

Bloquer le téléchargement de fichiers exécutables dans SWA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Avant de commencer](#)

[Configuration Steps](#)

[Validation du blocage des extensions de fichier](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus de configuration de Secure Web Appliance (SWA) pour bloquer le téléchargement de fichiers exécutables.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface utilisateur graphique (GUI) de SWA
- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Avant de commencer

Cisco SWA peut bloquer efficacement le téléchargement de fichiers exécutables en inspectant le type de contenu Web MIME (Multipurpose Internet Mail Extensions). En identifiant des types de fichiers tels que application/x-msdownload, application/x-msi et d'autres types MIME associés, SWA applique des politiques qui empêchent l'exécution de fichiers exécutables aux utilisateurs.

En plus de la détection de type MIME, SWA peut tirer parti du filtrage des extensions de fichiers, de l'analyse basée sur la réputation et des règles de stratégie personnalisées pour renforcer la protection contre les téléchargements indésirables ou risqués. Ces fonctionnalités aident les entreprises à maintenir un environnement de navigation sécurisé et à réduire les risques d'infection par des programmes malveillants.

 Conseil : SWA ne peut pas identifier le type MIME du fichier, sauf si le trafic est déchiffré.

application/octet-stream est un type MIME générique utilisé pour indiquer qu'un fichier contient des données binaires. Il ne spécifie pas la nature du fichier, il peut donc être utilisé pour n'importe quel fichier qui ne correspond pas à un type MIME plus spécifique. Ce type est généralement attribué aux fichiers exécutables, aux programmes d'installation et à d'autres fichiers non textuels lorsque le serveur Web ne peut pas déterminer un type plus précis.

Configuration Steps

Étape 1. Créez une catégorie d'URL personnalisée pour le site Web.

- Étape 1.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Custom and External URL Categories.
- Étape 1.2. Cliquez sur Ajouter une catégorie pour créer une nouvelle catégorie d'URL personnalisée.
- Étape 1.3. EnterName pour la nouvelle catégorie.
- Étape 1.4. Définissez le domaine et/ou les sous-domaines du site Web que vous essayez de bloquer le trafic de téléchargement (dans cet exemple, cisco.local et tous ses sous-domaines).
- Étape 1.5. Envoyez les modifications.

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:

Comments:

List Order:

Category Type: Local Custom Category

Sites:

Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Advanced

Regular Expressions:

Enter one regular expression per line. Maximum allowed characters 2048.

Cancel

Submit

Image - Créer une catégorie d'URL personnalisée

	Conseil : Pour plus d'informations sur la configuration des catégories d'URL personnalisées, consultez le site : https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Étape 2. Déchiffrez le trafic de l'URL	Mise en garde : Le déchiffrement d'un grand nombre d'URL peut entraîner une dégradation des performances. Étape 2.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Decryption Policies Étape 2.2. Cliquez sur Add Policy. Étape 2.3. EnterName pour la nouvelle stratégie. Étape 2.4. (Facultatif) Sélectionnez le profil d'identification auquel s'applique cette stratégie. Conseil : (Facultatif) Si vous souhaitez appliquer la stratégie à tous les utilisateurs, même s'ils ne sont pas authentifiés, sélectionnez Tous les utilisateurs (utilisateurs authentifiés et non authentifiés). Étape 2.5. Dans la section Définition de membre de stratégie, cliquez sur le lien Catégories d'URL pour ajouter la catégorie d'URL personnalisée. Étape 2.6. Sélectionnez la catégorie d'URL créée à l'étape 1. Étape 2.7. Cliquez sur Envoyer.

Decryption Policy: DecryptingTraffic

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. 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: 2

User Agents: None Selected

Image - Créer une stratégie de déchiffrement

Étape 2.8. In Decryption Policies page, cliquez sur le lien from URL Filtering pour la nouvelle stratégie.

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...						

Image : sélectionnez le filtrage des URL.

Étape 2.9. Choisir Déchiffrer comme action pour la catégorie d'URL personnalisée.

Étape 2.10. Cliquez sur Envoyer.

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	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)
		—			☒		—

	Image - Définir le déchiffrement comme action
Étape 3. Bloquer les fichiers exécutables	Étape 3.1. Dans l'interface utilisateur graphique, accédez à Web Security Manager et choisissez Access Policies. Étape 3.2. Cliquez sur Ajouter une stratégie. Étape 3.3. EnterName pour la nouvelle stratégie. Étape 3.4. (Facultatif) Sélectionnez le profil d'identification auquel s'applique cette stratégie.  Conseil : (Facultatif) Si vous souhaitez appliquer la stratégie à tous les utilisateurs, même s'ils ne sont pas authentifiés, sélectionnez Tous les utilisateurs (utilisateurs authentifiés et non authentifiés). Étape 3.5. Dans la section Définition de membre de stratégie, cliquez sur les liens Catégories d'URL pour ajouter la catégorie d'URL personnalisée. Étape 3.6. Sélectionnez la catégorie d'URL créée à l'étape 1. Étape 3.7. Cliquez sur Envoyer. Access Policy: Block Exec Policy Settings ☒ Enable Policy Policy Name: Block Exec 1 (e.g. my IT policy) 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 ☐ All Users (authenticated and unauthenticated users) ← If the "All Users" option is selected, at least one Advanced membership option must also be selected. ☒ Advanced 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: None Selected Proxy Ports: None Selected Subnets: None Selected Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges) URL Categories: Category ← 2 User Agents: None Selected Cancel Submit



Conseil : Pour les besoins du reporting, il est préférable de choisir un nom différent des autres politiques d'accès/décodage.

Étape 3.8. Dans la page Stratégies d'accès, assurez-vous que l'action Filtrage d'URL est définie sur Surveiller.

Étape 3.9. Dans la page Stratégies d'accès, cliquez sur le lien à partir de Objets pour la nouvelle stratégie.

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...									

Image - Sélectionner les objets

Image : sélectionnez le filtrage des URL.

Étape 3.10. Dans le menu déroulant, sélectionnez Définir les paramètres de blocage des objets personnalisés.

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

Image - Définir des objets personnalisés

Étape 3.11. Cliquez sur Code exécutable pour sélectionner les types d'objets à bloquer.

Étape 3.12. Cliquez sur Installers pour sélectionner les types d'objets que vous souhaitez bloquer.

Étape 3.13. En outre, vous pouvez entrer les types MIME des

fichiers que vous souhaitez bloquer dans la section Types MIME personnalisés.

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 **1**
 - ☒ Java Applet
 - ☒ UNIX Executable
 - ☒ Windows Executable
- ▾ Installers **2**
 - ☒ UNIX/LINUX Packages
- Media
- P2P Metafiles
- Web Page Content
- Miscellaneous

Custom MIME Types

Object and MIME Type Reference ⓘ

Block Custom MIME Types: **3**

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

Image : configuration des objets à bloquer



Conseil : Pour afficher la liste des types MIME, cliquez sur Object and MIME Type Reference.

Étape 3.14.Submit.

Étape 3.15.Validez les modifications.

Validation du blocage des extensions de fichier

Dans cet exemple, lorsqu'un utilisateur tente de télécharger un fichier exécutable, la page d'avertissement suivante s'affiche :

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

Informations connexes

- [Guide de l'utilisateur d'AsyncOS 15.2 pour Cisco Secure Web Appliance](#)
- [Guide d'installation de l'appliance virtuelle Cisco Secure Email and Web](#)
- [Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco](#)
- [Utilisation des meilleures pratiques de sécurisation des appliances Web](#)
- [Configurer le pare-feu pour l'appliance Web sécurisée](#)
- [Configurer le certificat de déchiffrement dans l'appareil Web sécurisé](#)
- [Configuration et dépannage du protocole SNMP dans SWA](#)
- [Configuration des journaux de transmission SCP dans l'appliance Web sécurisée avec Microsoft Server](#)
- [Activer une chaîne/vidéo YouTube spécifique et bloquer le reste de YouTube dans SWA](#)
- [Comprendre le format de journal d'accès HTTPS dans l'appliance Web sécurisée](#)
- [Accéder aux journaux de l'appliance Web sécurisée](#)
- [Contourner l'authentification dans l'appliance Web sécurisée](#)
- [Bloquer le trafic dans l'appliance Web sécurisée](#)
- [Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.