DNS 정책

다음 주제에서는 DNS 정책, DNS 규칙 및 매니지드 디바이스에 DNS 정책을 구축하는 방법을 설명합니다.

DNS 정책 개요

DNS 기반 보안 인텔리전스를 사용하면 클라이언트가 요청한 도메인 이름을 바탕으로 보안 인텔리전스 차단 목록을 통해 트래픽을 차단할 수 있습니다. Cisco에서는 트래픽을 필터링하는 데 사용할 수 있는 도메인 이름 인텔리전스를 제공합니다. 또한 환경에 맞는 도메인 이름 목록 및 피드를 사용자 설정할 수도 있습니다.

DNS 정책 차단 목록의 트래픽은 즉시 차단되므로 침입, 익스플로잇, 악성코드에 대한 추가 검사 대상이 되지 않을 뿐 아니라 네트워크 검색 대상도 되지 않습니다. 보안 인텔리전스 차단 안 함 목록을 사용하여 차단 목록을 재정의하고 액세스 제어 규칙 평가를 강제 적용할 수 있으며 보안 인텔리전트 필터링에 "모니터링 전용" 설정을 사용할 수도 있습니다(패시브 구축에 권장됨). 이렇게 하면 시스템에서 차단 목록에 의해 차단되었을 가능성이 있는 연결을 분석할 수 있을 뿐 아니라 차단 목록과 일치하는 항목을 로깅하고 연결 종료 보안 인텔리전스 이벤트를 생성할 수 있습니다.

참고 DNS 서버가 만료로 인해 도메인 캐시를 삭제하거나 클라이언트의 DNS 캐시 또는 로컬 DNS 서버의 캐시가 지워지거나 만료되지 않는 경우, DNS 기반 보안 인텔리전스가 도메인 이름에서 예상대로 작동하지 않을 수 있습니다.

DNS 정책 및 관련 DNS 규칙을 사용하여 DNS 기반 보안 인텔리전스를 구성합니다. 이 보안 인텔리전스를 디바이스에 구축하려면 DNS 정책을 액세스 제어 정책에 연결한 다음 매니지드 디바이스에 설정을 구축해야 합니다.

DLP 정책 구성 요소

DNS 정책을 사용하면 차단 목록을 사용하여 도메인 이름을 기준으로 연결을 차단하거나 Do Not Block(차단 금지) 목록을 사용하여 이러한 연결을 차단에서 제외할 수 있습니다. 다음 목록에서는 DNS 정책을 생성한 후에 변경할 수 있는 컨피그레이션에 대해 설명합니다.

이름 및 설명

각 DNS 정책에는 고유한 이름이 있어야 합니다. 설명은 선택 사항입니다.

다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.

규칙

규칙을 사용하면 도메인 이름을 기준으로 네트워크 트래픽을 더 자세히 처리할 수 있습니다. DNS 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 DNS 규칙과 일치하는지 확인합니다.

DNS 정책을 생성하면 시스템은 해당 정책에 DNS 규칙에 대한 기본 글로벌 차단 금지 목록 그리고 DNS 규칙에 대한 기본 글로벌 차단 목록을 입력합니다. 두 규칙 모두 해당 카테고리의 첫 번째 위치에 고정됩니다. 이러한 규칙을 수정할 수는 없지만 비활성화할 수는 있습니다.

다중 도메인 구축에서 시스템은 상위 도메인의 DNS 정책에 하위 항목 DNS 차단 금지 목록 및 하위 항목 DNS 차단 목록 규칙도 추가합니다. 이러한 규칙은 해당 카테고리의 두 번째 위치에 고정됩니다.

참고 Firepower Management Center에 멀티테넌시가 활성화된 경우, 시스템은 상위 및 하위 항목 도메인을 포함한 도메인 계층으로 구성됩니다. 이러한 도메인은 고유하며 DNS 관리에 사용되는 도메인 이름과 구별됩니다.

하위 항목 목록에는 Firepower System 서브도메인 사용자의 차단 또는 차단 금지 목록에 대한 도메인이 포함됩니다. 상위 도메인에서 하위 목록의 내용을 볼 수 없습니다. 하위 도메인 사용자가 차단 또는 차단 금지 목록에 도메인을 추가하지 못하게 하려면 다음을 수행합니다.

- 하위 항목 목록 규칙을 비활성화하고
- 액세스 제어 정책 상속 설정을 사용하여 보안 인텔리전스를 적용합니다.

시스템은 다음 순서로 규칙을 평가합니다.

- DNS 규칙에 대한 글로벌 차단 금지 목록(활성화되어 있을 경우)
- 하위 항목 DNS 차단 금지 목록 규칙(활성화된 경우)

- 차단 금지 목록 규칙
- DNS 규칙에 대한 글로벌 차단 목록(활성화된 경우)
- 하위 항목 DNS 차단 목록 규칙(활성화된 경우)
- 차단 금지 이외 작업 규칙

일반적으로 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 DNS 규칙에 따라 DN 기반 네트워크 트래픽을 처리합니다. 트래픽과 일치하는 DNS 규칙이 없으면 시스템은 연결된 액세스 제어 정책의 규칙을 기준으로 트래픽을 계속 평가합니다. DNS 규칙 조건은 단순할 수도 있고 복잡할 수도 있습니다.

DNS 정책을 위한 라이선스 요구 사항

FTD 라이선스

위협

기본 라이선스

보호

DNS 프로파일 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

DNS 정책 관리

DNS 정책 페이지(**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**)를 사용하여 맞춤형 DNS 정책을 관리합니다. 사용자가 생성하는 맞춤형 정책 외에도 시스템은 기본 차단 목록과 차단 금지 목록을

사용하는 기본 DNS 정책을 제공합니다. 시스템이 제공하는 이러한 맞춤형 정책을 편집하고 사용할 수 있습니다. 다중 도메인 구축에서 이 기본 정책은 기본 전역 DNS 차단 목록, 전역 DNS 차단 금지 목록, 하위 항목 DNS 차단 목록, 하위 항목 DNS 차단 금지 목록을 사용하며, 전역 도메인에서만 편집할 수 있습니다.

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.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**을(를) 선택합니다.

단계 **2** DNS 정책을 관리합니다.

- 비교 - DNS 정책을 비교하려면 **Compare Policies(**정책 비교**)**를 클릭하고 정책 비교에 설명된 대로 진행합니다.
- 복사 - DNS 정책을 복사하려면 **Copy(**복사**)** ( )을 클릭하고 DNS 정책 편집, 5 페이지에 설명된 대로 진행합니다.
- 생성 - 새 DNS 정책을 생성하려면 **Add DNS Policy(DNS** 정책 추가**)**를 클릭하고 기본 DNS 정책 생성, 4 페이지에 설명된 대로 진행합니다.
- 삭제 - DNS 정책을 삭제하려면 **Delete(**삭제**)** ( )을 클릭한 다음 정책 삭제 여부를 확인합니다.
- 편집 - 기존 DNS 정책을 편집하려면 **Edit(**수정**)** ( )을 클릭하고 DNS 정책 편집, 5 페이지에 설명된 대로 진행합니다.

기본 DNS 정책 생성

새 DNS 정책을 만들면 기본 설정이 포함됩니다. 그런 다음 이를 편집하여 동작을 맞춤화해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**을(를) 선택합니다.

단계 **2** **Add DNS Policy(DNS** 정책 추가**)**를 클릭합니다.

단계 **3** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

정책 구성 DNS 정책 편집, 5 페이지의 내용을 참조하십시오.

DNS 정책 편집

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 DNS 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장하려고 하면 저장된 변경 사항의 첫 번째 집합만 유지됩니다.

세션 프라이버시를 보호하기 위해 정책 편집기에서 30분간 아무런 활동이 없으면 경고가 표시됩니다. 60분이 지나면 시스템은 변경 사항을 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**을(를) 선택합니다.

단계 **2** 편집하려는 DNS 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** DNS 정책을 수정합니다.

- Name(이름) 및 Description(설명) - 이름이나 설명을 변경하려면 해당 필드를 클릭하고 새 정보를 입력합니다.
- Rules(규칙) - DNS 규칙을 추가, 분류, 활성화, 비활성화 또는 기타 방식으로 관리하려면 **Rules(**규칙**)**를 클릭하고 DNS 규칙 생성 및 편집, 6 페이지의 설명대로 작업을 진행합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 필요한 경우, Firepower Management Center 관리 가이드의 보안 인텔리전스로 연결 로깅에 설명된 대로 새 정책을 추가로 구성합니다.
- 컨피그레이션 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

DNS 규칙

DNS 규칙은 호스트가 요청한 도메인 이름에 따라 트래픽을 처리합니다. 이 평가는 보안 인텔리전스의 일환으로 트래픽 암호 해독 이후/액세스 제어 평가 전에 수행됩니다.

시스템은 사용자가 지정하는 순서대로 트래픽이 DNS와 일치하는지 확인합니다. 대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 DNS 규칙에 따라 네트워크 트래픽을 처리합니다.

각 DNS 규칙에는 고유한 이름이 지정되며 다음과 같은 기본 구성 요소가 포함됩니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

DNS 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. DNS 규칙은 DNS 피드 또는 목록 조건을 포함해야 하며, 보안 영역, 네트워크 또는 VLAN을 기준으로 트래픽 일치 여부를 확인할 수도 있습니다.

조치

규칙의 작업에 따라 시스템에서 일치하는 트래픽을 처리하는 방법이 결정됩니다.

- 차단 금지 동작이 있는 트래픽은 허용되며 추가 액세스 제어 검사가 수행됩니다.
- 모니터링된 트래픽의 경우 DNS 차단 목록에 대한 나머지 규칙에 따라 추가 평가가 수행됩니다. DNS 차단 목록 규칙과 일치하지 않는 트래픽의 경우 액세스 제어 규칙을 사용하여 검사합니다. 시스템은 트래픽에 대해 보안 인텔리전스 이벤트를 로깅합니다.
- 차단 목록의 트래픽은 추가 검사 없이 삭제됩니다. 또한 Domain Not Found(도메인을 찾을 수 없음) 응답을 반환하거나 DNS 쿼리를 싱크홀 서버로 리디렉션할 수도 있습니다.

관련 항목

보안 인텔리전스 정보

DNS 규칙 생성 및 편집

DNS 정책에서는 차단 목록 및 차단 금지 목록 규칙에 총 32767개의 DNS 목록을 추가할 수 있습니다. 즉, DNS 정책의 목록 수는 32767개를 초과할 수 없습니다.

프로시저

단계 **1** DNS 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add DNS Rule(DNS** 규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 **Edit(**수정**)** ( )을 클릭합니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** 규칙 구성 요소를 구성하거나 기본값을 승인합니다.

- Action(작업) — 규칙 **Action(**작업**)**을 선택합니다(DNS 규칙 작업, 8 페이지 참조).

- Conditions(조건) - 규칙의 조건을 구성합니다(DNS 규칙 조건, 9 페이지 참조).
- Enabled(활성화) — 규칙이 **Enabled(활성화)** 상태인지 여부를 지정합니다.

단계 **4** **Save(저장)**를 클릭합니다.

다음에 수행할 작업

- 컨피그레이션 변경사항을 구축합니다. 구성 변경 사항 구축를 참고하십시오.

DNS 규칙 관리

DNS 정책 편집기의 **Rules(규칙)** 탭에서는 정책 내의 DNS 규칙을 추가, 편집, 이동, 활성화, 비활성화, 삭제하고 기타 방식으로 관리할 수 있습니다.

정책 편집기는 각 규칙에 대해 그 이름, 조건의 요약, 규칙 작업을 표시합니다. 기타 아이콘은 **Warning(경고)** (), **Error(오류)** (), 기타 중요한 **Information(정보)** ()을 나타냅니다. 비활성화된 규칙은 흐리게 표시되며, 규칙 이름 아래에 `(disabled(비활성화))`가 표시됩니다.

DNS 규칙 활성화 및 비활성화

DNS 규칙은 생성하면 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. DNS 정책에서 규칙의 목록을 볼 때 비활성화된 규칙은 흐리게 표시됩니다. 단, 이 규칙은 수정 가능합니다. DNS 규칙 편집기를 사용하여 DNS 규칙을 활성화하거나 비활성화할 수도 있습니다.

프로시저

단계 **1** DNS 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

단계 **2** **Save(저장)**를 클릭합니다.

다음에 수행할 작업

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

DNS 규칙 순서 평가

DNS 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 DNS 규칙과 일치하는지 확인합니다. 대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 DNS 규칙에 따라 네트워크 트래픽을 처리합니다.

- 모니터링 규칙의 경우, 시스템은 트래픽을 로깅한 다음 우선 순위가 낮은 DNS 차단 목록 규칙을 기준으로 트래픽을 계속 평가합니다.
- 모니터링 규칙이 아닌 규칙의 경우, 시스템은 트래픽이 규칙과 일치하는 것으로 확인되고 나면 우선 순위가 낮은 추가 DNS 규칙을 기준으로 트래픽을 계속 평가하지 않습니다.

규칙 순서와 관련하여 다음 사항에 유의하십시오.

- DNS의 글로벌 차단 안 함 목록이 항상 첫 번째 규칙이며 기타 모든 규칙보다 우선적으로 적용됩니다.
- 하위 항목 DNS 차단 안 함 목록 규칙은 리프가 아닌 도메인의 다중 도메인 구축에서만 표시됩니다. 이 규칙은 항상 두 번째이며, 글로벌 차단 안 함 목록을 제외한 다른 모든 규칙보다 우선적으로 적용됩니다.
- 차단 안 함 목록 섹션이 차단 목록 섹션보다 위에 있으며 차단 안 함 목록 규칙이 항상 다른 규칙보다 우선적으로 적용됩니다.
- DNS에 대한 전역 차단 목록은 항상 차단 목록 섹션의 첫 번째 항목이며 다른 모든 모니터링 및 차단 목록 규칙보다 우선합니다.
- 하위 항목 DNS 차단 목록 규칙은 리프가 아닌 도메인의 다중 도메인 구축에서만 표시됩니다. 이는 항상 차단 목록 섹션의 두 번째 항목이며 전역 차단 목록을 제외한 다른 모든 모니터링 및 차단 목록 규칙보다 우선합니다.
- 차단 목록 섹션에는 모니터링 및 차단 목록 규칙이 포함됩니다.
- DNS 규칙을 처음 생성할 때 차단 안 함 작업을 할당하면 해당 규칙이 차단 안 함 섹션의 마지막에 배치되고, 다른 작업을 할당하면 차단 목록 섹션의 마지막에 배치됩니다.

규칙을 끌어 놓으면 규칙 순서를 변경할 수 있습니다.

DNS 규칙 작업

각 DNS 제어 규칙에는 일치하는 트래픽에 대해 다음을 결정하는 작업이 있습니다.

- 처리-차단 또는 차단 금지 목록을 기반으로 시스템이 규칙의 조건과 일치하는 트래픽을 차단, 차단 금지, 차단, 또는 모니터링할지를 제어하는 가장 중요한 규칙 작업
- 로깅-일치하는 트래픽에 관한 세부 사항을 로깅하는 시기와 방법을 결정하는 규칙 작업

구성된 경우, TID는 작업 우선 순위에도 영향을 미칩니다. 자세한 내용은 TID-FMC 작업 우선순위를 참고하십시오.

차단 금지 작업

차단 금지 작업은 트래픽이 검사의 다음 단계(액세스 제어 규칙)로 전달되도록 허용합니다.

시스템은 차단 금지 목록 일치 항목을 로깅하지 않습니다. 이러한 연결의 로깅 여부는 해당 연결의 최종 속성에 따라 달라집니다.

모니터링 작업

Monitor(모니터링**)** 작업은 연결 로깅을 강제하도록 설계됩니다. 따라서 일치하는 트래픽이 즉시 허용되거나 차단되지 않습니다. 대신, 트래픽이 허용할지 아니면 거부할지 여부를 결정하기 위해 추가 규칙에 일치됩니다. 첫 번째로 일치한 비모니터링 DNS 규칙이 시스템이 트래픽을 차단할지를 결정합니다. 추가로 일치하는 규칙이 없으면 트래픽에 대해 액세스 제어 평가가 수행됩니다.

DNS 정책에 의해 모니터링되는 연결의 경우, 시스템은 연결 종료 보안 인텔리전스 및 연결 이벤트를 Firepower Management Center 데이터베이스에 로깅합니다.

차단 작업

이들 작업은 어떤 종류의 추가 검사도 수행하지 않고 트래픽을 차단합니다.

- **Drop(**삭제**)** 작업에서는 패킷을 삭제합니다.
- **Domain Not Found(**도메인을 찾을 수 없음**)** 작업에서는 없는 인터넷 도메인 응답을 DNS 쿼리에 반환하므로 클라이언트가 DNS 요청을 확인할 수 없습니다.
- **Sinkhole(**싱크홀**)** 작업에서는 DNS 쿼리에 대한 응답으로 싱크홀 개체의 IPv4 또는 IPv6 주소를 반환합니다(A 및 AAAA 레코드만 해당). 싱크 홀 서버는 IP 주소에 대한 후속 연결을 로깅하거나 로깅 후 차단할 수 있습니다. **Sinkhole(**싱크홀**)** 작업을 구성하는 경우에는 싱크홀 개체도 구성해야 합니다.

Drop(삭제**)** 또는 **Domain Not Found(**도메인을 찾을 수 없음**)** 작업에 따라 차단된 연결의 경우, 시스템은 연결 시작 보안 인텔리전스 및 연결 이벤트를 로깅합니다. 차단된 트래픽은 추가 검사 없이 즉시 거부 당하기 때문에, 연결을 로깅하는 데 고유한 마무리 단계는 없습니다.

Sinkhole(싱크홀**)** 작업에 따라 차단된 연결의 경우에는 싱크홀 개체 구성에 따라 로깅 여부가 달라집니다. 싱크홀 연결만 로깅하도록 싱크홀 개체를 구성하면 시스템은 후속 연결에 대해 연결 종료 연결 이벤트를 로깅합니다. 싱크홀 연결을 로깅 후에 차단하도록 싱크홀 개체를 구성하면 시스템은 후속 연결에 대해 연결 시작 연결 이벤트를 로깅한 다음 해당 연결을 차단합니다.

DNS 규칙 조건

SSL 규칙의 조건은 규칙에서 처리하는 트래픽의 유형을 식별합니다. 조건은 단순할 수도 있고 복잡할 수도 있습니다. DNS 규칙 내에서 DNS 피드 또는 목록 조건을 정의해야 합니다. 필요한 경우, 보안 영역, 네트워크 또는 VLAN별로 트래픽을 제어할 수도 있습니다.

DNS 규칙에 조건을 추가할 때 적용되는 사항은 다음과 같습니다.

- 규칙에 대해 특정 조건을 구성하지 않으면 시스템은 해당 기준에 따라 트래픽을 매칭하지 않습니다.
- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용할 수 있으려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어 DNS 피드 또는 목록 조건과 네트워크 조건은 있지만 VLAN 태그 조건은 없는 규칙은 세션의 VLAN 태깅에 관계없이 도메인 이름과 소스 또는 대상을 기준으로 트래픽을 평가합니다.

- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어 규칙 하나를 사용하여 최대 50개의 DNS 목록과 피드를 기준으로 트래픽을 차단할 수 있습니다.

관련 항목

보안 영역 규칙 조건
네트워크 규칙 조건
VLAN 태그 규칙 조건
DNS 규칙 조건, 12 페이지

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.

DNS 규칙 조건

DNS 규칙의 DNS 조건을 사용하면 DNS 목록, 피드 또는 카테고리에 클라이언트가 요청한 도메인 이름이 포함되어 있는 경우 트래픽을 제어할 수 있습니다. DNS 규칙에서 DNS 조건을 정의해야 합니다.

DNS 조건에 추가하는 항목(글로벌 또는 맞춤형 차단 또는 차단 안 함 목록)에 관계없이 시스템은 구성된 규칙 작업을 트래픽에 적용합니다. 예를 들어 규칙에 글로벌 차단 안 함 목록을 추가하고 **Drop(**삭제**)** 작업을 구성하면 시스템은 다음 검사 단계로 전달하도록 허용되어야 하는 모든 트래픽을 차단합니다.

DNS 규칙을 생성하는 방법

다음 주제에서는 DNS 규칙을 생성하는 방법을 설명합니다.

관련 항목

DNS 및 보안 영역을 기준으로 트래픽 제어, 12 페이지
DNS 및 네트워크를 기준으로 트래픽 제어, 13 페이지
DNS 및 VLAN을 기준으로 트래픽 제어, 13 페이지
DNS 목록 또는 피드를 기준으로 트래픽 제어, 14 페이지

DNS 및 보안 영역을 기준으로 트래픽 제어

DNS 규칙의 영역 조건을 사용하면 해당 소스 보안 영역에 따라 트래픽을 제어할 수 있습니다. 보안 영역이란 하나 이상의 인터페이스를 그룹화한 것이며, 이 인터페이스는 여러 디바이스에 걸쳐 위치할 수도 있습니다.

프로시저

단계 **1** DNS 규칙 편집기에서 **Zones(**영역**)**을 클릭합니다.

단계 **2** **Available Zones(**사용 가능한 영역**)**에서 추가하려는 영역을 찾아 선택합니다. 영역을 찾아 추가하려면, **Available Zones(**사용 가능한 영역**)** 목록 위에 있는 **Search by name(**이름으로 검색**)** 프롬프트를 클릭한 후, 영역 이름을 입력합니다. 일치하는 영역을 입력하여 표시하면 목록이 업데이트됩니다.

단계 **3** 영역을 하나 클릭하여 선택하거나 마우스 오른쪽 버튼을 클릭하고 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Source(**소스에 추가**)**를 클릭하거나 마우스로 끌어서 놓습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

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

DNS 및 네트워크를 기준으로 트래픽 제어

DNS 규칙의 네트워크 조건을 통해 소스 IP 주소로 트래픽을 제어할 수 있습니다. 제어하려는 트래픽에 대해 소스 IP 주소를 명시적으로 지정할 수 있습니다.

프로시저

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

단계 **2** 다음과 같이, **Available Networks(**사용 가능한 네트워크**)**로부터 추가하려는 네트워크를 찾아 선택합니다.

- 네트워크 개체를 즉시 추가하려면(나중에 이 개체를 조건에 추가할 수 있음) **Available Networks(**사용 가능한 네트워크**)** 목록 위에 있는 **Add(**추가**)** (+)을 클릭하고 네트워크 개체 생성의 설명대로 작업을 진행합니다.
- 추가할 네트워크 개체를 검색하려면 **Available Networks(**사용 가능한 네트워크**)** 목록 위에 있는 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 후 개체 이름이나 개체 구성 요소 중 하나의 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.

단계 **3** **Add to Source(**소스에 추가**)**를 클릭하거나 마우스로 끌어서 놓습니다.

단계 **4** 수동으로 지정하려는 소스 IP 주소 또는 주소 블록을 추가합니다. **Source Networks(**소스 네트워크**)** 목록 아래에 있는 **Enter an IP address(IP** 주소 입력**)** 프롬프트를 클릭한 후 IP 주소 또는 주소 블록을 입력하고 **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. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

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

DNS 및 VLAN을 기준으로 트래픽 제어

DNS 규칙의 VLAN 조건을 사용하면 VLAN 태그가 지정된 트래픽을 제어할 수 있습니다. 시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다.

VLAN 기반 DNS 규칙 조건을 작성할 때 VLAN 태그를 수동으로 지정할 수 있습니다. 또는 VLAN 태그 객체를 사용하여 VLAN 조건을 구성할 수 있습니다. 이 객체는 재사용 가능하며 이름을 하나 이상의 VLAN 태그와 연결합니다.

프로시저

단계 **1** DNS 규칙 편집기에서 **VLAN Tags(VLAN** 태그**)**를 선택합니다.

단계 **2** **Available VLAN Tags(**사용 가능한 **VLAN** 태그**)**에서 추가할 VLAN을 다음과 같이 찾아 선택합니다.

- VLAN 태그 개체를 즉시 추가한 다음 조건에 추가하려면 Available VLAN Tags(사용 가능한 VLAN 태그) 목록 위의 **Add(**추가**)** (+)을 클릭하고 VLAN 태그 개체 생성에 설명된 대로 진행합니다.
- 추가할 VLAN 태그 개체 및 그룹을 검색하려면 **Available VLAN Tags(**사용 가능한 **VLAN** 태그**)** 목록 위에서 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 후 개체 이름 또는 개체의 VLAN 태그 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.

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

단계 **4** 수동으로 지정할 VLAN 태그를 추가합니다. **Selected VLAN Tags** 목록 아래의 **Enter a VLAN Tag** 프롬프트를 클릭합니다. 그런 다음 VLAN 태그 또는 범위를 입력하고 **Add**를 클릭합니다. 1~4094 범위의 VLAN 태그를 지정할 수 있으며, 하이픈을 사용하여 VLAN 태그의 범위를 지정합니다.

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.

단계 **5** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

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

DNS 목록 또는 피드를 기준으로 트래픽 제어

프로시저

단계 **1** DNS 규칙 편집기에서 **DNS**를 클릭합니다.

단계 **2** 다음과 같이 **DNS Lists and Feeds(DNS** 목록 및 피드**)**에서 추가할 DNS 목록과 피드를 찾아서 선택합니다.

- DNS 목록이나 피드를 즉시 추가한 다음 조건에 추가하려면 **DNS Lists and Feeds(DNS** 목록 및 피드**)** 목록 위에 있는 **Add(**추가**)** ( )을 클릭하고 보안 인텔리전스 피드 생성의 설명대로 작업을 진행합니다.
- 추가할 DNS 목록, 피드 또는 카테고리를 검색하려면 **DNS Lists and Feeds(DNS** 목록 및 피드**)** 목록 위에 있는 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 후 개체 이름이나 개체 구성 요소 중 하나의 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.
- 새 범주에 대한 설명은 보안 인텔리전스 카테고리의 내용을 참조하십시오.

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

단계 **4** 규칙을 저장하거나 계속 수정합니다.

다음에 수행할 작업

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

DNS 정책 구축

DNS 정책 구성 업데이트를 완료한 후 해당 업데이트를 액세스 제어 구성의 일부로 구축해야 합니다.

- 보안 인텔리전스 설정의 설명대로 DNS 정책을 액세스 제어 정책과 연결해야 합니다.
- Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.