How do you block unknown applications on Cisco Web Security Appliance?

Document ID: 118486

Contributed by Khoa Nguyen and Siddharth Rajpathak, Cisco TAC Engineers.

Oct 14, 2014

Contents

Question

How do you block unknown applications on Cisco Web Security Appliance?

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.

1. The first defense is to use "User Agent" strings to block such applications. Since we do not know all the user−agents for these application, you will need to search them on the links below.
   - We can 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).

2. If Application Visibility Controls (AVC) are enabled *(Under GUI > Security Services > Web Reputation and Anti−Malware)*, then we can block access based on application types like Proxies, File Sharing, Internet utilities. We can do this under ***Web Security Manager*** > ***Access Policies*** > ***'Applications'*** *column <for the required access policy>*.
3. If the User Agent does not exist, you can attempt to add the MIME type (Example: bit torrents applications).
   - We can add "MIME" types *under* ***Web Security Manager*** > ***Web Access Policies*** > ***Objects*** *column <for the required access policy>* .
   - −−−> Add in the object/mime type in ***'Block Custom MIME Types'*** section like application/x−bittorrent (one per line).

4. Ensure that the categories like Filter Avoidance, Illegal Activities are blocked in access policies. If some applications use known URLs or IP addresses for their connections, then we can block their assocaited predefined URL categories or configure them in a blocked custom URL category using their IP address, FQDN, or a regex matching the domains. We can do this *under* ***Web Security Manager*** > ***Access Policies*** > ***"URL Categories"*** column.
5. Some applications can use the HTTP CONNECT method to connect to different ports. Only allow known ports or specific ports 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:**'*

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

If you are unaware of which 'User Agent' or 'Mime type' is being used by certain applications, then you can do either of the following to find this information:

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

List of user agents:
==========
http://www.user−agents.org/

List of MIME types:
==========
http://www.webmaster−toolkit.com/mime−types.shtml

http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx

Updated: Oct 14, 2014 Document ID: 118486