Use Rule-Based Policies in Umbrella Secure Internet Gateway

Contents

Introduction

This document describes the Rule-Based Policy feature in Umbrella Secure Internet Gateway (SIG) and answers common questions.

Overview of Rule-Based Policy Transition

On March 31, 2021, Rule-Based Policy became Generally Available to Umbrella SIG customers. Umbrella SIG customers are gradually transitioned to Rule-Based Policy from legacy web policies over several weeks. Customers receive notification of the transition date and window through the Umbrella dashboard. This change does not impact Umbrella DNS customers or DNS policy settings.

Note: This FAQ is meant to address quick questions from both new and experienced Umbrella users about the shift from legacy web policies to rulesets. For more in-depth documentation please see the updated Umbrella Admin Guide.

Frequently Asked Questions

What Is a Web Policy?

A web policy is the collection of all rulesets in an Umbrella organization.

What Is a Ruleset?

A ruleset is a logical container for a set of rules and settings that apply to those rules within the ruleset.

Why Use Rulesets?

A ruleset can represent a specific geography, group of offices, or users that require management distinct from the rest of the organization.

What Settings Can Be Configured in a Ruleset?

Configure the provided settings in rulesets. These settings apply only to the rules within that ruleset:

- Ruleset Name
- Ruleset Identities
- Block Page
- Tenant Controls
- File Analysis
- File Type Control
- HTTPS Inspection
- PAC File
- Ruleset Logging
- SAML
- Security Settings

For detailed explanations, see: Configure a Ruleset.

What Are Rules?

A rule is a statement that defines what action to take when an identity and destination both match.

Why Use Rules?

Rules allow granular or broad access control. For example, a low-priority rule can block a wide range of websites for all users, while a higher-priority rule can allow access to specific sites for a targeted group, all within the same ruleset.

What Identities Are Supported?

Both rulesets and rules support these identities:

- AD user
- AD group
- Roaming computer (AnyConnect endpoint)
- Internal network
- Tunnel
- Network

What Destinations Are Supported?

Rules support these destinations:

- Content categories
- Application settings
- Destination lists

What Actions Are Supported?

Rules support these actions:

- Allow
- Block

- Warn
- Isolate

What Settings Can Be Configured in a Rule?

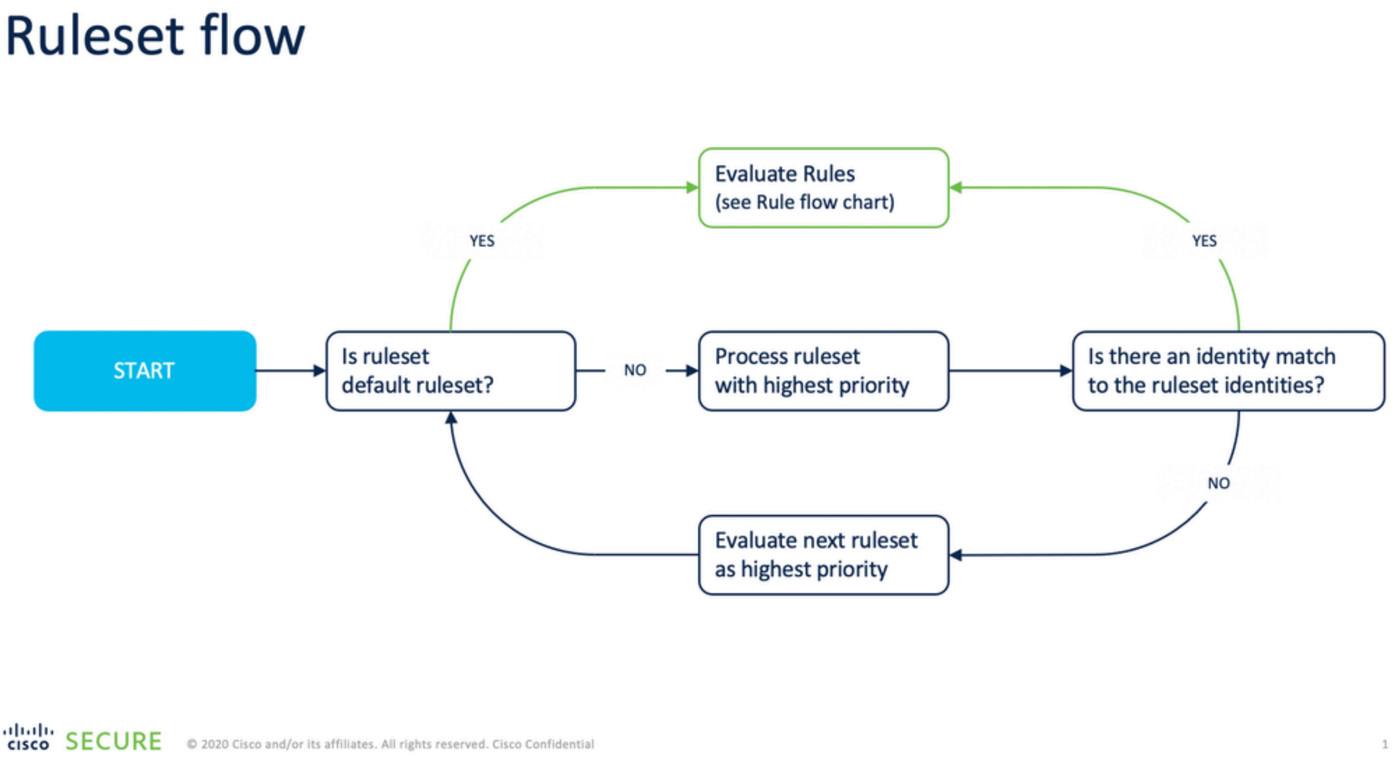
Rules can be configured with:

- Rule Name
- Action
- Identity
- Destination
- Time/Day Schedule

For more details, see Add Rules to a Ruleset.

How Are Rulesets Evaluated?

Rulesets are evaluated in a top-down hierarchy against available identities. The ruleset with the highest priority is evaluated first. If no match occurs, the next highest-priority ruleset is evaluated, and so on. If no match occurs in any ruleset, the default ruleset applies.



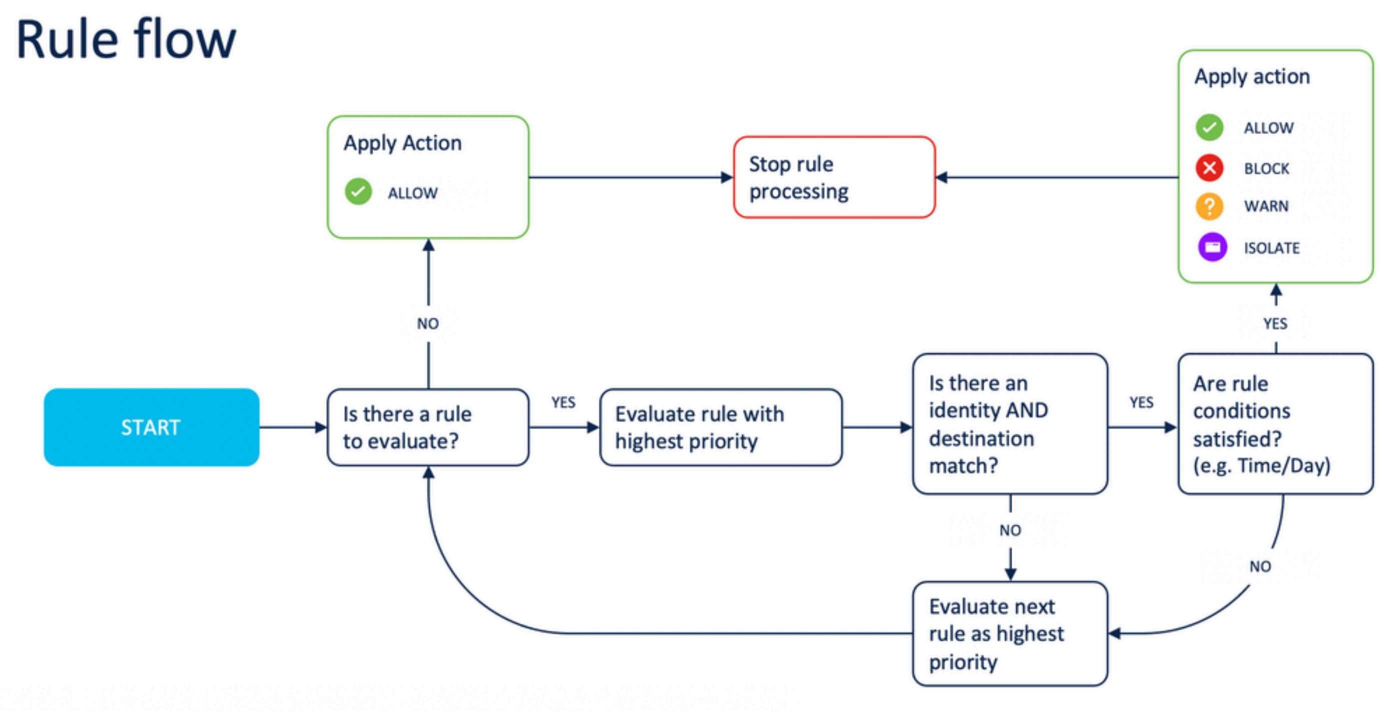
Ruleset flow

START
Is ruleset default ruleset?
NO
Process ruleset with highest priority
Is there an identity match to the ruleset identities?
YES
Evaluate Rules (see Rule flow chart)
YES
NO
Evaluate next ruleset as highest priority
cisco SECURE
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
1

Screen_Shot_2021-04-07_at_2.37.22_PM.png

How Are Rules Evaluated?

Rules within a selected ruleset are evaluated top-down against available identities and destinations. A rule applies only when both an identity and a destination match. The configured action for the rule (allow, block, warn, or isolate) is then applied.


Rule flow
START
Is there a rule to evaluate?
NO
Apply Action
ALLOW
YES
Evaluate rule with highest priority
Is there an identity AND destination match?
NO
YES
Are rule conditions satisfied? (e.g. Time/Day)
YES
Apply action
ALLOW
BLOCK
WARN
ISOLATE
Stop rule processing
NO
Evaluate next rule as highest priority

Screen_Shot_2021-05-10_at_10.33.03_AM.png

Does a Rule Apply to the Same Identity That Matched the Ruleset?

A rule can match the same identity as the ruleset, but this is not always the case. When Umbrella receives a web request, it collects all identities present. Rules within the selected ruleset are then evaluated against the same pool of identities and must also match a destination. The actual identity used by a rule can differ from the identity that matched the ruleset.

Example:

- JDoe works from Network B.
- The organization has these rulesets:
  - Ruleset 1: Network A
  - Ruleset 2: Network B
  - Ruleset 3: Network C

Only Ruleset 2 applies to JDoe. Within Ruleset 2:

- Rule 1: Identity ASmith, Destination Domain B, Action Allow
- Rule 2: Identity Marketing, Destination SomeSocialApp, Action Allow
- Rule 3: Identity Network B, Destination Content Categories (Domain B, SomeSocialApp), Action Block

Outcomes:

- JDoe is blocked from Domain B (Rule 3).
- JDoe, as a member of Marketing, is allowed access to SomeSocialApp (Rule 2).

Rule evaluation order determines the outcome. More specific identities (user, group) is placed before less specific ones (network). First match wins.

How Do I Know Which Rule Was Used in a Transaction?

The Activity Search report captures both the ruleset and rule used in a transaction. This information is found under Full Details for URL requests. The field is currently labeled "Policy/Rule" but changes to "Ruleset/Rule" as customers transition from legacy web policies to rulesets.

Where Can I Find Online Documentation for Rulesets?

Refer to the Umbrella Admin Guide Manage Web Policies.