ASA/PIX - Cisco IOS 라우터 LAN-to-LAN IPsec 터널 구성

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
표기 규칙
배경 정보
구성
네트워크 다이어그램
구성
ASDM을 사용한 구성
다음을 확인합니다.
문제 해결
문제 해결 명령
관련 정보

소개

이 문서에서는 PIX Security Appliance 7.x 이상 또는 내부 네트워크 하나가 포함된 ASA(Adaptive Security Appliance)에서 암호화 이미지를 실행하는 2611 라우터에 IPsec 터널을 구성하는 방법을 설명합니다. 고정 경로는 간소화를 위해 사용됩니다.

라우터와 PIX 간의 LAN-to-LAN 터널 컨피그레이션에 대한 자세한 내용은 IPSec - 라우터에서 PIX로 구성 을 참조하십시오.

PIX Firewall과 Cisco VPN 3000 Concentrator 간의 LAN-to-LAN 터널 컨피그레이션에 대한 자세한 내용은 Cisco VPN 3000 Concentrator와 PIX 방화벽 컨피그레이션 사이의 LAN-to-LAN IPSec 터널을 참조하십시오.

PIX와 VPN Concentrator 사이에 LAN-to-LAN 터널이 있는 시나리오에 대한 자세한 내용은 PIX 7.x와 VPN 3000 Concentrator 간 IPsec 터널 구성 예를 참조하십시오.

PIX 간 LAN-to-LAN 터널을 통해 VPN 클라이언트가 허브 PIX를 통해 스포크 PIX에 액세스할 수 있는 시나리오에 대한 자세한 내용은 PIX/ASA 7.x Enhanced Spoke-to-Client VPN with TACACS+ Authentication Configuration 예를 참조하십시오.

SDM을 참조하십시오. PIX/ASA Security Appliance에서 소프트웨어 버전 8.x를 실행하는 동일한 시나리오에 대해 자세히 알아보려면 ASA/PIX와 IOS 라우터 간 Site-to-Site IPsec VPN 구성 예

Configuration Professional을 참조하십시오. ASA/PIX와 IOS 라우터 간 Site-to-Site IPsec VPN

ASDM GUI를 사용하여 ASA 관련 컨피그레이션이 표시되고 Cisco CP GUI를 사용하여 라우터 관련 컨피그레이션이 표시되는 동일한 시나리오에 대해 자세히 알아보려면 예를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX-525(PIX 소프트웨어 버전 7.0 포함)
- Cisco 2611 라우터(Cisco IOS® 소프트웨어 릴리스 12.2(15)T13 포함)

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

PIX에서 **access-list** 및 **nat 0** 명령이 함께 작동합니다. 10.1.1.0 네트워크의 사용자가 10.2.2.0 네트워크로 이동하면 액세스 목록을 사용하여 10.1.1.0 네트워크 트래픽을 NAT(Network Address Translation) 없이 암호화할 수 있습니다. 라우터에서 **route-map** 및 **access-list** 명령은 10.2.2.0 네트워크 트래픽이 NAT 없이 암호화되도록 허용하는 데 사용됩니다. 그러나 동일한 사용자가 다른 곳으로 이동하면 PAT(Port Address Translation)를 통해 172.17.63.230 주소로 변환됩니다.

이는 PAT를 통해 터널을 통해 트래픽이 PAT를 통과하지 못하도록 PAT Security Appliance에서 필요한 컨피그레이션 명령 및 PAT를 통해 실행하기 위해 인터넷에 대한 트래픽입니다.

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

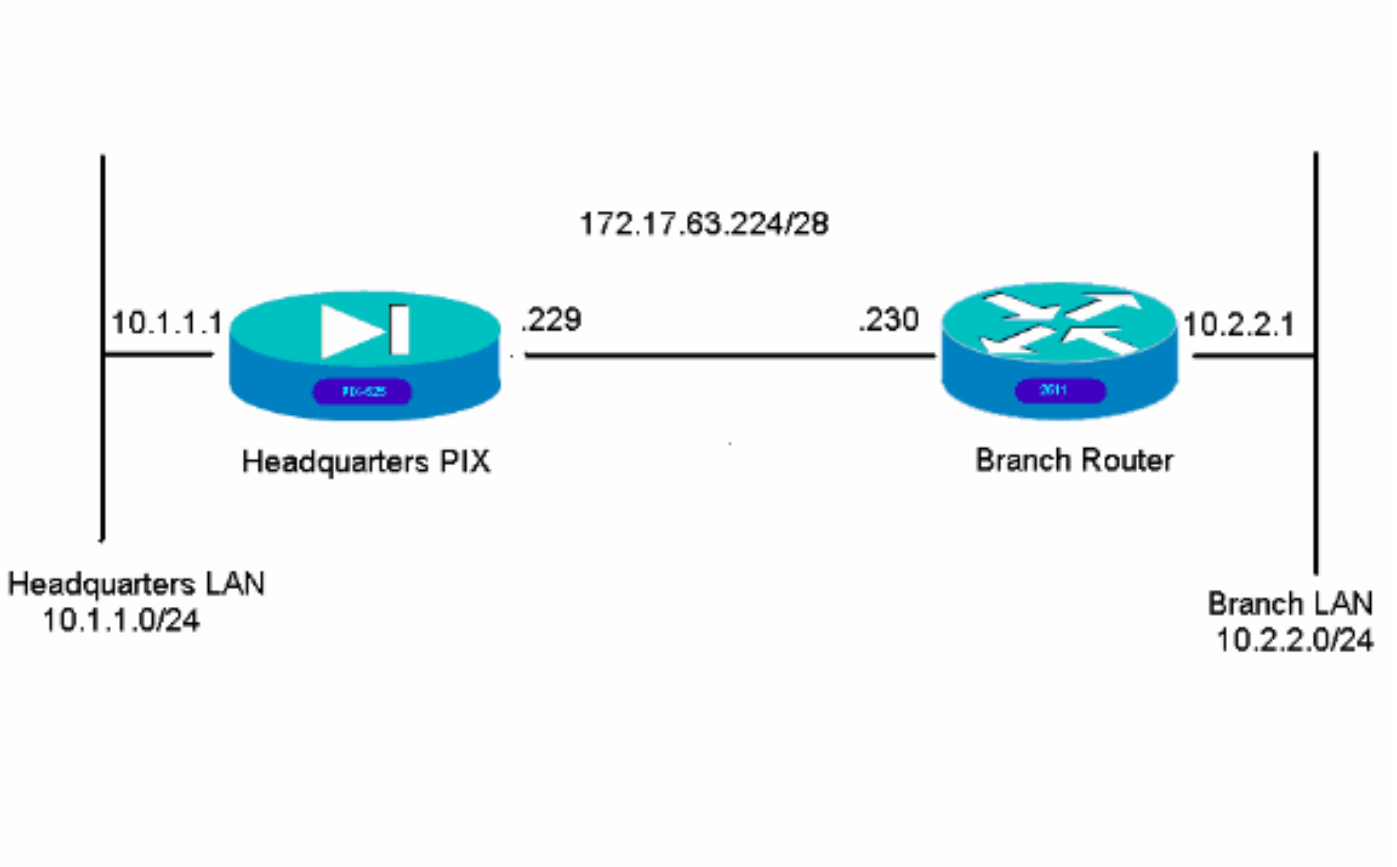
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이러한 컨피그레이션 예는 명령줄 인터페이스를 위한 것입니다. ASDM을 사용하여 구성하려면 이 문서의 Configuration using Adaptive Security Device Manager (ASDM) 섹션을 참조하십시오.

- 본사 PIX
- 브랜치 라우터

본사 PIX

```
HQPIX(config)#show run
PIX Version 7.0(0)102
names
!
interface Ethernet0
description WAN interface
nameif outside
security-level 0
ip address 172.17.63.229 255.255.255.240
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
```

```
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HQPIX
domain-name cisco.com
ftp mode passive
clock timezone AEST 10

access-list Ipsec-conn extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
access-list nonat extended permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0
pager lines 24
logging enable
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0
access-group 100 in interface inside
route outside 0.0.0.0 0.0.0.0 172.17.63.230 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
```

```
crypto ipsec transform-set avalanche esp-des esp-md5-
hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
crypto map forsberg 21 match address Ipsec-conn
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 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
telnet timeout 5
ssh timeout 5
console timeout 0
tunnel-group 172.17.63.230 type ipsec-l2l
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map asa_global_fw_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
inspect http
!
service-policy asa_global_fw_policy global
Cryptochecksum:3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
```

브랜치 라우터

```
BranchRouter#show run
Building configuration...

Current configuration : 1719 bytes
!
! Last configuration change at 13:03:25 AEST Tue Apr 5
2005
```

```
! NVRAM config last updated at 13:03:44 AEST Tue Apr 5
2005
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname BranchRouter
!
logging queue-limit 100
logging buffered 4096 debugging
!
username cisco privilege 15 password 0 cisco
memory-size iomem 15
clock timezone AEST 10
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!
!
crypto isakmp policy 11
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.17.63.229
!
!
crypto ipsec transform-set sharks esp-des esp-md5-hmac
!
crypto map nolan 11 ipsec-isakmp
set peer 172.17.63.229
set transform-set sharks
match address 120
!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan
```

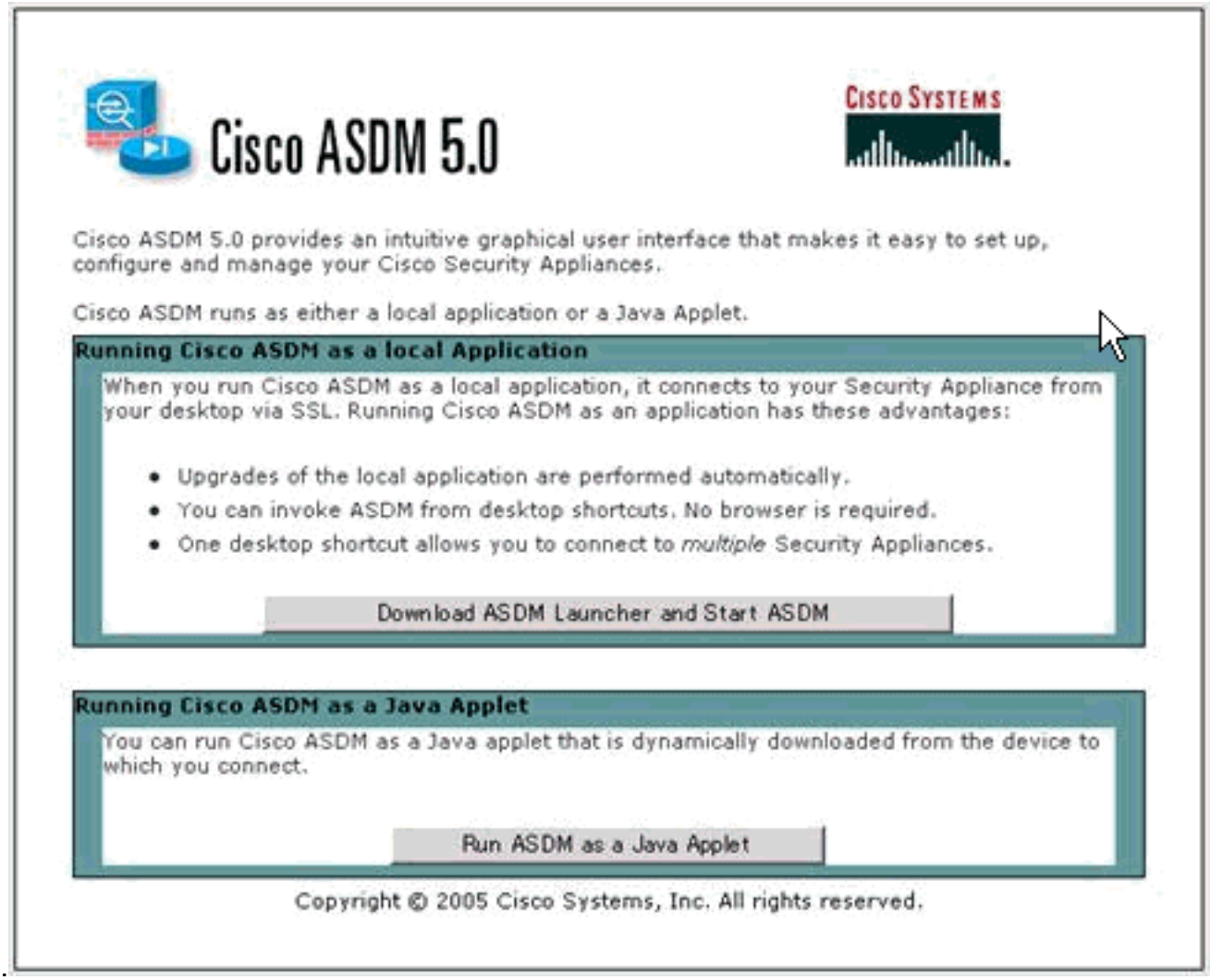
```
!
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex
!
ip nat pool branch 172.17.63.230 172.17.63.230 netmask
255.255.255.0
ip nat inside source route-map nonat pool branch
overload
no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
!
!
!
access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 130
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

ASDM을 사용한 구성

이 예에서는 ASDM GUI를 사용하여 PIX를 구성하는 방법을 보여 줍니다. 브라우저 및 IP 주소가 10.1.1.2인 PC가 PIX의 내부 인터페이스 e1에 연결됩니다. PIX에서 http가 활성화되어 있는지 확인합니다.

이 절차에서는 본사 PIX의 ASDM 컨피그레이션을 설명합니다.

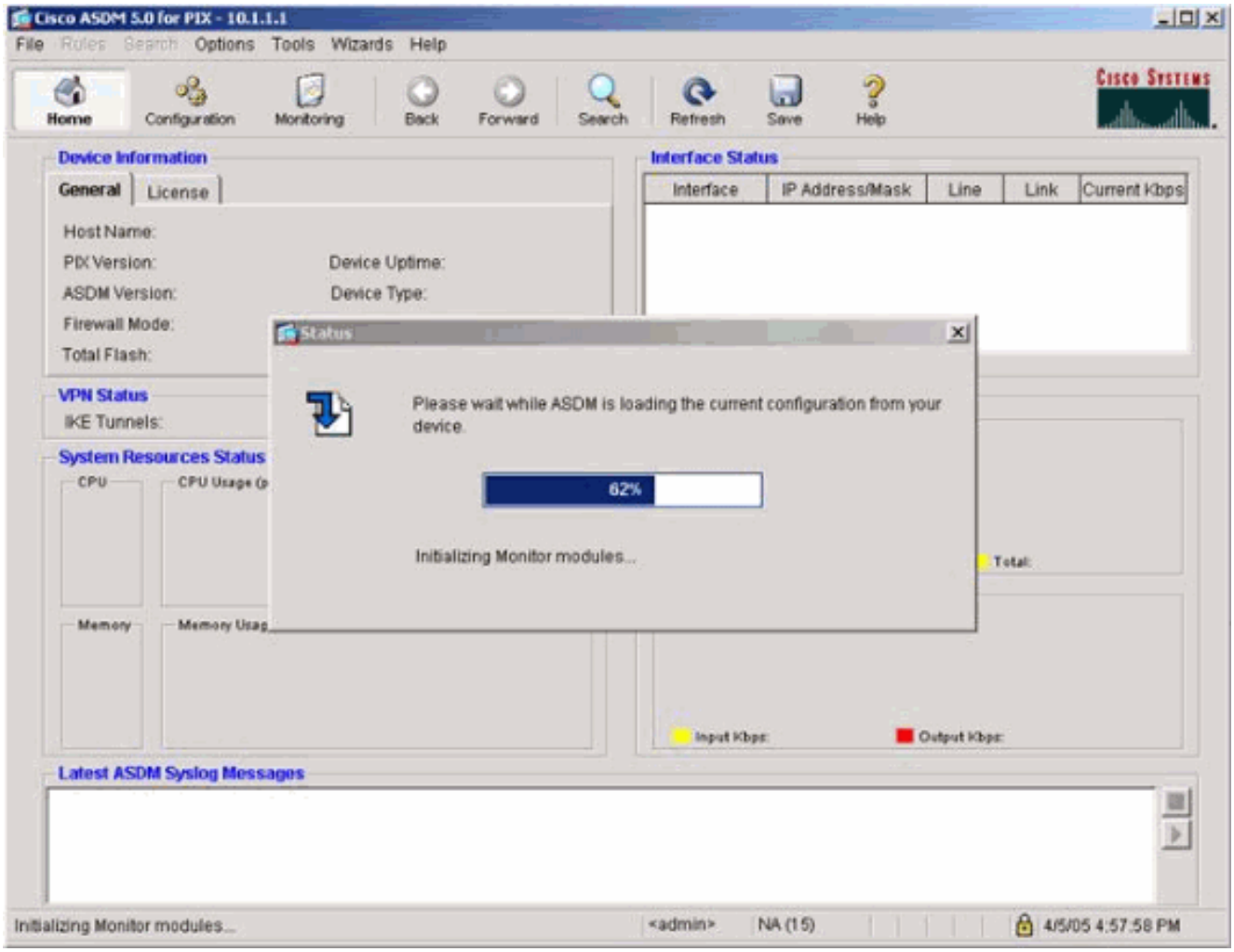
1. PC를 PIX에 연결하고 다운로드 방법을 선택합니다



.

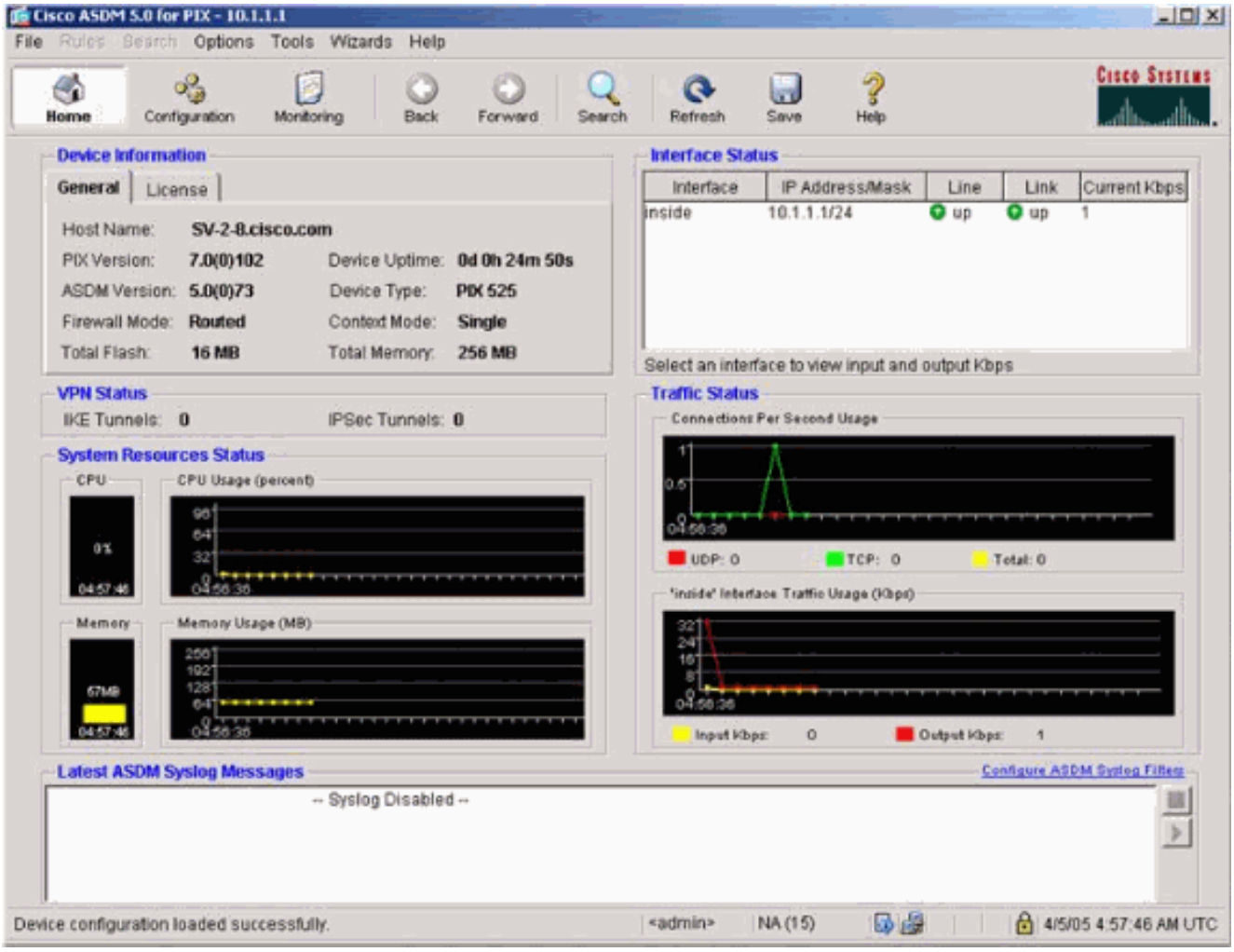
ASDM은 PIX에서 기존 컨피그레이션을 로드합니다

.



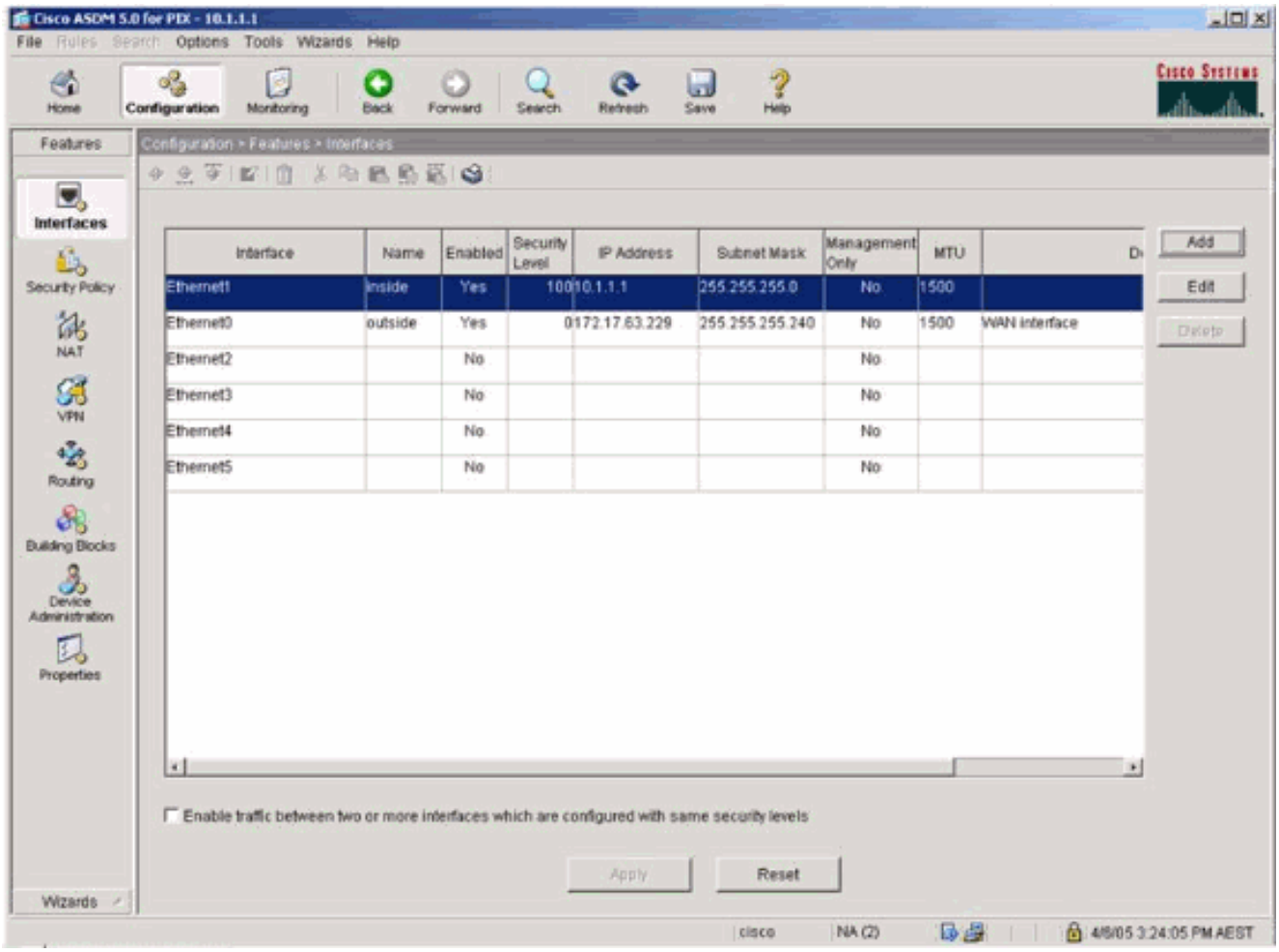
이 창에서는 모니터링 기기 및 메뉴를 제공합니다

.



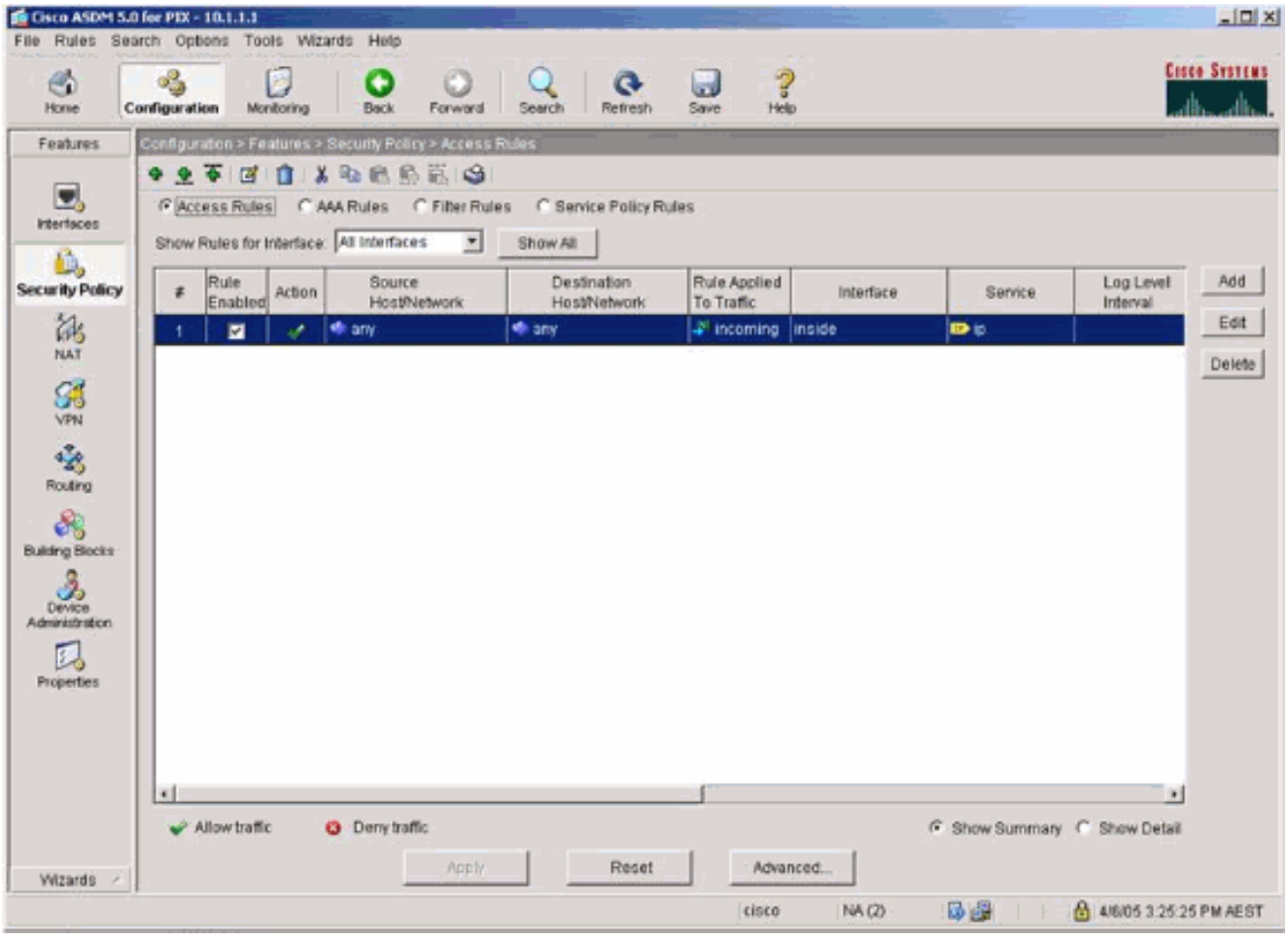
2. Configuration **> Features > Interfaces**를 선택하고 **Add** for new interfaces 또는 **Edit** for an existing configuration을 선택합니다

.



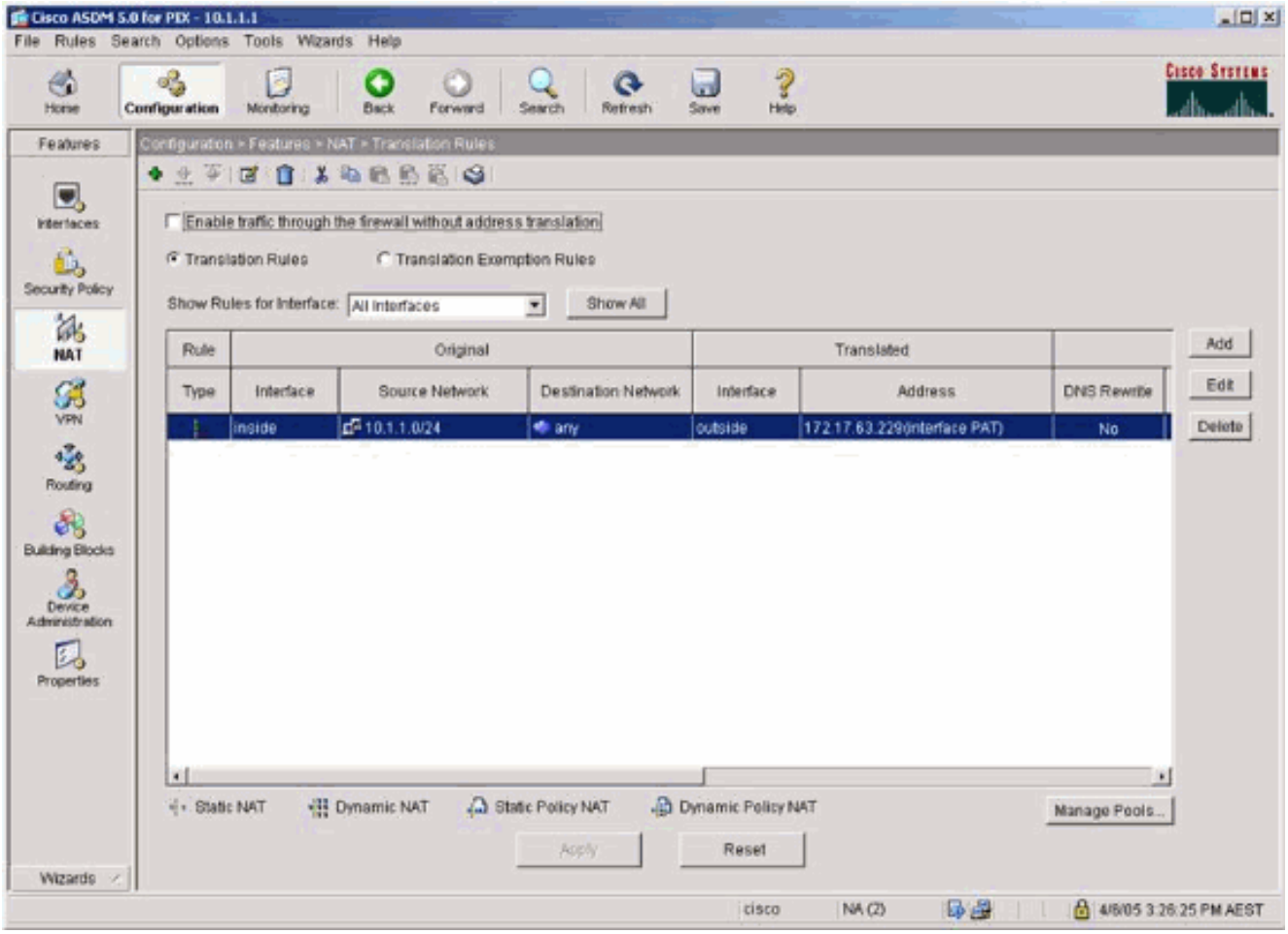
3. 내부 인터페이스의 보안 옵션을 선택합니다

.



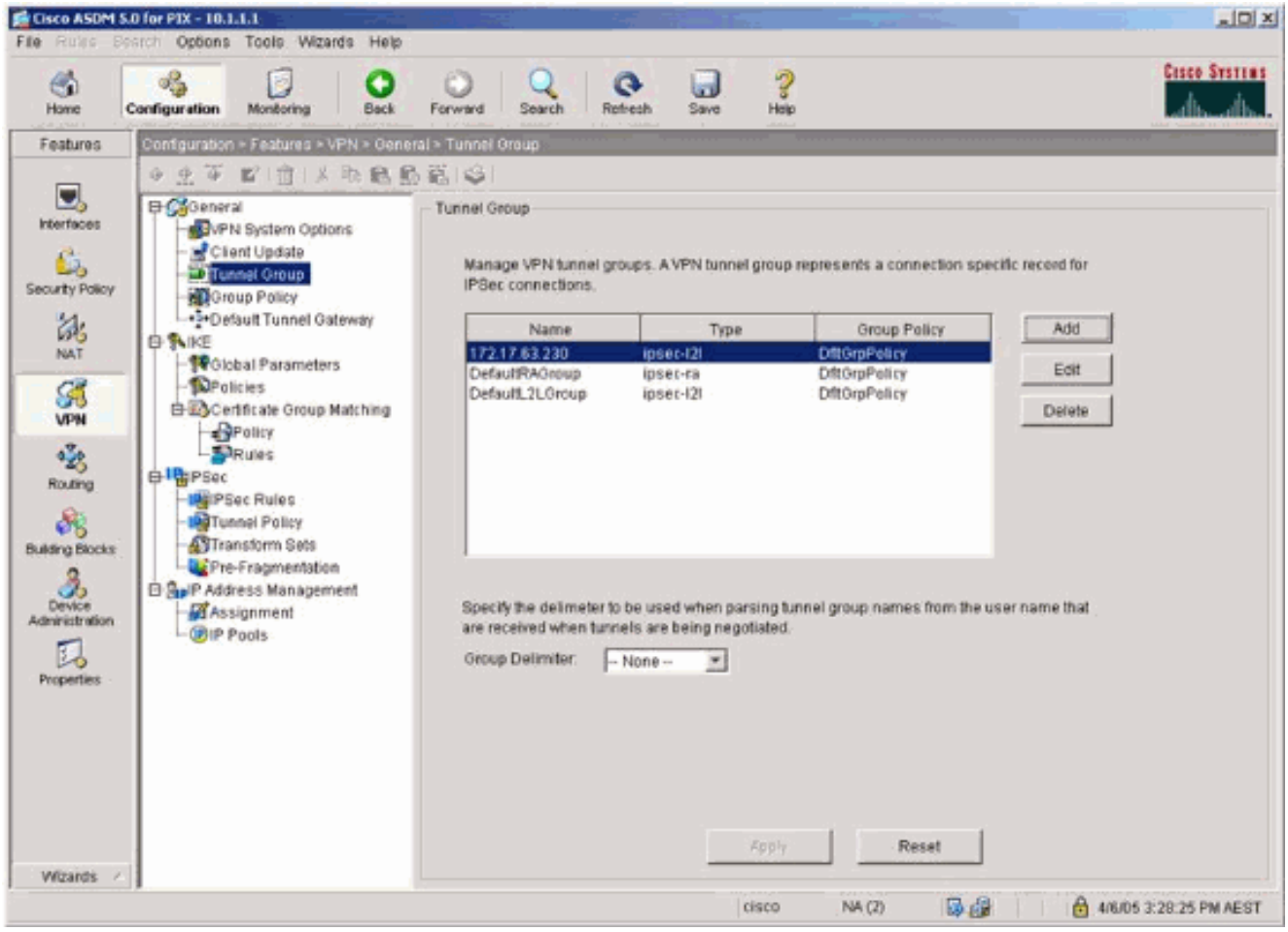
4. NAT 컨피그레이션에서 암호화된 트래픽은 NAT-exempt이며 다른 모든 트래픽은 외부 인터페이스에 대한 NAT/PAT입니다

.



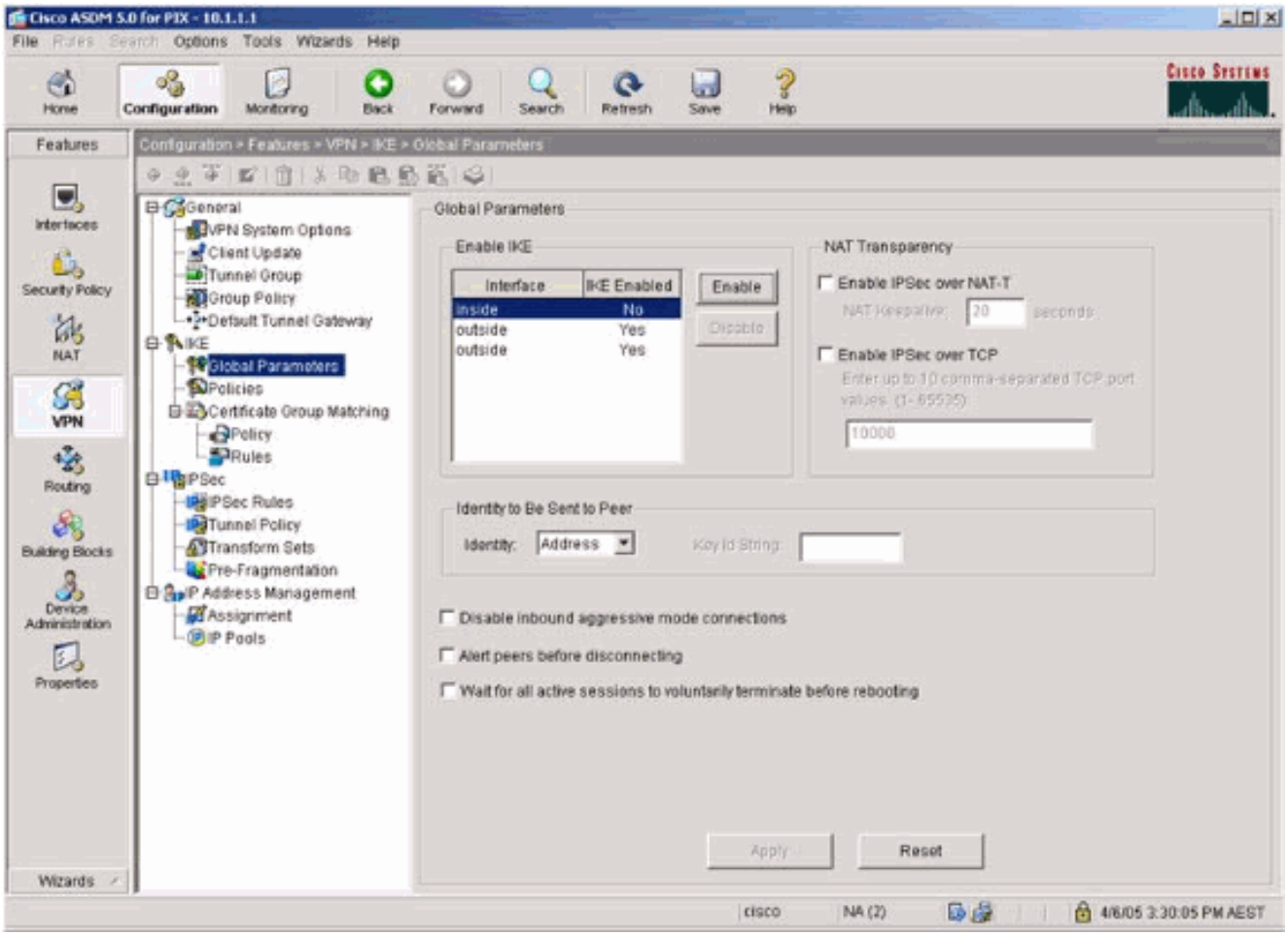
5. VPN **> General(일반) > Tunnel Group(터널 그룹)**을 선택하고 터널 그룹을 활성화합니다

.



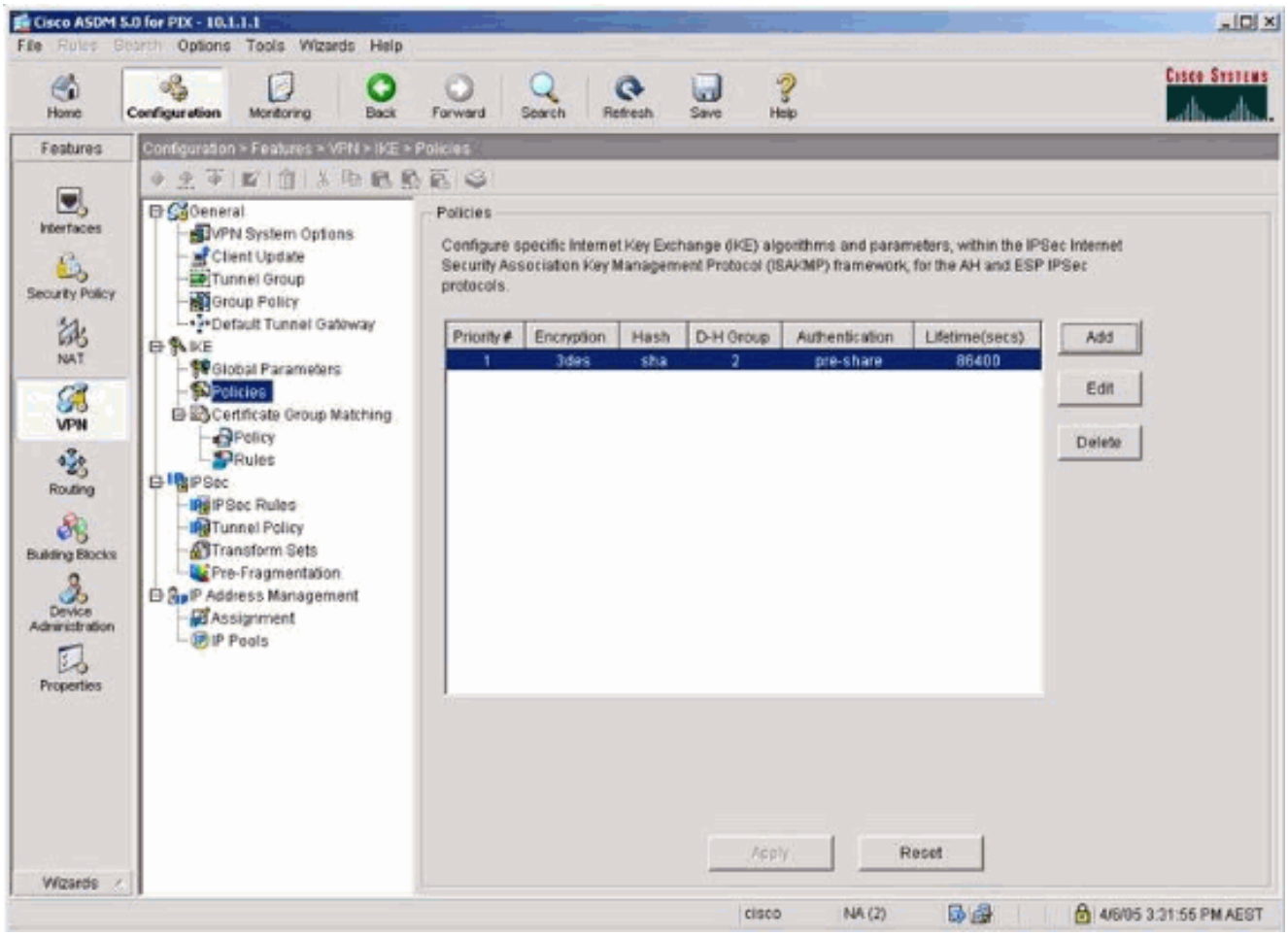
6. VPN **> IKE > Global Parameters**를 선택하고 외부 인터페이스에서 IKE를 활성화합니다

.



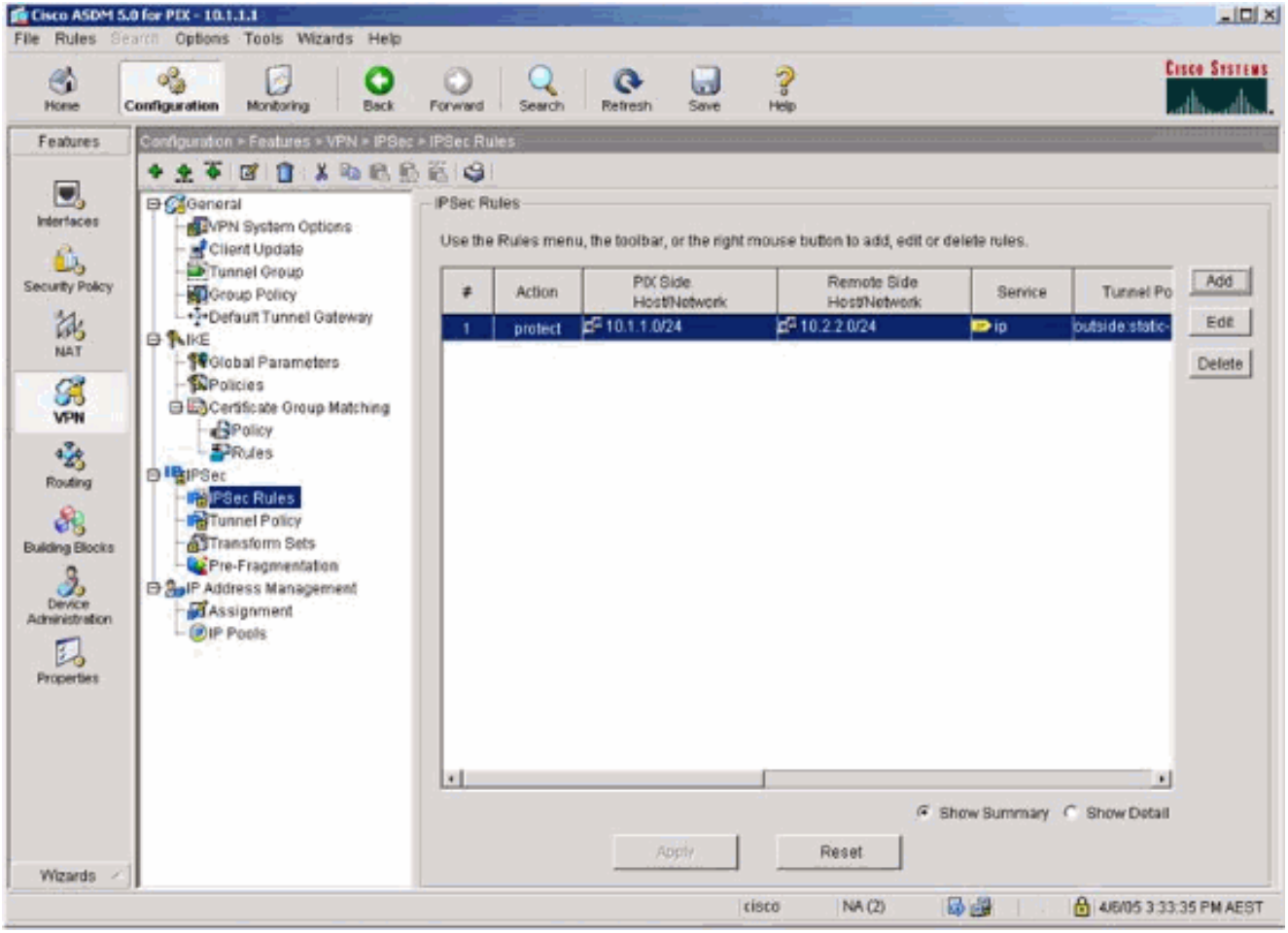
7. VPN **> IKE > Policies**를 선택하고 IKE 정책을 선택합니다

.



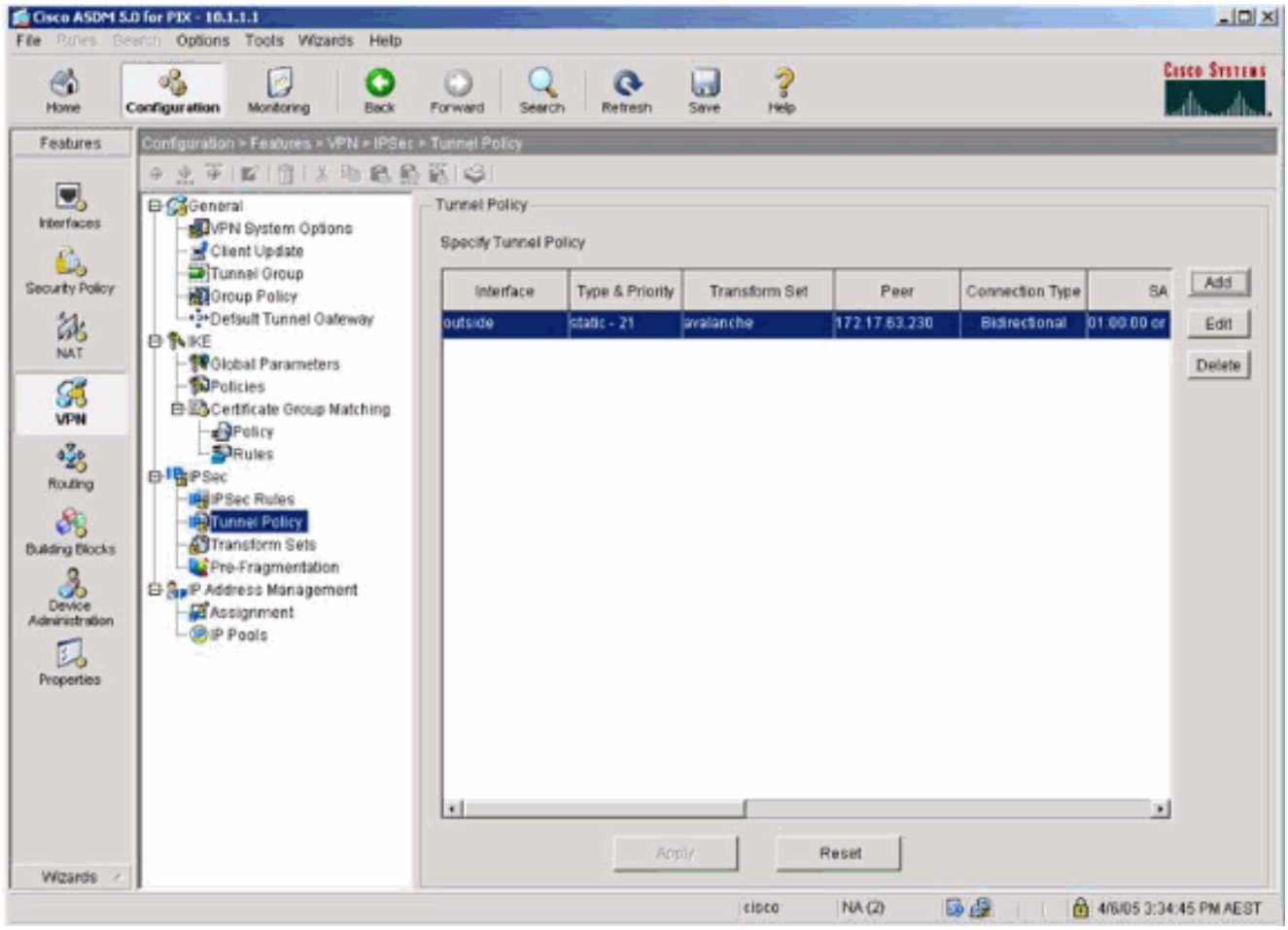
8. VPN **> IPsec > IPsec Rules**를 선택하고 로컬 터널 및 원격 주소 지정을 위해 IPsec을 선택합니다

.



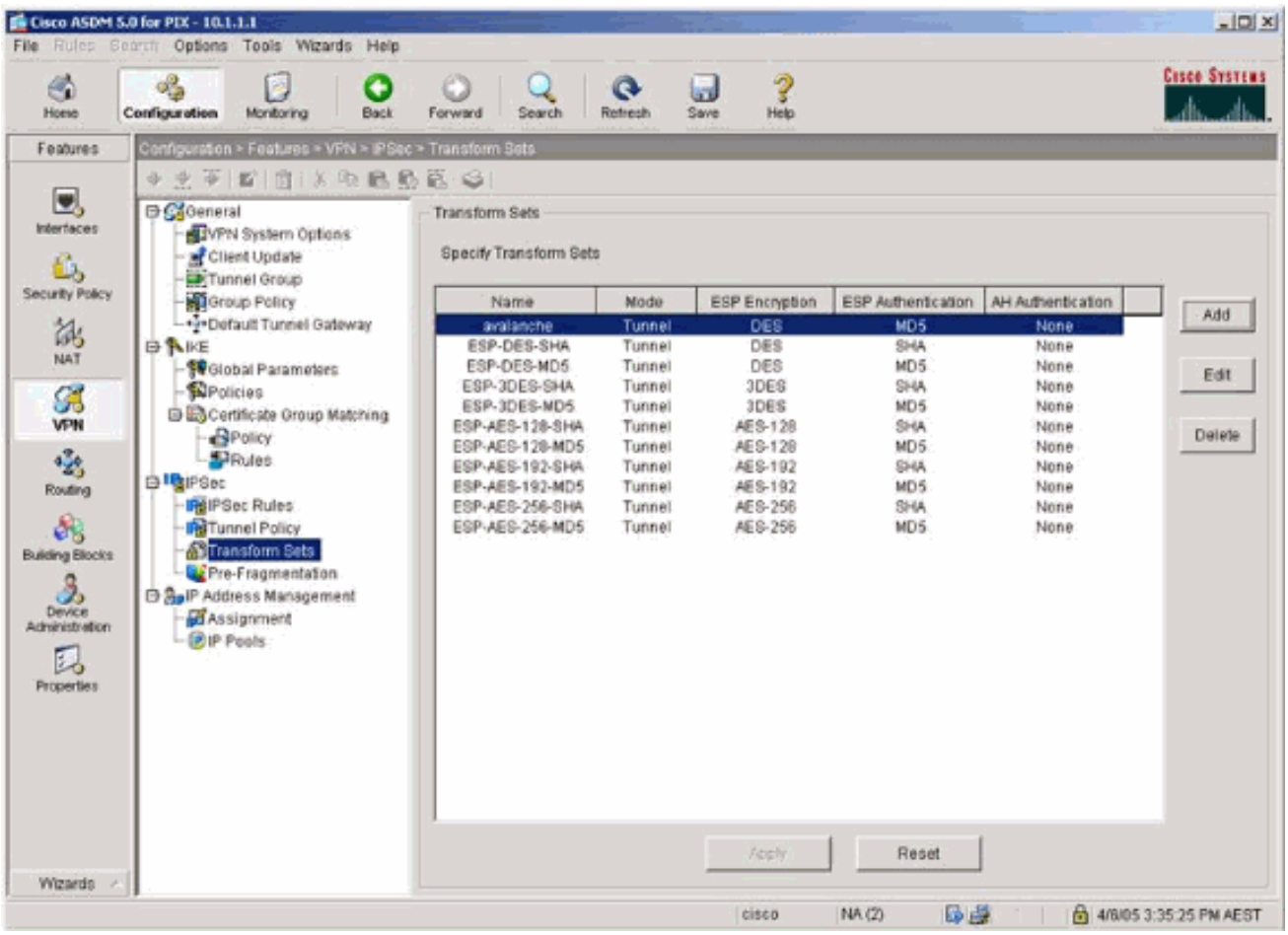
9. VPN **> IPsec > Tunnel Policy**를 선택하고 터널 정책을 선택합니다

.



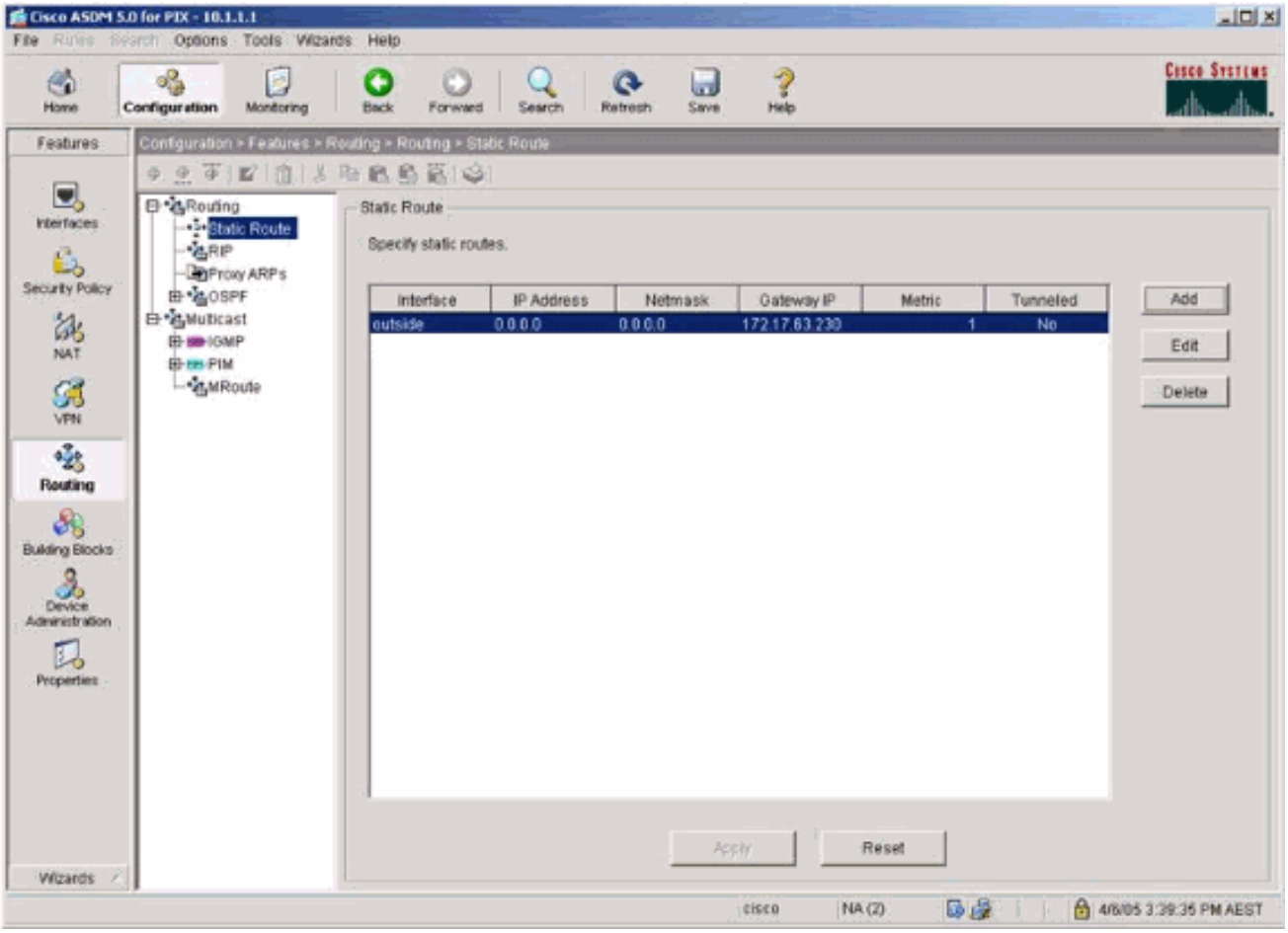
10. VPN **> IPsec > Transform Sets를 선택하고 Transform** set를 선택합니다

.



11. Routing(**라우팅) > Routing(라우팅) > Static Route(고정 경로)**를 선택하고 게이트웨이 라우터에 대한 고정 경로를 선택합니다. 이 예에서 고정 경로는 간소화를 위해 원격 VPN 피어를 가리킵니다

.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.

문제 해결

ASDM을 사용하여 로깅을 활성화하고 로그를 볼 수 있습니다.

- Configuration(**구성**) > **Properties(속성)** > **Logging(로깅)** > **Logging Setup(로깅 설정)을** 선택하고 Enable Logging(로깅 활성화)을 **선택한** 다음 Apply(적용)를 클릭하여 로깅을 활성화합니다.
- Monitoring(**모니터링**) > **Logging(로깅)** > **Log Buffer(로그 버퍼)** > **On Logging Level(로깅 레벨)을** 선택하고 **Logging Buffer(로깅 버퍼)**를 선택한 다음 View(**보기**)를 클릭하여 로그를 확인합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **clear crypto isakmp** - 1단계와 관련된 보안 연결을 지웁니다.
- **clear crypto sa** - 2단계와 관련된 보안 연결을 지웁니다.
- **debug icmp trace** - 호스트의 ICMP 요청이 PIX에 도달하는지 여부를 표시합니다. 이 디버그를 실행하려면 컨피그레이션에서 ICMP를 허용하려면 **access-list** 명령을 추가해야 합니다.
- **logging buffer debugging(로깅 버퍼 디버깅)** - PIX를 통과하는 호스트에 대해 설정 및 거부된 연결을 표시합니다. 정보는 PIX 로그 버퍼에 저장되며 **show log** 명령을 사용하여 출력을 볼 수 있습니다.

관련 정보

- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)