Umbrella Secure Internet Gateway에서 규칙 기반 정책 사용

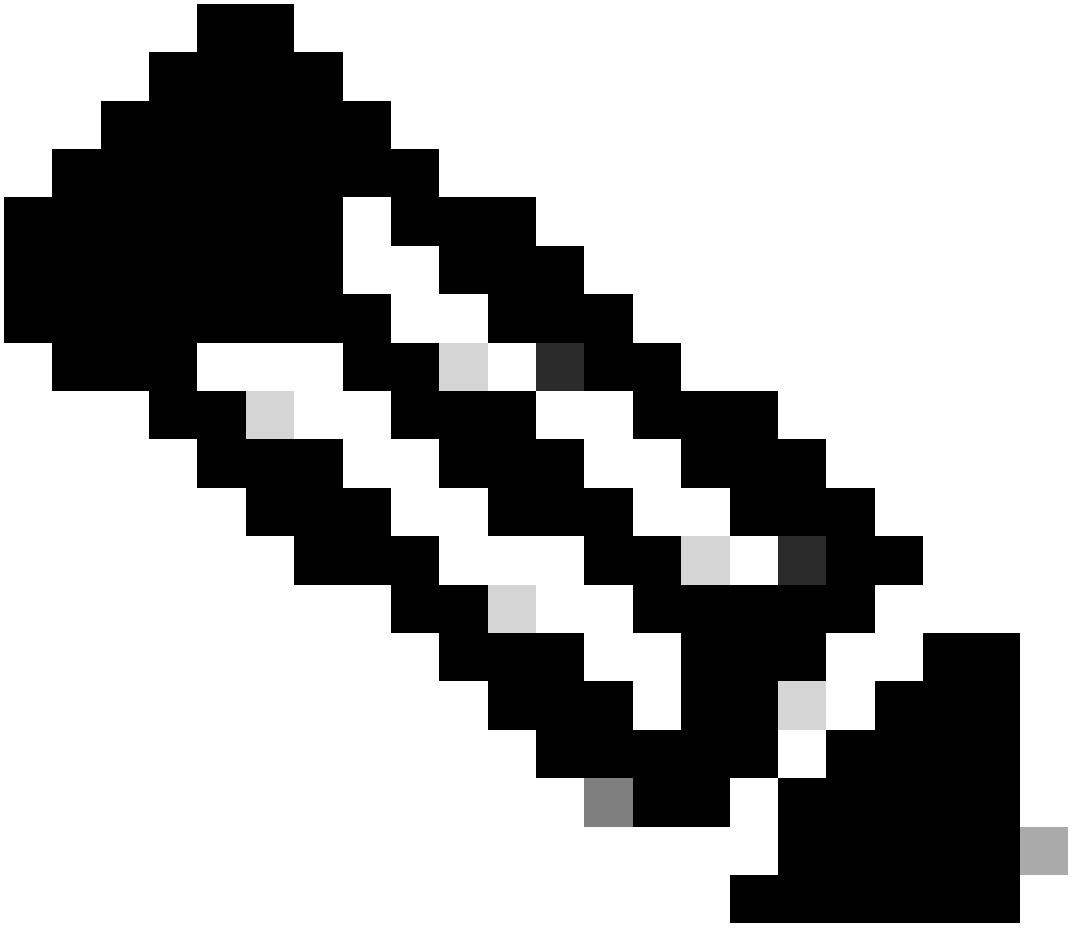
목차

소개

이 문서에서는 Umbrella SIG(Secure Internet Gateway)의 규칙 기반 정책 기능에 대해 설명하고 일반적인 질문에 답변합니다.

규칙 기반 정책 전환 개요

2021년 3월 31일, Umbrella SIG 고객에게 규칙 기반 정책이 GA되었습니다. Umbrella SIG 고객은 몇 주에 걸쳐 레거시 웹 정책에서 규칙 기반 정책으로 점진적으로 전환됩니다. 고객은 Umbrella 대시보드를 통해 전환 날짜 및 기간에 대한 알림을 받습니다. 이러한 변경은 Umbrella DNS 고객 또는 DNS 정책 설정에 영향을 주지 않습니다.



참고: 이 FAQ는 기존 웹 정책에서 규칙 집합으로의 전환에 대한 신규 및 숙련된 Umbrella 사용자의 빠른 질문에 답변하기 위한 것입니다. 자세한 내용은 업데이트된 Umbrella 관리 가이드를 참조하십시오.

자주 묻는 질문(FAQ)

웹 정책이란?

웹 정책은 Umbrella 조직에 있는 모든 규칙 세트의 모음입니다.

규칙 집합이란?

규칙 세트는 규칙 세트 내의 해당 규칙에 적용되는 규칙 및 설정 집합에 대한 논리적 컨테이너입니다.

규칙 세트를 사용해야 하는 이유

규칙 세트는 조직의 나머지 영역과 다른 관리가 필요한 특정 지역, 사무실 그룹 또는 사용자를 나타낼 수 있습니다.

규칙 집합에서 구성할 수 있는 설정은 무엇입니까?

규칙 세트에서 제공된 설정을 구성합니다. 이러한 설정은 해당 규칙 세트 내의 규칙에만 적용됩니다.

- 규칙 세트 이름
- 규칙 세트 ID
- 차단 페이지
- 테넌트 제어
- 파일 분석
- 파일 형식 제어
- HTTPS 검사
- PAC 파일
- 규칙 세트 로깅
- SAML
- 보안 설정

자세한 설명은 다음을 참조하십시오. 규칙 세트를 구성합니다.

규칙이란?

규칙은 ID와 대상이 모두 일치할 때 수행할 작업을 정의하는 명령문입니다.

규칙을 사용하는 이유

규칙은 세분화된 또는 광범위한 액세스 제어를 허용합니다. 예를 들어, 우선 순위가 낮은 규칙은 모든 사용자에 대해 광범위한 웹 사이트를 차단할 수 있는 반면, 우선 순위가 높은 규칙은 동일한 규칙 세트 내에서 모두 대상 그룹의 특정 사이트에 대한 액세스를 허용할 수 있습니다.

어떤 Id가 지원됩니까?

규칙 세트 및 규칙 모두 다음 ID를 지원합니다.

- AD 사용자
- AD 그룹
- 로밍 컴퓨터(AnyConnect 끝점)
- 내부 네트워크
- 터널
- 네트워크

어떤 대상이 지원됩니까?

규칙은 다음 대상을 지원합니다.

- 콘텐츠 범주
- 응용 프로그램 설정
- 대상 목록

어떤 조치가 지원됩니까?

규칙은 다음 작업을 지원합니다.

- 허용
- 차단
- 경고
- 격리

규칙에서 구성할 수 있는 설정은 무엇입니까?

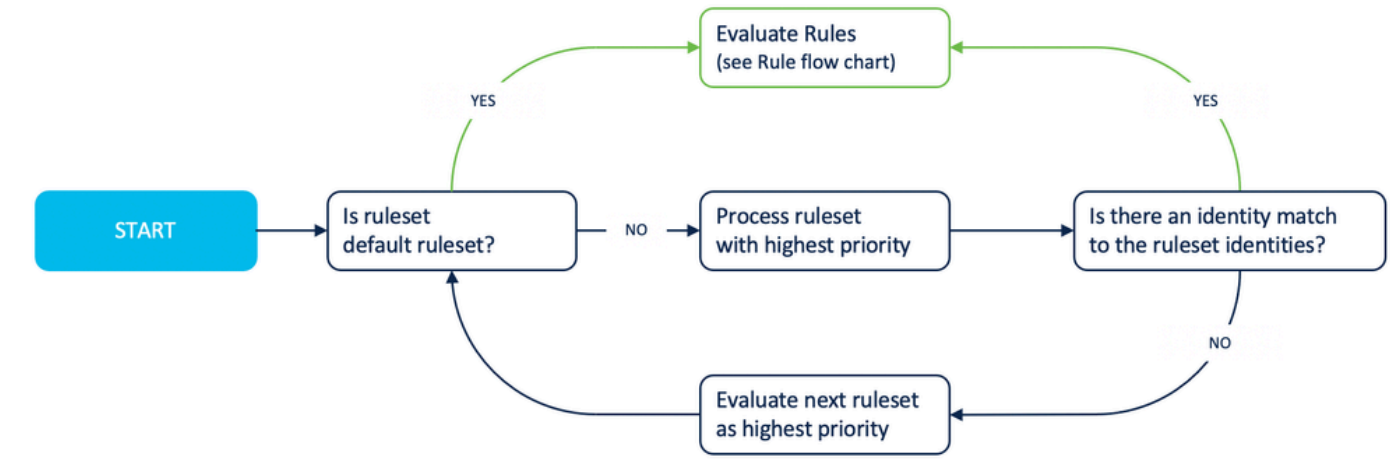
다음과 같이 규칙을 구성할 수 있습니다.

- 규칙 이름
- 작업
- 신원
- 대상
- 시간/일 일정

자세한 내용은 규칙 세트에 규칙 추가를 참조하십시오.

규칙 세트는 어떻게 평가됩니까?

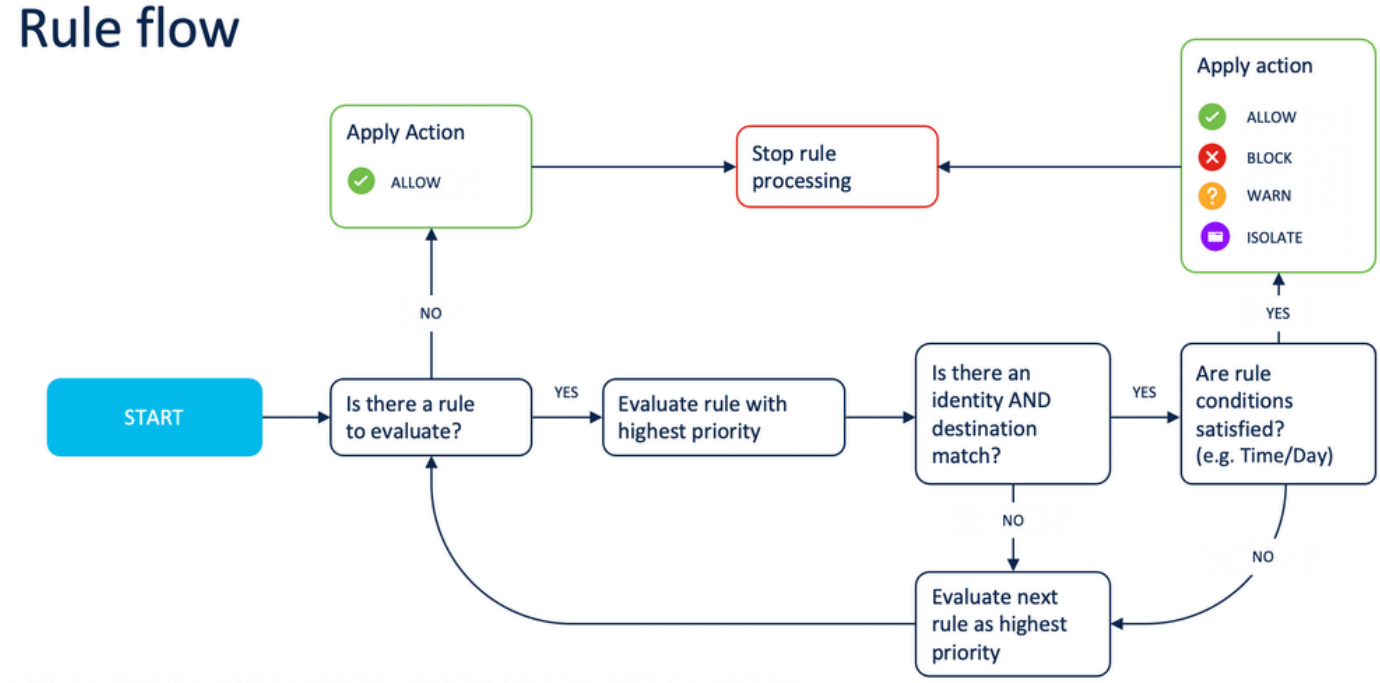
규칙 세트는 사용 가능한 ID와 비교하여 하향식 계층으로 평가됩니다. 우선 순위가 가장 높은 규칙 세트가 먼저 평가됩니다. 일치하는 항목이 없으면 다음으로 우선순위가 높은 규칙 세트가 평가되는 등의 작업을 수행합니다. 규칙 세트에서 일치하는 항목이 없으면 기본 규칙 세트가 적용됩니다.



Screen_Shot_2021-04-07_at_2.37.22_PM.png

규칙은 어떻게 평가됩니까?

선택한 규칙 세트 내의 규칙은 사용 가능한 ID 및 대상에 대해 하향식으로 평가됩니다. 규칙은 ID와 대상이 모두 일치하는 경우에만 적용됩니다. 그런 다음 규칙에 대해 구성된 작업(allow, block, warn 또는 isolate)이 적용됩니다.



Screen_Shot_2021-05-10_at_10.33.03_AM.png

규칙이 규칙 세트와 일치하는 동일한 Id에 적용됩니까?

규칙은 규칙 세트와 동일한 ID와 일치할 수 있지만 항상 그렇지는 않습니다. Umbrella는 웹 요청을 수신하면 존재하는 모든 ID를 수집합니다. 선택한 규칙 세트 내의 규칙은 동일한 ID 풀에 대해 평가되며 대상과도 일치해야 합니다. 규칙에서 사용하는 실제 ID는 규칙 세트와 일치하는 ID와 다를 수 있습니다.

예:

- JDoe는 네트워크 B에서 작동합니다.
- 조직에는 다음과 같은 규칙 세트가 있습니다.
    - 규칙 세트 1: 네트워크 A
    - 규칙 세트 2: 네트워크 B
    - 규칙 세트 3: 네트워크 C

규칙 세트 2만 JDoe에 적용됩니다. 규칙 세트 2 내에서:

- 규칙 1: ID ASmith, 대상 도메인 B, 작업 허용
- 규칙 2: Identity Marketing, 대상 SomeSocialApp, 작업 허용
- 규칙 3: ID 네트워크 B, 대상 콘텐츠 범주(도메인 B, SomeSocialApp), 작업 블록

결과:

- JDoe는 도메인 B에서 차단됩니다(규칙 3).
- JDoe는 Marketing의 회원으로서 SomeSocialApp에 대한 액세스가 허용됩니다(규칙 2).

규칙 평가 순서가 결과를 결정합니다. 더 구체적인 ID(사용자, 그룹)가 덜 구체적인 ID(네트워크)보다 먼저 배치됩니다. 첫 번째 일치가 승리합니다.

어떤 규칙이 거래에 사용되었는지 어떻게 알 수 있습니까?

활동 검색 보고서는 트랜잭션에 사용된 규칙 세트와 규칙을 모두 캡처합니다. 이 정보는 URL 요청에 대한 전체 세부사항에서 찾을 수 있습니다. 이 필드는 현재 "Policy/Rule(정책/규칙)" 레이블이 지정되었지만 고객이 레거시 웹 정책에서 규칙 세트로 전환하면 "Ruleset/Rule(규칙 세트/규칙)"로 변경됩니다.

규칙 세트에 대한 온라인 문서는 어디에서 찾을 수 있습니까?

Umbrella Admin Guide Manage Web Policies(Umbrella 관리 설명서 웹 정책 관리)를 참조하십시오
.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.