서비스 품질

다음 주제에서는 Firepower Threat Defense 디바이스의 QoS(Quality of Service)를 사용하여 네트워크 트래픽을 폴리싱하는 방법을 설명합니다.

QoS 소개

액세스 제어에서 허용되거나 신뢰하는 서비스 품질 또는 QoS, 속도 제한(정책) 네트워크 트래픽 시스템은 빠른 경로가 지정된 트래픽의 속도를 제한하지 않습니다.

QoS는 FTD 디바이스의 라우팅된 인터페이스에서만 지원되지만 사이트 간 VPN 및 VTI 인터페이스에서는 지원되지 않습니다.

속도 제한된 연결 로깅

QoS에 대한 로깅 구성이 없습니다. 연결은 로깅 없이 속도 제한을 받을 수 있으며 속도 제한을 이유로 연결을 로깅할 수 없습니다. 연결 이벤트에서 QoS 정보를 보려면 적절한 연결의 종료를 Firepower Management Center 데이터베이스에 개별적으로 기록해야 합니다. Firepower Management Center 관리 가이드의 기록할 수 있는 기타 연결을 참조하십시오.

속도 제한된 연결에 대한 연결 이벤트는 삭제된 트래픽의 양과 트래픽이 제한된 QoS 설정에 대한 정보를 포함합니다. 이 정보는 이벤트 보기(워크플로), 대시보드, 보고서에서 볼 수 있습니다.

QoS 정책 정보

매니지드 디바이스의 속도 제한을 제어하기 위해 구축된 QoS 정책 각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

QoS 정책에서는 최대 32개의 QoS 규칙이 네트워크 트래픽을 처리합니다. 시스템은 사용자가 지정하는 순서대로 트래픽이 QoS 규칙과 일치하는지 확인합니다. 시스템은 모든 규칙 조건이 트래픽과 일

치하는 첫 번째 규칙에 따라 트래픽의 속도를 제한합니다. 모든 규칙 조건과 일치하지 않는 트래픽의 속도는 제한되지 않습니다.

소스 또는 대상(라우팅) 인터페이스에서 QoS 규칙을 제한해야 합니다. 시스템은 각 인터페이스에서 개별적으로 속도를 제한합니다. 인터페이스 집합에 대해 합계 속도 제한을 지정할 수 없습니다.

QoS 규칙은 애플리케이션, URL, 사용자 ID, 사용자 정의 보안 그룹 태그(SGT)와 같은 상황 정보 및 다른 네트워크 특징으로도 트래픽 속도를 제한할 수 있습니다.

다운로드 트래픽과 업로드 트래픽의 속도를 개별적으로 제한할 수 있습니다. 시스템은 연결 이니시에이터에 따라 다운로드 및 업로드 규칙을 결정합니다.

참고 QoS는 메인 액세스 제어 설정에 속하지 않으며 독립적으로 구성됩니다. 그러나 동일한 디바이스의 공유 ID 설정에 구축된 액세스 제어 및 QoS 정책은 액세스 제어에 다른 정책 연결을 참조하십시오.

QoS 정책 및 멀티 테넌시

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인의 관리자는 다른 하위 도메인의 디바이스에 동일한 QoS 정책을 구축할 수 있습니다. 이 하위 도메인의 관리자는 상위에서 구축한 QoS 정책을 읽기 전용으로 사용하거나 로컬 정책으로 대체할 수 있습니다.

QoS 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

네트워크 관리자

QoS 정책을 사용한 속도 제한

정책 기반 속도 제한을 수행하려면 매니지드 디바이스에 QoS 정책을 구성 및 구축합니다. 각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **QoS**을(를) 선택합니다.

단계 **2** **New Policy(**새 정책**)**를 클릭해 새 QoS 정책을 생성하고, 원한다면 대상 디바이스를 할당합니다. 자세한 내용은 QoS 정책 생성, 4 페이지의 내용을 참조하십시오.

기존 정책을 **Copy(**복사**)** ( )하거나 **Edit(**수정**)** ( )할 수도 있습니다.

단계 **3** QoS 규칙 구성은 QoS 규칙 구성, 5 페이지과 QoS 규칙 조건, 7 페이지를 참조하십시오.

QoS 정책 편집기의 규칙은 평가 순서대로 규칙을 나열하고 규칙 조건 및 속도 제한 설정 요약을 표시합니다. 마우스 오른쪽 버튼 클릭 메뉴는 이동, 활성화 및 비활성화를 포함한 규칙 관리 옵션을 제공합니다.

디바이스별 필터를 사용하여 특정 디바이스 또는 디바이스 그룹에만 영향을 주는 규칙을 표시할 수 있어 대규모 구축에 유용합니다. 규칙에 대해 또는 규칙 내에서 검색할 수 있습니다. 시스템은 검색 조건 필드에 입력한 텍스트를 개체 및 개체 그룹을 포함해 규칙 이름, 조건 값과 일치시킵니다.

참고 규칙을 올바르게 생성하고 순서를 지정하는 것은 복잡한 작업이지만, 효과적인 구축에 필수적입니다. 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이선스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 아이콘은 설명, 경고 및 오류를 나타냅니다. 문제가 있을 경우 경고 표시를 클릭하면 목록이 표시됩니다. 자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례의 내용을 참고하십시오.

단계 **4** 정책 할당을 클릭하여 정책의 대상이 되는 매니지드 디바이스를 식별합니다. QoS 정책에 대한 대상 디바이스 설정, 4 페이지를 참조하십시오.

정책을 생성하는 중에 대상 디바이스를 식별한 경우 선택 사항을 확인합니다.

단계 **5** QoS 정책을 저장합니다.

단계 **6** 이 기능은 일부 패킷의 통과를 허용해야 하므로 해당 패킷을 검사하도록 시스템을 설정해야 합니다. 트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정를 참조하십시오.

단계 **7** Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.

QoS 정책 생성

규칙이 없는 새 QoS 정책은 속도 제한을 수행하지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **QoS**을(를) 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** 필요에 따라 정책을 구축할 사용 가능한 디바이스를 선택하고 정책에 추가 또는 드래그 앤 드롭을 클릭하여 선택한 디바이스를 추가합니다. 표시되는 디바이스의 범위를 좁히려면 검색 필드에 검색 문자열을 입력합니다.

정책을 구축하기 전에 디바이스를 할당해야 합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- QoS 정책을 구축하고 구성하려면 QoS 정책을 사용한 속도 제한, 3 페이지을 참조하십시오.

QoS 정책에 대한 대상 디바이스 설정

각 QoS 정책은 여러 장치를 대상으로 할 수 있습니다. 각 디바이스에는 한 번에 하나의 QoS 정책을 구축할 수 있습니다.

프로시저

단계 **1** QoS 정책 편집기에서 정책 할당을 클릭합니다.

단계 **2** 대상 목록 작성:

- 추가 - 하나 이상의 사용 가능한 디바이스를 선택한 다음 정책에 추가를 클릭하거나 선택한 디바이스 목록으로 드래그 앤 드롭합니다.
- 삭제 - 단일 디바이스 옆에 있는 **Delete(**삭제**)** ( )을 클릭하거나 여러 디바이스를 선택하고 오른쪽 클릭한 다음 **Delete Selected(**선택 항목 삭제**)**를 선택합니다.
- 검색 - 검색 필드에 검색 문자열을 입력합니다. **Clear(**지우기**)** ( )을 클릭하여 검색 내용을 삭제합니다.

단계 **3** **OK(**확인**)**를 클릭하여 정책 할당을 저장합니다.

단계 **4** **Save(**저장**)**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

QoS 규칙 구성

규칙을 생성하거나 편집할 때 규칙 편집기의 상단을 사용해 일반 규칙 속성을 설정할 수 있습니다. 규칙 편집기 하단을 사용하여 규칙 조건 및 설명을 설정합니다.

프로시저

단계 **1** QoS 정책 편집기의 규칙에는 다음이 있습니다.

- 규칙 추가 - **Add Rule(**규칙 추가**)**를 클릭합니다.
- Edit Rule(규칙 편집) - **Edit(**수정**)** ( )을 클릭합니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** 규칙 구성 요소를 구성합니다.

- Enabled(활성화) — 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.
- QoS 적용 켜기 - 대상 인터페이스 개체의 인터페이스 또는 소스 인터페이스 개체의 인터페이스 중 속도를 제한하려는 인터페이스를 선택합니다. 이때 선택은 생성된 인터페이스 제약**(Any(**모든**)**이 아닌)에 일치해야 합니다.
- 인터페이스별 트래픽 제한 - Mbit/초 단위로 다운로드 제한 용량 및 업로드 제한 용량을 입력합니다. **Unlimited(**무제한**)**의 기본값은 해당 방향의 일치하는 트래픽의 속도 제한을 방지합니다.
- 조건 - 추가할 조건을 클릭합니다. **Apply QoS On(QoS** 적용**)**에 대한 선택에 해당하는 소스 또는 대상 인터페이스 조건을 설정해야 합니다.
- 설명 - **Comment(**설명**)**를 클릭합니다. 설명을 추가하려면 **New Comment(**새 설명**)**을 클릭해 설명을 입력하고 **OK(**확인**)**을 클릭합니다. 규칙을 저장할 때까지 이 코멘트를 수정하거나 삭제할 수 있습니다.

규칙 구성 요소에 대한 자세한 내용은 QoS 규칙 구성 요소, 6 페이지을 참조하십시오.

단계 **4** 규칙을 저장합니다.

단계 **5** 정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규

칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례

QoS 규칙 구성 요소

상태(활성화/비활성화)

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하지 않으며, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

인터페이스(QoS 적용됨)

모든 트래픽의 속도를 제한하는 QoS 규칙은 저장할 수 없습니다. 각 QoS 규칙에 대해 다음의 경우 QoS를 적용해야 합니다.

- 소스 인터페이스 개체의 인터페이스 - 규칙의 소스 인터페이스를 통해 트래픽 속도를 제한합니다. 이 옵션을 선택하는 경우 하나 이상의 소스 인터페이스 제약 조건(**any** 불가)을 추가해야 합니다.
- 대상 인터페이스 개체의 인터페이스 - 규칙의 대상 인터페이스를 통해 트래픽 속도를 제한합니다. 이 옵션을 선택하는 경우 하나 이상의 대상 인터페이스 제약 조건 (**any** 불가)를 추가해야 합니다.

인터페이스별 트래픽 제한

QoS 규칙은 옵션에서 QoS 적용을 지정한 각 인터페이스에 개별적으로 속도를 제한합니다. 인터페이스 집합에 대해 통합적인 속도 제한을 지정할 수 없습니다.

초당 Mbits로 트래픽을 제한할 수 있습니다. **Unlimited**(무제한)의 기본값은 일치하는 트래픽의 속도 제한을 방지합니다.

다운로드 트래픽과 업로드 트래픽의 속도를 개별적으로 제한할 수 있습니다. 시스템은 연결 이니시에이터에 따라 다운로드 및 업로드 규칙을 결정합니다.

인터페이스의 최대 처리량보다 큰 한계를 지정하는 경우 시스템은 일치하는 트래픽의 속도 제한을 하지 않습니다. 최대 처리량은 각 디바이스의 속성에서 지정한 인터페이스의 하드웨어 설정에 영향을 받을 수 있습니다.(**Devices**(디바이스) > **Device Management**(디바이스 관리))

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 규칙마다 여러 조건을 구성할 수 있습니다. 트래픽은 규칙과 일치하는 모든 조건과 일치해야 합니다. 각 조건 유형은 규칙 편집기에 고유한 탭이 있습니다. 자세한 내용은 QoS 규칙 조건, 7 페이지를 참고하십시오.

코멘트

규칙에 대한 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다.

시스템 정책 편집기에서 시스템은 규칙에 포함될 코멘트 수를 표시합니다. 규칙 편집기에서 Comments(코멘트) 탭을 사용하여 기존 코멘트를 확인하고 새 코멘트를 추가합니다.

QoS 규칙 조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 규칙마다 여러 조건을 구성할 수 있습니다. 트래픽은 규칙과 일치하는 모든 조건과 일치해야 합니다. 각 조건 유형은 규칙 편집기에 고유한 탭이 있습니다. 다음을 사용하여 트래픽 속도를 제한할 수 있습니다.

자세한 내용은 다음 섹션 중 하나를 참조하십시오.

관련 항목

인터페이스 규칙 조건, 7 페이지
네트워크 규칙 조건, 8 페이지
사용자 규칙 조건, 8 페이지
애플리케이션 규칙 조건, 8 페이지
포트 규칙 조건, 10 페이지
URL 규칙 조건, 12 페이지
맞춤형 SGT 규칙 조건, 12 페이지

인터페이스 규칙 조건

인터페이스 규칙 조건은 소스 및 대상 인터페이스를 통해 트래픽을 제어합니다.

구축의 규칙 유형 및 디바이스에 따라, 보안 영역 또는 인터페이스 그룹이라는 사전 정의된 인터페이스 개체를 사용하여 인터페이스 조건을 만들 수 있습니다. 인터페이스 개체는 네트워크를 세그멘테이션화하여 여러 디바이스에 걸쳐 인터페이스를 그룹화하는 방법을 통해 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다(Interface(인터페이스) 참조).

팁 인터페이스로 규칙을 제한하는 것은 시스템 성능을 개선하는 가장 좋은 방법 중 하나입니다. 규칙이 모든 디바이스의 인터페이스를 제외할 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

인터페이스 개체의 모든 인터페이스가 동일한 유형이어야 하는 것과 마찬가지로(모든 인라인, 수동, 스위칭, 라우팅 또는 ASA FirePOWER), 인터페이스 조건에 사용된 모든 인터페이스 개체도 동일한

유형이어야 합니다. 패시브 방식으로 구축된 디바이스는 트래픽을 전송하지 않으므로, 패시브 구축에서는 대상 인터페이스를 통해 규칙을 제한할 수 없습니다.

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.

사용자 규칙 조건

사용자 규칙 조건은 연결을 시작한 사용자 또는 사용자가 속한 그룹을 기준으로 트래픽을 매칭합니다. 예를 들어, Finance 그룹의 모든 사용자가 네트워크 리소스에 액세스하는 것을 금지하도록 Block(차단) 규칙을 구성할 수 있습니다.

액세스 제어 규칙의 경우에만 먼저 액세스 제어에 다른 정책 연결에 설명된 대로 ID 정책을 액세스 제어 정책과 연결해야 합니다.

구성된 영역에 대한 사용자 및 그룹을 구성하는 것 외에도 다음 특수 ID 사용자에 대한 정책을 설정할 수 있습니다.

- Failed Authentication(실패한 인증): 캡티브 포털(captive portal) 인증에 실패한 사용자입니다.
- Guest(게스트): 캡티브 포털에서 게스트 사용자로 구성된 사용자입니다.
- No Authentication Required(인증 필요 없음): ID가 **No Authentication Required(**인증 필요 없음**)** 규칙 작업과 일치하는 사용자입니다.
- Unknown(알 수 없음): 식별할 수 없는 사용자입니다. 예를 들어 구성된 영역에 의해 다운로드되지 않은 사용자입니다.

애플리케이션 규칙 조건

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.

(Snort 2만 해당.) 애플리케이션 컨트롤의 일부로, 액세스 제어 규칙을 사용하여 콘텐츠 제한(예: 안전 검색 및 YouTube EDU)을 시행할 수도 있습니다.

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 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.

관련 항목

애플리케이션 제어 구성 모범 사례

포트 규칙 조건

포트 조건을 사용하면 소스 및 대상 포트를 기준으로 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.

포트, 프로토콜 및 ICMP 코드 규칙 조건

포트 조건은 소스 및 대상 포트를 기준으로 트래픽과 일치합니다. 규칙 유형에 따라, "포트"는 다음 중 하나를 나타낼 수 있습니다.

- TCP 및 UDP — 포트를 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
- Protocol(프로토콜) - 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. 사전 필터 규칙에서는 애플리케이션 필터링을 사용할 수 없습니다.

FTP와 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 대상 포트 조건으로 추가할 수 있습니다.

비 **TCP** 트래픽을 포트 조건과 일치

비 포트 기반 프로토콜을 매칭할 수 있습니다. 기본적으로 포트 조건을 지정하지 않으면 IP 트래픽이 일치하게 됩니다. 비 TCP 트래픽과 일치하도록 포트 조건을 구성할 수 있지만, 몇 가지 제한 사항이 있습니다.

- 액세스 제어 규칙 - 기본 디바이스의 경우 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. Firepower Threat Defense 디바이스의 경우, 사전 필터 정책의 터널 규칙을 사용하여 GRE 캡슐화된 트래픽을 제어합니다.
- SSL 규칙 — SSL 규칙은 TCP 포트 조건만 지원합니다.
- 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.

URL 규칙 조건

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

자세한 내용은 URL 필터링를 참조하십시오.

맞춤형 SGT 규칙 조건

ISE/ISE-PIC를 ID 소스로 구성하지 않을 경우, ISE에서 할당하지 않은 SGT(Security Group Tags)를 사용하여 트래픽을 제어할 수 있습니다. SGT는 신뢰할 수 있는 네트워크 내에서 트래픽 소스의 권한을 지정합니다.

맞춤형 SGT 규칙 조건은 시스템이 ISE 서버에 연결하여 가져온 ISE SGT 대신 수동으로 생성한 SGT 개체를 사용하여 트래픽을 필터링합니다. 이러한 수동으로 생성한 SGT 개체는 제어하려는 트래픽의 SGT 속성에 해당합니다. 맞춤형 SGT를 사용하여 트래픽을 제어하는 것은 사용자 제어로 간주되지 않습니다.

ISE SGT 및 맞춤형 SGT 규칙 조건 비교

할당된 SGT를 바탕으로 한 일부 규칙을 사용해 트래픽을 제어할 수 있습니다. 규칙 유형 및 ID 소스 설정에 따라 할당 SGT 속성에 트래픽을 일치시키기 위해 ISE 할당 SGT 또는 사용자 지정 SGT를 사용할 수 있습니다.

참고 패킷에 할당 SGT 속성이 없는 경우에도 트래픽을 일치시키기 위해 ISE SGT를 사용하는 경우 패킷의 소스 IP 주소와 관련된 SGT가 ISE에 알려진 경우 패킷은 ISE SGT 규칙을 따릅니다.

조건 유형	필수 요건	규칙 편집기에 표시된 **SGT**
ISE SGT	ISE ID 소스	자동으로 업데이트된 메타데이터와 ISE 서버 쿼리로 확보한 SGT
사용자 정의 SGT	No ISE/ISE-PIC ID 소스	사용자가 생성한 고정 SGT 개체

사용자 정의 SGT에서 ISE SGT로 자동 전환

사용자 정의 SGT와 일치하는 규칙을 생성하고 ID 소스로 ISE/ISE-PIC를 설정하면 시스템은 다음을 실행합니다.

- 개체 관리자에서 **Security Group Tag(**보안 그룹 태그**)** 옵션을 비활성화합니다. 그러나 시스템은 기존 SGT 개체를 유지하기만 하고 이를 수정하거나 새로운 개체를 추가할 수 없습니다.
- 사용자 정의 SGT 규칙이 포함된 기존 규칙을 유지합니다. 그러나 이런 규칙은 트래픽에 일치하지 않습니다. 또한 기존 규칙에 추가 사용자 정의 SGT 기준을 추가하거나 사용자 정의 SGT 조건이 포함된 새 규칙을 생성할 수 없습니다.

ISE를 설정하는 경우 사용자 정의 SGT 조건을 포함한 기존 규칙을 삭제하거나 비활성화하는 것이 좋습니다. 대신 ISE 속성 조건을 사용해 SGT 속성이 있는 트래픽을 일치시킵니다.

QoS 기록

기능	버전	세부 사항
평판이 알려지지 않은 URL의 처리를 지정할 수 있는 기능	6.7	자세한 내용은 URL 필터링 기록 섹션을 참조해 주십시오.
속도 제한 증가	6.2.1	최대 제한 속도를 1,000Mbps에서 100,000Mbps로 증가시킵니다. 수정된 화면: QoS 규칙 편집기 지원 플랫폼: Firepower Threat Defense
사용자 정의 SGT 및 원본 클라이언트 네트워크 필터링	6.2.1	QoS는 이제 사용자 정의 보안 그룹 태그(SGT)와 원본 클라이언트 네트워크 정보(XFF, True-Client-IP, 사용자 정의 HTTP헤더)를 사용해 트래픽 속도를 제한할 수 있습니다. 수정된 화면: QoS 규칙 편집기 지원 플랫폼: Firepower Threat Defense
QoS(속도 제한)	6.1	도입된 기능. 액세스 제어에서 허용되거나 신뢰하는 QoS 속도 제한(정책) 네트워크 트래픽 새 화면: 디바이스 > **QoS** 지원 플랫폼: Firepower Threat Defense