How to Block Unknown Applications on Secure Web Appliance

Contents

Introduction

This document describes several methods to block unknown applications on Cisco Secure Web Appliance.

Methods to Block Unknown Applications

You can use any of these methods alone or in combination.

> **Note**: This Knowledge Base article references software which is not maintained or supported by Cisco. The information is provided as a courtesy for your convenience. For further assistance, please contact the software vendor.

Block Applications Based on User Agent Strings

The first defense is to use User Agent strings to block unknown applications.

- Add the User Agent under **Web Security Manager** > **Access Policies** > **Protocols and User Agents** column <for the required access policy>.
- Add the User Agent string under **Block Custom User Agents** (one per line).

> **Note**: You can use the links provided under Reference to search for User Agents.

Block Applications Based on Application Visibility Controls

If Application Visibility Controls (AVC) are enabled (under **GUI** > **Security Services** > **Web Reputation and**

Anti-Malware), then you can block access based on application types such as Proxies, File Sharing, Internet Utilities, and so on. You can do this under **Web Security Manager** > **Access Policies** > **Applications** column <for the required access policy>.

Block Applications Based on MIME Type

If the User Agent does not exist, you can attempt to add the Multipurpose Internet Mail Extensions (MIME) type:

- Add MIME types under **Web Security Manager** > **Web Access Policies** > **Objects** column <for the required access policy>.
- Add the object/MIME type in the **Block Custom MIME Types** section (one per line). For example, to block BitTorrent applications, enter application/x-bittorrent.

Note: You can use the links provided under Reference to search for MIME types.

Block URL Categories in Access Policies

Ensure that categories such as Filter Avoidance, Illegal Activities, Illegal Downloads, and so on are blocked in access policies. If some applications use known URLs or IP addresses for their connections, then you can block their associated predefined URL categories or configure them in a blocked custom URL category using their IP address, Fully Qualified Domain Name (FQDN), or a regex that matches the domains. You can do this under **Web Security Manager** > **Access Policies** > **URL Categories** column.

Restrict HTTP CONNECT Ports Configuration in Access Policy

Some applications can use the HTTP CONNECT method to connect to different ports. Only allow known ports or the specific ports that are needed in your environment in the HTTP CONNECT ports configuration domains:

- HTTP CONNECT can be configured under **Web Security Manager** > **Access Policies** > **Protocols and User Agents** column <for the required access policy>.
- Add allowed ports under **HTTP CONNECT Ports**.

Block Access for Specific IP Addresses

For applications where you only know about destination IP addresses that are being accessed, you can use the L4 Traffic Monitor feature to block access for those specific IP addresses. You can add the destination IPs under **Web Security Manager** > **L4 Traffic Monitor** > **Additional Suspected Malware Addresses**.

How to Find Which User Agent or MIME Type an Application Uses

If you do not know which User Agent or MIME type is being used by certain applications, then you can perform either of these steps to find this information:

- Run a packet capture with WireShark (Ethereal) on the client's machine and filter for 'http' protocol.
- Run the capture on Secure Web Appliance (under **Support and Help** > **Packet Capture**), filtered on the client's IP address.

Reference

> **Note**: The external websites listed here are provided for reference only. Links and content are not controlled by Cisco and are subject to change.

List of User Agents

User Agent String.Com (at useragentstring.com)

List of MIME Types

- Common MIME types (at mozilla.org)
- MIME types: Complete list of MIME types (at w3cub.com)
- The Complete List of MIME Types (at sitepoint.com)