RIP가 포함된 ASA/PIX 컨피그레이션 예

목차

소개

이 문서에서는 RIP(Routing Information Protocol)를 통해 경로를 학습하고 인증 및 재배포를 수행하기 위해 Cisco ASA를 구성하는 방법에 대해 설명합니다.

PIX/ASA 8.X 참조:EIGRP 컨피그레이션에 대한 자세한 내용을 보려면 Cisco ASA(Adaptive Security Appliance)에서 EIGRP를 구성합니다.

참고: 이 문서 구성은 RIP 버전 2를 기반으로 합니다.

참고: 비대칭 라우팅은 ASA/PIX에서 지원되지 않습니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco ASA/PIX는 버전 7.x 이상을 실행해야 합니다.
- 다중 컨텍스트 모드에서는 RIP가 지원되지 않습니다.단일 모드에서만 지원됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.0 이상을 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)
- Cisco ASDM(Adaptive Security Device Manager) 소프트웨어 버전 6.0 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

이 문서의 정보는 소프트웨어 버전 8.0 이상을 실행하는 Cisco 500 Series PIX 방화벽에도 적용됩니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

RIP는 경로 선택을 위한 메트릭으로 hop count를 사용하는 거리 벡터 라우팅 프로토콜입니다.인터페이스에서 RIP가 활성화된 경우, 인터페이스는 경로에 대해 동적으로 배우고 광고하기 위해 인접 디바이스와 RIP 브로드캐스트를 교환합니다.

보안 어플라이언스는 RIP 버전 1 및 RIP 버전 2를 모두 지원합니다. RIP 버전 1은 라우팅 업데이트와 함께 서브넷 마스크를 전송하지 않습니다.RIP 버전 2는 라우팅 업데이트와 함께 서브넷 마스크를 전송하고 가변 길이 서브넷 마스크를 지원합니다.또한 RIP 버전 2는 라우팅 업데이트가 교환될 때 인접 디바이스 인증을 지원합니다.이 인증은 보안 어플라이언스가 신뢰할 수 있는 소스에서 신뢰할 수 있는 라우팅 정보를 수신하도록 보장합니다.

제한 사항:

1. 보안 어플라이언스가 인터페이스 간에 RIP 업데이트를 전달할 수 없습니다.
2. RIP 버전 1은 VLSM(Variable-Length Subnet Mask)을 지원하지 않습니다.
3. RIP의 최대 hop 개수는 15입니다. 홉이 15보다 큰 경로는 연결할 수 없는 것으로 간주됩니다.
4. RIP 컨버전스는 다른 라우팅 프로토콜에 비해 상대적으로 느립니다.
5. 보안 어플라이언스에서 단일 RIP 프로세스만 활성화할 수 있습니다.

참고: 이 정보는 RIP 버전 2에만 적용됩니다.

1. 인접 디바이스 인증을 사용하는 경우 인터페이스에 RIP 버전 2 업데이트를 제공하는 모든 인접 디바이스에서 인증 키와 키 ID가 동일해야 합니다.
2. RIP 버전 2에서는 보안 어플라이언스가 멀티캐스트 주소 224.0.0.9을 사용하여 기본 경로 업데이트를 전송하고 수신합니다. 패시브 모드에서는 해당 주소에서 경로 업데이트를 수신합니

다.
3. 인터페이스에서 RIP 버전 2를 구성하면 멀티캐스트 주소 224.0.0.9이 해당 인터페이스에 등록됩니다.인터페이스에서 RIP 버전 2 컨피그레이션을 제거하면 해당 멀티캐스트 주소가 등록되지 않습니다.

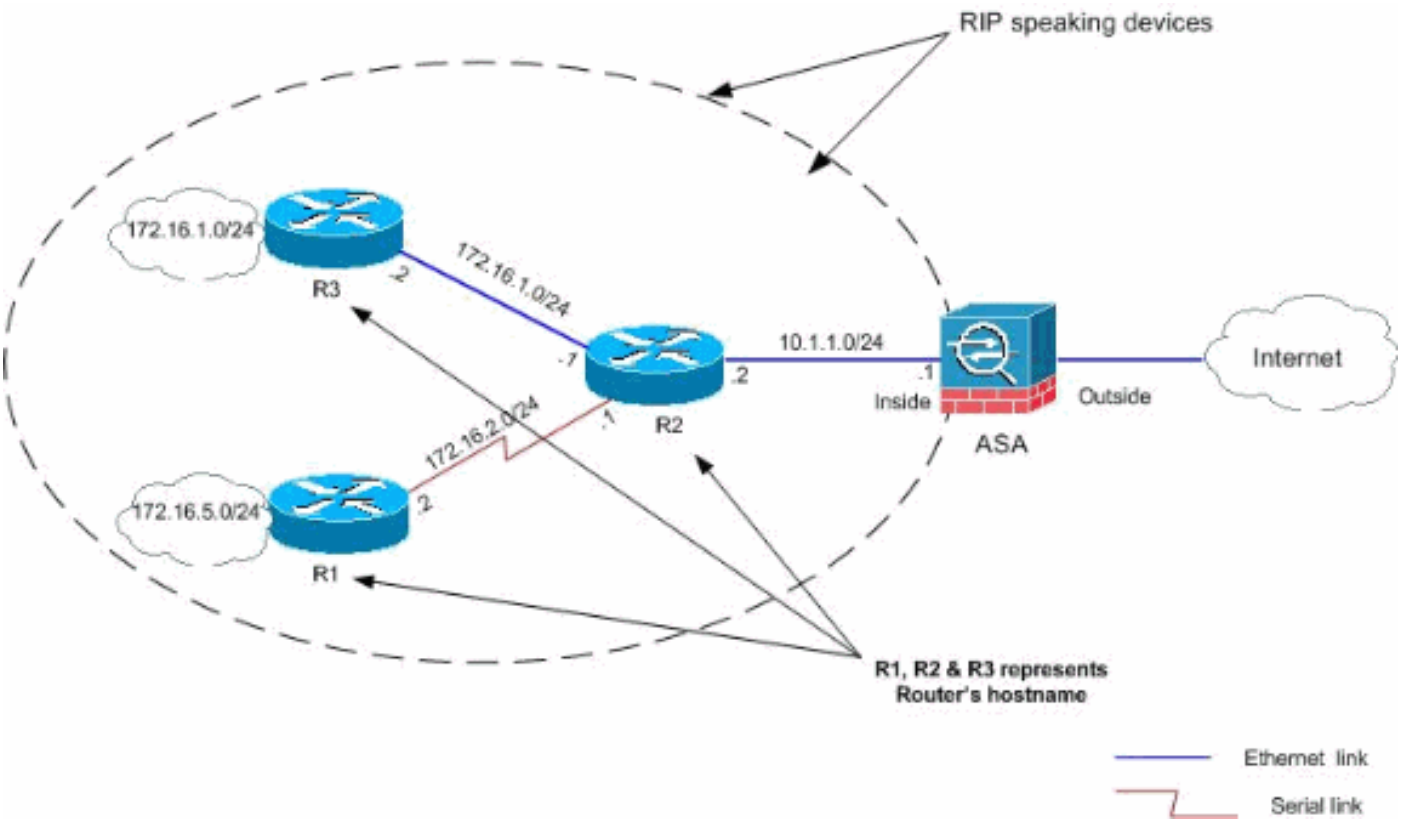
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- ASDM 컨피그레이션
- RIP 인증 구성
- Cisco ASA CLI 컨피그레이션
- Cisco IOS 라우터(R2) CLI 컨피그레이션
- Cisco IOS 라우터(R1) CLI 컨피그레이션
- Cisco IOS 라우터(R3) CLI 컨피그레이션

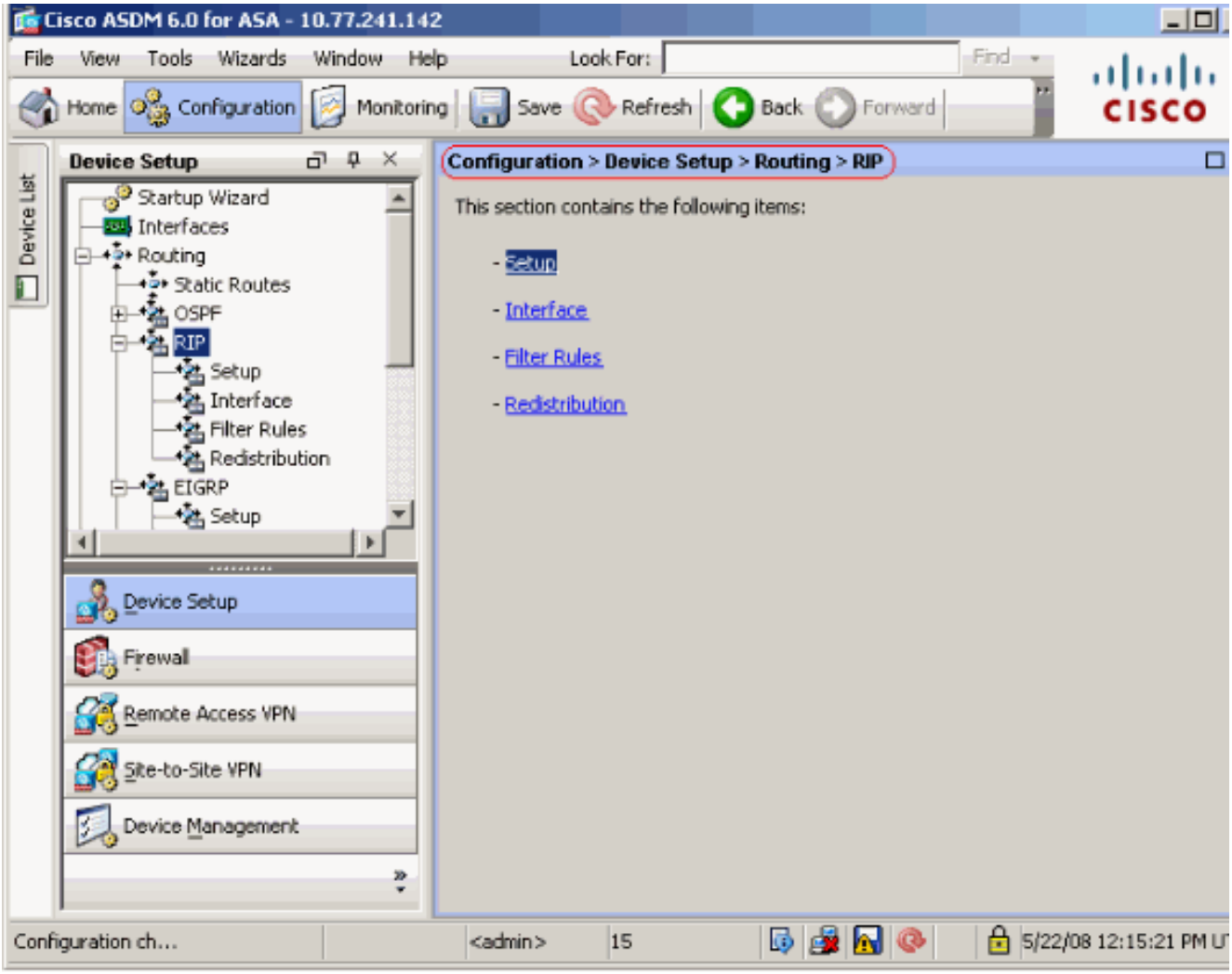
ASDM 컨피그레이션

ASDM(Adaptive Security Device Manager)은 보안 어플라이언스에서 소프트웨어를 구성하고 모니터링하는 데 사용되는 브라우저 기반 애플리케이션입니다.ASDM은 보안 어플라이언스에서 로드된 다음 디바이스를 구성, 모니터링 및 관리하는 데 사용됩니다.또한 ASDM Launcher(Windows®만 해당)를 사용하여 Java 애플릿보다 빠르게 ASDM 애플리케이션을 시작할 수 있습니다.이 섹션에서는 ASDM을 사용하여 이 문서에 설명된 기능을 구성하는 데 필요한 정보에 대해 설명합니다.

Cisco ASA에서 RIP를 구성하려면 다음 단계를 완료합니다.

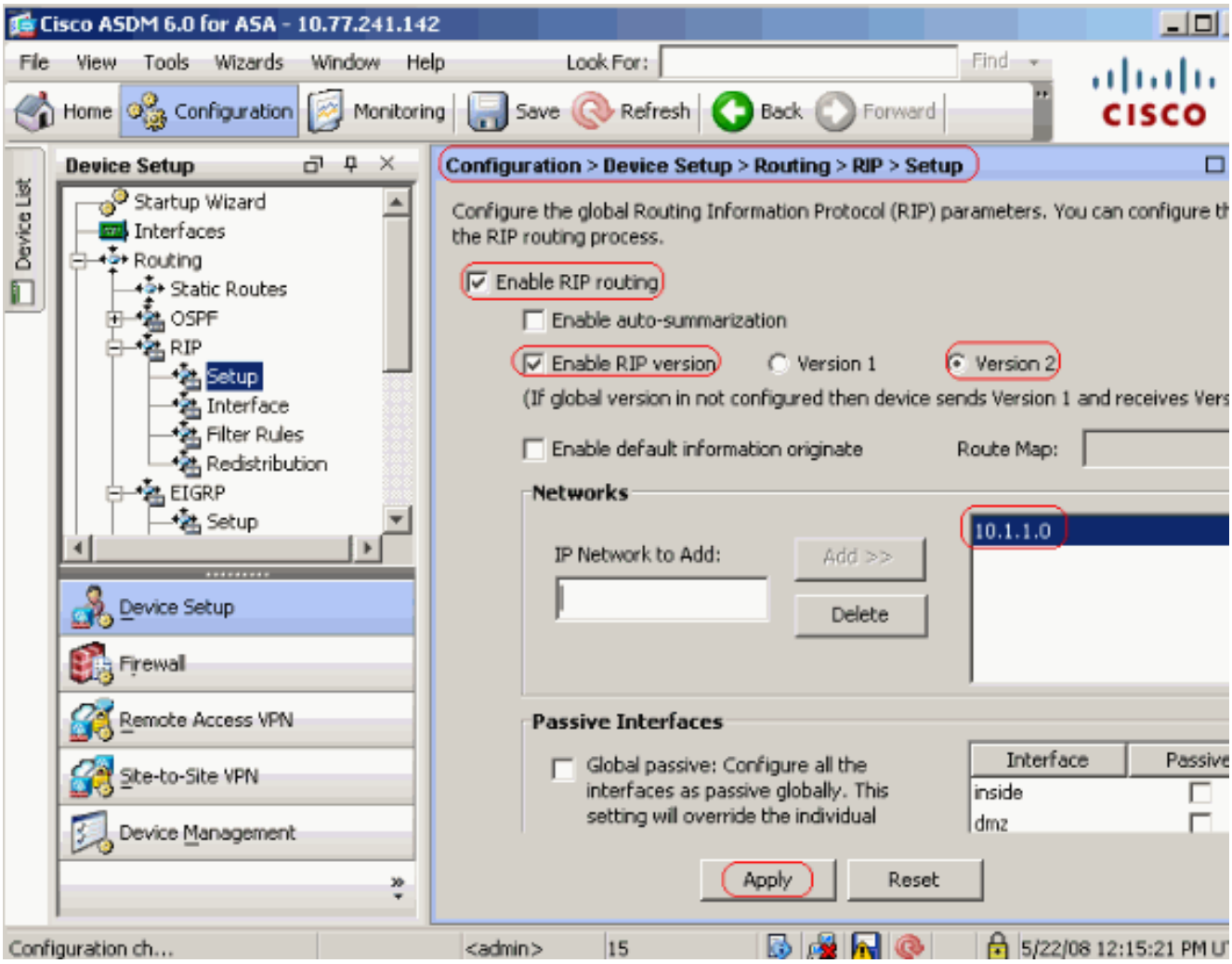
1. Cisco ASA with ASDM에 로그인합니다.
2. 스크린샷과 **같이 ASDM** 인터페이스에서 Configuration > Device Setup > Routing > RIP를 선택합니다

.



3. 표시된 대로 RIP **라우팅을 활성화하려면 Configuration > Device Setup > Routing > RIP > Setup**을 선택합니다.Enable RIP routing 확인란을 **선택합니다**.Enable RIP **version with** 라디오 버튼 **Version 2(버전 2**와 함께 RIP **버전 활성화) 확인란을 선택합니다**.Networks 탭에서 네트워크 **10.1.1.0을 추가합니다**.Apply를 **클릭합니다**

.



필드Enable RIP Routing(RIP 라우팅 활성화) - 보안 어플라이언스에서 RIP 라우팅을 활성화하려면 이 확인란을 선택합니다.RIP를 활성화하면 모든 인터페이스에서 활성화됩니다.이 확인란을 선택하면 이 창의 다른 필드도 활성화됩니다.보안 어플라이언스에서 RIP 라우팅을 비활성화하려면 이 확인란의 선택을 취소합니다.Enable Auto-summarization(자동 요약 활성화) - 자동 경로 요약을 비활성화하려면 이 확인란의 선택을 취소합니다.자동 경로 요약을 다시 활성화하려면 이 확인란을 선택합니다.RIP 버전 1은 항상 자동 요약을 사용합니다.RIP 버전 1의 자동 요약을 비활성화할 수 없습니다. RIP 버전 2를 사용하는 경우 이 확인란의 선택을 취소하면 자동 요약을 해제할 수 있습니다.연결이 끊긴 서브넷 간의 라우팅을 수행해야 하는 경우 자동 요약을 비활성화합니다.자동 요약이 비활성화되면 서브넷이 광고됩니다.Enable RIP version(RIP 버전 활성화) - 보안 어플라이언스에서 사용하는 RIP 버전을 지정하려면 이 확인란을 선택합니다.이 확인란을 선택하지 않으면 보안 어플라이언스가 RIP 버전 1 업데이트를 전송하고 RIP 버전 1 및 버전 2 업데이트를 수락합니다.이 설정은 인터페이스 창에서 인터페이스별로 재정의할 수 있습니다.버전 1 - 보안 어플라이언스가 RIP 버전 1 업데이트만 보내고 받도록 지정합니다.받은 버전 2 업데이트는 삭제됩니다.Version 2(버전 2) - 보안 어플라이언스가 RIP 버전 2 업데이트만 보내고 받도록 지정합니다.받은 버전 1 업데이트는 삭제됩니다.Enable default information originate(기본 정보 시작 활성화) - RIP 라우팅 프로세스에 대한 기본 경로를 생성하려면 이 확인란을 선택합니다.기본 경로를 생성하기 전에 충족해야 하는 경로 맵을 구성할 수 있습니다.Route-map - 적용할 경로 맵의 이름을 입력합니다.경로 맵이 충족되면 라우팅 프로세스에서 기본 경로를 생성합니다.IP Network to Add(추가할 IP 네트워크) - RIP 라우팅 프로세스의 네트워크를 정의합니다.지정된 네트워크 번호는 서브넷 정보를 포함할 수 없습니다.보안 어플라이언스 컨피그레이션에 추가할 수 있는 네트워크 수에는 제한이 없습니다.RIP 라우팅 업데이트는 지정된 네트워크의 인터페이스를 통해서만 전송 및 수신됩니다.또한 인터페이스의 네트워크를 지정하지 않으면 RIP 업데이트에서 인터페이스가 광고되지 않습니다.Add(추가) - 지정된 네트워크를 네트워크 목록에 추가하려면 이 버튼을 클릭합니

다.Delete(삭제) - 선택한 네트워크를 네트워크 목록에서 제거하려면 이 버튼을 클릭합니다 .Configure interfaces as passive globally(인터페이스를 패시브로 구성) - 보안 어플라이언스의 모든 인터페이스를 패시브 RIP 모드로 설정하려면 이 확인란을 선택합니다.보안 어플라이언스는 모든 인터페이스에서 RIP 라우팅 브로드캐스트를 수신하며 이 정보를 사용하여 라우팅 테이블을 채우지만 라우팅 업데이트를 브로드캐스트하지 않습니다.특정 인터페이스를 패시브 RIP로 설정하려면 Passive Interfaces 테이블을 사용합니다.Passive Interfaces(패시브 인터페이스) 테이블 - 보안 어플라이언스에 구성된 인터페이스를 나열합니다.패시브 모드에서 작동할 인터페이스에 대한 Passive 열의 확인란을 선택합니다.다른 인터페이스는 여전히 RIP 브로드캐스트를 보내고 받습니다.

RIP 인증 구성

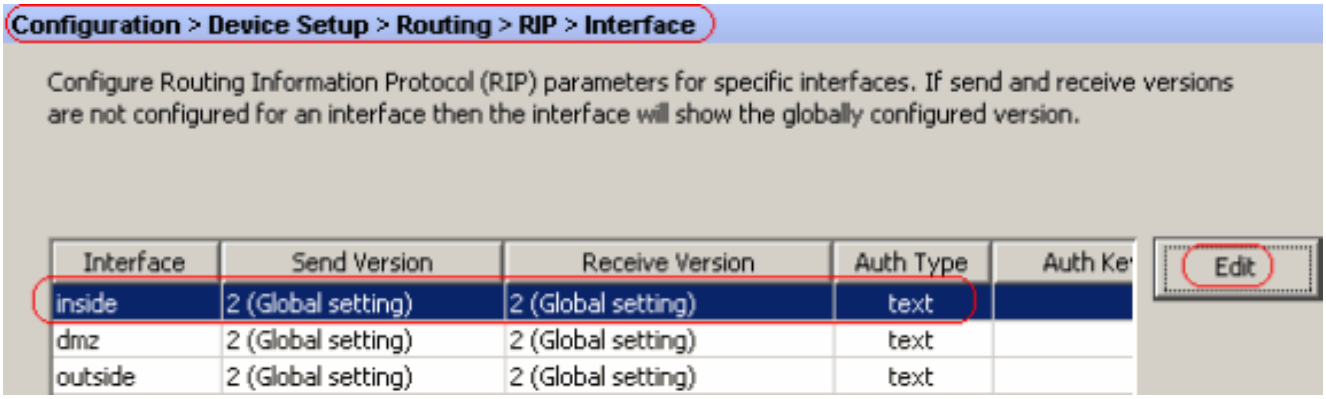
Cisco ASA는 RIP v2 라우팅 프로토콜에서 라우팅 업데이트의 MD5 인증을 지원합니다.각 RIP 패킷의 MD5 키 다이제스트는 승인되지 않은 소스에서 승인되지 않은 또는 잘못된 라우팅 메시지를 유입하는 것을 방지합니다.RIP 메시지에 인증을 추가하면 라우터와 Cisco ASA가 동일한 사전 공유 키로 구성된 다른 라우팅 디바이스의 라우팅 메시지만 수락할 수 있습니다.이 인증이 구성되지 않은 경우 네트워크에 서로 다른 경로 정보가 있거나 반대 경로 정보가 있는 다른 라우팅 디바이스를 도입하면 라우터 또는 Cisco ASA의 라우팅 테이블이 손상될 수 있으며 서비스 거부 공격이 발생할 수 있습니다.ASA를 포함하는 라우팅 디바이스 간에 전송되는 RIP 메시지에 인증을 추가하면 네트워크에 다른 라우터를 의도하거나 실수로 추가하는 것과 문제가 발생하지 않습니다.

RIP 경로 인증은 인터페이스별로 구성됩니다.RIP 메시지 인증을 위해 구성된 인터페이스의 모든 RIP 인접 디바이스는 동일한 인증 모드 및 키로 구성해야 합니다.

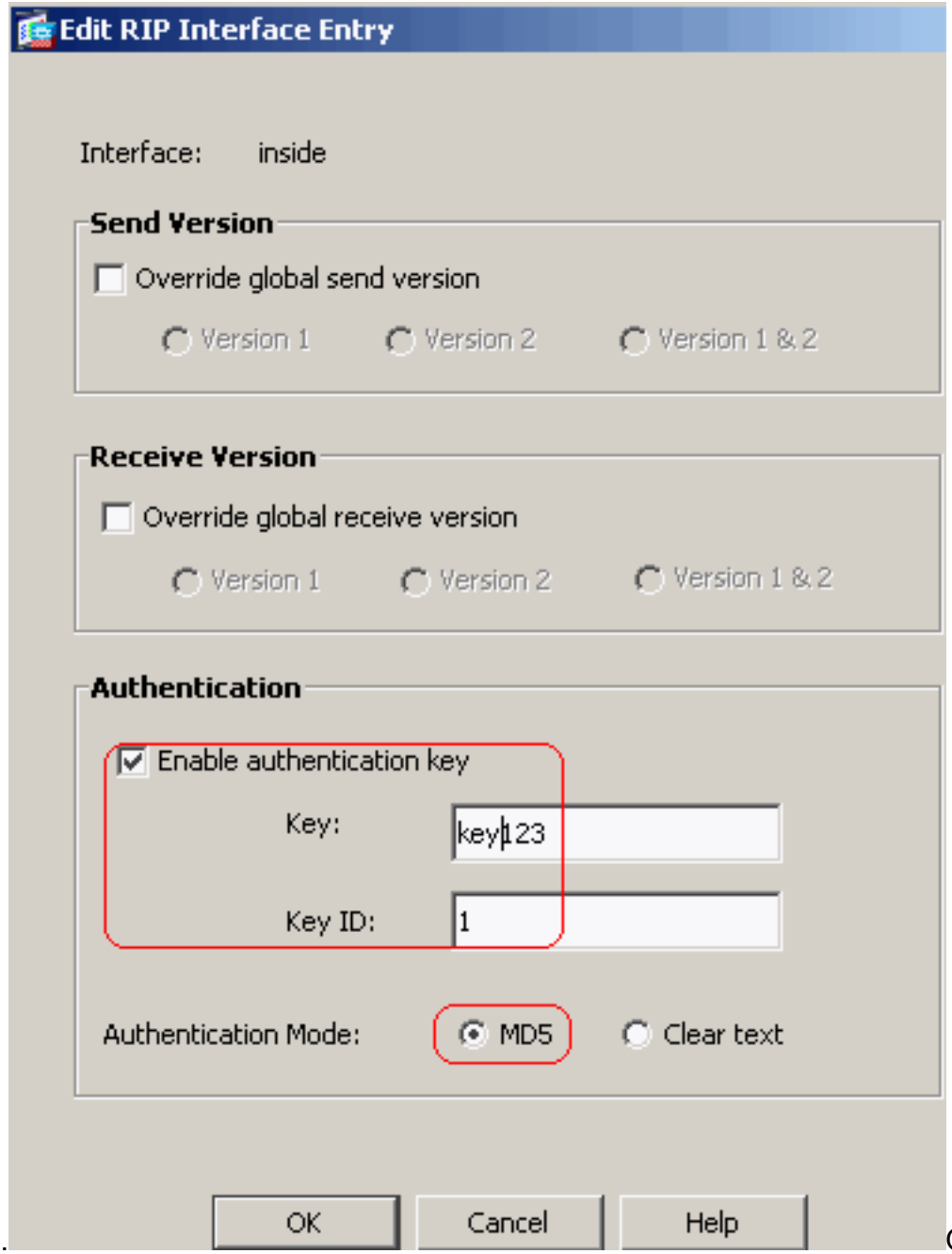
Cisco ASA에서 RIP MD5 인증을 활성화하려면 다음 단계를 완료하십시오.

1. ASDM에서 **Configuration > Device Setup > Routing > RIP > Interface**를 선택하고 마우스로 내부 인터페이스를 선택합니다.Edit를 **클릭합니다**

.



2. Enable **authentication key(인증 키** 활성화) 확인란을 선택한 다음 **Key** value(**키** 값)와 **Key ID(키** ID) 값을 입력합니다



OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.

Cisco ASA CLI 컨피그레이션

Cisco ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- RIP authentication is
configured on the inside interface. rip authentication
```

```
mode md5
 rip authentication key




!

!--- Output Suppressed !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0 !-
-- RIP Configuration router rip
 network 10.0.0.0
 version 2

!--- This is the static default gateway configuration in
!--- order to reach the Internet. route outside 0.0.0.0
0.0.0.0 192.168.1.1 1
```

Cisco IOS 라우터(R2) CLI 컨피그레이션

Cisco IOS 라우터(R2)

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain 1

!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
```

Cisco IOS 라우터(R1) CLI 컨피그레이션

Cisco IOS 라우터(R1)

```
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

Cisco IOS 라우터(R3) CLI 컨피그레이션

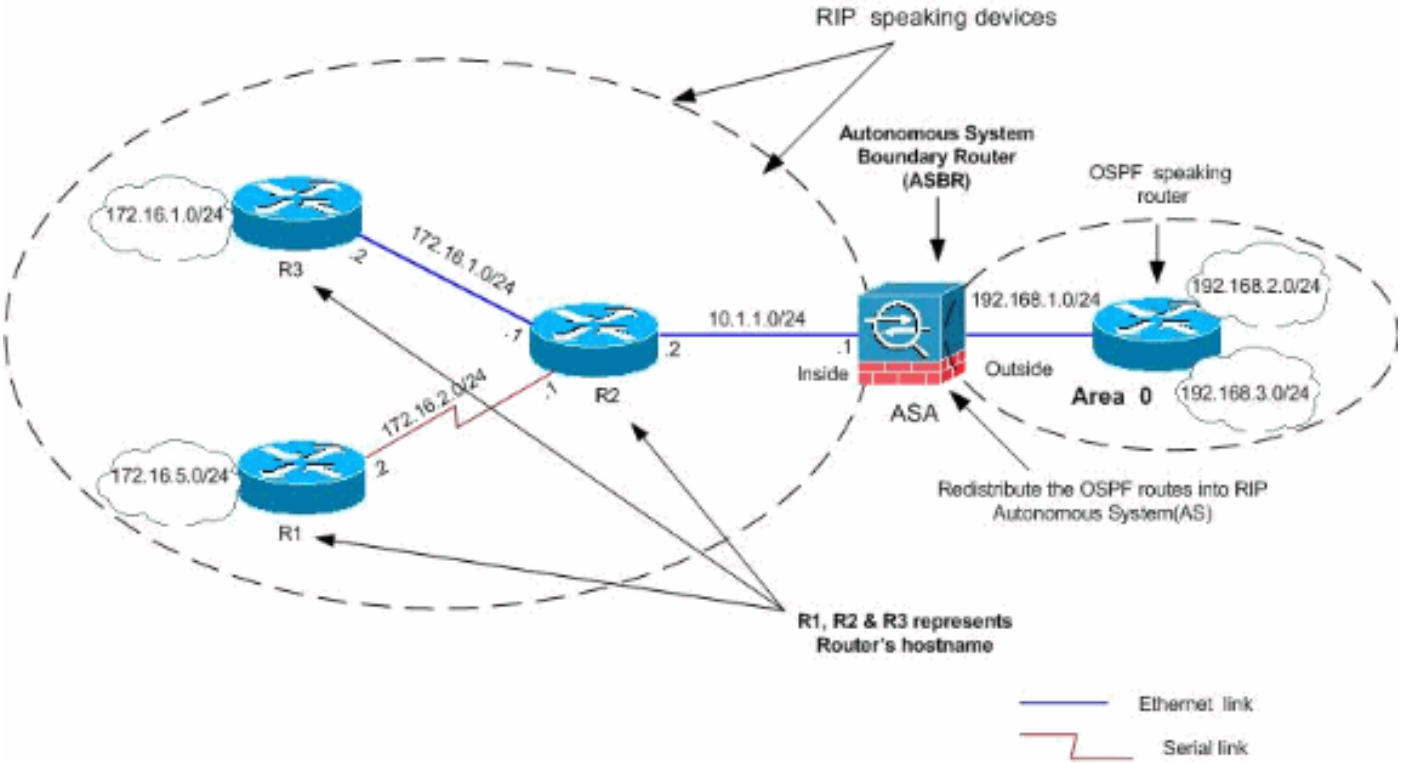
Cisco IOS 라우터(R3)

```
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

ASA를 사용하여 RIP로 재배포

OSPF, EIGRP, 고정 및 연결된 라우팅 프로세스의 경로를 RIP 라우팅 프로세스로 재배포할 수 있습니다.

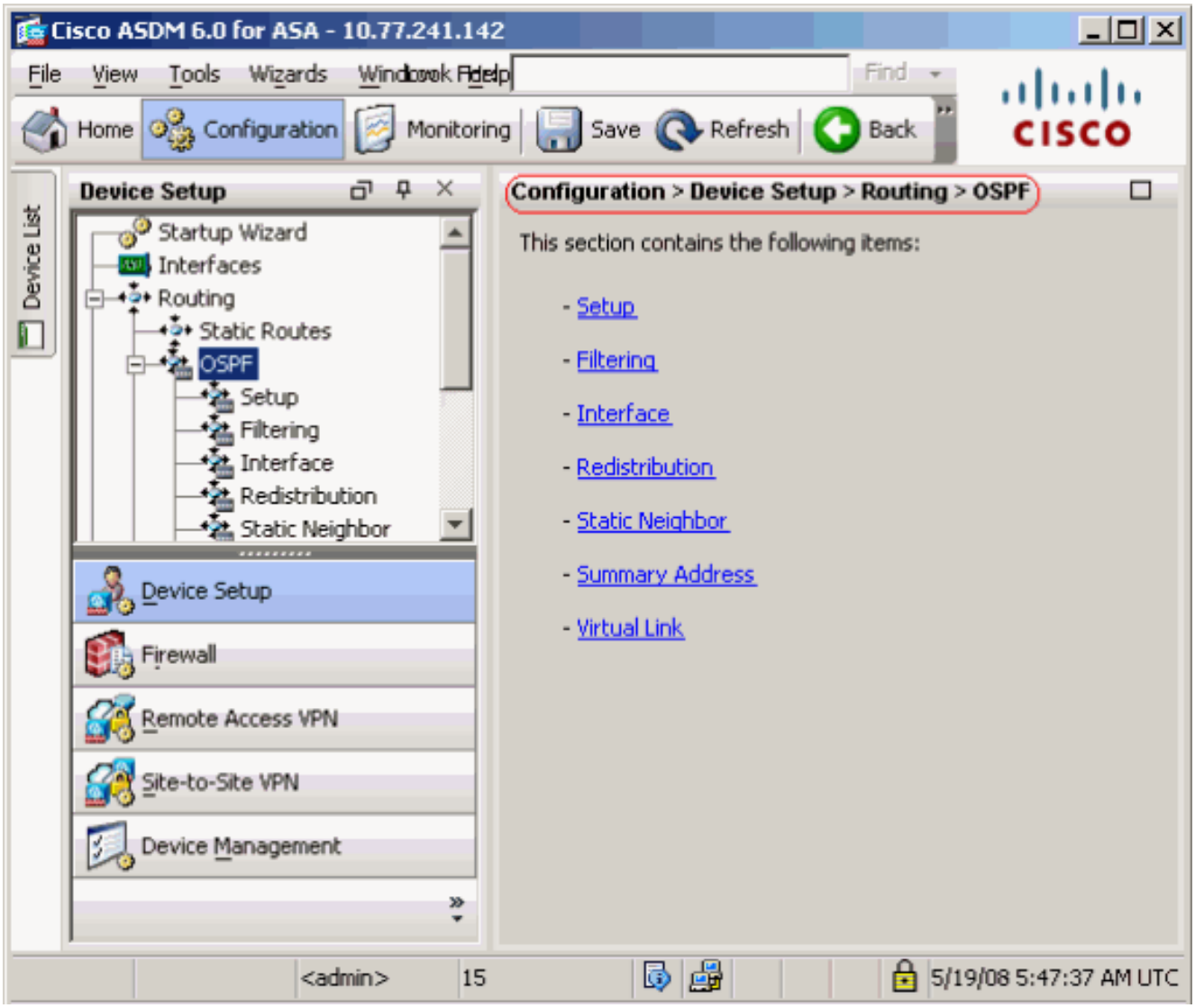
이 예에서는 네트워크 다이어그램으로 OSPF 경로를 RIP로 재배포하는 것이 표시됩니다.



ASDM 컨피그레이션

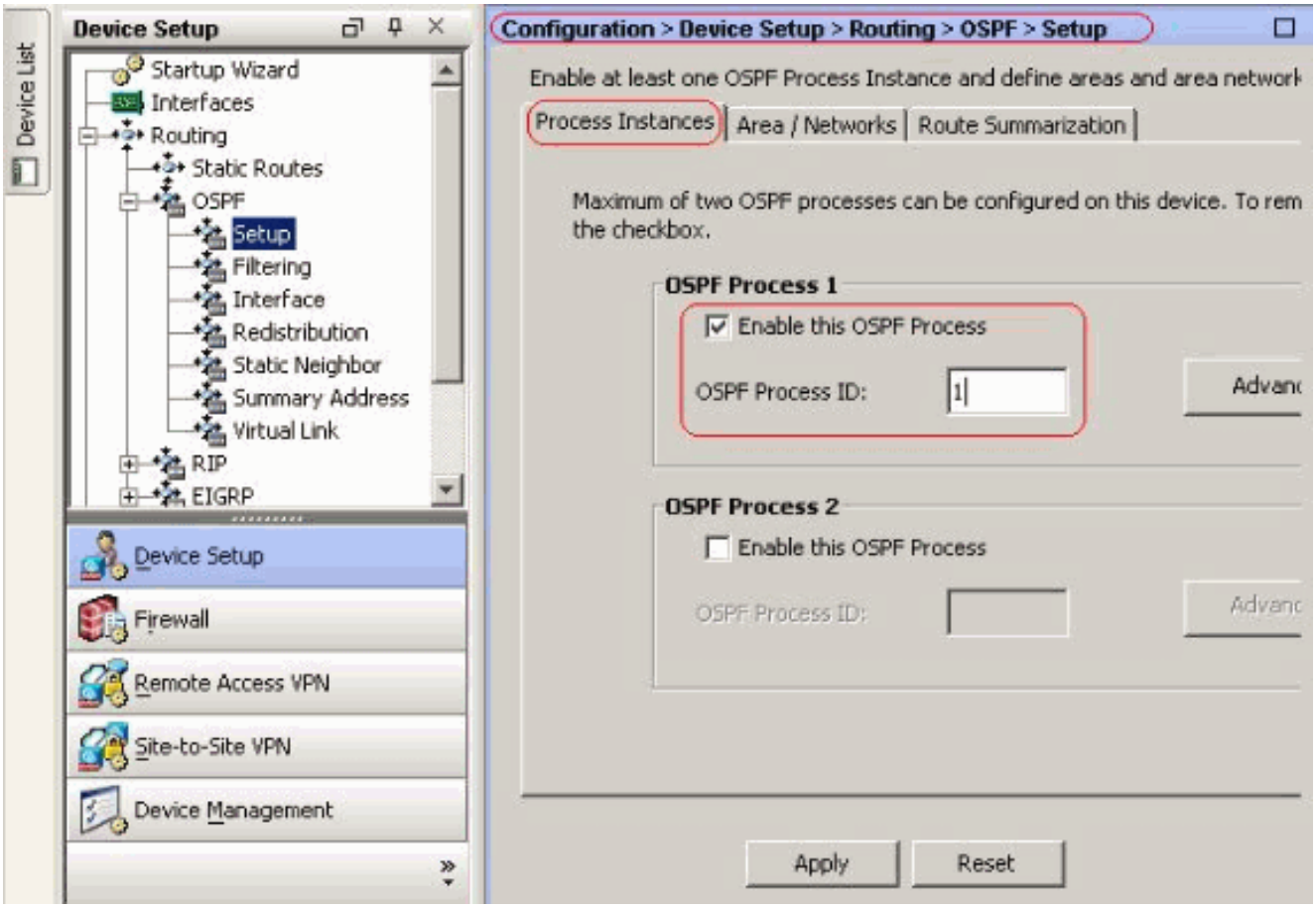
다음 단계를 완료하십시오.

1. **OSPF 컨피그레이션**스크린샷과 **같이 ASDM** 인터페이스에서 Configuration > Device Setup > Routing > OSPF를 선택합니다
.



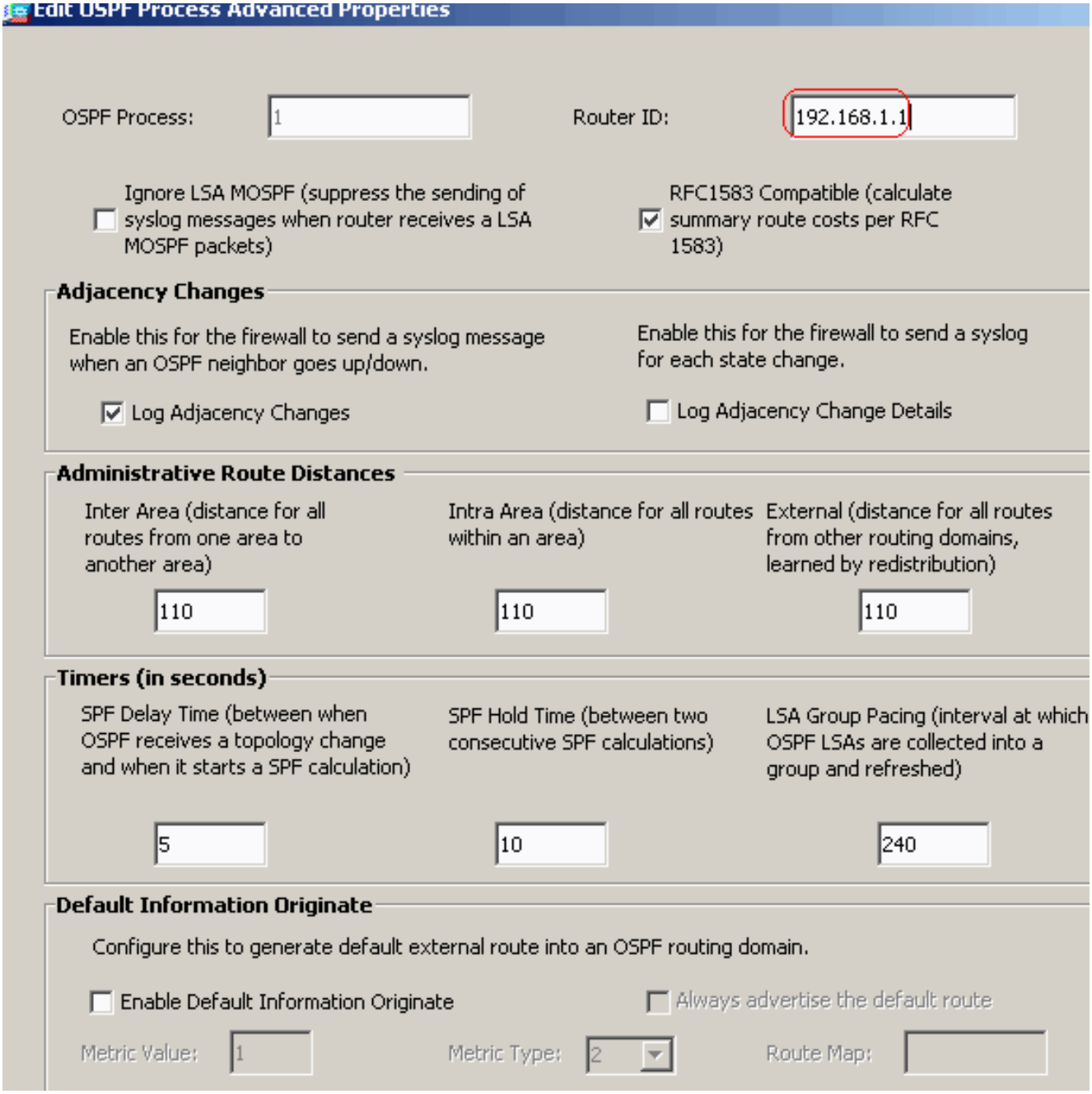
스크린샷과 같이 **Setup > Process Instances** 탭에서 OSPF 라우팅 프로세스를 활성화합니다 .이 예에서는 OSPF ID 프로세스가 **1**입니다

.



선택적 고급 OSPF 라우팅 프로세스 매개변수를 구성하려면 **Setup > Process Instances** 탭에서 Advanced를 클릭합니다.라우터 ID, 인접성 변경, 관리 경로 거리, 타이머 및 기본 정보 시작 설정과 같은 프로세스별 설정을 편집할 수 있습니다

.



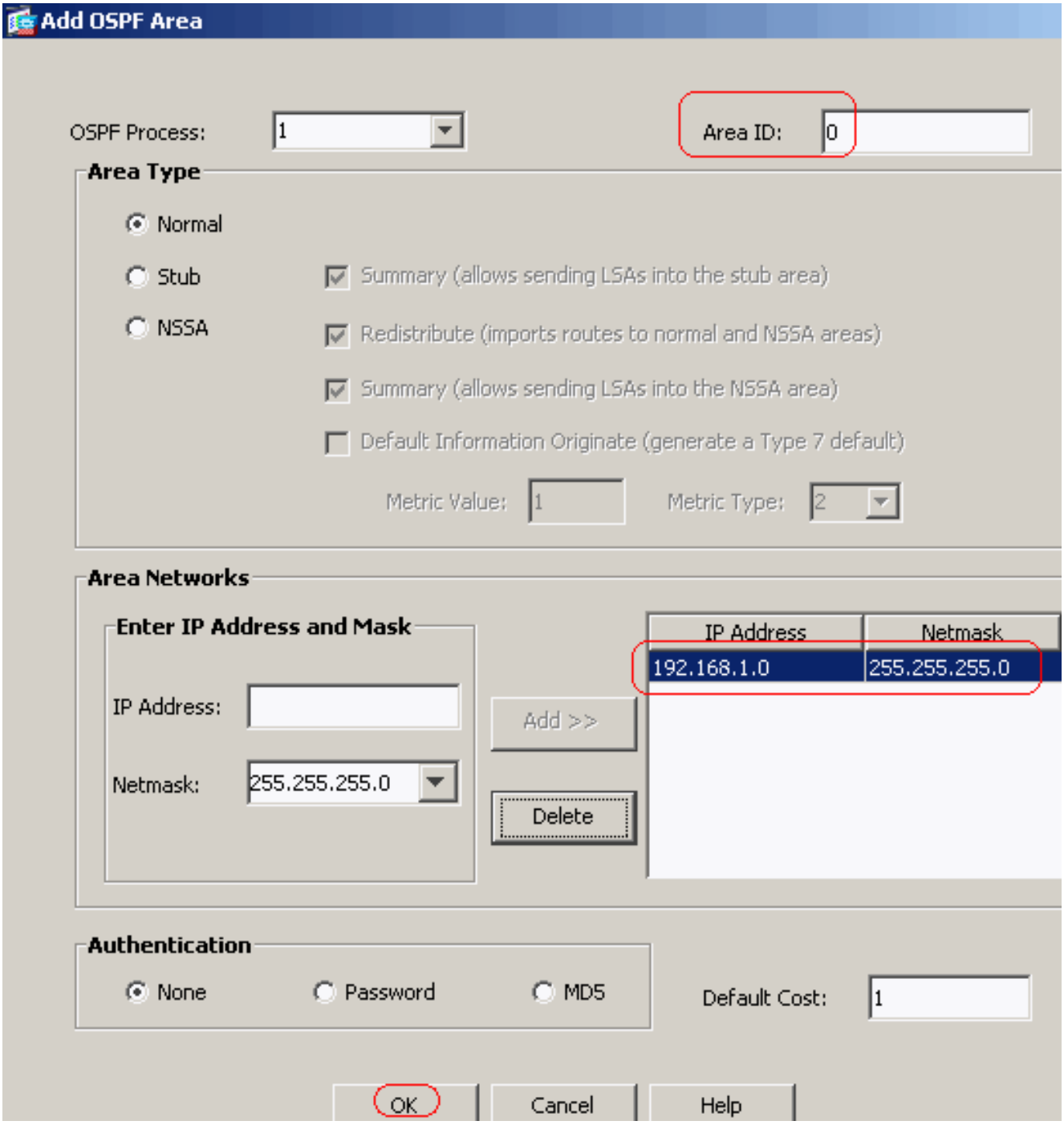
확인을 **클릭합니다**.이전 단계를 완료한 후 Setup(설정) > Area/**Networks** 탭에서 OSPF 라우팅에 참여하는 네트워크 및 인터페이스를 정의합니다.이 스크린샷과 같이 Add를 클릭합니다

.

이 화면이 나타납니다.이 예에서는 OSPF가 외부 인터페이스에서만 활성화되므로 외부 네트워크(192.168.1.0/24)만 추가합니다.**참고:** 정의된 네트워크에 속하는 IP 주소를 가진 인터페이

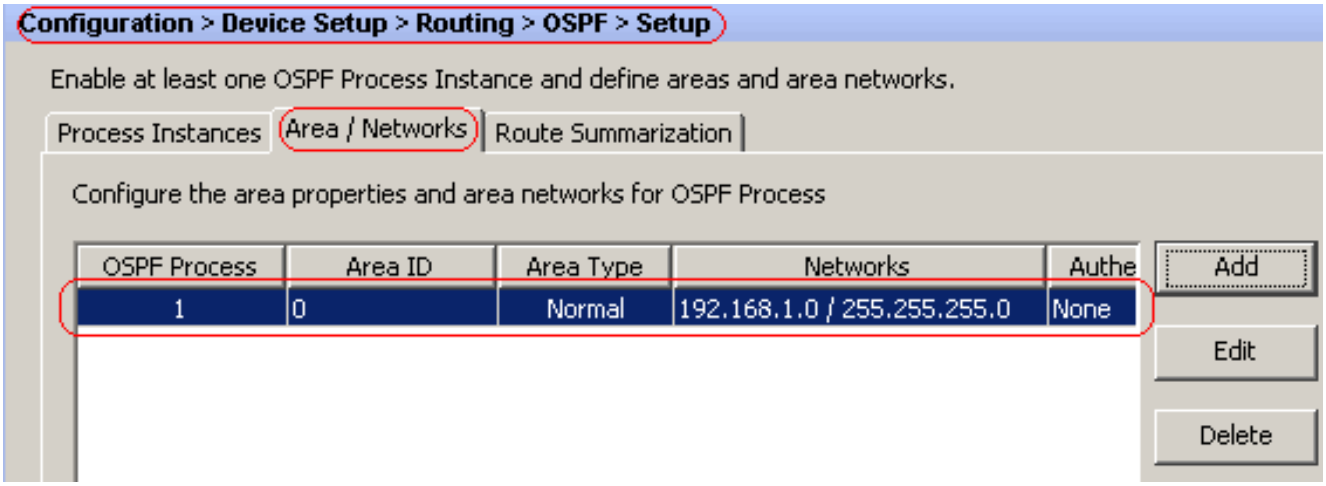
스만 OSPF 라우팅 프로세스에 참여합니다

.



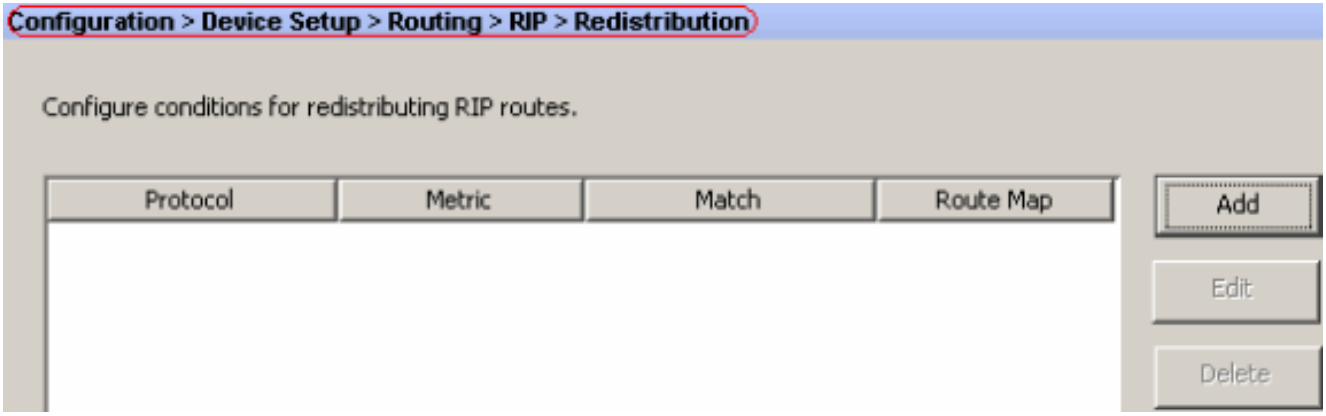
확인을 클릭합니다.Apply를 **클릭합니다**

.

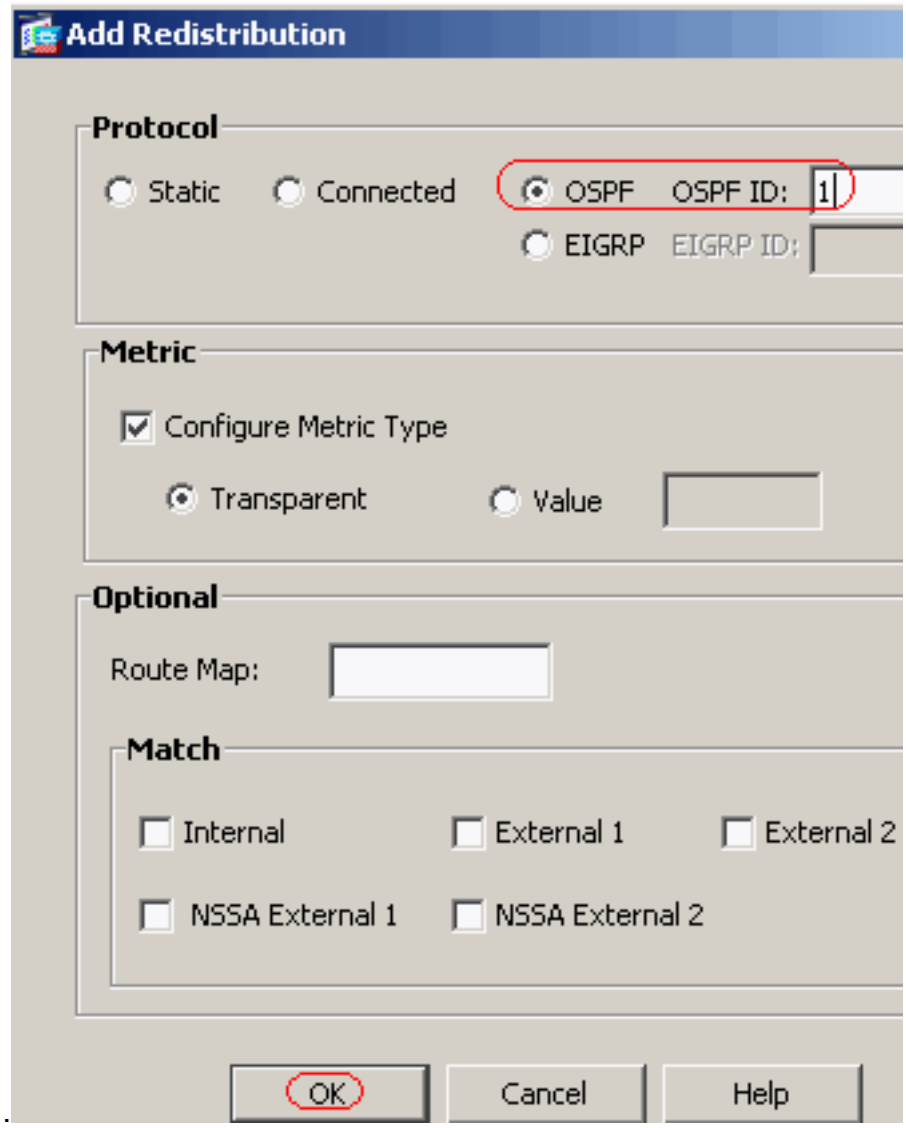


2. OSPF **경로를 RIP로 재배포하려면 Configuration > Device Setup > Routing > RIP > Redistribution > Add**를 선택합니다

.



3. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**



동등한 CLI 컨피그레이션

RIP AS에 OSPF를 재배포하기 위한 ASA의 CLI 컨피그레이션
router rip network 10.0.0.0 **redistribute ospf 1 metric transparent** version 2 ! router ospf 1 router-id 192.168.1.1 network 192.168.1.0 255.255.255.0 area 0 area 0 log-adj-changes

OSPF 경로를 RIP AS로 재배포한 후 인접 디바이스 Cisco IOS Router(R2)의 라우팅 테이블을 볼 수 있습니다.

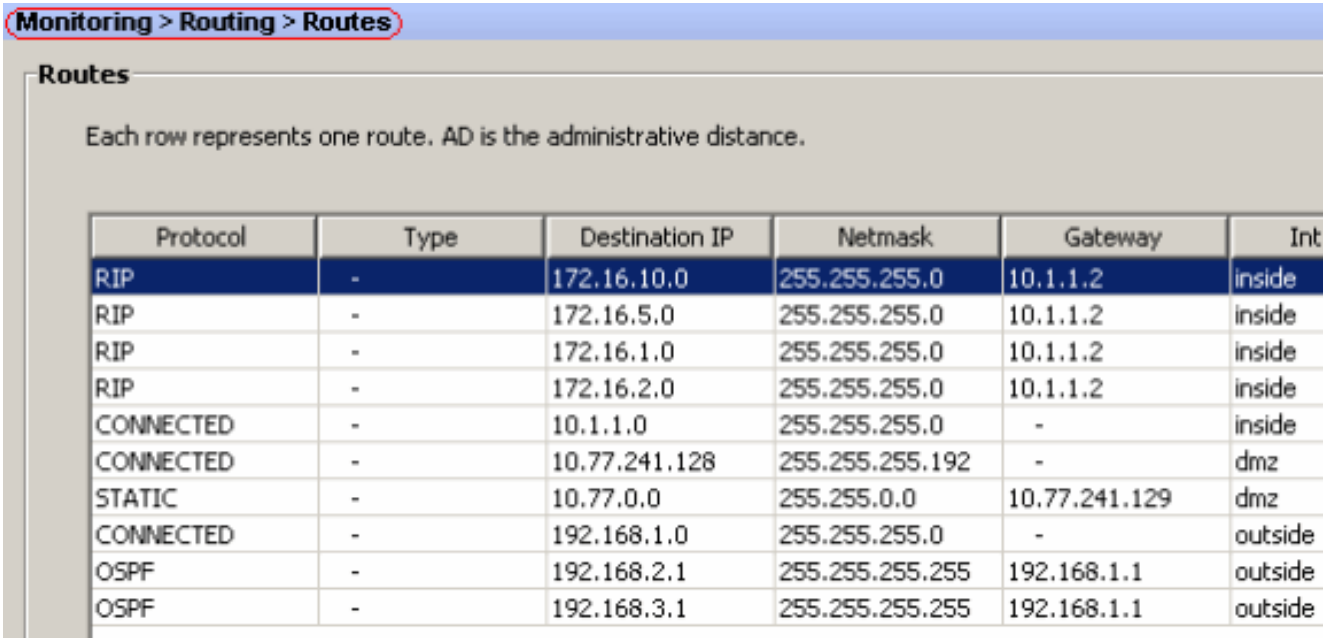
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, su - IS-IS summary, 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 not set

     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1
R       172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1
C       172.16.1.0 is directly connected, Ethernet1
C       172.16.2.0 is directly connected, Serial1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Ethernet0
R       10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.2.0/32 is subnetted, 1 subnets
R       192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.3.0/32 is subnetted, 1 subnets
R       192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
!--- Redistributed route advertised by Cisco ASA
```

다음을 확인합니다.

구성을 확인하려면 다음 단계를 완료하십시오.

1. Monitoring(모니터링) > Routing(라우팅) **> Routes(경로)**로 이동하면 라우팅 테이블을 확인할 수 있습니다.이 스크린샷에서는 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 및 172.16.10.0/24 네트워크가 R2(10.1.1.2)과 RIP를 통해 학습되는 것을 확인할 수 있습니다
.



Protocol	Type	Destination IP	Netmask	Gateway	Int
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	outside
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	outside

2. CLI에서 동일한 출력을 가져오기 위해 **show route** 명령을 사용할 수 있습니다.

```
ciscoasa#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 not set

R    172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
R    172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
C    10.1.1.0 255.255.255.0 is directly connected, inside
C    10.77.241.128 255.255.255.192 is directly connected, dmz
S    10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C    192.168.1.0 255.255.255.0 is directly connected, outside
O    192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
O    192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
ciscoasa#
```

문제 해결

이 섹션에서는 OSPF 문제를 해결하는 데 유용한 debug 명령에 대한 정보를 제공합니다.

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 rip events** - RIP 이벤트의 디버깅을 활성화합니다.

```
ciscoasa#debug rip events
rip_route_adjust for inside coming up
RIP: sending request on inside to 224.0.0.9
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build flash update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
RIP: Update contains 5 routes
RIP: Update queued
RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1)
RIP: build flash update entries - suppressing null update
RIP: Update sent via dmz rip-len:112
RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
```

```
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 8 routes
RIP: Update queued
RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1)
RIP: build update entries
        10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 4 routes
RIP: Update queued
RIP: Update sent via dmz rip-len:172
RIP: Update sent via inside rip-len:92
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
```

관련 정보

- Cisco 5500 Series Adaptive Security Appliance 지원 페이지
- Cisco 500 Series PIX 지원 페이지
- PIX/ASA 8.X:Cisco ASA(Adaptive Security Appliance)에서 EIGRP 구성
- 기술 지원 및 문서 – Cisco Systems