Block Upload Traffic in Secure Web Appliance

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configuration Steps

Reporting and Logs

- Logs
- Reporting

Related Content

Introduction

This document describes the process of blocking upload traffic to certain websites in the Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

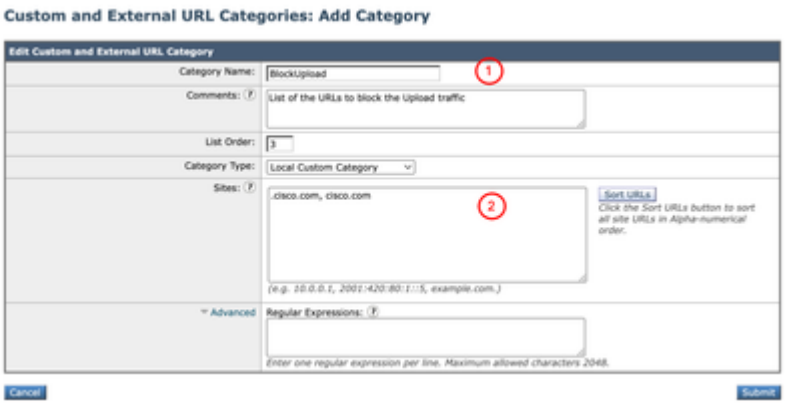
- Access To Graphic User Interface (GUI) of SWA
- Administrative Access to the SWA.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Configuration Steps

Step 1. Create a Custom URL Category for the website.	**Step 1.1.** From the GUI, navigate to **Web Security Manage**r and choose **Custom and External URL Categories**. **Step 1.2.** Click **Add Category** to create a new Custom URL Category. **Step 1.3.** Enter **Name** for the new category. **Step 1.4.** Define the domain and/or subdomains of the website for which you want to block upload traffic. In this example, the domain is cisco.com and all its subdomains. **Step 1.5. Submit** the changes.  *Image - Create Custom URL Category* **Tip**: For more information about how to configure Custom URL Categories, visit: Configure Custom URL Categories in Secure Web Appliance.
Step 2. Decrypt the traffic for the URL	**Step 2.1.** From the GUI, Navigate to **Web Security Manager** and choose **Decryption Policies** **Step 2.2.** Click **Add Policy**. **Step 2.3.** Enter **Name** for the new policy. **Step 2.4.** (Optional) Select the **Identification Profile** that you need this policy applies to. **Step 2.5.** From **Policy Member Definition** section, Click **URL Categories** links to add the Custom URL Category. **Step 2.6.** Select the URL Category that was created in **Step 1**. **Step 2.7.** Click **Submit**.

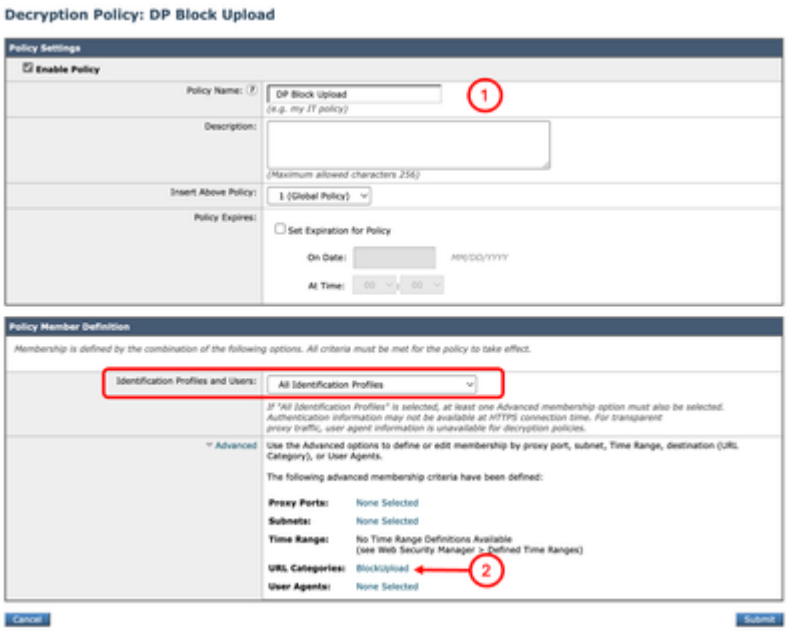
<table>
<tr>
<td></td>
<td>


Image - Create a Decryption Policy

Step 2.8. In **Decryption Policies** page, click the link from **URL Filtering** for the new policy.



Image - Select the URL Filtering

Step 2.9. Choose **Decrypt** as the action for Custom URL Category.

Step 2.10. Click **Submit**.

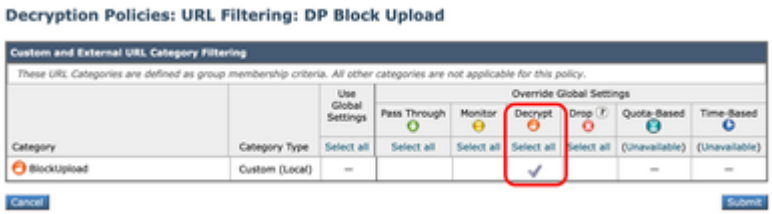


Image - Set Decrypt as Action

Step 3. Block the Upload Traffic	**Step 3.1.** From the GUI, Navigate to **Web Security Manager** and choose **Cisco Data Security**. **Step 3.2.** Click **Add Policy**. **Step 3.3.** Enter **Name** for the new policy. **Step 3.4.** (Optional) Select the **Identification Profile** that you need this policy applies to.

Step 3.5. From **Policy Member Definition** section, Click **URL Categories** links to add the Custom URL Category.

Step 3.6. Select the URL Category that was created in **Step 1**.

Step 3.7. Click **Submit**.

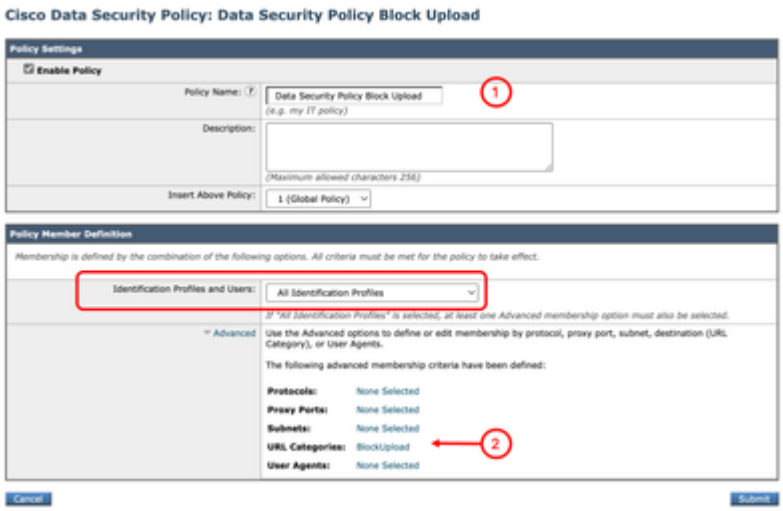


Image - Cisco Data Security Policy

Tip: For reporting purposes, choose a unique name that is different from other access and decryption policies.

Step 3.8. In **Cisco Data Security Policy** page, click the link from **URL Filtering** for the new policy.



Image - Select the URL Filtering

Step 3.9. Choose **Block** as the action for Custom URL Category.

Step 3.10. Click **Submit**.



Image - Block Upload

Step 3.11. Commit changes.

Reporting and Logs

Logs

You can view the logs related to the upload traffic from CLI by choosing **idsdataloss_logs** which is the default logging name for **Data Security Logs**.

Use these steps to access the logs:

Step 1. Log in to the CLI .

Step 2. Type **grep** and press **Enter**.

Step 3. Find and type the number associated with **idsdataloss_logs**:

- **Type: Data Security Logs.**
- **Retrieval: FTP Poll** and press **Enter**.

Step 4. (Optional) Enter the regular expression to **grep** you can filter by keywords, or you can press **Enter**, to view all the logs.

Step 5. (Optional) **Do you want this search to be case insensitive? [Y]>** If you select any keywords in the **Step 4** you can choose the filter be case insensitive or not.

Step 6. (Optional) **Do you want to search for non-matching lines? [N]>** In case you need to filter all the logs except the selected keywords defined in **Step 4** you can use this section, else, you can press **Enter**.

Step 7. (Optional) **Do you want to tail the logs? [N]>** If you need to view the live logs, type **Y** and press Enter. Otherwise, press Enter to display all the available logs.

Step 8. (Optional) **Do you want to paginate the output? [N]>** If you need to see the results per page, you can type **Y** and press Enter, else press **Enter** to use the default value **[N]**.

Reporting

You can generate Web Tracking report to view the reports of the blocked upload traffic by the **Cisco Data Security** policy name.

Use these steps to generate the reports:

Step 1. From the GUI, select **Reporting** and choose **Web Tracking**.

Step 2. Choose your desired **Time Range.**

Step 3. Click the **Advanced** link to search transactions using advanced criteria.

Step 4. In the **Policy** section, select **Filter by Policy** and type the name of the **Cisco Data Security** that was created previously.

Step 5. Click **Search** to review the report.

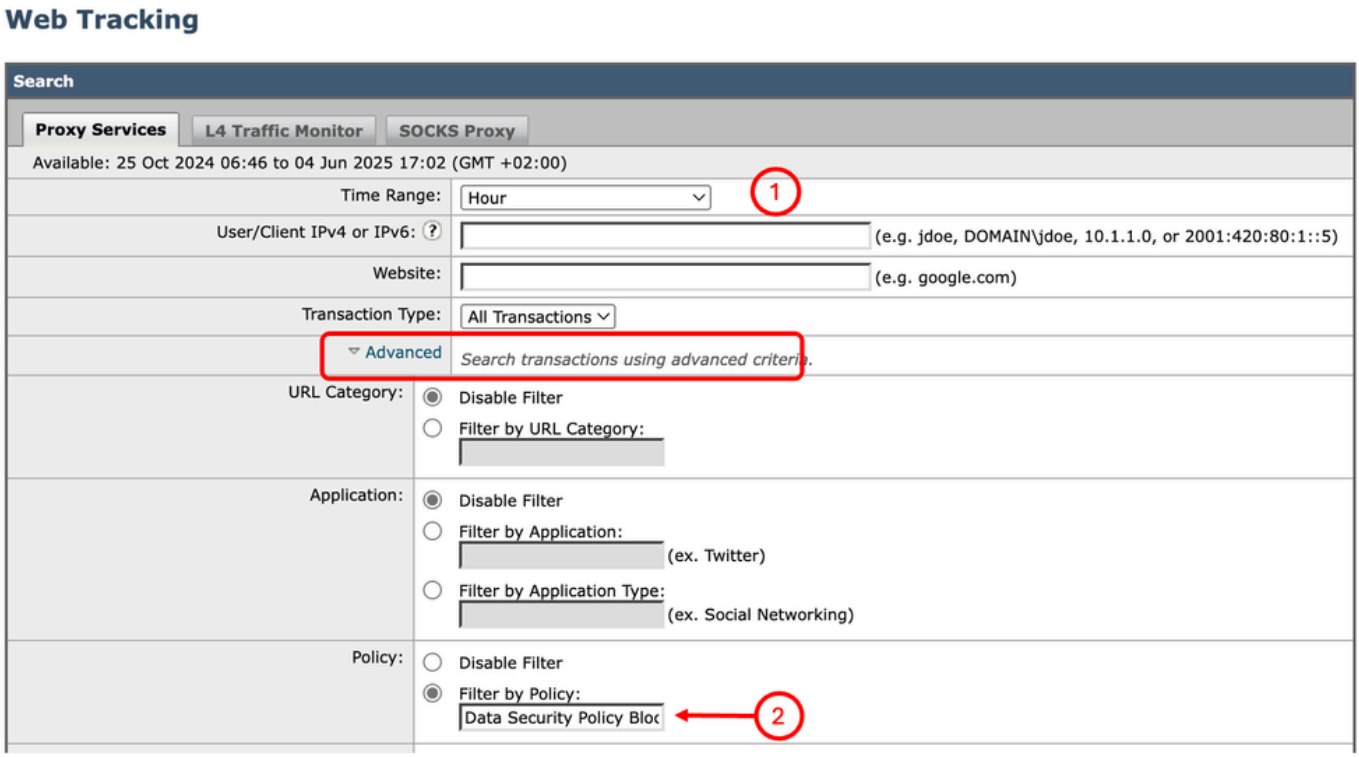


Image - Filtering the Web Tracking Reports

Related Content

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Cisco Secure Email and Web Virtual Appliance Installation Guide
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- Use Secure Web Appliance Best Practices
- Configure Firewall for Secure Web Appliance
- Configure Decryption Certificate in Secure Web Appliance
- Configure and Troubleshoot SNMP in SWA
- Configure SCP Push Logs in Secure Web Appliance with Microsoft Server
- Enable Specific YouTube Channel/Video and Block Rest of YouTube in SWA
- Understand HTTPS Accesslog Format in Secure Web Appliance
- Access Secure Web Appliance Logs

- Bypass Authentication in Secure Web Appliance
- Block Traffic in Secure Web Appliance
- Bypass Microsoft Updates Traffic in Secure Web Appliance