End of Life for IP Layer Enforcement Feature of the Umbrella Roaming Client

Contents

Introduction

This document describes the Cisco Umbrella announcement that IP Layer Enforcement is end of life on **July 31, 2022**.

Overview

IP Layer Enforcement is an optional feature for roaming clients made available with the Umbrella Intelligent Proxy for select Cisco Umbrella packages.

IP Layer Enforcement is no longer be included in Cisco Umbrella packages ordered by customers from and after **August 31, 2021**. For customers who previously ordered a package that contained the IP Layer Enforcement option, the feature continues to work until **July 31, 2022**. Cloud-side services required to operate IP Layer Enforcement is shut down on **July 31, 2022**.

Cisco Umbrella DNS Essentials and DNS Advantage packages provide a simple to deploy, easy to manage powerful DNS security solution. These DNS packages continue to protect DNS subscribers against malicious servers for all connections - even to unknown, uncategorized domains that resolve to a malicious IP address - that begin with an Umbrella DNS request (through DNS layer enforcement).

Cisco Umbrella Secure Internet Gateway (SIG) packages include even more advanced security coverage across all traffic (DNS, IP, web, and more). SIG includes a Secure Web Gateway (“SWG”) to analyze all traffic on web ports (IP or domain destinations), and a Cloud Delivered Firewall (“CDFW”) that layers on a cloud-based firewall in addition to SWG. This enhances the portfolio of Cisco cloud security efficacies far beyond DNS with IP Layer Enforcement, and beyond the requirement of endpoint software to deliver more-than-DNS protection. We encourage anyone who requires more-than-DNS coverage to consider the Umbrella SIG package.

Protect your network stack with Cisco Umbrella and speak with your Cisco Umbrella account manager today to learn more about the Cisco Secure Internet Gateway solution.

Supplemental Information

AnyConnect Version Support

IP Layer Enforcement is supported on AnyConnect version 4.x through the IP Layer Enforcement end-of-life date. Version 5.x does not support IP Layer Enforcement. The Cisco Secure Client branded client does not contain IP Layer Enforcement support. Existing AnyConnect users must continue use of the AnyConnect 4.x client to make use of IP Layer Enforcement functionality through the IP Layer

Enforcement end-of-life date.

Cisco Alternatives

Cisco Secure Endpoint (formerly AMP) provides on-device protection against direct to IP threats. This includes functionality called "DFC" which evaluates new connections for new processes. This functionality is slated to grow to further supplant Umbrella IPLE functionality. Contact your account manager to discuss adding Cisco Secure Endpoint to your ELA.

SIG provides coverage for all web traffic on SWG and all public Internet traffic with Cloud Firewall. **Over 95% of IPLE blocks are web traffic that is covered by SWG!** (web traffic over TCP 443 and 80). This functionality is provided by SWG and is not powered by IPLE.

View the IPLE Added Value for Your Organization

To calculate the current IP Layer Enforcement blocks for your organization per million log lines, perform these steps:

1. Log into the Umbrella Dashboard and open the Activity Search report.
2. Navigate to the "IP Layer Enforcement" log type (changing from "All").
3. Export a CSV of 1,000,000 rows and download the exported report.
4. Filter out all lines that do not contain a category of "Malware" or "Botnet".
    - Exclude "Unauthorized IP Tunnel Traffic". This category is traffic hitting the IPSec tunnel that is not an enforcement list. It is automatically dropped from our services.
    - Note the traffic port. Ports 443 and 80 would have been fully covered by our SIG Essentials package.
5. The total number of blocks is the block count for your organization. Compare this to the total DNS requests in your "Total Requests" report to calculate a percentage of efficacy.