

Executable File Download blokkeren in SWA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voordat u begint](#)

[Configuratiestappen](#)

[Validatie van blokkering van bestandsextensies](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces van het configureren van Secure Web Appliance (SWA) om het downloaden van uitvoerbare bestanden te blokkeren.

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.

Voordat u begint

Cisco SWA kan het downloaden van uitvoerbare bestanden effectief blokkeren door het MIME-type (Multipurpose Internet Mail Extensions) van webinhoud te inspecteren. Door bestandstypen te identificeren zoals application/x-msdownload, application/x-msi en andere gerelateerde MIME-typen, handhaaft SWA beleid dat voorkomt dat uitvoerbare bestanden aan gebruikers worden geleverd. Naast MIME-typedetectie kan SWA gebruikmaken van bestandsextensiefiltering, op

reputatie gebaseerde analyse en aangepaste beleidsregels om de bescherming tegen ongewenste of risicovolle downloads verder te versterken. Deze mogelijkheden helpen organisaties een veilige browse-omgeving te behouden en het risico op malware-infecties te verminderen.



Tip: SWA kan het MIME-type van het bestand niet identificeren, tenzij het verkeer is gedecodeerd.

application/octet-stream is een generiek MIME-type dat wordt gebruikt om aan te geven dat een bestand binaire gegevens bevat. Het specificeert niet de aard van het bestand, dus het kan worden gebruikt voor elk bestand dat niet past bij een meer specifiek MIME-type. Dit type wordt gewoonlijk toegewezen aan uitvoerbare bestanden, installatieprogramma's en andere niet-tekstbestanden wanneer de webserver geen preciezer type kan bepalen.

Configuratiestappen

Stap 1. Maak een aangepaste URL-categorie voor de website.

Stap 1.1. Navigeer van de GUI naar Web Security Manager en 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 in voor de nieuwe categorie.

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

Stap 1.5. Wijzigingen indienen.

Custom and External URL Categories: Edit Category

The screenshot shows the 'Edit Custom and External URL Category' form. It has the following fields and elements:

- Category Name:** A text input field with the value 'Category'. A red circle with the number '1' is next to it.
- Comments:** A text area with a question mark icon.
- List Order:** A numeric input field with the value '1'.
- Category Type:** A dropdown menu set to 'Local Custom Category'.
- Sites:** A text area containing 'cisco.local, .cisco.local'. A red circle with the number '2' is next to it. To the right of this field is a 'Sort URLs' button with a tooltip that says 'Click the Sort URLs button to sort all site URLs in Alpha-numerical order.'
- Regular Expressions:** A text area with a question mark icon. Below it is a note: 'Enter one regular expression per line. Maximum allowed characters 2048.'
- Advanced:** A toggle switch that is currently turned off.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom.

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-cu...
Stap 2. Het verkeer voor de URL decoderen	 Let op: het decoderen van een groot aantal URL's kan leiden tot verslechtering van de prestaties.
	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.
	 Tip: (Optioneel) Als u het beleid voor alle gebruikers wilt toepassen, zelfs als ze niet zijn geverifieerd, kiest u Alle gebruikers (geverifieerde en niet-geverifieerde gebruikers).
	Stap 2.5. Klik in het gedeelte Definitie van beleidslid op URL-categoriekoppelingen 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: DecryptingTraffic

Policy Settings

☒ **Enable Policy**

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

Description:
 (Maximum allowed characters 256)

Insert Above Policy: 1 (Global Policy)

Policy Expires:
 ☐ Set Expiration for Policy
 On Date: MM/DD/YYYY
 At Time: 00 : 00

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:
 All Identification Profiles
 ☒ All Authenticated Users
 ☐ Selected Groups and Users (?)
 Groups: No groups entered
 Users: No users entered
 2 ☐ All Users (authenticated and unauthenticated users)
 If the "All Users" option 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: None Selected
 Subnets: None Selected
 Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
 URL Categories: Category
 User Agents: None Selected

[Cancel](#) [Submit](#)

Afbeelding - Een decoderingsbeleid maken

Stap 2.8. In Decryptie Beleid pagina, klik op de link van URL Filtering voor het nieuwe beleid.

Decryption Policies

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DecryptingTraffic Identification Profile: All All Identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		
Edit Policy Order...						

Afbeelding - Selecteer de URL-filtering

Stap 2.9. Kies Decrypt als de actie voor de aangepaste URL-categorie.

Stap 2.10. Klik op Indienen.

Decryption Policies: URL Filtering: DecryptingTraffic

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
Category		Select all	Select all	Select all	Select all	Select all	(Unavailable)
Category	Custom (Local)	—			✓		—

[Cancel](#) [Submit](#)

Stap 3.1. Navigeer vanuit de GUI naar Web Security Manager en kies Access Policies.

Stap 3.2. Klik op Beleid toevoegen.

Stap 3.3. Voer een naam in voor het nieuwe beleid.

Stap 3.4. (Optioneel) Selecteer het identificatieprofiel waarop dit beleid van toepassing is.



Tip: (Optioneel) Als u het beleid voor alle gebruikers wilt toepassen, zelfs als ze niet zijn geverifieerd, kiest u Alle gebruikers (geverifieerde en niet-geverifieerde gebruikers).

Stap 3.5. Klik in het gedeelte Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen.

Stap 3.6. Selecteer de URL-categorie die is gemaakt in Stap 1.

Stap 3.7. Klik op Indienen.

Stap 3. De uitvoerbare bestanden blokkeren

Access Policy: Block Exec

Policy Settings

☒ Enable Policy

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

Description:
(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy
 On Date: MM/DD/YYYY
 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:

☒ All Authenticated Users
☐ Selected Groups and Users (?)
Groups: No groups entered
Users: No users entered
☐ All Users (authenticated and unauthenticated users) 2

If the "All Users" option 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, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols:
Proxy Ports:
Subnets:
Time Range:
(see Web Security Manager > Defined Time Ranges)
URL Categories: 2
User Agents:



Tip: Voor de rapportage is het het beste om een naam te kiezen die niet hetzelfde is als elk ander toegangs- / decoderingsbeleid.

Stap 3.8. InAccess Policies pagina, zorg ervoor dat de URL Filtering actie is ingesteld op Monitor.

Stap 3.9. Klik op de pagina Access Policies op de koppeling van Objecten voor het nieuwe beleid.

Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	Block Exec Identification Profile: All All Identified users URL Categories: Category	(global policy)	Monitor: 1	Monitor: 325	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 325	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		
Edit Policy Order...									

Afbeelding - De objecten selecteren

Afbeelding - Selecteer de URL-filtering

Stap 3.10. Kies in de vervolgkeuzelijst Aangepaste objecten definiëren en blokinstellingen instellen.

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

☒ Use Global Policy Objects Blocking Settings

Define Custom Objects Blocking Settings

☐ Disable Object Blocking for this Policy

HTTP/HTTPS Max Download Size: No Maximum

FTP Max Download Size: No Maximum

Block Object Type

Not Defined

Custom MIME Types

Block Custom MIME Types: Not Defined

[Cancel](#) [Submit](#)

Afbeelding – Aangepaste objecten definiëren

Stap 3.11. ClickExecutable Code om de typen objecten te selecteren die u wilt blokkeren.

Stap 3.12. Klik op Installateurs om de typen objecten te selecteren die u wilt blokkeren.

Stap 3.13. Bovendien kunt u de MIME-typen invoeren van de bestanden die u wilt blokkeren in de sectie Aangepaste MIME-typen.

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

Define Custom Objects Blocking Settings

Objects Blocking Settings

Object Size

HTTP/HTTPS Max Download Size: ☐ 0 MB ☒ No Maximum

FTP Max Download Size: ☐ 0 MB ☒ No Maximum

Block Object Type

Object and MIME Type Reference

Archives

Inspectable Archives

Document Types

Executable Code

Java Applet

UNIX Executable

Windows Executable

Installers

UNIX/LINUX Packages

Media

P2P Metafiles

Web Page Content

Miscellaneous

Custom MIME Types

Object and MIME Type Reference

Block Custom MIME Types:

application/x-msdownload
application/x-msdos-program
application/x-msi

(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/* are valid entries. Maximum allowed characters 2048.)

Cancel

Submit

Afbeelding - Objecten configureren om te blokkeren



Tip: Als u de lijst met MIME-typen wilt weergeven, klikt u op Object en MIME-typeverwijzing.

Stap 3.14. Indienen.

Stap 3.15. Wijzigen vastleggen.

Validatie van blokkering van bestandsextensies

In dit voorbeeld wordt deze waarschuwingspagina weergegeven wanneer een gebruiker probeert een uitvoerbaar bestand te downloaden:

toegangsbeleid	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup- NONE-NONE-NONE-LAB_Access-NONE <"C_Cate", ns,0"- ", 0,0,0,-,"-,--,"-,--,"-,--,"-,--,"-,--,"-", "Unknown",- ","Unknown","-,--,"-,--", 0.00,-,"Unknown","-,--,"-,--,"-,--" "-,-,"-,--,"-,-->
----------------	---

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.