Understand the Limitations of the Umbrella DNS Policy Tester

Contents

Introduction

This document describes restrictions and limitations of the Umbrella DNS Policy Tester.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Secure Web Gateway
- Secure Internet Gateway
- Umbrella (DNS Added Layer)

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

The Umbrella Policy Tester can be used to determine whether a given destination can be blocked or allowed by Cisco when visited by a given identity. However, there are a few circumstances under which the Policy Tester currently cannot return accurate (or any) information for a given destination. This article outlines these restrictions.

Technical Details

The Policy Tester general overview can be found in the Umbrella documentation for Umbrella Policy Tester.

These Policy Tester results can be incorrect:

Secure Web Gateway

- Unsupported

Secure Internet Gateway

- Unsupported

Umbrella (DNS Added Layer)

- Destinations which are blocked by the Intelligent Proxy can be incorrectly reported as "Allowed" by the Policy Tester. This also includes:
  - Custom URL block lists
  - Proxy-blocklist or greylist domains
  - File inspection blocks
- Destination type "Application" (like Dropbox, Box, Facebook, etc by name) which are blocked can be incorrectly reported as "Allowed" by the Policy Tester.
- When a network is also applied to a web policy, the web policy can incorrectly show. The policy tester is not supported at this time for networks which are also a part of web policies.
- Tests which do not supply all relevant identity information can show incorrect results. For example, a roaming computer with the Active Directory (AD) integration turned on while on a protected network: the test can fail if only the AD user is supplied but the roaming computer wins policy decisions.
- Destinations blocked due to content categories can show as allowed if they are entered with upper and lower case letters or are capitalized. For example, if you are blocking the "nudity" category, the domain playboy.com can show as blocked while Playboy.com appears as allowed.
- "Dynamic DNS" destinations can be blocked if that security category is selected, but can be incorrectly reported as "Allowed" by the Policy Tester.
- Destinations allowed by application control can incorrectly show as blocked in the Policy Tester.
- Destinations that are blocked by the Umbrella Enforcement API for Custom Integrations can be incorrectly reported as "Allowed" by the Policy Tester.
- Destinations that are blocked by the Umbrella AMP Threat Grid Integration can be incorrectly reported as "Allowed" by the Policy Tester.
- Destinations that are blocked due to a CNAME can be incorrectly reported as "Allowed" by the Policy Tester.
- Destinations which are IP addresses are unsupported in the Policy Tester at this time.
- Destinations which are URLs are unsupported in thePolicy Tester at this time.
- Destinations blocked for resolving to a malicious IP can be incorrectly reported as "Allowed" by the Policy Tester.
- "Potentially Harmful" destinations can be blocked if that security category is selected, but can be incorrectly reported as "Allowed" by the Policy Tester.
- Destinations where automated DDOS protections temporarily prevent DNS from responding for the affected domain are not visible by the Policy Tester.
- Destinations blocked under the content category "German Youth Protection" can be incorrectly reported as "Allowed" by the Policy Tester. This category cannot be mentioned in the results of the Policy Tester.
- Destinations blocked due to "Cryptocurrency" security classification can incorrectly appear as "Allowed" even when blocked by security settings.
- Blocks due to DNS Tunneling VPN categories cannot correctly show results in the Policy Tester.

They incorrectly show as allowed.

- Chromebook devices behind a Virtual Appliance can show incorrect policy. Chromebook (UCC) identity blocks can override Virtual Appliance applied policies, but Virtual Appliance blocks can override UCC allows.
- Members of AD groups where the group are not synced to Umbrella (including groups part of a parent or child domain and groups which are members of groups not selectively synced to Umbrella) can be shown as matching the shown policy in the Policy Tester. The user policy cannot apply in the cloud. Confirm by adding the single user to your policy and confirm it applies correctly within 5 minutes.
- Destinations that are on the Internal Domains list. The Policy Tester does not take the Internal Domains list when reporting a test result.
- Categories that do not appear at the OpenDNS Community domain tagging site are not guaranteed to show the correct category on the Policy Tester. Only one source of categorizations are represented.
- The Policy Tester is limited to showing 20 results when searching for an identity.
- An AD user is a member of a Nested AD group, but only the Parent AD group is selected in identities when creating DNS policy. Policy Tester lookup can fail to match correct policy.
- Destinations in the protected allow list can be incorrectly reported as "Blocked" by the Policy Tester.