ASA/PIX 7.x:이중화 또는 백업 ISP 링크 컨피그레이션 예

목차

소개

고정 경로의 문제는 경로가 작동 또는 작동 중지되었는지 확인할 기본 메커니즘이 없다는 것입니다.다음 hop 게이트웨이를 사용할 수 없게 되더라도 경로는 라우팅 테이블에 남아 있습니다.고정 경로는 보안 어플라이언스의 연결된 인터페이스가 다운된 경우에만 라우팅 테이블에서 제거됩니다.이 문제를 해결하기 위해 고정 경로 추적 기능을 사용하여 고정 경로의 가용성을 추적하고, 해당 경로가 실패하면 라우팅 테이블에서 제거하고 백업 경로로 대체합니다.

이 문서에서는 디바이스가 이중화 또는 백업 인터넷 연결을 사용할 수 있도록 PIX 500 Series Security Appliance 또는 ASA 5500 Series Adaptive Security Appliance에서 고정 경로 추적 기능을 사용하는 방법에 대한 예를 제공합니다.이 예에서는 고정 경로 추적을 통해 보안 어플라이언스가 기본 임대 회선을 사용할 수 없게 되는 경우 보조 ISP(인터넷 서비스 공급자)에 대한 저렴한 연결을 사용할 수 있습니다.

이러한 이중화를 실현하기 위해 보안 어플라이언스는 고정 경로를 사용자가 정의한 모니터링 대상

과 연결합니다.SLA(Service Level Agreement) 작업은 주기적인 ICMP(Internet Control Message Protocol) 에코 요청으로 대상을 모니터링합니다.에코 응답이 수신되지 않으면 객체는 다운된 것으로 간주되며 연관된 경로가 라우팅 테이블에서 제거됩니다.이전에 구성한 백업 경로가 제거된 경로 대신 사용됩니다.백업 경로가 사용 중인 동안 SLA 모니터 작업은 모니터링 대상에 도달하려고 계속 시도합니다.대상이 다시 사용 가능해지면 라우팅 테이블에서 첫 번째 경로가 대체되고 백업 경로가 제거됩니다.

참고: 이 문서에 설명된 컨피그레이션은 ASA/PIX에서 지원되지 않으므로 로드 밸런싱 또는 로드 공유에 사용할 수 없습니다.이중화 또는 백업 용도로만 이 컨피그레이션을 사용합니다.기본 ISP가 실패하는 경우 발신 트래픽은 기본 ISP를 사용한 다음 보조 ISP를 사용합니다.기본 ISP가 실패하면 트래픽이 일시적으로 중단됩니다.

사전 요구 사항

요구 사항

ICMP 에코 요청에 응답할 수 있는 모니터링 대상을 선택합니다.대상은 사용자가 선택하는 모든 네트워크 객체일 수 있지만 ISP 연결과 밀접하게 연결된 대상을 사용하는 것이 좋습니다.몇 가지 가능한 모니터링 대상은 다음과 같습니다.

- ISP 게이트웨이 주소
- 다른 ISP 관리 주소
- 보안 어플라이언스가 통신해야 하는 AAA 서버와 같은 다른 네트워크의 서버
- 다른 네트워크에 있는 영구 네트워크 개체(밤에도 종료할 수 있는 데스크톱 또는 노트북 컴퓨터는 좋은 선택이 아님)

이 문서에서는 Cisco ASDM이 컨피그레이션을 변경할 수 있도록 보안 어플라이언스가 완전히 작동 중이고 구성되었다고 가정합니다.

참고: ASDM에서 디바이스를 구성할 수 있도록 허용하는 방법에 대한 자세한 내용은 ASDM용 HTTPS 액세스 허용을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco PIX Security Appliance 515E(소프트웨어 버전 7.2(1) 이상)
- Cisco Adaptive Security Device Manager 5.2(1) 이상

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

Cisco ASA 5500 Series Security Appliance 버전 7.2(1)에서 이 컨피그레이션을 사용할 수도 있습니다.

참고: ASA 5505에서 네 번째 인터페이스를 구성하려면 backup **interface** 명령이 필요합니다.자세한 내용은 백업 인터페이스를 참조하십시오.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

이 예에서는 보안 어플라이언스가 인터넷에 대한 두 개의 연결을 유지합니다.첫 번째 연결은 기본 ISP에서 제공하는 라우터를 통해 액세스하는 고속 임대 회선입니다.두 번째 연결은 보조 ISP에서 제공하는 DSL 모뎀을 통해 액세스하는 저속 DSL(Digital Subscriber Line) 회선입니다.

참고: 이 예에서는 로드 밸런싱이 발생하지 않습니다.

임대 회선이 활성 상태이고 기본 ISP 게이트웨이에 연결할 수 있으면 DSL 연결이 유휴 상태가 됩니다.그러나 기본 ISP에 대한 연결이 끊기면 보안 어플라이언스는 라우팅 테이블을 변경하여 트래픽을 DSL 연결로 전송합니다.고정 경로 추적은 이러한 이중화를 달성하는 데 사용됩니다.

보안 어플라이언스는 모든 인터넷 트래픽을 기본 ISP로 전달하는 고정 경로로 구성됩니다.SLA 모니터 프로세스는 10초마다 기본 ISP 게이트웨이가 연결 가능한지 확인합니다.SLA 모니터 프로세스에서 기본 ISP 게이트웨이에 연결할 수 없다고 판단하면 해당 인터페이스로 트래픽을 전달하는 고정 경로가 라우팅 테이블에서 제거됩니다.고정 경로를 대체하기 위해 보조 ISP로 트래픽을 전달하는 대체 고정 경로가 설치됩니다.이 대체 고정 경로는 기본 ISP에 연결할 수 있을 때까지 DSL 모뎀을 통해 보조 ISP로 트래픽을 전달합니다.

이 컨피그레이션은 보안 어플라이언스 뒤에 있는 사용자가 아웃바운드 인터넷 액세스를 계속 사용할 수 있도록 하는 비교적 저렴한 방법을 제공합니다.이 문서에서 설명한 대로 이 설정은 보안 어플라이언스 뒤에 있는 리소스에 대한 인바운드 액세스에 적합하지 않을 수 있습니다.원활한 인바운드 연결을 위해서는 고급 네트워킹 기술이 필요합니다.이 문서에서는 이러한 기술을 다루지 않습니다.

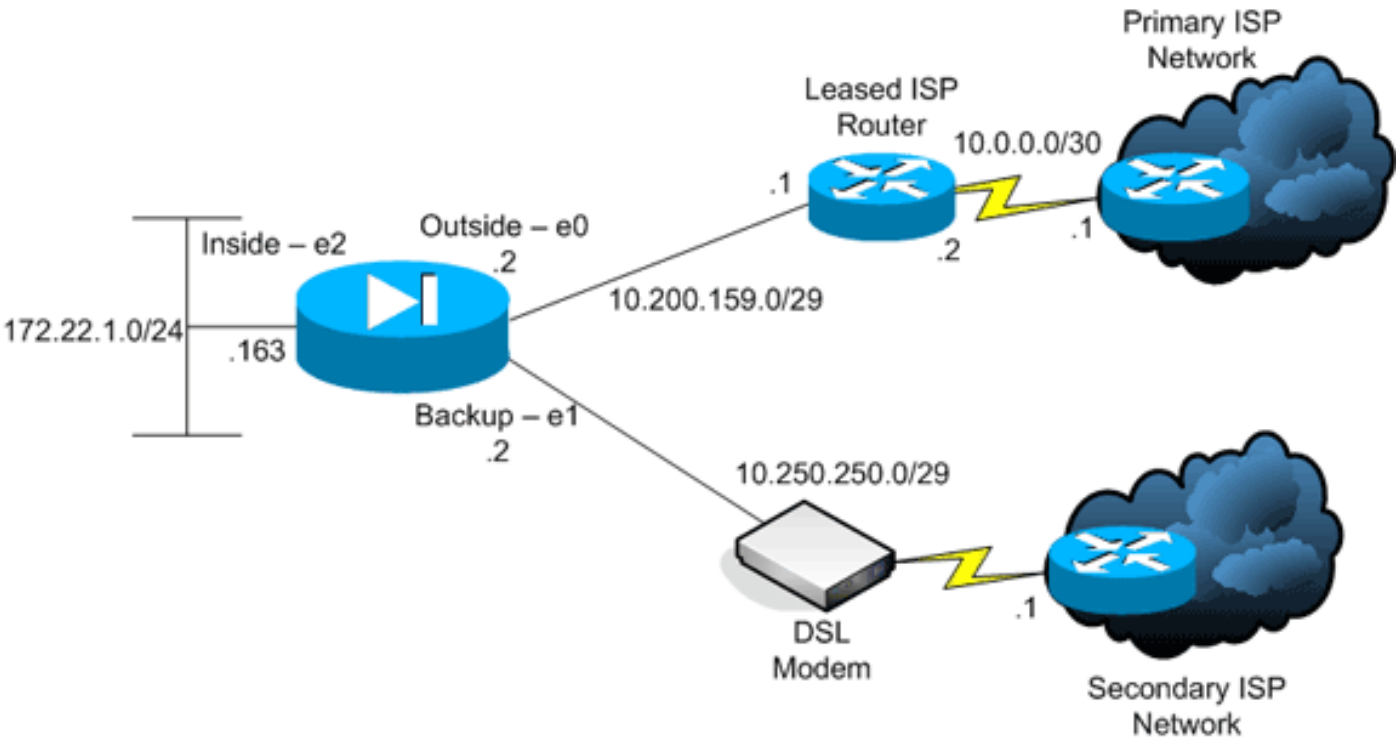
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 구성에 사용된 IP 주소는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용되는 RFC 1918 주소입니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- CLI(Command-Line Interface)
- ASDM(Adaptive Security Device Manager)

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

CLI 컨피그레이션

PIX

```
pix# show running-config
: Saved
:
PIX Version 7.2(1)
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
 nameif backup
!--- The interface attached to the Secondary ISP. !---
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
```

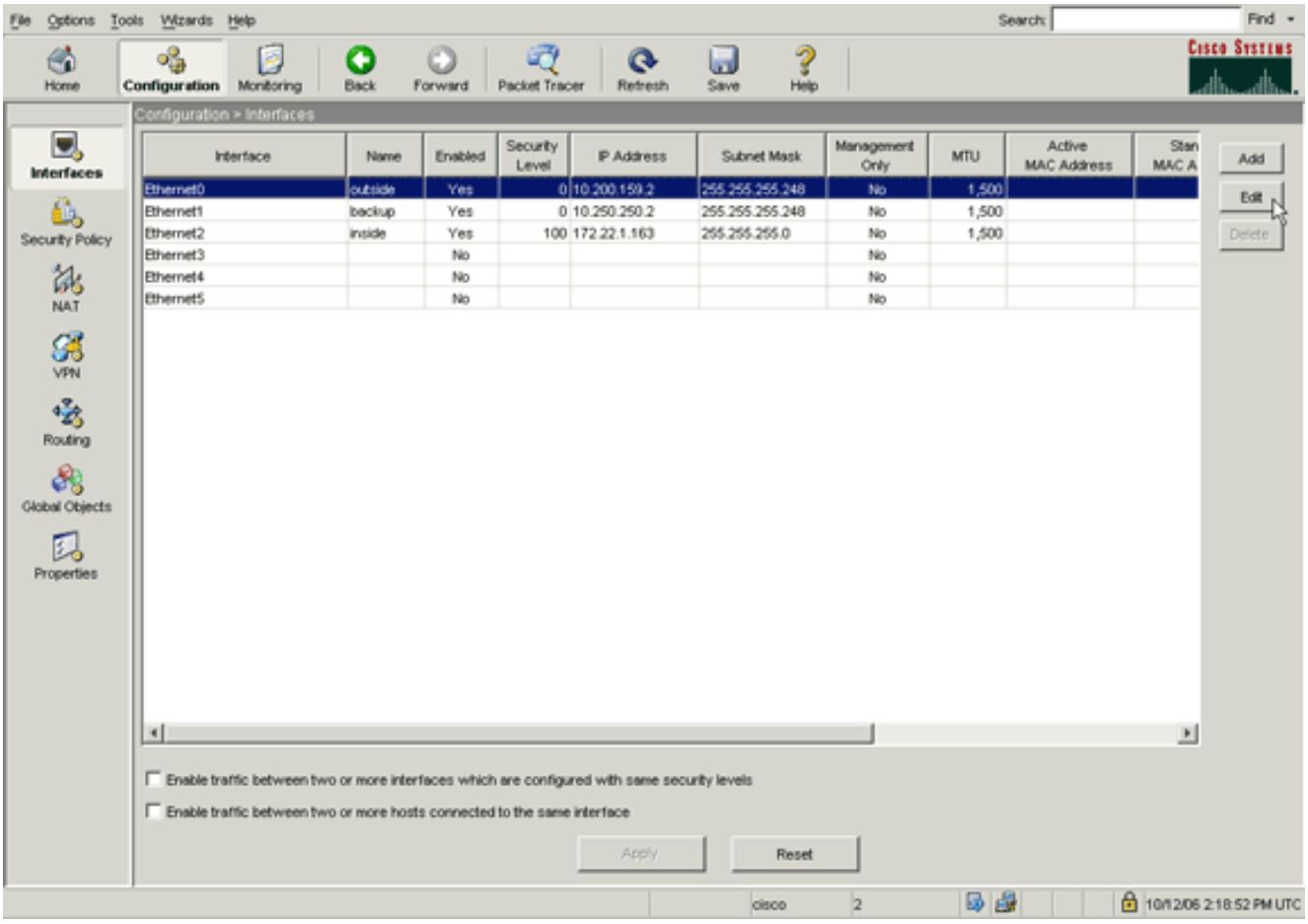
```
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging buffered debugging mtu outside 1500 mtu backup
1500 mtu inside 1500 no failover asdm image
flash:/asdm521.bin no asdm history enable arp timeout
14400 global (outside) 1 interface
global (backup) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0
!--- NAT Configuration for Outside and Backup route
outside 0.0.0.0 0.0.0.0 10.200.159.1 1 track 1
!--- Enter this command in order to track a static
route. !--- This is the static route to be installed in
the routing !--- table while the tracked object is
reachable. The value after !--- the keyword "track" is a
tracking ID you specify. route backup 0.0.0.0 0.0.0.0
10.250.250.1 254
!--- Define the backup route to use when the tracked
object is unavailable. !--- The administrative distance
of the backup route must be greater than !--- the
administrative distance of the tracked route. !--- If
the primary gateway is unreachable, that route is
removed !--- and the backup route is installed in the
routing table !--- instead of the tracked route. 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable http 172.22.1.0 255.255.255.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface
outside
 num-packets 3
 frequency 10
!--- Configure a new monitoring process with the ID 123.
Specify the !--- monitoring protocol and the target
network object whose availability the tracking !---
process monitors. Specify the number of packets to be
sent with each poll. !--- Specify the rate at which the
monitor process repeats (in seconds). sla monitor
schedule 123 life forever start-time now
!--- Schedule the monitoring process. In this case the
lifetime !--- of the process is specified to be forever.
The process is scheduled to begin !--- at the time this
command is entered. As configured, this command allows
the !--- monitoring configuration specified above to
determine how often the testing !--- occurs. However,
you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times. !
track 1 rtr 123 reachability
!--- Associate a tracked static route with the SLA
monitoring process. !--- The track ID corresponds to the
track ID given to the static route to monitor: !---
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1 !---
"rtr" = Response Time Reporter entry. 123 is the ID of
the SLA process !--- defined above.
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
prompt hostname context
Cryptochecksum:a4a0e9be4593ad43bc17a1cc25e32dc2
: end
```

ASDM 컨피그레이션

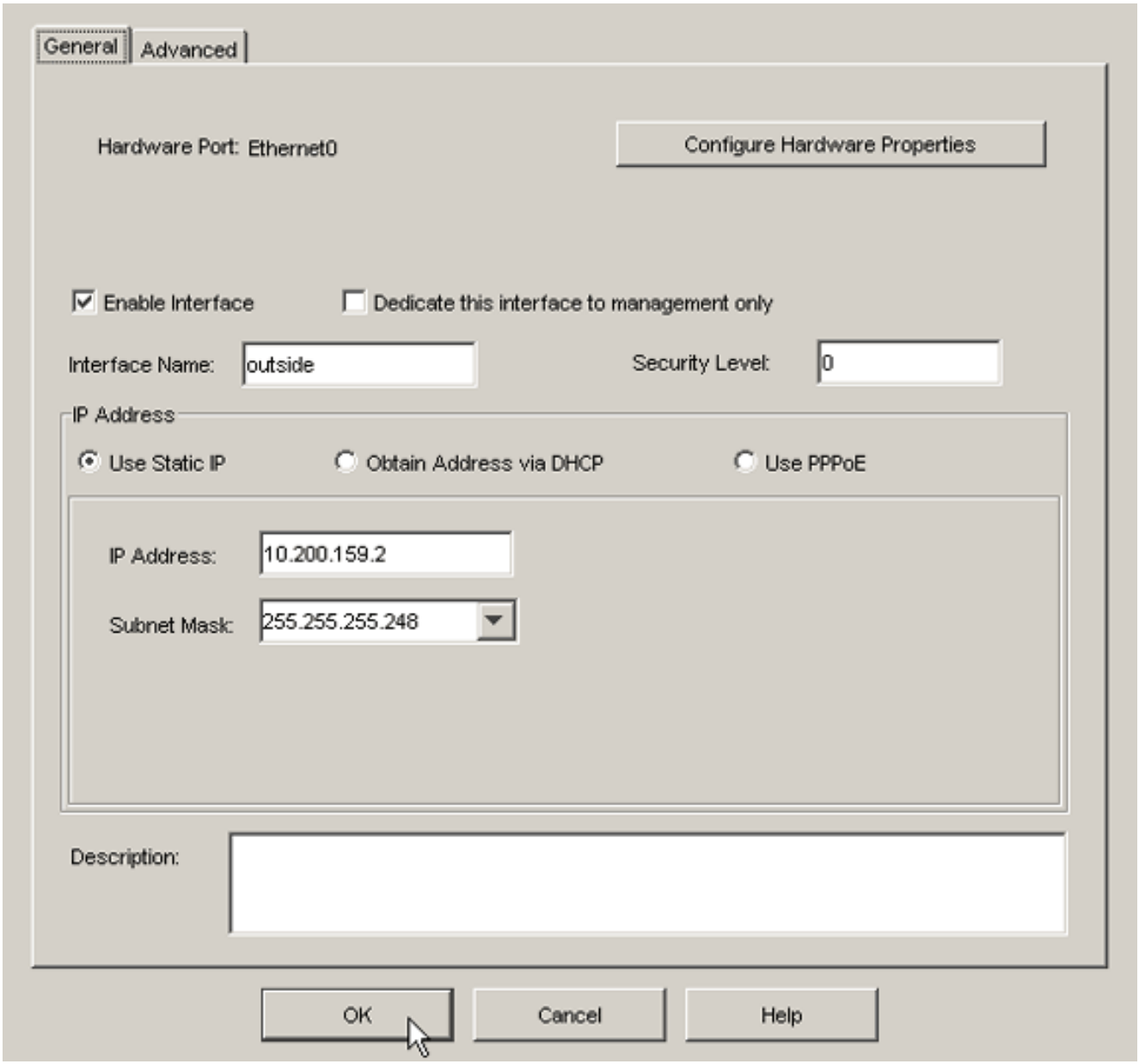
ASDM 애플리케이션을 사용하여 이중화 또는 백업 ISP 지원을 구성하려면 다음 단계를 완료하십시오.

1. ASDM 애플리케이션에서 Configuration(컨피그레이션)을 클릭한 다음 Interfaces(인터페이스)를 **클릭합니다**
   .



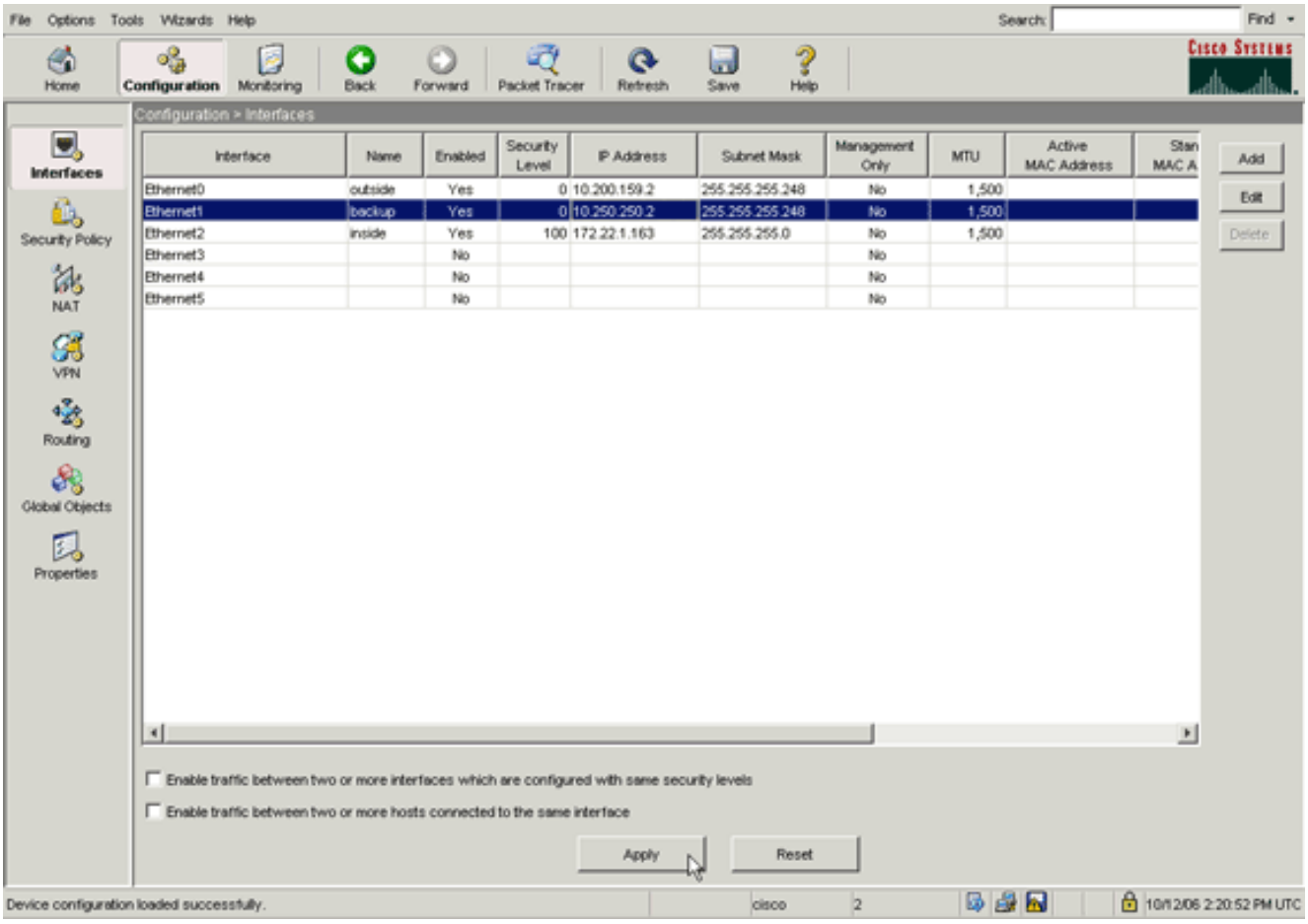
2. Interfaces(인터페이스) 목록에서 **Ethernet0**을 선택한 다음 Edit(수정)를 **클릭합니다**.이 대화 상자가 나타납니다

.



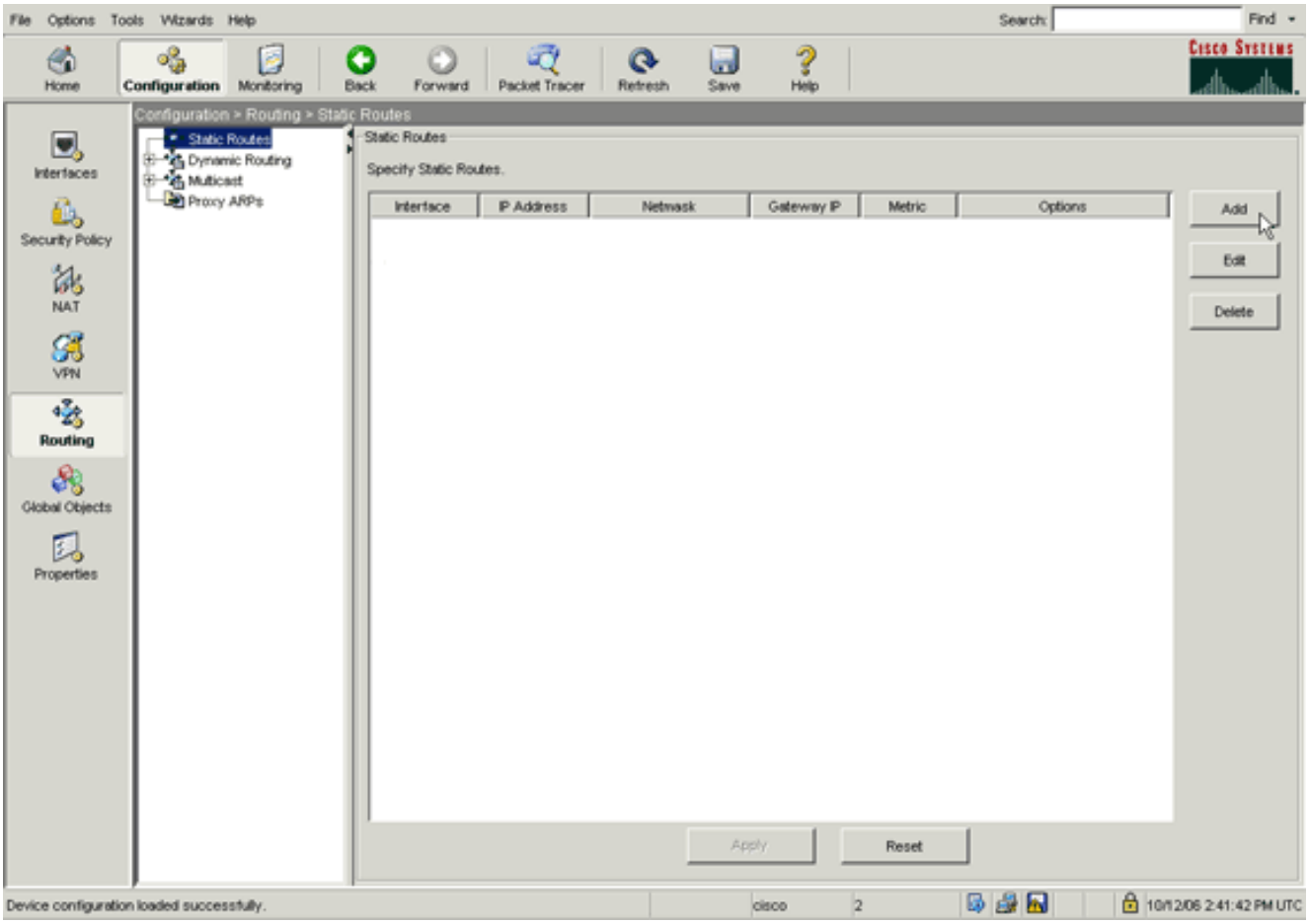
3. Enable **Interface** 확인란을 선택하고 Interface Name, Security Level, IP Address 및 Subnet Mask 필드에 값을 입력합니다.
4. 확인**을** 클릭하여 대화 상자를 닫습니다.
5. 필요에 따라 다른 인터페이스를 구성하고 Apply(**적용)를** 클릭하여 보안 어플라이언스 컨피그레이션을 업데이트합니다

.

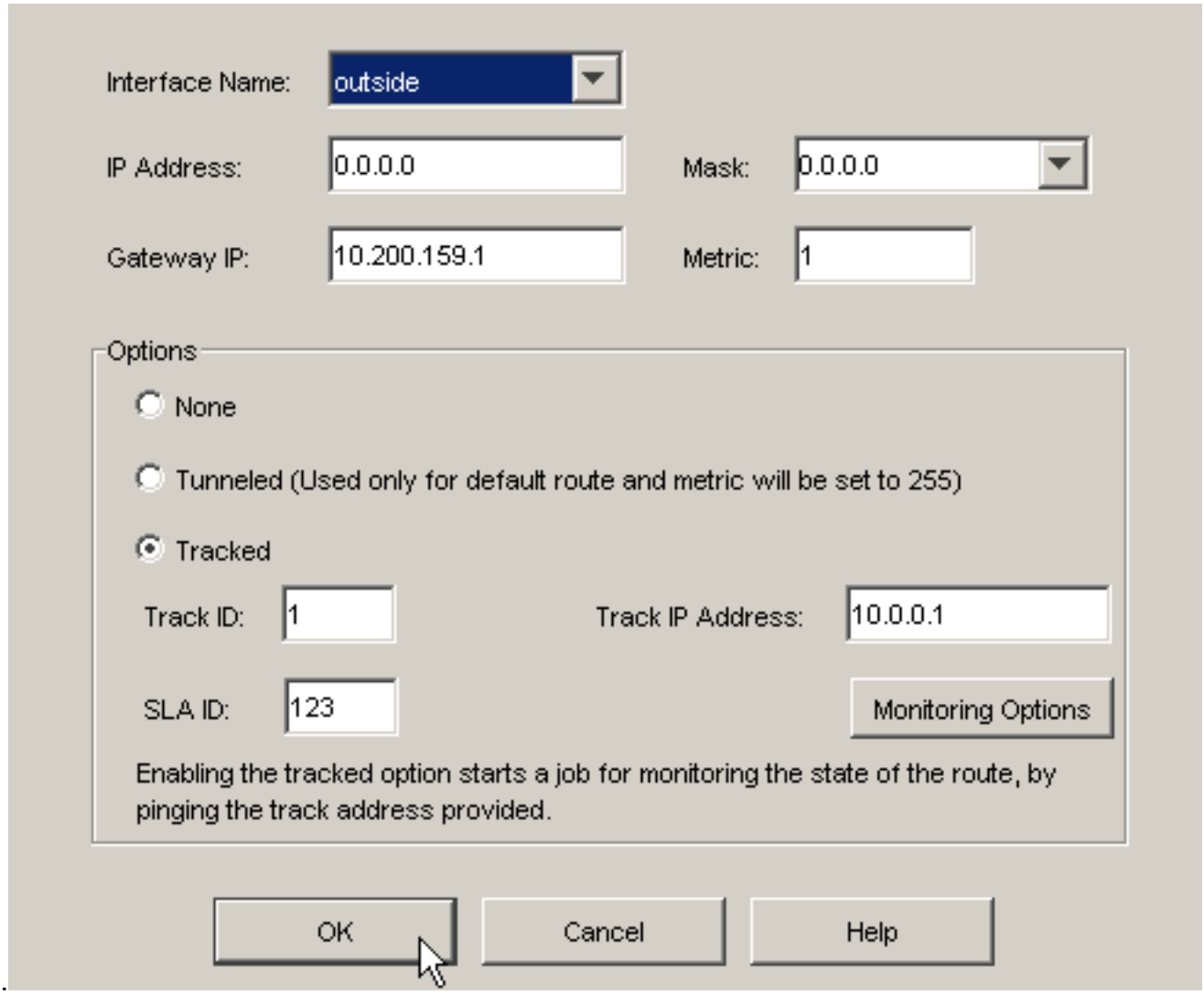


6. ASDM 애플리케이션 왼쪽에 있는 Routing을 클릭합니다

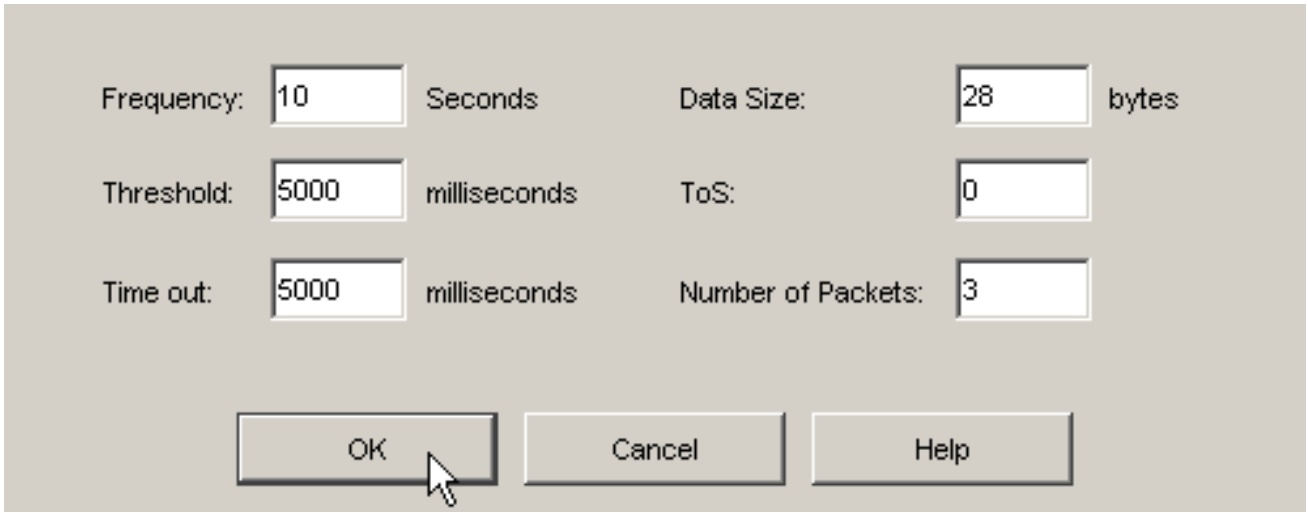
.



7. 새 고정 경로를 추가하려면 **Add**를 클릭합니다.이 대화 상자가 나타납니다



8. Interface Name 드롭다운 목록에서 경로가 상주하는 인터페이스를 선택하고 게이트웨이에 도달할 기본 경로를 구성합니다.이 예에서 10.0.0.1은 기본 ISP 게이트웨이는 물론 ICMP 추적으로 모니터링할 객체입니다.
9. Options(옵션) 영역에서 Tracked(추적됨) 라디오 버튼을 클릭하고 Track ID, SLA ID 및 Track IP Address(추적 IP 주소) 필드에 값을 입력합니다.
10. Monitoring **Options를 클릭합니다**.이 대화 상자가 나타납니다

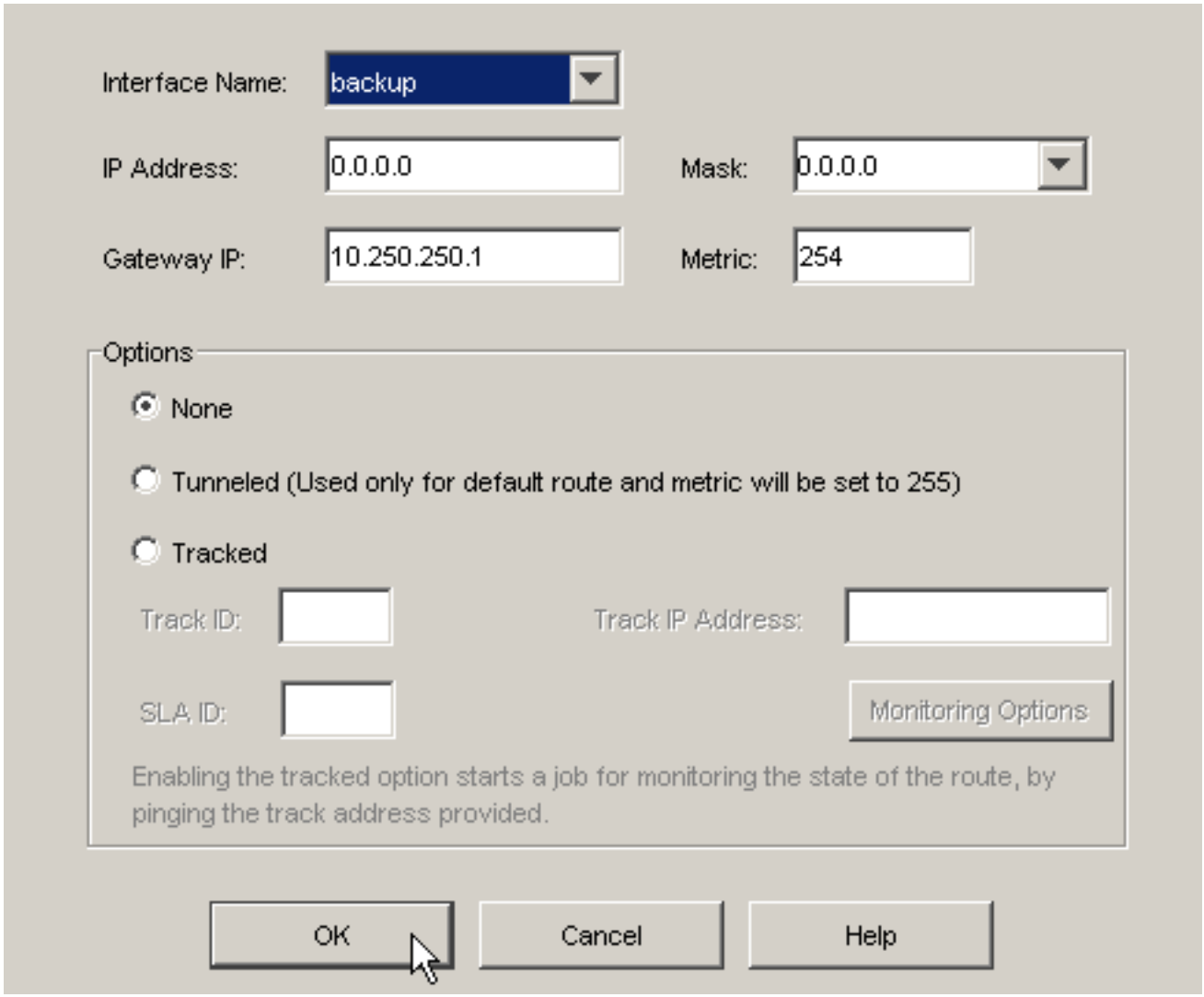


11. 빈도 및 기타 모니터링 옵션에 대한 값을 입력하고 **확인**을 클릭합니다.
12. 인터넷에 연결할 경로를 제공하려면 보조 ISP에 다른 고정 경로를 추가합니다.보조 경로로 만들려면 254와 같이 더 높은 메트릭으로 이 경로를 구성합니다. 기본 경로(기본 ISP)가 실패

하면 해당 경로가 라우팅 테이블에서 제거됩니다.이 보조 경로(보조 ISP)는 대신 PIX 라우팅 테이블에 설치됩니다.

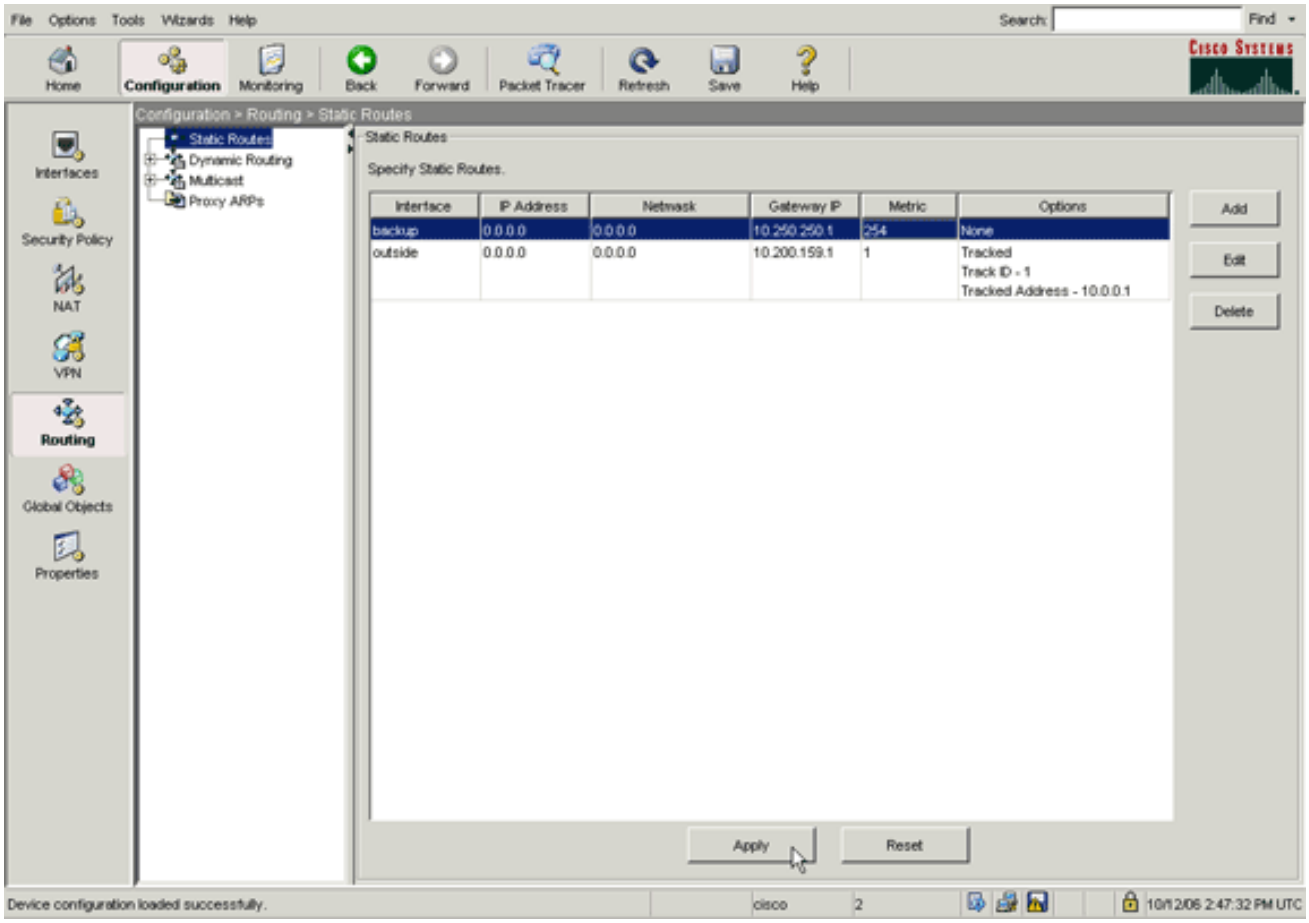
13. 확인을 클릭하여 대화 상자를 닫습니다

.



Interface(인터페이스) 목록에 컨피그레이션이 나타납니다

.



14. 라우팅 컨피그레이션을 선택하고 Apply(**적용)를** 클릭하여 보안 어플라이언스 컨피그레이션을 업데이트합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

구성이 완료되었는지 확인

이 **show** 명령을 사용하여 컨피그레이션이 완료되었는지 확인합니다.

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

- **show running-config sla monitor** - 컨피그레이션의 SLA 명령을 표시합니다.

```
pix# show running-config sla monitor
sla monitor 123
 type echo protocol ipIcmpEcho 10.0.0.1 interface outside
 num-packets 3
 frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** - 작업의 현재 컨피그레이션 설정을 표시합니다.

```
pix# show sla monitor configuration 123
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
```

```
Target address: 10.0.0.1
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

- **show sla monitor operational-state** - SLA 작업의 운영 통계를 표시합니다.기본 ISP에 장애가 발생하기 전에 이는 작동 상태입니다.

```
pix# show sla monitor operational-state 123
Entry number: 123
Modification time: 13:59:37.824 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 367
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: 15:00:37.825 UTC Thu Oct 12 2006
Latest operation return code: OK
RTT Values:
RTTAvg: 1       RTTMin: 1       RTTMax: 1
NumOfRTT: 3     RTTSum: 3       RTTSum2: 3
```

기본 ISP에 실패하고 ICMP에서 시간 초과가 발생하면 작동 상태가 됩니다.

```
pix# show sla monitor operational-state
Entry number: 123
Modification time: 13:59:37.825 UTC Thu Oct 12 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 385
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 15:03:27.825 UTC Thu Oct 12 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

백업 경로가 설치되었는지 확인(CLI 방법)

백업 경로가 설치된 시기를 확인하려면 **show route** 명령을 사용합니다.

- 기본 ISP에 장애가 발생하기 전에 라우팅 테이블은 다음과 같습니다.

```
pix# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.200.159.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.200.159.1, outside
```

- 기본 ISP에 장애가 발생하면 고정 경로가 제거되고 백업 경로가 설치되면 이는 라우팅 테이블입니다.

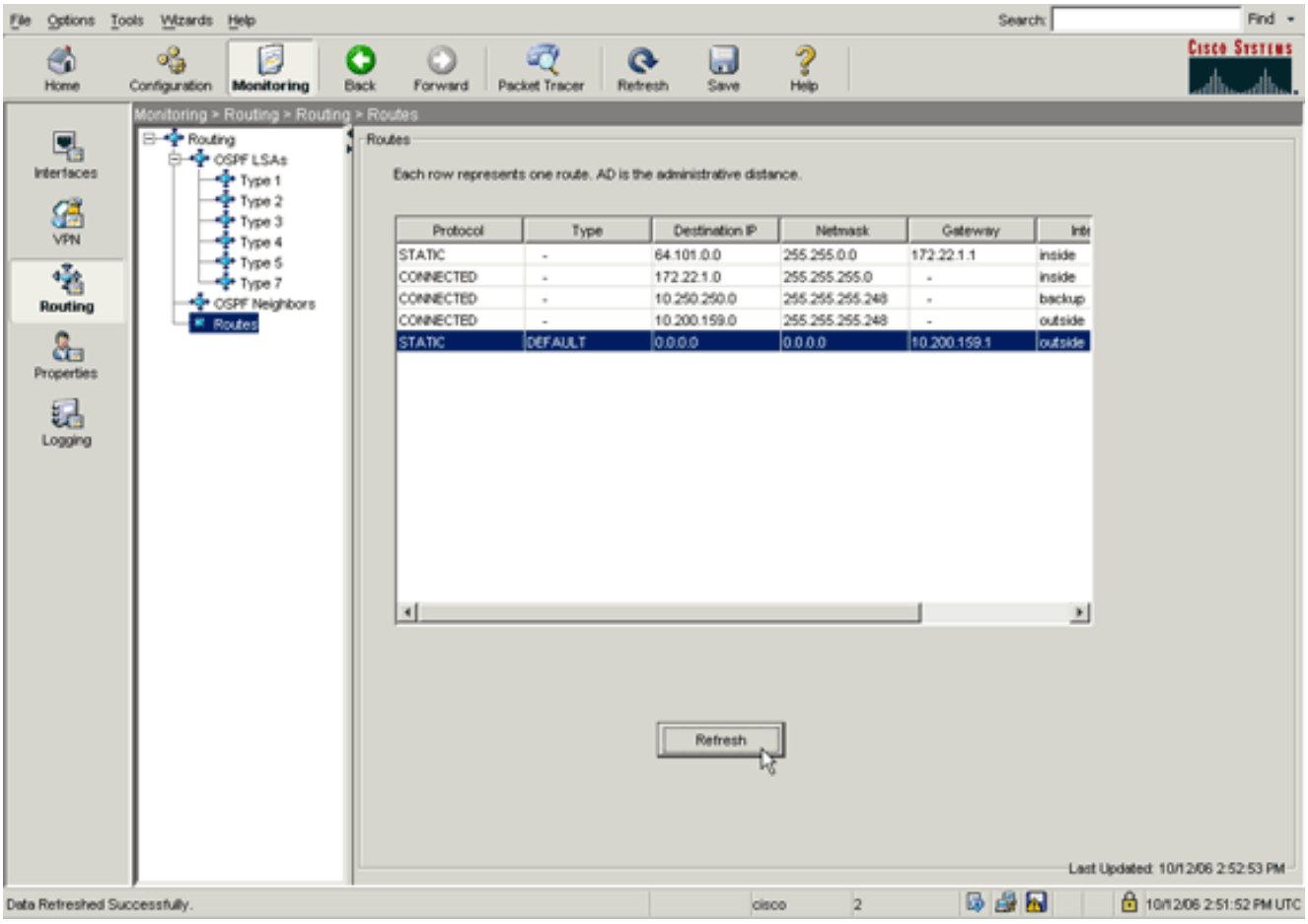
```
pix(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.250.250.1 to network 0.0.0.0

S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
C    172.22.1.0 255.255.255.0 is directly connected, inside
C    10.250.250.0 255.255.255.248 is directly connected, backup
C    10.200.159.0 255.255.255.248 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

백업 경로가 설치되었는지 확인(ASDM 방법)

백업 경로가 설치되었는지 ASDM에 확인하려면 다음 단계를 완료하십시오.

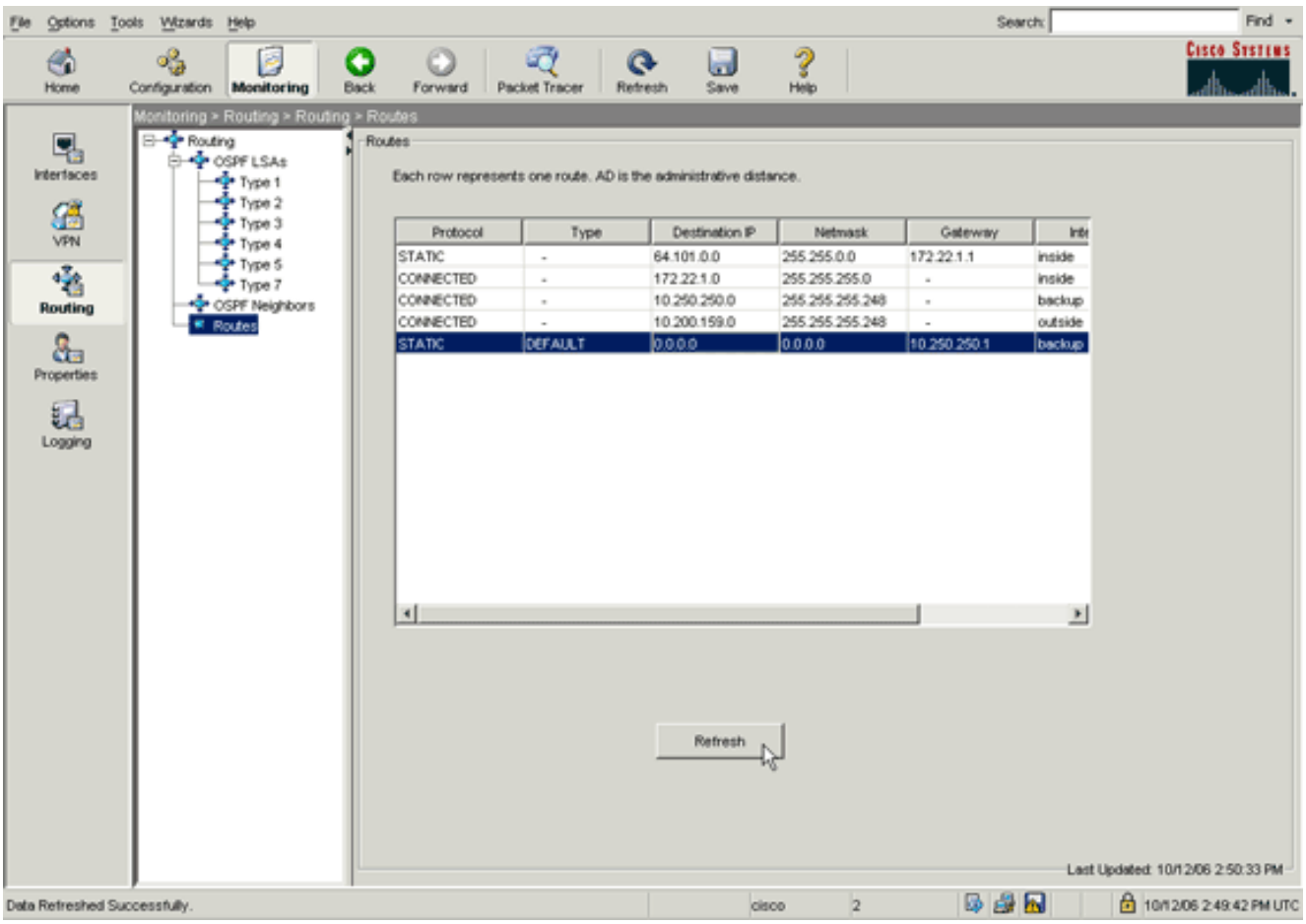
1. Monitoring(**모니터링**)을 클릭한 다음 Routing(라우팅)을 **클릭합니다**.
2. Routing(라우팅) 트리에서 Routes(경로)를 **선택합니다**.기본 ISP에 장애가 발생하기 전에 라우팅 테이블은 다음과 같습니다

.



DEFAULT 경로는 외부 인터페이스를 통해 10.0.0.2을 가리킵니다.기본 ISP에 장애가 발생하면 경로가 제거되고 백업 경로가 설치됩니다.이제 DEFAULT 경로가 백업 인터페이스를 통해 10.250.250.1을 가리킵니다

.



문제 해결

디버그 명령

- **debug sla monitor trace** - 에코 작업의 진행 상황을 표시합니다.추적된 개체(기본 ISP 게이트웨이)가 작동하며 ICMP가 성공적으로 수행됩니다.

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=4 OK
IP SLA Monitor(123) Scheduler: Updating result
```

추적된 개체(기본 ISP 게이트웨이)가 다운되었으며 ICMP가 실패합니다.

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```

- **debug sla monitor error** - SLA 모니터 프로세스에서 발생하는 오류를 표시합니다.추적된 개체(기본 ISP 게이트웨이)가 작동되고 ICMP가 성공했습니다.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52696 laddr 10.200.159.2/52696
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52696 laddr 10.200.159.2/52696
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2 duration
               0:00:00
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               0.200.159.2/52697 laddr 10.200.159.2/52697
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/52697 laddr 10.200.159.2/52697
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:00
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00
```

추적된 개체(기본 ISP 게이트웨이)가 다운되고 추적된 경로가 제거됩니다.

```
%PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2
%PIX-7-609001: Built local-host outside:10.0.0.1
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2
               duration 0:00:02
%PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:02
%PIX-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.200.159.1,
               distance 1, table Default-IP-Routing-Table, on interface
```

```
                outside
!--- 10.0.0.1 is unreachable, so the route to the Primary ISP is removed.
```

추적된 경로가 불필요하게 제거됨

추적된 경로가 불필요하게 제거되면 모니터링 대상이 에코 요청을 받을 수 있도록 항상 사용 가능한지 확인합니다.또한 모니터링 대상의 상태(즉, 대상에 연결할 수 있는지 여부)가 기본 ISP 연결 상태와 밀접하게 연결되어 있는지 확인합니다.

ISP 게이트웨이보다 멀리 있는 모니터링 대상을 선택하면 해당 경로를 따라 다른 링크가 실패하거나 다른 디바이스가 방해할 수 있습니다.이 컨피그레이션으로 인해 SLA 모니터가 기본 ISP에 대한 연결에 실패했으며 보안 어플라이언스가 보조 ISP 링크로 불필요하게 장애 조치될 수 있습니다.

예를 들어, 지사 라우터를 모니터링 대상으로 선택할 경우 지사에 대한 ISP 연결은 물론 그 과정에서 다른 링크도 실패할 수 있습니다.모니터링 작업에 의해 전송되는 ICMP 추적이 실패하면 기본 ISP 링크가 여전히 활성 상태이지만 기본 추적 경로가 제거됩니다.

이 예에서는 모니터링 대상으로 사용되는 기본 ISP 게이트웨이가 ISP에 의해 관리되고 ISP 링크의 반대편에 있습니다.이 컨피그레이션은 모니터링 작업에 의해 전송되는 ICMP 초기가 실패할 경우 ISP 링크가 거의 확실하게 다운되도록 보장합니다.

ASA의 SLA 모니터링

문제/장애:

ASA가 버전 8.0으로 업그레이드된 후에는 SLA 모니터링이 작동하지 않습니다.

해결책:

문제는 **OUTSIDE** 인터페이스에 구성된 **IP Reverse-Path** 명령 때문일 수 있습니다.ASA에서 명령을 제거하고 SLA 모니터링을 확인합니다.

관련 정보

- 고정 경로 추적 구성
- PIX/ASA 7.2 명령 참조
- Cisco ASA 5500 Series 보안 어플라이언스
- Cisco PIX 500 Series 보안 어플라이언스
- 기술 지원 및 문서 – Cisco Systems