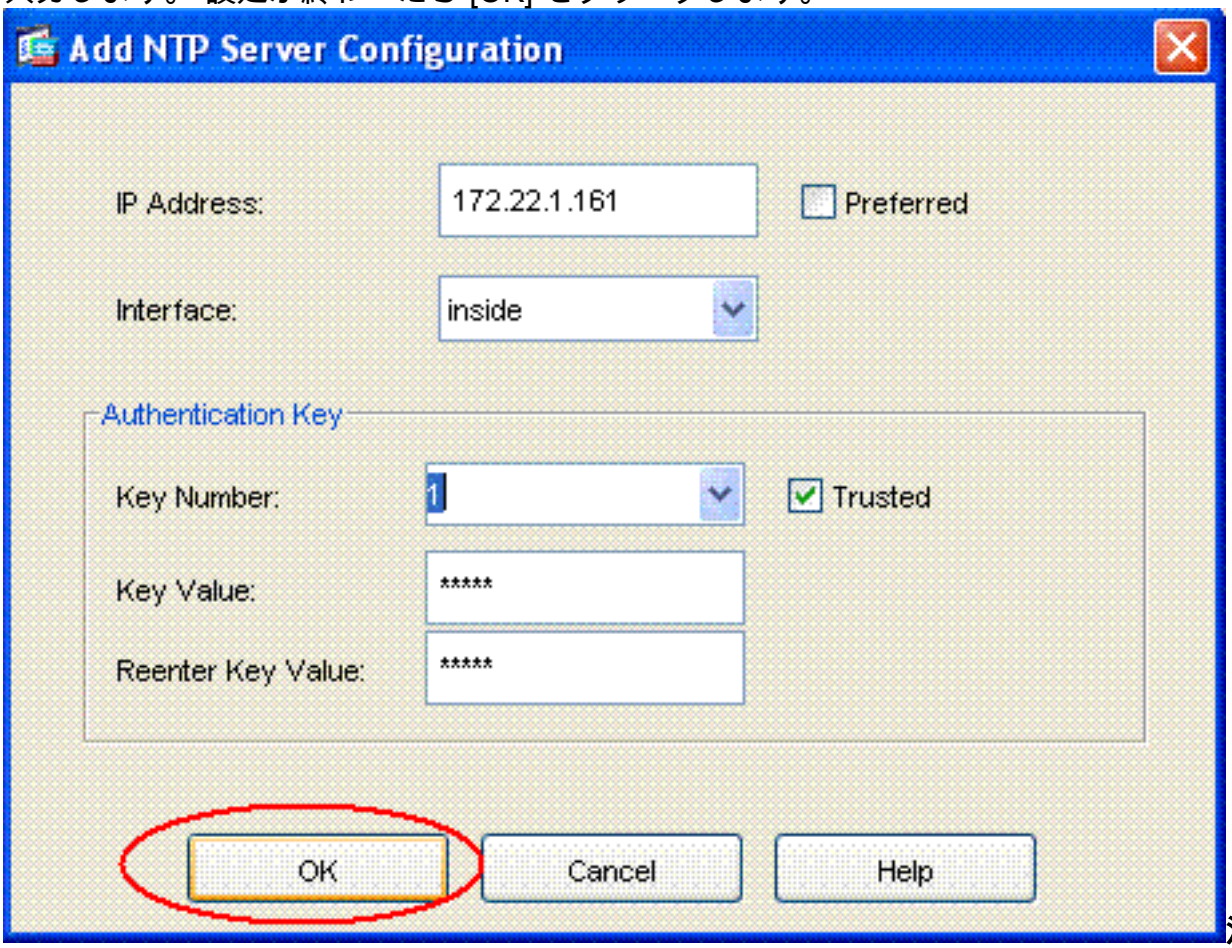


2. 次に、[Properties] > [Device Management] > [NTP] を選択し、以下に示す ASDM の **NTP** の設定ページを開きます。



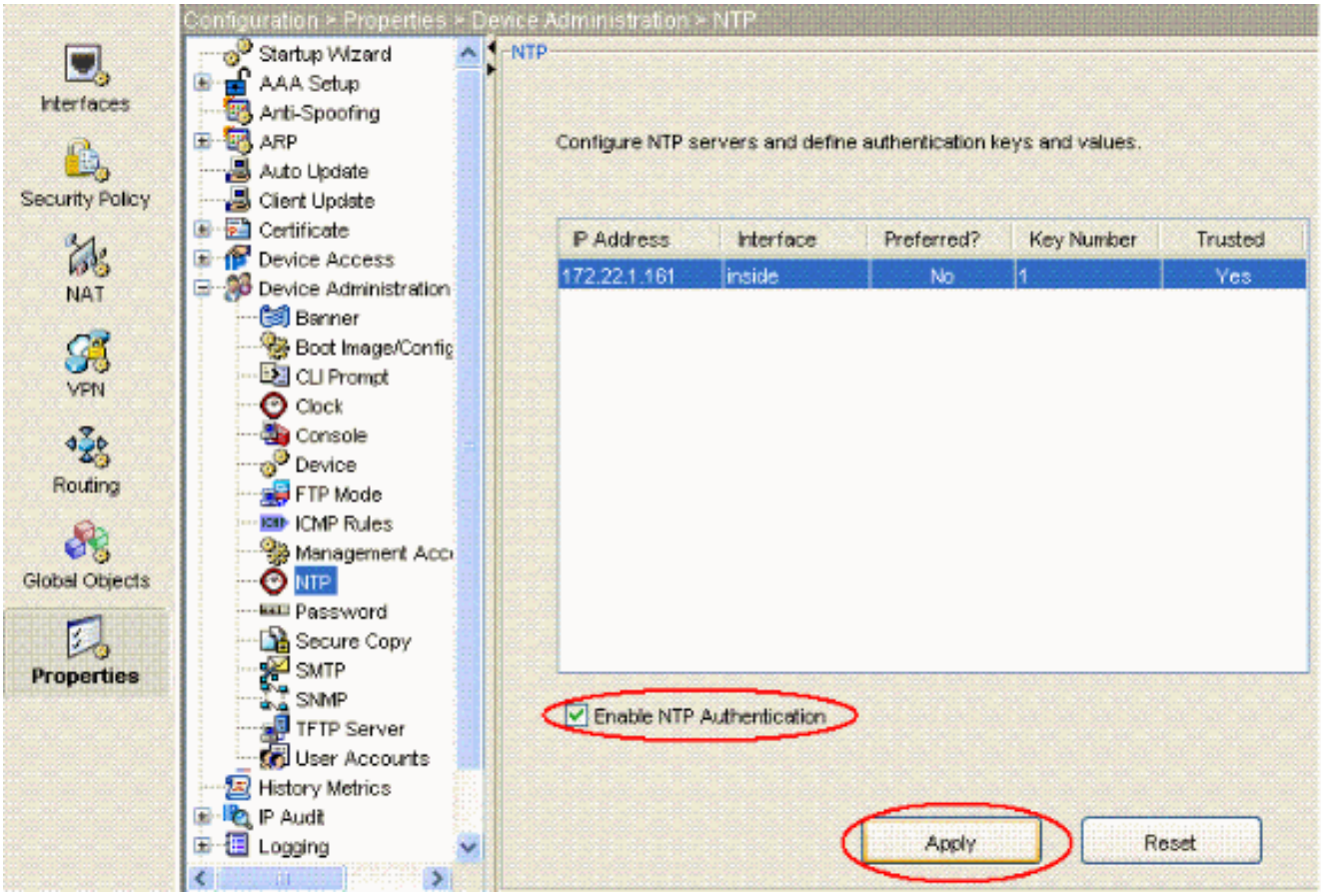
3. NTP サーバを追加するために [Add] ボタンをクリックします。[Add] ボタンをクリックした

後に表示される新しいウィンドウで、次のスクリーン ショットに示すように、IP アドレス、インターフェイス名（内部または外部）、認証用のキー番号とキー値などの必要な属性を入力します。 設定が終わったら [OK] をクリックします。



注: インターフェイス名として、ASA1 では [inside]、ASA2 では [outside] を選択する必要があります。**注: NTP の認証キー**は、ASA と NTP サーバで同じである必要があります。ASA1 と ASA2 の CLI での認証属性設定を以下に示します。`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. 次に、[Enable NTP Authentication] チェック ボックスをオンにし、[Apply] をクリックして、NTP の設定作業を完了します。



ASA1 CLI の設定

ASA1

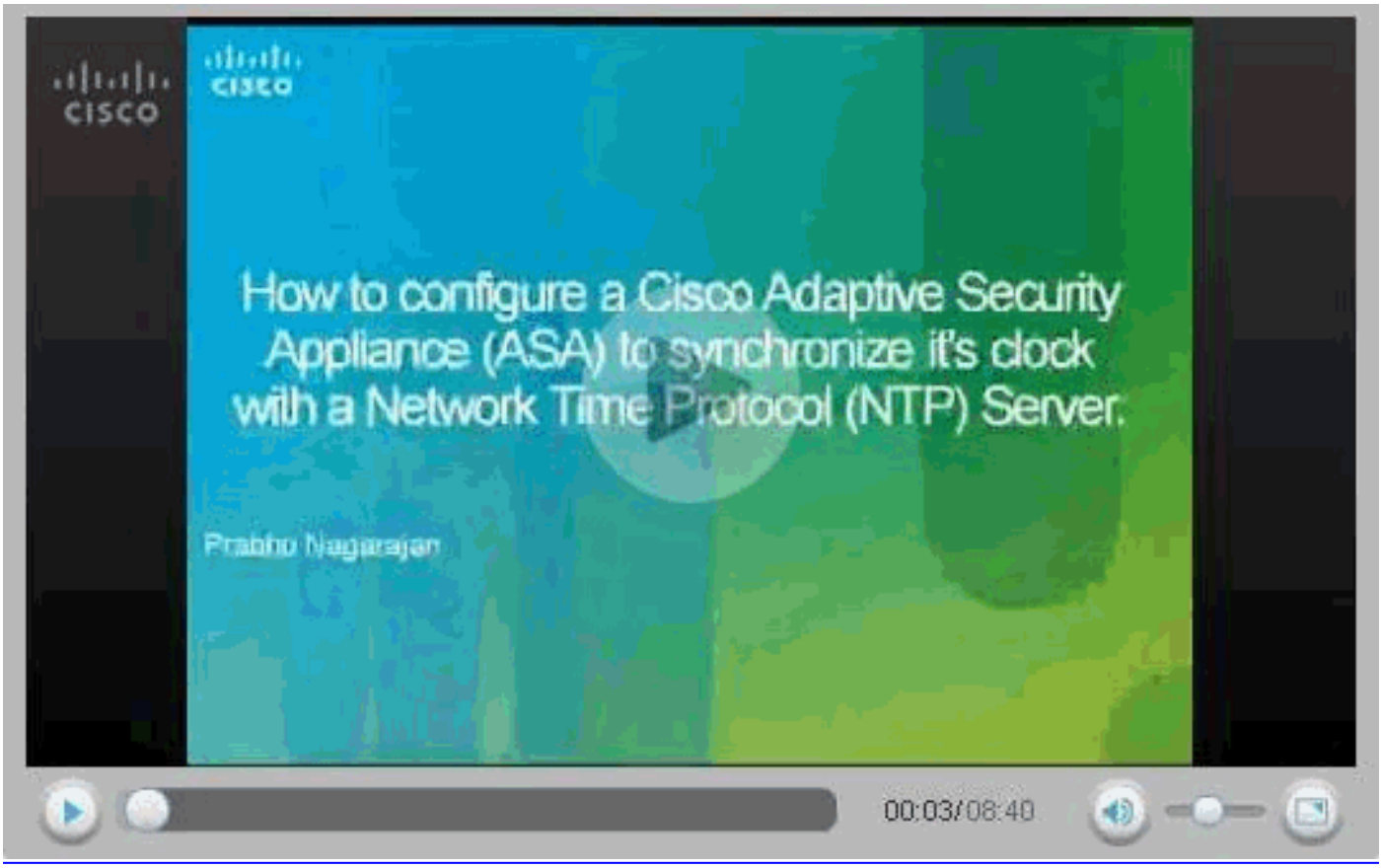
```
ASA#show run : Saved ASA Version 7.1(1) ! hostname ASA1
domain-name default.domain.invalid enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0
nameif outside security-level 0 ip address 10.10.10.1
255.255.255.0 !--- Configure the outside interface. !
interface Ethernet1 nameif 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
```

シスコ サポート コミュニティ に投稿されたこのビデオは、 ASA を NTP クライアントとして設

定するための手順を説明するデモです。

クロックをネットワーク タイム プロトコル（NTP）サーバと同期するように Cisco 適応型セキュリティ アプライアンス（ASA）を設定する方法



ASA2 CLI の設定

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#
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- show ntp status ：NTP クロック情報を表示します。`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]：設定されているネットワーク タイム サーバとの関連付けを表示します。`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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- **debug ntp validity**：NTP ピア クロックの有効性を表示します。次の例は、キーが一致しない場合の **debug** 出力です。
  NTP: packet from 172.22.1.161 failed validity tests 10 Authentication failed
- **debug ntp packet**：NTP パケット情報を表示します。サーバから応答がない場合は、ASA に NTP xmit パケットだけが表示され、NTP rcv パケットは表示されません。
```
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)
```

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems