라우팅 기본 사항 및 정적 경로

시스템은 라우팅 테이블을 사용하여 시스템으로 들어오는 패킷용 이그레스 인터페이스를 결정합니다. 다음 주제에서는 라우팅의 기본 사항과 디바이스에서 정적 라우팅을 구성하는 방법을 설명합니다.

라우팅에 대한 모범 사례

네트워크에서 라우팅 프로세스를 설계하는 것은 복잡한 프로세스일 수 있습니다. 이 장에서는 위협 방어 디바이스가 기존 네트워크 내에서 작동하도록 구성하고, 네트워크에 이미 설정된 라우팅 프로세스에 참여하도록 구성하는 것으로 가정합니다.

그 대신 새 네트워크를 생성할 경우, 시간을 내어 라우팅 프로토콜에 대한 내용 및 네트워크에서 작동하는 효과적인 라우팅 계획을 설계하는 방법을 참조하십시오. 이 장에서는 프로토콜 선택에 대한 권장 사항을 다루지 않으며, 프로토콜이 작동하는 방식을 심층적으로 다루지 않습니다.

네트워크가 매우 소규모이고 ISP에만 연결하려는 경우, 정적 경로가 몇 개만 필요할 수 있으며 라우팅 프로토콜을 구현할 필요가 전혀 없을 수 있습니다.

그러나 많은 라우터가 포함된 대규모 네트워크를 설정할 경우에는 OSPF 같은 내부 라우팅에 대해 하나 이상의 라우팅 프로토콜을 구현해야 할 수 있습니다. 여기에는 BGP 같은 외부 라우팅에 대한 라우팅 프로토콜도 해당될 수 있습니다. 통신 사업자의 도움을 받아 귀사에 어떤 외부 라우팅이 필요한지 파악할 수 있습니다. 이러한 상황에서는 우선 위협 방어를 사용해 구성할 수 있는 라우팅 프로토콜을 파악한 다음, 네트워크를 계획하고, 계획에 따라 위협 방어 디바이스를 구성합니다.

라우팅 개요

다음 주제에서는 위협 방어 디바이스 내에서 라우팅이 동작하는 방식을 설명합니다. 라우팅은 소스에서 대상까지 네트워크에 걸친 정보의 이동입니다. 그 과정에서 적어도 하나의 중간 노드를 일반적

으로 만나게 됩니다. 라우팅에는 2가지 기본적인 작업이 포함되는데, 최적의 라우팅 경로를 결정하는 것과 네트워크를 통한 패킷 전송입니다.

지원되는 라우팅 프로토콜

다음 표에서는 device manager을 사용하여 threat defense 디바이스에서 구성할 수 있는 라우팅 프로토콜과 기술, 그리고 컨피그레이션을 완료하는 데 사용해야 하는 방법에 대해 설명합니다.

표 *1:* 지원되는 라우팅 프로토콜

라우팅 기능	컨피그레이션 방법	참고
BGP	Smart CLI	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 BGP 스마트 CLI 개체를 구성합니다. **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체를 사용하여 BGP에서 사용되는 개체(예: 경로 맵)를 구성합니다.
BFD(Bi-directional Forwarding Detection)	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 BFD를 구성합니다. BFD는 BGP에서만 지원됩니다.
EIGRP	Smart CLI	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 EIGRP 스마트 CLI 개체를 구성합니다. **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체를 사용하여 EIGRP에서 사용되는 개체(예: 경로 맵)를 구성합니다.
IS-IS	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 IS-IS를 구성합니다.
멀티캐스트 라우팅	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 멀티캐스트 라우팅을 구성합니다.
OSPFv2	Smart CLI	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 OSPFv2 스마트 CLI 개체를 구성합니다. **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 스마트 CLI 개체를 사용하여 OSPFv2에서 사용되는 개체(예: 경로 맵)를 구성합니다.
OSPFv3	—	OSPFv3 프록시 설정은 지원되지 않습니다.
PBR(Policy-Based Routing)	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 PBR(Policy-Based Routing)을 구성합니다.

라우팅 기능	컨피그레이션 방법	참고
RIP	FlexConfig	**Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)** 페이지에서 FlexConfig 개체를 사용하여 RIP를 구성합니다.
정적 경로	Device Manager	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 전역으로 또는 가상 라우터당 정적 경로를 구성합니다.
가상 라우터, VRF	Device Manager	**Device(**디바이스**)** > **Routing(**라우팅**)** 페이지에서 가상 라우터를 구성합니다.

경로 유형

경로에는 정적 유형과 동적 유형이 있습니다.

정적 경로는 명시적으로 정의하는 것입니다. 이 경로는 안정적이고 일반적으로 우선 순위가 높으며, 경로 대상으로 가는 트래픽이 항상 올바른 인터페이스로 전송되게 하는 데 사용합니다. 예를 들어 기본 정적 경로를 생성하여 기타 경로(IPv4의 경우 0.0.0.0/0, IPv6의 경우 ::/0)에서 아직 처리하지 않는 모든 트래픽을 처리할 수 있습니다. 또 다른 예로 항상 사용하려는 내부 syslog 서버로 가는 정적 경로를 들 수 있습니다.

동적 경로는 OSPF, BGP, EIGRP, IS-IS, RIP 등 라우팅 프로토콜 작업을 통해 학습된 것입니다. 경로를 직접 정의하지 않습니다. 그 대신에 라우팅 프로토콜을 컨피그레이션하면 시스템에서 인접 라우터와 통신하여 라우팅 업데이트를 전송하고 그 결과로 라우팅 업데이트를 수신합니다.

동적 라우팅 프로토콜에서는 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 따라 라우팅 테이블을 조정합니다. 네트워크 변경 사실을 알리는 메시지가 표시되면 시스템에서 경로를 다시 계산하여 새로운 라우팅 업데이트 메시지를 전송합니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

정적 라우팅은 간단하여 기본 라우팅에 알맞습니다. 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다. 하지만 직접 수정하지 않으면 정적 경로를 변경할 수 없기 때문에 네트워크에 변동이 발생한 경우, 이에 대응할 수 없습니다.

소형 네트워크가 없는 경우, 일반적으로 정적 경로를 하나 이상의 동적 라우팅 프로토콜에 결합할 수 있습니다. 하나 이상의 정적 경로를 명시적 경로와 일치하지 않는 모든 트래픽에 대한 기본 경로로 정의합니다.

참고 스마트 CLI를 사용하여 라우팅 프로토콜인 OSPF 및 BGP를 컨피그레이션할 수 있습니다. FlexConfig를 사용하여 ASA 소프트웨어에서 지원하는 다른 라우팅 프로토콜을 컨피그레이션합니다.

라우팅 테이블과 경로 선택

NAT 변환(xlates) 및 규칙에서 이그레스 인터페이스를 결정하지 않는 경우, 시스템에서는 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

라우팅 테이블의 경로에는 지정된 경로에 대한 상대적 우선순위를 제공하는 "관리 거리"라는 메트릭이 있습니다. 패킷이 둘 이상의 경로 항목과 일치하는 경우에는 거리가 가장 짧은 항목이 사용됩니다. 직접 연결된 네트워크(인터페이스에서 정의된 네트워크)는 거리가 0이므로 항상 기본적으로 사용됩니다. 고정 경로의 기본 거리는 1이지만 1~254 범위의 원하는 거리를 사용하여 고정 경로를 생성할 수 있습니다.

특정 대상을 식별하는 경로는 기본 경로(대상이 0.0.0.0/0 또는 ::/0인 경로)보다 먼저 적용됩니다.

라우팅 테이블을 채우는 방법

threat defense 라우팅 테이블은 정적으로 정의된 경로, 직접 연결된 경로, 그리고 동적 라우팅 프로토콜에서 검색한 경로로 채울 수 있습니다. threat defense 디바이스는 라우팅 테이블에 고정 경로와 연결 경로를 가지는 것 외에도 여러 라우팅 프로토콜을 실행할 수 있기 때문에 같은 경로가 하나 이상의 방법으로 다시 발견되거나 입력될 수 있습니다. 같은 목적지로의 두 경로를 라우팅 테이블에 넣으면 라우팅 테이블에 유지되는 항목은 다음과 같이 결정됩니다.

- 두 경로의 네트워크 접두사 길이(네트워크 마스크)가 다르면 두 경로 모두 고유한 것으로 간주되어 라우팅 테이블에 입력됩니다. 그런 다음 패킷 전달 로직에서 둘 중 어느 것을 사용할지 결정합니다.

  예를 들어 RIP 및 OSPF 프로세스에서 다음 경로를 검색한 경우

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  비록 OSPF 경로의 관리 영역이 더 낮지만, 접두사 길이(서브넷 마스크)가 다르기 때문에 두 경로 모두 라우팅 테이블에 설치됩니다. 이들은 다른 목적지로 간주되며 패킷 전달 로직에서 사용할 경로를 결정합니다.

- threat defense 디바이스가 RIP와 같이 단일 라우팅 프로토콜에서 같은 대상으로의 여러 경로를 학습하는 경우 메트릭이 더 나은 경로(라우팅 프로토콜이 결정)가 라우팅 테이블에 입력됩니다.

  메트릭은 특정 경로와 연결되는 값이며, 선호도가 가장 높은 것부터 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 목적지의 다중 경로가 메트릭 값이 같을 경우 이 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

- threat defense 디바이스가 두 개 이상이 라우팅 프로토콜로부터 대상에 대해 학습하는 경우 경로의 AD(Administrative Distance)를 비교하고 AD가 짧은 경로가 라우팅 테이블에 입력됩니다.

경로의 관리 거리

라우팅 프로토콜에서 검색 또는 재배포되는 경로에 대한 관리 영역을 변경할 수 있습니다. 서로 다른 두 라우팅 프로토콜의 두 경로가 관리 영역이 같을 경우 기본 관리 영역이 낮은 경로가 라우팅 테이

블에 입력됩니다. EIGRP 및 OSPF 경로의 경우 EIGRP 경로와 OSPF 경로가 관리 영역이 같으면 기본적으로 EIGRP 경로가 선택됩니다.

관리 영역은 서로 다른 두 라우팅 프로토콜로부터 동일한 목적지의 서로 다른 경로가 2개 이상 나올 경우 최적의 경로를 선택하기 위해 위협 방지 디바이스에서 사용하는 경로 매개변수입니다. 라우팅 프로토콜은 다른 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 서로 다른 라우팅 프로토콜에서 생성된 동일 목적지의 경로 2개 중에서 최적의 경로를 결정하는 것이 가능하지 않을 수도 있습니다.

각 라우팅 프로토콜은 관리 영역 값을 사용하여 우선순위가 지정됩니다. 다음 표에는 위협 방지 디바이스에서 지원하는 라우팅 프로토콜의 기본 관리 거리 값이 정리되어 있습니다.

표 ***2:*** 지원되는 라우팅 프로토콜의 기본 관리 영역

경로 소스	기본 관리 영역
연결된 인터페이스	0
VPN 경로	1
고정 경로	1
EIGRP 요약 경로	5
외부 BGP	20
내부 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 외부 경로	170
내부 및 로컬 BGP	200
알 수 없음	255

관리 영역의 값이 작을수록 프로토콜 우선순위가 높습니다. 예를 들어, 위협 방지 디바이스가 OSPF 라우팅 프로세스(기본 관리 거리 - 110)와 RIP 라우팅 프로세스(기본 관리 거리 - 120)로부터 모두 특정 네트워크로의 경로를 수신할 경우 위협 방지 디바이스는 우선순위가 더 높은 OSPF 경로를 선택합니다. 이러한 경우 라우터가 라우팅 테이블에 경로의 OSPF 버전을 추가합니다.

VPN 광고 경로(V-Route/RRI)는 기본 AD(Administrative Distance)가 1인 고정 경로와 같습니다. 그러나 네트워크 마스크 255.255.255.255와 마찬가지로 기본 설정이 더 높습니다.

이 예제에서, OSPF 파생 경로의 소스가 손실된 경우(예: 전원 꺼짐) 위협 방지 디바이스는 OSPF 파생 경로가 다시 나타날 때까지 RIP 파생 경로를 사용합니다.

관리 영역은 로컬 설정입니다. 예를 들어 OSPF를 통해 얻은 경로의 관리 거리를 변경하면 이 변경 사항은 이 명령을 입력한 위협 방지 디바이스의 라우팅 테이블에만 영향을 미칩니다. 관리 영역은 라우팅 업데이트에서 광고되지 않습니다.

관리 영역은 라우팅 프로세스에 영향을 주지 않습니다. 라우팅 프로세스에서는 라우팅 프로세스를 통해 검색되었거나 라우팅 프로세스로 재배포된 경로만 알립니다. 예를 들어 RIP 라우팅 프로세스는 OSPF 라우팅 프로세스를 통해 발견된 경로가 라우팅 테이블에 사용되더라도 RIP 경로를 광고합니다.

동적 및 부동 정적 경로 백업

다른 경로가 설치되었기 때문에 라우팅 테이블에 경로를 설치하려는 첫 번째 시도가 실패하면 백업 경로가 등록됩니다. 라우팅 테이블에 설치된 경로가 실패할 경우 라우팅 테이블 유지 관리 프로세스는 백업 경로를 등록한 각 라우팅 프로토콜 프로세스를 호출하고 해당 경로를 라우팅 테이블에 다시 설치하도록 요청합니다. 실패한 경로에 대해 백업이 등록된 프로토콜이 여럿인 경우 관리 영역을 기준으로 우선 경로가 선택됩니다.

이 프로세스 때문에 동적 라우팅 프로토콜을 통해 발견된 경로가 실패할 때 라우팅 테이블에 설치된 유동 고정 경로를 생성할 수 있습니다. 유동 고정 경로는 단순히 위협 방지 디바이스에서 실행되는 동적 라우팅 프로토콜보다 큰 관리 영역으로 설정된 고정 경로입니다. 동적 라우팅 프로세스에서 발견한 경로가 실패하면 라우팅 테이블에 고정 경로가 설치됩니다.

포워딩 결정 방법

포워딩 결정은 다음과 같이 이루어집니다.

- 목적지가 라우팅 테이블 내의 항목과 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 포워딩됩니다. 기본 경로가 구성되지 않은 경우 패킷이 폐기됩니다.
- 목적지가 라우팅 테이블의 단일 항목과 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 포워딩됩니다.
- 목적지가 라우팅 테이블에 있는 두 개 이상의 항목과 일치하면 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷은 라우팅 테이블의 다음 경로를 통해 인터페이스에 도착합니다.

- 192.168.32.0/24 게이트웨이 10.1.1.2
- 192.168.32.0/19 게이트웨이 10.1.1.3

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 이 주소는 라우팅 테이블 내 다른 경로에도 포함되지만, 라우팅 테이블의 다른 경로 접두사는 19비트인 데 비해 192.168.32.0/24의 접두사는 24비트이므로 이 경로의 접두사가 가장 깁니다. 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

참고 새로운 유사한 연결이 경로 변경으로 인해 다른 동작을 유발하는 경우에도 기존의 연결은 계속해서 설정된 인터페이스를 사용합니다.

관리 트래픽용 라우팅 테이블

표준 보안 관행으로 데이터 트래픽에서 관리 트래픽(디바이스에서)을 분리 및 격리할 필요가 있는 경우가 많습니다. 이 격리를 달성하기 위해 threat defense 디바이스에서는 데이터 트래픽과 관리 전용 트래픽에 대해 각각 별도의 라우팅 테이블을 사용합니다. 별도의 라우팅 테이블을 사용하면 데이터 및 관리를 위해 별도의 기본 경로도 생성할 수 있습니다.

각 라우팅 테이블의 트래픽 유형

디바이스를 통과하는 트래픽에서는 항상 데이터 라우팅 테이블을 사용합니다.

디바이스에서 시작되는 트래픽에서는 유형에 따라 기본적으로 관리 전용 라우팅 테이블 또는 데이터 라우팅 테이블 중 하나를 사용합니다. 기본 라우팅 테이블에서 일치하는 항목을 찾을 수 없으면 다른 라우팅 테이블을 확인합니다.

- 디바이스에서 시작되는 트래픽의 관리 전용 테이블에는 AAA 서버 통신이 포함됩니다.
- 디바이스에서 시작되는 트래픽의 데이터 테이블에는 DNS 서버 조회 및 DDNS가 포함됩니다. 단, DNS에 대해 진단 인터페이스만 지정하는 경우, threat defense 디바이스는 관리 전용 테이블만 사용합니다.

관리 전용 라우팅 테이블에 포함된 인터페이스

관리 전용 인터페이스에는 관리 x/x 인터페이스뿐 아니라 관리 전용으로 컨피그레이션한 모든 인터페이스도 포함됩니다.

참고 관리 가상 인터페이스는threat defense 경로 조회에 속하지 않는 자체 Linux 라우팅 테이블을 사용합니다. 관리 인터페이스에서 시작되는 트래픽에는 device manager 관리 세션, 라이선싱 통신 및 데이터베이스 업데이트가 포함됩니다. 그러나 논리적 진단 인터페이스는 이 섹션에서 설명된 관리 전용 라우팅 테이블을 사용합니다.

다른 라우팅 테이블로 대체

기본 라우팅 테이블에서 일치하는 항목을 찾을 수 없으면 다른 라우팅 테이블을 확인합니다.

비기본 라우팅 테이블 사용

기본 라우팅 테이블에 없는 인터페이스에서 외부로 이동하는 데 즉시 사용 가능한 트래픽이 필요한 경우, 다른 테이블로 대체하지 않고 구성할 때 해당 인터페이스를 지정해야 할 수 있습니다. threat defense에서는 지정된 인터페이스에 대한 경로만 확인합니다. 예를 들어, 데이터 인터페이스에서 RADIUS 서버와 통신해야 하는 경우, RADIUS 설정에서 해당 인터페이스를 지정합니다. 그렇지 않으면 관리 전용 라우팅 테이블에 기본 경로가 있는 경우, 이는 기본 경로와 일치하며 데이터 라우팅 테이블로 대체되지 않습니다.

ECMP(Equal-Cost Multi-Path) 라우팅

위협 방지 디바이스에서는 ECMP(Equal-Cost Multi-Path) 라우팅을 지원합니다.

인터페이스당 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 외부 인터페이스에서 서로 다른 게이트웨이를 지정하는 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

여기서는 외부 인터페이스에서 0.1.1.2, 10.1.1.3, 10.1.1.4끼리 트래픽 로드 밸런싱을 수행합니다. 트래픽은 소스와 대상 IP 주소, 수신 인터페이스, 프로토콜, 소스 및 대상 포트를 해싱하는 알고리즘에 따라 지정된 게이트웨이 사이에서 분배됩니다.

트래픽 영역을 사용하는 여러 인터페이스의 **ECMP**

인터페이스 그룹을 포함하도록 트래픽 영역을 구성할 경우, 하나의 영역 내에서 최대 8개의 인터페이스에 걸쳐 최대 8개의 동일 비용 정적 또는 동적 경로가 가능합니다. 예를 들어 다음과 같이 영역 내 인터페이스 3개의 전 범위에 걸쳐 여러 개의 기본 경로를 컨피그레이션할 수 있습니다.

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

또한 동적 라우팅 프로토콜은 동일 비용 경로를 자동으로 구성할 수 있습니다. 위협 방지 디바이스에서는 더 강력한 로드 밸런싱 메커니즘을 통해 인터페이스 간의 트래픽을 로드 밸런싱합니다.

어떤 경로가 사라지면 디바이스에서는 다른 경로로 원활하게 플로우를 이동합니다.

고정 경로

네트워크에 대한 기본 라우팅을 제공하기 위해 정적 경로를 생성할 수 있습니다.

고정 경로 및 기본 경로 소개

비연결 호스트 또는 네트워크에 트래픽을 라우팅하려면 정적 또는 동적 라우팅을 사용하여 해당 호스트 또는 네트워크로 가는 경로를 정의해야 합니다. 일반적으로 최소한 하나의 고정 경로를 구성해야 합니다. 다른 방법으로는 기본 네트워크 게이트웨이(대개는 다음 홉 라우터)에 라우팅되지 않는 모든 트래픽을 위한 기본 경로입니다.

기본 라우터

가장 간단한 옵션은 트래픽을 라우팅해주는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 정적 경로를 컨피그레이션하는 것입니다. 기본 고정 경로는 위협 방지 디바이스가 학습 경로나 고정 경로를 가지고 있지 않은 모든 IP 패킷을 보낼 게이트웨이 IP 주소를 식별합니다. 기본 정적 경로는 대상 IP 주소가 0.0.0.0/0(IPv4) 또는 ::/0(IPv6)인 정적 경로일 뿐입니다.

항상 기본 경로를 정의해야 합니다.

threat defense 디바이스에서는 데이터 트래픽 및 관리 트래픽에 대해 별도의 라우팅 테이블을 사용하므로 선택적으로 데이터 트래픽에 대한 기본 경로를 구성하고 관리 트래픽에 대한 또 다른 기본 경로를 구성할 수 있습니다. 디바이스에서 시작되는 트래픽에서는 유형에 따라 기본적으로 관리 전용 또는 데이터 라우팅 테이블 중 하나를 사용합니다. 그러나 경로를 찾을 수 없는 경우 다른 라우팅 테이블로 폴백됩니다. 기본 경로는 항상 트래픽과 일치하며 다른 라우팅 테이블로 대체되는 것을 방지합니다. 이 경우, 해당 인터페이스가 기본 라우팅 테이블에 없다면 이그레스 트래픽에 사용할 인터페이스를 지정해야 합니다. 진단 인터페이스는 관리 전용 테이블에 포함되어 있습니다. 특수 관리 인터페이스는 별도의 Linux 라우팅 테이블을 사용하며, 자체 기본 경로가 있습니다.

고정 경로

다음과 같은 경우, 고정 경로를 사용할 수 있습니다.

- 네트워크에서 지원하지 않는 라우터 검색 프로토콜을 사용합니다.
- 네트워크 규모가 작고 고정 경로를 쉽게 관리할 수 있습니다.
- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.
- 기본 경로만으로 충분하지 않을 때도 있습니다. 기본 게이트웨이가 목적지 네트워크에 도달할 수 없는 경우가 있기 때문에 보다 구체적인 고정 경로도 구성해야 합니다. 예를 들어 기본 게이트웨이가 밖에 있는 경우 기본 경로는 위협 방지 디바이스에 직접 연결되지 않은 내부 네트워크로 트래픽을 안내할 수 없습니다.
- 동적 라우팅 프로토콜을 지원하지 않는 기능을 사용 중입니다.

고정 경로 백업 및 고정 경로 추적

고정 경로의 문제 중 하나는 경로가 정상인지 다운되었는지 확인할 수 있는 내재적인 메커니즘이 없다는 것입니다. 다음 홉 게이트웨이를 사용할 수 없게 된다 해도 고정 경로는 라우팅 테이블에 남아 있습니다. 고정 경로는 연결된 인터페이스가 다운되는 경우에만 라우팅 테이블에서 제거됩니다.

SLA(Service Level Agreement) 모니터를 사용해 경로 추적을 실행함으로써 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 백업 경로를 자동으로 설치할 수 있습니다. 예를 들어 기본 ISP를 사용할 수 없는 경우에 대비하여 ISP 게이트웨이로의 기본 경로와 보조 ISP로의 보조 기본 경로를 정의할 수 있습니다.

경로 추적을 사용하는 경우, 추적된 경로에 대상 네트워크의 대상 IP 주소를 연결합니다. 그러면 시스템에서는 ICMP 에코 요청을 사용하여 주기적으로 주소 연결 가능 여부를 확인합니다. 지정한 시간 내에 시스템에 에코 응답이 수신되지 않으면 호스트는 연결할 수 없는 것으로 간주되고, 시스템에서는 연결된 경로를 라우팅 테이블에서 제거합니다. 그러면 시스템에서는 메트릭이 높은 비추적 백업 경로를 제거된 경로 대신 사용할 수 있습니다.

따라서 기본 경로를 포함한 특정 대상에 대한 백업 고정 경로를 사용하려면 다음 작업을 수행해야 합니다.

1. 게이트웨이 또는 상시 가동 서버(예: 웹 서버 또는 syslog 서버) 등 대상 네트워크에서 신뢰할 수 있는 IP 주소를 모니터링하는 SLA 모니터를 생성합니다. 대상 네트워크가 정상 상태이고 사용 가능한 동안에는 오프라인 상태로 전환될 수 있는 시스템의 IP 주소를 모니터링하지 마십시오. SLA 모니터 개체 컨피그레이션, 13 페이지를 참조하십시오.

2. 대상으로 연결되는 기본 경로를 생성하고 이 경로에 대해 SLA 모니터를 선택합니다. 이 경로에 대한 메트릭은 일반적으로 1이어야 합니다. 고정 경로 구성, 11 페이지를 참조하십시오.
3. 기본 경로가 실패할 경우 사용할 백업 정적 경로를 생성합니다. 이 경로의 메트릭은 기본 경로보다 커야 합니다. 예를 들어 기본 경로가 1이면 백업 경로는 10일 수 있습니다. 또한 일반적으로 백업 경로에 대해 다른 인터페이스를 선택합니다.

정적 라우팅에 대한 지침

브리지 그룹

- 라우티드 모드에서는 BVI를 게이트웨이로 지정해야 하며 멤버 인터페이스는 지정할 수 없습니다.
- 위협 방지 디바이스(예: syslog 또는 SNMP)에서 발생하고 브리지 그룹 멤버 인터페이스를 거쳐 직접 연결되지 않은 네트워크로 가는 트래픽의 경우, 기본 경로 또는 정적 경로를 컨피그레이션하여 위협 방지 디바이스에서 어떤 브릿지 그룹 멤버 인터페이스로 트래픽을 보낼지 알 수 있게 해야 합니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다.
- 브리지 그룹 멤버 인터페이스 또는 BVI에 대해서는 정적 경로 추적을 지원하지 않습니다.

IPv6

- 고정 경로 추적(SLA 모니터링)은 IPv6에서 지원되지 않습니다.

ECMP(Equal-Cost Multi-Path) 트래픽 영역

- 서로 다른 액세스, SSL 또는 ID 규칙이 해당 인터페이스에 적용되지 않도록 ECMP 트래픽 영역의 멤버 인터페이스를 동일한 보안 영역에 유지합니다.
- 지정된 ECMP 트래픽 영역에서 네트워크에 대해 최대 8개의 동일 비용 경로를 가질 수 있습니다.
- 영역당 최대 8개의 인터페이스를 사용하여 최대 256개의 ECMP 트래픽 영역을 생성할 수 있습니다.
- ECMP 트래픽 영역은 이름이 지정된 물리적 인터페이스, 하위 인터페이스 및 Etherchannel을 포함할 수 있습니다. 여기에는 다음을 포함할 수 없습니다.
  - 브리지 그룹(BVI) 또는 멤버
  - Etherchannel 멤버 인터페이스
  - HA 인터페이스(페일오버 또는 상태 링크)
  - 관리 전용 인터페이스
  - 사이트 대 사이트 VPN 또는 원격 액세스 VPN 연결에 사용되는 인터페이스.
  - VTI(Virtual Tunnel Interface) 또는 해당 소스 인터페이스.

- VPN 관리 액세스용으로 구성된 인터페이스.

- 영역의 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.

고정 경로 구성

시스템의 인터페이스에 직접 연결된 네트워크로 이동하지 않는 패킷을 전송할 위치를 시스템에 지시하려면 고정 경로를 정의합니다.

네트워크 0.0.0.0/0에 대해 하나 이상의 고정 경로(기본 경로)가 필요합니다. 이 경로는 기존 NAT xlate(변환)나 고정 NAT 규칙 또는 기타 정적 경로를 통해 이그레스 인터페이스를 확인할 수 없는 패킷을 전송할 위치를 정의합니다.

기본 게이트웨이를 사용하여 모든 네트워크에 액세스할 수 없는 경우 다른 고정 경로가 필요할 수 있습니다. 예를 들어 기본 경로는 대개 외부 인터페이스의 업스트림 라우터입니다. 디바이스에 직접 연결되지 않는 추가 내부 네트워크가 있으며 기본 게이트웨이를 통해 해당 네트워크에 액세스할 수 없는 경우에는 이러한 각 내부 네트워크에 대해 고정 경로가 필요합니다.

시스템 인터페이스에 직접 연결된 네트워크에 대해서는 고정 경로를 정의할 수 없습니다. 시스템에서 이러한 경로를 자동으로 생성합니다.

프로시저

단계 **1** 디바이스를 클릭한 다음, **Routing(**라우팅**)** 요약의 링크를 클릭합니다.

단계 **2** 가상 라우터를 활성화한 경우 정적 경로를 구성 중인 라우터의 보기 아이콘( )을 클릭합니다.

단계 **3** **Static Routing(**정적 라우팅**)** 페이지에서 다음 중 하나를 수행합니다.

- 새 경로를 추가하려면 +를 클릭합니다.
- 수정할 경로의 수정 아이콘( )을 클릭합니다.

경로가 더 이상 필요하지 않은 경우 해당 경로의 휴지통 아이콘을 클릭하여 경로를 삭제합니다.

단계 **4** 경로 속성을 구성합니다.

- **Name(**이름**)** — 경로의 표시 이름입니다.
- **Description(**설명**)** — 경로의 용도에 대한 설명(선택 사항)입니다.
- **Interface(**인터페이스**)** — 트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다.

  브리지 그룹의 경우 멤버 인터페이스가 아닌 BVI(브리지 그룹 인터페이스)에 대해 경로를 구성합니다.

  가상 라우팅 및 전달을 활성화한 경우 다른 가상 라우터에 속한 인터페이스를 선택할 수 있습니다. 가상 라우터에서 다른 가상 라우터의 인터페이스에 대한 정적 경로를 생성하는 경우, 이 경로는 가상 라우터 경계를 통과하며 이 가상 라우터의 트래픽이 다른 가상 라우터로 유출될 위험이 있습니다. 이는 원하는 결과일 수 있지만, 이러한 경로 유출이 필요한지 신중하게 판단하십시

오. 인터페이스를 선택하면 인터페이스가 속한 가상 라우터의 이름이 인터페이스 오른쪽에 표시됩니다.

- **Protocol(**프로토콜**)** — 경로가 **IPv4** 또는 **IPv6** 주소에 대한 경로인지 선택합니다.
- **Networks(**네트워크**)** — 이 경로에서 게이트웨이를 사용해야 하는 대상 네트워크 또는 호스트를 식별하는 네트워크 개체를 선택합니다.

  기본 경로를 정의하거나, 사전 정의된 임의의 ipv4 또는 ipv6 네트워크 개체를 사용하거나, 0.0.0.0/0(IPv4) 또는 ::/0(IPv6) 네트워크에 대해 개체를 생성합니다.
- **Gateway(**게이트웨이**)** — 게이트웨이의 IP 주소를 식별하는 호스트 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다. 둘 이상의 인터페이스에서 경로에 대해 동일한 게이트웨이를 사용할 수 없습니다.

  가상 라우터에서 경로를 정의하고 있으며 인터페이스가 다른 가상 라우터에 속하는 경우, 게이트웨이를 비워두어야 합니다. 시스템에서는 이러한 네트워크에 대한 트래픽을 다른 가상 라우터로 라우팅한 다음, 대상 가상 라우터의 라우팅 테이블을 사용하여 게이트웨이를 결정합니다.
- **Metric(**메트릭**)** — 경로의 관리 거리(1~254)입니다. 정적 경로의 경우 기본값은 1입니다. 인터페이스와 게이트웨이 간에 추가 라우터가 있으면 홉 수를 관리 거리로 입력합니다.

  관리 거리는 경로를 비교하는 데 사용되는 파라미터입니다. 값이 작을수록 경로에는 더 높은 우선 순위가 지정됩니다. 연결된 경로(디바이스의 인터페이스에 직접 연결되는 네트워크)가 항상 고정 경로보다 우선적으로 사용됩니다.

단계 **5** (선택 사항, IPv4 경로만 해당) 이 경로의 실행 가능성을 추적해야 하는 **SLA Monitor(SLA** 모니터**)**를 선택합니다.

SLA 모니터에서는 대상 네트워크의 항상 사용 가능한 호스트에 연결 가능한지 확인할 수 있습니다. 연결할 수 없게 되면 시스템에서 백업 경로를 설치할 수 있습니다. 따라서 SLA 모니터를 구성하는 경우 이 네트워크에 대해 더 큰 메트릭을 사용하여 또 다른 정적 경로를 구성해야 합니다. 예를 들어 이 경로에 메트릭 1이 있는 경우 메트릭 10을 사용하여 백업 경로를 생성합니다. 자세한 내용은 고정 경로 백업 및 고정 경로 추적, 9 페이지의 내용을 참고하십시오.

SLA 모니터 개체가 아직 없는 경우 목록 하단에서 **Create SLA Monitor(SLA** 모니터 생성**)** 링크를 클릭하여 바로 생성합니다.

참고 모니터링되는 주소를 ping할 수 없으므로 모니터링되는 경로가 제거되면 해당 경로가 경로에 연결할 수 없다는 경고와 함께 정적 경로 테이블에 표시됩니다. 이 문제가 일시적인지 또는 경로를 재구성해야 하는지 확인하십시오. 경로를 실행할 수는 있지만 모니터링되는 주소를 충분히 신뢰할 수는 없는 경우일 수도 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

SLA 모니터 개체 컨피그레이션

정적 경로와 함께 사용할 SLA(Service Level Agreement) 모니터 개체를 컨피그레이션합니다. SLA 모니터를 사용하여 정적 경로의 상태를 추적하고 실패한 경로를 새것으로 자동 교체할 수 있습니다. 경로 추적에 관한 자세한 내용은 고정 경로 백업 및 고정 경로 추적, 9 페이지를 참조하십시오.

모니터링 대상을 선택할 때, ICMP 에코 요청에 응답할 수 있는지 확인해야 합니다. 타겟은 호스트 네트워크 개체에 정의된 모든 IP 주소가 될 수 있지만, 다음 항목을 사용하는 것이 좋습니다.

- 이중 ISP 지원을 위한 ISP 게이트웨이 주소
- 다음 홉 게이트웨이 주소(게이트웨이의 가용성이 우려되는 경우)
- syslog 서버와 같이 시스템에서 통신해야 하는 대상 네트워크에 있는 서버
- 대상 네트워크에 있는 지속적인 IP 주소 야간에 꺼질 수 있는 워크스테이션은 좋은 선택이 아닙니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**를 선택한 다음, **SLA Monitors(SLA** 모니터**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 Name(이름) 및 설명(선택 사항)을 입력합니다.

단계 **4** 다음과 같이 SLA 모니터의 필수 옵션을 정의합니다.

- **Monitor Address(**모니터 주소**)** — 대상 네트워크에서 모니터링할 주소를 정의하는 호스트 네트워크 개체를 선택합니다. 필요한 개체가 없는 경우에는 **Create New Network(**새 네트워크 생성**)**를 클릭하면 됩니다.

  이 주소는 SLA 모니터를 정적 경로에 연결하는 경우에만 모니터링됩니다.

- **Target Interface(**대상 인터페이스**)** — 에코 요청 패킷을 전송할 인터페이스를 선택합니다. 일반적으로 정적 경로를 정의하는 인터페이스입니다. 인터페이스 소스 주소는 에코 요청 패킷의 소스 주소로 사용됩니다.

단계 **5** (선택 사항). **IP ICMP Echo Options(IP ICMP** 에코 옵션**)**를 조정합니다.

모든 ICMP 옵션의 기본값은 대부분의 경우에 적합하지만, 이는 필요에 따라 조정할 수 있습니다.

- **Threshold(**임계값**)** — 선언할 상승 임계값에 대한 밀리초 수(0~2147483647). 기본값은 5,000(5초)입니다. 이 값은 시간 초과에 대해 설정된 값보다 클 수 없습니다. 임계값은 연결성에 영향을 주지 않는 임계값 이벤트를 통해 표시할 때만 사용됩니다. 임계값 이벤트의 빈도를 사용해 시간 초과에 대한 설정을 평가할 수 있습니다.

- **Timeout(**시간 초과**)** — 경로 모니터링 작업에서 요청 패킷의 응답을 기다려야 할 밀리초 단위 시간입니다(0~604800000밀리초, 7일 기준). 기본값은 5,000밀리초입니다(5초). 이 기간에 모니터에서 하나 이상의 에코 요청에 대해 응답을 가져오지 않는 경우, 프로세스에서는 백업 경로를 설치합니다.
- **Frequency(**빈도**)** — SLA 프로브 사이의 밀리초 수이며(1,000~604,800,000) 1,000의 배수입니다. 시간 초과 값보다 낮은 빈도는 설정할 수 없습니다. 기본값은 60,000밀리초입니다(60초).
- **Type of Service(**서비스 유형**)** — ICMP 에코 요청 패킷의 IP 헤더에서 ToS(Type of Service) 유형을 정의하는 정수입니다(0~255). 기본값은 0입니다.
- **Number of Packets(**패킷 수**)** — 각 폴과 함께 전송되는 패킷의 수입니다(1~100). 기본값은 1패킷입니다.
- **Data Size(**데이터 크기**)** — 에코 요청 패킷에 사용할 데이터 페이로드의 크기입니다(0~16384바이트). 기본값은 28입니다. 이 설정은 페이로드의 크기만 지정하며 전체 패킷의 크기는 지정하지 않습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

이제 정적 경로에서 SLA 모니터 개체를 사용할 수 있습니다.

라우팅 모니터링

라우팅을 모니터링하고 트러블슈팅하려면 CLI 콘솔을 열거나 디바이스 CLI에 로그인하여 다음 명령을 사용합니다. Routing(라우팅) 페이지의 **Commands(**명령**)** 메뉴에서 이러한 명령 중 일부를 선택할 수도 있습니다.

- **show route** 직접 연결된 네트워크의 경로를 비롯하여 데이터 인터페이스에 대한 라우팅 테이블을 표시합니다.
- **show ipv6 route** 직접 연결된 네트워크의 경로를 비롯하여 데이터 인터페이스에 대한 IPv6 라우팅 테이블을 표시합니다.
- **show network**에서 관리 게이트웨이를 비롯하여 가상 관리 인터페이스의 설정을 표시합니다. 관리 게이트웨이로 데이터 인터페이스를 지정하는 경우가 아니면 가상 관리 인터페이스를 통한 라우팅은 데이터 인터페이스 라우팅 테이블에 의해 처리되지 않습니다.
- **show network-static-routes**에서는 **configure network static-routes** 명령을 사용해 가상 관리 인터페이스에 대해 설정된 정적 경로를 표시합니다. 대부분의 경우에는 관리 라우팅에 관리 게이트웨이만 사용하면 되므로, 일반적으로는 정적 경로가 없습니다. 데이터 인터페이스의 트래픽에는 이러한 경로를 사용할 수 없습니다. 이 명령은 CLI 콘솔에서 사용할 수 없습니다.
- **show ospf** OSPF 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show ospf ?**를 사용하여 OSPF에 대한 특정 정보를 보기 위해 포함할 수 있는 옵션 목록을 가져옵니다.

- **show bgp** 는 BGP 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show bgp ?**를 사용하여 BGP에 대한 특정 정보를 보기 위해 포함할 수 있는 옵션 목록을 가져옵니다.
- **show eigrp** *option*은 EIGRP 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show eigrp ?**를 사용하여 포함할 수 있는 옵션 목록을 가져옵니다. 옵션을 제공해야 합니다.
- **show isis** *option*은 IS-IS 프로세스 및 확인된 경로에 대한 정보를 표시합니다. **show isis ?**를 사용하여 포함할 수 있는 옵션 목록을 가져옵니다. 옵션을 제공해야 합니다.
- **show rip database** 는 RIP 프로세스 및 확인된 경로에 대한 정보를 표시합니다.
- **show vrf** 시스템에 정의된 가상 라우터에 대한 정보를 표시합니다.
- **show zone** 각 영역의 일부인 인터페이스를 포함하여 ECMP 트래픽 영역에 대한 정보를 표시합니다.