Troubleshoot Which Policy Is Applied for SWG Proxy

Contents

Introduction

This document describes how to troubleshoot which policy is being applied for SWG Proxy.

Overview

Through Web policies, you set the rules as to how Umbrella applies security and access control to your identities Web traffic. This article helps an Umbrella administrator:

- Confirm that Web traffic is routed to Umbrella's Secure Web Gateway (SWG)
- Identify the applied Web Policy for a given identity
- Conduct basic Web policy troubleshooting

Confirm Traffic is Reaching the SWG

If traffic is sent to the SWG the public IP address falls within the 146.112.0.0/16 or 155.190.0.0/16 range. This test determines if traffic is reaching the SWG.

https://www.whatismyip.com https://myipv4.p1.opendns.com/get_my_ip	The external IP falls within the 146.112.0.0/16, 155.190.0.0/16 or 151.186.0.0/16
https://www.toolsvoid.com/proxy-test	Information about any proxy servers on your internet connection
http://httpbin.org	A simple HTTP Request and Response Service. Run a GET request and look for the origin of the JSON output
View the SSL certificate chain within the Web browser	

Determine the Web Policy

To know which Web policy the identity is matching a given identity, the administrator needs to open a Web browser on the client machine and navigate to this debug link:

https://policy-debug.checkumbrella.com/

The output looks similar to the example below:
<OrgID> is a unique organization identifier
<Bundle ID> is a unique policy identifier

<#root>

```
https://dashboard.umbrella.com/o/<OrgID>/#/configuration/policy/<Bundle-ID>
```


Screen_Shot_2019-07-21_at_1.51.41_PM.png

If the administrator is logged into the Umbrella dashboard, clicking the link directs them to the applied Web Policy. In the screenshot below, we see the 'webpolicy' (bundle 1215094) is applied.
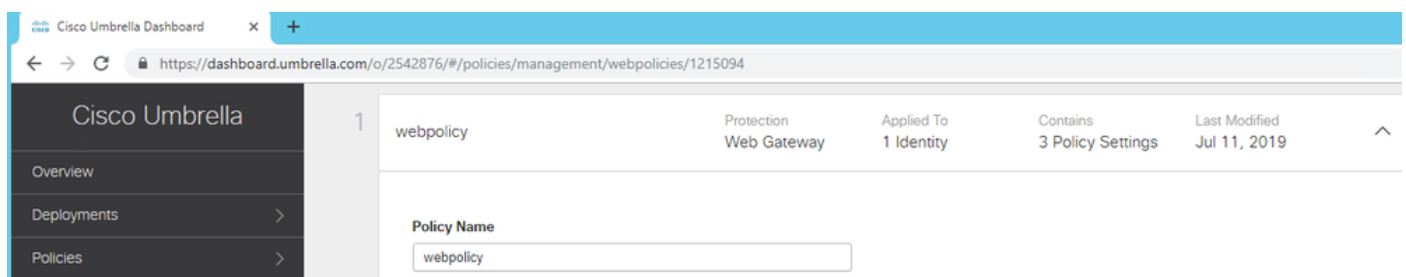

Screen_Shot_2019-07-21_at_2.51.27_PM.png

Basic Troubleshooting

- Ensure traffic is routed to the SWG
- Ensure the Web policy is applied to the expected identity. Please see: https://docs.umbrella.com/umbrella-user-guide/docs/manage-web-policies
- If the domain is bypassing the SWG, check if the domain is listed in the dashboard's 'External Domains' list. Found under **Deployments > Configuration > Domain Management**

If you are raising a Support case, please provide:

- A copy of the debug link
- The expected identity and Web policy
- Method of connection to the SWG: PAC file, AnyConnect SWG module or Tunnel

---
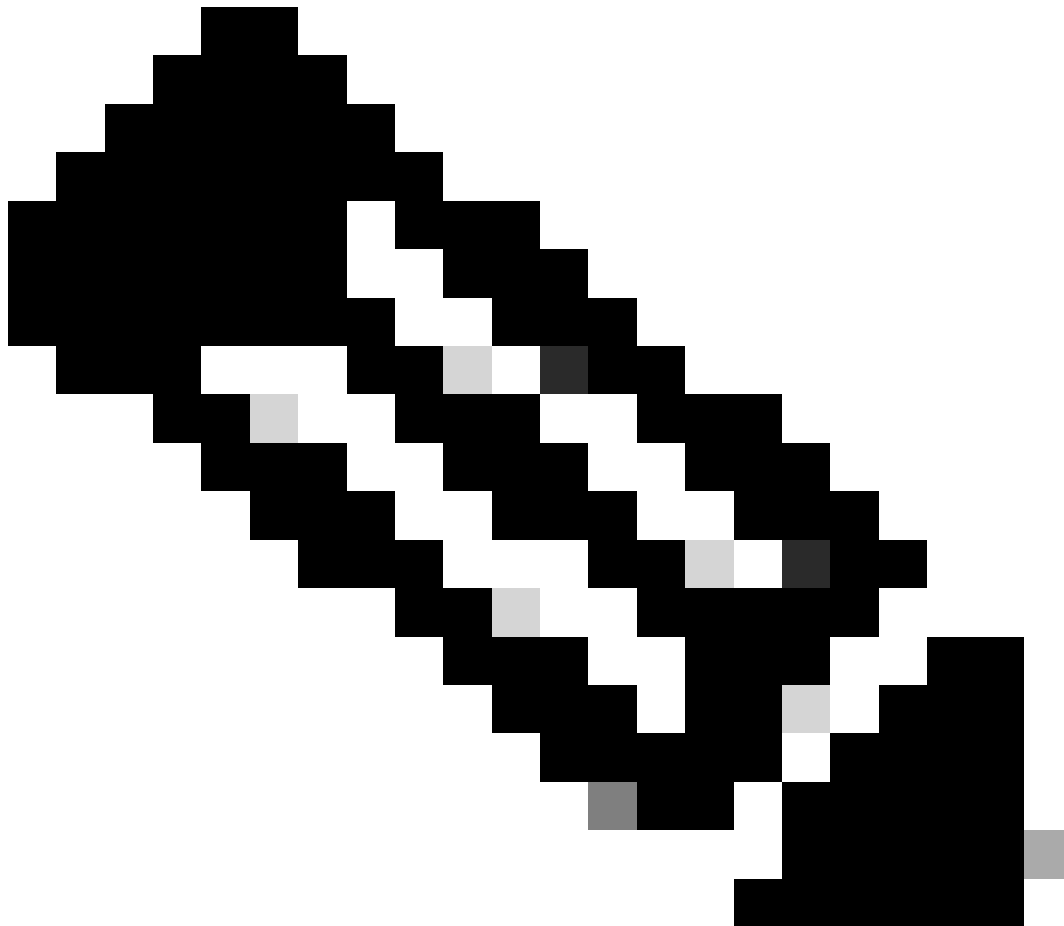
Note: The command nslookup-q=txt debug.opendns.com cannot be used to determine policy for SWG and is only limited to determining policy for DNS.