Change from Web Policies to Rule-Based Policies in Umbrella

Contents

Introduction

This document describes the change from web policies to rule-based policies in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella Secure Internet Gateway (SIG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Starting March 31, 2021, a new feature called "Rule-Based Policy" was made Generally Available to Umbrella Secure Internet Gateway (SIG) customers. Web policies were transitioned for their current policy model to a rule model. The old web policies used a static order of operations for policy components which represent one or more destinations as the components include Allow/Block Destination Lists, Application Settings, and Content Categories. The static order of operations was as follows:

1. Allow Destination Lists

2. Allow Application Settings

3. Security Category Blocks

4. Block Destination Lists

5. Block Application Settings

6. Content Category Blocks

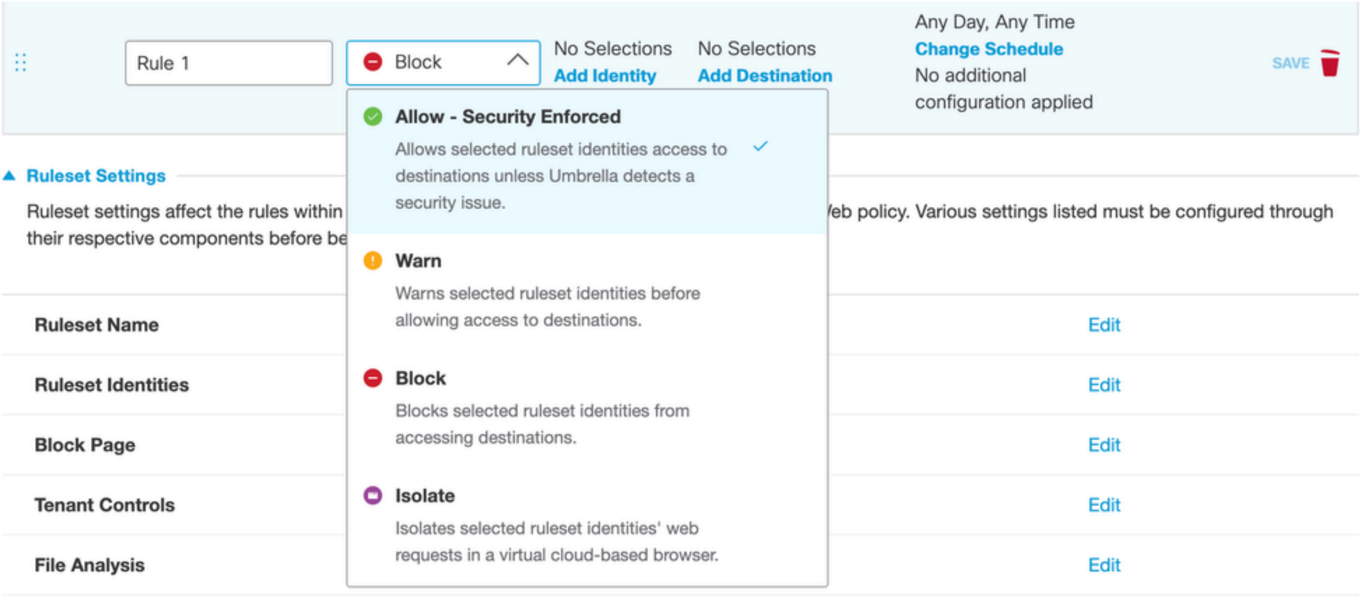
Another restriction of the policy model was that all identities associated with the policy would receive policy. So if a single user or group of identities need a change in their web policy, a new web policy must be created for them.

However, the new rule model places full control in the hands of the administrator. Some rules were created that affect a large group of identities while other rules apply to a single identity or smaller groups of identities with no need to move these identities to a separate policy. Also, the order of operations is easily controlled by the administrator by simply reordering rules.

Comparing Rules to Old Policy Model

New rules allow end users to perform these actions while the old model cannot:

- Override security after an "Allow" action is performed
- Time of Day and Day of Week Schedules for rule application
- Perform a "Warn" action for content categories
- Create a virtual browser that "Isolates" the hosts requests to destinations by the rule's set identities



Allow - Security Enforced ✓
Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.

Warn
Warns selected ruleset identities before allowing access to destinations.

Block
Blocks selected ruleset identities from accessing destinations.

Isolate
Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

Ruleset settings affect the rules within /eb policy. Various settings listed must be configured through their respective components before be

Screen_Shot_2021-05-05_at_3.51.38_PM.png

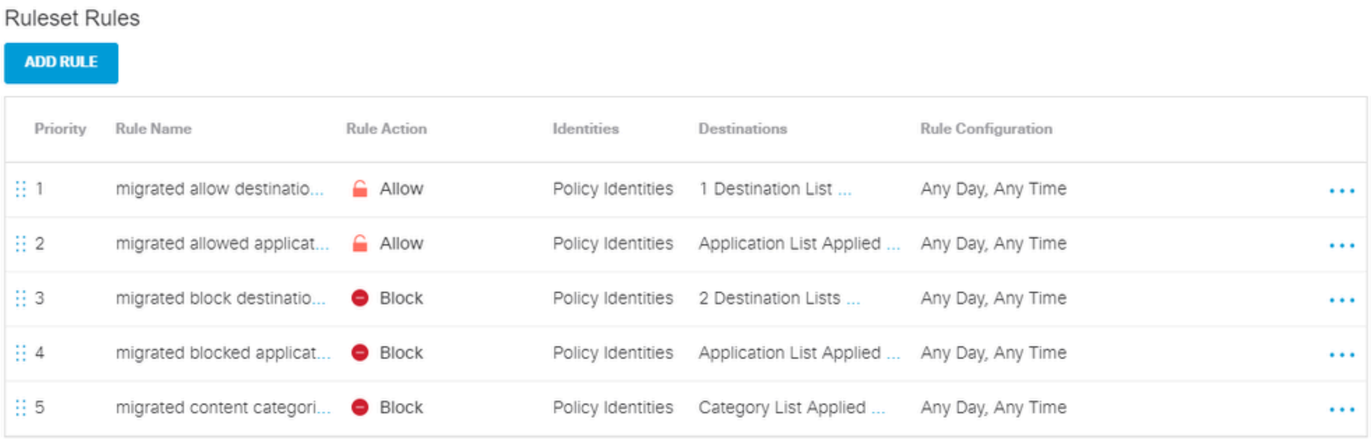
For more information, please read the Umbrella set up documentation: Manage the Web Policy

Transition Actions

A new rule language had to be created in Umbrella to facilitate the processing of rules, and with that a new database was created to store these rules. The transition had two steps:

1. Existing policy components were copied from the old database used by web policies to the new database

used by rules. These components were stripped of any action (like allow or block) as rules can carry the action. Thus, policy components became action agnostic. However, the copied components inherited an “allow” or “block” label to their name to designate what their intention was in the old system for context. Application settings were a special case because they were unique in that they carried both allow and block actions. Any application settings component that carried both actions were be split into two: one for the allowed apps and one for the blocked apps. Up to 5 rules were created for each transitioned web policy. If a web policy did not have all types of policy components configured for it, then only the components that were configured for that web policy that were transitioned resulting in fewer auto-generated rules. This screenshot is an example of a web policy that was transitioned with all 5 rules auto-generated:



Ruleset Rules

Priority	Rule Name	Rule Action	Identities	Destinations	Rule Configuration	
1	migrated allow destinatio...	🔓 Allow	Policy Identities	1 Destination List ...	Any Day, Any Time	•••
2	migrated allowed applicat...	🔓 Allow	Policy Identities	Application List Applied ...	Any Day, Any Time	•••
3	migrated block destinatio...	⛔ Block	Policy Identities	2 Destination Lists ...	Any Day, Any Time	•••
4	migrated blocked applicat...	⛔ Block	Policy Identities	Application List Applied ...	Any Day, Any Time	•••
5	migrated content categori...	⛔ Block	Policy Identities	Category List Applied ...	Any Day, Any Time	•••

2. Once the back end was fully transitioned the new UI was enabled. Note that until the new UI is enabled, anyone logging into the dashboard still saw and was able to interact with the old UI.

- Any changes made to web policies at this incomplete stage were saved when the new UI was enabled.

Transition Timing

You were provided a date and timeframe in which the transition occurred and was relayed by your Customer Success representative and/or Umbrella's messaging system in your dashboard. An auto-generated rule took the place and priority order of each configured policy component for all previous web policies. Once the new UI was enabled the cutover was seamless and, since the auto-generated rules reflected the same action and priority of the legacy web policies, there was no change in behavior transitioning from web policies to rulesets. There was no down time for Web Policy enforcements during this transition.

Changes after March 31, 2021

During the transition, any changes made to your web policies were captured in the new rulesets. This is due to copying existing policy components from the old database to the new database. Once the copy is complete there was a delay in enabling the new UI. Until the new UI was enabled, web policies were active, and any changes to those web policies were written to the old database and not converted to rules.

Technical Support

If you are working with a Customer Success Manager, Technical Account Manager, or Service Delivery Manager, then they can answer questions.Report technical issues to Cisco Umbrella Support.