

Bloquear la descarga de archivos ejecutables en SWA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antes de comenzar](#)

[Configuration Steps](#)

[Validación del bloqueo de extensiones de archivo](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de configuración de Secure Web Appliance (SWA) para bloquear la descarga de archivos ejecutables.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz gráfica de usuario (GUI) de SWA
- Acceso administrativo al SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

Cisco SWA puede bloquear de forma eficaz la descarga de archivos ejecutables inspeccionando el tipo de contenido web MIME (Extensiones multipropósito de correo de Internet). Al identificar

tipos de archivos como application/x-msdownload, application/x-msi y otros tipos MIME relacionados, SWA aplica políticas que impiden que el ejecutable se entregue a los usuarios. Además de la detección de tipo MIME, SWA puede aprovechar el filtrado de extensiones de archivos, el análisis basado en la reputación y las reglas de políticas personalizadas para reforzar aún más la protección frente a descargas no deseadas o arriesgadas. Estas funciones ayudan a las organizaciones a mantener un entorno de navegación seguro y reducir el riesgo de infecciones de malware.



Consejo: SWA no puede identificar el tipo MIME del archivo, a menos que se descifre el tráfico.

application/octet-stream es un tipo MIME genérico utilizado para indicar que un archivo contiene datos binarios. No especifica la naturaleza del archivo, por lo que se puede utilizar para cualquier archivo que no se ajuste a un tipo MIME más específico. Este tipo se suele asignar a archivos ejecutables, instaladores y otros archivos que no son de texto cuando el servidor Web no puede determinar un tipo más preciso.

Configuration Steps

Paso 1. Cree una categoría de URL personalizada para el sitio web.

Paso 1.1. Desde la GUI vaya a Web Security Manager y elija Categorías de URL externas y personalizadas.

Paso 1.2. Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada.

Paso 1.3. EnterName para la nueva categoría.

Paso 1.4. Defina el dominio y/o los subdominios del sitio web que está intentando bloquear el tráfico de carga (en este ejemplo es cisco.local y todos sus subdominios).

Paso 1.5. Envíe los cambios.

Custom and External URL Categories: Edit Category

The screenshot shows the 'Edit Custom and External URL Category' form. The form 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 help icon (?) and a small 'x' icon.
- List Order:** A numeric input field with the value '1'.
- Category Type:** A dropdown menu with the selected value 'Local Custom Category'.
- Sites:** A text area with the value '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.' Below the text area is a small example text: '(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)'.
- Advanced:** A section with a 'Regular Expressions' field and a help icon (?). Below this field is a note: 'Enter one regular expression per line. Maximum allowed characters 2048.'
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom.

	Imagen - Crear categoría de URL personalizada  Consejo: Para obtener más información sobre cómo configurar categorías de URL personalizadas, visite: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Paso 2.Descifrar el tráfico para la URL	 Precaución: El descifrado de un gran número de URL puede reducir el rendimiento. Paso 2.1. Desde la GUI, vaya aAdministrador de seguridad web y elijaPolíticas de descifrado Paso 2.2.Haga clic en Agregar directiva. Paso 2.3.EnterName para la nueva política. Paso 2.4.(Opcional) Seleccione el perfil de identificación al que necesita que se aplique esta política.  Consejo: (Opcional) Si desea aplicar la política para todos los usuarios, incluso si no están autenticados, elija Todos los usuarios (usuarios autenticados y no autenticados). Paso 2.5.Desde la sección Definición de miembro de política, haga clic en los enlaces URL para agregar la categoría de URL personalizado. Paso 2.6.Seleccione la categoría de URL que se creó enPaso 1. Paso 2.7.Haga clic en Enviar.

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

Imagen - Crear una política de descifrado

Paso 2.8. En la página Políticas de descifrado, haga clic en el enlace de Filtrado de URL para la nueva política.

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...						

Imagen: seleccione el filtrado de URL

Paso 2.9. Choose Decrypt como la acción para Custom URL Category.

Paso 2.10. Haga clic en Enviar.

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	(Unavailable)

Imagen - Establecer descifrado como acción

Paso 3.1.En la GUI, vaya aAdministrador de seguridad web y elijaDirectivas de acceso.

Paso 3.2.Haga clic en Agregar directiva.

Paso 3.3.EnterName para la nueva política.

Paso 3.4.(Opcional) Seleccione el perfil de identificación al que necesita que se aplique esta política.



Consejo: (Opcional) Si desea aplicar la política para todos los usuarios, incluso si no están autenticados, elija Todos los usuarios (usuarios autenticados y no autenticados).

Paso 3.5.Desde la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado.

Paso 3.6.Seleccione la categoría de URL que se creó enPaso 1.

Paso 3.7.Haga clic en Enviar.

Paso 3.Bloquear los archivos ejecutables

Access Policy: Block Exec

Policy Settings

☒ Enable Policy

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

Description: (Maximum allowed characters 256)

Insert Above Policy: 1 (Global Policy) v

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 v

☒ 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: 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

Imagen - Política de acceso



Consejo: A efectos de generación de informes, es mejor elegir un nombre que no sea el mismo que el de cualquier otra política de acceso o descifrado.

Paso 3.8. En la página Políticas de acceso, asegúrese de que la acción Filtrado de URL está establecida en Monitor.

Paso 3.9. En la página Directivas de InAccess, haga clic en el enlace de Objetos para la nueva directiva.

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...									

Imagen: seleccione los objetos

Imagen: seleccione el filtrado de URL

Paso 3.10. En el menú desplegable, seleccione Definir configuración de bloqueo de objetos personalizados.

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](#)

Imagen - Definir objetos personalizados

Paso 3.11. Haga clic en Código ejecutable para seleccionar los tipos de objetos que desea bloquear.

Paso 3.12. Haga clic en Instaladores para seleccionar los tipos de objetos que desea bloquear.

Paso 3.13. Además puede introducir los tipos MIME de los archivos que desea bloquear en la sección Tipos MIME personalizados.

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

Object and MIME Type Reference

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

Cancel Submit

Imagen - Configuración de objetos para bloquear



Consejo: Para ver la lista de tipos MIME, haga clic en Referencia de tipo MIME y objeto.

Paso 3.14.Enviar.

Paso 3.15.Registrar cambios.

Validación del bloqueo de extensiones de archivo

En este ejemplo, cuando un usuario intenta descargar un archivo ejecutable, se muestra esta página de advertencia:

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).