고정 경로 및 기본 경로

이 장에서는 threat defense에서 고정 경로와 기본 경로를 구성하는 방법을 설명합니다.

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 defense에서는 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(관리 트래픽용 라우팅 테이블, 13 페이지 참조). 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. **configure network** 명령을 참조하십시오.

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.
- 가상 라우터는 고정 경로를 사용하여 경로 누수를 생성합니다. 경로 누수는 가상 라우터의 인터페이스에서 다른 가상 라우터의 다른 인터페이스로 향하는 트래픽 흐름을 활성화합니다. 자세한 내용은 인터커넥트 가상 라우터를 참고하십시오.

원치 않는 트래픽을 지우기 위한 null0 인터페이스로의 경로

액세스 규칙을 통해 패킷 헤더의 정보에 따라 패킷을 필터링할 수 있습니다. null0 인터페이스에 대한 고정 경로는 액세스 규칙을 보완합니다. null0 경로를 사용하여 원치 않는 트래픽을 전달하여 트래픽이 삭제되도록 할 수 있습니다.

고정 null0 경로는 성능을 향상시킵니다. 또한 라우팅 루프를 방지하는 데 고정 null0 경로를 사용할 수 있습니다. BGP는 Remotely Triggered Black Hole 라우팅을 위해 고정 null0 경로를 활용할 수 있습니다.

경로 우선 순위

- 특정 대상을 식별하는 경로가 기본 경로보다 우선합니다.
- 동일한 목적지에 대한 여러 경로(고정 또는 동적)가 있을 경우 경로의 관리 영역에 따라 우선 순위가 결정됩니다. 고정 경로는 1로 설정되므로 대개 우선 순위가 높은 경로입니다.
- 동일한 관리 거리에서 동일한 대상에 대해 여러 고정 경로가 있는 경우, ECMP(Equal-Cost Multi-Path) 라우팅, 14 페이지를 참조하십시오.
- 터널링 옵션을 사용하여 터널로부터 생성된 트래픽의 경우 이 경로는 구성되었거나 학습된 다른 기본 경로를 무시합니다.

투명 방화벽 모드 및 브리지 그룹 경로

위협 방지 디바이스에서 발생하고 브리지 그룹 멤버 인터페이스를 거쳐 직접 연결되지 않은 네트워크로 가는 트래픽의 경우, 기본 경로 또는 고정 경로를 구성하여 위협 방지 디바이스에서 어떤 브리

지 그룹 멤버 인터페이스로 트래픽을 보낼지 알 수 있게 해야 합니다. 위협 방지 디바이스에서 발생하는 트래픽은 syslog 서버 또는 SNMP 서버로의 통신을 포함할 수 있습니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다. 투명 모드에서는 BVI를 게이트웨이 인터페이스로 지정할 수 없습니다. 멤버 인터페이스만 사용할 수 있습니다. 라우팅 모드의 브리지 그룹에 대해서는 고정 경로에서 BVI를 지정해야 합니다. 멤버 인터페이스는 지정할 수 없습니다. 자세한 내용은 #unique_892를 참조하십시오.

고정 경로 추적

고정 경로의 문제 중 하나는 경로가 정상인지 다운되었는지 확인할 수 있는 내재적인 메커니즘이 없다는 것입니다. 다음 홉 게이트웨이가 사용할 수 없게 되어도 라우팅 테이블에 남습니다. 고정 경로는 위협 방지 디바이스의 연결된 인터페이스가 다운되는 경우에만 라우팅 테이블에서 제거됩니다.

고정 경로 추적 기능은 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 보조 경로를 설치하는 수단을 제공합니다. 예를 들어 기본 ISP를 사용할 수 없는 경우에 대비하여 ISP 게이트웨이로의 기본 경로와 보조 ISP로의 보조 기본 경로를 정의할 수 있습니다.

위협 방지 디바이스에서는 위협 방지 디바이스에서 ICMP 에코 요청을 통해 모니터링하는 목적지 네트워크의 모니터링 대상 호스트와 고정 경로를 연결하는 방법으로 고정 경로 추적을 구현합니다. 에코 응답이 지정된 시간 동안 수신되지 않으면 호스트는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다. 메트릭이 높은 비추적 백업 경로를 제거된 경로 대신 사용합니다.

모니터링 대상을 선택할 때, ICMP 에코 요청에 응답할 수 있는지 확인해야 합니다. 대상은 사용자가 선택하는 아무 네트워크 객체나 될 수 있지만 다음을 사용할 것을 고려해야 합니다.

- ISP 게이트웨이(이중 ISP 지원) 주소
- 다음 홉 게이트웨이 주소(게이트웨이의 가용성이 우려되는 경우)
- syslog 서버와 같이 위협 방지 디바이스가 통신해야 하는 대상 네트워크에 있는 서버
- 목적지 네트워크에 있는 지속적인 네트워크 객체

참고 야간에 꺼질 수 있는 PC는 좋은 선택이 아닙니다.

DHCP 나 PPPoE를 통해 얻은 고정으로 정의된 경로나 기본 경로를 위해 고정 경로 추적을 구성할 수 있습니다. 경로 추적이 구성된 여러 인터페이스에서만 PPPoE 클라이언트를 활성화할 수 있습니다.

정적 경로 요구 사항 및 사전 요건

모델 지원

Threat Defense

지원되는 도메인

모든

사용자 역할

관리자

네트워크 관리자

고정 경로 및 기본 경로를 위한 지침

방화벽 모드 및 브리지 그룹

- 투명 모드의 경우, 정적 경로에서는 브리지 그룹 멤버 인터페이스를 게이트웨이로 사용해야 하며 BVI는 지정할 수 없습니다.
- 라우티드 모드에서는 BVI를 게이트웨이로 지정해야 하며 멤버 인터페이스는 지정할 수 없습니다.
- 브리지 그룹 멤버 인터페이스 또는 BVI에 대해서는 고정 경로 추적이 지원되지 않습니다.

지원되는 네트워크 주소

- 고정 경로 추적은 IPv6에서 지원되지 않습니다.
- ASA는 CLASS E 라우팅을 지원하지 않습니다. 따라서 CLASS E 네트워크는 고정 경로로 라우팅할 수 없습니다.

클러스터링 및 다중 상황 모드

- 클러스터링에서는 정적 경로 추적을 기본 유닛에서만 지원합니다.
- 정적 경로 추적은 상황 모드에서 지원되지 않습니다.

네트워크 개체 그룹

정적 경로를 구성하는 동안에는 IP 주소 범위를 포함하는 네트워크 개체 그룹 또는 네트워크 개체 범위를 사용할 수 없습니다.

ASP 및 리브 경로 항목

디바이스에 설치된 모든 경로 및 해당 거리는 ASP 라우팅 테이블에 캡처됩니다. 이는 모든 정적 및 동적 라우팅 프로토콜에 공통적으로 적용됩니다. 최적의 거리 경로만 리브 테이블에 캡처됩니다.

고정 경로 추가

고정 경로는 특정 목적지 네트워크로 향하는 트래픽을 어디로 보낼지 정의합니다. 최소한 하나의 기본 경로를 정의해야 합니다. 기본 경로는 단순히 목적지 IP 주소가 0.0.0.0/0인 고정 경로입니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집합니다.

단계 **2** **Routing(**라우팅**)**을 클릭합니다.

단계 **3** (가상 라우터를 인식하는 디바이스의 경우) 가상 라우터 드롭다운 목록에서 정적 경로를 구성할 가상 라우터를 선택합니다.

단계 **4** 정적 경로를 선택합니다.

단계 **5** 경로 추가를 클릭합니다.

단계 **6** 추가하려는 정적 경로 유형에 따라 **IPv4** 또는 **IPv6**를 클릭합니다.

단계 **7** 고정 경로를 적용하려는 인터페이스를 선택합니다.

투명 모드에서는 브리지 그룹 멤버 인터페이스 이름을 선택합니다. 브리지 그룹에 라우팅된 모드에서 BVI 이름에 대해 둘 중 하나의 브리지 그룹 멤버 인터페이스를 선택할 수 있습니다. 원치 않는 트래픽을 "완전히 사라지게 하려면" **Null0** 인터페이스를 선택합니다.

가상 라우팅을 사용하는 디바이스의 경우 다른 가상 라우터에 속한 인터페이스를 선택할 수 있습니다. 이 가상 라우터에서 다른 가상 라우터로 트래픽을 누출해야 한다면 고정 경로를 생성하면 됩니다. 자세한 내용은 인터커넥트 가상 라우터의 내용을 참고하십시오.

단계 **8** 사용 가능한 네트워크 목록에서 대상 네트워크를 선택합니다.

기본 경로를 정의하려면 주소 0.0.0.0/0 인 개체를 생성하고 여기에서 선택합니다.

참고 IP 주소 범위를 포함하는 네트워크 개체 그룹을 생성하고 선택할 수는 있지만, management center는 정적 경로를 설정하는 동안 네트워크 개체 범위 사용을 지원하지 않습니다.

단계 **9** 게이트웨이 또는 **IPv6** 게이트웨이 필드에 입력하거나 이 경로의 다음 홉인 게이트웨이 라우터를 선택합니다. IP 주소 또는 네트워크/호스트 개체를 제공할 수 있습니다. 가상 라우터에 정적 경로 구성을 사용하여 경로 누수가 발생하는 경우 다음 홉 게이트웨이를 지정하지 마십시오.

단계 **10** 메트릭 필드에 대상 네트워크 홉의 개수를 입력합니다. 유효한 범위는 1~255이고 기본값은 1입니다. 메트릭은 특정 호스트에 상주하는 네트워크 홉(홉 수)를 기반으로 경로 "확대"에 대한 측정 항목입니다. 홉 수는 대상 네트워크를 포함해 네트워크 패킷이 최종 대상에 도달하기 전 통과해야 하는 네트워크의 수입니다. 메트릭은 다른 라우팅 프로토콜의 경로를 비교하는 데 사용됩니다. 고정 경로에서 기본 관리 영역은 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다. OSPF가 발견한 경로에 대한 기본 관리 영역은 110입니다. 고정 경로의 관리 영역이 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

참고 듀얼 ISP/WAN 인터페이스 구성의 경우 기본 및 보조 데이터 인터페이스 모두에 동일한 메트릭 값을 할당해야 합니다. 기본적으로 두 인터페이스에 대해 동일한 메트릭 값을 구성할 수 없습니다. 검증 오류를 재정의하려면 두 인터페이스가 단일 ECMP 영역에 속해야 합니다.

단계 **11** (선택 사항) 기본 경로에서 터널링 체크 박스를 클릭하여 VPN 트래픽에 대해 별도의 기본 경로를 정의합니다.

VPN 트래픽이 비 VPN 트래픽과 다른 기본 경로를 사용하도록 하기 위해, VPN 트래픽에 대해 별도의 기본 경로를 정의할 수 있습니다. 예를 들어 VPN 연결에서 들어오는 트래픽은 내부 네트워크를 향하도록 쉽게 방향을 정할 수 있는 반면, 내부 네트워크의 트래픽은 외부를 향하도록 방향을 정할 수 있습니다. 터널링 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 디바이스에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 디바이스당 터널링된 기본 게이트웨이를 하나만 구성할 수 있습니다. 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

단계 **12** (IPv4 고정 경로 한정) 경로 가용성을 모니터링하려면 경로 추적 필드에서 모니터링 정책을 정의하는 SLA(Service Level Agreement) 모니터 개체의 이름을 선택합니다.

SLA 모니터링의 내용을 참조하십시오.

참고 기본 및 보조 데이터 인터페이스의 고정 경로에 대해 SLA를 할당해야 합니다(이중 ISP/WAN 인터페이스 구성).

단계 **13** **Ok(**확인**)**를 클릭합니다.

라우팅을 위한 참조

이 섹션에서는 threat defense 내 라우팅 동작 및 지원되는 라우팅 프로토콜의 중요 개념을 설명합니다.

경로 결정

라우팅 프로토콜은 메트릭을 사용하여 패킷이 이동할 최적의 경로를 평가합니다. 메트릭은 경로 대역폭과 같은 측정 기준이며, 목적지에 대한 최적 경로를 결정하는 라우팅 알고리즘에 사용됩니다. 라우팅 알고리즘은 경로 결정을 돕기 위해 경로 정보를 포함하는 라우팅 테이블을 초기화하고 유지합니다. 경로 정보는 사용된 경로 알고리즘에 따라 달라집니다.

라우팅 알고리즘은 다양한 정보로 라우팅 테이블을 채웁니다. 목적지 또는 다음 홉 연결은 최종 목적지로 향하는 과정에서 다음 홉에 해당하는 라우터에 패킷을 전달하는 것이 목적지에 도달하는 최적의 방식임을 라우터에 알립니다. 라우터가 수신 패킷을 수신하면 목적지 주소를 확인하고 이 주소를 다음 홉과 연결하려고 시도합니다.

라우팅 테이블은 또한 경로의 선호도와 같은 다른 정보도 포함합니다. 라우터는 메트릭을 비교하여 최적의 경로를 결정하고 이러한 메트릭은 사용된 라우팅 알고리즘의 설계에 따라 달라집니다.

라우터는 서로 통신하며 다양한 메시지의 전송을 통해 라우팅 테이블을 유지합니다. 라우팅 업데이트 메시지는 일반적으로 라우팅 테이블 전체 또는 일부로 구성되는 메시지입니다. 라우터는 다른 모

든 라우터의 라우팅 업데이트를 분석함으로써 네트워크 토폴로지에 대한 자세한 그림을 그릴 수 있습니다. 라우터 간에 전송되는 메시지의 또 다른 예인 링크-상태 알림은 다른 라우터에 발신자 링크의 상태를 알려줍니다. 연결 정보는 라우터가 네트워크 목적지로의 최적의 경로를 결정할 수 있도록 네트워크 토폴로지의 완전한 그림을 그리는 데에도 사용됩니다.

지원되는 경로 유형

라우터는 몇 가지 경로 유형을 사용할 수 있습니다. 위협 방지 디바이스는 다음 경로 유형을 사용합니다.

- 고정 대 동적
- 단일 경로 대 다중 경로
- 평면 대 계층형
- 연결 상태 대 거리 벡터

고정 대 동적

고정 라우팅 알고리즘은 실제로 네트워크 관리자가 설정한 테이블 매핑입니다. 이러한 매핑은 네트워크 관리자가 변경하지 않는 한 변경되지 않습니다. 고정 경로를 사용하는 알고리즘은 설계하기가 쉽고 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다.

고정 라우팅 시스템은 네트워크 변화에 대응할 수 없기 때문에 꾸준히 변화하는 대규모 네트워크에는 일반적으로 적합하지 않습니다. 대부분의 주요 라우팅 알고리즘은 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 대응하는 동적 라우팅 알고리즘입니다. 메시지가 네트워크 변경 사실을 알리면 라우팅 소프트웨어가 경로를 다시 계산하고 새로운 라우팅 업데이트 메시지를 보냅니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

동적 라우팅 알고리즘은 고정 경로로 적절히 보완할 수 있습니다. 예를 들어 최후의 수단으로 사용하는 라우터(모든 라우팅 불가 패킷이 전송되는 라우터의 기본 경로)는 모든 라우팅 불가 패킷에 대한 저장소 역할을 하도록 지정되어 모든 메시지가 어떻게든 처리되도록 할 수 있습니다.

단일 경로 대 다중 경로

일부 고급 라우팅 프로토콜은 동일 목적지에 대한 다중 경로를 지원합니다. 단일 경로 알고리즘과 달리 이러한 다중 경로 알고리즘은 여러 회선에 걸친 트래픽 멀티플렉싱을 허용합니다. 다중 경로 알고리즘의 이점은 보통 로드 공유라고 부르는 훨씬 뛰어난 처리량과 신뢰성입니다.

평면 대 계층형

일부 라우팅 알고리즘은 평면 공간에서 작동하고 또 다른 일부는 라우팅 계층을 사용합니다. 평면 라우팅 시스템에서 라우터는 다른 모든 라우터의 피어입니다. 계층형 라우팅 시스템에서는 일부 라우터가 모여 라우팅 백본을 형성합니다. 비 백본 라우터의 패킷은 백본 라우터로 이동하고 여기서 백본

을 통해 목적지의 일반 영역에 전달됩니다. 이 지점에 이르면 마지막 백본 라우터에서 하나 이상의 비 백본 라우터를 거쳐 최종 목적지로 이동합니다.

대개 라우팅 시스템은 도메인, 자율 시스템 또는 영역이라고 하는 논리적인 노드 그룹을 지정합니다. 계층형 시스템에서는 다른 도메인의 라우터와 통신할 수 있는 라우터도 있고 같은 도메인의 라우터하고만 통신할 수 있는 라우터도 있습니다. 대규모 네트워크에서는 추가적인 계층 수준이 있을 수 있고 가장 높은 계층 수준의 라우터가 라우팅 백본을 형성합니다.

계층형 라우팅의 가장 큰 장점은 기업 대부분의 조직 구조와 비슷하기 때문에 조직의 트래픽 패턴도 잘 지원한다는 점입니다. 대부분의 네트워크 통신은 소규모 기업 그룹(도메인) 내에서 발생합니다. 인트라도메인 라우터는 도메인 내의 다른 라우터에 대해서만 알면 되므로 라우팅 알고리즘을 간소화할 수 있고 사용되는 라우팅 알고리즘에 따라 라우팅 업데이트 트래픽을 줄일 수 있습니다.

연결 상태 대 거리 벡터

링크 상태 알고리즘 (최단 경로 우선 알고리즘)은 인터네트워크의 모든 노드로 라우팅 정보를 전달합니다. 하지만 각 라우터는 자신의 링크 상태를 설명하는 라우팅 테이블의 일부만 전송합니다. 링크 상태 알고리즘에서는 각 라우터가 라우팅 테이블에서 전체 네트워크의 상태를 그립니다. 거리 벡터 알고리즘(Bellman-Ford 알고리즘이라고도 함)은 각 라우터를 호출하여 라우팅 테이블의 전체 또는 일부를 네이버에 한해 전송하도록 합니다. 기본적으로 링크 상태 알고리즘은 모든 곳으로 소규모 업데이트를 전송하는 반면 거리 벡터 알고리즘은 대규모 업데이트를 인접 디바이스로만 보냅니다. 거리 벡터 알고리즘은 네이버에 대해서만 알고 있습니다. 일반적으로 링크 상태 알고리즘은 OSPF 라우팅 프로토콜과 함께 사용됩니다.

라우팅을 위한 지원되는 인터넷 프로토콜

위협 방지 디바이스는 라우팅을 위해 몇 가지 인터넷 프로토콜을 지원합니다. 이 섹션에서는 각 프로토콜에 대해 간단하게 설명합니다.

- EIGRP(Enhanced Interior Gateway Routing Protocol)

  EIGRP는 IGRP 라우터와의 호환성 및 원활한 상호 작용을 제공하는 Cisco 고유의 프로토콜입니다. 자동 재배포 메커니즘이 IGRP 경로를 Enhanced IGRP로 또한 그 반대로 가져올 수 있게 합니다. 따라서 Enhanced IGRP를 기존 IGRP 네트워크에 점진적으로 추가할 수 있습니다.

- OSPF(Open Shortest Path First)

  OSPF는 IETF(Internet Engineering Task Force)의 IGP(interior gateway protocol) 작업 그룹에서 IP(Internet Protocol) 네트워크를 위해 개발한 라우팅 프로토콜입니다. OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터는 동일한 링크 상태 데이터베이스를 갖고 있는데, 이는 각 라우터에서 사용 가능한 인터페이스 및 연결 가능한 네이버의 목록입니다.

- RIP(Routing Information Protocol)

  RIP는 홉 카운트를 메트릭으로 사용하는 거리 벡터 프로토콜입니다. RIP는 글로벌 인터넷에서 라우팅 트래픽을 위해 널리 사용되며 내부 게이트웨이 프로토콜(IGP)이기 때문에 단일 자율 시스템 내에서 라우팅을 수행합니다.

- BGP(Border Gateway Protocol)

BGP는 자율 시스템 간 라우팅 프로토콜입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. AS(autonomous system) 사이에서 BGP가 사용될 때 이 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때의 프로토콜은 IBGP(Interior BGP)라고 합니다.

라우팅 테이블

threat defense에서는 (디바이스를 통한) 데이터 트래픽과 (디바이스에서의) 관리 트래픽에 별도의 라우팅 테이블을 사용합니다. 이 섹션에서는 라우팅 테이블을 작동 방식을 설명합니다.관리 라우팅 트래픽에 관한 내용은 관리 트래픽용 라우팅 테이블, 13 페이지의 내용을 참조하십시오.

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 ***1:*** 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.

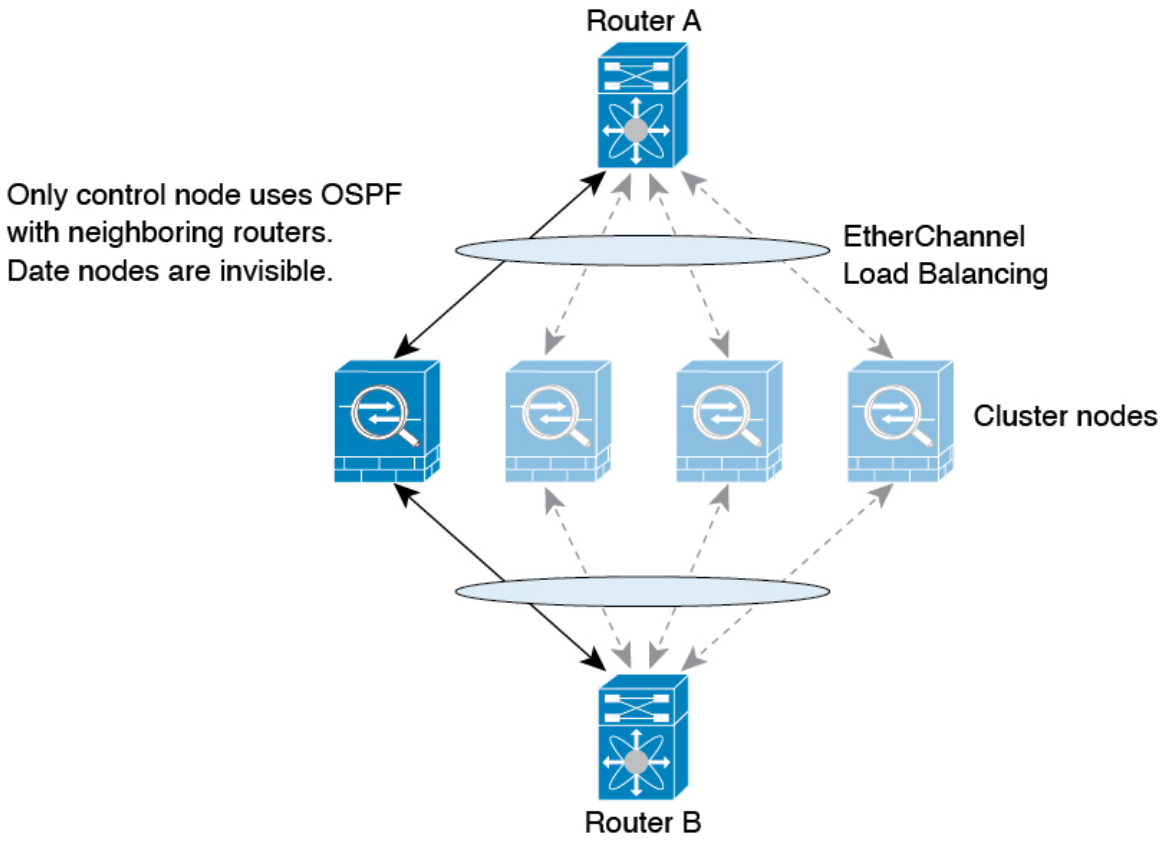
동적 라우팅 및 고가용성

라우팅 테이블이 액티브 유닛에서 변경될 때 동적 경로는 스탠바이 유닛에서 동기화됩니다. 즉, 액티브 유닛의 모든 추가, 삭제 또는 변경 작업은 즉시 스탠바이 유닛에 전파됩니다. 스탠바이 유닛이 액티브/스탠바이 준비 고가용성 쌍에서 액티브 상태가 되면 경로가 고가용성 대량 동기화 및 연속 복제 프로세스의 일부로 동기화되므로 해당 유닛은 이전 액티브 유닛과 동일한 라우팅 테이블을 이미 갖게 됩니다.

클러스터링의 동적 라우팅

라우팅 프로세스는 제어 노드에서만 실행되며, 제어 노드를 통해 경로가 파악되고 데이터 노드에 복제됩니다. 라우팅 패킷이 데이터 노드에 전송되면 해당 패킷은 제어 노드에 리디렉션됩니다.

그림 *1:* 클러스터링의 동적 라우팅



데이터 노드가 제어 노드에서 경로를 학습하면 각 노드에서는 전달과 관련된 결정을 독립적으로 수행합니다.

OSPF LSA 데이터베이스는 제어 노드에서 데이터 노드로 동기화되지 않습니다. 제어 노드 전환이 있을 경우, 인접한 라우터에서 재시작을 탐지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

관리 트래픽용 라우팅 테이블

표준 보안 관행으로 데이터 트래픽에서 관리(디바이스에서 시작) 트래픽을 분리 및 격리할 필요가 있는 경우가 많습니다. 이 격리를 달성하기 위해 threat defense에서는 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 진단 x/x 인터페이스뿐 아니라 관리 전용으로 컨피그레이션한 모든 인터페이스도 포함됩니다.

참고 관리 논리적 인터페이스는 threat defense 경로 조회에 속하지 않는 자체 Linux 라우팅 테이블을 사용합니다. 관리 인터페이스에서 시작되는 트래픽에는 management center 통신, 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 defense 디바이스에서는 지정된 인터페이스에 대한 경로만 확인합니다. 예를 들어, 데이터 인터페이스에서 RADIUS 서버와 통신해야 하는 경우 RADIUS 설정에서 해당 인터페이스를 지정합니다. 그렇

지 않으면 관리 전용 라우팅 테이블에 기본 경로가 있는 경우, 이는 기본 경로와 일치하며 데이터 라우팅 테이블로 대체되지 않습니다.

동적 라우팅

관리 전용 라우팅 테이블에서는 데이터 인터페이스 라우팅 테이블과 별도로 동적 라우팅을 지원합니다. 지정된 동적 라우팅 프로세스는 관리 전용 인터페이스 또는 데이터 인터페이스에서 실행해야 합니다. 두 유형을 혼용할 수는 없습니다.

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.

경로 맵 정보

경로 맵은 경로를 OSPF, RIP, EIGRP 또는 BGP 라우팅 프로세스로 재배포할 때 사용됩니다. 또한 OSPF 라우팅 프로세스로 기본 경로를 생성할 때도 사용됩니다. 경로 맵은 지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 정의합니다.

경로 맵은 널리 알려진 ACL과 여러 기능을 공유합니다. 다음은 두 가지에서 모두 일반적인 특성입니다.

- 이들은 순서가 정해진 개별 구문이며 각각 허용 또는 거부라는 결과를 갖습니다. ACL 또는 경로 맵의 평가는 사전 정의된 순서에 따른 목록 스캔과 그에 일치하는 각 구문의 기준에 대한 평가로

구성됩니다. 목록 스캔은 첫 번째 구문 일치가 발견되고 해당 구문 일치와 연결된 작업이 수행되면 중단됩니다.

- 이들은 일반 메커니즘입니다. 기준 일치와 일치 해석은 적용되는 방식과 이를 사용하는 기능에 따라 정해집니다. 같은 경로 맵이라도 다른 기능에 적용되면 다르게 해석될 수 있습니다.

다음은 경로 맵과 ACL의 차이점입니다.

- 경로 맵은 ACL보다 유연하며 ACL이 확인할 수 없는 기준으로 경로를 확인할 수 있습니다. 예를 들어 경로 맵은 경로 유형이 내부인지 확인할 수 있습니다.
- 각 ACL은 설계 관행에 따라 암시적 거부 문구로 종료됩니다. 일치 시도 중에 경로 맵의 끝에 도달하는 경우 결과는 경로 맵의 애플리케이션이 무엇인지에 따라 달라집니다. 재배포에 적용되는 경로 맵은 ACL과 동일하게 작동합니다. 경로가 경로 맵의 조항과 일치하지 않으면 마치 경로 맵이 끝에 거부 구문을 포함한 것처럼 경로 재배포가 거부됩니다.

허용 및 거부 절

경로 맵은 허용 및 거부 절을 가질 수 있습니다. 거부 절은 재배포에서 경로 일치를 거부합니다. 경로 맵의 일치 기준으로 ACL을 사용할 수 있습니다. ACL에도 허용 및 거부 절이 있으므로 패킷이 ACL과 일치하는 경우 다음 규칙이 적용됩니다.

- ACL 허용 + 경로 맵 허용: 경로가 재배포됩니다.
- ACL 허용 + 경로 맵 거부: 경로가 재배포되지 않습니다.
- ACL 거부 + 경로 맵 허용 또는 거부: 경로 맵 절이 일치하지 않으며 다음 경로 맵 절이 평가됩니다.

절의 일치 및 설정 값

각 경로 맵 절은 두 가지 값을 갖습니다.

- 일치 값은 이 절을 적용할 경로를 선택합니다.
- 설정 값은 대상 프로토콜로 재배포될 정보를 수정합니다.

재배포되는 각 경로에 대해 라우터는 먼저 경로 맵에 있는 절의 일치 기준을 평가합니다. 일치 기준이 성공하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부되고 set 명령에서 설정된 값으로 일부 속성이 수정될 수 있습니다. 일치 기준이 실패하면 이 절은 경로에 적용되지 않고 소프트웨어가 경로 맵의 다음 절에 대해 경로를 평가합니다. 절이 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 스캔이 계속됩니다.

다음 조건 중 하나가 존재할 경우 각 절의 일치 또는 설정 값은 누락되거나 여러 번 반복될 수 있습니다.

- 절에 여러 match 항목이 존재하는 경우 주어진 경로에 대해 모두 성공해야 경로가 절에 일치할 수 있습니다(논리 AND 알고리즘이 여러 일치 명령에 적용됨).
- match 항목이 하나의 항목에서 여러 개체를 참조하는 경우 둘 중 하나가 일치해야 합니다(논리 OR 알고리즘 적용).

- match 항목이 존재하지 않으면 모든 경로가 절과 일치합니다.
- set 항목이 경로 맵 허용 절에 없는 경우 현재 속성의 수정 없이 경로가 재배포됩니다.

참고 경로 맵의 set 항목이 절을 거부하도록 구성하지 마십시오. 거부 절은 경로 재배포를 금지하므로 수정할 정보가 없기 때문입니다.

match 또는 set 항목이 없는 경로 맵 절이 작업을 수행합니다. 빈 허용 절은 수정 없이 남은 경로의 재배포를 허용합니다. 빈 거부 절은 다른 경로의 재배포를 허용하지 않습니다(경로 맵을 완전히 스캔했으나 정확한 match 항목을 찾지 못한 경우 이것이 기본 작업).