

Uploadverkeer blokkeren in Secure Web Appliance

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen](#)

[Rapportage en logboeken](#)

[Logboeken](#)

[verslaggeving](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces van het blokkeren van uploadverkeer naar bepaalde websites in de Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratiestappen

Stap 1. Maak een aangepaste	Stap 1.1. Navigeer vanuit de GUI naar Web Security Manager en
-----------------------------	---

URL-categorie voor de website.

kies Aangepaste en Externe URL-categorieën.

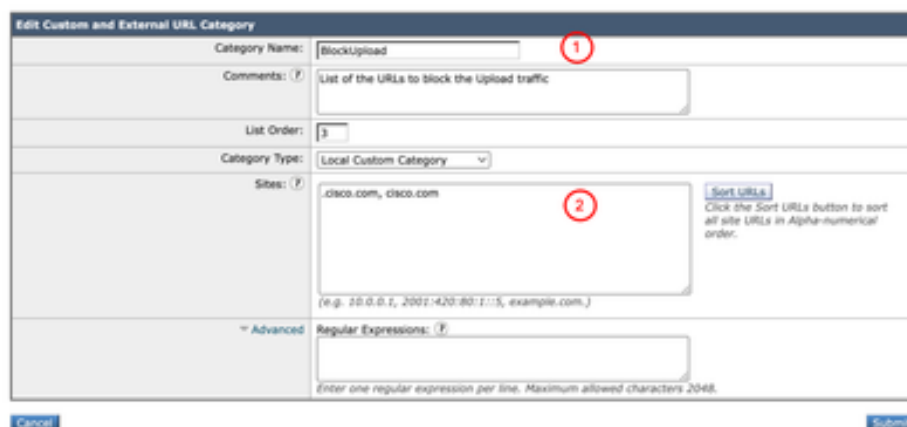
Stap 1.2. Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken.

Stap 1.3. Voer de naam voor de nieuwe rubriek in.

Stap 1.4. Definieer het domein en/of de subdomeinen van de website die u probeert te blokkeren uploadverkeer (In dit voorbeeld is cisco.com en al zijn subdomeinen).

Stap 1.5. Dien de wijzigingen in.

Custom and External URL Categories: Add Category



Afbeelding - Aangepaste URL-rubriek maken



Tip: Ga voor meer informatie over het configureren van aangepaste URL-categorieën naar:

<https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html>

Stap 2. Het verkeer voor de URL decoderen

Stap 2.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid

Stap 2.2. Klik op Beleid toevoegen.

Stap 2.3. Voer een naam in voor het nieuwe beleid.

Stap 2.4. (Optioneel) Selecteer het identificatieprofiel waarop dit beleid van toepassing is.

Stap 2.5. Klik in de sectie Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen.

Stap 2.6. Selecteer de URL-categorie die is gemaakt in stap 1.

Stap 2.7. Klik op Indienen.

Decryption Policy: DP Block Upload

Policy Settings

☒ Enable Policy

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

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:

User Agents:

Afbeelding - Een decoderingsbeleid maken

Stap 2.8. Klik op de pagina Decryptiebeleid op de koppeling URL-filtering voor het nieuwe beleid.

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)		
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 107	Disabled	Decrypt		

Afbeelding - Selecteer de URL-filtering

Stap 2.9. Kies Decrypt als de actie voor Aangepaste URL-rubriek.

Stap 2.10. Klik op Indienen.

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)	☒	☐	☐	☒	☐	☐

Afbeelding - Decoderen als actie instellen

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Stap 3. Het uploadverkeer blokkeren

Afbeelding - Selecteer de URL-filtering

Stap 3.9. Kies Blokkeren als actie voor aangepaste URL-rubriek.

Stap 3.10. Klik op Indienen.

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

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

Afbeelding - Uploaden blokkeren

Stap 3.11. Wijzigen doorvoeren.

Rapportage en logboeken

Logboeken

U kunt de logs met betrekking tot het uploadverkeer vanuit CLI bekijken door `idsdataloss_logs` te kiezen, de standaardlogboeknaam voor gegevensbeveiligingslogs.

Gebruik deze stappen om toegang te krijgen tot de logs:

Stap 1. Log in bij de CLI

Stap 2. Typ `grep` en druk op Enter.

Stap 3. Zoek en typ het nummer dat is gekoppeld aan `disdataloss_logs`:

- Type: "Logboeken voor gegevensbeveiliging"
- Retrieval: FTP Poll en druk op Enter.

Stap 4. (Optioneel) Voer de reguliere expressie in om u te greppen door te filteren op trefwoorden, of u kunt op Enter drukken, om alle logs te bekijken

Stap 5. (Optioneel) Wilt u dat deze zoekopdracht hoofdletterongevoelig is? [Y]> Als u in stap 4 trefwoorden selecteert, kunt u kiezen of het filter hoofdlettergevoelig is of niet.

Stap 6. (Optioneel) Wilt u zoeken naar niet-overeenkomende regels? [N]> Als u alle logs behalve de geselecteerde trefwoorden die zijn gedefinieerd in stap 4 moet filteren, kunt u deze sectie gebruiken, anders kunt u op Enter drukken.

Stap 7. (Optioneel) Wilt u de logs bijhouden? [N]> Als u de live logs wilt bekijken, typt u Y en drukt u op Enter. Druk anders op Enter om alle beschikbare logs weer te geven.

Stap 8. (Optioneel) Wilt u de uitvoer pagineren? [N]> Als u de resultaten per pagina wilt zien, kunt

u Y typen en op Enter drukken, anders drukt u op Enter om de standaardwaarde [N] te gebruiken.

verslaggeving

U kunt een webtrackingrapport genereren om de rapporten van het geblokkeerde uploadverkeer te bekijken met de naam van het Cisco-beleid voor gegevensbeveiliging.

Gebruik deze stappen om de rapporten te genereren:

Stap 1. Selecteer in de GUI Rapportage en kies Webtracking.

Stap 2. Kies het gewenste tijdsbereik.

Stap 3. Klik op de Geavanceerde link om transacties te zoeken met behulp van geavanceerde criteria.

Stap 4. Selecteer in het gedeelte Beleid de optie Filter op beleid en typ de naam van de Cisco-gegevensbeveiliging die eerder is gemaakt.

Stap 5. Klik op Zoeken om het rapport te bekijken.

Web Tracking

The screenshot shows the 'Search' section of the Cisco Secure Web Appliance GUI. It includes tabs for 'Proxy Services', 'L4 Traffic Monitor', and 'SOCKS Proxy'. The 'Time Range' is set to 'Hour'. The 'User/Client IPv4 or IPv6' field is empty. The 'Website' field is empty. The 'Transaction Type' is set to 'All Transactions'. The 'Advanced' search criteria are highlighted with a red box and a red circle with the number 1. The 'URL Category' is set to 'Disable Filter'. The 'Application' is set to 'Disable Filter'. The 'Policy' is set to 'Filter by Policy' with the value 'Data Security Policy Bloc' highlighted by a red circle with the number 2 and an arrow.

Afbeelding - De rapporten voor webtracering filteren

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance](#)
- [Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance](#)
- [Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco](#)

- [Best practices voor veilige webapparaten gebruiken](#)
- [Firewall configureren voor Secure Web Appliance](#)
- [Decryptiecertificaat configureren in Secure Web Appliance](#)
- [SNMP configureren en oplossen in SWA](#)
- [SCP Push Logs configureren in Secure Web Appliance met Microsoft Server](#)
- [Specifieke YouTube-kanaal / video inschakelen en de rest van YouTube blokkeren in SWA](#)
- [Inzicht in HTTPS-toegangslogindeling in Secure Web Appliance](#)
- [Toegang tot beveiligde logbestanden van webapparaten](#)
- [Verificatie omzeilen in Secure Web Appliance](#)
- [Verkeer blokkeren in Secure Web Appliance](#)
- [Microsoft Updates-verkeer omzeilen in Secure Web Appliance](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.