

Block Upload Traffic in Secure Web Appliance

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration Steps](#)

[Reporting and Logs](#)

[Logs](#)

[Reporting](#)

[Related Information](#)

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 Manager 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 that you
--	---

are trying to block upload traffic (In this example is cisco.com and all its subdomains).

Step 1.5.Submit the changes.

Custom and External URL Categories: Add Category

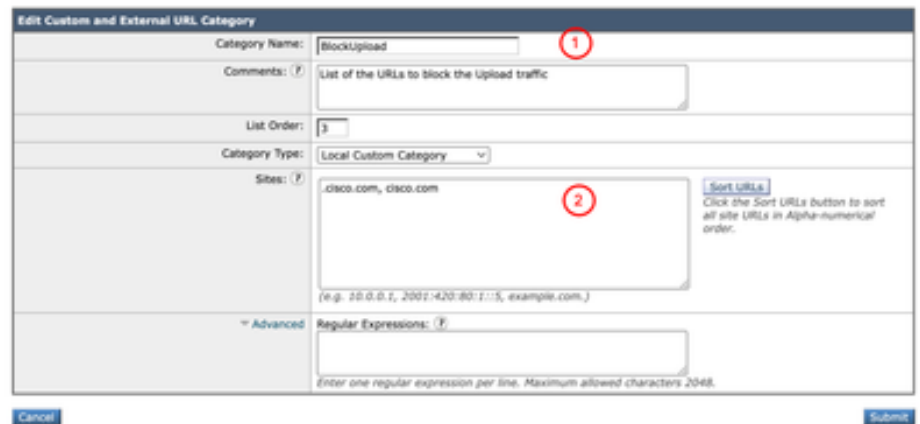


Image - Create Custom URL Category



Tip: For more information about how to configure Custom URL Categories, kindly visit: <https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

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**.

Decryption Policy: DP Block Upload

Policy Settings

☒ **Enable Policy**

Policy Name: 1

Description:

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date:

At Time:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports:

Subnets:

Time Range:

URL Categories: 2

User Agents:

Image - Create a Decryption Policy

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

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP Block Upload Identification Profile: All URL Categories: BlockUpload	Monitor: 1	(global policy)	(global policy)	<input type="button" value="Clone"/>	<input type="button" value="Delete"/>
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 107	Disabled	Decrypt		
Edit Policy Order...						

Image - Select the URL Filtering

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

Step 2.10. Click **Submit**.

Decryption Policies: URL Filtering: DP Block Upload

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings				
			Pass Through	Monitor	Decrypt	Drop	Quota-Based
BlockUpload	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)

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**.

Cisco Data Security Policy: Data Security Policy Block Upload

Policy Settings

☒ Enable Policy

Policy Name: (e.g. my IT policy) 1

Description:

(Maximum allowed characters 256)

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Advanced

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected. Use the Advanced options to define or edit membership by protocol, proxy port, subnet, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: None Selected
Proxy Ports: None Selected
Subnets: None Selected
URL Categories: BlockUpload 2
User Agents: None Selected

Image - Cisco Data Security Policy



Tip: For the reporting purpose, It is best to choose a name that is not same as any other Access/Decryption Policies.

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

Order	Cisco Data Security Policy	URL Filtering	Web Reputation	Content	Clone Policy	Delete
1	Data Security Policy Block Upload Identification Profile: All URL Categories: BlockUpload	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 108	Enabled	No maximum size for HTTP/HTTPS No maximum size for FTP		

Image - Select the URL Filtering

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

Step 3.10. Click **Submit**.

Cisco Data Security Policies: URL Filtering: Data Security Policy Block Upload

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings			
			Allow	Monitor	Block	Block
BlockUpload	Custom (Local)	Select all	Select all	Select all	Select all	Select all

Cancel

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**.

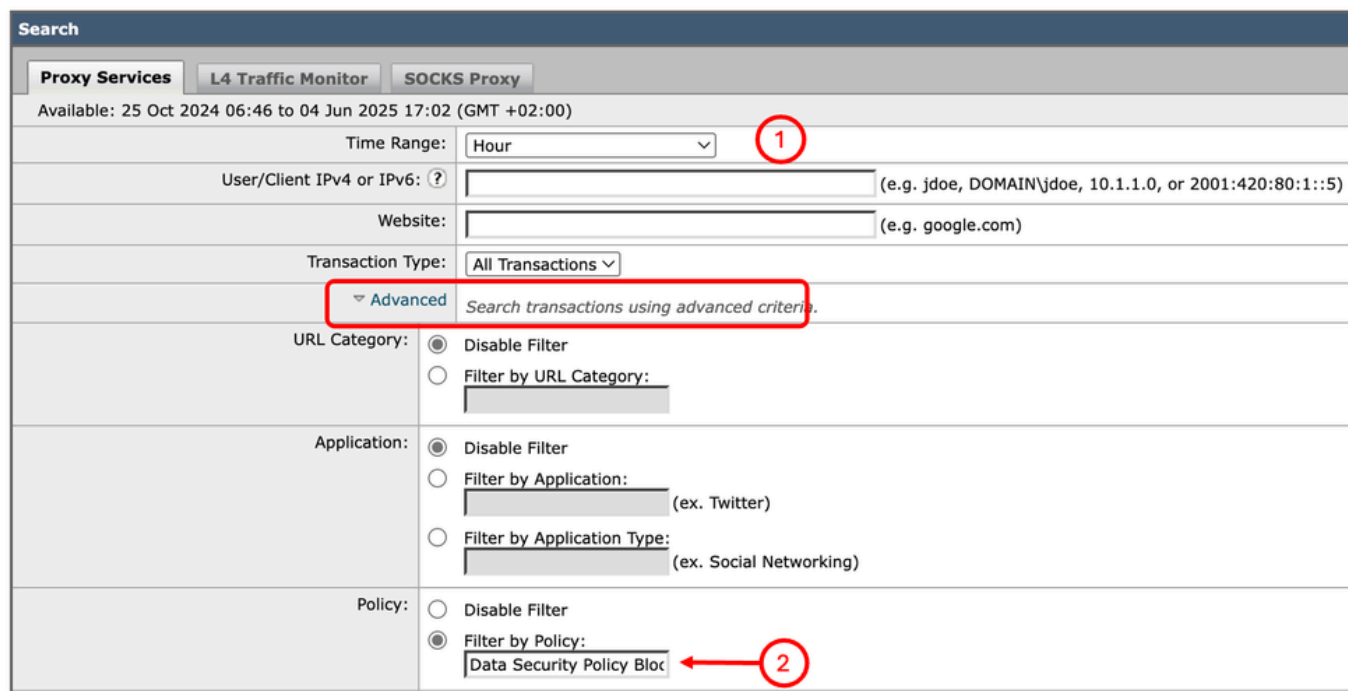
Step 2. Choose your desired **Time Range**.

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.

Web Tracking



Search

Proxy Services **L4 Traffic Monitor** **SOCKS Proxy**

Available: 25 Oct 2024 06:46 to 04 Jun 2025 17:02 (GMT +02:00)

Time Range: (1)

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type:

☒ **Advanced** Search transactions using advanced criteria.

URL Category: ☒ Disable Filter
☐ Filter by URL Category:

Application: ☒ Disable Filter
☐ Filter by Application: (ex. Twitter)
☐ Filter by Application Type: (ex. Social Networking)

Policy: ☐ Disable Filter
☒ Filter by Policy: (2)

Image - Filtering the Web Tracking Reports

Related Information

- [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](#)