네트워크 맵 사용

다음 주제에서는 네트워크 맵을 사용하는 방법을 설명합니다.

네트워크 맵 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf

사용자 역할

- 관리자
- 검색 관리자

네트워크 맵

Firepower System은 네트워크를 통해 이동하는 트래픽을 모니터링하고, 트래픽 데이터를 디코딩한 다음 데이터를 설정된 운영체제 및 핑거프린트와 비교합니다. 그런 다음 시스템은 이 데이터를 사용하여 네트워크 맵이라고 하는, 네트워크의 자세한 표현을 작성합니다. 다중 도메인 구축의 경우, 시스템은 각 리프 도메인에 대한 개별 네트워크 맵을 생성합니다.

시스템은 네트워크 검색 정책에서 모니터링용으로 식별된 매니지드 디바이스에서 데이터를 수집합니다. 매지니드 디바이스는 네트워크 자산을 모니터링하는 트래픽에서는 직접적으로, 처리된 NetFlow

기록에서는 간접적으로 탐지합니다. 여러 디바이스가 동일한 네트워크 자산을 탐지하면 시스템은 하나의 복합 자산 표현으로 정보를 결합합니다.

수동 탐지에서 데이터를 보강하는 방법은 다음과 같습니다.

- 오픈 소스 스캐너인 Nmap™을 이용해 호스트를 적극적으로 스캔하고, 스캔 결과를 네트워크 맵에 추가합니다.
- 호스트 입력 기능을 이용해 타사 애플리케이션의 호스트 데이터를 수동으로 추가합니다.

네트워크 맵은 탐지한 호스트 및 네트워크 디바이스를 중심으로 네트워크 토폴로지를 표시합니다.

네트워크 맵을 사용하면 다음 작업을 수행할 수 있습니다.

- 전체 네트워크를 빠르게 확인.
- 수행할 분석에 맞게 각기 다른 보기 선택. 네트워크 맵의 각 보기는 확장 가능한 카테고리 및 하위 카테고리가 있는 계층적 트리의 동일한 형식을 가지고 있습니다. 카테고리를 클릭하면 그 아래의 하위 카테고리가 표시되도록 카테고리가 확장됩니다.
- 맞춤형 토폴로지 기능을 통해 서브넷 구성 및 식별. 예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 맞춤형 토폴로지 기능을 사용하여 친숙한 레이블을 서브넷에 할당할 수 있습니다.
- 임의의 모니터링 호스트의 호스트 프로파일로 드릴다운하여 상세 정보 확인
- 더 이상 조사하지 않으려는 자산 삭제

참고 네트워크 맵에서 삭제된 호스트와 관련된 활동이 탐지되면, 해당 호스트는 네트워크 맵에 다시 추가됩니다. 마찬가지로, 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하면 삭제된 애플리케이션이 네트워크 맵에 다시 추가됩니다. 호스트를 취약하게 만드는 변경 사항이 탐지되면 특정 호스트에서 취약성이 다시 활성화됩니다.

팁 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오. 과도하거나 관련 없는 이벤트를 생성하는 것으로 확인된 로드 밸런서와 NAT 디바이스는 모니터링에서 제외할 수 있습니다.

관련 항목

네트워크 검색 정책 설정

호스트 네트워크 맵

Hosts(호스트) 탭의 네트워크 맵은 호스트 카운트와 호스트 IP 주소 및 기본 MAC 주소 목록을 표시합니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다. 이 네트워크 맵 보기는 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 호스트의 카운트를 제공합니다.

호스트 네트워크 맵을 사용하면 계층적 트리에 서브넷으로 구성된 네트워크의 호스트를 볼 수 있으며, 특정 호스트에 대한 호스트 프로파일로 드릴다운할 수도 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

네트워크에 대한 맞춤형 토폴로지를 생성하면, 부서 이름과 같은 의미 있는 레이블(예: 부서 이름)을 서브넷에 할당할 수 있으며, 이는 호스트 네트워크 맵에 나타납니다. 또한 맞춤형 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.

호스트 네트워크 맵에서 전체 네트워크, 서브넷 또는 개별 호스트를 삭제할 수 있습니다. 특정 호스트가 네트워크에 더 이상 연결되어 있지 않음을 알고 있다면 분석을 간소화하기 위해 해당 호스트를 삭제할 수 있습니다. 삭제된 호스트와 관련된 활동이 이후에 탐지되면 해당 호스트는 네트워크 맵에 다시 추가됩니다. 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오.

주의 네트워크 맵에서 네트워크 디바이스를 삭제하지 마십시오. 시스템은 이러한 디바이스를 이용해 네트워크 토폴로지를 확인합니다.

호스트 네트워크 맵 페이지에서는 기본 MAC 주소만 검색할 수 있으며, Hosts [MAC] 카운트에는 기본 MAC 주소만 포함됩니다. 기본 및 보조 MAC 주소에 대한 설명은 호스트 프로파일의 기본 호스트 정보 섹션을 참조하십시오.

네트워크 디바이스 네트워크 맵

Network Devices(네트워크 디바이스) 탭의 네트워크 맵은 네트워크의 세그먼트를 다른 세그먼트와 연결하는 네트워크 디바이스(브리지, 라우터, NAT 디바이스, 로드 밸런서)를 표시합니다. 맵에는 IP 주소로 식별한 디바이스를 나열하는 섹션과 MAC 주소로 식별한 디바이스를 나열하는 섹션이 있습니다.

또한 맵은 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 네트워크 디바이스의 카운트도 제공합니다.

네트워크에 대해 맞춤형 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 네트워크 디바이스 네트워크 맵에 나타납니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스가 CDP를 사용하여 통신하는 경우 IP 주소가 하나 이상일 수 있습니다. STP를 사용하여 통신하는 경우 MAC 주소가 하나뿐일 수 있습니다.

네트워크 맵에서는 네트워크 디바이스를 삭제할 수 없습니다. 시스템은 이러한 디바이스의 위치를 이용해 네트워크 토폴로지를 결정하기 때문입니다.

네트워크 디바이스의 호스트 프로파일에는 Operating Systems 섹션이 아닌 Systems 섹션이 있습니다. 여기에는 네트워크 디바이스 뒤에서 탐지되는 모바일 디바이스에 대한 하드웨어 플랫폼을 반영하는 Hardware 열이 포함됩니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

모바일 디바이스 네트워크 맵

Mobile Devices(모바일 디바이스) 탭의 네트워크 맵은 네트워크에 연결된 모바일 디바이스를 표시합니다. 이 네트워크 맵은 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 모바일 디바이스의 카운트도 제공합니다.

각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다. 서브넷이나 IP 주소를 삭제할 수도 있습니다. 시스템이 디바이스를 다시 검색하면, 디바이스는 네트워크 맵에 다시 추가됩니다.

드릴다운을 통해 모바일 디바이스에 대한 호스트 프로파일을 확인할 수도 있습니다.

모바일 디바이스 식별을 위해 시스템은 다음을 수행합니다.

- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 User-Agent(사용자 에이전트) 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크에 대해 맞춤형 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 모바일 디바이스 네트워크 맵에 나타납니다.

보안 침해 지표 네트워크 맵

Indications of Compromise(보안 침해 지표) 탭의 네트워크 맵은 IOC 카테고리별로 조직화된, 네트워크 상의 침해된 호스트를 표시합니다. 영향받는 호스트는 각 카테고리 아래에 나열됩니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다.

IOC 네트워크 맵에서는 특정 방법으로 침해된 것으로 판단된 각 호스트의 호스트 프로파일을 볼 수 있습니다. 특정 IOC 카테고리 또는 특정 호스트를 삭제(또는 해결된 것으로 표시)할 수 있는데, 그렇게 하면 관련 호스트에서 IOC 태그가 제거됩니다. 예를 들어 문제가 해결되어 재발하지 않을 것으로 판단한 경우 네트워크 맵에서 IOC 카테고리를 삭제할 수 있습니다.

네트워크 맵에서 호스트 또는 IOC 카테고리를 해결된 것으로 표시하더라도 해당 항목이 네트워크에서 제거되지는 않습니다. 해당 IOC를 트리거하는 정보가 새로 탐지되면 네트워크 맵에 해결된 호스트 또는 IOC 카테고리가 다시 나타납니다.

시스템이 보안 침해 지표를 결정하는 방법에 대한 자세한 내용은 보안 침해 지표 데이터 및 하위 항목을 참조하십시오.

애플리케이션 프로토콜 네트워크 맵

Application Protocols(애플리케이션 프로토콜) 탭의 네트워크 맵은 애플리케이션 이름, 벤더, 버전별로, 그리고 마지막에는 각 애플리케이션을 실행하는 호스트별로 계층형 트리에 구성되어 있는, 네트워크 상의 애플리케이션을 표시합니다.

시스템 소프트웨어와 VDB가 업데이트되는 경우, 그리고 애드온 탐지기를 가져오는 경우 시스템에서 탐지하는 애플리케이션이 변경될 수 있습니다. 각 시스템 또는 VDB 업데이트에 대한 릴리스 정보나 자문 텍스트에는 새 탐지기 및 업데이트된 탐지기에 대한 정보가 포함되어 있습니다. 포괄적인 최신 탐지기 목록은 Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)를 참조하십시오.

이 네트워크 맵에서는 특정 애플리케이션을 실행하는 각 호스트의 호스트 프로파일을 확인할 수 있습니다.

또한 모든 애플리케이션 카테고리, 모든 호스트에서 실행 중인 모든 애플리케이션, 특정 호스트에서 실행 중인 모든 애플리케이션을 삭제할 수 있습니다. 예를 들어 애플리케이션이 호스트에서 비활성화된 것을 알고 있으며 시스템이 영향 레벨 자격에 애플리케이션을 사용하지 않도록 하려면 네트워크 맵에서 해당 애플리케이션을 삭제할 수 있습니다.

네트워크 맵에서 애플리케이션을 삭제해도 네트워크에서 제거되지는 않습니다. 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하거나 시스템의 검색 기능을 다시 시작하는 경우 삭제된 애플리케이션이 네트워크 맵에 다시 나타납니다.

삭제한 내용에 따라 동작이 달라집니다.

- 애플리케이션 카테고리 - 삭제하면 네트워크 맵에서 애플리케이션 카테고리가 제거됩니다. 카테고리에 속하는 모든 애플리케이션이 해당 호스트 프로파일에서 제거됩니다.

  예를 들어 **http**를 삭제하면 **http**로 식별되는 모든 애플리케이션이 모든 호스트 프로파일에서 제거되며, 네트워크 맵의 애플리케이션 보기에 **http**가 더 이상 나타나지 않습니다.

- 특정 애플리케이션, 벤더 또는 버전 - 삭제하면 영향받는 애플리케이션이 네트워크 맵 및 해당 호스트 프로파일에서 제거됩니다.

  예를 들어 **http** 카테고리를 확장하고 **Apache**를 삭제하면, Apache 아래에 나열된 버전과 상관없이 Apache로서 나열된 모든 애플리케이션이 해당 호스트 프로파일에서 제거됩니다. 마찬가지로, **Apache**를 삭제하는 대신 특정 버전(예: **1.3.17**)을 삭제하면 선택한 버전만이 영향받는 호스트 프로파일에서 삭제됩니다.

- 특정 IP 주소 - 삭제하면 애플리케이션 목록에서 해당 IP 주소가 제거되며, 선택한 IP 주소의 호스트 프로파일에서 애플리케이션 자체도 제거됩니다.

  예를 들어 **http**, **Apache**, **1.3.17(Win32)**을 확장한 다음 **172.16.1.50:80/tcp**를 삭제하면 Apache 1.3.17(Win32) 애플리케이션이 IP 주소 172.16.1.50의 호스트 프로파일에서 삭제됩니다.

취약성 네트워크 맵

Vulnerabilities(취약성) 탭의 네트워크 맵은 시스템이 네트워크에서 탐지한 취약성을 레거시 취약성 ID(SVID), CVE ID 또는 Snort ID별로 조직화해 표시합니다.

이 네트워크 맵에서는 특정 취약성의 상세정보와, 특정 취약성에 대한 호스트의 호스트 프로파일을 확인할 수 있습니다. 이 정보는 해당 취약성이 영향받는 특정 호스트에 미치는 위협을 평가하는 데 도움이 됩니다.

특정 취약성이 (패치 적용 등의 이유로) 네트워크의 호스트에 영향을 미치지 않는 것 같다면 해당 취약성을 비활성화할 수 있습니다. 비활성화된 취약성은 여전히 네트워크 맵에 나타나지만 영향받는 이전 호스트의 IP 주소는 회색의 기울임꼴로 나타납니다. 그러한 호스트의 호스트 프로파일은 비활성화된 취약성을 무효 상태로 표시합니다(개별 호스트에 대해 수동으로 취약성을 유효 상태로 표시할 수는 있음).

호스트에서 애플리케이션이나 운영체제의 ID 충돌이 있는 경우 시스템은 잠재적인 두 ID에 대한 취약성을 나열합니다. ID 충돌이 해결되면 취약성과 현재 ID의 연결 상태가 유지됩니다.

기본적으로, 패킷에 애플리케이션의 벤더 및 버전이 포함된 경우에만 네트워크 맵에 탐지된 애플리케이션의 취약성이 표시됩니다. 그러나 Firepower Management Center 설정에서 애플리케이션에 대한 취약성 매핑 설정을 활성화함으로써, 벤더 및 버전 데이터가 없는 애플리케이션에 대한 취약성을 나열하도록 시스템을 구성할 수 있습니다.

취약성 ID(또는 취약성 ID의 범위) 옆에 있는 숫자는 두 개의 카운트를 나타냅니다.

영향받은 호스트

첫 번째 숫자는 취약성의 영향을 받는 고유하지 않은 호스트의 카운트입니다. 하나의 호스트가 둘 이상의 취약성에 의해 영향을 받으면 여러 번으로 계산됩니다. 따라서 카운트가 네트워크에 있는 호스트의 수보다 클 수 있습니다. 취약성을 비활성화하면 해당 취약성의 영향을 받을 가능성이 있는 호스트의 수만큼 이 카운트가 줄어듭니다. 취약성 또는 취약성 범위의 영향을 받을 가능성이 있는 호스트에 대해 취약성을 비활성화하지 않은 경우 이 카운트가 표시되지 않습니다.

영향받았을 가능성이 있는 호스트

두 번째 숫자는 시스템이 취약성의 영향을 받을 가능성이 있는 것으로 판단한, 고유하지 않은 총 호스트의 카운트입니다.

취약성을 비활성화하면 지정한 호스트에 대해서만 비활성이 적용됩니다. 취약한 것으로 판단한 모든 호스트에 대해 또는 취약한 개별 지정 호스트에 대해 취약성을 비활성화할 수 있습니다. 취약성이 비활성화되면, 해당하는 호스트의 IP 주소가 네트워크 맵에서 회색 기울임꼴로 표시됩니다. 또한 그러한 호스트의 호스트 프로파일에는 비활성화된 취약성이 무효 상태로 표시됩니다.

그 후 비활성화되지 않은 호스트(예: 네트워크 맵의 새 호스트)에서 취약성이 탐지되면, 시스템은 해당 호스트에 대해 취약성을 활성화합니다. 새로 검색된 취약성은 명시적으로 비활성화해야 합니다. 또한 호스트에 대해 운영체제 또는 애플리케이션 변경이 탐지되면 시스템은 비활성화된 관련 취약성을 다시 활성화할 수 있습니다.

호스트 속성 네트워크 맵

Host Attributes(호스트 속성) 탭의 네트워크 맵은 네트워크 상의 호스트를 사용자 정의 또는 규정준수 화이트 목록 호스트 속성 중 하나를 기준으로 조직화해 표시합니다. 이 화면에서는 사전 정의된 호스트 속성을 이용해 호스트를 조직화할 수는 없습니다.

호스트를 구성하는 데 사용할 호스트 속성을 선택하면, Firepower Management Center은(는) 네트워크 맵에서 해당 특성에 대해 사용할 수 있는 값을 나열하고 할당된 값을 기반으로 호스트를 그룹화합니다. 예를 들어 화이트 목록 호스트 속성을 기준으로 호스트를 조직화하는 경우, 시스템은 호스트를 Compliant(규정준수), Non-Compliant(규정 미준수), Not Evaluated(미평가) 카테고리로 구분해 표시합니다.

또한 특정 호스트 속성 값이 할당된 호스트의 호스트 프로파일을 볼 수도 있습니다.

관련 항목

호스트 프로파일의 호스트 속성

네트워크 맵 보기

네트워크 맵을 보려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**를 선택합니다.

단계 **2** 보려는 네트워크 맵을 클릭합니다.

단계 **3** 해당하는 작업을 계속 진행합니다.

- 도메인 선택 — 다중 도메인 환경의 경우, **Domain(**도메인**)** 드롭다운 목록에서 리프 도메인을 선택합니다.
- 호스트 필터링 — IP 주소 또는 MAC 주소로 필터링하려는 경우, 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기( )을 클릭합니다.
- 드릴다운 — 카테고리 또는 호스트 프로파일을 조사하려는 경우, 맵의 카테고리 또는 서브넷을 드릴다운합니다. 맞춤형 토폴로지가 정의된 경우 보려는 **Hosts(**호스트**)**에서 **(topology)(**토폴로지**)**를 클릭한 다음, 기본 보기로 다시 토글하려면 **(hosts)(**호스트**)**를 클릭합니다.
- 삭제 — 해당 요소 옆에 있는 삭제( )을 클릭합니다.
  - **Hosts(**호스트**)**, **Network Devices(**네트워크 디바이스**)**, **Mobile Devices(**모바일 디바이스**)** 또는 **Application Protocols(**애플리케이션 프로토콜**)** 의 맵에서 요소를 제거합니다.
  - **Indications of Compromise(**보안 침해 지표**)**에서 확인된 IOC 카테고리, 보안 침해된 호스트 또는 보안 침해된 호스트 그룹을 표시합니다.
  - **Vulnerabilities(**취약점**)**에서 모든 호스트 또는 단일 호스트의 취약점을 비활성화합니다.
- 취약점 등급 지정 — **Vulnerabilities(**취약점**)**의 **Type(**유형**)** 드롭다운 목록에서 보려는 취약점 등급을 선택합니다.

- 구성 속성 지정 — **Host Attributes(**호스트 속성**)**의 **Attribute(**속성**)** 드롭다운 목록에서 속성을 선택합니다.

관련 항목

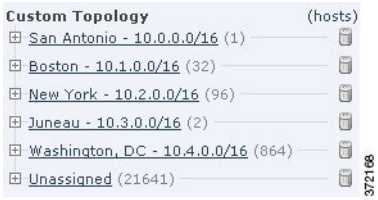
맞춤형 네트워크 토폴로지, 8 페이지
호스트 프로파일

맞춤형 네트워크 토폴로지

맞춤형 토폴로지 기능을 사용하면 호스트 및 네트워크 디바이스 네트워크 맵에서 서브넷을 구성 및 식별하는 데 도움이 될 수 있습니다.

예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 맞춤형 토폴로지 기능을 사용하여 서브넷에 레이블을 지정할 수 있습니다.

또한 사용자 정의 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.



다음 방법 중 하나 또는 모두를 사용하여 맞춤형 토폴로지의 네트워크를 지정할 수 있습니다.

- 네트워크 검색 정책에서 네트워크를 가져와 시스템이 모니터링하도록 설정한 네트워크에 추가할 수 있습니다.
- 네트워크를 수동으로 네트워크 토폴로지에 추가할 수 있습니다.

Custom Topology(맞춤형 토폴로지) 페이지는 맞춤형 토폴로지와 토폴로지의 상태를 열거합니다. 정책 이름 옆에 있는 전구 아이콘이 밝게 표시되면 토폴로지가 활성 상태이며 네트워크 맵에 영향을 미치게 됩니다. 아이콘 흐리게 표시된다면, 토폴로지는 비활성 상태입니다.

관련 항목

호스트 네트워크 맵, 2 페이지
네트워크 디바이스 네트워크 맵, 3 페이지

맞춤형 토폴로지 생성

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** 툴바에서 **Custom Topology(**맞춤형 토폴로지**)**를 클릭합니다.

단계 **3** **Create Topology(**토폴로지 생성**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 네트워크를 토폴로지에 추가합니다. 다음의 전략 중 하나 또는 모두를 사용할 수 있습니다.

- 네트워크 검색 정책에서 네트워크 가져오기, 9 페이지에 설명된 대로 네트워크 검색 정책에서 네트워크를 가져옵니다.
- 맞춤형 토폴로지에 수동으로 네트워크 추가, 10 페이지에 설명된 대로 네트워크를 수동으로 추가합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 10 페이지에 설명된 대로 토폴로지를 활성화합니다.

네트워크 검색 정책에서 네트워크 가져오기

프로시저

단계 **1** 네트워크를 가져올 맞춤형 토폴로지에 액세스합니다.

- 맞춤형 토폴로지를 생성합니다(맞춤형 토폴로지 생성, 8 페이지 참조).
- 기존 맞춤형 토폴로지를 편집합니다(맞춤형 토폴로지 편집, 11 페이지 참조).

단계 **2** **Import Policy Networks(**정책 네트워크 가져오기**)**를 클릭합니다.

단계 **3** **Load(**로드**)**를 클릭합니다. 시스템은 네트워크 검색 정책에 대한 토폴로지 정보를 표시합니다.

단계 **4** 토폴로지를 정리하려면

- 네트워크 옆에 있는 수정( )을 클릭하고, 이름을 입력하고, **Rename(**이름 변경**)**을 클릭해 토폴로지의 네트워크 이름을 변경합니다.
- 삭제( )을 클릭하고 **OK(**확인**)**를 클릭해 토폴로지에서 네트워크를 제거합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 10 페이지에 설명된 대로 토폴로지를 활성화합니다.

맞춤형 토폴로지에 수동으로 네트워크 추가

프로시저

단계 **1** 네트워크를 추가할 맞춤형 토폴로지에 액세스합니다.

- 맞춤형 토폴로지를 생성합니다(맞춤형 토폴로지 생성, 8 페이지 참조).
- 기존 맞춤형 토폴로지를 편집합니다(맞춤형 토폴로지 편집, 11 페이지 참조).

단계 **2** **Add Network(**네트워크 추가**)**를 클릭합니다.

단계 **3** 호스트 및 네트워크 디바이스 네트워크 맵에 네트워크에 대한 맞춤형 라벨을 추가하려면, **Name(**이름**)**을 입력합니다.

단계 **4** 추가할 네트워크를 나타내는 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**(IPv4)를 입력합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 10 페이지에 설명된 대로 토폴로지를 활성화합니다.

관련 항목

Firepower System IP 주소 규칙

맞춤형 토폴로지 활성화 및 비활성화

참고 언제든 하나의 맞춤형 토폴로지만 활성 상태를 유지할 수 있습니다. 여러 토폴로지를 생성한 경우 하나를 활성화하면 현재 활성 상태인 토폴로지는 자동으로 비활성화됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Topology(**맞춤형 토폴로지**)**를 선택합니다.

단계 **3** 토폴로지 옆에 있는 슬라이더를 클릭하여 토폴로지를 활성화 또는 비활성화합니다.

맞춤형 토폴로지 편집

활성 토폴로지에 적용한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Topology(**맞춤형 토폴로지**)**를 클릭합니다.

단계 **3** 편집할 토폴로지 옆에 있는 수정( )을 클릭합니다.

단계 **4** 맞춤형 토폴로지 생성, 8 페이지에 설명된 대로 토폴로지를 편집합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.