규칙 관리: 일반 특성

다음 주제에서는 Firepower Management Center의 다양한 정책에 있는 규칙의 일반 특성을 관리하는 방법에 대해 설명합니다.

규칙 관리 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

규칙 소개

다양한 정책의 규칙은 네트워크 트래픽에 대해 세분화된 제어를 시행합니다. 시스템은 사용자가 지정한 순서에 따라 첫 번째 일치 알고리즘을 사용해 규칙에 대한 트래픽을 평가합니다.

이러한 규칙은 다음과 같은 기본 특성 및 설정 메커니즘을 공유하는 일치하지 않는 정책 간의 다른 설정을 포함할 수 있습니다.

- 조건: 규칙 조건은 각 규칙을 처리하는 특정 트래픽을 지정합니다. 규칙마다 여러 조건을 구성할 수 있습니다. 트래픽은 규칙과 일치하는 모든 조건과 일치해야 합니다.
- 작업: 규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 규칙에 선택할 수 있는 작업 목록이 포함되지 않더라도 규칙과 관련된 작업이 있습니다. 예를 들어 사용자 지정 네트워크 분석 규칙은 "작업"으로 네트워크 분석 정책을 사용합니다. 다른 예로 모든 QoS 규칙이 동일하게 제한 트래픽을 평가하므로 QoS 규칙에는 명시적인 작업이 없습니다
- 위치: 규칙의 위치는 평가 순서를 결정합니다. 트래픽 평가에 정책을 사용할 경우 시스템은 트래픽이 사용자가 지정한 순서에 따른 규칙과 일치하는지 확인합니다. 일반적으로 시스템은 모든 규칙 조건이 트래픽과 일치하는 첫 번째 규칙에 따라 트래픽을 처리합니다. (추적 및 기록용인 모니터링 규칙은 예외입니다.) 적절한 규칙 순서는 네트워크 트래픽 처리에 필요한 리소스를 줄여 규칙 선점을 방지합니다.
- 범주: 일부 규칙 유형을 구조화하기 위해 각 상위 정책에서 사용자 지정 규칙 카테고리를 만들 수 있습니다.
- 로깅: 많은 규칙의 경우 로깅 설정은 규칙에 의해 처리되는 시스템 로그 연결 여부 및 그 방법을 제어합니다. 규칙이 최종 연결 속성을 결정하거나 특별히 연결을 기록하도록 되어있지 않으므로 일부 규칙(ID 및 네트워크 분석 규칙 등)은 로깅 설정을 포함하지 않습니다. 다른 예로 QoS 규칙은 로깅 설정을 포함하지 않습니다. 속도 제한이 있으므로 연결 기록을 할 수 없습니다.
- 설명: 일부 규칙 유형은 변경 사항을 저장할 때마다 설명을 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다.

팁 여러 정책 편집기의 오른쪽 클릭 메뉴는 편집, 삭제, 이동, 활성화 및 비활성화를 비롯해 많은 규칙 관리 옵션에 대한 바로 가기를 제공합니다.

공유 특성이 포함된 규칙

이 장에서 다음 규칙 및 구성에 대한 여러 공통 측면을 다룹니다. 비공유 설정에 대한 내용은 다음을 참조하십시오.

- 액세스 제어 규칙: 액세스 제어 규칙
- SSL 규칙: TLS/SSL 규칙 생성 및 수정
- DNS 규칙: DNS 규칙 생성 및 편집

- ID 규칙: ID 규칙 생성
- 네트워크 분석 규칙: 네트워크 분석 규칙 설정
- QoS 규칙: QoS 규칙 구성
- IAB(Intelligent Application Bypass): IAB(Intelligent Application Bypass)
- 애플리케이션 필터: 애플리케이션 필터

공유 속성 없는 규칙 -

이 장에 설명되지 않은 설정 규칙은 다음과 같습니다.

- 침입 규칙: 규칙을 사용하여 침입 정책 조정
- 파일 및 악성코드 규칙: 파일 규칙
- 상관관계 규칙: 상관관계 규칙 설정
- NAT 규칙(기본): 7000 및 8000 Series 디바이스용 NAT
- NAT 규칙(Firepower Threat Defense): Firepower Threat Defense용 NAT(네트워크 주소 변환)
- 8000 Series 빠른 경로(Fast-Path) 규칙: 빠른 경로 규칙(8000 Series) 설정

규칙 조건 유형

다음 표에는 이 장에 나오는 일반 규칙 조건이 설명되어 있으며, 이러한 조건이 사용되는 컨피그레이션이 나열되어 있습니다.

조건	트래픽 제어 기준	지원되는 규칙/컨피그레이션
보안 영역 조건, 6 페이지	소스 및 대상 보안 영역	액세스 제어 규칙 SSL 규칙 DNS 규칙 ID 규칙 네트워크 분석 규칙
네트워크 조건, 7 페이지	소스 및 대상 IP 주소, (지원되는 경우) 지리위치	액세스 제어 규칙 SSL 규칙 DNS 규칙 ID 규칙 네트워크 분석 규칙 QoS 규칙

조건	트래픽 제어 기준	지원되는 규칙/컨피그레이션
VLAN 조건, 9 페이지	VLAN 태그	액세스 제어 규칙 참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다. SSL 규칙 DNS 규칙 ID 규칙 네트워크 분석 규칙
포트 및 ICMP 코드 조건, 10 페이지	소스 및 대상 포트, 프로토콜, ICMP 코드	액세스 제어 규칙 SSL 규칙 ID 규칙 QoS 규칙
애플리케이션 조건(애플리케이션 컨트롤), 12 페이지	애플리케이션 또는 애플리케이션 특성(유형, 위험, 사업 타당성, 카테고리 및 태그)	액세스 제어 규칙 SSL 규칙 ID 규칙 QoS 규칙 애플리케이션 필터 IAB(Intelligent Application Bypass)
URL 조건(URL 필터링), 23 페이지	URL, 지원되는 영역, URL 특성(카테고리 및 평판)	액세스 제어 규칙 SSL 규칙 QoS 규칙
사용자, 영역 및 ISE 속성 조건(사용자 제어), 23 페이지	호스트의 로그인한 권한 있는 사용자 또는 사용자의 영역, 그룹 또는 ISE 속성	액세스 제어 규칙 SSL 규칙(ISE 속성 없음) QoS 규칙

규칙 조건 메커니즘

규칙 조건은 각 규칙이 처리하는 트래픽을 지정합니다. 다양한 조건에 맞는 각 규칙을 설정하고 트래픽은 규칙과 일치하는 모든 조건에 일치해야 합니다. 사용할 수 있는 조건 유형은 규칙 유형에 따라 다릅니다.

규칙 편집기에는 각 조건 유형의 탭이 있습니다. 일치시키려는 트래픽 속성을 선택하여 조건을 구성합니다. 일반적으로 왼쪽에서 하나 또는 두 목록의 사용 가능한 항목 중 기준을 선택한 뒤 해당 기준을 오른쪽에서 선택한 하나 또는 두 항목의 조건에 추가하거나 결합합니다. 예를 들어 액세스 제어 규칙의 URL 조건에서 URL 카테고리와 평판 기준을 결합하여 블록할 단일 웹 사이트 그룹을 생성할 수 있습니다.

조건을 구축하기 위해 영역, ISE 속성, 다양한 유형의 개체 및 개체 그룹을 포함해 시스템이 제공하는 다양한 사용자 지정 설정을 사용해 트래픽을 일치시킬 수 있습니다. 종종 사용자가 수동으로 규칙 기준을 지정할 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.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

소스 및 대상 기준

소스 및 대상 기준(영역, 네트워크, 포트)과 관련된 규칙의 경우 일반적으로 둘 중 하나 또는 두 제약 기준 모두를 사용할 수 있습니다. 두 제약 기준 모두를 사용하는 경우 일치하는 트래픽은 지정된 소스 영역, 네트워크, 포트 중 하나에서 생성되고 대상 영역, 네트워크, 포트를 통과해야 합니다.

조건당 항목

각 조건에 최대 50개의 항목을 추가할 수 있습니다. 소스 및 대상 기준 규칙은 각각 최대 50개까지 사용할 수 있습니다. 선택된 항목과 일치하는 트래픽은 조건과 일치해야 합니다.

간단한 규칙 메커니즘

규칙 편집기에서 다음과 같은 일반적인 선택을 할 수 있습니다. 조건 구성에 대한 자세한 지침은 각 조건 유형에 대한 항목을 참고하십시오.

- 항목 선택 - 항목을 클릭하거나 해당 항목의 확인란을 선택합니다. Ctrl 또는 Shift를 사용해 여러 항목을 선택하거나 모두 선택하려면 오른쪽 클릭을 사용할 수 있습니다.
- 검색 - 검색 필드에 기준을 입력합니다. 입력하면 항목이 업데이트됩니다. 시스템은 항목 이름 및 개체, 개체 그룹, 그 값을 검색합니다. 다시 로드( ) 또는 지우기( )을 클릭하여 검색 내용을 삭제합니다.
- 사전 정의된 항목 추가 - 하나 이상의 사용 가능한 항목을 선택한 후 추가 버튼을 클릭하거나 드래그 앤 드롭을 사용합니다. 시스템은 중복, 유효하지 않은 조합 등 유효하지 않은 항목을 추가하지 않도록 방지합니다.
- 직접 항목 추가 - 선택한 항목 목록의 필드를 클릭하고 유효한 값을 입력한 뒤 추가를 클릭합니다. 포트를 추가하는 경우 드롭다운 목록에서 프로토콜을 선택할 수도 있습니다.
- 개체 생성 - 추가( )을 클릭하여 구성 중인 조건에 즉시 사용할 수 있는 새롭거나 재사용할 수 있는 개체를 생성하고 개체 관리자에서 관리할 수 있습니다. 상황에 따라 애플리케이션 필터를 추가하기 위해 이 방법을 사용할 경우 다른 사용자 생성 필터를 포함하는 필터를 저장할 수 없습니다.
- 삭제 - 한 항목을 삭제하는 경우 삭제( )을 클릭하거나 선택한 항목 삭제를 하려는 경우 오른쪽 클릭으로 하나 이상의 항목을 선택합니다.

보안 영역 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, 라우팅 또는 ASA FirePOWER), 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.

보안 영역 조건이 포함된 규칙

다음 규칙은 보안 영역 조건을 지원합니다.

- 액세스 제어
- SSL
- DNS(소스 영역 제약 조건만)
- ID
- 네트워크 분석

예: 보안 영역을 사용한 액세스 제어

호스트에 인터넷에 대한 무제한 액세스를 허용하더라도 수신 트래픽에서 침입 및 악성코드를 검사하여 호스트를 보호하는 경우의 구축을 고려하십시오.

우선, 내부 및 외부의 보안 영역 2개를 생성합니다. 그런 다음, 하나 이상의 디바이스에 있는 인터페이스 쌍을 이러한 영역에 할당합니다. 각 쌍의 인터페이스 하나는 내부 영역에, 다른 인터페이스 하나는 외부 영역에 할당합니다. 내부에서 네트워크에 연결된 호스트는 보호된 자산을 나타냅니다.

참고 모든 내부 (또는 외부) 인터페이스를 단일 영역으로 그룹화할 필요는 없습니다. 구축 및 보안 정책에 알맞은 그룹화를 선택합니다.

그런 다음 대상 영역 조건을 Internal로 설정한 액세스 제어 규칙을 구성합니다. 이 단순한 규칙은 내부 영역 내의 모든 인터페이스에서 디바이스를 나가는 트래픽과 일치됩니다. 일치하는 트래픽에서 침입 및 악성코드를 검사하려면 **Allow(**허용**)** 규칙 작업을 선택한 다음 해당 규칙을 침입 및 파일 정책과 연결합니다.

네트워크 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.

네트워크 조건의 지리위치

어떤 규칙은 소스 또는 대상의 지리위치 정보를 사용하여 트래픽을 매치할 수 있습니다. 규칙 유형이 지리위치를 지원할 경우, 네트워크와 지리위치 기준을 혼합할 수 있습니다. 최신 지리위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(Geolocation Database)를 정기적으로 업데이트하는 것이 좋습니다.

네트워크 조건이 포함된 규칙

규칙 유형	지리위치 제약 조건 지원 여부
액세스 제어	예
SSL	예
DNS(소스 네트워크만)	아니요
Identity(ID)	예
네트워크 분석	아니요

네트워크 조건 구성

프로시저

단계 **1** 규칙 편집기에서 **Networks(**네트워크**)**를 클릭합니다.

단계 **2** **Available Networks(**사용 가능한 네트워크**)** 목록에서 추가하려는 사전 정의된 네트워크를 찾아 선택합니다.

규칙이 지리위치를 지원할 경우 네트워크와 지리위치 기준을 동일 규칙에 병합할 수 있습니다.

- 네트워크 - 네트워크를 선택하려면 **Networks(**네트워크**)**를 클릭합니다.
- 지리위치 - 지리위치 개체를 선택하려면 **Geolocation(**지리위치**)**를 클릭합니다.

단계 **3** **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**를 클릭하거나 드래그 앤 드롭을 사용합니다.

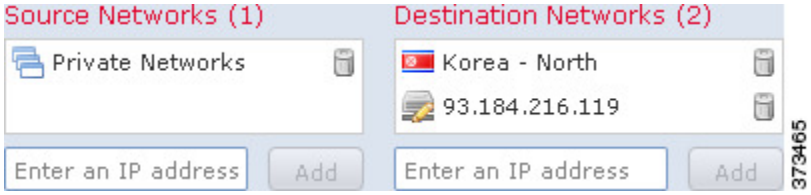
단계 **4** 수동 지정을 원하는 네트워크를 추가합니다. 소스 또는 대상 IP 주소 또는 주소 블록을 입력하고 추가를 클릭합니다.

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.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

예: 액세스 제어 규칙의 네트워크 조건

다음 그림은 사용자의 내부 네트워크에서 시작해 북한 또는 93.184.216.119(example.com)의 리소스에 액세스를 시도하는 연결을 차단하는 액세스 제어 규칙에 대한 네트워크 조건을 보여줍니다.



이 예에서 (보이지 않는 IPv4 및 IPv6 Private Networks 네트워크 개체로 구성된) Private Networks라는 네트워크 개체 그룹은 사용자의 내부 네트워크를 나타냅니다. 또한 이 예에서는 example.com의 IP 주소를 수동으로 특정하고 북한 IP 주소를 대신해 시스템이 제공한 북한 지리위치 개체를 사용합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

VLAN 조건

VLAN 규칙 조건은 Q-in-Q(스택 VLAN) 트래픽을 포함한 VLAN 태그가 있는 트래픽을 제어합니다. 시스템은 가장 안쪽의 VLAN 태그를 사용하여 VLAN 트래픽을 필터링하며.

다음 Q-in-Q 지원에 유의하십시오.

- NGIPSv, Firepower 7000, Firepower 8000 - 모든 인터페이스 유형에 Q-in-Q를 지원합니다.
- ASA FirePOWER 모듈 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- Firepower 4100/9300의 FTD - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 기타 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, **1**에서 **4094** 사이의 VLAN 태그를 수동으로 입력할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

최대 50개의 VLAN 조건을 지정할 수 있습니다.

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.

VLAN 조건이 포함된 규칙

다음 규칙 유형은 VLAN 조건을 지원합니다.

• 액세스 제어

참고 , 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. 방화벽 인터페이스에 적용된 액세스 규칙에는 사용할 수 없습니다.

• SSL

• DNS

• ID

• 네트워크 분석

포트 및 **ICMP** 코드 조건

포트 조건을 사용하면 소스 및 대상 포트를 기준으로 트래픽을 제어할 수 있습니다. 규칙 유형에 따라, "포트"는 다음 중 하나를 나타낼 수 있습니다.

• TCP 및 UDP — 전송 레이어 프로토콜을 기준으로 TCP 및 UDP 트래픽을 제어할 수 있습니다. 시스템은 괄호 내 프로토콜 번호와 선택적으로 결합된 포트 또는 포트 범위를 사용하여 이 구성을 나타냅니다. 예: TCP(6)/22

• ICMP — 인터넷 레이어 프로토콜과 선택적 유형 및 코드에 따라 ICMP 및 ICMPv6(IPv6-ICMP) 트래픽을 제어할 수 있습니다. 예: ICMP(1):3:3

• 포트 없음 — 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 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.

포트 기반 규칙 모범 사례

포트를 지정하는 것은 애플리케이션을 대상으로 하는 기존의 방법입니다. 그러나 고유한 포트를 사용하여 액세스 제어 블록을 우회하도록 애플리케이션을 설정할 수 있습니다. 따라서 트래픽을 대상으로 지정하려면 가능한 경우 항상 포트 기준 대신 애플리케이션 필터링 기준을 사용하십시오.

FTD와 같이 제어와 데이터 흐름을 위해 별도의 채널을 동적으로 여는 애플리케이션에도 애플리케이션 필터링이 권장됩니다. 포트 기반 액세스 제어 규칙을 사용하면 이러한 종류의 애플리케이션이 올바르게 작동하지 못하게 되어 적절한 연결이 차단될 수 있습니다.

소스 및 대상 포트 제약 조건 사용

소스 및 대상 포트 제약 조건을 모두 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

소스 포트만 또는 대상 포트만 추가할 경우 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 소스 포트 조건으로 추가할 수 있습니다.

비 **TCP** 트래픽을 포트 조건과 일치

비 TCP 트래픽과 일치하도록 포트 조건을 구성할 수 있지만, 몇 가지 제한 사항이 있습니다.

- 액세스 제어 규칙 - GRE(47) 프로토콜을 대상 포트 조건으로 사용하는 방법으로 GRE 캡슐화 트래픽을 액세스 제어 규칙과 매치할 수 있습니다. GRE 제한 규칙에는 네트워크 기반 조건(영역, IP 주소, 포트, VLAN 태그)만 추가할 수 있습니다. 또한, 시스템은 외부 헤더를 사용하여 액세스 제어 정책의 모든 트래픽을 GRE 제한 규칙과 일치시킵니다.
- SSL 규칙 — SSL 규칙은 TCP 포트 조건만 지원합니다.
- ⚠

  주의 SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오.

  액티브 인증 규칙에는 **Active Authentication(**액티브 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있음에 유의하십시오.
- IMCP 에코 - 대상 ICMP 포트의 유형이 0으로 설정되었거나 대상 ICMPv6 포트의 유형이 129로 설정된 경우 요청하지 않은 에코 응답만 매치합니다. ICMP 에코 요청에 대한 응답으로 전송된 ICMP 에코 응답은 무시됩니다. 모든 ICMP 에코에 일치하는 규칙의 경우, ICMP 유형 8 또는 ICMPv6 유형 128을 사용합니다.

포트 조건이 포함된 규칙

다음 규칙은 포트 조건을 지원합니다.

- 액세스 제어
- SSL(TCP 트래픽만 지원)
- ID(액티브 인증은 TCP 트래픽만 지원)
- QoS

포트 조건 구성

프로시저

단계 **1** 규칙 편집기에서 **Ports(**포트**)**를 클릭합니다.

단계 **2** **Available Ports(**사용 가능한 포트**)** 목록에서 추가하려는 사전 정의된 포트를 찾아 선택합니다.

단계 **3** **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**을 클릭하거나 끌어서 놓습니다.

단계 **4** 직접 지정하려는 소스 포트 또는 대상 포트를 추가합니다.

- 소스—프로토콜을 선택하고 0 ~ 65535 범위에서 단일 포트를 입력한 다음 **Add(**추가**)**를 클릭합니다.
- 대상(비 ICMP)—프로토콜을 선택하거나 입력합니다. 프로토콜을 지정하고 싶지 않거나 **TCP** 또는 **UDP**를 선택할 경우 0 ~ 65535 범위에서 단일 포트를 입력합니다. **Add(**추가**)**를 클릭합니다.
- 대상(ICMP)— **Protocol(**프로토콜**)** 드롭다운 목록에서 **ICMP** 또는 **IPv6-ICMP**를 선택한 다음 팝업 창이 나타나면 유형 및 코드를 선택합니다. ICMP 유형 및 코드에 대한 자세한 내용은 IANA(Internet Assigned Numbers Authority) 웹사이트를 참조하십시오.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

애플리케이션 조건(애플리케이션 컨트롤)

시스템에서 IP 트래픽을 분석할 때, 사용자의 네트워크에서 자주 사용되는 애플리케이션을 식별하여 분류할 수 있습니다. 이 검색 기반 애플리케이션 인식은 애플리케이션 컨트롤을 위한 기본 요소로, 애플리케이션 트래픽을 제어하는 기능입니다.

시스템에서 제공되는 애플리케이션 필터는 유형, 위험, 사업 타당성, 카테고리, 태그라는 기본 특성에 따라 애플리케이션을 구성하여 애플리케이션 컨트롤을 수행할 수 있도록 지원합니다. 시스템에서 제공되는 필터를 조합하거나 애플리케이션을 맞춤형으로 조합하여 재사용 가능한 사용자 정의 필터를 생성할 수 있습니다.

정책의 애플리케이션 규칙 조건마다 적어도 하나의 탐지기가 활성화되어야 합니다. 애플리케이션에 탐지기가 활성화되지 않은 경우, 시스템은 시스템에서 제공된 모든 탐지기를 해당 애플리케이션에 자동으로 활성화합니다. 시스템에서 제공된 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 활성화합니다. 애플리케이션 탐지기에 대한 자세한 내용은 애플리케이션 탐지기 기초을 참조하십시오.

두 애플리케이션 필터를 모두 사용하거나 개별적으로 지정된 애플리케이션을 사용하여 완전한 커버리지를 보장할 수 있습니다. 그러나 액세스 제어 규칙 순서를 지정하기 전에 다음을 참고하십시오.

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

애플리케이션 필터의 이점

애플리케이션 필터는 애플리케이션 컨트롤을 신속하게 구성하는 데 도움이 됩니다. 예를 들어 시스템에서 제공되는 필터를 손쉽게 사용하여 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하고 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 시스템에서는 해당 세션을 차단합니다.

애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 애플리케이션 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 애플리케이션 탐지기를 자주 업데이트하고 추가하므로, 시스템에서는 최신 탐지기를 사용하여 애플리케이션 트래픽을 모니터링할 수 있습니다. 자체 탐지기를 생성하고 이러한 탐지기로 탐지한 애플리케이션에 특성을 할당할 수도 있으며, 이는 기존 필터에 자동으로 추가됩니다.

애플리케이션 조건이 포함된 컨피그레이션

다음 표의 컨피그레이션은 애플리케이션 컨트롤을 수행하는 데 도움이 됩니다. 이 표에는 컨피그레이션에 따라 애플리케이션 컨트롤을 제한할 수 있는 방법도 나와 있습니다.

컨피그레이션	유형,위험,타당성,카테고리	태그	사용자 정의 필터
액세스 제어 규칙	예	예	예

컨피그레이션	유형,위험,타당성,카테고리	태그	사용자 정의 필터
SSL 규칙	예	아니요. SSL 프로토콜 태그를 통해 암호화된 애플리케이션 트래픽에 자동으로 제한됨	아니요
IID 규칙(액티브 인증에서 애플리케이션을 제외할 목적)	예	아니요. User-Agent Exclusion 태그를 통해 자동으로 제한됨	아니요
개체 관리자의 사용자 정의 애플리케이션 필터	예	예	아니요. 사용자 정의 필터는 중첩할 수 없음
IAB(Intelligent Application Bypass)	예	예	예

관련 항목

개요: 애플리케이션 탐지

애플리케이션 조건 및 필터 구성

애플리케이션 조건 또는 필터를 구성하려면 사용 가능한 애플리케이션 목록에서 제어를 원하는 트래픽의 애플리케이션을 선택합니다. 선택적으로(권장 사항), 필터를 사용해 사용 가능한 애플리케이션을 제약합니다. 동일한 조건에서 필터 및 개별적으로 지정된 애플리케이션을 사용할 수 있습니다.

시작하기 전에

- 적응형 프로파일은 애플리케이션 제어를 수행하기 위해 적응형 프로파일 구성의 설명대로 액세스 제어 규칙에 대해 반드시 활성화가 되어 있어야 합니다.
- 클래식 디바이스 모델의 경우 이러한 조건을 설정하려면 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** 규칙 또는 구성 편집기를 호출합니다.

- 액세스 제어, SSL, QoS 규칙 조건 - 규칙 편집기에서 **Applications(**애플리케이션**)**을 클릭합니다.
- ID 규칙 조건 - 규칙 편집기에서 **Realms & Settings(**영역 및 설정**)**을 클릭하고 액티브 인증을 활성화하려면 ID 규칙 생성를 참조합니다.
- 애플리케이션 필터 - 개체 관리자의 애플리케이션 필터 페이지에서 애플리케이션 필터를 추가하거나 편집합니다. 필터의 고유 이름을 제공합니다.
- 인텔리전트 애플리케이션 우회(IAB) - 액세스 제어 정책 편집기에서 **Advanced(**고급**)**을 클릭하고 IAB 세팅을 편집한 뒤 **Bypassable Applications and Filters(**우회 가능한 애플리케이션 및 필터**)**를 클릭합니다.

단계 **2** **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 추가하려는 애플리케이션을 찾아 선택합니다.

Available Applications(사용 가능한 애플리케이션**)**에 표시된 애플리케이션을 제한하기 위해 하나 이상의 **Application Filters(**애플리케이션 필터**)**를 선택하거나 개별 애플리케이션을 검색합니다.

팁 요약 정보 및 내부 검색 링크를 표시하기 위해 애플리케이션 옆의 정보() 을 클릭합니다. **Unlock(**잠금 해제**)**은 시스템이 암호화된 트래픽에서만 확인할 수 있는 애플리케이션을 표시합니다.

하나 또는 여러 필터를 선택할 때 사용 가능한 애플리케이션 목록은 조건에 맞는 애플리케이션만 표시합니다. 시스템에서 제공된 여러 필터를 선택할 수 있지만 사용자 지정 필터는 선택할 수 없습니다.

- 동일한 속성(위험, 비즈니스 연관성 등)에 대한 여러 필터 - 애플리케이션 트래픽은 하나의 필터에만 일치해야 합니다. 중간 또는 고위험 필터를 선택하는 경우 사용 가능한 애플리케이션 목록은 모든 중간 및 고위험 애플리케이션을 표시합니다.
- 다른 애플리케이션 속성에 대한 필터 - 애플리케이션 트래픽은 두 필터 유형에 모두 일치해야합니다. 예를 들어 고위험 및 비즈니스 연관성이 낮은 필터를 선택하는 경우 사용 가능한 애플리케이션 목록은 두 조건을 모두 만족하는 애플리케이션만을 표시합니다.

단계 **3** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

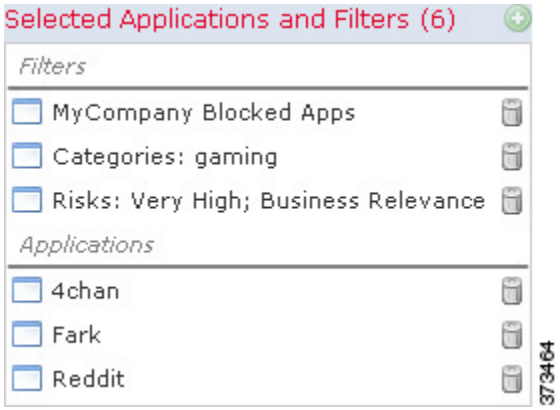
팁 더 많은 필터 및 애플리케이션을 추가하기 전에 현재 선택 사항을 지우려면 **Clear Filters(**필터 지우기**)**를 클릭합니다.

웹 인터페이스는 위의 조건에 추가된 필터 및 개별적으로 추가된 애플리케이션을 표시합니다.

단계 **4** 규칙 또는 설정을 저장하거나 편집합니다.

예**:** 액세스 제어 규칙의 애플리케이션 조건

다음 그림은 MyCompany, 위험도가 높고 비즈니스 연관성이 낮은 모든 애플리케이션, 게임 애플리케이션, 일부 개별 선택 애플리케이션에 대해 사용자 정의된 애플리케이션 필터를 차단하는 액세스 제어 규칙의 애플리케이션 조건을 표시합니다.



다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

애플리케이션 특성

시스템은 다음 표에서 설명하는 조건을 사용해 탐지하는 각 애플리케이션을 구별합니다. 애플리케이션 필터로 이러한 특성을 사용합니다.

표 *1:* 애플리케이션 특성

특성	설명	예
유형	애플리케이션 프로토콜은 호스트 간 통신을 나타냅니다. 클라이언트는 호스트에서 실행 중인 소프트웨어를 나타냅니다. 웹 애플리케이션은 HTTP 트래픽에 대한 콘텐츠 또한 요청 URL을 나타냅니다.	HTTP 및 SSH는 애플리케이션 프로토콜입니다. 웹 브라우저 및 이메일 클라이언트는 클라이언트입니다. MPEG 비디오 및 Facebook은 웹 애플리케이션입니다.
위험	애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성입니다.	피어 투 피어 애플리케이션은 고위험 경향이 있습니다.
사업 타당성	애플리케이션이 오락이 아닌 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성입니다.	게임 애플리케이션은 비즈니스 연관성이 매우 낮은 경향이 있습니다.
Category(카테고리)	가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.	Facebook은 소셜 네트워킹 카테고리에 포함됩니다.
Tag(태그)	애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.	비디오 스트리밍 웹 애플리케이션은 종종 높은 대역폭 및 광고 표시 태그가 지정됩니다.

애플리케이션 제어 모범 사례

애플리케이션 제어와 관련해서 다음의 지침과 제한 사항에 유의해야 합니다.

애플리케이션 탐지기 자동 활성화

탐지하려는 애플리케이션에 대해 탐지기를 사용하고 있지 않으면 시스템은 해당 애플리케이션에 대해 모든 시스템 제공 탐지기를 자동으로 사용합니다. 시스템 제공 탐지기가 없으면 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 대해 사용합니다.

애플리케이션이 식별되기 전에 통과해야 하는 패킷을 검사하도록 정책 설정

시스템은 다음의 두 가지 조건을 만족하지 않는 경우 인텔리전트 애플리케이션 우회(IAB) 및 속도 제한을 포함한 애플리케이션 제어를 수행할 수 없습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 애플리케이션 식별

이 식별은 3~5개 패킷 내에서 이루어지거나 트래픽이 암호화된 경우 SSL 핸드셰이크의 서버 인증 교환 이후에 이루어져야 합니다.

중요! 시스템에서 이러한 초기 패킷을 검사하도록 하려면 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정의 내용을 참조하십시오.

초기 트래픽이 기타 모든 기준과는 일치하는데 애플리케이션 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 또는 SSL 핸드셰이크 완료를 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 작업을 적용합니다.

URL 및 애플리케이션 필터링용 별도의 규칙 생성

애플리케이션과 URL 기준을 결합하면 특히 암호화된 트래픽에 대해 예기치 않은 결과가 발생할 수 있으므로 가능하면 URL 및 애플리케이션 필터링에 대한 별도의 규칙을 만듭니다.

애플리케이션+URL 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 애플리케이션 및 URL 기준을 모두 포함하는 규칙은 애플리케이션 전용 또는 URL 전용 규칙 뒤에 와야 합니다.

애플리케이션 및 기타 규칙 이전의 **URL** 규칙

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

암호화된 트래픽과 암호 해독된 트래픽에 대한 애플리케이션 제어

시스템은 암호화된 트래픽과 암호 해독된 트래픽을 식별하고 필터링할 수 있습니다.

- 암호화된 트래픽 - 시스템은 SMTPS, POPS, FTPS, TelnetS, IMAPS를 비롯하여 StartTLS로 암호화된 애플리케이션 트래픽을 탐지할 수 있습니다. 또한, TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서의 주체로 구별되는 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다. 이러한 애플리케이션은 `SSL` 프로토콜 태그가 지정됩니다. SSL 규칙에서는 이런 애플리케이션만 선택할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다.
- 암호 해독된 트래픽 - 시스템은 암호화되거나 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에 `decrypted traffic` 태그를 할당합니다.

TLS 서버 ID 검색 및 애플리케이션 제어

RFC 8446에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.

자세한 내용은 액세스 제어 정책 고급 설정를 참고하십시오.

활성 권한 부여에서 애플리케이션 제외

ID 정책에서는 특정 애플리케이션을 액티브 인증에서 제외하여 트래픽이 액세스 제어로 계속 이동하도록 허용할 수 있습니다. 이러한 애플리케이션에는 `User-Agent Exclusion` 태그가 지정됩니다. ID 규칙에서는 이러한 애플리케이션만 선택할 수 있습니다.

페이로드 없이 애플리케이션 트래픽 패킷 처리

액세스 제어를 수행할 때 시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.

참조된 애플리케이션 트래픽 처리

광고물 트래픽과 같이 웹 서버에서 참조된 트래픽을 처리하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션의 일치 여부를 확인합니다.

다중 프로토콜을 사용하는 애플리케이션(Skype, Zoho)의 애플리케이션 트래픽 제어

일부 애플리케이션은 다중 프로토콜을 사용합니다. 해당 트래픽을 제어하려면 액세스 제어 정책이 모든 관련 옵션을 포함하는지 확인합니다. 예를 들면 다음과 같습니다.

- Skype - Skype 트래픽을 제어하려면 개별 애플리케이션을 선택하는 대신 **Application Filters(**애플리케이션 필터**)** 항목에서 **Skype** 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다.
- Zoho - Zoho 메일을 제어하려면 사용 가능한 애플리케이션 목록에서 **Zoho** 및 **Zoho mail**을 모두 선택합니다.

콘텐츠 제한 기능용으로 지원되는 검색 엔진

시스템은 특정 검색 엔진에 대해서만 안전 검색 필터링을 지원합니다. 이러한 검색 엔진의 애플리케이션 트래픽에는 `safesearch supported` 태그가 할당됩니다.

우회 애플리케이션 트래픽 제어

애플리케이션 관련 참고 사항 및 제한 사항, 20 페이지의 내용을 참조하십시오.

애플리케이션 제어 순서 지정에 대한 추가 규칙

애플리케이션 제어 순서를 결정하는 규칙에 대한 지침은 애플리케이션 제어 구성 모범 사례, 19 페이지을 참조하십시오.

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사
애플리케이션 탐지 특별 고려 사항

애플리케이션 제어 구성 모범 사례

다음과 같이 네트워크에 대한 애플리케이션의 액세스를 제어하는 것이 좋습니다.

- 보안 수준이 낮은 네트워크에서 보안 수준이 높은 네트워크로 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Port(**포트**)** (Selected Destination Port)(선택한 대상 포트) 조건을 사용합니다.

  예를 들어, 인터넷(보안 수준 낮음)에서 내부 네트워크(보안 수준 높음)으로 ICMP 트래픽을 허용합니다.

- 사용자 그룹의 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Application(**애플리케이션**)** 조건을 사용합니다.

  예를 들어, 계약업체 그룹 구성원의 Facebook 액세스를 차단합니다.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

다음 표에서 액세스 제어 규칙을 설정하는 방법에 대한 예시가 제공됩니다.

제어의 유형	조치	영역, 네트워크, **VLAN** 태그	사용자	애플리케이션	포트	**URL**	**SGT/ISE** 속성	검사, 로깅, 코멘트
애플리케이션에서 포트(예: SSH)를 사용하는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow**(허용))	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	사용 가능한 포트: **SSH** **Selected Destination Ports**(선택한 대상 포트)에 추가	Any(모든)	ISE/ISE-PIC에만 사용합니다.	Any(모든)
애플리케이션에서 포트(예: ICMP)를 사용하지 않는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow**(허용))	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	선택한 대상 포트 프로토콜: **ICMP** **Type**(유형): **Any**(모든)	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	Any(모든)
사용자 그룹의 애플리케이션 액세스	선택(이 예에서는 **Block**(차단))	선택	사용자 그룹(이 예에서는 계약업체 그룹)을 선택합니다.	애플리케이션의 이름(이 예에서는 **Facebook**)을 선택합니다.	설정하지 마십시오.	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	선택

애플리케이션 관련 참고 사항 및 제한 사항

- Office 365 관리자 포털:

  제한 사항: 액세스 정책이 시작 및 종료 시 로깅을 활성화한 경우 첫 번째 패킷은 Office 365로 감지되고 연결 종료는 Office 365 관리자 포털로 감지됩니다. 이는 블로킹에 영향을 주지 않습니다.

- Skype:

  애플리케이션 제어 모범 사례, 16 페이지의 내용을 참조하십시오.

- GoToMeeting

  GoToMeeting을 완벽하게 탐지하려면 규칙에 다음 애플리케이션이 모두 있어야 합니다.

  - GoToMeeting

- Citrix Online
- Citrix GoToMeeting 플랫폼
- LogMeIn
- STUN

- Zoho:

  애플리케이션 제어 모범 사례, 16 페이지의 내용을 참조하십시오.

- Bittorrent, Tor, Psyphon, Ultrasurf 등의 우회 애플리케이션:

  우회 애플리케이션의 경우 기본적으로 가장 신뢰도가 높은 시나리오만 인식됩니다. 이 트래픽의 활동(차단 또는 QoS 구현 등)이 필요한 경우 효율성을 높이기 위해 더 적극적인 탐지 설정이 필요합니다. 이런 변경으로 오탐이 발생할 수 있으므로 이 작업을 수행하기 위해서는 설정을 검토하기 위한 TAC에 연결합니다.

- WeChat:

  WeChat을 허용하는 경우 선택적으로 WeChat Media를 차단할 수 없습니다.

애플리케이션 제어 규칙 문제 해결

애플리케이션 제어 규칙이 예상대로 작동하지 않는 경우 이 섹션에서 설명한 지침을 사용합니다.

다음과 같이 네트워크에 대한 애플리케이션의 액세스를 제어하는 것이 좋습니다.

- 보안 수준이 낮은 네트워크에서 보안 수준이 높은 네트워크로 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Port(**포트**)** (Selected Destination Port)(선택한 대상 포트) 조건을 사용합니다.

  예를 들어, 인터넷(보안 수준 낮음)에서 내부 네트워크(보안 수준 높음)으로 ICMP 트래픽을 허용합니다.

- 사용자 그룹의 애플리케이션 액세스를 허용하거나 차단하려면 액세스 제어 규칙에서 **Application(**애플리케이션**)** 조건을 사용합니다.

  예를 들어, 계약업체 그룹 구성원의 Facebook 액세스를 차단합니다.

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

다음 표에서 액세스 제어 규칙을 설정하는 방법에 대한 예시가 제공됩니다.

제어의 유형	조치	영역, 네트워크, **VLAN** 태그	사용자	애플리케이션	포트	**URL**	**SGT/ISE** 속성	검사, 로깅, 코멘트
애플리케이션에서 포트(예: SSH)를 사용하는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	사용 가능한 포트: **SSH** **Selected Destination Ports(**선택한 대상 포트**)**에 추가	Any(모든)	ISE/ISE-PIC에만 사용합니다.	Any(모든)
애플리케이션에서 포트(예: ICMP)를 사용하지 않는 경우 보안 수준이 높은 네트워크에서 보안 수준이 낮은 네트워크로 애플리케이션 액세스	선택(이 예에서는 **Allow(**허용**)**)	외부 인터페이스를 사용하는 대상 영역 또는 네트워크	Any(모든)	설정하지 마십시오.	선택한 대상 포트 프로토콜: **ICMP** **Type(**유형**)**: **Any (**모든**)**	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	Any(모든)

제어의 유형	조치	영역, 네트워크, VLAN 태그	사용자	애플리케이션	포트	URL	SGT/ISE 속성	검사, 로깅, 코멘트
사용자 그룹의 애플리케이션 액세스	선택(이 예에서는 **Block**(차단))	선택	사용자 그룹(이 예에서는 계약업체 그룹)을 선택합니다.	애플리케이션의 이름(이 예에서는 **Facebook**)을 선택합니다.	설정하지 마십시오.	설정하지 마십시오.	ISE/ISE-PIC에만 사용합니다.	선택

초기 패킷이 검사되지 않고 통과됨

트래픽이 식별되기 전에 통과하는 패킷 검사 및 하위 항목을 참조하십시오.

관련 항목

규칙 순서 지정 모범 사례

URL 조건(URL 필터링)

네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어하기 위해 URL 조건을 사용합니다.

자세한 내용은 URL 필터링를 참조하십시오.

사용자, 영역 및 ISE 속성 조건(사용자 제어)

Firepower System에서 수집한 권한 있는 사용자 *ID* 데이터로 사용자 제어를 수행할 수 있습니다.

ID 소스는 로그인 및 로그아웃하는 사용자를 모니터링하거나, 사용자가 Microsoft AD(Active Directory) 또는 LDAP 접속 정보를 사용하여 인증하는 사용자를 모니터링합니다. 그런 다음 이렇게 수집된 ID 데이터를 사용하는 규칙을 구성하여, 모니터링된 호스트와 관련된 로그인한 권한 있는 사용자를 기준으로 트래픽을 처리할 수 있습니다. 사용자가 로그오프하거나(ID 소스를 통해 보고됨), 영역의 세션 시간이 초과되거나, 시스템의 데이터베이스에서 사용자 데이터를 삭제할 때까지 사용자는 호스트에 계속 연결되어 있습니다.

현재 보유한 버전의 Firepower System에서 지원되는 권한 있는 사용자 ID 소스에 대한 자세한 내용은 사용자 ID 소스 정보를 참조하십시오.

다음 규칙 조건을 사용하여 사용자 제어를 수행할 수 있습니다.

- 사용자 및 영역 조건 — 호스트의 로그인한 권한 있는 사용자를 기준으로 트래픽을 일치시킵니다. 영역, 개별 사용자 또는 해당 사용자가 속한 그룹을 기준으로 트래픽을 제어할 수 있습니다.

- ISE 속성 조건 — 사용자의 ISE 할당 SGT(Security Group Tag), 디바이스 유형(엔드포인트 프로파일이라고도 함) 또는 위치 IP(엔드포인트 위치라고도 함)를 기준으로 트래픽을 일치시킵니다. ISE를 ID 소스로 구성해야 합니다.

참고 ISE-PIC ID 소스는 ISE 속성 데이터를 제공하지 않습니다.

사용자 조건이 포함된 규칙

규칙 유형	사용자 및 영역 조건 지원 여부	**ISE** 속성 조건 지원 여부
액세스 제어	예	예
SSL	예	아니요
QoS	예	예 SGT 매칭은 소스 매칭 기준으로만 지원되며, 대상 일치 기준은 지원되지 않습니다.

관련 항목

ISE/ISE-PIC ID 소스
캡티브 포털 ID 소스

사용자 제어 사전 요구 사항

ID 소스/인증 방법 구성

수행하려는 인증 유형에 대한 ID 소스를 구성합니다. 자세한 내용은 사용자 ID 소스 정보를 참고하십시오.

여러 사용자 그룹을 모니터링하기 위한 ISE 디바이스를 설정하는 경우, 또는 네트워크의 호스트에 다수의 사용자가 매핑된 경우, 시스템은 Firepower Management Center 사용자 제한에 따라 그룹을 기반으로 한 사용자 매핑이 삭제될 수 있습니다. 그 결과 영역, 사용자, 사용자 그룹 조건의 규칙은 정상적인 트래픽과 일치하지 않을 수 있습니다.

여러 사용자 그룹을 모니터링하기 위한 ISE/ISE/PIC 또는 TS 에이전트, ISE/ISE-PIC 디바이스를 설정하는 경우, 또는 네트워크의 호스트에 다수의 사용자가 매핑된 경우, 시스템은 Firepower Management Center 사용자 제한에 따라 그룹을 기반으로 한 사용자 매핑이 삭제될 수 있습니다. 그 결과 영역, 사용자, 사용자 그룹 조건의 규칙은 정상적인 트래픽과 일치하지 않을 수 있습니다.

영역 설정

ISE 서버를 포함해 모니터링하려는 각 AD 또는 LDAP 서버 영역을 설정하고 사용자 다운로드를 수행합니다. 자세한 내용은 영역 생성를 참고하십시오.

ISE/ISE-PIC 및 TS 에이전트 서버를 포함해 모니터링하려는 각 AD 또는 LDAP 서버 영역을 설정하고 사용자 다운로드를 수행합니다. 자세한 내용은 영역 생성를 참고하십시오.

영역을 설정할 때 활동을 모니터링할 사용자 및 사용자 그룹을 지정할 수 있습니다. 사용자 그룹을 포함하면 해당 그룹의 모든 멤버(보조 그룹 멤버 포함)가 자동으로 포함됩니다. 그러나 규칙 기준으로 보조 그룹을 사용하려면 영역 설정에 보조 그룹을 명시적으로 포함해야 합니다.

각 영역에 대해 신뢰할 수 있는 사용자 또는 사용자 그룹의 데이터를 새로 고침하거나 사용자 데이터의 자동 다운로드를 활성화할 수 있습니다.

ID 정책 생성

인증 방법과 영역을 연결하고 해당 정책을 액세스 제어와 연결하는 ID 정책을 생성합니다. 자세한 내용은 ID 정책 생성를 참고하십시오.

디바이스에 사용자 제어를 수행하는 정책(액세스 제어, SSL, QoS)은 ID 정책을 공유합니다. ID 정책은 해당 디바이스의 트래픽에 영향을 미치는 규칙에서 사용할 수 있는 영역, 사용자, 그룹을 결정합니다.

QoS 규칙에서 사용자 조건을 설정하기 전에 QoS 정책의 대상이 되는 디바이스가 반드시 디바이스가 구축한 액세스 제어 정책에서 정의된 것과 같은 올바른 ID 정책을 사용해야 합니다. 동일한 디바이스에 배포된 QoS 정책 및 액세스 제어 정책이 명시적으로 연결된 것은 아니기 때문에 QoS 규칙 편집기를 사용해 유효하지 않은 영역, 사용자, 그룹을 선택할 수 있습니다. 유효하지 않은 이런 요소는 Firepower Management Center의 ID 정책에는 존재하지만 QoS 대상 디바이스에는 적용되지 않습니다. 이러한 요소를 사용하는 경우 시스템은 구축 시간 이전에 사용자가 유효하지 않은 선택을 했는지 식별할 수 없습니다.

사용자 및 영역 조건 구성

영역, 또는 해당 영역에 속한 사용자 그룹 및 사용자에 따른 규칙을 제한할 수 있습니다.

시작하기 전에

- 사용자, 영역 및 ISE 속성 조건(사용자 제어), 23 페이지에서 설명된 사용자 제어 전제 조건을 충족합니다.
- 클래식 디바이스 모델의 경우 이러한 조건을 설정하려면 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** 규칙 편집기에서 **Users(**사용자**)**를 클릭합니다.

단계 **2** (선택 사항) **Available Realms(**사용 가능한 영역**)**에서 사용하려는 영역을 찾아 선택합니다.

단계 **3** (선택 사항) **Available Users(**사용 가능한 사용자**)** 목록에서 사용자 및 그룹을 선택하여 규칙을 추가로 제한할 수 있습니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

ISE 속성 조건 구성

시작하기 전에

- 사용자, 영역 및 ISE 속성 조건(사용자 제어), 23 페이지에서 설명한 사용자 제어 전제 조건을 충족합니다.
- 클래식 디바이스 모델의 경우 이러한 조건을 구성하려면 제어 라이센스가 있어야 합니다.

프로시저

단계 **1** 규칙 편집기에서 ISE 속성 조건에 대해 다음을 클릭합니다.

- 액세스 제어 - **SGT/ISE Attributes(SGT/ISE** 속성**)**를 클릭합니다.

ISE가 할당된 SGT(보안 그룹 태그)를 사용하면 ISE 속성 조건을 제한할 수 있습니다.

단계 **2** 항목의 **Available ISE Session Attributes(**사용 가능한 **ISE** 세션 속성**)**에서 사용하려는 ISE 속성을 찾아 선택합니다.

- 보안 그룹 태그(SGT)
- 디바이스 유형(또는 엔드포인트 프로파일)
- QoS - **ISE Attributes(ISE** 속성**)**를 클릭합니다.
- 위치 IP(또는 엔드포인트 위치)

단계 **3** 항목의 **Available ISE Metadata(**사용 가능한 **ISE** 메타데이터**)**의 속성 메타데이터를 선택하여 규칙을 추가로 제한합니다. 또는 기본값 모든을 유지합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭하거나 개체를 끌어서 놓습니다.

단계 **5** (선택 사항) **Add a Location IP Address(IP** 주소 위치 추가**)** 필드의 IP 주소 규칙을 제한하고 **Add(**추가**)**를 클릭합니다.

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.

단계 **6** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

사용자 제어 문제 해결

사용자 규칙 동작이 정상적이지 않을 경우 규칙, ID 소스 또는 영역 컨피그레이션을 조정하는 방법을 고려하십시오. 기타 관련 문제 해결 정보를 보려면 다음을 참조하십시오.

- ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결
- 캡티브 포털(captive portal) ID 소스 문제 해결
- 영역 및 사용자 다운로드 문제 해결

영역, 사용자 또는 사용자 그룹을 대상으로 하는 규칙이 트래픽과 일치하지 않음

다수의 사용자 그룹을 모니터링하는 ISE 디바이스를 설정하거나 네트워크의 호스트에 매우 많은 사용자가 매핑된 경우, Firepower Management Center 사용자 제한으로 인해 사용자 레코드가 삭제될 수 있습니다. 그 결과, 사용자 조건이 있는 규칙은 정상적으로 트래픽과 일치하지 않을 수 있습니다.

다수의 사용자 그룹을 모니터링하는 TS 에이전트, 또는 ISE/ISE-PIC 디바이스를 설정하거나 네트워크의 호스트에 매우 많은 사용자가 매핑된 경우, Firepower Management Center 사용자 제한으로 인해 사용자 레코드가 삭제될 수 있습니다. 그 결과, 사용자 조건이 있는 규칙은 정상적으로 트래픽과 일치하지 않을 수 있습니다.

사용자 그룹 내의 사용자 그룹 또는 사용자를 대상으로 하는 규칙이 정상적으로 트래픽과 일치하지 않음

사용자 그룹 조건이 포함된 규칙을 구성할 경우, LDAP 또는 Active Directory 서버에 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.

보조 그룹의 사용자를 대상으로 하는 규칙이 정상적으로 트래픽과 일치하지 않음

Active Directory 서버에 있는 보조 그룹의 구성원인 사용자를 포함하거나 제외하는 사용자 그룹 조건이 포함된 규칙을 구성할 경우, 서버에서는 보고하는 사용자 수를 제한할 수 있습니다.

기본적으로 Active Directory 서버는 보조 그룹에서 보고하는 사용자 수를 제한합니다. 보조 그룹의 모든 사용자를 Firepower Management Center에 보고하고 사용자 조건이 포함된 규칙에서 사용할 수 있도록 하려면 이 제한을 맞춤설정해야 합니다.

사용자가 최초로 확인된 경우 규칙이 해당 사용자와 일치하지 않음

이전에 확인되지 않은 사용자의 활동이 탐지되면 시스템은 서버에서 해당 사용자에 대한 정보를 검색합니다. 시스템이 이러한 정보를 성공적으로 검색할 때까지 해당 사용자가 보여준 활동이 일치하는 규칙으로 처리되지 않습니다. 그 대신, 일치하는 다음 규칙(또는 해당하는 경우 정책의 기본 작업)에 따라 사용자 세션이 처리됩니다.

다음과 같은 경우를 예로 들 수 있습니다.

- 사용자 그룹의 구성원인 사용자가 사용자 그룹 조건이 포함된 규칙과 일치하지 않음
- 사용자 데이터 회수에 사용된 서버가 액티브 디렉토리 서버인 경우, 또는 ISE/ISE-PIC 디바이스가 보고한 사용자가 규칙과 일치하지 않습니다.

이 경우 시스템에서 이벤트 보기 및 분석 툴에 사용자 데이터를 표시하는 것이 지연될 수 있습니다.

규칙이 모든 **ISE** 사용자와 일치하지 않음

이는 정상적인 동작입니다. Active Directory 도메인 컨트롤러에서 인증된 ISE 사용자에 대해 사용자 제어를 수행할 수 있습니다. LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.

규칙이 모든 **ISE/ISE-PIC** 사용자와 일치하지 않음

이는 정상적인 동작입니다. Active Directory 도메인 컨트롤러에서 인증된 ISE/ISE-PIC 사용자에 대해 사용자 제어를 수행할 수 있습니다. LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE/ISE-PIC 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.

너무 많은 메모리를 사용하는 사용자 및 그룹

처리 중인 사용자 및 그룹이 너무 많은 메모리를 사용하는 경우 상태 알림이 표시됩니다. 모든 사용자 세션은 FMC에서 관리하는 모든 디바이스로 전파됩니다. FMC가 메모리가 다른 디바이스를 관리하는 경우, 메모리가 가장 적은 디바이스가 시스템이 오류 없이 처리할 수 있는 사용자 세션 수를 결정합니다.

문제가 지속되는 경우 다음 옵션 중 하나를 선택합니다.

- 서브넷에서 저용량 관리 디바이스를 분리하고 패시브 인증 데이터를 해당 서브넷에 보고하지 않도록 ISE/ISE-PIC를 설정합니다.

  Cisco ISE(Identity Services Engine) 관리자 설명서의 네트워크 디바이스 관리 장을 참조하십시오.

- SGT(Security Group Tag)에서 구독을 취소합니다.

  자세한 내용은 사용자 제어를 위한 ISE/ISE-PIC 설정를 참고하십시오.

- 더 많은 메모리를 사용하여 매니지드 디바이스를 모델로 업그레이드합니다.

날짜 및 시간 기준 규칙 적용

다음 유형의 정책에서는 날짜와 시간에 따라 규칙을 적용할 수 있습니다.

- 액세스 제어
- 사전 필터
- VPN 그룹

연속 시간 범위 또는 반복 기간을 지정할 수 있습니다.

예를 들어 규칙은 주중 근무 시간 중 또는 매주 또는 공휴일 셧다운 기간에만 적용할 수 있습니다.

시간 기반 규칙은 트래픽을 처리하는 디바이스의 로컬 시간을 기준으로 적용됩니다.

시간 기반 규칙은 FTD 디바이스에서만 지원됩니다. 시간 기반 규칙이 있는 정책을 다른 유형의 디바이스에 할당하는 경우 해당 디바이스에서 규칙과 연결된 시간 제한이 무시됩니다. 이 경우 경고가 표시됩니다.

프로시저

단계 **1** (선택 사항) 각 디바이스에 로컬 표준 시간대를 할당합니다. 기본적으로 디바이스는 UTC 표준 시간대를 사용합니다.

Devices(디바이스**)** > **Platform Settings(**플랫폼 설정**)**로 이동하여 표준 시간대 개체를 생성하고 할당합니다.

단계 **2** 지원되는 규칙에서 적용 가능한 시간 범위를 지정합니다.

규칙을 구성하는 동안 시간 범위 개체를 생성하고 선택합니다.

단계 **3** 변경 사항을 구축합니다.

규칙 검색

많은 정책 및 규칙 내에서 검색할 수 있습니다. 시스템은 개체 및 개체 그룹의 이름 및 조건 값을 제어하는 입력에 일치시킵니다.

보안 인텔리전스 또는 URL 목록이나 피드의 값을 검색할 수 없습니다.

프로시저

단계 **1** 정책 편집기에서 **Rules(**규칙**)**를 클릭합니다.

단계 **2** (액세스 제어 규칙만 해당) **Search Rules(**검색 규칙**)**를 클릭하고 하나 이상의 필드에 전체 또는 부분 검색 문자열을 입력한 다음 Enter 키를 누릅니다.

여러 필드에 기준을 입력할 경우, 검색 결과에는 입력한 모든 기준(논리적 "AND" 검색)과 일치하는 규칙이 포함됩니다.

단일 필드에 여러 검색 기준을 포함하려면 값을 쉼표로 구분합니다. 검색 결과에는 입력한 값과 일치하는 규칙(논리적 "OR" 검색)이 포함됩니다.

단계 **3** (기타 규칙 유형) **Search Rules(**검색 규칙**)**를 클릭하고 전체 또는 부분 검색 문자열을 입력한 뒤 Enter 키를 누릅니다.
일치 값은 각 일치하는 규칙에 강조 표시됩니다. 상태 메시지는 현재 일치하는 규칙과 일치하는 총 수를 나타냅니다.

단계 **4** 관심 있는 규칙을 확인합니다.

일치하는 규칙을 탐색하려면 **Next-Match(**다음 일치**)** 또는 **Previous-Match(**이전 일치**)**를 클릭합니다.

(액세스 제어 규칙만 해당) 일치하는 규칙의 목록만 표시하거나 일치하는 규칙이 강조 표시된 모든 규칙의 목록을 표시하려면 다음을 클릭합니다. 검색 규칙( )

다음에 수행할 작업

- 새 검색을 시작하기 전에 검색 또는 강조 표시를 지우려면 지우기( )를 클릭합니다.

디바이스별 규칙 필터링

일부 정책 편집기를 사용하면 영향 받는 디바이스에 따른 규칙 보기를 필터링할 수 있습니다.

디바이스별 필터링은 영역 또는 인터페이스 그룹을 사용하는 규칙에 대해서만 작동합니다. (그렇지 않으면 모든 디바이스에 규칙이 적용됩니다.)

시스템은 규칙의 인터페이스 제약 조건을 사용하여 규칙이 디바이스에 영향을 미치는지 결정합니다. (보안 영역 조건) 인터페이스로 규칙을 제한하는 경우, 해당 인터페이스가 위치한 디바이스는 해당 규칙에 영향을 받습니다. 인터페이스 제약 조건이 없는 규칙은 모든 인터페이스에 적용되므로 모든 디바이스에 적용됩니다.

QoS 규칙은 항상 인터페이스에 의해 제한됩니다.

프로시저

단계 **1** 정책 편집기에서 **Rules(**규칙**)**를 클릭하고 **Filter by Device(**디바이스로 필터링**)**를 클릭합니다. 대상 디바이스 및 디바이스 그룹의 목록이 표시됩니다.

단계 **2** 이런 디바이스 또는 그룹에 적용되는 규칙만을 표시하려면 하나 이상의 체크 박스에 체크합니다. 또는 재설정하여 모든 규칙을 표시하려는 경우 모두를 체크합니다.

팁 해당 값을 확인하려면 규칙 기준으로 마우스 포인터를 이동합니다. 기준이 디바이스 한정 오버라이드가 포함된 개체를 나타내는 경우 시스템은 해당 디바이스에 한정한 규칙 목록을 필터링할 때 오버라이드 값을 표시합니다. 기준이 도메인 한정 오버라이드가 포함된 개체를 나타내는 경우 시스템은 해당 도메인의 디바이스의 규칙 목록을 필터링할 때 오버라이드 값을 표시합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

관련 항목

액세스 제어 규칙 생성 및 수정
QoS 규칙 구성
Threat Defense NAT 구성

문제가 있는 규칙 식별

시스템은 규칙 순서의 다른 상위 규칙이 대신 일치하므로(노란색 아이콘으로 표시) 구축을 예방하는 각 규칙에 플래그를 지정하거나(빨간색 아이콘으로 표시) 트래픽을 일치시키지 않습니다.

중요 시스템은 다른 규칙과 일부 일치하고 하위 규칙과 일치하지 않도록 하는 규칙에 플래그를 지정하지 않습니다.

프로시저

단계 **1** **Policies(**정책**) > Access Control(**액세스 컨트롤**) > Access Control(**액세스 컨트롤**)**을 선택합니다.

단계 **2** 정책 이름을 클릭합니다.

단계 **3** 다음 중 하나를 또는 둘 다 수행합니다.

- 창의 상단 근처에 있는 **Show Warnings(**경고 표시**)**를 찾습니다.

  시스템이 문제를 식별하지 않는 경우 이 버튼이 표시되지 않습니다.

  문제가 있는 경우 이 버튼을 눌러 문제와 관련된 모든 규칙 목록을 표시합니다.

  모든 문제를 보려면 두 탭(규칙 오류 및 규칙 경고)을 클릭합니다.

  아래의 규칙 테이블의 규칙을 찾으려면 오류 또는 경고 목록에서 규칙 이름을 클릭합니다.

- **Show Rule Conflicts(**규칙 충돌 표시**)** 체크 박스를 선택합니다.

  목록에서 오류(빨간색) 또는 경고(노란색)로 각 문제 규칙을 나타냅니다.

  필요한 경우 정책의 모든 규칙을 보려면 아래로 스크롤하십시오.

단계 **4** 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

단계 **5** 일부만 일치하고 이를 처리하여 플래그로 지정되지 않은 중복을 검색합니다.

단계 **6** 변경하는 경우 **Save(**저장**)**를 클릭하거나 **Show Rule Conflicts(**규칙 충돌 보기**)**를 다시 선택 또는 선택 취소하여 충돌하는 규칙 변경을 다시 평가합니다.

다음에 수행할 작업

- 문제가 되는 규칙을 제거 또는 수정하여 관련 문제를 처리합니다.
- 유사한 오류 및 경고에 대한 SSL 또는 QoS 정책을 평가하고 이러한 문제를 처리합니다.

규칙 및 기타 정책 경고

정책 및 규칙 편집기는 아이콘을 사용하여 트래픽 분석 및 흐름에 부정적인 영향을 미칠 수 있는 설정을 표시합니다. 문제에 따라 구축 시 시스템이 경고하거나 완전 구축을 차단할 수 있습니다.

팁 경고, 오류 또는 정보를 제공하는 텍스트를 읽을 아이콘에 마우스 포인터를 놓습니다.

표 *2:* 정책 오류 아이콘

아이콘	설명	예
오류(✖) 오류	규칙 또는 설정에 오류가 있는 경우, 영향을 받는 규칙을 비활성화해도 문제를 수정하기 전까지는 구축할 수 없습니다.	카테고리 및 평판 기반 URL 필터링을 수행하는 규칙은 URL 필터링 라이선스가 없는 디바이스를 대상으로 하기 전까지 유효합니다. 이 경우 규칙 옆에 오류 아이콘이 표시되며 규칙을 편집 또는 삭제하거나 정책의 대상을 다시 설정하거나 라이선스를 활성화하기 전까지 구축할 수 없습니다.
경고(⚠) 경고	규칙 또는 다른 경고를 표시하는 정책을 구축할 수 있습니다. 그러나, 경고가 표시된 오류 구성은 적용되지 않습니다. 경고가 표시된 규칙을 비활성화하는 경우, 경고 아이콘이 사라집니다. 경고 아이콘은 근본적인 문제를 해결하지 않고 규칙을 활성화하는 경우 다시 나타납니다.	선점된 규칙 또는 설정 오류로 트래픽과 일치하지 않는 규칙은 효과가 없습니다. 이는 제외된 LDAP 사용자, 유효하지 않은 포트 등 애플리케이션과 일치하지 않는 빈 개체 그룹, 애플리케이션 필터를 사용한 조건을 포함합니다. 그러나 경고 아이콘이 라이선싱 오류 또는 모델 불일치를 표시하는 경우 해당 문제를 해결하기 전까지 구축할 수 없습니다.
정보(ⓘ) 정보	정보 아이콘은 트래픽의 흐름에 영향을 줄 수 있는 구성에 대한 유용한 정보를 제공합니다. 이 문제는 구축을 방해하지 않습니다.	애플리케이션 제어이 있는 경우, 시스템은 연결 애플리케이션 또는 웹 트래픽을 식별하기 전까지 일부 규칙과 다른 초기 연결 패킷을 일치시키는 작업을 건너 뛸 수 있습니다. 이는 애플리케이션 및 HTTP 요청을 확인할 수 있도록 연결을 설정할 수 있게 합니다.

관련 항목

애플리케이션 제어 모범 사례, 16 페이지
URL 필터링 모범 사례

규칙 관리 기록: 일반 특성

기능	버전	세부 사항
사전 필터 정책에서 개체 세부 사항 보기	6.6	이제 사전 필터 정책의 규칙에서 소스 및 대상 네트워크(IP 주소), 포트, VLAN 태그 개체 및 개체 그룹을 볼 수 있습니다. 적합한 개체를 마우스 오른쪽 버튼으로 클릭하고 **Object Details(**개체 세부 사항**)**를 선택합니다. 신규/수정된 페이지: Prefilter rules(사전 필터 규칙) 페이지 지원되는 플랫폼: FMC
설정된 규칙에 대한 향상된 검색	6.6	이제 여러 열에서 설정된 규칙을 검색할 수 있습니다(액세스 제어 정책만 해당). 신규/수정된 페이지: Access control rules(액세스 제어 규칙) 페이지 지원되는 플랫폼: FMC
사전 필터 규칙에 대한 시간 범위 지원	6.6	적용할 규칙에 대해 절대적이거나 반복되는 시간 또는 시간 범위를 지정할 수 있습니다. 규칙은 트래픽을 처리하는 디바이스의 표준 시간대에 따라 적용됩니다. 신규/수정된 페이지: Prefilter rule configuration(사전 필터 규칙 설정) 페이지 지원되는 플랫폼: FTD 디바이스 전용
URL 조건에 대한 정보는 새 URL 필터링 장으로 이동	6.3	URL 조건에 관한 전용 항목을 포함해 URL 필터링에 대한 정보는 URL 필터링을 참고하십시오.