



네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정

다음 주제에서는 네트워크 분석 및 침입 정책에 대한 고급 설정 구성 방법을 설명합니다.

- [네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정 정보, 1 페이지](#)
- [네트워크 분석 및 침입 정책에 대한 고급 액세스 제어 설정 요구 사항 및 사전 요건, 1 페이지](#)
- [트래픽이 식별되기 전에 통과하는 패킷 검사, 2 페이지](#)
- [네트워크 분석 정책 고급 설정, 4 페이지](#)

네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정 정보

액세스 제어 정책의 고급 설정 대부분은 구성을 위한 특정 전문성을 요구하는 침입 탐지 및 방지 구성을 제어합니다. 고급 설정은 일반적으로 거의 또는 전혀 수정할 필요가 없으며 모든 배포에 공통적으로 적용하지는 않습니다.

네트워크 분석 및 침입 정책에 대한 고급 액세스 제어 설정 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

트래픽이 식별되기 전에 통과하는 패킷 검사

URL 필터링, 애플리케이션 탐지, 속도 제한 및 지능형 애플리케이션 우회를 비롯한 일부 기능의 경우, 연결을 설정하고 시스템에서 트래픽을 식별하고 어떤 액세스 제어 규칙(있을 경우)이 해당 트래픽을 처리할지 결정할 수 있도록 하려면 몇 개의 패킷이 통과해야 합니다.

액세스 제어 정책을 명시적으로 설정하여 이러한 패킷을 검사하고 패킷이 대상에 도달하는 것을 방지하고 이벤트를 생성해야 합니다. [트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정, 3 페이지](#)의 내용을 참조하십시오.

시스템이 액세스 제어 규칙 또는 연결을 처리해야 하는 기본 작업을 확인하면, 연결의 나머지 패킷이 처리되고 그에 따라 검사됩니다.

트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례

- 액세스 제어 정책에 대해 지정된 기본 작업은 이러한 패킷에 적용되지 않습니다.
- 대신 다음 지침을 사용하여 액세스 제어 정책의 고급 설정에서 액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책의 값을 선택합니다.
 - 시스템에서 생성한 정책 또는 맞춤형 침입 정책을 선택할 수 있습니다. 예를 들어 **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결)를 선택할 수 있습니다.
 - 성능상의 이유로 특별한 이유가 없는 한 이 설정은 액세스 제어 정책에 대해 설정된 기본 작업과 일치해야 합니다.
 - 시스템이 침입 검사를 수행하지 않는 경우(예: 검색 전용 구축) **No Rules Active**(활성 규칙 없음)를 선택합니다. 시스템은 이러한 초기 패킷을 검사하지 않으며 통과할 수 있습니다.
 - 기본적으로 이 설정은 기본 변수 집합을 사용합니다. 이것이 용도에 적합한지 확인하십시오. 자세한 내용은 [변수 집합](#)를 참조하십시오.
 - 처음으로 일치하는 네트워크 분석 규칙과 관련된 네트워크 분석 정책은 사용자가 선택하는 정책에 대한 트래픽을 사전 처리합니다. No 네트워크 분석 규칙 또는 none(없음)가 일치, 경우 기본 네트워크 분석 정책에 사용 됩니다.

트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정





참고 이 설정을 기본 침입 정책이라고도 합니다. (액세스 제어 정책에 대한 기본 작업과는 다릅니다.)

시작하기 전에


이러한 설정에 대한 모범 사례를 검토합니다. [트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례, 2 페이지](#)의 내용을 참조하십시오.


프로시저

단계 1 액세스 제어 정책 편집기에서 **Advanced**(고급)를 클릭하고 **Network Analysis**(네트워크 분석) 및 **Intrusion Policies**(침입 정책) 섹션 옆에 있는 **Edit**(수정) ()을 클릭합니다.

보기 아이콘(**View**(보기) ()이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy**(기본 정책에서 상속)의 선택을 취소하여 수정을 활성화합니다.

단계 2 **Intrusion Policy used before Access Control rule is determined**(액세스 컨트롤 규칙이 결정되기 전에 사용된 침입 정책) 드롭다운 목록에서 침입 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, **Edit**(수정) ()을 클릭하여 새 창에서 정책을 편집할 수 있습니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 3 **Intrusion Policy Variable Set**(침입 정책 변수 집합) 드롭다운 목록에서 다른 변수 집합을 선택하는 방법도 있습니다. 또는 변수 집합 옆에 있는 **Edit**(수정) ()을 선택하여 변수 집합을 생성하고 편집해도 됩니다. 사용자가 변수 집합을 변경하지 않는 경우, 시스템은 기본 집합을 사용합니다.

단계 4 **OK**(확인)를 클릭합니다.

단계 5 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- **Deploy configuration changes**(구성 변경 사항 구축), [Firepower Management Center 관리 가이드](#) 참조.

관련 항목

[변수 집합](#)

네트워크 분석 정책 고급 설정

네트워크 분석 정책은 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽을 향후에 평가할 수 있도록 트래픽을 해독하고 전처리하는 방법을 제어합니다. 이러한 트래픽 전처리는 보안 인텔리전스 매칭 및 트래픽 해독이 수행된 후 하지만 침입 정책이 패킷을 세부적으로 검사하기 전에 이루어집니다. 기본적으로, 시스템이 제공한 **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본 네트워크 정책이 됩니다.



팁 시스템이 제공하는 **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 **Balanced Security and Connectivity**(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트할 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다. 복합적인 배포를 사용하는 고급 사용자의 경우, 다수의 네트워크 분석 정책을 생성할 수 있는데, 각각은 트래픽을 다르게 전처리하기 위해 조정된 것입니다. 그런 다음 이러한 정책을 사용하도록 시스템을 구성하여 서로 다른 보안 영역, 네트워크 또는 VLAN을 사용하는 트래픽의 전처리를 제어할 수 있습니다.

이를 수행하려면, 액세스 제어 정책에 사용자 지정 네트워크 분석 규칙을 추가합니다. 네트워크 분석 규칙은 해당 자격과 일치하는 트래픽을 어떻게 전처리할지 단순히 지정한 일련의 구성과 조건입니다. 사용자는 기존의 액세스 제어 정책의 고급 옵션에서 네트워크 분석 규칙을 만들고 수정합니다. 각 규칙은 하나의 정책에만 속합니다.

각 규칙에는 다음이 포함되어 있습니다.

- 전처리하려는 특정 트래픽을 확인하는 일련의 규칙 조건
- 모든 규칙의 조건을 충족하는 트래픽을 전처리하는 데 사용하려는 결합된 네트워크 분석 정책

시스템이 트래픽을 전처리할 시간이 되면, 큰 규칙 번호에서 작은 번호 순서로 패킷을 네트워크 분석 규칙에 일치시킵니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.


기본 네트워크 분석 정책 설정


시스템에서 생성된 정책 또는 사용자가 생성한 정책을 선택할 수 있습니다.




참고 전처리기를 비활성화했지만 시스템이 활성화된 침입 또는 전처리기 규칙에 대해 전처리한 패킷을 평가해야 하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 비활성화 상태로 남아 있는 상태라 해도 시스템은 전처리기를 자동으로 활성화하여 사용합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 반드시 주의하여 서로 보완하는 단일 패킷을 검토하는 네트워크 분석 및 침입 정책을 허용해야 합니다.

프로시저

단계 1 액세스 컨트롤 정책 편집기에서 **Advanced(고급)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 **Edit(수정)** ()을 클릭합니다.

보기 아이콘(**View(보기)** ()이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(기본 정책에서 상속)**의 선택을 취소하여 수정을 활성화합니다.

단계 2 **Default Network Analysis Policy(기본 네트워크 분석 정책)** 드롭다운 목록에서 기본 네트워크 분석 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, **Edit(수정)** ()을 클릭하여 새 창에서 정책을 편집할 수 있습니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 3 **OK(확인)**를 클릭합니다.

단계 4 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축), [Firepower Management Center 관리 가이드 참조](#).

관련 항목

[사용자 지정 정책의 한계](#)

네트워크 분석 규칙

액세스 제어 정책의 고급 설정에서, 네트워크 분석 규칙을 사용하여 네트워크 트래픽에 대한 전처리 구성을 맞춤화할 수 있습니다.

네트워크 분석 규칙은 1부터 번호가 지정됩니다. 시스템이 트래픽을 전처리할 시간이 되면, 오름차순 규칙 번호가 적어지는 순서로 패킷을 네트워크 분석 규칙에 일치시키며, 모든 규칙의 조건이 일치하는 첫 번째 규칙에 따라 트래픽을 전처리합니다.

규칙에 영역, 네트워크 및 VLAN 태그 조건을 추가할 수 있습니다. 규칙에 대해 특정 조건을 구성하지 않으면 시스템은 해당 기준에 따라 트래픽을 매칭하지 않습니다. 예를 들어, 네트워크 조건은 있지만 영역 조건이 없는 규칙의 경우 인그레스 또는 이그레스 인터페이스에 상관없이 소스 또는 대상 IP 주소에 따라 트래픽을 평가합니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

네트워크 분석 정책 규칙 조건

규칙 조건을 사용하면 제어하려는 사용자 및 네트워크를 대상으로 네트워크 분석 정책을 미세 조정할 수 있습니다. 자세한 내용은 다음 섹션 중 하나를 참조하십시오.

관련 항목

[보안 영역 규칙 조건](#)

[네트워크 규칙 조건](#)

[VLAN 태그 규칙 조건](#)

보안 영역 규칙 조건

보안 영역은 네트워크를 세그멘테이션화하여 여러 디바이스에 걸쳐 인터페이스를 그룹화하는 방법을 통해 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다.

영역 규칙의 조건은 소스 및 대상 보안 영역을 통해 트래픽을 제어합니다. 소스 및 대상 영역 모두 영역 조건에 추가할 경우 소스 영역 중 하나의 인터페이스에서 트래픽 매치를 시작하고 대상 영역 중 하나의 인터페이스에서 종료해야 합니다.

영역의 모든 인터페이스가 동일한 유형이어야 하는 것과 마찬가지로(모든 인라인, 수동, 스위칭 또는 라우팅), 영역 조건에 사용된 모든 영역도 동일한 유형이어야 합니다. 패시브 방식으로 구축된 디바이스는 트래픽을 전송하지 않으므로 패시브 인터페이스를 대상 영역으로 하면서 영역을 사용할 수 없습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.



팁 영역으로 규칙을 제한하는 것은 시스템 성능을 개선할 수 있는 가장 좋은 방법 중 하나입니다. 규칙이 디바이스의 인터페이스를 통과하는 트래픽에 적용되지 않을 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

보안 영역 조건 및 멀티테넌시

다중 도메인 구축에서, 상위 도메인에 생성된 영역은 다른 도메인의 디바이스에 있는 인터페이스를 포함할 수 있습니다. 하위 도메인의 영역 조건을 구성할 경우, 컨피그레이션은 사용자가 볼 수 있는 인터페이스에만 적용됩니다.

네트워크 규칙 조건

네트워크 규칙 조건은 내부 헤더를 사용하여 트래픽의 소스 및 대상 IP 주소를 기준으로 삼아 트래픽을 제어합니다. 외부 헤더를 사용하는 터널 규칙에는 네트워크 조건 대신 터널 엔드포인트 조건이 있습니다.

사전 정의된 개체를 사용하여 네트워크 조건을 작성하거나, 수동으로 개별 IP 주소 또는 주소 블록을 지정할 수 있습니다.



참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

VLAN 태그 규칙 조건



참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. VLAN 태그가 있는 액세스 규칙은 방화벽 인터페이스의 트래픽과 일치하지 않습니다.

VLAN 규칙 조건은 Q-in-Q(스택 VLAN) 트래픽을 포함한 VLAN 태그가 있는 트래픽을 제어합니다. 시스템은 가장 안쪽의 VLAN 태그를 사용하여 VLAN 트래픽을 필터링하며, 규칙에서 가장 바깥쪽의 VLAN 태그를 사용하는 사전 필터 정책은 예외입니다.

다음 Q-in-Q 지원에 유의하십시오.

- Firepower 4100/9300의 FTD - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 다른 모든 모델의 FTD:
 - 인라인 집합 및 패시브 인터페이스 - Q-in-Q를 지원합니다(최대 2개의 VLAN 태그 지원).
 - 방화벽 인터페이스 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).

사전 정의된 개체를 사용하여 VLAN 조건을 작성하거나, 1에서 4094 사이의 VLAN 태그를 수동으로 입력할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

최대 50개의 VLAN 조건을 지정할 수 있습니다.

클러스터에서 VLAN 일치에 문제가 발생하면 액세스 제어 정책 고급 옵션인 Transport/Network Preprocessor Settings(전송/네트워크 전처리기 구성)를 편집하고 **Ignore VLAN header when tracking connections**(연결 추적 시 VLAN 헤더 무시) 옵션을 선택합니다.



참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

네트워크 분석 규칙 설정

프로시저

단계 1 액세스 컨트롤 정책 편집기에서 **Advanced**(고급)를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 **Edit**(수정) (✎)을 클릭합니다.

보기 아이콘(**View**(보기) (🔍))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy**(기본 정책에서 상속)의 선택을 취소하여 수정을 활성화합니다.

팁 **Network Analysis Policy List**(네트워크 분석 정책 목록)를 클릭해 기존 맞춤형 네트워크 분석 정책을 확인하고 편집합니다.

단계 2 **Network Analysis Rules**(네트워크 분석 규칙) 옆에 있는 보유하고 있는 사용자 지정 규칙의 수를 표시하는 문장을 클릭합니다.

단계 3 **Add Rule**(규칙 추가)을 클릭합니다.

단계 4 추가할 조건을 클릭해 규칙 조건을 설정합니다. [네트워크 분석 규칙 설정, 8 페이지](#)을 참조하십시오.

단계 5 **Network Analysis**(네트워크 분석)을 클릭하고 이 규칙과 일치하는 트래픽을 전처리하는 데 사용할 **Network Analysis Policy**(네트워크 분석 정책)를 선택합니다.

Edit(수정) (✎)을 클릭해 새 창에서 맞춤형 정책을 편집합니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 6 **Add**(추가)를 클릭합니다.

다음에 수행할 작업


- Deploy configuration changes(구성 변경 사항 구축), [Firepower Management Center 관리 가이드](#) 참조.

네트워크 분석 규칙 관리

네트워크 분석 규칙은 해당 자격과 일치하는 트래픽을 어떻게 전처리할지 단순히 지정한 일련의 구성과 조건입니다. 사용자는 기존의 액세스 제어 정책의 고급 옵션에서 네트워크 분석 규칙을 만들고 수정합니다. 각 규칙은 하나의 정책에만 속합니다.



프로시저

단계 1 액세스 컨트롤 정책 편집기에서 **Advanced**(고급)을 클릭하고 Intrusion and Network Analysis Policies(침입 및 네트워크 분석 정책) 섹션 옆에 있는 **Edit**(수정) (✎)을 클릭합니다.

보기 아이콘(**View**(보기) ())이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy**(기본 정책에서 상속)의 선택을 취소하여 수정을 활성화합니다.

단계 2 Network Analysis Rules(네트워크 분석 규칙) 옆에 있는 보유하고 있는 사용자 지정 규칙의 수를 표시하는 문장을 클릭합니다.

단계 3 사용자 지정 규칙을 수정합니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 조건을 수정하거나 규칙에 의해 호출된 네트워크 분석 정책을 변경하기 위해서는 규칙 옆에 있는 **Edit**(수정) ()을 클릭합니다.
- 규칙의 평가 순서를 변경하려면, 정확한 위치에 규칙을 클릭하여 끌어옵니다. 여러 규칙을 선택하려면 **Shift**와 **Ctrl** 키를 사용합니다.
- 규칙을 삭제하려면 규칙 옆에 있는 **Delete**(삭제) ()을 클릭합니다.

팁 마우스 오른쪽 버튼으로 규칙을 클릭하면 새로운 네트워크 분석 규칙을 잘라내기, 복사, 붙여넣기, 편집, 삭제, 추가할 수 있는 컨텍스트 메뉴가 표시됩니다.

단계 4 OK(확인)를 클릭합니다.

단계 5 Save를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- **Deploy configuration changes**(구성 변경 사항 구축), [Firepower Management Center 관리 가이드 참조](#).

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.