Firepower Threat Defense 정적 및 기본 경로

이 장에서는 FTD에서 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 FTD 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.

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 FTD 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) 라우팅를 참조하십시오.
- 터널링 옵션을 사용하여 터널로부터 생성된 트래픽의 경우 이 경로는 구성되었거나 학습된 다른 기본 경로를 무시합니다.

투명 방화벽 모드 및 브리지 그룹 경로

Firepower Threat Defense 디바이스에서 발생하고 브리지 그룹 멤버 인터페이스를 거쳐 직접 연결되지 않은 네트워크로 가는 트래픽의 경우, 기본 경로 또는 고정 경로를 구성하여 Firepower Threat Defense 디바이스에서 어떤 브리지 그룹 멤버 인터페이스로 트래픽을 보낼지 알 수 있게 해야 합니다. Firepower Threat Defense 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 MAC 주소 대 경로 조회 비교를 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 Firepower Threat Defense 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.

Firepower Threat Defense 디바이스에서는 Firepower Threat Defense 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 Firepower Threat Defense 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

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(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.

IPv6

- 고정 경로 추적은 IPv6에서 지원되지 않습니다.

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.

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 FTD 디바이스를 수정합니다.

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, FMC는 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.

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 모니터 개체의 내용을 참조하십시오.

단계 **13** **Ok(**확인**)**를 클릭합니다.