사전 필터링 및 사전 필터 정책

사전 필터링 정보

사전 필터링은 시스템에서 더 많은 리소스를 사용하는 평가를 수행하기 전에 이루어지는 첫 번째 액세스 제어 단계입니다. 사전 필터링은 간단하고 빠르며 일찍 이루어집니다. 사전 필터링은 제한된 외부 헤더 기준을 사용하여 신속하게 트래픽을 처리합니다. 내부 헤더를 사용하며 검사 기능이 더 강력한 후속 평가와 사전 필터링을 비교해 보십시오.

다음 경우에 사전 필터링을 구성하십시오.

- 성능 향상 - 검사가 필요하지 않은 트래픽은 일찍 제외할수록 좋습니다. 캡슐화된 연결을 검사하지 않고 외부 캡슐화 헤더를 기반으로 특정 유형의 일반 텍스트, 패스스루 터널을 단축 경로 지정 또는 차단할 수 있습니다. 조기에 처리하는 것이 유리한 그 밖의 연결도 단축 경로를 지정하거나 차단할 수 있습니다.
- 캡슐화된 트래픽에 심층 검사 맞춤 설정 - 동일한 검사 기준을 사용하여 나중에 캡슐화된 연결을 처리할 수 있도록 특정 터널 유형의 영역을 다시 지정할 수 있습니다. 영역 재지정이 필요한 이유는 사전 필터링 후 액세스 제어가 내부 헤더를 사용하기 때문입니다.

사전 필터 정책 정보

사전 필터링은 정책 기반 기능입니다. 디바이스에 할당하려면 디바이스에 할당된 액세스 제어 정책에 할당합니다.

정책 구성 요소: 규칙 및 기본 작업

사전 필터 정책에서는 터널 규칙, 사전 필터 규칙, 기본 작업이 네트워크 트래픽을 처리합니다.

- 터널 및 사전 필터 규칙 - 우선 사전 필터 정책의 규칙은 사용자가 지정하는 순서로 트래픽을 처리합니다. 터널 규칙은 특정 터널만 일치를 확인하고 영역 다시 지정을 지원합니다. 사전 필터 규칙은 제약 조건이 더 광범위하고 영역 다시 지정을 지원하지 않습니다. 자세한 내용은 터널 규칙과 사전 필터 규칙 비교, 2 페이지를 참고하십시오.
- 기본 작업(터널만 해당) - 터널이 어느 규칙과도 일치하지 않으면 기본 작업이 이를 처리합니다. 기본 작업은 이러한 터널을 차단하거나 캡슐화된 개별 연결에서 액세스 제어를 계속할 수 있습니다. 기본 작업으로 터널의 영역을 다시 지정할 수 없습니다.

  캡슐화되지 않은 트래픽에 대한 기본 작업은 없습니다. 캡슐화되지 않은 연결이 어느 사전 필터 규칙과도 일치하지 않으면 시스템이 액세스 제어를 계속합니다.

연결 로깅

사전 필터 정책에 의해 단축 경로가 지정되고 차단된 연결을 로깅할 수 있습니다.

연결 이벤트에는 전체 터널을 포함하여 로깅된 연결이 사전 필터링되었는지 여부와 그 방법에 대한 정보가 포함되어 있습니다. 이벤트 보기(워크플로), 대시보드, 보고서에서 이 정보를 확인하고 상관관계 기준으로 사용할 수 있습니다. 단축 경로가 지정되고 차단된 연결은 심층 검사 대상이 아니므로 연결된 연결 이벤트에는 제한된 정보가 포함되어 있음에 유의하십시오.

기본 사전 필터 정책

모든 액세스 제어 정책에는 연결된 사전 필터 정책이 있습니다.

맞춤형 사전 필터링을 구성하지 않은 경우, 기본 정책이 사용됩니다. 시스템이 제공하는 이 정책은 처음에는 모든 트래픽을 액세스 제어의 다음 단계로 통과시킵니다. 정책의 기본 작업을 변경하고 로깅 옵션을 구성할 수 있지만 규칙을 추가하거나 삭제할 수는 없습니다.

사전 필터 정책 상속 및 멀티 테넌시

액세스 제어는 멀티 테넌시를 보완하는 계층적 구현을 사용합니다. 다른 고급 설정과 함께 사전 필터 정책 연결을 잠가 모든 하위 항목 액세스 제어 정책에서 해당 연결을 적용할 수 있습니다. 자세한 내용은 액세스 제어 정책 상속를 참고하십시오.

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. 기본 사전 필터 정책은 전역 도메인에 속합니다.

터널 규칙과 사전 필터 규칙 비교

터널 규칙 또는 사전 필터 규칙 중 어느 것을 구성할 것인지는 일치할 특정 유형의 트래픽, 그리고 수행하려는 작업이나 추가 분석에 따라 결정됩니다.

특성	터널 규칙	사전 필터 규칙
기본 기능	일반 텍스트, 통과 터널의 단축 경로 지정, 차단, 영역 다시 지정을 신속하게 수행합니다.	조기에 처리하는 것이 유리한 모든 기타 연결의 단축 경로 지정 또는 차단을 신속하게 수행합니다.
캡슐화 및 포트/프로토콜 기준	캡슐화 조건은 캡슐화 규칙 조건, 15 페이지에 나와 있는 선택한 프로토콜을 통한 일반 텍스트 터널에만 일치됩니다.	포트 조건은 터널 규칙보다 더 광범위한 포트 및 프로토콜 제약 조건을 사용할 수 있습니다(포트, 프로토콜 및 ICMP 코드 규칙 조건 참조).
네트워크 기준	터널 엔드포인트 조건은 처리할 터널의 엔드포인트를 제한합니다(네트워크 규칙 조건 참조).	네트워크 조건은 각 연결의 소스 및 대상 호스트를 제약합니다. 네트워크 규칙 조건의 내용을 참조하십시오.
방향	양방향 또는 단방향(구성 가능). 터널 규칙은 기본적으로 양방향이므로, 터널 엔드포인트 간의 모든 트래픽을 처리할 수 있습니다.	단방향 전용(구성 불가). 사전 필터 규칙은 소스-대상 트래픽만 매치합니다.
추가 분석을 위한 세션 영역 다시 지정	지원됨, 터널 영역 사용(터널 영역 및 사전 필터링, 15 페이지 참조).	지원되지 않음

사전 필터링 및 액세스 제어 비교

사전 필터 정책과 액세스 제어 정책은 모두 트래픽을 차단하고 신뢰하도록 해 주지만 사전 필터링 '신뢰' 기능은 더 많은 검사를 건너뛰기 때문에 '단축 경로 설정(fastpathing)'이라고 합니다. 다음 표에서는 맞춤형 사전 필터링을 구성해야 하는지 결정하는 데 도움이 되도록 사전 필터링과 액세스 제어의 이러한 차이점 및 그 밖의 차이점을 설명합니다.

맞춤형 사전 필터링을 구성하지 않는 경우, 액세스 제어 정책에서 조기 배치된 Block(차단) 및 Trust(신뢰) 규칙으로 사전 필터 기능을 비슷하게 모방할 수 있을 뿐 복제할 수는 없습니다.

특성	사전 필터링	액세스 제어	자세한 내용은 다음을 참고하십시오.
기본 기능	특정 유형의 일반 텍스트 통과 터널을 신속히 단축 경로 지정 또는 차단(캡슐화 규칙 조건, 15 페이지 참조)하거나 캡슐화된 트래픽에 맞게 후속 검사를 조정합니다. 조기에 처리하는 것이 유리한 그 밖의 연결도 단축 경로를 지정하거나 차단할 수 있습니다.	상황별 정보 및 심층 검사 결과를 포함하여 간단하거나 복잡한 기준을 사용하여 모든 네트워크 트래픽을 검사하고 제어합니다.	사전 필터링 정보, 1 페이지

특성	사전 필터링	액세스 제어	자세한 내용은 다음을 참고하십시오.
구현	사전 필터 정책. 사전 필터 정책은 액세스 제어 정책에 의해 호출됩니다.	액세스 제어 정책 액세스 제어 정책은 주요 구성입니다. 액세스 제어 정책은 하위 정책 호출 외에도 자체 규칙을 갖습니다.	사전 필터 정책 정보, 1 페이지 액세스 제어에 다른 정책 연결
액세스 제어 내 순서	첫 번째. 시스템은 다른 모든 액세스 제어 구성 전에 트래픽과 사전 필터 기준의 일치를 확인합니다.	—	—
규칙 작업	더 적습니다. 추가 검사(단축 경로 지정 및 차단)를 중지하거나 나머지 액세스 제어(분석)로 추가 분석을 허용할 수 있습니다.	자세한 내용. 액세스 제어 규칙에는 모니터링, 심층 검사, 차단 후 재설정, 인터랙티브 차단을 포함하여 훨씬 다양한 작업이 있습니다.	터널 및 사전 필터 규칙 구성 요소, 10 페이지 액세스 제어 규칙 작업
우회 기능	단축 경로 지정 규칙 작업. 사전 필터 단계에서 트래픽 단축 경로를 지정하면 다음을 포함한 모든 추가 검사 및 처리를 우회합니다. • 보안 인텔리전스 • ID 정책이 적용하는 인증 요건 • SSL 암호 해독 • 액세스 제어 규칙 • 패킷 페이로드 심층 검사 • 검색 • 속도 제한	Trust(신뢰) 규칙 작업. 액세스 제어 규칙이 신뢰할 수 있는 트래픽은 심층 검사 및 검색에서만 제외됩니다.	액세스 제어 규칙 소개

특성	사전 필터링	액세스 제어	자세한 내용은 다음을 참고하십시오.
규칙 기준	제한적. 사전 필터 정책의 규칙은 IP 주소, VLAN 태그, 포트, 프로토콜 등 간단한 네트워크 기준을 사용합니다. 터널의 경우, 터널 엔드포인트 조건은 터널 양쪽에 있는 네트워크 디바이스의 라우팅된 인터페이스의 IP 주소를 지정합니다.	강력합니다. 액세스 제어 규칙은 네트워크 기준뿐 아니라 사용자, 애플리케이션, 요청된 URL 및 패킷 페이로드에서 사용할 수 있는 기타 상황별 정보도 사용합니다. 네트워크 조건은 소스 및 대상 호스트의 IP 주소를 지정합니다.	터널 규칙과 사전 필터 규칙 비교, 2 페이지 사전 필터 규칙 조건, 12 페이지 터널 규칙 조건, 15 페이지
사용되는 IP 헤더(터널 처리)	가장 바깥쪽입니다. 외부 헤더를 사용하면 전체 일반 텍스트, 통과 터널을 처리할 수 있습니다. 비캡슐화 트래픽의 경우, 사전 필터링은 '외부' 헤더(이 경우에는 유일한 헤더)를 계속 사용합니다.	가장 안쪽도 가능합니다. 암호화되지 않은 터널의 경우, 액세스 제어는 전체 터널이 아니라 캡슐화된 개별 연결에 적용됩니다.	통과 터널 및 액세스 제어, 5 페이지
추가 분석을 위해 캡슐화된 연결 영역 다시 지정	터널링된 트래픽 영역을 다시 지정합니다. 터널 영역을 사용하면 사전 필터링된 캡슐화된 트래픽에 맞게 후속 검사를 조정할 수 있습니다.	터널 영역을 사용합니다. 액세스 제어는 사전 필터링 중에 할당하는 터널 영역을 사용합니다.	터널 영역 및 사전 필터링, 15 페이지
연결 로깅	단축 경로가 지정되고 차단된 트래픽만. 허용되는 연결은 다른 구성에 의해 계속 로깅될 수 있습니다.	모든 연결.	
지원되는 장치	Secure Firewall Threat Defense 수정할 수 있습니다.	All.	—

통과 터널 및 액세스 제어

일반 텍스트(암호화되지 않은) 터널은 종종 불연속 네트워크 사이를 흐르는 다중 연결을 캡슐화할 수 있습니다. 이러한 터널은 IP 네트워크를 통한 맞춤형 프로토콜, IPv4 네트워크를 통한 IPv6 트래픽 등을 라우팅하는 데 특히 유용합니다.

외부 캡슐화 헤더는 터널 양쪽에 있는 네트워크 디바이스의 라우티드 인터페이스인 터널 엔드포인트의 소스 및 대상 IP 주소를 지정합니다. 내부 페이로드 헤더는 캡슐화된 연결의 실제 엔드포인트의 소스 및 대상 IP 주소를 지정합니다.

네트워크 보안 디바이스는 종종 일반 텍스트 터널을 통과 트래픽으로 처리합니다. 즉, 해당 디바이스는 터널 엔드포인트 중 하나가 아닙니다. 그 대신, 이러한 디바이스는 터널 엔드포인트 간에 구축되고 터널 엔드포인트 간의 트래픽 플로우를 모니터링합니다.

(Secure Firewall Threat Defense 대신) Cisco ASA 소프트웨어를 실행하는 Cisco ASA 방화벽과 같은 일부 네트워크 보안 디바이스는 외부 IP 헤더를 사용하여 보안 정책을 시행합니다. 일반 텍스트 터널의 경우에도, 이러한 디바이스는 캡슐화된 개별 연결 및 해당 페이로드를 제어할 수 없거나 이를 파악할 수 없습니다.

이와 달리, Firepower System은 다음과 같이 액세스 제어를 활용합니다.

- 외부 헤더 평가 — 첫째, 사전 필터링이 외부 헤더를 사용하여 트래픽을 처리합니다. 이 단계에서 전체 일반 텍스트, 통과 터널을 차단하거나 단축 경로를 지정할 수 있습니다.
- 내부 헤더 평가 — 그 다음, 나머지 액세스 제어(및 QoS 같은 기타 기능) 기능은 가장 내부에 있는 탐지 가능한 수준의 헤더를 사용하여 가장 세부적인 수준의 검사 및 처리를 보장합니다.

  통과 터널이 암호화되지 않은 경우, 이 단계에서 시스템은 캡슐화된 개별 연결에서 작동합니다. 모든 캡슐화된 연결에서 작동하려면 (터널 영역 및 사전 필터링, 15 페이지 참조) 터널의 영역을 다시 지정해야 합니다.

액세스 제어로는 암호화된 통과 터널을 파악할 수 없습니다. 예를 들어 액세스 제어 규칙은 통과 VPN 터널을 하나의 연결로 간주합니다. 시스템은 외부의 캡슐화 헤더에 있는 정보만 사용하여 전체 터널을 처리합니다.

단축경로(Fastpath) 모범 사례

사전 필터 규칙에서 fastpath 작업을 사용하는 경우 일치하는 트래픽은 검사를 우회하고 디바이스를 통해 전송됩니다. 신뢰할 수 있지만 사용 가능한 보안 기능을 활용할 수 없는 트래픽에 대해 이 작업을 사용합니다.

다음 트래픽 유형은 단축 경로 지정에 적합합니다. 예를 들어 엔드포인트 또는 서버의 IP 주소를 오가는 모든 트래픽의 경로를 단축하도록 규칙을 구성할 수 있습니다. 사용되는 포트를 기준으로 규칙을 추가로 제한할 수 있습니다.

- 디바이스를 통과하는 사이트 간 VPN 트래픽입니다. 즉, 디바이스는 VPN 토폴로지의 엔드포인트가 아닙니다.
- 스캐너 트래픽. 스캐너 프로브는 침입 정책에서 많은 오탐 응답을 생성할 수 있습니다.
- 비디오/비디오.
- 백업.
- threat defense 디바이스를 통과하는 관리 트래픽입니다. 액세스 제어 정책을 사용하여 관리 트래픽에 대한 심층 검사를 수행하면 문제가 발생할 수 있습니다.

캡슐화된 트래픽 처리 모범 사례

이 항목에서는 다음 유형의 캡슐화된 트래픽에 대한 지침을 설명합니다.

- GRE(일반 라우팅 캡슐화)
- PPTP(Point-to-Point Protocol)
- IPinIP
- IPv6inIP
- Teredo

매니지드 디바이스에 대한 **Snort** 버전 지원 이해

매니지드 디바이스에서 사용하는 검사 엔진을 Snort라고 합니다. Snort 3은 Snort 2보다 더 많은 기능을 지원합니다. 이러한 기능이 네트워크의 매니지드 디바이스에 어떤 영향을 미치는지 이해하려면 다음을 알아야 합니다.

- 디바이스에서 지원하는 Snort 버전

  Snort 버전 지원은 *Cisco Firepower* 호환성 가이드의 번들 구성 요소에 대한 섹션에서 확인할 수 있습니다.

- management center 및 threat defense 소프트웨어가 Snort 2 및 Snort 3을 지원하는 방법

  Snort 2 및 Snort 3의 제한 사항은 Cisco Secure Firewall Management Center Snort 3 구성 가이드의 *Management Center* 매니지드 *Threat Defense*에 대한 *Snort 3*의 기능 제한 사항에서 확인할 수 있습니다.

GRE v1 및 **PPTP** 우회 외부 플로우 처리

GRE v1(상태 저장 *GRE*라고도 함) 및 PPTP 트래픽은 외부 플로우 처리를 우회합니다.

승객 플로우 처리는 IPv6inIP 및 Teredo에 대해 지원되지만 다음 제한 사항이 적용됩니다.

- 세션이 로드 밸런싱되지 않은 단일 터널을 통해 이루어집니다.
- HA 또는 클러스터링 복제 없음
- 기본 및 보조 플로우 관계가 유지되지 않음
- 사전 필터 정책 화이트리스트 및 블랙리스트가 지원되지 않음

GRE v0 시퀀스 번호 필드는 선택 사항이어야 함

네트워크에서 트래픽을 전송하는 모든 엔드포인트는 시퀀스 번호 필드를 선택 사항으로 사용하여 GREv0 트래픽을 전송해야 합니다. 그렇지 않으면 시퀀스 번호 필드가 제거됩니다. RFC 1701 및 RFC 2784는 모두 시퀀스 필드를 선택 사항으로 지정합니다.

인터페이스에서 터널이 작동하는 방식

사전 필터 및 액세스 제어 정책 규칙은 라우팅, 투명, 인라인 집합, 인라인 탭 및 패시브 인터페이스의 모든 터널 유형에 적용됩니다.

참조

GRE 및 PPTP 프로토콜에 대한 자세한 내용은 다음을 참조하십시오.

- RFC 1701, RFC 2784 및 RFC 2890 (GRE 프로토콜 v0)
- RFC 2637(PPTP 및 GRE 프로토콜 v1)

사전 필터 정책 요구 사항 및 사전 요건

모델 지원

Threat Defense

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

사전 필터링 설정

맞춤형 사전 필터링을 수행하려면 사전 필터 정책을 구성하고 액세스 제어 정책에 정책을 할당합니다. 액세스 제어 정책을 통해 사전 필터 정책이 매니지드 디바이스에 할당됩니다.

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** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Prefilter(**사전 필터**)**을(를) 선택합니다.

단계 **2** **New Policy(**새 정책**)**을 클릭하여 맞춤형 사전 필터 정책을 생성합니다.

새 사전 필터 정책에는 Analyze all tunnel traffic(모든 터널 트래픽 분석)에 대한 규칙 및 기본 작업이 없습니다. 이 정책은 로깅을 수행하거나 터널 영역을 다시 지정하지 않습니다. 기존 정책을 **Copy(**복사**)** ( )하거나 **Edit(**수정**)** ( )할 수도 있습니다.

단계 **3** 사전 필터 정책의 기본 작업 및 로깅 옵션을 구성합니다.

- 기본 작업 — 지원되는 일반 텍스트, 통과 터널에 대한 기본 작업을 **Analyze all tunnel traffic(**모든 터널 트래픽 분석**)**(액세스 제어 포함) 또는 **Block all tunnel traffic(**모든 터널 트래픽 차단**)** 중에서 선택합니다.
- 기본 작업 로깅 - 기본 작업 옆의 **Logging(**로깅**)** ( )을 클릭합니다.을 참조하십시오. 차단된 터널에 대해서만 기본 작업 로깅을 구성할 수 있습니다.

단계 **4** 터널 및 사전 필터 규칙을 구성합니다.

맞춤형 사전 필터 정책에서 순서에 상관없이 두 가지 규칙을 모두 사용할 수 있습니다. 일치할 특정 유형의 트래픽, 그리고 수행하려는 작업이나 추가 분석에 따라 규칙을 생성합니다(터널 규칙과 사전 필터 규칙 비교, 2 페이지 참조).

주의 터널 규칙을 사용하여 터널 영역을 할당할 경우 주의하십시오. 향후 평가 시, 영역이 다시 지정된 터널의 연결은 보안 영역 제약 조건과 일치하지 않을 수 있습니다. 자세한 내용은 터널 영역 및 사전 필터링, 15 페이지를 참고하십시오.

규칙 구성 요소를 구성하는 방법에 대한 자세한 내용은 터널 및 사전 필터 규칙 구성 요소, 10 페이지의 내용을 참조하십시오.

단계 **5** 규칙 순서를 평가합니다. 규칙을 이동하려면 클릭하여 끌거나, 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

규칙을 올바르게 생성하고 순서를 지정하는 것은 복잡한 작업이지만, 효과적인 구축에 필수적입니다. 정책을 신중하게 계획하지 않을 경우, 규칙이 다른 규칙을 선점하거나 잘못된 컨피그레이션을 포함할 수 있습니다. 자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례를 참고하십시오.

단계 **6** 사전 필터 정책을 저장합니다.

단계 **7** 터널 영역 제약 조건을 지원하는 컨피그레이션의 경우, 영역이 다시 지정된 터널을 올바르게 처리합니다.

터널 영역을 소스 영역 제약 조건으로 사용하면서 영역 재지정 터널에서 연결을 매치합니다.

단계 **8** 사전 필터 정책을 매니지드 디바이스에 구축된 액세스 제어 정책과 연결합니다.

액세스 제어에 다른 정책 연결의 내용을 참조하십시오.

단계 **9** Deploy configuration changes(구성 변경 사항 구축)참조.

참고 사전 필터 정책을 구축할 때 해당 규칙은 기존 터널 세션에 적용되지 않습니다. 따라서 기존 연결의 트래픽은 구축된 새 정책에 의해 바인딩되지 않습니다. 또한 정책 적중 횟수는 정책과 일치하는 연결의 첫 번째 패킷에 대해서만 증가합니다. 따라서 정책과 일치할 수 있는 기존 연결의 트래픽은 적중 횟수에서 생략됩니다. 정책 규칙을 효과적으로 적용하려면 기존 터널 세션을 지운 다음 정책을 구축합니다.

다음에 수행할 작업

시간 기반 규칙을 구축할 경우, 정책이 할당된 디바이스의 표준 시간대를 지정합니다. 정책 애플리케이션에 대한 디바이스 표준 시간대 구성의 내용을 참조하십시오.

터널 및 사전 필터 규칙 구성 요소

상태(활성화/비활성화)

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

위치

규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽과 일치하는 첫 번째 규칙은 규칙 유형(터널 또는 사전 필터)에 관계없이 트래픽을 처리하는 규칙입니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하고 로깅하는 방법을 결정합니다.

- Fastpath(단축 경로) - 액세스 제어, ID 요건, 속도 제한 등의 모든 이후 검사와 제어에서 일치하는 트래픽을 제외합니다. 터널을 빠른 경로로 지정하면 캡슐화된 모든 연결이 빠른 경로로 지정됩니다.
- Block(차단) - 어떤 종류든 추가 검사 없이 일치하는 트래픽을 차단합니다. 터널을 차단하면 캡슐화된 모든 연결이 차단됩니다.
- Analyze(분석) - 내부 헤더를 사용하여 나머지 액세스 제어를 통해 트래픽을 계속 분석할 수 있습니다. 트래픽이 액세스 제어 및 관련 심층 검사에서 통과하는 경우 트래픽 속도도 제한할 수 있습니다. 터널 규칙의 경우, Assign Tunnel Zone(터널 영역 할당) 옵션으로 영역 다시 지정을 활성화합니다.

방향(터널 규칙에만 해당)

터널 규칙의 방향에 따라 시스템의 소스 및 대상 기준으로 다음 작업을 수행하는 방식이 결정됩니다.

- 소스로부터만 터널 매치(단방향) - 소스-대상 트래픽만 매치합니다. 매치하는 트래픽은 지정된 소스 인터페이스 또는 터널 엔드포인트 중 하나에서 시작되고 대상 인터페이스 또는 터널 엔드포인트 중 하나에서 끝나야 합니다.
- 소스 및 대상으로부터 터널 매치(양방향) - 소스-대상 트래픽과 대상-소스 트래픽 모두 매치합니다. 두 개의 단방향 규칙을 작성하는 데 미치는 영향은 동일하며, 한쪽이 다른 한쪽을 미러링합니다.

사전 필터 규칙은 항상 단방향입니다.

터널 영역 할당**(**터널 규칙에만 해당**)**

터널 규칙의 경우, 터널 영역(기존 또는 즉시 생성된 영역 모두 해당)을 할당하면 일치하는 터널의 영역이 다시 지정됩니다. 영역을 다시 지정하려면 Analyze(분석) 작업을 수행해야 합니다.

터널의 영역을 다시 지정하면 기타 컨피그레이션(예: 액세스 제어 규칙)은 모든 터널의 캡슐화된 연결을 서로에게 속한 것으로 인식할 수 있습니다. 터널의 할당된 터널 영역을 인터페이스 제약 조건으로 사용하여, 검사를 캡슐화된 연결에 맞춤 설정할 수 있습니다. 자세한 내용은 터널 영역 및 사전 필터링, 15 페이지를 참고하십시오.

주의 터널 영역을 할당할 경우 주의하십시오. 향후 평가 시, 영역이 다시 지정된 터널의 연결은 보안 영역 제약 조건과 일치하지 않을 수 있습니다. 터널 영역 구현에 대한 간략한 단계별 안내, 그리고 영역이 다시 지정된 트래픽을 명시적으로 처리하지 않고 영역을 다시 지정했을 때 발생하는 영향에 대한 내용은 터널 영역 사용, 16 페이지을 참조하십시오.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 트래픽은 규칙과 일치하는 모든 규칙의 조건과 일치해야 합니다. 각 조건 유형은 규칙 편집기에 고유한 탭이 있습니다.

다음 외부 헤더 제약 조건을 사용하여 트래픽을 사전 필터링할 수 있습니다. 캡슐화 프로토콜별로 터널 규칙을 제한해야 합니다.

- 인터페이스 —인터페이스 규칙 조건
- 네트워크(사전 필터 규칙)/터널 엔드포인트(터널 규칙) -네트워크 규칙 조건
- VLAN —VLAN 태그 규칙 조건
- 포트(사전 필터 규칙)/캡슐화 및 포트(터널 규칙) - 사전 필터 규칙에 대한 포트 규칙 조건, 14 페이지 또는 캡슐화 규칙 조건, 15 페이지
- 시간 범위—시간 및 날짜 규칙 조건

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다.

터널 및 사전 필터 규칙에서는 단축 경로가 지정되고 차단된 트래픽을 로깅할 수 있습니다(단축 경로 및 차단 작업). 추가 분석(분석 작업)할 트래픽의 경우, 다른 컨피그레이션에 의해 일치하는 연결이 계속 로깅될 수 있긴 하지만 사전 필터 정책에서 로깅이 비활성화됩니다. 기록은 캡슐화 플로우가 아닌 내부 플로우에서 수행됩니다.

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.

규칙을 저장한 후에는 이러한 코멘트를 수정하거나 삭제할 수 없습니다.

관련 항목

액세스 제어 규칙 순서에 대한 모범 사례

사전 필터 규칙 조건

규칙 조건을 사용하면 제어하려는 네트워크를 대상으로 사전 필터 정책을 미세 조정할 수 있습니다. 자세한 내용은 다음 섹션 중 하나를 참조하십시오.

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 ID 규칙에서 FDQN 네트워크 개체를 사용할 수 없습니다.

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 Threat Defense - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 다른 모든 모델의 Threat Defense:
  - 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.

사전 필터 규칙에 대한 포트 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.

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. 사전 필터 규칙의 다른 프로토콜과 일치하도록 포트 조건을 구성할 수 있지만, GRE, IP in IP, IP in IPv6 및 Toredo Port 3544를 일치시킬 때는 터널 규칙을 대신 사용해야 합니다.

시간 및 날짜 규칙 조건

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.

터널 규칙 조건

규칙 조건을 사용하면 제어하려는 네트워크를 대상으로 터널 정책을 미세 조정할 수 있습니다. 터널 규칙의 경우 다음 조건을 사용할 수 있습니다.

- **Interface Objects(**인터페이스 개체**)** - 연결이 통과하는 디바이스 인터페이스를 정의하는 보안 영역 또는 인터페이스 그룹입니다. 인터페이스 규칙 조건의 내용을 참조하십시오.
- **Tunnel Endpoints(**터널 엔드포인트**)** - 터널의 소스 및 대상 IP 주소를 정의하는 네트워크 개체입니다.
- **VLAN Tags(VLAN** 태그**)** - 터널의 가장 바깥쪽 VLAN 태그입니다. VLAN 태그 규칙 조건의 내용을 참조하십시오.
- **Encapsulation and Ports(**캡슐화 및 포트**)** - 터널의 캡슐화 프로토콜입니다. 캡슐화 규칙 조건, 15 페이지의 내용을 참조하십시오.
- **Time Range(**시간 범위**)** - 규칙이 활성화된 요일과 시간입니다. 시간 범위를 지정하지 않을 경우 규칙은 항상 활성 상태입니다. 시간 및 날짜 규칙 조건의 내용을 참조하십시오.

캡슐화 규칙 조건

캡슐화 조건은 터널 규칙에만 적용됩니다.

이 조건은 캡슐화 프로토콜에 따라 특정 유형의 일반 텍스트, 통과 터널을 제어합니다. 규칙을 저장하려면 먼저 하나 이상의 일치하는 프로토콜을 선택해야 합니다. 다음 중에서 선택할 수 있습니다.

- GRE(47)
- IP-in-IP(4)
- IPv6-in-IP(41)
- Teredo(UDP(17)/3455)

터널 영역 및 사전 필터링

터널 영역은 사전 필터링을 사용하여 후속 트래픽 처리를 캡슐화된 연결에 맞춰 설정할 수 있도록 지원합니다.

일반적으로 시스템은 가장 내부에 있는 탐지 가능한 수준의 헤더를 사용하여 트래픽을 처리하므로 특수 메커니즘이 필요합니다. 이를 통해 가장 세부적인 수준의 검사를 보장할 수 있습니다. 그러나 이는 통과 터널이 암호화되지 않은 경우, 시스템은 캡슐화된 개별 연결에서 작동한다는 것을 의미하기도 합니다(통과 터널 및 액세스 제어, 5 페이지 참조).

터널 영역으로 이 문제를 해결할 수 있습니다. 액세스 제어의 첫 번째 단계(사전 필터링) 동안 외부 헤더를 사용하여 특정 유형의 일반 텍스트, 통과 터널을 식별할 수 있습니다. 그런 다음, 맞춤형 터널 영역을 할당하여 이러한 터널의 영역을 다시 지정할 수 있습니다.

터널의 영역을 다시 지정하면 기타 컨피그레이션(예: 액세스 제어 규칙)은 모든 터널의 캡슐화된 연결을 서로에게 속한 것으로 인식할 수 있습니다. 터널의 할당된 터널 영역을 인터페이스 제약 조건으로 사용하여, 검사를 캡슐화된 연결에 맞춤 설정할 수 있습니다.

터널 영역은 이름과 달리, 보안 영역이 아닙니다. 터널 영역은 인터페이스 집합을 의미하지 않습니다. 터널 영역은 일종의 태그로 간주하는 편이 더 정확하며, 캡슐화된 연결과 관련된 보안 영역을 대체하는 경우가 있습니다.

⚠

주의 터널 영역 제약 조건을 지원하는 컨피그레이션의 경우, 영역이 다시 지정된 터널의 연결은 보안 영역 제약 조건과 일치하지 않습니다. 예를 들어 터널의 영역을 다시 지정하면, 액세스 제어 규칙은 캡슐화된 연결을 원래 보안 영역이 아닌 새로 할당된 터널 영역과 일치시킬 수 있습니다.

터널 영역 구현에 대한 간략한 단계별 안내, 그리고 영역이 다시 지정된 트래픽을 명시적으로 처리하지 않고 영역을 다시 지정했을 때 발생하는 영향에 대한 내용은 터널 영역 사용, 16 페이지을 참조하십시오.

터널 영역 제약 조건을 지원하는 컨피그레이션

액세스 제어 규칙만 터널 영역 제약 조건을 지원합니다.

다른 컨피그레이션은 터널 영역 제약 조건을 지원하지 않습니다. 예를 들어 QoS를 사용하여 일반 텍스트 터널의 속도를 전체적으로 제한할 수 없으며, 캡슐화된 개별 세션만 속도를 제한할 수 있습니다.

터널 영역 사용

이 예시 절차에는 터널 영역을 사용하여 추가 분석을 위해 GRE 터널의 영역을 다시 지정할 수 있는 방법이 요약되어 있습니다. 일반 텍스트, 통과 터널의 캡슐화된 연결에 대한 트래픽 검사를 맞춤 설정해야 하는 다른 시나리오를 대상으로 이 예시에 설명된 개념을 응용할 수 있습니다.

조직의 내부 트래픽 플로우가 신뢰할 수 있는 보안 영역을 통과하는 상황을 고려해보십시오. 신뢰할 수 있는 보안 영역은 다양한 위치에 구축된 여러 매니지드 디바이스 전체의 인터페이스 집합을 나타냅니다. 조직의 보안 정책은 익스플로잇 및 악성코드에 대한 심층 검사 후 내부 트래픽을 허용해야 합니다.

내부 트래픽에 특정 엔드포인트 간의 일반 텍스트, 통과, GRE 터널이 포함될 때가 있습니다. 이러한 캡슐화된 트래픽의 트래픽 프로파일은 알려진 무해한 프로파일이라고 해도 "정상적인" 사내 활동과 다르기 때문에, 특정한 캡슐화된 트래픽에 대한 검사를 제한하는 동시에 보안 정책을 계속 준수할 수 있습니다.

이 예에서 컨피그레이션 변경 사항을 구축한 후의 결과는 다음과 같습니다.

- 신뢰할 수 있는 영역에서 탐지된 일반 텍스트, 통과, GRE 캡슐화 터널의 캡슐화된 개별 연결은 단일한 침입 및 파일 정책 집합으로 평가되었습니다.
- 신뢰할 수 있는 영역의 모든 기타 트래픽은 다른 침입 및 파일 정책으로 평가되었습니다.

GRE 터널의 영역을 다시 지정하여 이 작업을 수행합니다. 영역을 다시 지정하면 액세스 제어에서는 GRE 캡슐화 연결을 원래의 신뢰할 수 있는 보안 영역이 아닌 맞춤형 터널 영역과 연결합니다. 영역

을 다시 지정해야 하는 이유는 액세스 제어에서 캡슐화된 트래픽을 처리하는 방식 때문입니다(통과 터널 및 액세스 제어, 5 페이지 및 터널 영역 및 사전 필터링, 15 페이지 참조).

프로시저

단계 **1** 캡슐화된 트래픽에 심층 검사를 맞춤 설정하는 맞춤형 침입 및 파일 정책을 구성하고, 비 캡슐화된 트래픽에 맞춤 설정된 다른 침입 및 파일 정책을 구성합니다.

단계 **2** 맞춤형 사전 필터링을 구성하여 신뢰할 수 있는 보안 영역을 통과하는 GRE 터널의 영역을 다시 지정합니다.

맞춤형 사전 필터 정책을 생성하고 이를 액세스 제어와 연결합니다. 맞춤형 사전 필터 정책에서 터널 규칙(이 예에서는**GRE_tunnel_rezone**) 및 해당 터널 영역(**GRE_tunnel**)을 생성합니다. 자세한 내용은 사전 필터링 설정, 8 페이지를 참고하십시오.

표 ***1: GRE_tunnel_rezone*** 터널 규칙

규칙 구성 요소	설명
인터페이스 개체 조건	신뢰 보안 영역을 소스 인터페이스 개체 및 대상 인터페이스 개체 제약 조건 모두로 사용하면서 내부 전용 터널을 매치합니다.
터널 엔드포인트 조건	조직에서 사용된 GRE 터널에 대한 소스 및 대상 엔드포인트를 지정합니다. 터널 규칙은 기본적으로 양방향입니다. **Match tunnels from...(**다음의 터널 매치**)** 옵션을 변경하지 않으면 어떤 엔드포인트를 소스 및 대상으로 지정하는지는 중요하지 않습니다.
캡슐화 조건	GRE 트래픽과 일치합니다.
터널 영역 지정	**GRE_tunnel** 터널 영역을 생성하고, 이를 규칙과 일치하는 터널에 할당합니다.
작업	분석(나머지 액세스 제어와 함께 사용).

단계 **3** 영역이 다시 지정된 터널의 연결을 처리하기 위한 액세스 제어를 구성합니다.

매니지드 디바이스에 구축된 액세스 제어 정책에서, 영역을 다시 지정한 트래픽을 처리하는 규칙(이 예에서는 **GRE_inspection**)을 구성합니다. 자세한 내용은 액세스 제어 규칙 생성 및 수정를 참고하십시오.

표 ***2: GRE_inspection*** 액세스 제어 규칙

규칙 구성 요소	설명
보안 영역 조건	GRE_tunnel 보안 영역을 소스 영역 제약 조건으로 사용하면서 영역 재지정된 터널을 매치합니다.

규칙 구성 요소	설명
작업	허용(심층 검사 활성화됨). 캡슐화된 내부 트래픽을 검사하도록 맞춤 설정된 파일 및 침입 정책을 선택합니다.

주의 이 단계를 건너뛸 경우, 영역이 다시 지정된 연결은 보안 영역에 의해 제한되지 않는 모든 액세스 제어 규칙과 일치할 수 있습니다. 영역이 다시 지정된 연결이 액세스 제어 규칙과 일치하지 않을 경우, 이는 액세스 제어 정책 기본 작업으로 처리됩니다. 이 작업이 원하는 설정인지 확인하십시오.

단계 **4** 신뢰할 수 있는 보안 영역을 통과하는 비 캡슐화된 연결을 처리하기 위한 액세스 제어를 구성합니다.

동일한 액세스 제어 정책에서, 신뢰할 수 있는 보안 영역의 영역이 다시 지정되지 않은 트래픽을 처리하는 규칙(이 예에서는 **internal_default_inspection**)을 구성합니다.

표 ***3: internal_default_inspection*** 액세스 제어 규칙

규칙 구성 요소	설명
보안 영역 조건	신뢰 보안 영역을 보안 영역 및 대상 영역 제약 조건 모두로 사용하면서 영역 재지정되지 않은 내부 전용 트래픽을 매치합니다.
작업	허용(심층 검사 활성화됨). 비캡슐화된 내부 트래픽을 검사하도록 맞춤 설정된 파일 및 침입 정책을 선택합니다.

단계 **5** 기존 규칙과 관련하여 새 액세스 제어 규칙의 위치를 평가합니다. 필요한 경우 규칙 순서를 변경합니다.

새로운 액세스 제어 규칙 두 개를 나란히 함께 배치할 경우, 어떤 규칙을 먼저 배치해도 무관합니다. GRE 터널의 영역을 다시 지정했으므로, 두 가지 규칙이 서로를 선점할 수 없습니다.

단계 **6** 모든 변경된 컨피그레이션을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

터널 영역 생성

다음 절차에서는 개체 관리자에서 터널 영역을 생성하는 방법을 설명합니다. 터널 규칙을 편집할 때 영역을 생성할 수도 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.
단계 **2** 개체 유형 목록에서 **Tunnel Zone(**터널 영역**)**을 선택합니다.
단계 **3** **Add Tunnel Zone(**터널 영역 추가**)**을 클릭합니다.
단계 **4** **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 사전 필터링의 일부로 일반 텍스트, 통과 터널에 터널 영역을 할당합니다. 사전 필터링 설정, 8 페이지 참조.

사전 필터 규칙을 액세스 제어 정책으로 이동

액세스 제어 규칙을 액세스 제어 정책에서 연결된 사전 필터 정책으로 이동할 수 있습니다.

시작하기 전에

계속하기 전에 다음 사항에 유의하십시오.

- 사전 필터 규칙만 액세스 제어 정책으로 이동할 수 있습니다. 터널 규칙은 이동할 수 없습니다.
- 사전 필터 규칙은 연결된 액세스 제어 정책으로만 이동할 수 있습니다.
- 구성된 인터페이스 그룹이 있는 사전 필터 규칙은 이동할 수 없습니다.
- 이동하면 사전 필터 규칙의 **Action(**작업**)** 매개 변수가 액세스 제어 규칙의 적절한 작업으로 변경됩니다. 사전 필터 규칙의 각 작업이 무엇에 매핑되는지 확인하려면 다음 표를 참조하십시오.

사전 필터 규칙의 작업	액세스 제어 규칙 작업
분석	허용
차단	Block(차단)
Fastpath(단축 경로)	신임

- 마찬가지로 사전 필터 규칙에 구성된 작업을 기반으로 다음 표에 나와 있는 것처럼 규칙을 이동한 후 로깅 구성이 적절한 설정으로 설정됩니다.

사전 필터 규칙의 작업	액세스 제어 규칙에서 활성화된 로깅 구성
분석	활성화된 로그 설정이 없습니다.

사전 필터 규칙의 작업	액세스 제어 규칙에서 활성화된 로깅 구성
Block(차단)	• Log at Beginning of Connection(연결 시작 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩
Fastpath(단축 경로)	• Log at Beginning of Connection(연결 시작 시 로깅) • Log at End of Connection(연결 종료 시 로깅) • 이벤트 뷰어 • Syslog 서버 • SNMP 트랩

- 규칙을 이동하면 사전 필터 규칙 구성의 코멘트가 손실됩니다. 그러나 소스 사전 필터 정책을 언급하는 새로운 주석이 이동된 규칙에 추가됩니다.
- 소스 정책에서 규칙을 이동하는 동안 다른 사용자가 해당 규칙을 수정하면 FMC에 메시지가 표시됩니다. 페이지를 새로 고친 후 프로세스를 계속 진행할 수 있습니다.

프로시저

단계 **1** 사전 필터 정책 편집기에서 마우스 왼쪽 버튼을 클릭하여 이동할 규칙을 선택합니다.

팁 여러 규칙을 선택하려면 키보드에서 Ctrl(컨트롤) 키를 사용합니다.

단계 **2** 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Move to another policy(**다른 정책으로 이동**)**를 선택합니다.

단계 **3** **Access Policy(**액세스 정책**)** 드롭 다운 목록에서 대상 액세스 제어 정책을 선택합니다.

단계 **4** **Place Rules(**규칙 배치**)** 드롭 다운 목록에서 이동한 규칙을 배치할 위치를 선택합니다.

- **Default(**기본값**)** 섹션에서 마지막 규칙 집합으로 배치하려면 **At the bottom(**맨 아래 **)(Default(**기본**)** 섹션 내**)**를 선택합니다.
- **Mandatory(**의무**)** 섹션에서 첫번째 규칙 집합으로 배치하려면 **At the top(**맨 위 **)(Mandatory(**의무**)** 섹션 내**)**를 선택합니다.

단계 **5** **Move(**이동**)**를 클릭합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

사전 필터 정책 적중 횟수

적중 횟수는 정책 규칙이 일치하는 연결을 트리거한 횟수를 나타냅니다.

사전 필터 정책 적중 횟수 보기에 대한 자세한 내용은 정책 적중 횟수 보기를 참조하십시오.

대규모 플로우 오프로드

FXOS를 실행하는 디바이스(예:Firepower 4100/9300 섀시)에서 사전 필터 정책에 의해 단축 경로가 되도록 구성하는 특정 트래픽은 threat defense 소프트웨어가 아닌 하드웨어(특히 NIC)에서 처리됩니다. 이러한 연결 플로우를 오프로드하면 처리량이 증가하고, 특히 다량 파일 전송과 같은 데이터 집약적인 애플리케이션의 경우 레이턴시가 낮아집니다. 이 기능은 특히 데이터 센터에 유용합니다. 이것을 정적 플로우 오프로드라고 합니다.

또한 기본적으로 threat defense 디바이스 오프로드는 신뢰를 비롯한 다른 기준에 따라 플로우를 오프로드합니다. 이것을 동적 플로우 오프로드라고 합니다.

오프로드 플로우는 기본 TCP 플래그 및 옵션 확인 등 제한된 상태를 추적할 수 있는 검사를 계속 진행합니다. 시스템은 필요한 경우 추가 처리를 위해 선택적으로 패킷을 방화벽 시스템에 에스컬레이트할 수 있습니다.

대규모 플로우 오프로드의 이점을 누릴 수 있는 애플리케이션의 예는 다음과 같습니다.

- HPC(고성능 컴퓨팅) 연구 사이트는 스토리지와 고성능 컴퓨팅 스테이션 간 threat defense 디바이스가 구축되는 곳입니다. 하나의 연구 사이트가 FTP 파일 전송 또는 NFS를 통한 파일 동기화를 통해 백업되면 대규모 데이터 트래픽이 모든 연결에 영향을 끼칩니다. FTP 파일 전송 및 NFS를 통한 파일 전송을 오프로드하면 다른 트래픽에 끼치는 영향을 줄일 수 있습니다.
- HTF(고주파수 거래)는 주로 규정 준수를 위해 워크스테이션과 익스체인지 간 threat defense 디바이스가 구축되는 곳입니다. 보안은 주요 관심사가 아니지만 지연은 주요 관심사입니다.

다음 유형의 플로우는 오프로드할 수 없습니다.

- (정적 플로우 오프로드에만 해당합니다.) 사전 필터 정책에 따라 단축 경로가 지정됩니다.
- 표준 또는 802.1Q 태그 지정된 이더넷 프레임에만 해당합니다.
- (동적 플로우 오프로드에만 해당합니다.)
  - 검사 완료된 플로우는 검사 엔진이 검사가 필요하지 않다고 결정한 것입니다. 이러한 플로우는 다음과 같습니다.
    - 신뢰 작업을 적용하며 보안 영역, 소스 및 대상 네트워크 및 포트 일치만 기반으로 하는 액세스 제어 규칙에 의해 처리되는 플로우입니다.

- SSL 정책을 사용하여 암호 해독을 위해 선택되지 않은 TLS/SSL 플로우.
- 명시적이거나 플로우 우회 한도 초과로 IAB(Intelligent Application Bypass) 정책에 의해 신뢰할 수 있는 플로우입니다.
- 플로우를 신뢰하게 하는 파일 또는 침입 정책과 일치하는 플로우입니다.
- 더 이상 검사할 필요가 없는 허용되는 모든 플로우

- 다음 IPS 전처리기 흐름을 검사합니다.
  - SSH 및 SMTP
  - FTP 전처리기 보조 연결을 검사합니다.
  - SIP(세션 시작 프로토콜) 전처리기 보조 연결을 검사합니다.
- (옵션이라고도 하는) 키워드를 사용하는 침입 규칙

중요 위의 세부 사항, 예외 및 제한 사항은 플로우 오프로드 제한, 23 페이지의 내용을 참조하십시오.

정적 플로우 오프로드 사용

적합한 트래픽을 하드웨어에 오프로드하려면 **Fastpath** 작업에 적용되는 사전 필터 정책 규칙을 생성합니다. TCP/UPD에 사전 필터 규칙을, GRE에 터널 규칙을 사용합니다.

(Not recommended.) 정적 플로우 오프로드를 비활성화하고 부산물로서 제품의 동적 플로우 오프로드를 비활성화하려면 FlexConfig를 사용하여 **no flow-offload enable** 명령을 실행합니다. 이 명령에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html에서 제공되는 *Cisco ASA Series Command Reference*를 참조하십시오.

동적 플로우 오프로드 사용

동적 플로우 오프로드는 지원되지 않는 Secure Firewall 3100와 같은 디바이스를 제외하고 .

동적 오프로드를 비활성화하려면

```
> configure flow-offload dynamic whitelist disable
```

동적 오프로드를 다시 활성화하려면

```
> configure flow-offload dynamic whitelist enable
```

동적 오프로드는 사전 필터링의 구성 여부에 관계 없이 정적 플로우 오프로드가 활성화된 경우에만 발생합니다.

플로우 오프로드 제한

모든 플로우의 오프로드가 가능한 것은 아닙니다. 오프로드 후에도 특정 조건을 만족하는 경우 플로우가 오프로드에서 제거될 수 있습니다. 다음은 몇 가지 제한 사항입니다.

오프로드가 불가능한 플로우

다음 유형의 플로우는 오프로드할 수 없습니다.

- IPv4 주소 지정을 사용하지 않는 모든 플로우(예: IPv6 주소 지정).
- TCP, UDP, GRE 외의 프로토콜을 사용하는 플로우

참고 PPTP GRE 연결은 오프로드할 수 없습니다.

- 패시브, 인라인, 인라인 탭 모드에서 구성된 인터페이스의 플로우 라우팅 및 스위치 인터페이스 유형만 지원됩니다.
- Snort 또는 다른 검사 엔진에서 검사해야 하는 플로우 FTP와 같은 일부 경우에는 제어 채널은 오프로드되지 않지만 보조 데이터 채널은 오프로드될 수 있습니다.
- 디바이스에서 종료되는 IPsec 및 TLS/DTLS VPN 연결.
- 암호화 또는 암호 해독이 필요한 플로우 예를 들어, SSL 정책으로 인해 연결이 암호 해독되었습니다.
- 라우팅 모드의 멀티캐스트 플로우 이는 브리지 그룹에 멤버 인터페이스가 2개 뿐인 경우 투명 모드에서 지원됩니다.
- TCP 인터셉트 플로우
- TCP 상태 우회 플로우. 동일한 트래픽에서 플로우 오프로드 및 TCP 상태 우회를 구성할 수 없습니다.
- 보안 그룹 태그가 지정된 플로우
- 하나의 클러스터에 대해 비대칭플로우일 때 다른 클러스터 노드에서 포워딩된 역방향 플로우
- 플로우 소유자가 제어 유닛이 아닌 경우 클러스터에 중앙 집중된 플로우
- 동적 오프로드가 불가능한 IP 옵션을 포함한 플로우

추가 제한 사항

- 플로우 오프로드 및 DCD(Dead Connection Detection)가 호환되지 않습니다. 오프로드할 수 있는 연결에서 DCD를 구성하지 마십시오.
- 플로우 오프로드 조건과 일치하는 둘 이상의 플로우가 하드웨어의 동일한 위치에 동시에 오프로드되도록 대기열에 있는 경우 첫 번째 플로우만 오프로드됩니다. 다른 플로우는 정

상적으로 처리됩니다. 이를 충돌이라고합니다. 이 상황에 대한 통계를 표시하려면 CLI에서 **show flow-offload flow** 명령을 사용합니다.

- 동적 플로우 오프로드는 모든 TCP 노멀라이저 검사를 비활성화합니다.
- 오프로드된 플로우는 FXOS 인터페이스를 통과하지만 이러한 플로우에 대한 통계는 논리적 디바이스 인터페이스에 표시되지 않습니다. 따라서 논리적 디바이스 인터페이스 카운터 및 패킷 속도는 오프로드된 플로우를 반영하지 않습니다.

역방향 오프로드 조건

플로우 오프로드 이후 플로우 내 패킷이 다음 조건을 만족할 경우 추가 처리를 위해 threat defense로 반환됩니다.

- 타임스탬프 이외의 TCP 옵션이 포함됩니다.
- 프래그먼트화됩니다.
- 이들은 ECMP(Equal-cost Multi-path) 라우팅의 대상이며 인그래스 패킷은 하나의 인터페이스에서 다른 인터페이스로 이동합니다.