

阻止安全Web裝置中的上傳流量

目錄

簡介
必要條件
需求
採用元件
設定步驟
報告和日誌
記錄檔
報告
相關資訊

簡介

本檔案介紹在安全網路裝置(SWA)中封鎖將流量上傳到特定網站的流程。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的圖形使用者介面(GUI)
- 對SWA的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

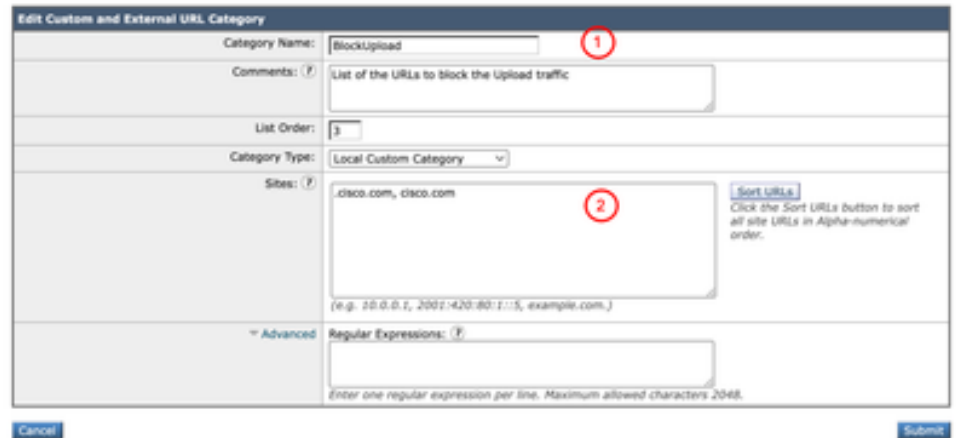
設定步驟

步驟1.為網站建立自定義URL類別。	步驟1.1.從GUI導覽至Web Security Manager並選擇Custom and External URL Categories。 步驟1.2.單擊Add Category以建立新的自定義URL類別。 步驟1.3.輸入Name作為新類別。
--------------------	---

步驟1.4.定義您嘗試阻止上傳流量的網站的域和/或子域(本示例為cisco.com及其所有子域)。

步驟1.5.提交變更。

Custom and External URL Categories: Add Category



影象 — 建立自定義URL類別



提示：有關如何配置自定義URL類別的詳細資訊，請訪問：
<https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

步驟2.解密URL的流量

步驟2.1.在GUI中，導覽至Web Security Manager，然後選擇Decryption Policies

步驟2.2.單擊Add Policy。

步驟2.3.輸入新策略的名稱。

第2.4步(可選)選擇需要應用此策略的Identification Profile。

步驟2.5.在策略成員定義部分，按一下URL類別連結以新增自定義URL類別。

步驟2.6.選擇在步驟1中建立的URL類別。

步驟2.7.按一下Submit。

Decryption Policy: DP Block Upload

Policy Settings

☒ **Enable Policy**

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

Description:

(Maximum allowed characters 256)

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: 2

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

☒ **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:

影象 — 建立解密策略

步驟2.8.在Decryption Policies頁面中，點選新策略的URL Filtering中的連結。

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)	Clone	Delete
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 107	Disabled	Decrypt		
Edit Policy Order...						

影象 — 選擇URL過濾

步驟2.9.選擇Decrypt作為Custom URL Category的操作。

步驟2.10.單擊提交。

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	<input checked="" type="text" value="Select all"/> ✓	Select all	(Unavailable)

影象 — 將解密設定為操作

步驟3.封鎖上傳流量

步驟3.1.在GUI中，導覽至Web Security Manager，然後選擇Cisco Data Security。

步驟3.2.單擊Add Policy。

步驟3.3.輸入新策略的名稱。

第3.4步(可選)選擇需要應用此策略的Identification Profile (標識配置檔案)。

步驟3.5.在Policy Member Definition部分中，按一下URL Categories連結以新增自定義URL類別。

步驟3.6.選擇在步驟1中建立的URL類別。

步驟3.7.按一下Submit。

Cisco Data Security Policy: Data Security Policy Block Upload

Policy Settings

☒ Enable Policy

Policy Name: ①
(e.g. my IT policy)

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: ②

Advanced

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
User Agents: None Selected

影象 — 思科資料安全策略

 提示：出於報告目的，最好選擇與任何其他訪問/解密策略不同的名稱。

步驟3.8.在Cisco Date Security Policy頁面中，點選新策略的URL Filtering中的連結。

Cisco Data Security Policies						
Add 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		
Edit Policy Order...						

影象 — 選擇URL過濾

步驟3.9.選擇Block作為Custom URL Category的操作。

步驟3.10。單擊提交。

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
BlockUpload	Custom (Local)	Select all	Select all	Select all	Select all

Cancel Submit

影象 — 阻止上傳

步驟3.11。提交更改。

報告和日誌

記錄檔

您可以通過選擇idsdataloss_logs (資料安全日誌的預設日誌名稱) 來從CLI檢視與上傳流量相關的日誌。

使用以下步驟訪問日誌：

步驟1.登入到CLI

步驟2.輸入grep，然後按Enter。

步驟3.查找並鍵入與idsdataloss_logs關聯的編號：

- Type:"資料安全日誌"
- 檢索：FTP Poll並按Enter。

步驟4.(可選)輸入正規表示式，以便按關鍵字進行篩選，或者按Enter檢視所有日誌

步驟5. (可選) 是否希望此搜尋不區分大小寫？[Y]>如果在步驟4中選擇了任何關鍵字，則可以選擇不區分大小寫的過濾器。

步驟6. (可選) 是否要搜尋不匹配的行？[N]>如果您需要過濾除步驟4中定義的選定關鍵字之外的所有日誌，您可以使用此部分，否則可以按Enter鍵。

步驟7. (可選) 是否要跟蹤日誌？[N]>如果需要檢視即時日誌，請鍵入Y，然後按Enter。否則，按Enter鍵顯示所有可用的日誌。

步驟8. (可選) 是否要對輸出進行分頁？[N]> 如果需要檢視每頁的結果，可以鍵入Y並按Enter鍵，否則按Enter鍵使用預設值[N]。

報告

您可以生成Web跟蹤報告，以便按照思科資料安全策略名稱檢視被阻止的上傳流量的報告。

使用以下步驟生成報告：

步驟1.在GUI中選擇Reporting，然後選擇Web Tracking。

步驟2.選擇所需的時間範圍。

步驟3.單擊Advanced連結以使用高級條件搜尋事務。

步驟4.在Policy部分，選擇Filter by Policy，然後鍵入先前建立的Cisco Data Security的名稱。

步驟5.按一下Search以檢視報告。

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: Hour (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: All Transactions

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: Data Security Policy Bloc (2)

影象 — 過濾Web跟蹤報告

相關資訊

- [Cisco Secure Web Appliance AsyncOS 15.2使用手冊](#)
- [思科安全電子郵件和網路虛擬裝置安裝指南](#)
- [在Secure Web Appliance中配置自定義URL類別 — Cisco](#)
- [使用安全Web裝置最佳做法](#)
- [為安全Web裝置配置防火牆](#)
- [在安全Web裝置中配置解密證書](#)
- [在SWA中配置SNMP並對其進行故障排除](#)
- [使用Microsoft Server在安全Web裝置中配置SCP推送日誌](#)

- [在SWA中啟用特定的YouTube頻道/影片並阻止YouTube的其餘部分](#)
- [瞭解Secure Web Appliance中的HTTPS訪問日誌格式](#)
- [訪問安全Web裝置日誌](#)
- [繞過安全Web裝置中的身份驗證](#)
- [阻止安全Web裝置中的流量](#)
- [繞過安全Web裝置中的Microsoft更新流量](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。