

Bloquear la carga de tráfico en el dispositivo web seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Informes y registros](#)

[Registros](#)

[Informes](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de bloqueo del tráfico de carga a ciertos sitios web en el dispositivo web seguro (SWA).

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.

Configuration Steps

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

- Paso 1.1. Desde la GUI vaya a Web Security Manager y elija Custom and External URL Categories.
- Paso 1.2. Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada.
- Paso 1.3. Introduzca Nombre para la nueva categoría.
- Paso 1.4. Defina el dominio y/o subdominios del sitio web que está intentando bloquear el tráfico de carga (en este ejemplo está cisco.com y todos sus subdominios).
- Paso 1.5. Envíe los cambios.

Custom and External URL Categories: Add Category

The screenshot shows the 'Edit Custom and External URL Category' form. The 'Category Name' field contains 'BlockUpload' and is circled in red with the number '1'. The 'Comments' field contains 'List of the URLs to block the Upload traffic'. The 'List Order' is set to '3'. The 'Category Type' is 'Local Custom Category'. The 'Sites' field contains 'cisco.com, cisco.com' and is circled in red with the number '2'. There is a 'Sort URLs' button with a tooltip that says 'Click the Sort URLs button to sort all site URLs in Alpha-numerical order.' The 'Regular Expressions' field is empty. At the bottom, there are 'Cancel' and 'Submit' buttons.

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-custom-url-categories-in-secur.html>

Paso 2. Descifrar el tráfico para la URL

- Paso 2.1. Desde la GUI, navegue hasta Web Security Manager y elija Políticas de descifrado
- Paso 2.2. Haga clic en Agregar directiva.
- Paso 2.3. Introduzca Name para la nueva política.
- Paso 2.4. (Opcional) Seleccione el perfil de identificación al que necesita que se aplique esta política.
- Paso 2.5. En la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado.

Paso 2.6. Seleccione la categoría de URL que se creó en el Paso 1.

Paso 2.7. Haga clic en Enviar.

Decryption Policy: DP Block Upload

Policy Settings
 Enable Policy
Policy Name: 1
(e.g. my IP 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:
If "All Identification Profiles" 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 (Use Web Security Manager's Refined 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.

Policies						
<input type="button" value="Add Policy..."/>						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP Block Upload Identification Profile: All URL Categories: BlockUpload	<input type="text" value="Monitor: 1"/> 	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 107	Disabled	Decrypt		

Imagen: seleccione el filtrado de URL

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

Paso 2.10. Haga clic en Enviar.

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	Quote-Based
		Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
BlockUpload	Custom (Local)	--			<input checked="" type="checkbox"/>		

Imagen: seleccione Decrypt como la acción para Custom URL Category

Imagen - Establecer descifrado como acción

Paso 3.1. Desde la GUI, navegue hasta Web Security Manager y elija Cisco Data Security.

Paso 3.2. Haga clic en Agregar directiva.

Paso 3.3. Introduzca Name para la nueva política.

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

Paso 3.5. En 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 en el Paso 1.

Paso 3.7. Haga clic en Enviar.

Paso 3. Bloqueo del tráfico de carga

Cisco Data Security Policy: Data Security Policy Block Upload

The screenshot displays the configuration page for a Cisco Data Security Policy. The top section, 'Policy Settings', includes a checkbox for 'Enable Policy' which is checked. The 'Policy Name' field contains 'Data Security Policy Block Upload'. Below this is a 'Description' field and an 'Insert Above Policy' dropdown menu. The bottom section, 'Policy Member Definition', shows 'Identification Profiles and Users' set to 'All Identification Profiles'. Underneath, there are several criteria selection options: 'Protocols: None Selected', 'Proxy Ports: None Selected', 'Subnets: None Selected', 'URL Categories: BlockUpload', and 'User Agents: None Selected'. A red circle with the number '1' is placed around the policy name, and another red circle with the number '2' is placed around the 'BlockUpload' category, with a red arrow pointing to it.

Imagen - Política de seguridad de datos de Cisco



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 Cisco Date Security Policy, haga clic en el enlace de Filtrado de URL para la nueva política.

Order	Cisco Data Security Policy	URL Filtering	Web Reputation	Content	Clone Policy	Delete
1	Data Security Policy Block Upload Identification Profile: All URL Categories: BlockUpload	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 108	Enabled	No maximum size for HTTP/HTTPS No maximum size for FTP		

Imagen: seleccione el filtrado de URL

Paso 3.9. Elija Block como la acción para Custom URL Category.

Paso 3.10. Haga clic en Enviar.

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

Custom and External URL Category Filtering		Override Global Settings			
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.		Use Global Settings	Allow (?)	Monitor	Block
Category	Category Type	Select all	Select all	Select all	Select all
BlockUpload	Custom (Local)	--	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Imagen - Bloquear carga

Paso 3.11. Realice los cambios.

Informes y registros

Registros

Puede ver los registros relacionados con el tráfico de carga desde CLI eligiendo `idsdataloss_logs`, que es el nombre de registro predeterminado para Registros de seguridad de datos.

Siga estos pasos para acceder a los registros:

Paso 1. Inicie sesión en la CLI

Paso 2. Escriba `grep` y presione `Enter`.

Paso 3. Busque y escriba el número asociado a `idsdataloss_logs`:

- Tipo: "Registros de seguridad de datos"
- Recuperación: FTP Poll y pulse `Intro`.

Paso 4. (Opcional) Ingrese la expresión regular para `grep` que le gusta filtrar por palabras clave, o puede presionar `Intro`, para ver todos los registros

Paso 5. (Opcional) ¿Desea que esta búsqueda no distinga entre mayúsculas y minúsculas? [Y]>
Si selecciona cualquier palabra clave en el Paso 4, puede elegir que el filtro no distinga entre mayúsculas y minúsculas.

Paso 6. (Opcional) ¿Desea buscar líneas que no coincidan? [N]> En caso de que necesite filtrar todos los registros excepto las palabras clave seleccionadas definidas en el Paso 4, puede utilizar esta sección; de lo contrario, puede presionar Intro.

Paso 7. (Opcional) ¿Desea finalizar los registros? [N]> Si necesita ver los registros en directo, escriba Y y pulse Intro. De lo contrario, pulse Intro para mostrar todos los registros disponibles.

Paso 8. (Opcional) ¿Desea paginar la salida? [N]> Si necesita ver los resultados por página, puede escribir Y y presionar Enter; de lo contrario, presione Enter para usar el valor predeterminado [N].

Informes

Puede generar un informe de seguimiento web para ver los informes del tráfico de carga bloqueado por el nombre de la política de seguridad de datos de Cisco.

Siga estos pasos para generar los informes:

Paso 1. En la GUI, seleccione Reporting y elija Web Tracking.

Paso 2. Elija el rango de tiempo deseado.

Paso 3. Haga clic en el enlace Avanzado para buscar transacciones utilizando criterios avanzados.

Paso 4. En la sección Política, seleccione Filtrar por Política y escriba el nombre de Cisco Data Security que se creó anteriormente.

Paso 5. Haga clic en Buscar para revisar el informe.

Web Tracking

Search

Proxy Services | L4 Traffic Monitor | SOCKS Proxy

Available: 25 Oct 2024 06:46 to 04 Jun 2025 17:02 (GMT +02:00)

Time Range: Hour 1

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type: All Transactions

Advanced Search transactions using advanced criteria.

URL Category: Disable Filter
 Filter by URL Category:

Application: Disable Filter
 Filter by Application: (ex. Twitter)
 Filter by Application Type: (ex. Social Networking)

Policy: Disable Filter
 Filter by Policy: 2 ←

Información Relacionada

- [Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance](#)
- [Guía de instalación de Cisco Secure Email and Web Virtual Appliance](#)
- [Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco](#)
- [Uso de las prácticas recomendadas de Secure Web Appliance](#)
- [Configuración del firewall para el dispositivo web seguro](#)
- [Configurar certificado de descifrado en dispositivo web seguro](#)
- [Configuración y solución de problemas de SNMP en SWA](#)
- [Configuración de registros de inserción de SCP en un dispositivo web seguro con Microsoft Server](#)
- [Habilitar canal/vídeo específico de YouTube y bloquear el resto de YouTube en SWA](#)
- [Comprensión del formato de registro de acceso HTTPS en el dispositivo web seguro](#)
- [Acceder a registros de appliances web seguros](#)
- [Omitir autenticación en dispositivo web seguro](#)
- [Bloqueo del tráfico en el dispositivo web seguro](#)
- [Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro](#)

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).