Troubleshoot Network and Tunnel Identities for CSC Users

Contents

Introduction

This document describes how to troubleshoot Network and Tunnel identities for Cisco Secure Client (CSC) users.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella Secure Web Gateway (SWG).

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

Network and Tunnel Identities for Cisco Secure Client Users is now Generally Available to customers. Umbrella can now apply network/tunnel-based rulesets/rules to CSC SWG installed computers when they are connected to a company network. This feature was enabled for all customers on January 27, 2022.

Reviewing Your Deployment

This enhancement resulted in a change in the applied policy for a customer in this scenario:

- Using CSC SWG module
- Have Registered Networks or Network Tunnels in Umbrella
- Have created Web Rulesets for Tunnels / Networks (non-default)

- Have Web Rulesets/Rules for Tunnels at a**higher priority** than rules for CSC, AD Users, or AD Groups

Web Policy Settings

Your web policy was not applied as expected if:

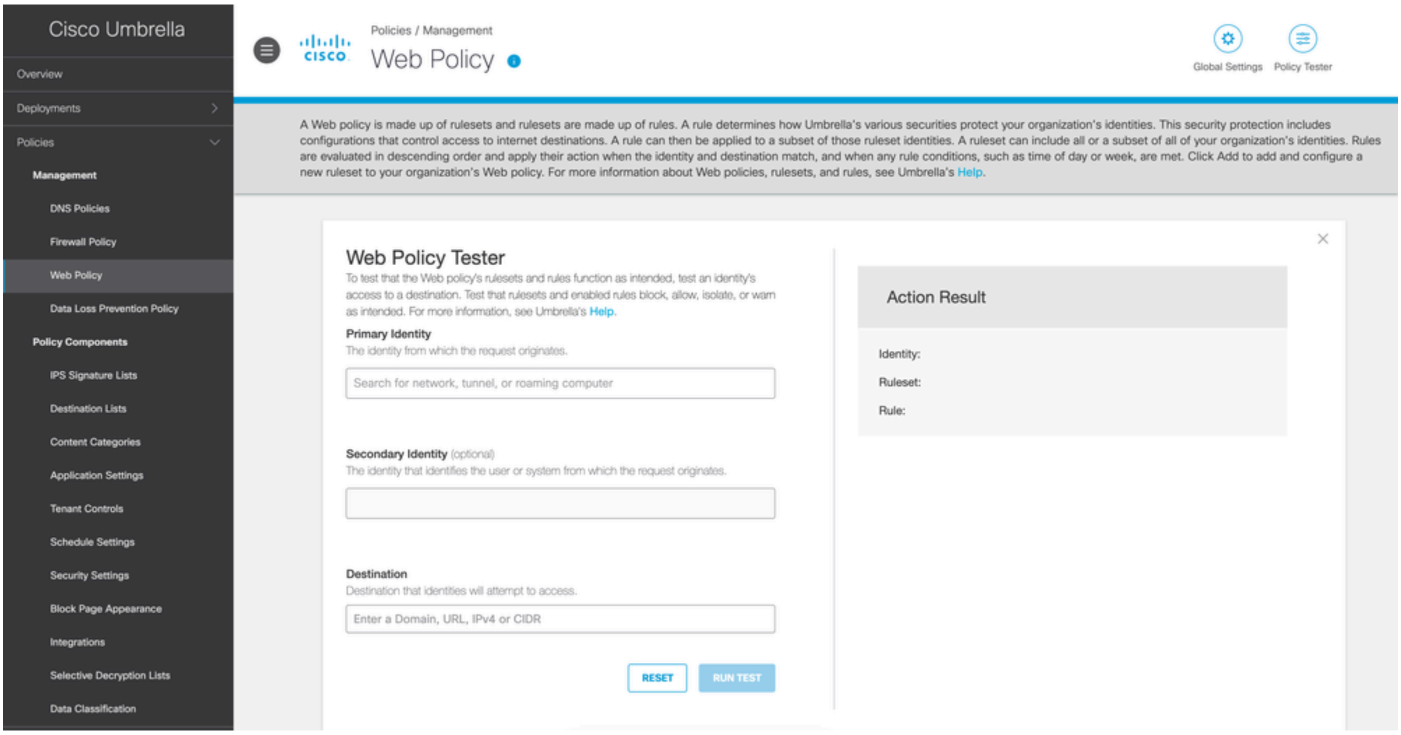
- The Network/Tunnel rules are at a higher precedence than rules which affect CSC.
- The Network/Tunnel rules are at a higher precedence than rules which affect Users/Groups.

To ensure that the rules are behaving as expected, depending on the desired outcome, you can:

- Increase the priority of CSC, User, and Group rules to maintain the current behaviour where CSC provided identities are always applied; or
- Leave the Network/Tunnel rules at a higher priority so that CSC users are subject to the Network/Tunnel policy when visiting the office network.

Troubleshooting

If your web policy is not being applied correctly you can check by using the Web Policy Tester on the Umbrella Dashboard:



A Web policy is made up of rulesets and rulesets are made up of rules. A rule determines how Umbrella's various securities protect your organization's identities. This security protection includes configurations that control access to internet destinations. A rule can then be applied to a subset of those ruleset identities. A ruleset can include all or a subset of all of your organization's identities. Rules are evaluated in descending order and apply their action when the identity and destination match, and when any rule conditions, such as time of day or week, are met. Click Add to add and configure a new ruleset to your organization's Web policy. For more information about Web policies, rulesets, and rules, see Umbrella's Help.

Web Policy Tester

To test that the Web policy's rulesets and rules function as intended, test an identity's access to a destination. Test that rulesets and enabled rules block, allow, isolate, or warn as intended. For more information, see Umbrella's Help.

Primary Identity

The identity from which the request originates.

Search for network, tunnel, or roaming computer

Secondary Identity (optional)

The identity that identifies the user or system from which the request originates.

Destination

Destination that identities will attempt to access.

Enter a Domain, URL, IPv4 or CIDR

Action Result

Identity:

Ruleset:

Rule:

4409292051348

If you have any questions about how your rules and rulesets are being applied, you can use the Umbrella Policy Debug Tool, copy or download the results, and submit a ticket to Cisco Umbrella Support with the results included.