

Download ausführbarer Dateien in SWA blockieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Vorbereitungen](#)

[Konfigurationsschritte](#)

[Validierung der Blockierung von Dateierweiterungen](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt den Prozess der Konfiguration der Secure Web Appliance (SWA), um das Herunterladen ausführbarer Dateien zu blockieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Vorbereitungen

Die Cisco SWA können den Download ausführbarer Dateien effektiv blockieren, indem sie die Webinhalte vom Typ MIME (Multipurpose Internet Mail Extensions) überprüfen. Durch die Identifizierung von Dateitypen wie application/x-msdownload, application/x-msi und anderen

verwandten MIME-Typen erzwingt SWA Richtlinien, die verhindern, dass ausführbare Dateien an Benutzer übermittelt werden. Zusätzlich zur MIME-Typerkennung kann SWA Dateierweiterungsfilterung, reputationsbasierte Analysen und benutzerdefinierte Richtlinienregeln nutzen, um den Schutz vor unerwünschten oder riskanten Downloads weiter zu verbessern. Diese Funktionen unterstützen Unternehmen bei der Aufrechterhaltung einer sicheren Browsing-Umgebung und reduzieren das Risiko von Malware-Infektionen.



Tipp: SWA kann den MIME-Typ der Datei nur identifizieren, wenn der Datenverkehr entschlüsselt wird.

application/octet-stream ist ein generischer MIME-Typ, der angibt, dass eine Datei Binärdaten enthält. Es gibt nicht die Art der Datei an, sodass sie für jede Datei verwendet werden kann, die nicht zu einem spezifischeren MIME-Typ passt. Dieser Typ wird normalerweise ausführbaren Dateien, Installationsprogrammen und anderen Nicht-Textdateien zugewiesen, wenn der Webserver keinen genaueren Typ bestimmen kann.

Konfigurationsschritte

Schritt 1: Erstellen einer benutzerdefinierten URL-Kategorie für die Website

Schritt 1.1. Navigieren Sie von der GUI zu Web Security Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus.

Schritt 1.2. Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen.

Schritt 1.3. Enter Name für die neue Kategorie.

Schritt 1.4. Definieren Sie die Domäne und/oder Subdomänen der Website, die Sie versuchen, den Upload-Datenverkehr zu blockieren (in diesem Beispiel cisco.local und alle Subdomänen).

Schritt 1.5. Senden Sie die Änderungen.

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name: **1**

Comments:

List Order:

Category Type: Local Custom Category

Sites: **2**

[Sort URLs](#)
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

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

	Bild: Benutzerdefinierte URL-Kategorie erstellen  Tipp: Weitere Informationen zum Konfigurieren benutzerdefinierter URL-Kategorien finden Sie unter https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu.
Schritt 2:Entschlüsseln des Datenverkehrs für die URL	 Vorsicht: Das Entschlüsseln einer großen Anzahl von URLs kann zu Leistungseinbußen führen. Schritt 2.1. Navigieren Sie in der GUI zuWeb Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus. Schritt 2.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 2.3.EnterName für die neue Richtlinie. Schritt 2.4 (Optional) Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.  Tipp: (Optional) Wenn Sie die Richtlinie auf alle Benutzer anwenden möchten, auch wenn diese nicht authentifiziert sind, wählen Sie Alle Benutzer (authentifizierte und nicht authentifizierte Benutzer) aus. Schritt 2.5.AusPolicy Member Definition Abschnitt, Klicken Sie auf URL-KategorienLinks, um die benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 2.6.Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde. Schritt 2.7: Klicken Sie auf Senden.

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:

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 Identification Profiles

☒ 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

Bild - Entschlüsselungsrichtlinie erstellen

Schritt 2.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

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...						

Bild: Auswahl der URL-Filterung

Schritt 2.9. Choose Decrypt als Aktion für die benutzerdefinierte URL-Kategorie.

Schritt 2.10. Klicken Sie auf Senden.

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	Time-Based
Category	Custom (Local)	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

☒ **Decrypt** 2

Bild - Als Aktion entschlüsseln

Schritt 3.1. Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Access Policies (Zugriffsrichtlinien) aus.

Schritt 3.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 3.3. EnterName für die neue Richtlinie.

Schritt 3.4 (Optional) Wählen Sie das Identifikationsprofil aus, auf das diese Richtlinie angewendet werden soll.



Tipp: (Optional) Wenn Sie die Richtlinie auf alle Benutzer anwenden möchten, auch wenn diese nicht authentifiziert sind, wählen Sie Alle Benutzer (authentifizierte und nicht authentifizierte Benutzer) aus.

Schritt 3.5. From Policy Member Definition: Klicken Sie auf URL Categories-Links, um die benutzerdefinierte URL-Kategorie hinzuzufügen.

Schritt 3.6. Wählen Sie die URL-Kategorie aus, die in Schritt 1 erstellt wurde.

Schritt 3.7: Klicken Sie auf Senden.

Schritt 3: Blockieren der ausführbaren Dateien

Access Policy: Block Exec

Policy Settings	
☒ Enable Policy	
Policy Name: ?	Block Exec 1
Description:	
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) 2
☐ Advanced	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: 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

Bild - Zugriffsrichtlinie



Tipp: Für die Berichterstellung empfiehlt es sich, einen Namen zu wählen, der nicht mit anderen Zugriffs-/Entschlüsselungsrichtlinien übereinstimmt.

Schritt 3.8. Vergewissern Sie sich auf der Seite Access Policies (Zugriffsrichtlinien), dass die Aktion URL-Filterung auf Monitor (Überwachen) festgelegt ist.

Schritt 3.9. Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) auf den Link von Objects (Objekte) für die neue Richtlinie.

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...									

Bild - Objekte auswählen

Bild: Auswahl der URL-Filterung

Schritt 3.10. Wählen Sie aus dem Dropdown-Menü Benutzerdefinierte Einstellungen für Objektspernung definieren.

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

Bild - Benutzerdefinierte Objekte definieren

Schritt 3.11. ClickExecutable Code, um die zu blockierenden Objekttypen auszuwählen.

Schritt 3.12. Klicken Sie auf Installationsprogramme, um die zu blockierenden Objekttypen auszuwählen.

Schritt 3.13. Zusätzlich können Sie die MIME-Typen der Dateien, die Sie blockieren möchten, im Abschnitt Benutzerdefinierte MIME-Typen eingeben.

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

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

Bild - Konfigurieren von zu blockierenden Objekten



Tipp: Um die Liste der MIME-Typen anzuzeigen, klicken Sie auf Objekt- und MIME-Typreferenz.

Schritt 3.14.Senden.

Schritt 3.15.Änderungen bestätigen.

Validierung der Blockierung von Dateierweiterungen

Wenn in diesem Beispiel ein Benutzer versucht, eine ausführbare Datei herunterzuladen, wird diese Warnseite angezeigt:

Zugriffsrichtlinie	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,"-,-,-","-,-,-","-,-,-","-,-,-","-,-,-","-,-,-","-,-,-",
--------------------	--

Zugehörige Informationen

- [Bedienungsanleitung für AsyncOS 15.2 für Cisco Secure Web Appliance](#)
- [Installationsleitfaden für die Cisco Secure Email und Web Virtual Appliance](#)
- [Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco](#)
- [Best Practices für sichere Web-Appliances](#)
- [Firewall für sichere Web-Appliance konfigurieren](#)
- [Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren](#)
- [SNMP in SWA konfigurieren und Fehlerbehebung dafür durchführen](#)
- [Konfigurieren von SCP-Push-Protokollen in der sicheren Web-Appliance mit Microsoft Server](#)
- [Aktivierung bestimmter YouTube-Kanäle/Videos und Blockierung sonstiger YouTube-Inhalte in SWA](#)
- [HTTPS-Zugriffsformat in sicherer Web-Appliance](#)
- [Zugreifen auf Protokolle der sicheren Web-Appliance](#)
- [Umgehen der Authentifizierung in einer sicheren Web-Appliance](#)
- [Blockieren von Datenverkehr in einer sicheren Web-Appliance](#)
- [Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.