

Bloqueo del tráfico en el dispositivo web seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Bloqueo del tráfico](#)

[Motivos del bloqueo por origen](#)

[Motivos del bloqueo por destino](#)

[Pasos para bloquear el tráfico](#)

[Bloqueo de sitios mediante expresiones regulares en una implementación de proxy transparente](#)

[Información Relacionada](#)

Introducción

En este documento se describen los pasos para bloquear el tráfico en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.

Cisco recomienda que tenga:

- SWA físico o virtual instalado.
- Acceso administrativo a la interfaz gráfica de usuario (GUI) de 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.

Bloqueo del tráfico

El bloqueo del tráfico en el SWA es un paso crucial para garantizar la seguridad de la red, mantener el cumplimiento de las políticas internas y protegerse frente a actividades malintencionadas. A continuación se indican algunas razones comunes para bloquear el tráfico:

Motivos del bloqueo por origen

- Inundación por parte de uno o varios usuarios: cuando uno o más usuarios generan un tráfico excesivo, puede saturar la red, lo que conduce a una degradación del rendimiento y a posibles interrupciones del servicio.
- Acceso a recursos no fiables por aplicaciones (agentes de usuario): ciertas aplicaciones podrían intentar acceder a recursos no fiables o potencialmente dañinos. El bloqueo de estos agentes de usuario ayuda a evitar brechas de seguridad y filtraciones de datos.
- Restricción del acceso a Internet para rangos de IP específicos: es posible que algunas direcciones o rangos de IP deban tener restringido el acceso a Internet debido a políticas de seguridad o para evitar el uso no autorizado.
- Comportamiento de tráfico sospechoso: el tráfico que muestra patrones o comportamientos inusuales que podrían indicar actividad maliciosa o amenazas de seguridad debe bloquearse para proteger la red.

Motivos del bloqueo por destino

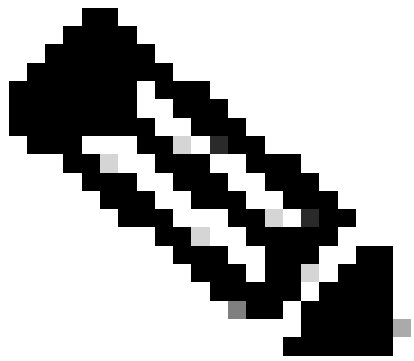
- Cumplimiento de las políticas internas de la empresa: las organizaciones a menudo cuentan con políticas que restringen el acceso a determinados sitios web o recursos online para garantizar la productividad y el cumplimiento de los requisitos legales o normativos.
- Sitios no fiables: bloquear el acceso a sitios web que se consideran no fiables o potencialmente peligrosos ayuda a proteger a los usuarios frente a la suplantación de identidad (phishing), el malware y otras amenazas online.
- Comportamiento malintencionado: los sitios que alojan contenido malintencionado o realizan actividades dañinas deben bloquearse para evitar incidentes de seguridad y violaciones de datos.

Pasos para bloquear el tráfico

En general, hay 3 etapas principales para bloquear el tráfico en SWA:

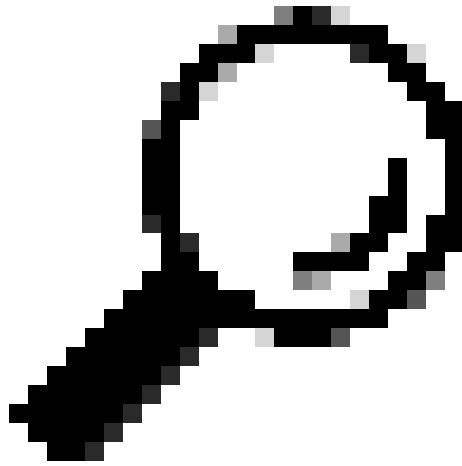
- Cree un perfil de identificación para el usuario o usuarios.
- Bloquee el tráfico HTTPS en la Política de descifrado.
- Bloquee el tráfico HTTP en la política de acceso.

Etapas	Bloquear el acceso de usuarios	Bloquear el acceso de usuarios
--------	--------------------------------	--------------------------------

	específicos a cualquier sitio web	específicos a determinados sitios web
Categoría de URL personalizada	No aplicable	<p>Cree una Categoría de URL personalizada para los sitios que planea bloquear el acceso a ellos.</p> <p>Para obtener más información, visite:</p> <p>Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco</p>
Perfil de identificación	<p>Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Perfiles de identificación.</p> <p>Paso 2. Haga clic en Add Profile para agregar un perfil.</p> <p>Paso 3. Utilice la casilla de verificación Enable Identification Profile para habilitar este perfil o para deshabilitarlo rápidamente sin eliminarlo.</p> <p>Paso 4. Asigne un nombre de perfil único.</p> <p>Paso 5. (Opcional) Agregar descripción.</p> <p>Paso 6. En la lista desplegable Insert Above, elija dónde debe aparecer este perfil en la tabla.</p> <p>Paso 7. En la sección Método de identificación de usuario, elija Exento de autenticación/identificación.</p> <p>Paso 8. En Definir miembros por subred, introduzca las direcciones IP o las subredes que debe aplicar este perfil de identificación. Puede utilizar direcciones IP, bloques de enrutamiento entre dominios sin clase (CIDR) y subredes.</p>	 <p>Nota: para bloquear el acceso de todos los usuarios a determinados sitios web, no es necesario crear un perfil de ID independiente. Esto se puede administrar de manera eficiente a través de la política de acceso/descifrado global.</p> <p>Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Perfiles de identificación.</p> <p>Paso 2. Haga clic en Add Profile para agregar un perfil.</p> <p>Paso 3. Utilice la casilla de verificación Enable Identification Profile para habilitar este perfil o para deshabilitarlo rápidamente sin eliminarlo.</p> <p>Paso 4. Asigne un nombre de perfil único.</p>

		<p>Paso 5. (Opcional) Agregar descripción.</p> <p>Paso 6. En la lista desplegable Insert Above, elija dónde debe aparecer este perfil en la tabla.</p> <p>Paso 7. En la sección Método de identificación de usuario, elija Exento de autenticación/identificación.</p> <p>Paso 8. En Definir miembros por subred, introduzca las direcciones IP o las subredes que debe aplicar este perfil de identificación. Puede utilizar direcciones IP, bloques de enrutamiento entre dominios sin clase (CIDR) y subredes.</p> <p>Paso 9. Haga clic en Advanced y agregue la categoría de URL a la que desea bloquear el acceso.</p>
<p>Política de descifrado</p>	<p>Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Política de descifrado.</p> <p>Paso 2. Haga clic en Add Policy para agregar una política de descifrado.</p> <p>Paso 3. Utilice la casilla de verificación Enable Policy para habilitar esta directiva.</p> <p>Paso 4. Asigne un nombre de directiva único.</p> <p>Paso 5. (Opcional) Agregar descripción.</p> <p>Paso 6. En la lista desplegable Insert Above Policy, elija la primera política.</p> <p>Paso 7. En Identification Profiles and Users, elija el perfil de identificación que creó en los pasos anteriores.</p> <p>Paso 8. Enviar.</p> <p>Paso 9. En la página Políticas de descifrado, en Filtrado de URL, haga</p>	<p>Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Política de descifrado.</p> <p>Paso 2. Haga clic en Add Policy para agregar una política de descifrado.</p> <p>Paso 3. Utilice la casilla de verificación Enable Policy para habilitar esta directiva.</p> <p>Paso 4. Asigne un nombre de directiva único.</p> <p>Paso 5. (Opcional) Agregar descripción.</p> <p>Paso 6. En la lista desplegable Insert Above Policy, elija la primera política.</p> <p>Paso 7. En Identification Profiles and Users, elija el perfil de identificación que creó en los pasos anteriores.</p> <p>Paso 8. Enviar.</p> <p>Paso 9. En la página Políticas de descifrado, en Filtrado de URL, haga</p>

clic en el enlace asociado a esta nueva política de descifrado.



Sugerencia: dado que está bloqueando todas las categorías de URL, puede optimizar la política eliminando las categorías de URL personalizadas y utilizando solo las categorías de URL predefinidas. Esto reduce la carga de procesamiento en el SWA al evitar el paso adicional de hacer coincidir las URL con las categorías de URL personalizadas.

Paso 10. Seleccione Drop como la acción para cada categoría de URL.

Paso 11. En la misma página, desplácese hasta Uncategorized URLs y elija Drop de la lista desplegable.

Paso 12. Enviar.

Decryption Policies

Policies						
Add Policy						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Block All Decryption Policy Identification Profile: Blocked User All identified users	Drop: 100	(global policy)	(global policy)		

Imagen - Política de descifrado para bloquear todo el sitio web para ciertos usuarios

clic en el enlace asociado a esta nueva política de descifrado.


Paso 10. Seleccione Drop como acción para la categoría de URL personalizado creada para los sitios web bloqueados.

Paso 11. Haga clic en Submit (Enviar).

Decryption Policies

Policies						
Add Policy						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Block Some URLs Decryption Policy Identification Profile: ID profile Block some URL All identified users	Drop: 1	(global policy)	(global policy)		

Imagen - Bloquear algunas URL en la política de descifrado

<p>Política de acceso</p>	<p>Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Access Policy.</p> <p>Paso 2. Haga clic en Add Policy para agregar una política de acceso.</p> <p>Paso 3. Utilice la casilla de verificación Enable Policy para habilitar esta directiva.</p> <p>Paso 4. Asigne un nombre de directiva único.</p> <p>Paso 5. (Opcional) Agregar descripción.</p> <p>Paso 6. En la lista desplegable Insert Above Policy, elija la primera política.</p> <p>Paso 7. En Identification Profiles and Users, elija el perfil de identificación que creó en los pasos anteriores.</p> <p>Paso 8. Enviar.</p> <p>Paso 9. En la página Directivas de acceso, en Protocolos y agentes de usuario, haga clic en el enlace asociado a esta nueva directiva de acceso.</p> <p>Paso 10. En la lista desplegable Editar protocolos y configuración de agentes de usuario, elija Definir configuración personalizada.</p> <p>Paso 11. IN Bloquear protocolos seleccione la casilla de verificación para ambos FTP sobre HTTP y HTTP.</p> <p>Paso 12. IN Puertos HTTP CONNECT, elimine todos los números de puerto para bloquear todos los puertos.</p>	<p>Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Access Policy.</p> <p>Paso 2. Haga clic en Add Policy para agregar una política de acceso.</p> <p>Paso 3. Utilice la casilla de verificación Enable Policy para habilitar esta directiva.</p> <p>Paso 4. Asigne un nombre de directiva único.</p> <p>Paso 5. (Opcional) Agregar descripción.</p> <p>Paso 6. En la lista desplegable Insert Above Policy, elija la primera política.</p> <p>Paso 7. En Identification Profiles and Users, elija el perfil de identificación que creó en los pasos anteriores.</p> <p>Paso 8. Enviar.</p> <p>Paso 9. En la página Políticas de acceso, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de acceso</p> <p>Paso 10. Seleccione Block (Bloquear) como acción para la categoría de URL personalizado creada para los sitios web bloqueados.</p> <p>Paso 11. Enviar.</p> <p>Paso 12. Registrar cambios.</p>  <p>Imagen- Bloquear algunas URL en la política de acceso</p>
---------------------------	--	---

Access Policies: Protocols and User Agents: AP Blocked

Edit Protocols and User Agents Settings
Define Custom Settings

Predefined Centralia

Block Protocols: FTP over HTTP
 HTTP

Note: Blocking of HTTPS is not available in Access policies when the HTTPS proxy is enabled. If the HTTPS proxy is enabled, use Observation policies to control HTTPS access.

HTTP CONNECT Ports: /

Enter 1-65535 to allow all ports via HTTP CONNECT. Leave field blank to block all ports.

Custom User Agents

Block Custom User Agents:

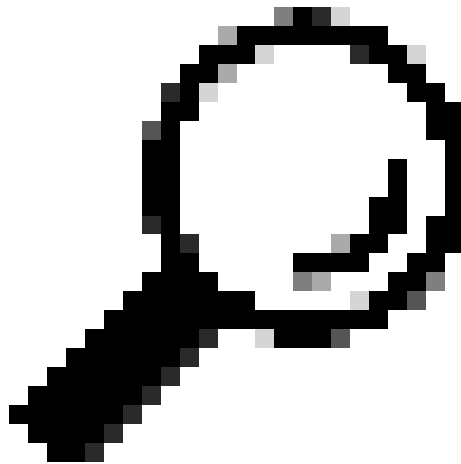
Example User Agent Patterns

(Enter any regular expression, one regular expression per line, to block user agents. Maximum allowed characters 2048.)

Imagen - Bloqueo de protocolos y puertos de conexión en la política de acceso

Paso 13. Enviar.

Paso 14. (Opcional) En la página Políticas de acceso, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de acceso y seleccione Block como la acción para cada categoría de URL y el Las URL no categorizadas se envían.



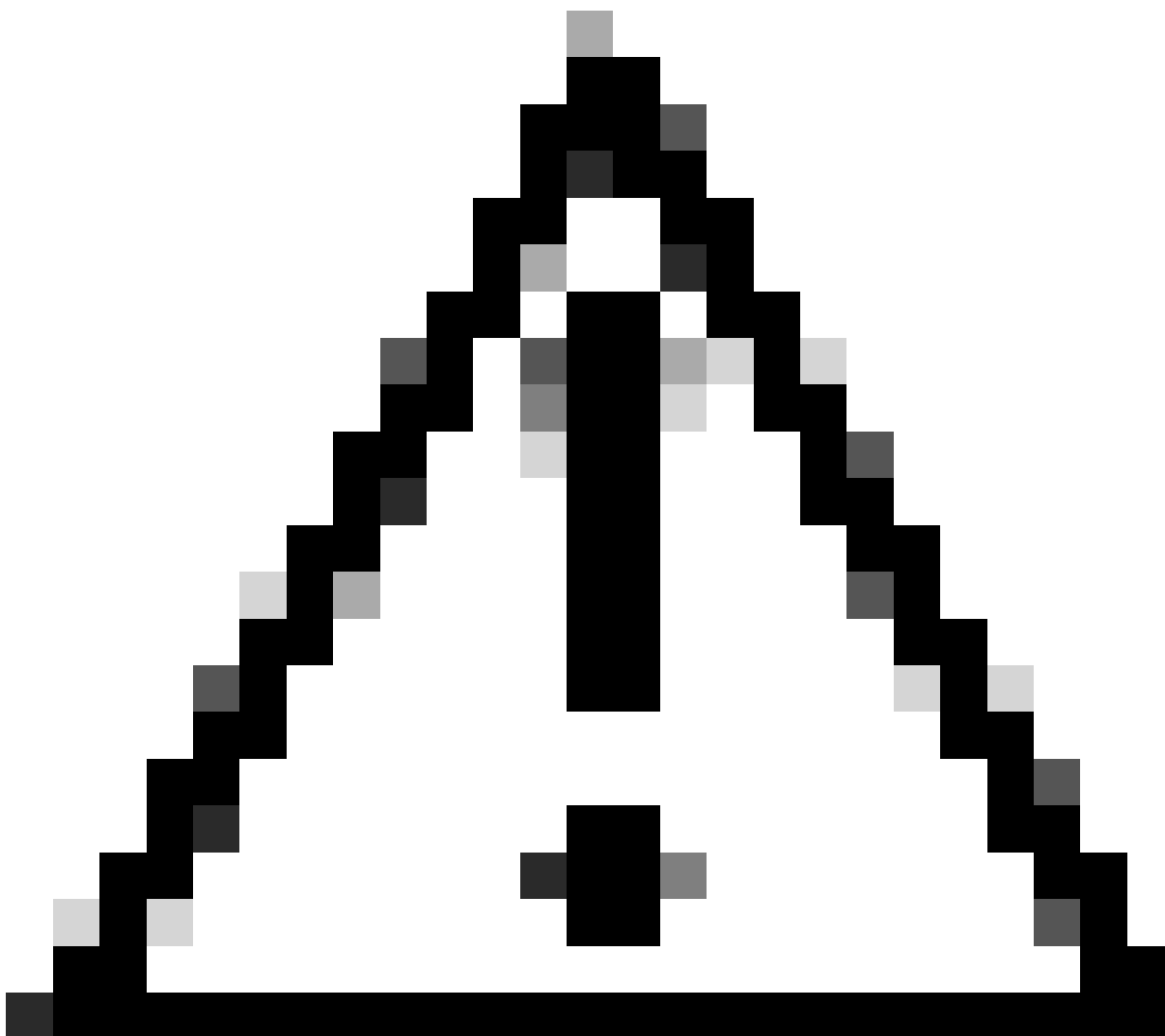
Sugerencia: dado que está bloqueando todas las categorías de URL, puede optimizar la política eliminando las categorías de URL personalizadas y utilizando solo las categorías de URL predefinidas. Esto reduce la carga de procesamiento en el SWA al evitar el paso adicional de hacer coincidir las URL con las categorías de URL personalizadas.

Paso 16. Registrar cambios.

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP Response Profile	Class Policy	Delete
1	Blocked Access Policy	Blocked user All Identifier users	Block: 2 Protocols Block: 108	Block: 15 Members: 24	(global policy)	Web Reputation: Enabled Secure Engines: Enabled Network: Enabled Malware: Enabled Sophos: Enabled	(global policy)		

Política de acceso a imágenes para bloquear todos los sitios



Precaución: en la implementación de proxy transparente, SWA no puede leer los agentes de usuario ni la URL completa para el tráfico HTTPS a menos que se descifre el tráfico. Como resultado, si configura el perfil de identificación mediante agentes de usuario o una categoría de URL personalizada con expresiones regulares, este tráfico no coincide con el perfil de identificación.

Bloqueo de sitios mediante expresiones regulares en una

implementación de proxy transparente

En la implementación de proxy transparente, si tiene pensado bloquear una categoría de URL personalizada que tenga la condición de expresiones regulares (por ejemplo, está bloqueando el acceso a algunos canales de YouTube), puede seguir estos pasos:

Paso 1. Cree una categoría de URL personalizada para el sitio principal. (En este ejemplo: YouTube.com).

Paso 2. Cree una política de descifrado, asigne esta categoría de URL personalizado y establezca la acción en Descifrar.

Paso 3. Cree una política de acceso, asigne la categoría de URL personalizado con las expresiones regulares (en este ejemplo, la categoría de URL personalizado para los canales de YouTube) y establezca la acción en Block (Bloquear).

Información Relacionada

- [Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - GD\(General Deployment\) - Clasificación de usuarios finales para la aplicación de políticas \[Cisco Secure Web Appliance\] - Cisco](#)
- [Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco](#)
- [Cómo eximir el tráfico de Office 365 de la autenticación y el descifrado en Cisco Web Security Appliance \(WSA\): Cisco](#)

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).