ASA 9.x EIGRP 컨피그레이션 예

목차

소개

이 문서에서는 ASA 소프트웨어 버전 9.x 이상에서 지원되는 EIGRP(Enhanced Interior Gateway Routing Protocol)를 통해 경로를 학습하고 인증을 수행하기 위해 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이 구성을 시도하기 전에 다음 조건을 충족해야 합니다.

- Cisco ASA는 버전 9.x 이상을 실행해야 합니다.

- EIGRP는 다중 컨텍스트 모드에서 지원되지 않으므로 단일 컨텍스트 모드여야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 소프트웨어 버전 9.2.1
- Cisco ASDM(Adaptive Security Device Manager) 버전 7.2.1
- 버전 12.4를 실행하는 Cisco IOS®Router

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.

배경 정보

지침 및 제한 사항

- 단일 모드에서 단일 EIGRP 인스턴스와 다중 모드의 컨텍스트별로 지원됩니다.
- 다중 모드의 EIGRP 인스턴스당 컨텍스트당 두 개의 스레드가 생성되며 show 프로세스를 통해 볼 수 있습니다.
- 자동 요약은 기본적으로 비활성화되어 있습니다.
- 개별 인터페이스 모드의 클러스터 유닛 간에 네이버 관계가 설정되지 않았습니다.
- [<acl>]의 기본 정보는 들어오는 후보 기본 경로의 외부 비트를 필터링하는 데 사용됩니다.
- 나가는 후보 기본 경로에서 외부 비트를 필터링하기 위해 [<acl>]에서 기본 정보가 사용됩니다.

EIGRP 및 장애 조치

Cisco ASA 코드 버전 8.4.4.1 이상에서는 ACTIVE 유닛에서 STANDBY 유닛으로 동적 경로를 동기화합니다. 또한 경로 삭제는 STANDBY 유닛에도 동기화됩니다. 그러나 피어 인접성의 상태가 동기화되지 않습니다. ACTIVE 디바이스만 인접 상태를 유지하고 동적 라우팅에 적극적으로 참여합니다. ASA FAQ를 참조하십시오. 동적 경로가 동기화되면 장애 조치 후 어떻게 됩니까? 자세한 내용을 참조하십시오.

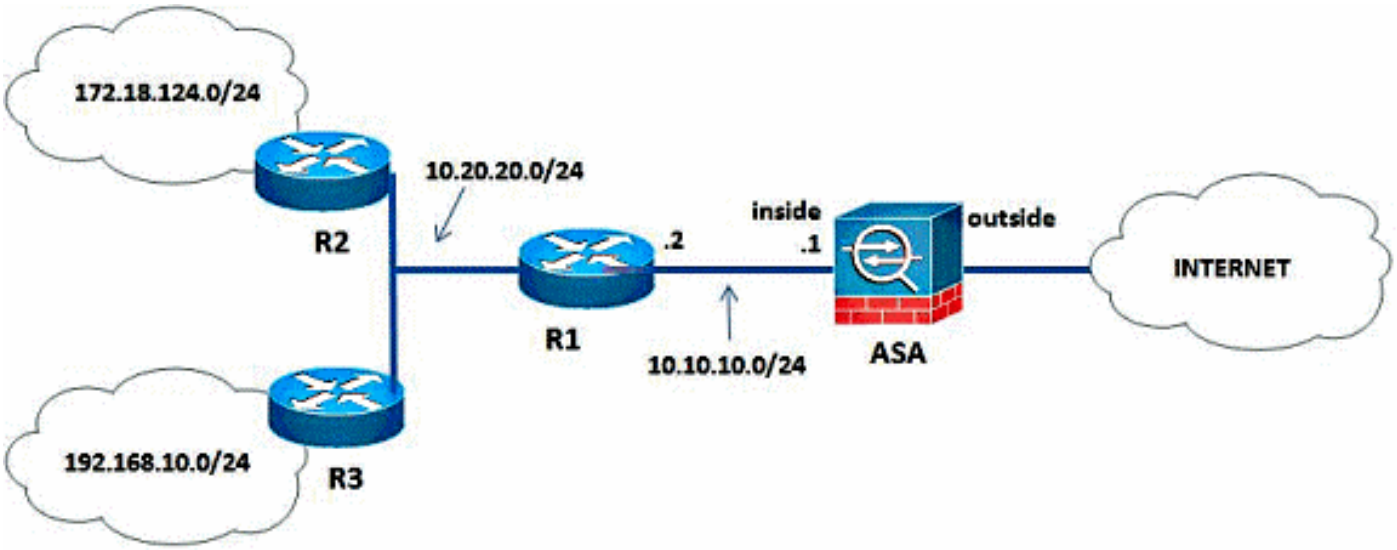
구성

이 섹션에서는 이 문서에서 다루는 기능을 구성하는 방법에 대해 설명합니다.

> **참고:** 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표시된 네트워크 토폴로지에서 Cisco ASA 내부 인터페이스 IP 주소는 10.10.10.1/24입니다. 목표는 인접 라우터(R1)를 통해 동적으로 내부 네트워크 경로(10.20.20.0/24, 172.18.124.0/24 및 192.168.10.0/24)을 학습하기 위해 Cisco ASA에서 EIGRP를 구성하는 것입니다. R1은 다른 두 라우터(R2 및 R3)를 통해 원격 내부 네트워크에 대한 경로를 학습합니다.

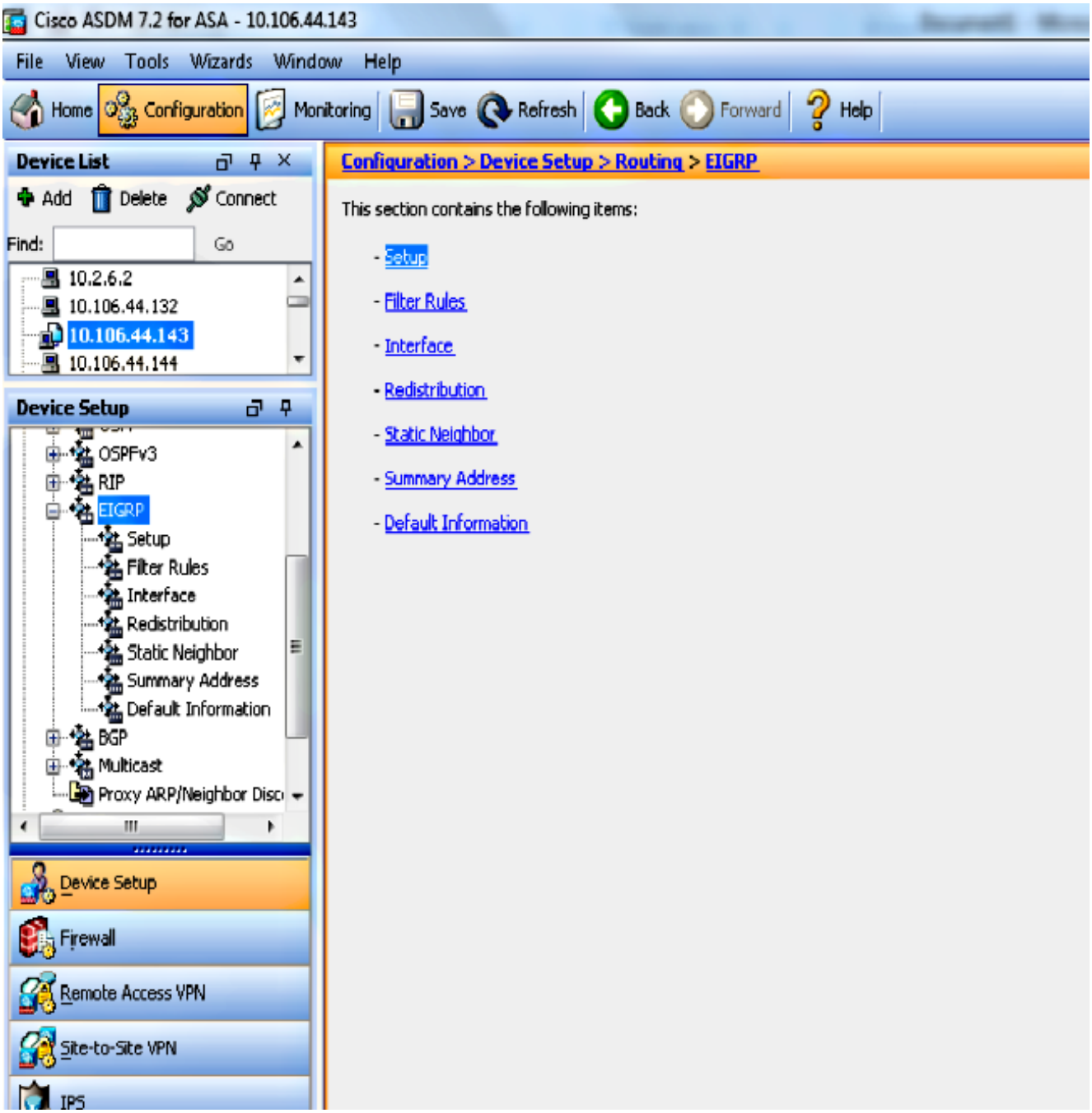
ASDM 컨피그레이션

ASDM은 보안 어플라이언스에서 소프트웨어를 구성하고 모니터링하는 데 사용되는 브라우저 기반 애플리케이션입니다. ASDM은 보안 어플라이언스에서 로드되고 디바이스를 구성, 모니터링 및 관리하는 데 사용됩니다. 또한 ASDM Launcher를 사용하여 Java 애플릿보다 빠르게 ASDM 애플리케이션을 시작할 수 있습니다. 이 섹션에서는 ASDM을 사용하여 이 문서에 설명된 기능을 구성하기 위해 필요한 정보에 대해 설명합니다.

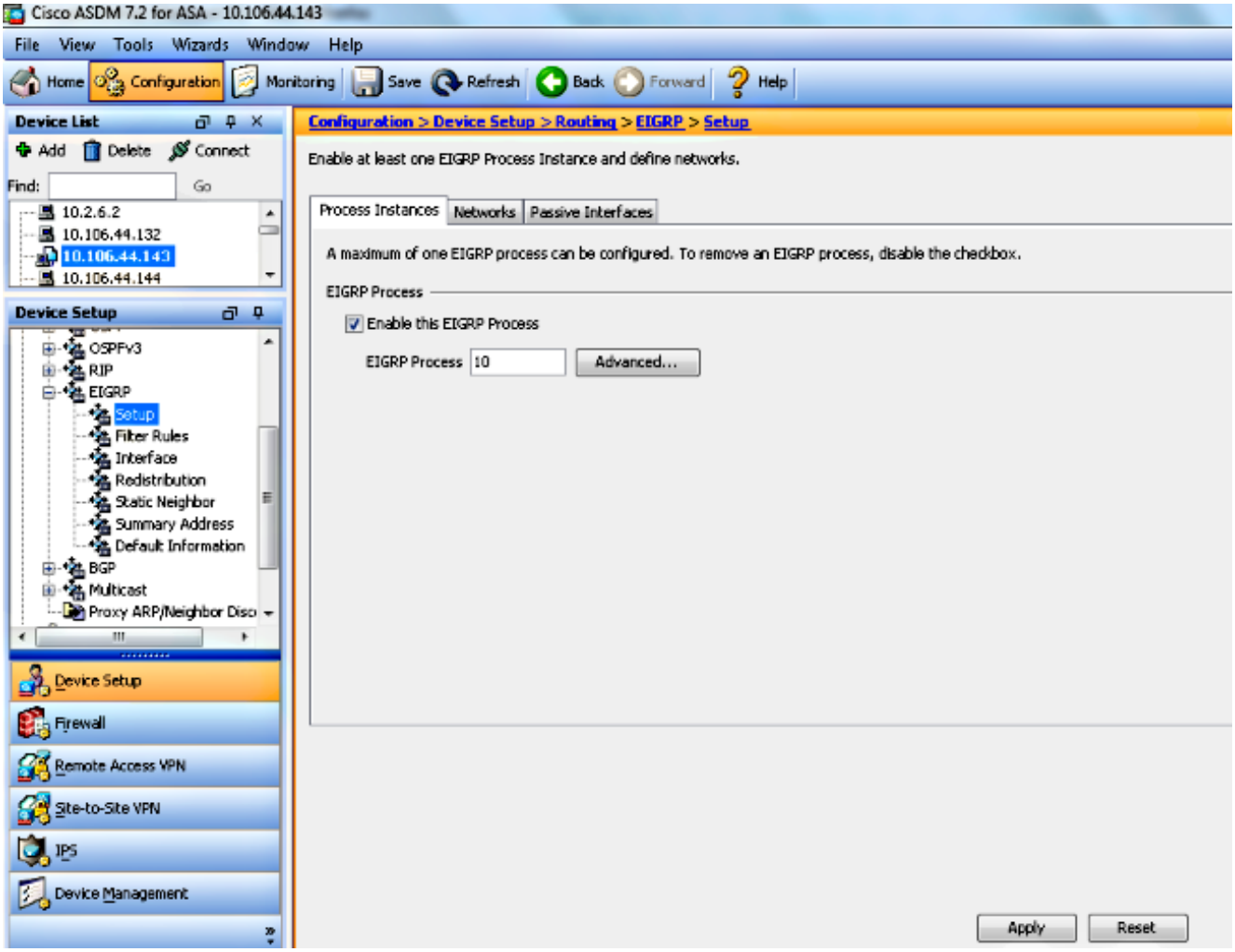
Cisco ASA에서 EIGRP를 구성하려면 다음 단계를 완료합니다.

1. ASDM을 사용하여 Cisco ASA에 로그인합니다.

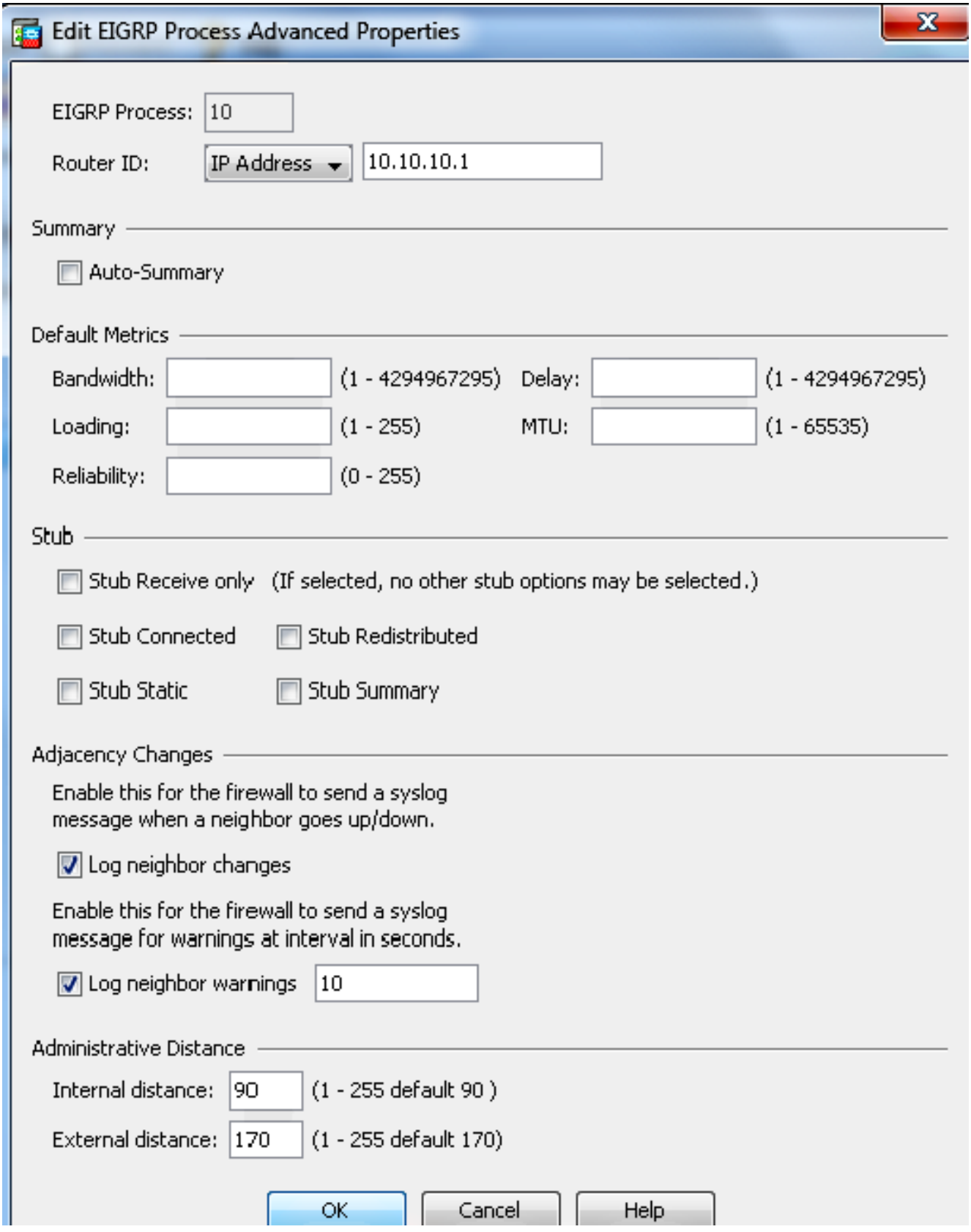
2. 이 스크린샷과 같이 ASDM 인터페이스의 **Configuration > Device Setup > Routing > EIGRP** 영역으로 이동합니다.



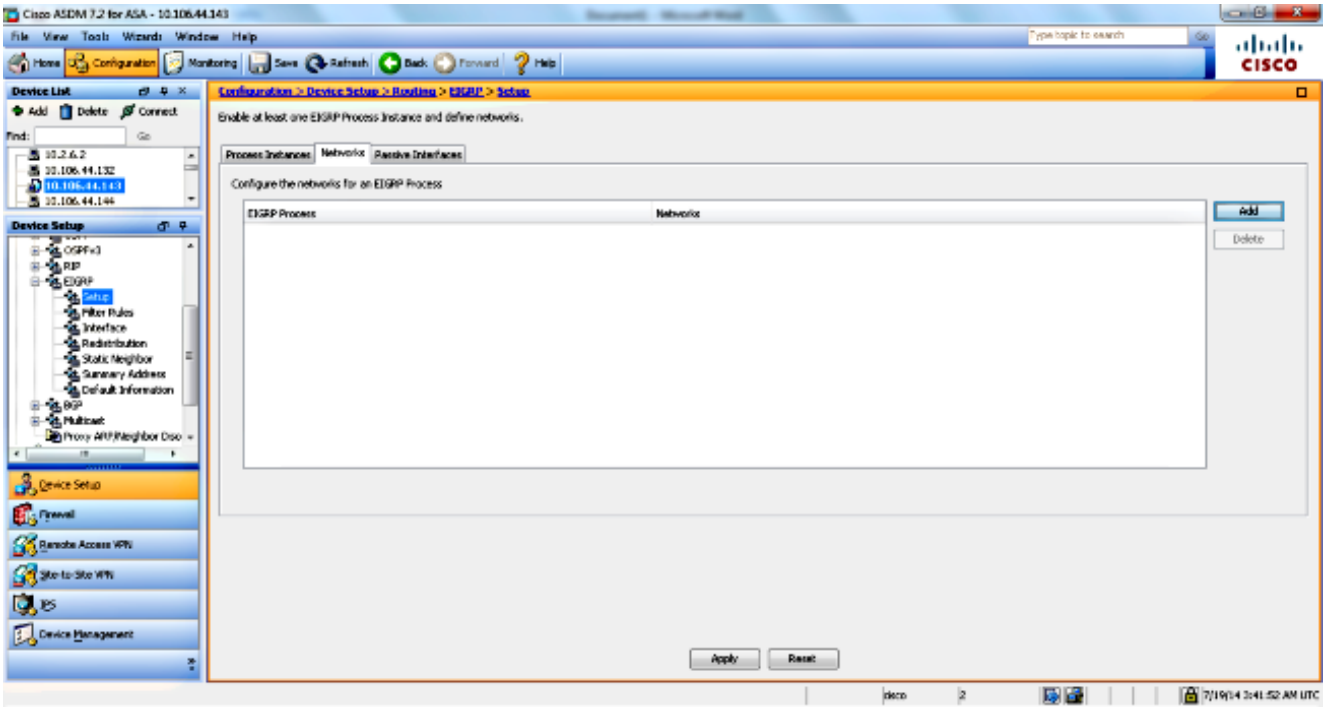
3. 이 스크린샷과 같이 **Setup > Process Instances** 탭에서 EIGRP 라우팅 프로세스를 활성화합니다. 이 예에서 EIGRP 프로세스는 **10입니다**.



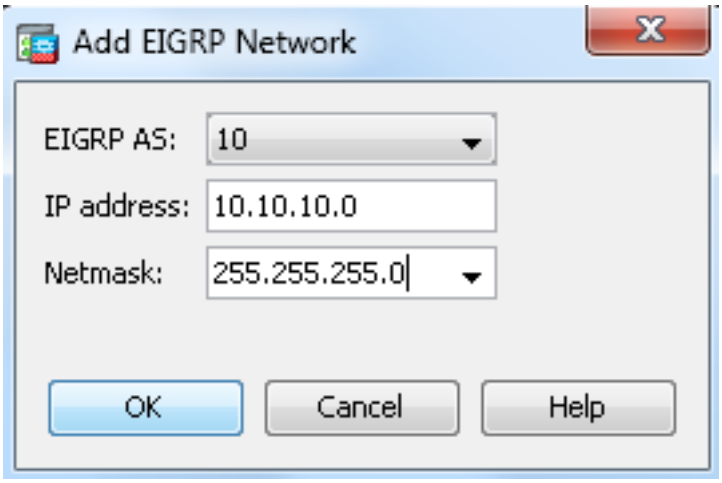
4. 선택적 고급 EIGRP 라우팅 프로세스 매개변수를 구성할 수 있습니다. Setup(**설정**) **> Process Instances(프로세스 인스턴스**) 탭에서 Advanced(**고급)를** 클릭합니다. EIGRP 라우팅 프로세스를 stub 라우팅 프로세스로 구성하고, 자동 경로 요약을 비활성화하고, 재배포된 경로에 대한 기본 메트릭을 정의하고, 내부 및 외부 EIGRP 경로에 대한 관리 거리를 변경하고, 고정 라우터 ID를 구성하고, 인접성 변경 로깅의 활성화 또는 비활성화할 수 있습니다. 이 예에서 EIGRP 라우터 ID는 내부 인터페이스의 IP 주소(10.10.10.1)으로 정적으로 구성됩니다. 또한 자동 **요약**이 비활성화됩니다. 다른 모든 옵션은 기본값으로 구성됩니다.



5. 이전 단계를 완료한 후 Setup(설정) > Networks(네트워크) 탭에서 EIGRP 라우팅에 참여하는 네트워크 및 인터페이스를 정의합니다. 이 스크린샷과 같이 Add를 클릭합니다.



6. 이 화면이 나타납니다. 이 예에서는 EIGRP가 내부 인터페이스에서만 활성화되기 때문에 내부 네트워크(10.10.10.0/24)을 추가하는 유일한 네트워크입니다.



정의된 네트워크에 속하는 IP 주소를 가진 인터페이스만 EIGRP 라우팅 프로세스에 참여합니다. EIGRP 라우팅에 참여하지 않으려는 인터페이스가 있지만 광고하려는 네트워크에 연결된 경우 인터페이스가 연결된 네트워크를 포함하는 Setup **> Networks** 탭에서 네트워크 항목을 구성한 다음 해당 인터페이스를 패시브 인터페이스로 구성하여 인터페이스가 EIGRP 업데이트를 보내거나 받을 수 없도록 구성합니다.

참고: 패시브로 구성된 인터페이스는 EIGRP 업데이트를 보내거나 받지 않습니다.

7. 선택적으로 Filter Rules 창에서 경로 필터를 정의할 수 있습니다. 경로 필터링은 EIGRP 업데이트에서 보내거나 받을 수 있는 경로에 대한 더 많은 제어를 제공합니다.

8. 선택적으로 경로 재배포를 구성할 수 있습니다. Cisco ASA는 RIP(Routing Information Protocol) 및 OSPF(Open Shortest Path First)에서 검색된 경로를 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. 고정 경로 및 연결된 경로를 EIGRP 라우팅 프로세스로 재배포할 수도 있습니다. 고정 경로 또는 연결된 경로가 **Setup > Networks** 탭에 구성된 네트워크 범위에 속

할 경우 재배포할 필요가 없습니다. Redistribution(재배포) 창에서 경로 재배포를 정의합니다.

9. EIGRP Hello 패킷은 멀티캐스트 패킷으로 전송됩니다. EIGRP 인접 디바이스가 비 브로드캐스트 네트워크 전체에 있는 경우 해당 인접 디바이스를 수동으로 정의해야 합니다. EIGRP 인접 디바이스를 수동으로 정의하면 Hello 패킷이 유니캐스트 메시지로 해당 인접 디바이스로 전송됩니다. 고정 EIGRP 인접 디바이스를 정의하려면 Static **Neighbor** 창으로 이동합니다.

10. 기본적으로 기본 경로는 전송 및 수락됩니다. 기본 경로 정보의 송수신을 제한하거나 비활성화하려면 Configuration(구성) **> Device Setup(디바이스 설정) > Routing(라우팅) > EIGRP > Default Information(기본 정보)** 창을 엽니다. Default Information(기본 정보) 창에는 EIGRP 업데이트의 기본 경로 정보 송수신을 제어하는 규칙 테이블이 표시됩니다.

    참고: 각 EIGRP 라우팅 프로세스에 대해 "*in*" 및 "*out*" 규칙을 하나로 가질 수 있습니다. (현재 하나의 프로세스만 지원됩니다.)

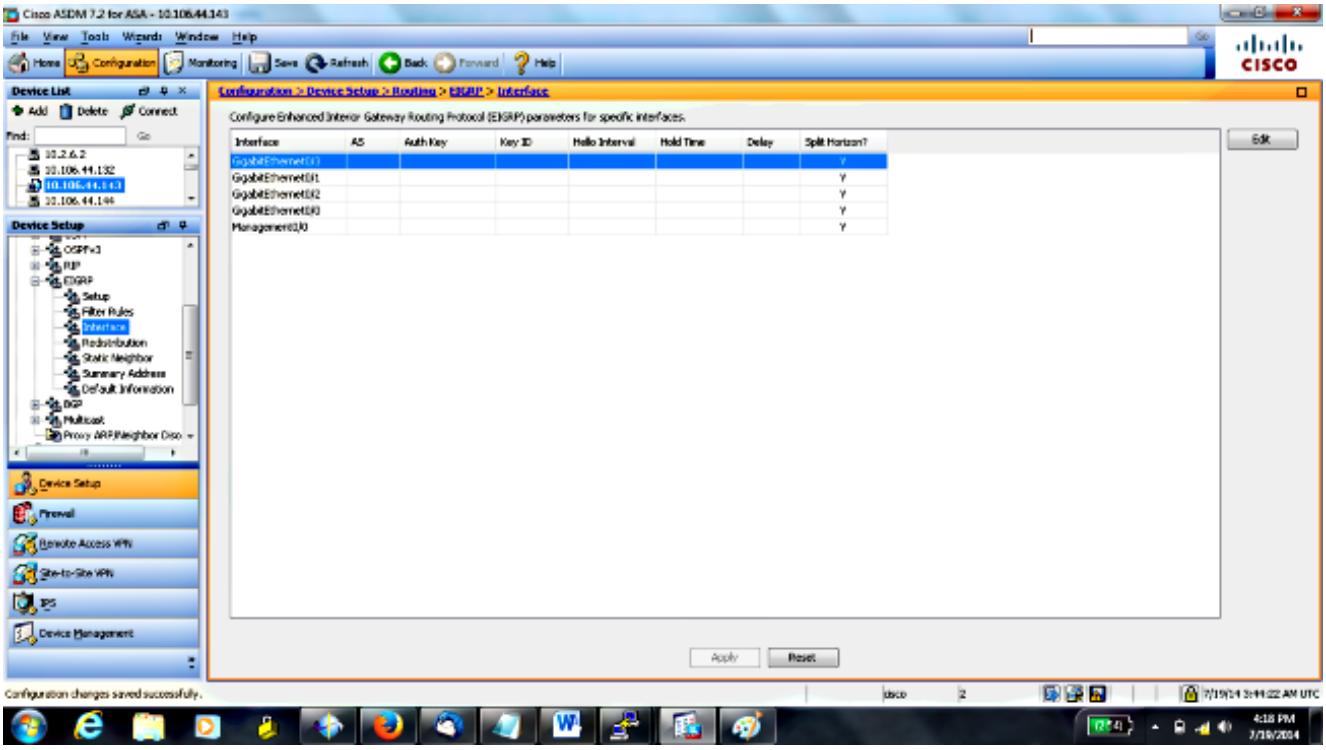
EIGRP 인증 구성

Cisco ASA는 EIGRP 라우팅 프로토콜에서 라우팅 업데이트의 MD5 인증을 지원합니다. 각 EIGRP 패킷의 MD5 키 다이제스트는 승인되지 않은 소스에서 승인되지 않은 또는 잘못된 라우팅 메시지를 유입하는 것을 방지합니다. EIGRP 메시지에 인증을 추가하면 라우터와 Cisco ASA가 동일한 사전 공유 키로 구성된 다른 라우팅 디바이스의 라우팅 메시지만 수락할 수 있습니다. 이 인증을 구성하지 않으면 다른 라우팅 디바이스가 네트워크에 서로 다르거나 반대 경로 정보를 제공하는 경우 라우터 또는 Cisco ASA의 라우팅 테이블이 손상될 수 있으며 서비스 거부 공격이 발생할 수 있습니다. 라우팅 디바이스(ASA 포함) 간에 전송되는 EIGRP 메시지에 인증을 추가하면 라우팅 토폴로지에 EIGRP 라우터가 무단으로 추가되는 것을 방지합니다.

EIGRP 경로 인증은 인터페이스별로 구성됩니다. EIGRP 메시지 인증을 위해 구성된 인터페이스의 모든 EIGRP 네이버는 인접성을 위해 동일한 인증 모드 및 키로 구성해야 합니다.

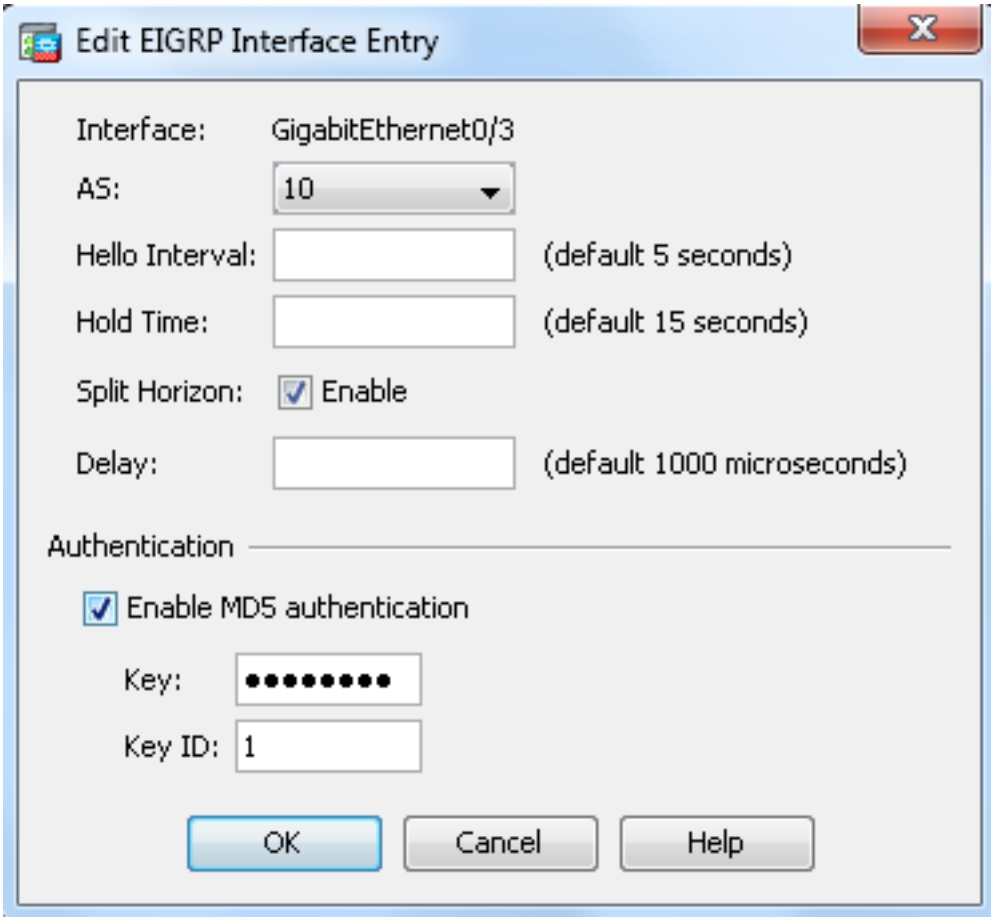
Cisco ASA에서 EIGRP MD5 인증을 활성화하려면 다음 단계를 완료합니다.

1. ASDM에서 표시된 대로 **Configuration > Device Setup > Routing > EIGRP > Interface로** 이동합니다.



2. 이 경우 EIGRP는 내부 인터페이스(GigabitEthernet 0/1)에서 활성화됩니다. GigabitEthernet **0/1** 인터페이스를 선택하고 Edit를 **클릭합니다**.

3. Authentication(인증)에서 Enable **MD5 authentication(MD5 인증 활성화)을** 선택합니다. 인증 매개변수에 대한 추가 정보를 여기에 추가합니다. 이 경우 사전 공유 키는 **cisco123**이고 키 ID는 **1입니다**.



EIGRP 경로 필터링

EIGRP를 사용하면 전송 및 수신된 라우팅 업데이트를 제어할 수 있습니다. 이 예에서는 R1 뒤에 있는 네트워크 접두사 192.168.10.0/24에 대해 ASA에서 라우팅 업데이트를 차단합니다. 경로 필터링의 경우 **STANDARD** ACL만 사용할 수 **있습니다**.

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

다음을 확인합니다.

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

구성

Cisco ASA CLI 컨피그레이션

Cisco ASA CLI 컨피그레이션입니다.

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
nameif management
security-level 99
```

```
ip address 10.10.20.1 255.255.255.0 management-only
!
!

!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Cisco IOS 라우터(R1) CLI 컨피그레이션

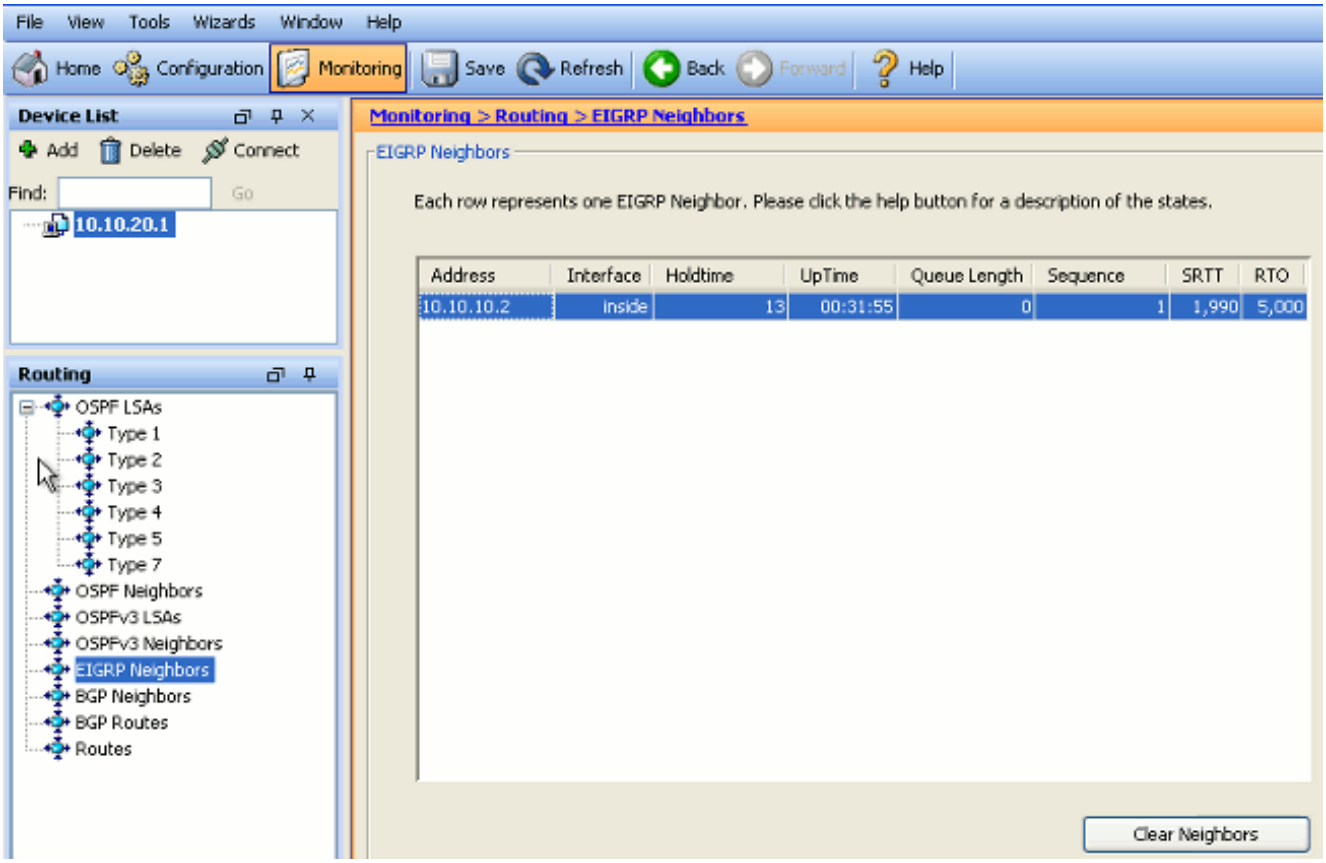
R1(내부 라우터)의 CLI 컨피그레이션입니다.

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
paramenters.


interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
!
!

! EIGRP Configuration

router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.20.20.0 0.0.0.255
network 172.18.124.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

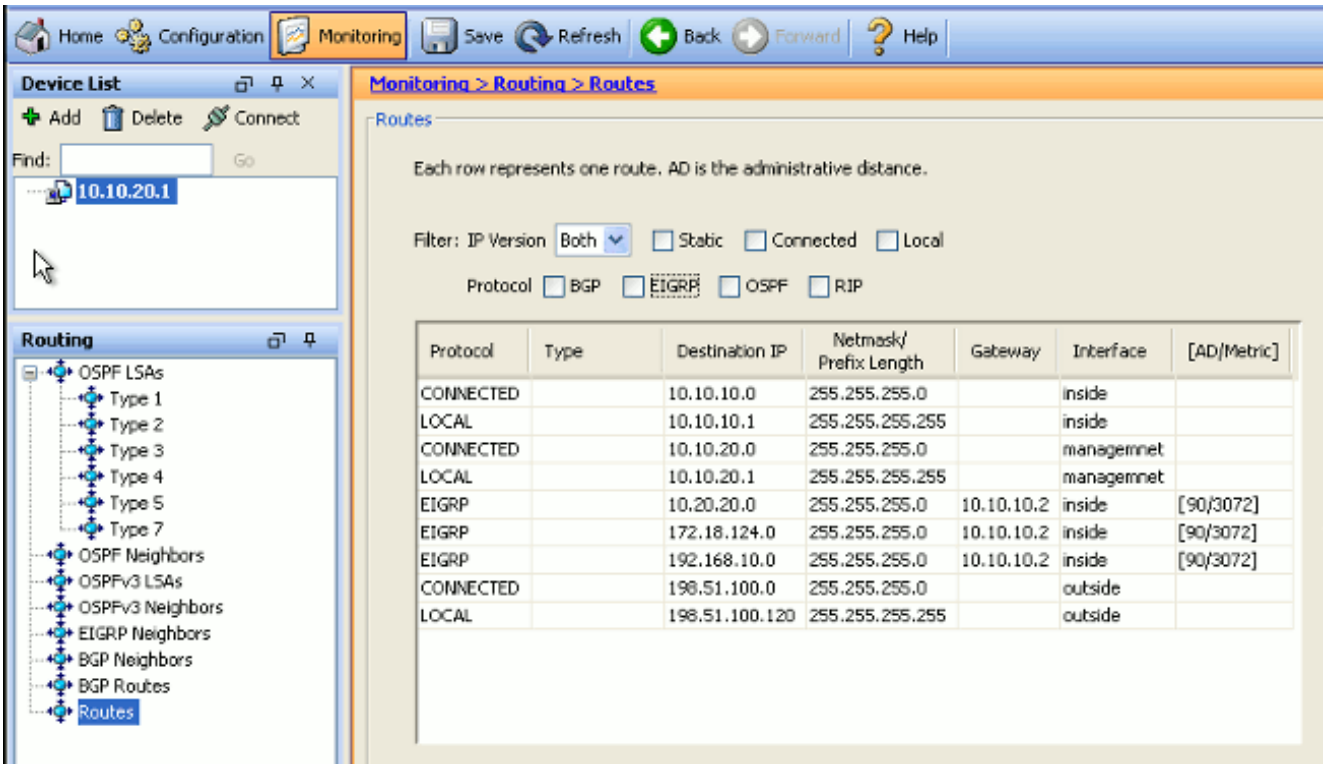
다음을 확인합니다.

구성을 확인하려면 다음 단계를 완료하십시오.

1. ASDM에서 각 EIGRP 네이버를 보려면 **Monitoring > Routing > EIGRP Neighbor**로 이동할 수 있습니다. 이 스크린샷은 내부 라우터(R1)를 활성 인접 디바이스로 보여줍니다. 또한 이 인접 디바이스가 상주하는 인터페이스, 대기 시간 및 인접 디바이스 관계가 작동(UpTime)된 기간도 볼 수 있습니다.



2. 또한 Monitoring(모니터링) > Routing(라우팅) **> Routes(경로)**로 이동하면 라우팅 테이블을 확인할 수 있습니다. 이 스크린샷에서는 **192.168.10.0/24, 172.18.124.0/24** 및 **10.20.20.0/24** 네트워크가 R1(**10.10.10.2**)을 통해 학습됨을 볼 수 있습니다.



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 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

ASA 버전 9.2.1 이상에서는 EIGRP 경로만 표시하려면 **show route eigrp** 명령을 사용할 수 있습니다.

```
ciscoasa(config)# show route eigrp

Codes: L - local, C - connected, S - static, 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
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, + - replicated route

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. 또한 **show eigrp topology** 명령을 사용하여 학습된 네트워크 및 EIGRP 토폴로지에 대한 정보를 얻을 수 있습니다.

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. show eigrp neighbors 명령은 활성 네이버 및 연락처 정보를 확인하는 데에도 유용합니다. 이 예에서는 1단계에서 ASDM에서 가져온 것과 동일한 정보를 보여 줍니다.

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

패킷 흐름

패킷 플로우입니다.

1. ASA는 링크를 통해 나타나며 모든 EIGRP 구성 인터페이스를 통해 mCast Hello 패킷을 전송합니다.

2. R1은 Hello 패킷을 수신하고 mCast Hello 패킷을 전송합니다.

13 5.572557	10.10.10.1	224.0.0.10	EIGRP	86 0x3b1a (15130)	Hello
14 5.573335	10.10.10.2	224.0.0.10	EIGRP	86 0x2321 (8993)	Hello
15 5.575212	10.10.10.1	10.10.10.2	EIGRP	54 0x0589 (1417)	Update
16 5.581712	10.10.10.2	10.10.10.1	EIGRP	54 0x19d9 (6617)	Update
17 5.585145	10.10.10.1	10.10.10.2	EIGRP	54 0x755e (30046)	Hello (Ack)
18 5.589373	10.10.10.1	10.10.10.2	EIGRP	96 0x1c93 (7315)	Update
19 5.591919	10.10.10.2	10.10.10.1	EIGRP	54 0x6695 (26261)	Hello (Ack)
20 5.591950	10.10.10.2	10.10.10.1	EIGRP	180 0x7925 (31013)	Update
21 5.595200	10.10.10.1	10.10.10.2	EIGRP	96 0x62e8 (25320)	Update
22 5.601913	10.10.10.2	10.10.10.1	EIGRP	54 0x08a7 (2215)	Hello (Ack)
23 5.601944	10.10.10.2	10.10.10.1	EIGRP	96 0x31c5 (12741)	Update

3. ASA는 Hello 패킷을 수신하고 초기 비트 집합으로 업데이트 패킷을 전송합니다. 이는 초기화 프로세스임을 나타냅니다.

4. R1은 업데이트 패킷을 수신하고 초기 비트 집합으로 업데이트 패킷을 전송합니다. 이는 초기화 프로세스임을 나타냅니다.

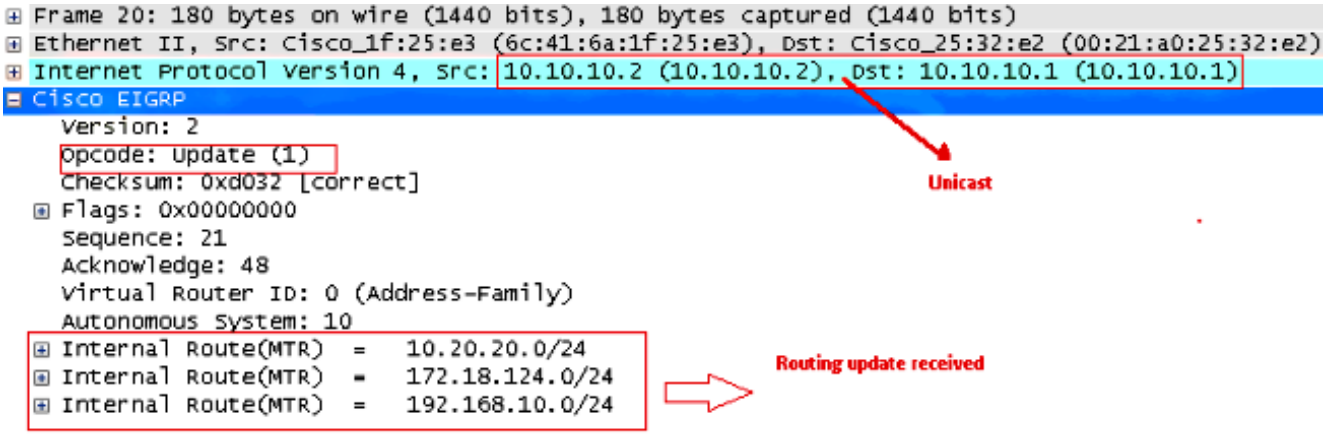
```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: Update (1)
    Checksum: 0xfdc4 [correct]
  ⊟ Flags: 0x00000001, Init
      .... .... .... .... .... .... .... ...1 = Init: Set
      .... .... .... .... .... .... .... ..0. = Conditional Receive: Not set
      .... .... .... .... .... .... .... .0.. = Restart: Not set
      .... .... .... .... .... .... .... 0... = End Of Table: Not set
    Sequence: 47
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
```

5. ASA와 R1이 모두 Hello를 교환하고 네이버 인접성이 설정되면 ASA와 R1 모두 ACK 패킷으로 응답합니다. 이는 업데이트 정보가 수신되었음을 나타냅니다.

6. ASA는 업데이트 패킷의 R1에 라우팅 정보를 전송합니다.

7. R1은 토폴로지 테이블에 패킷 업데이트 정보를 삽입합니다. 토폴로지 테이블에는 네이버가 광고한 모든 대상이 포함됩니다. 각 대상이 나열되고 목적지로 이동할 수 있는 모든 네이버 및 관련 메트릭이 나열됩니다.

8. 그런 다음 R1은 업데이트 패킷을 ASA에 전송합니다.



9. 업데이트 패킷을 수신하면 ASA는 R1에 ACK 패킷을 전송합니다. ASA와 R1이 서로 Update 패킷을 수신한 후 토폴로지 테이블에서 successor(best) 및 실행 가능한 successor(backup) 경로를 선택하고 후속 경로를 라우팅 테이블에 제공할 수 있습니다.

문제 해결

이 섹션에는 EIGRP 문제를 해결하는 데 유용한 debug 및 **show 명령**에 대한 정보가 포함되어 있습니다.

문제 해결 명령

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

> **참고: debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오. 디버그 정보를 DUAL(Diffusing Update Algorithm) 유한 상태 시스템에 표시하려면 특권 EXEC 모드에서 **debug eigrp fsm** 명령을 사용합니다. 이 명령을 사용하면 EIGRP 실행 가능한 후속 작업 관찰 및 라우팅 프로세스에 의해 경로 업데이트가 설치 및 삭제되는지 확인할 수 있습니다.

이것은 **debug** 명령의 성공적인 R1 피어링 출력입니다. 시스템에 성공적으로 설치된 각 경로를 확인할 수 있습니다.

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
```

```
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

debug eigrp neighbor 명령을 사용할 수도 있습니다. Cisco ASA가 R1과 함께 새 네이버 관계를 성공적으로 생성한 경우 이 **debug** 명령의 출력입니다.

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

Cisco ASA와 해당 피어 간의 자세한 EIGRP 메시지 교환 정보에 대해 디버그 EIGRP 패킷을 사용할 수도 있습니다. 이 예에서는 라우터(R1)에서 인증 키가 변경되었으며 디버그 출력에서는 문제가 인증 불일치임을 보여줍니다.

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

EIGRP Neighbor가 Syslogs ASA-5-336010으로 다운됨

EIGRP 배포 목록의 변경 사항이 있을 경우 ASA는 EIGRP 인접 디바이스를 삭제합니다. 이 Syslog 메시지가 표시됩니다.

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

이 컨피그레이션에서는 **새 acl 엔트리가** ACL에 **추가될** 때마다 Eigrp**-network-list** EIGRP 인접 디바이스가 재설정됩니다.

```
router eigrp 10
distribute-list Eigrp-network-list in
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static

access-list Eigrp-network-list standard permit any
```

인접 디바이스 관계가 인접 디바이스와 일치하는지 확인할 수 있습니다.

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

이제 **access-list Eigrp-network-list 표준 deny 172.18.24.0 255.255.255.0을** 추가할 수 있습니다.

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

이러한 로그는 debug eigrp fsm에서 볼 수 **있습니다**.

```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

이는 8.4 및 8.6~9.1의 모든 새 ASA 버전에서 예상되는 동작입니다. 12.4~15.1 코드 트레인을 실행하는 라우터에서도 이러한 동작이 관찰되었습니다. 그러나 ACL을 변경해도 EIGRP 인접성이 재설정되지 않으므로 ASA 버전 8.2 및 이전 ASA 소프트웨어 버전에서는 이러한 동작이 관찰되지 않습니다.

EIGRP는 인접 디바이스가 처음 나타날 때 전체 토폴로지 테이블을 인접 디바이스로 전송한 다음 변경 사항만 전송하므로, EIGRP의 이벤트 중심 특성으로 배포 목록을 구성하면 인접 디바이스 관계의 전체 재설정 없이 변경 사항을 적용하기 어렵습니다. 라우터는 현재 배포 목록에 지정된 대로

변경 사항을 적용하려면 어떤 경로가 변경되었는지(즉, 전송/수락되지 않을 것인지) 확인하기 위해 네이버로 전송되거나 인접 디바이스에서 수신되는 모든 경로를 추적해야 합니다. 인접 디바이스 간의 인접성을 단순히 분리하고 재설정하는 것이 훨씬 쉽습니다.

인접성이 해제되고 다시 설정되면 특정 인접 디바이스 간에 학습된 모든 경로가 단순히 잊혀지고 인접 디바이스 간의 전체 동기화가 새로 수행되며 새로운 배포 목록이 적용됩니다.

Cisco IOS 라우터의 문제를 해결하기 위해 사용하는 대부분의 EIGRP 기술은 Cisco ASA에 적용할 수 있습니다. EIGRP의 문제를 해결하려면 주 트러블슈팅 흐름도를 사용합니다. **Main**으로 표시된 상자에서 시작합니다.