

웹 정책 관리를 위한 규칙 기반 정책의 규칙 작업 구성

목차

소개

이 문서에서는 웹 정책 관리를 위해 규칙 기반 정책에서 규칙 작업을 구성하는 방법에 대해 설명합니다.

개요

규칙 기반 정책은 ID에 따라 일치하는 규칙 세트를 사용합니다. 각 규칙 세트에는 규칙이 포함되며 각 규칙은 ID, 대상 및 일정을 기반으로 일치합니다. 시스템은 하향식 우선 순위에 따라 규칙 세트와 규칙을 모두 적용합니다. ID가 첫 번째 적용 가능한 규칙 세트에 매칭된 다음 ID, 대상 및 일정과 매칭하는 첫 번째 규칙이 적용됩니다.

관리자는 규칙 기반 정책의 새로운 기능을 사용하여 특정 대상 및 애플리케이션의 규칙 ID에 작업을 허용, 경고, 차단 또는 격리할 수 있습니다.

규칙 세트 및 규칙을 구성하는 방법에 대한 지침은 [웹 정책 관리 설명서](#)를 참조하십시오.

작업: 허용, 허용(보안), 경고, 차단 및 격리

규칙 세트의 개별 규칙에 다음 작업 중 하나를 할당할 수 있습니다.

허용(보안)	보안 문제가 탐지되지 않는 한 대상 또는 애플리케이션에 대한 액세스를 허용합니다. 파일 검사 및 보안 카테고리가 계속 적용됩니다. 보안 재정의의 선택하지 않는 한 "허용"에 대한 기본 작업입니다.
허용	보안 보호 없이 대상 또는 애플리케이션에 액세스할 수 있습니다. 전체 콘텐츠 범주에 대해 보안 설정을 재정의할 수 없습니다.
경고	액세스를 차단하는 대신 경고 페이지와 계속할 수 있는 옵션을 사용하여 규칙 ID를 표시합니다.
차단	대상에 대한 액세스를 거부합니다. 규칙 ID는 차단 페이지를 재정의하거나 계속 진행할 수 없습니다.

격리	클라우드 기반 브라우저는 대상 엔드포인트에서 ID를 차단하는 대신 해당 대상에 대한 탐색 세션을 호스팅합니다.
----	---

규칙 작업 설정

규칙을 생성하거나 수정할 때 규칙 작업을 선택합니다.

1. Web Policy(웹 정책) > [적절한 규칙 세트 선택]으로 이동합니다.
2. 규칙 추가(Add Rule)또는 규칙 편집(Edit Rule)을 클릭합니다.

The screenshot shows the Cisco Umbrella 'Web Policy' management page. On the left, the 'Web Policy' menu item is highlighted. The main content area displays a table of rulesets. A red box highlights the 'ADD RULE' button. A red arrow points to the 'ADD RULE' button with the text 'Add a rule'. Another red arrow points to the 'EDIT RULE' button with the text 'Click "...\" to expand rule setting'. A third red arrow points to the 'EDIT RULE' button with the text 'Edit a rule'.

3. 드롭다운 메뉴에서 대상에 대해 Allow,Warn,Block 또는 Isolatefor를 선택합니다.

Ruleset Rules

The screenshot shows the 'Ruleset Rules' configuration page. The 'ADD RULE' button is highlighted. Below it, a table shows the configuration for 'Rule 1'. A dropdown menu is open, showing options: 'Allow - Security Enforced', 'Warn', 'Block', and 'Isolate'. The 'Allow' option is selected.

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration
	Rule 1	Block	No Selections Add Identity	No Selections Add Destination	Any Day, Any Time Change Schedule No additional configuration applied CANCEL
1	Content Warn Sites	Allow - Security Enforced Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.			Any Day, Any Time No additional configuration applied ...
2	Allowed Sites	Warn Warns selected ruleset identities before allowing access to destinations.			Any Day, Any Time No additional configuration applied ...
3	Security Block	Block Blocks selected ruleset identities from accessing destinations.			Any Day, Any Time No additional configuration applied ...
4	Security Block - Apps	Isolate Isolates selected ruleset identities' web requests in a virtual cloud-based browser.			Any Day, Any Time No additional configuration applied ...

- "allow"의 기본값은 보안을 적용하고 위협이 탐지될 경우 대상을 차단합니다.
- 보안 보호 없이 액세스를 허용하려면 "보안 무시" 옵션을 선택합니다.

1	Marketing Access to So...	Allow ▼ Override Security	1 AD Group... Edit Identity	2 Applications ... Edit Destination	Any Day, Any Time Change Schedule	CANCEL SAVE 
2	Block Games/Social	Block	All AD Groups All Networks	2 Categories ...	Mon-Fri 09:00-17:00	...

▲ Ruleset Settings

자세한 내용은 [Umbrella Learning Hub](#)에서 규칙 기반 정책에 대한 비디오를 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.