Firepower Threat Defense RIP

이 장에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 RIP(Routing Information Protocol)를 사용하여 FTD를 구성하는 방법을 설명합니다. 가상 라우팅을 사용하는 디바이스의 경우 RIP는 전역 가상 라우터에만 구성할 수 있으며 사용자 정의 가상 라우터에는 구성할 수 없습니다.

RIP 정보

RIP(Routing Information Protocol)는 일반적으로 모든 라우팅 프로토콜 중에서 가장 오래 지속되는 프로토콜 중 하나입니다. RIP에는 라우팅 업데이트 프로세스, RIP 라우팅 메트릭, 라우팅 안정성 및 라우팅 타이머의 네 가지 기본 구성 요소가 있습니다. RIP를 지원하는 디바이스는 정기적인 간격으로 네트워크 토폴로지가 변경될 때 라우팅 업데이트 메시지를 전송합니다. 이러한 RIP 패킷에는 디바이스가 도달할 수 있는 네트워크 정보 및 패킷이 대상 주소에 도달하기 위해 통과해야 하는 라우터 또는 게이트웨이의 수가 포함됩니다. RIP는 OSPF보다 많은 트래픽을 생성하지만 더욱 쉽게 구성할 수 있습니다.

RIP는 경로 선택 항목을 메트릭으로 사용하는 거리 벡터 프로토콜입니다. 인터페이스에서 RIP가 활성화되면 해당 인터페이스는 인접 디바이스와 RIP 브로드캐스트를 교환하여 경로를 동적으로 학습하고 알립니다.

Firepower Threat Defense 디바이스에서는 RIP 버전 1과 RIP 버전 2를 모두 지원합니다. RIP 버전 1은 라우팅 업데이트를 통해 서브넷 마스크를 전송하지 않습니다. RIP 버전 2는 라우팅 업데이트를 통해 서브넷 마스크를 전송하고 가변 길이 서브넷 마스크를 지원합니다. 또한 RIP 버전 2는 라우팅 업데이트가 교환될 때 네이버 인증을 지원합니다. 이 인증은 Firepower Threat Defense 디바이스가 신뢰할 수 있는 소스에서 믿을 수 있는 라우팅 정보를 수신하도록 보장합니다.

RIP는 초기 구성이 간단하고 토폴로지가 변경될 때 구성을 업데이트할 필요가 없기 때문에 정적 경로에 비해 이점이 있습니다. RIP의 단점은 정적 라우팅보다 네트워크 및 처리 오버헤드가 많다는 것입니다.

라우팅 업데이트 프로세스

RIP는 정기적인 간격으로 네트워크 토폴로지가 변경될 때 라우팅 업데이트 메시지를 전송합니다. 라우터가 항목의 변경 사항을 포함하는 라우팅 업데이트를 수신하면 라우팅 테이블을 업데이트하여 새 경로를 반영합니다. 경로의 메트릭 값은 1이 증가하고 발신자는 next hop으로 표시됩니다. RIP 라우터는 최상의 경로(메트릭 값이 가장 낮은 경로)만 대상에 유지합니다. 라우팅 테이블을 업데이트한 후 라우터는 즉시 라우팅 업데이트 전송을 시작하여 다른 네트워크 라우터에 변경 사항을 알립니다. 이러한 업데이트는 RIP 라우터가 전송하는 정기적으로 예약된 업데이트와 별개로 전송됩니다.

RIP 라우팅 메트릭

RIP는 단일 라우팅 메트릭(홉 수)을 사용하여 소스 및 대상 네트워크 간의 거리를 측정합니다. 소스에서 대상까지의 경로에 있는 각 홉에는 홉 수 값이 할당되며 이는 일반적으로 1입니다. 라우터가 새 대상 네트워크 항목 또는 변경된 대상 네트워크 항목을 포함하는 라우팅 업데이트를 수신하면 라우터는 업데이트에 표시된 메트릭 값에 1을 더하고 라우팅 테이블에 네트워크를 입력합니다. 발신자의 IP 주소는 next hop으로 사용됩니다.

RIP 안정성 기능

RIP는 소스에서 대상까지 경로에 허용되는 홉 수에 대한 제한을 구현하여 라우팅 루프가 무기한 지속되지 않도록 방지합니다. 경로의 최대 홉 수는 15입니다. 라우터가 새 항목 또는 변경된 항목을 포함하는 라우팅 업데이트를 수신하고 메트릭 값을 1만큼 높여 메트릭이 무한대(16)가 되면 네트워크 대상이 도달할 수 없는 것으로 간주됩니다. 이 안정성 기능의 단점은 RIP 네트워크의 최대 직경을 16홉 미만으로 제한한다는 것입니다.

RIP에는 많은 라우팅 프로토콜에 공통적인 여러 다른 안정성 기능이 포함되어 있습니다. 이러한 기능은 네트워크 토폴로지의 급격한 변화에도 불구하고 안정성을 제공하도록 설계되었습니다. 예를 들어 RIP는 올바르지 않은 라우팅 정보가 전파되지 않도록 수평 분할(split horizon) 및 보류 메커니즘을 구현합니다.

RIP 타이머

RIP는 수많은 타이머를 사용하여 성능을 규제합니다. 여기에는 routing-update 타이머, route-timeout 타이머 및 route-flush 타이머가 포함됩니다. routing-update 타이머는 주기적인 라우팅 업데이트 간격을 측정합니다. 일반적으로 타이머가 재설정될 때마다 임의의 시간이 추가되어 30초로 설정됩니다. 이는 모든 라우터가 동시에 네이버 라우터를 업데이트하려고 시도할 때 발생할 수 있는 혼잡을 방지하는 데 도움이 됩니다. 각 라우팅 테이블 항목에는 route-timeout 타이머가 있습니다. route-timeout 타이머가 만료되면 경로가 무효로 표시되지만 route-flush 타이머가 만료될 때까지 테이블에 유지됩니다.

RIP에 대한 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

RIP 가이드라인

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

다음 정보는 RIP 버전 2에만 적용됩니다.

- 네이버 인증을 사용하는 경우 인터페이스에 RIP 버전 2 업데이트를 제공하는 모든 네이버 디바이스에서 인증 키와 키 ID가 동일해야 합니다.
- RIP 버전 2를 통해 Firepower Threat Defense 디바이스는 멀티캐스트 주소 224.0.0.9를 사용하여 기본 경로 업데이트를 전송하고 수신합니다. 패시브 모드에서는 해당 주소에서 경로 업데이트를 수신합니다.
- RIP 버전 2가 인터페이스에 구성되면 멀티캐스트 주소 224.0.0.9가 해당 인터페이스에 등록됩니다. RIP 버전 2 구성이 인터페이스에서 제거되면 해당 멀티캐스트 주소는 등록 취소됩니다.

제한 사항

- Firepower Threat Defense 디바이스는 인터페이스 간에 RIP 업데이트를 전달할 수 없습니다.
- RIP 버전 1은 가변 길이 서브넷 마스크를 지원하지 않습니다.
- RIP의 최대 홉 수는 15입니다. 홉 수가 15보다 큰 경로는 도달할 수 없는 것으로 간주됩니다.
- 통합 RIP는 다른 라우팅 프로토콜에 비해 상대적으로 느립니다.

• Firepower Threat Defense 디바이스에서 단일 RIP 프로세스만 활성화할 수 있습니다.

RIP 설정

RIP는 경로 선택 항목을 메트릭으로 사용하는 거리 벡터 프로토콜입니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 FTD 디바이스를 수정합니다.

단계 **2** **Routing(**라우팅**)**을 선택합니다.

단계 **3** 목차에서 **RIP**를 선택합니다.

단계 **4** RIP 설정을 구성하려면 **Enable RIP(RIP** 활성화**)** 확인란을 선택합니다.

단계 **5** **RIP Version(RIP** 버전**)** 드롭다운 목록에서 RIP 업데이트를 송수신하기 위한 RIP 버전을 선택합니다.

단계 **6** (선택 사항) 지정한 경로 맵에 따라 **Generate Default Route(**기본 경로 생성**)** 확인란을 선택하여 배포할 기본 경로를 생성합니다.

a) **Route Map(**경로 맵**)** 필드에서 기본 경로 생성에 사용할 경로 맵 이름을 지정합니다.
기본 경로 0.0.0.0/0은 **Route Map(**경로 맵**)** 필드에 지정된 경로 맵이 있을 때 특정 인터페이스를 통해 배포용으로 생성됩니다.

단계 **7** 송수신하기 위해 선택한 RIP 버전이 버전 2인 경우 **Enable Auto Summary(**자동 요약 활성화**)** 옵션을 사용할 수 있습니다. **Enable Auto Summary(**자동 요약 활성화**)** 확인란을 선택하는 경우 자동 경로 요약이 활성화되어 있습니다. 연결되지 않은 서브넷 간의 라우팅을 수행해야 하는 경우 자동 요약을 비활성화합니다. 자동 요약이 비활성화되면 서브넷이 알려집니다.

참고 RIP 버전 1은 항상 자동 요약 기능을 사용하므로 비활성화할 수 없습니다.

단계 **8** **Networks(**네트워크**)**를 클릭합니다. RIP 라우팅에 대 한 하나 이상의 네트워크를 정의 합니다. IP 주소를 입력하거나 원하는 네트워크/호스트 개체를 입력하거나 선택합니다. 보안 어플라이언스 구성에 추가할 수 있는 네트워크 수에는 제한이 없습니다. 이 명령으로 정의된 네트워크에 속하는 모든 인터페이스는 RIP 라우팅 프로세스에 참여합니다. RIP 라우팅 업데이트는 지정된 네트워크의 인터페이스를 통해서만 송수신됩니다. 또한, 인터페이스의 네트워크를 지정하지 않으면 RIP 업데이트가 인터페이스로 알려지지 않습니다.

참고 RIP는 IPv4 개체만 지원합니다.

단계 **9** (선택 사항) **Passive Interfaces(**패시브 인터페이스**)**를 클릭합니다. 어플라이언스에서 패시브 인터페이스를 지정하고 활성 인터페이스를 확장하려면 이 옵션을 사용합니다. 해당 디바이스는 패시브 인터페이스에서 RIP 라우팅 브로드캐스트를 수신하고 해당 정보를 사용하여 라우팅 테이블을 채우지만 패시브 인터페이스에서 라우팅 업데이트를 브로드캐스트 처리하지는 않습니다. 패시브로 지정되지 않은 인터페이스는 업데이트를 송수신합니다.

단계 **10** **Redistribution(**재배포**)**을 클릭하여 재배포 경로를 관리합니다. 이는 다른 라우팅 프로세스에서 RIP 라우팅 프로세스로 재배포되는 경로입니다.

a) 재분배 경로를 지정하려면 **Add(**추가**)**를 클릭합니다.
b) **Protocol(**프로토콜**)** 드롭다운 목록에서 RIP 라우팅 프로세스로 재배포할 라우팅 프로토콜을 선택합니다.

참고 OSPF 프로토콜에 대한 프로세스 ID를 지정합니다. 마찬가지로 BGP에 대한 AS 경로를 지정합니다. **Protocol(**프로토콜**)** 드롭다운 목록에서 Connected(연결됨) 옵션을 선택하면 직접 연결된 네트워크를 RIP 라우팅 프로세스로 재배포할 수 있습니다.

c) (선택 사항) OSPF 경로를 RIP 라우팅 프로세스로 재배포하는 경우 **Match(**일치**)** 드롭다운 목록에서 재배포할 OSPF 경로의 특정 유형을 선택할 수 있습니다. 다음과 같이 여러 유형을 선택하려면 ctrl 키를 클릭합니다.

- Internal – AS(Autonomous System) 내부의 경로가 재배포됩니다.
- External 1 - AS 외부의 유형 1 경로가 재배포됩니다.
- External 2 - AS 외부의 유형 2 경로가 재배포됩니다.
- NSSA External 1 - NSSA(not-so-stubby area) 외부의 유형 1 경로가 재배포됩니다.
- NSSA External 2 - NSSA 외부의 유형 2 경로가 재배포됩니다.

참고 기본값은 Internal, External 1 및 External 2와 일치합니다.

d) **Metric(**메트릭**)** 드롭다운 목록에서 재배포된 경로에 적용할 RIP 메트릭 유형을 선택합니다. 두 가지 선택 사항은 다음과 같습니다.

- Transparent(투명) – 현재 경로 메트릭을 사용합니다.
- Specified Value(지정된 값) - 특정 메트릭 값을 지정합니다. **Metric Value(**메트릭 값**)** 필드에 0~16 사이의 특정 값을 입력합니다.
- None(없음) - 메트릭이 지정되지 않습니다. 재배포된 경로에 적용하려면 메트릭 값을 사용하지 마십시오.

e) (선택 사항) 경로가 RIP 라우팅 프로세스로 재배포되기 전에 **Route Map(**경로 맵**)** 필드에 충족되어야 하는 경로 맵의 이름을 입력합니다. 경로는 IP 주소가 경로 맵 주소 목록의 allow 문과 일치하는 경우에만 재배포됩니다.
f) **OK(**확인**)**를 클릭합니다.

단계 **11** (선택 사항) RIP 정책에 대한 필터를 관리하려면 **Filtering(**필터링**)**을 클릭합니다. 이 섹션에서 필터는 인터페이스를 통한 라우팅 업데이트 방지, 라우팅 업데이트의 경로 알림 제어, 라우팅 업데이트 처리 및 라우팅 업데이트 소스 필터링에 사용됩니다.

a) **Add(**추가**)**를 클릭하여 RIP 필터를 추가합니다.
b) **Traffic Direction(**트래픽 방향**)** 필드에서 필터링할 트래픽 유형을 선택합니다(인바운드 또는 아웃바운드).

참고 트래픽 방향이 인바운드인 경우 인터페이스 필터만 정의할 수 있습니다.

c) **Filter On(**필터 켜기**)** 필드에서 해당 라디오 버튼을 선택하여 필터가 Interface(인터페이스) 또는 Route(경로) 기반인지 여부를 지정합니다. Interface(인터페이스)를 선택하는 경우 라우팅 업데이트를 필터링할 인터페이스의 이름을 입력하거나 선택합니다. Route(경로)를 선택하는 경우 경로 유형을 선택합니다.

- Static(정적) - 정적 경로만 필터링됩니다.
- Connected(연결됨) - 연결된 경로만 필터링됩니다.
- OSPF - 지정된 OSPF 프로세스에서 검색한 OSPFv2 경로만 필터링됩니다. 필터링할 OSPF 프로세스의 프로세스 ID를 입력합니다.
- BGP - 지정된 BGP 프로세스에서 검색한 BGPv4 경로만 필터링됩니다. 필터링할 BGP 프로세스의 AS 경로를 입력합니다.

d) **Access List(**액세스 목록**)** 필드에서 RIP 경로 알림에서 허용 또는 제거할 네트워크를 정의하는 하나 이상의 ACL(액세스 제어 목록)의 이름을 입력하거나 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **12** (선택 사항) **Broadcast(**브로드캐스트**)**를 클릭하여 인터페이스 구성을 추가하거나 편집합니다. Broadcast(브로드캐스트)를 사용하여 인터페이스별로 전송 또는 수신할 전역 RIP 버전을 재정의할 수 있습니다. 인증을 구현하여 유효한 RIP 업데이트를 확인하려는 경우 인터페이스당 인증 파라미터를 정의할 수도 있습니다.

a) 인터페이스 구성을 추가하려면 **Add(**추가**)**를 클릭합니다.

b) **Interface(**인터페이스**)** 필드에서 이 어플라이언스에 정의된 인터페이스를 입력하거나 선택합니다.

c) Send(전송) 옵션에서 해당 상자를 선택하여 RIP **Version 1(**버전 **1)**, **Version 2(**버전 **2)**, 또는 둘 다를 사용하여 업데이트를 전송하도록 지정합니다. 이러한 옵션을 사용하면 지정된 인터페이스에 대해 지정된 전역 Send(전송) 버전을 재정의할 수 있습니다.

d) Receive(수신) 옵션에서 해당 상자를 선택하여 RIP **Version 1(**버전 **1)**, **Version 2(**버전 **2)**, 또는 둘 다를 사용하여 업데이트를 수락하도록 지정합니다. 이러한 옵션을 사용하면 지정된 인터페이스에 대해 지정된 전역 Receive(수신) 버전을 재정의할 수 있습니다.

e) RIP 브로드캐스트에 대해 이 인터페이스에서 사용되는 **Authentication(**인증**)**을 선택합니다.

- None(없음) - 인증 없음
- MD5 - MD5 사용
- Clear Text(일반 텍스트) - 사용할 일반 텍스트 인증

MD5 또는 Clear Text(일반 텍스트)를 선택하는 경우 다음 인증 파라미터도 제공해야 합니다.

- Key ID(키 ID) - 인증 키의 ID입니다. 유효한 값은 0 ~ 255입니다.
- Key(키) - 선택한 인증 방법에서 사용하는 키입니다. 최대 16자를 포함할 수 있습니다.
- Confirm(확인) - 확인을 위해 인증 키를 다시 입력합니다.

f) **OK(**확인**)**를 클릭합니다.