# ASA/PIX:IPsec 터널 컨피그레이션 포함 및 없는 NTP 예

## 목차



## 소개

이 문서에서는 NTP(Network Time Protocol)를 사용하여 PIX/ASA Security Appliance 시계를 네트워크 시간 서버와 동기화하는 샘플 컨피그레이션을 제공합니다.ASA1은 네트워크 시간 서버와 직접 통신합니다.ASA2는 IPsec 터널을 통해 NTP 트래픽을 ASA1로 전달하며, ASA1은 패킷을 네트워크 시간 서버로 전달합니다.

ASA 8.3 이상을 참조하십시오.버전 8.3 이상의 Cisco ASA에서 동일한 컨피그레이션에 대한 자세한 내용은 IPsec 터널 컨피그레이션을 포함 및 포함하지 않는 NTP를 참조하십시오.

**참고:** 라우터는 PIX/ASA Security Appliance 시계를 동기화하는 데 NTP 서버로 사용할 수도 있습니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 이 NTP 컨피그레이션을 시작하기 전에 엔드 투 엔드 IPsec 연결을 설정해야 합니다.

- DES(Data Encryption Standard) 암호화(최소 암호화 수준)에 대해 Security Appliance 라이센스를 활성화해야 합니다.

## 사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 버전 7.x 이상
- ASDM 버전 5.x.이상

**참고:** ASDM에서 ASA를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 관련 제품

이 컨피그레이션은 버전 7.x 이상을 실행하는 Cisco PIX 500 Series Security Appliance에서도 사용할 수 있습니다.

**참고:** PIX 버전 6.2에 NTP 지원이 추가되었습니다. PIX 6.2를 참조하십시오.Cisco PIX Firewall에서 NTP를 구성하기 위한 IPsec Tunnel Configuration 예시 및 IPsec Tunnel Configuration 포함 안 함

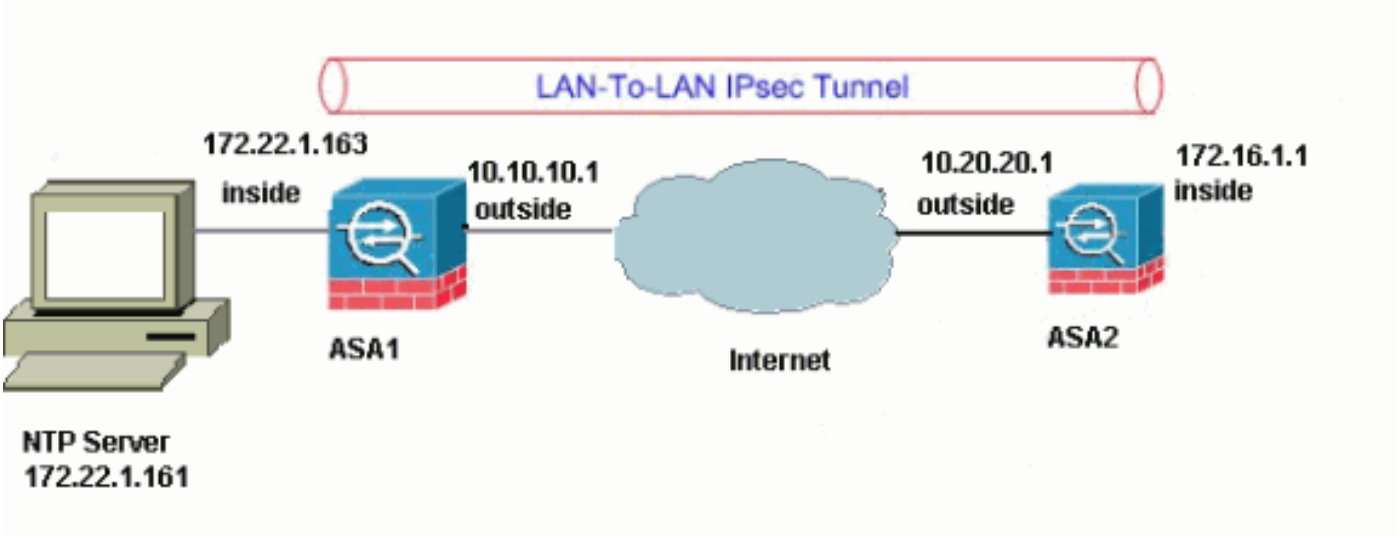
## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

# 구성

## 네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.




**참고:** 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실

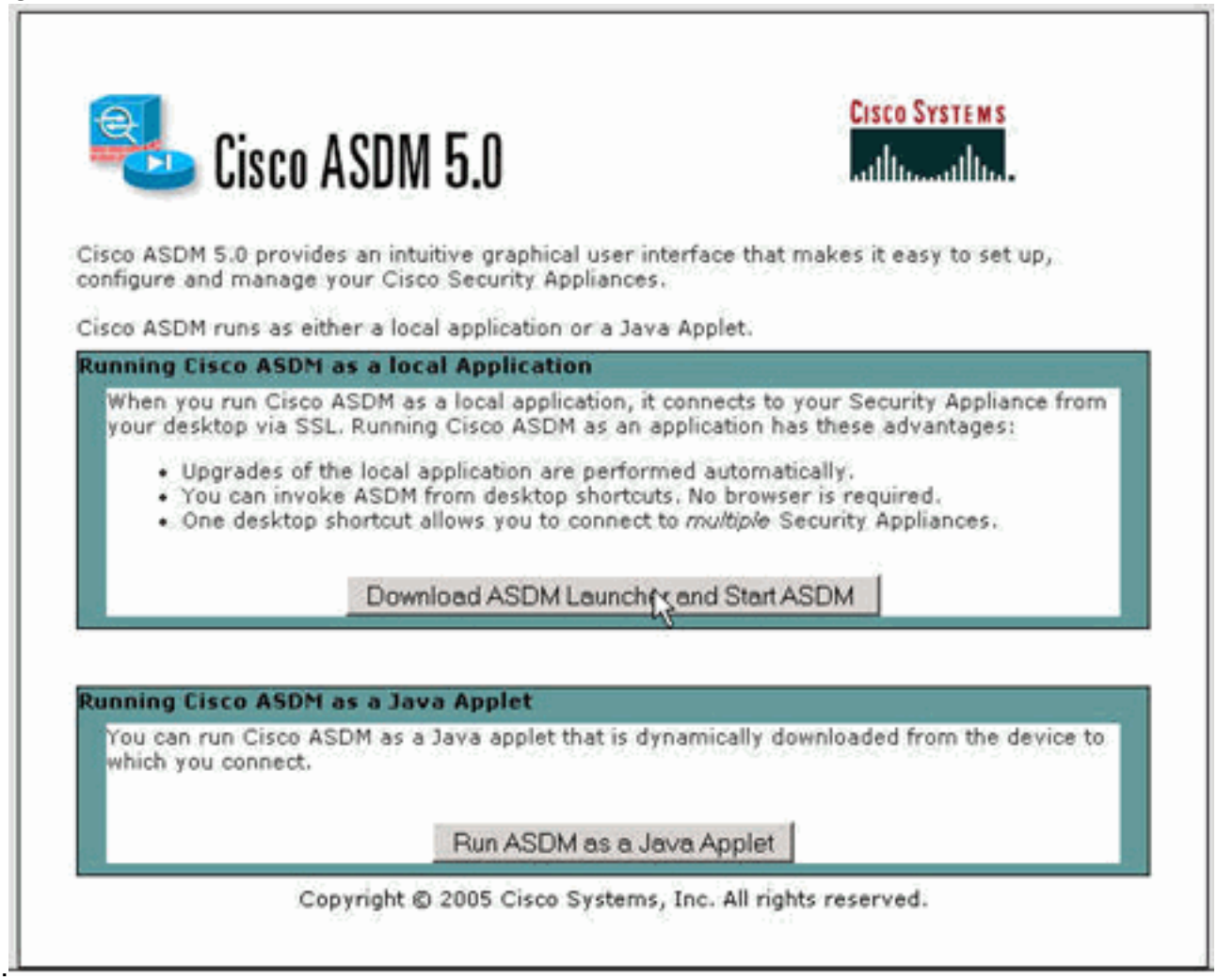
습 환경에서 사용된 RFC 1918 주소입니다.

- VPN 터널 ASDM 컨피그레이션
- NTP ASDM 컨피그레이션
- ASA1 CLI 컨피그레이션
- ASA2 CLI 컨피그레이션

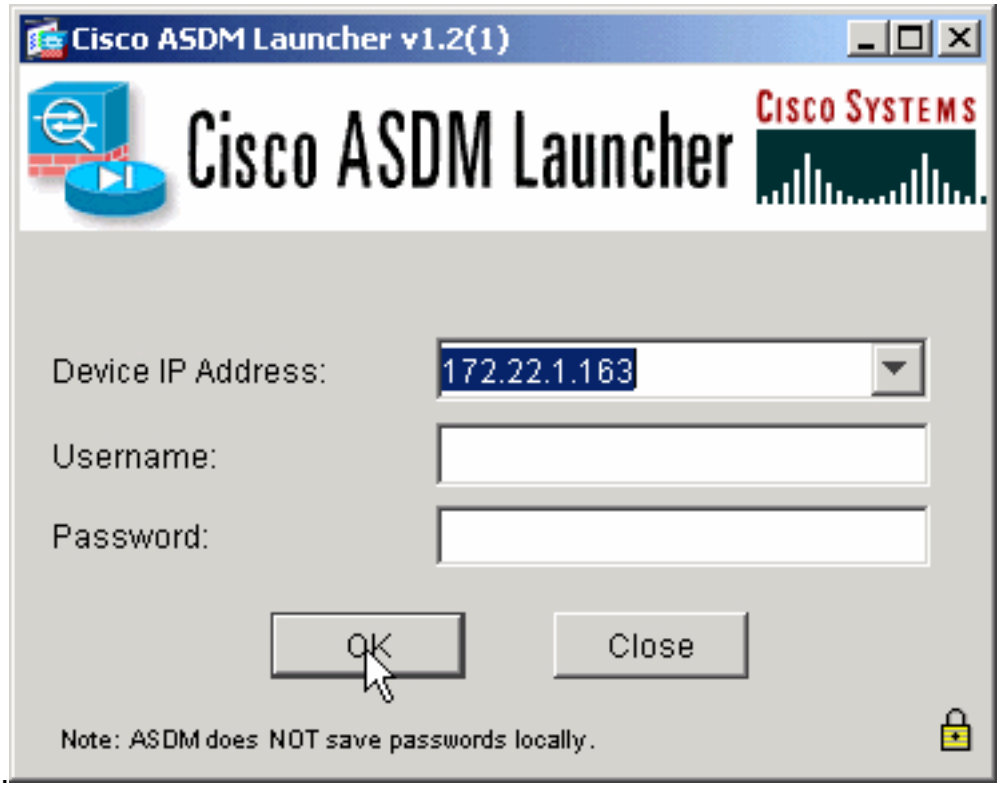
## VPN 터널 ASDM 컨피그레이션

VPN 터널을 생성하려면 다음 단계를 완료합니다.

1. 브라우저를 열고 **https://<Inside_IP_Address_of_ASA>를 입력하여** ASA의 ASDM에 액세스합니다.브라우저에서 SSL 인증서 신뢰성과 관련된 경고를 승인해야 합니다.기본 사용자 이름과 비밀번호는 모두 비어 있습니다.ASA는 ASDM 애플리케이션을 다운로드할 수 있도록 이 창을 표시합니다.이 예에서는 응용 프로그램을 로컬 컴퓨터에 로드하며 Java 애플릿에서 실행되지 않습니다



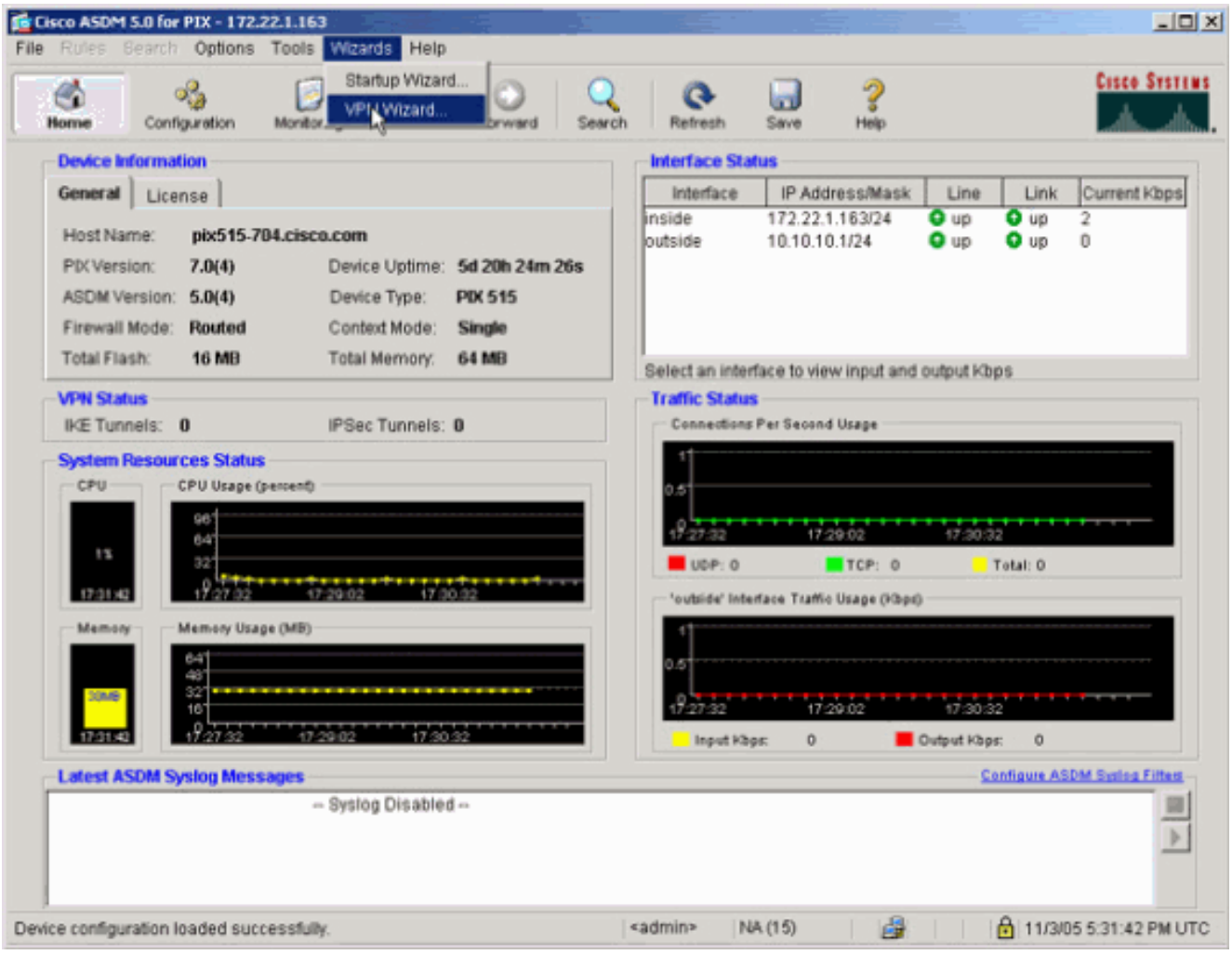

2. ASDM 애플리케이션 **설치** 프로그램을 다운로드하려면 **Download ASDM Launcher and Start ASDM(ASDM 시작** 시작 **시작**)을 클릭합니다.
3. ASDM Launcher가 다운로드되면, 소프트웨어를 설치하고 Cisco ASDM Launcher를 실행하기 위해 프롬프트에 의해 지시된 단계를 완료합니다.
4. **http -** 명령으로 구성한 인터페이스의 IP 주소와 사용자 이름 및 비밀번호를 지정한 경우 입력합니다.이 예에서는 기본 빈 사용자 이름과 비밀번호를 사용합니다



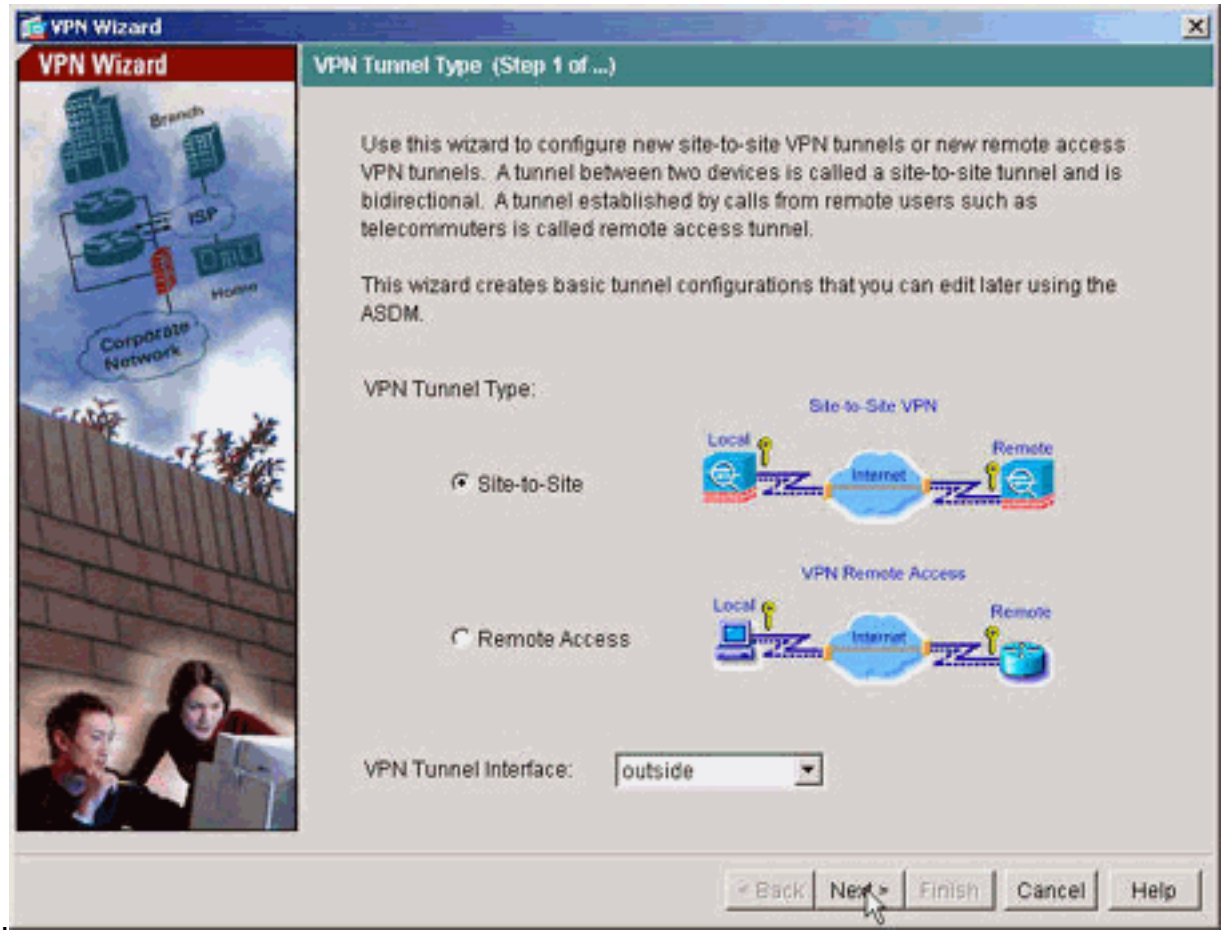

.

5. ASDM 애플리케이션이 ASA에 연결되면 VPN 마법사를 실행합니다

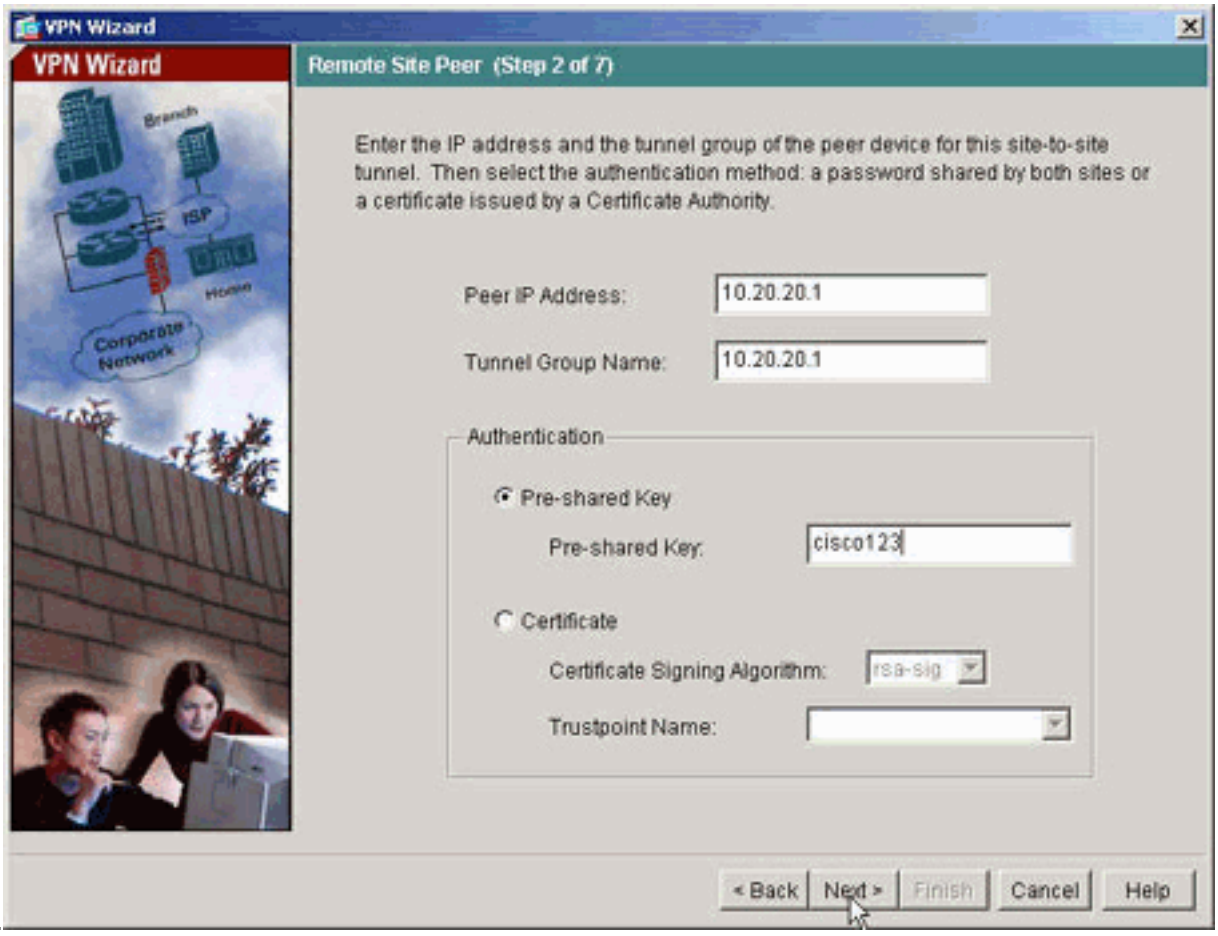
.




6. Site-**to-Site IPsec** VPN 터널 유형을 선택합니다

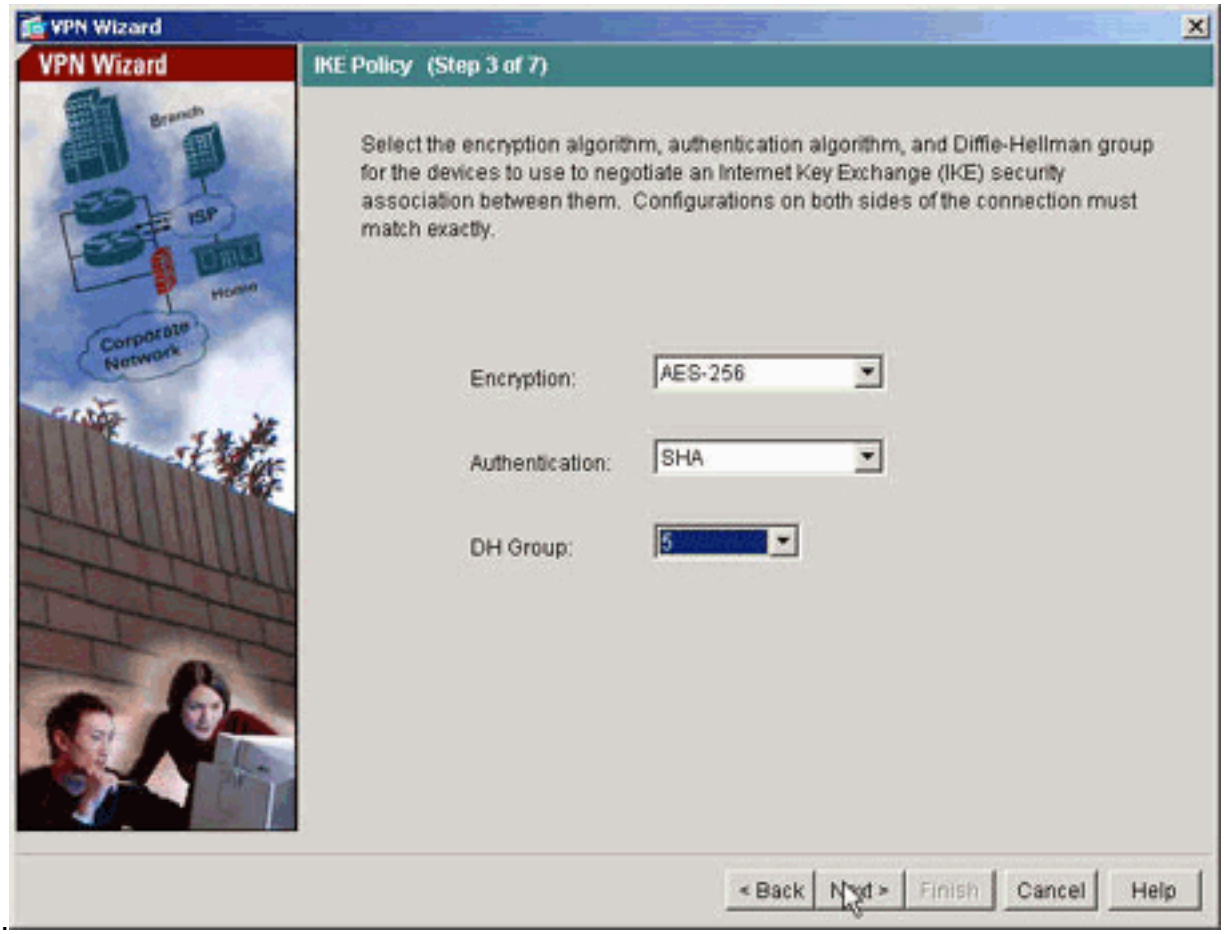



7. 원격 피어의 외부 IP 주소를 지정합니다.이 예에서 사전 공유 키인 사용할 인증 정보를 입력합

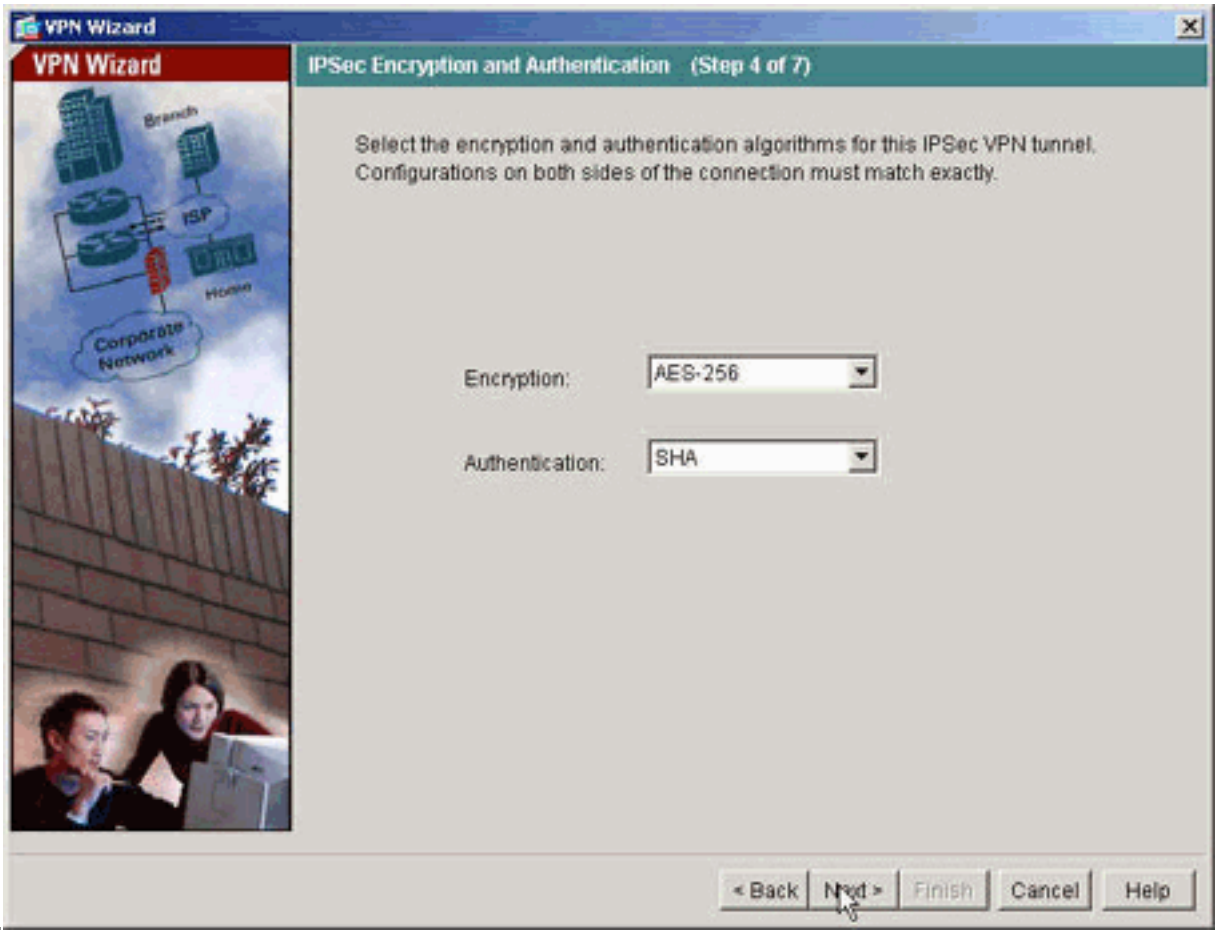



니다.

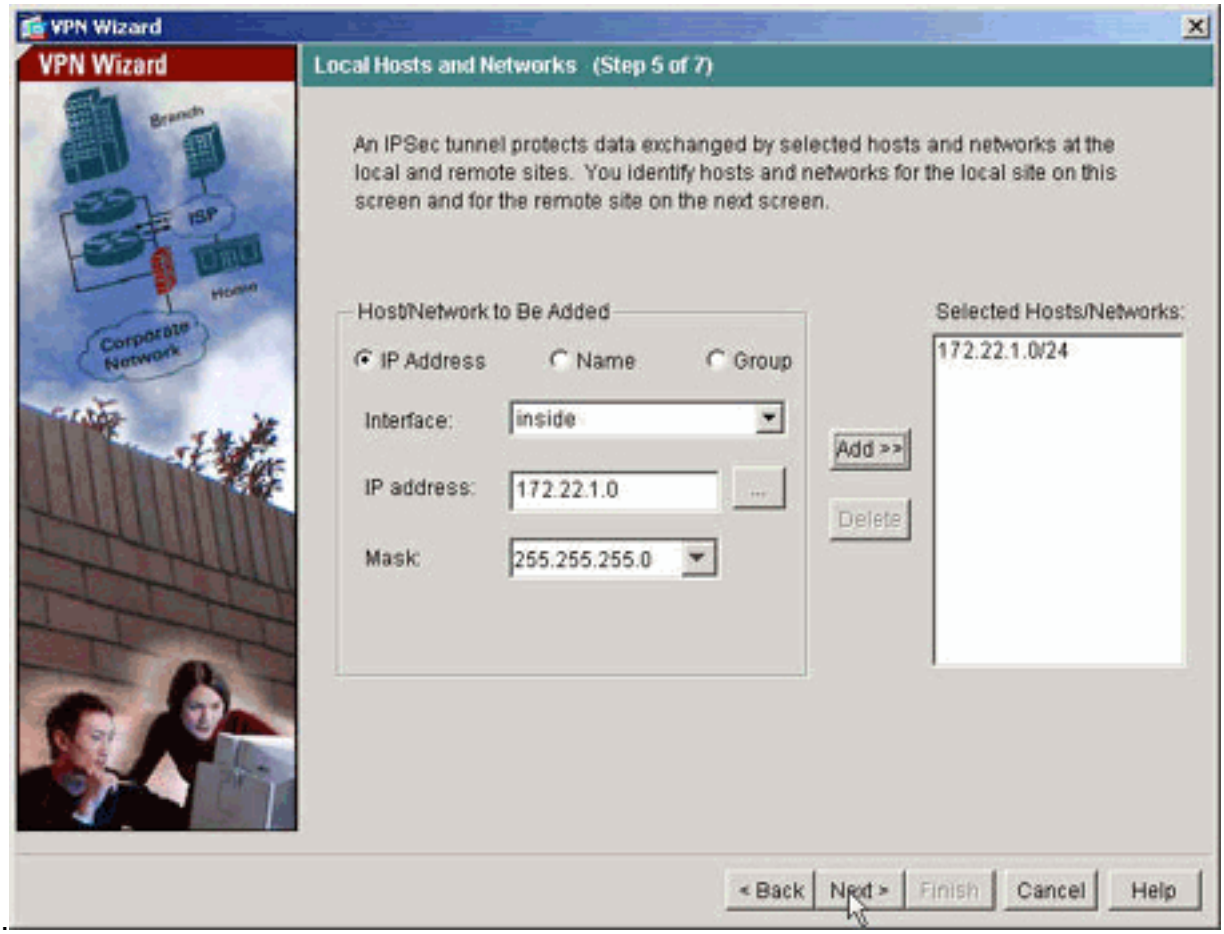
8. IKE에 사용할 특성을 1단계라고도 합니다. 이러한 특성은 터널의 양쪽에서 동일해야 합니다



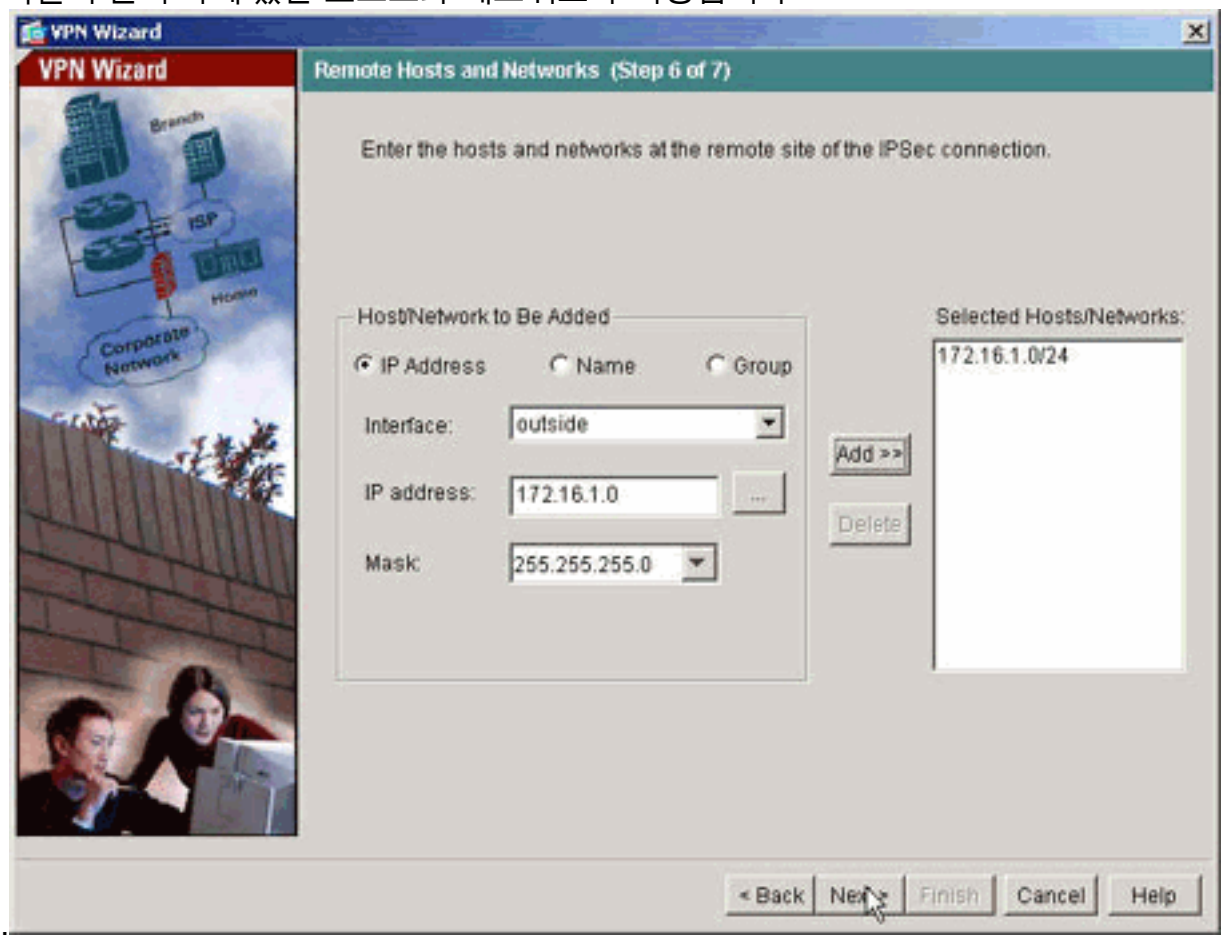

9. 2단계라고도 하는 IPsec에 사용할 특성을 지정합니다. 이러한 특성은 양쪽에서 일치해야 합니다.



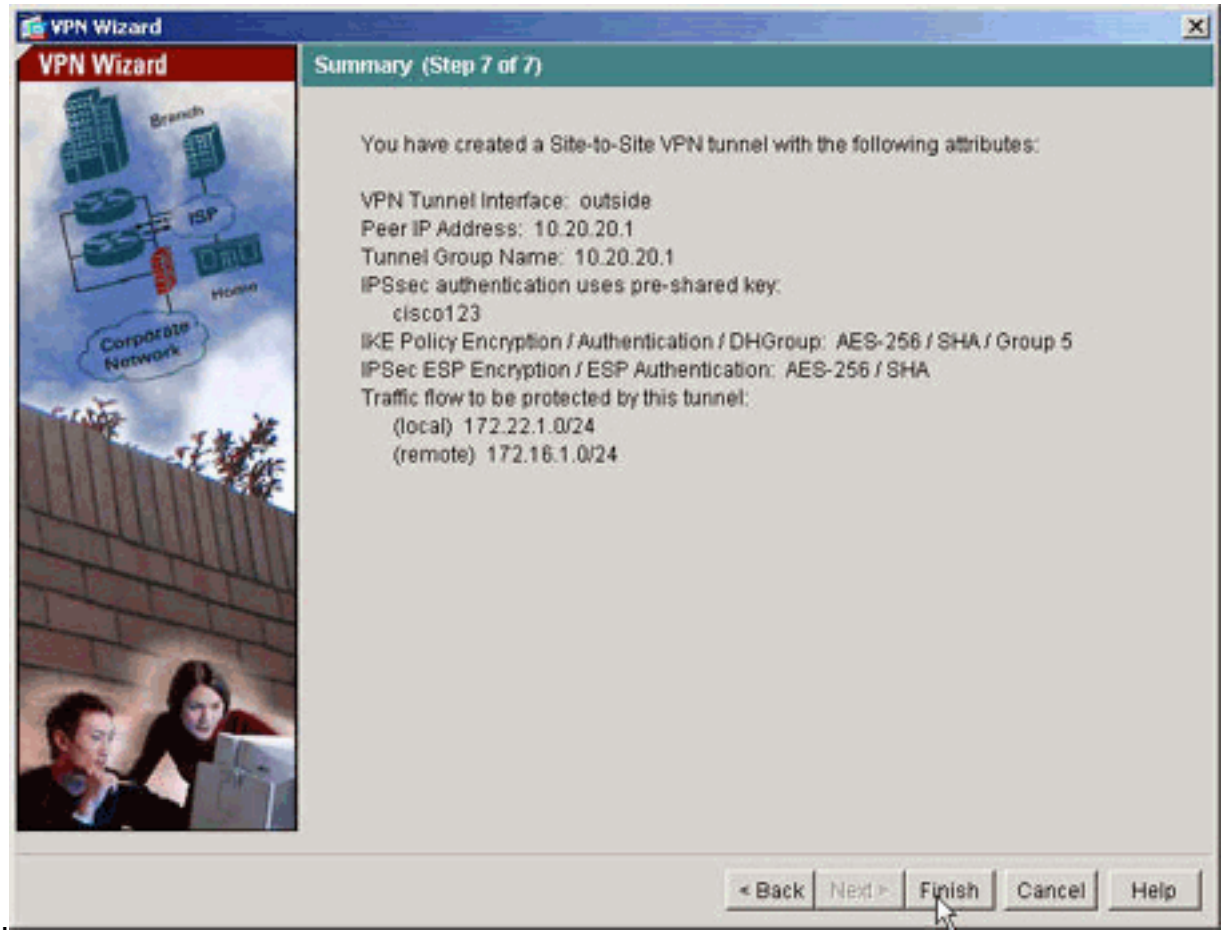

10. VPN 터널을 통과하도록 트래픽을 허용할 호스트를 지정합니다.이 단계에서는 ASA1에 로컬인 호스트가 지정됩니다




11. 터널의 원격 쪽에 있는 호스트와 네트워크가 지정됩니다



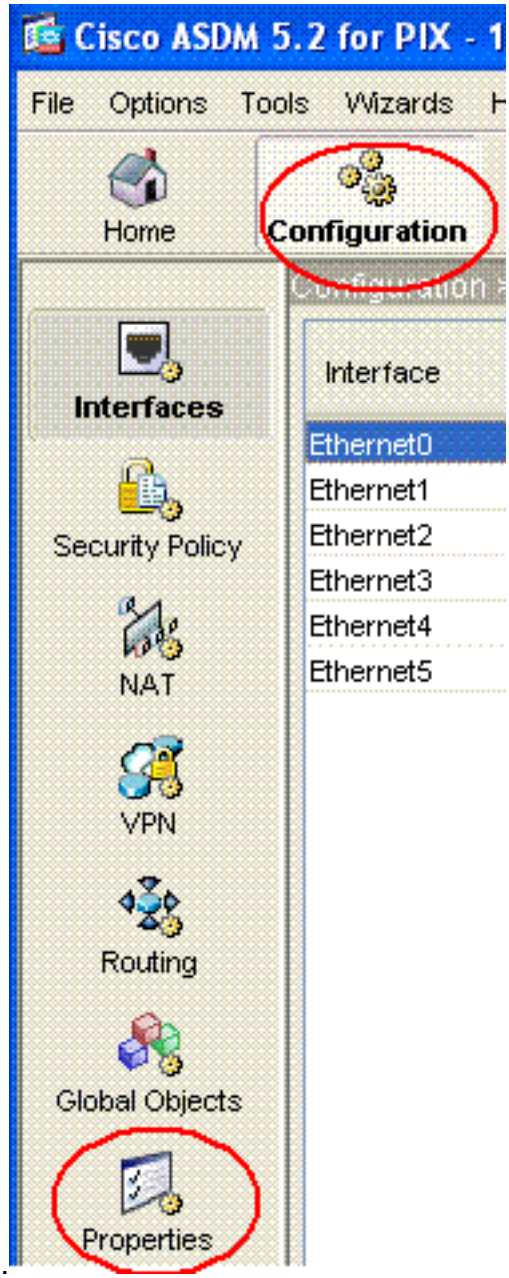

12. VPN 마법사에서 정의한 특성이 이 요약에 표시됩니다.설정이 올바르면 구성을 다시 확인하고 **Finish(마침)**를 클릭합니다




## NTP ASDM 컨피그레이션

Cisco Security Appliance에서 NTP를 구성하려면 다음 단계를 완료합니다.

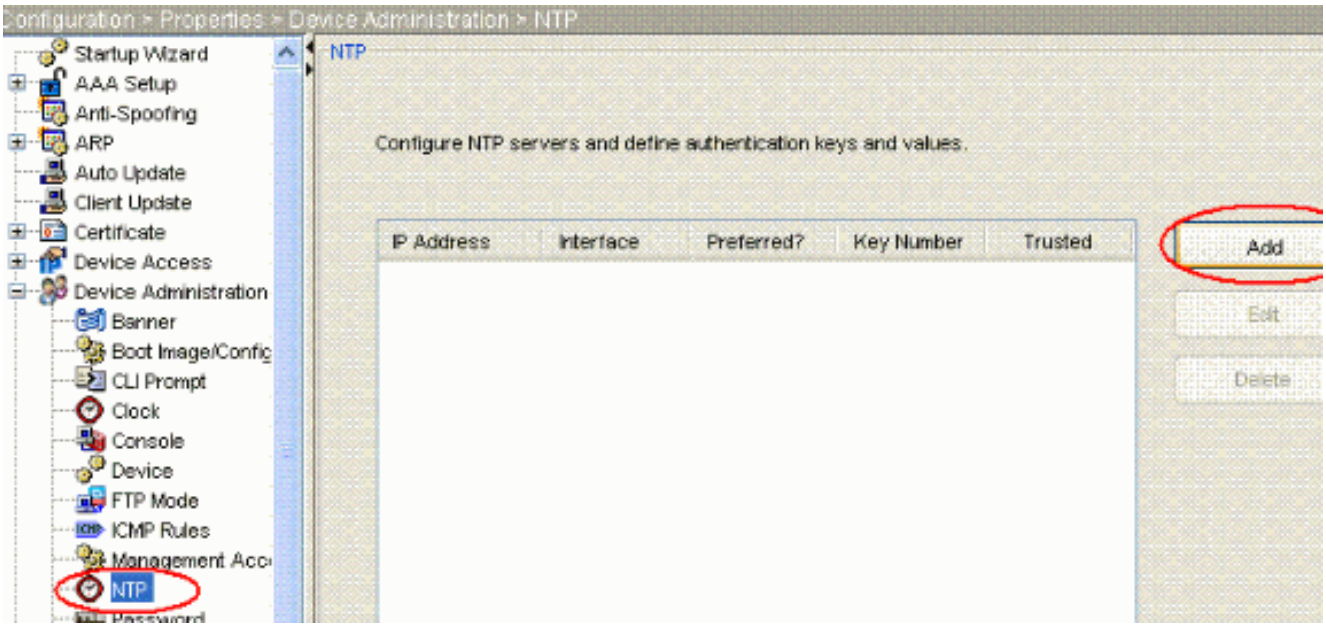
1. ASDM 홈 페이지에서 다음과 같이 Configuration을 선택합니다



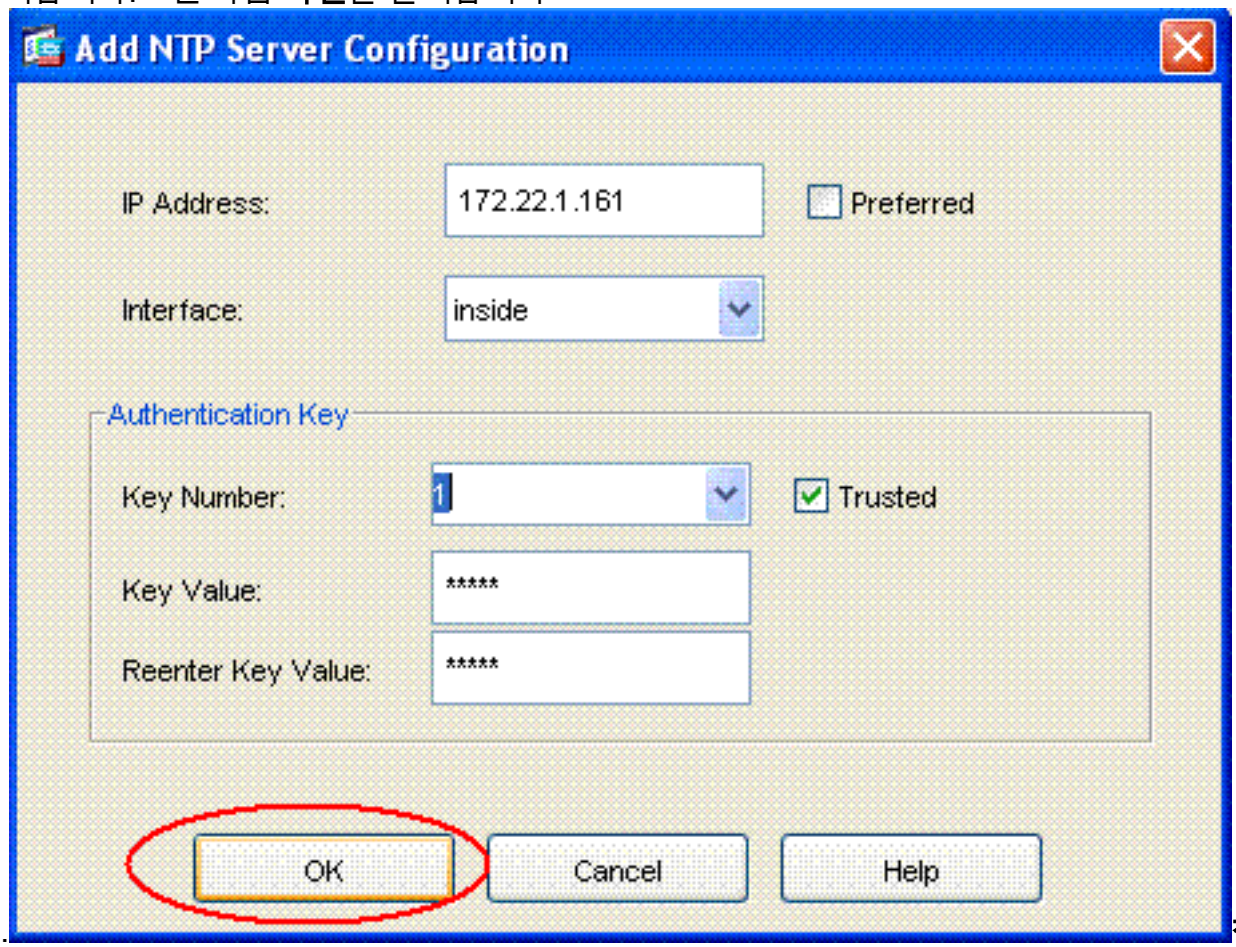

.

2. 이제 ASDM의 **NTP** 컨피그레이션 페이지**를 열려면 Properties(속성) > Device Management(디바이스 관리) > NTP**를 선택합니다

.



3. NTP 서버를 추가하고 **ADD** 버튼을 클릭한 후 표시되는 새 창에서 IP 주소, 인터페이스 이름(내부 또는 외부), 키 번호 및 인증 키 값과 같은 필수 특성을 제공하려면 ADD(**추가**) 버튼을 클릭합니다.그런 다음 **확인**을 클릭합니다

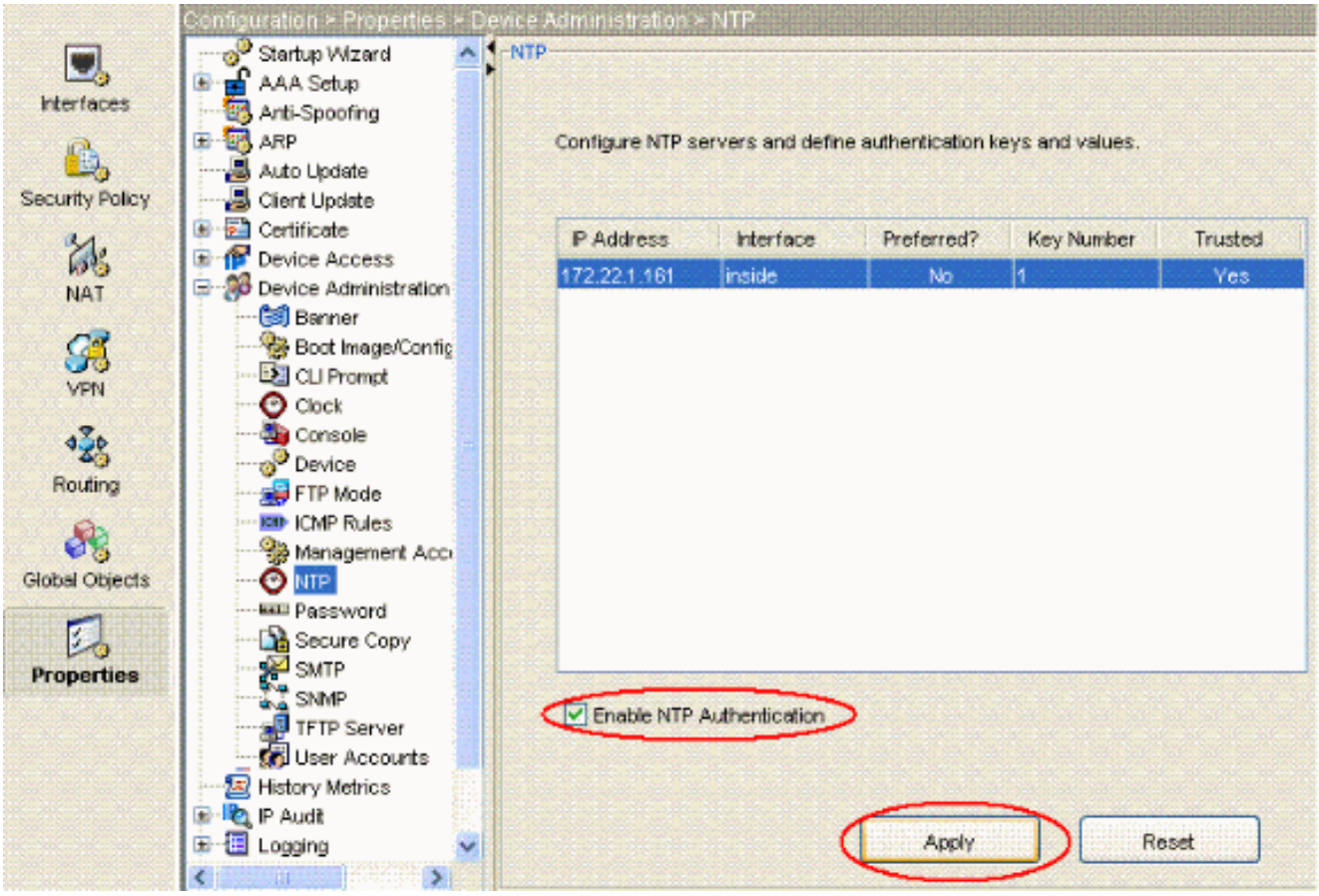



**참고:** 인터페이스 이름은 ASA1의 내부 및 ASA2의 외부 이름으로 선택해야 합니다.**참고:** ntp **인증 키는** ASA 및 NTP 서버에서 동일해야 합니다.ASA1 및 ASA2용 cli의 인증 특성 컨피그레이션은 다음과 같습니다.

```
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. 이제 Enable NTP Authentication(**NTP 인증 활성화) 확인란을** 클릭하고 **Apply(적용)**를 클릭하여 NTP 컨피그레이션 작업을 완료합니다

.




## ASA1 CLI 컨피그레이션

**ASA1**

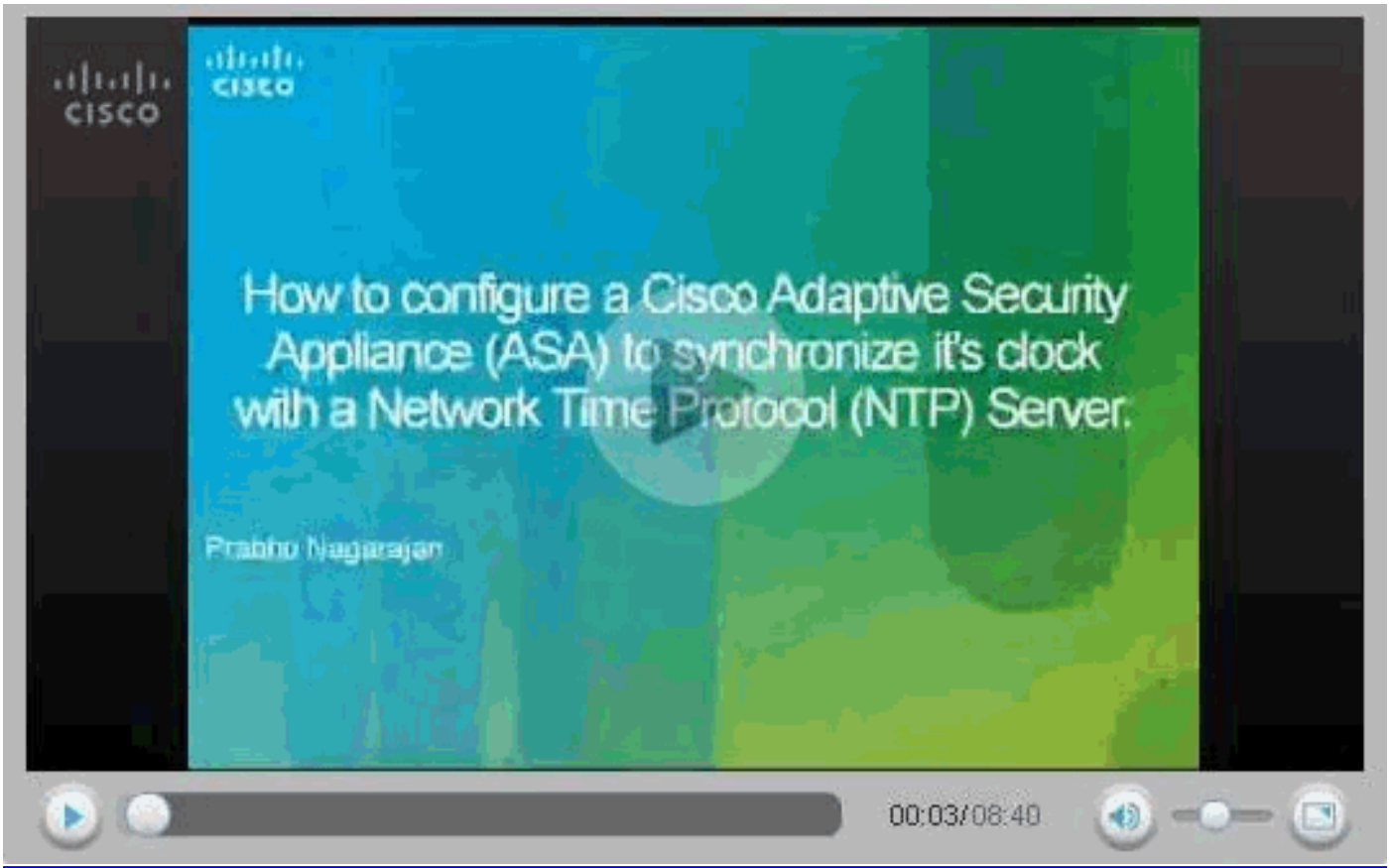
```
ASA#show run
: Saved
ASA Version 7.1(1)
!
hostname ASA1
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
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
```

Cisco Support Community에 게시된 이 비디오 데모에서는 ASA를 NTP 클라이언트로 구성하는 절차를 설명합니다.

시계를 NTP(Network Time Protocol) 서버와 동기화하도록 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법.




## ASA2 CLI 컨피그레이션

**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#
```

# 다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show ntp status** - NTP 시계 정보를 표시합니다.

```
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]** - 구성된 네트워크 시간 서버 연결을 표시합니다.

```
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
```

# 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

## 문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

**참고:** debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug ntp validity**—NTP 피어 클럭 유효성을 표시합니다.키 불일치의 디버그 출력입니다.

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

- **debug ntp packet** - NTP 패킷 정보를 표시합니다.서버에서 응답이 없을 경우 NTP rcv 패킷이 없는 ASA에서 NTP xmit 패킷만 .

```
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)
```

## 관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Secure PIX Firewall 명령 참조
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems