Bloquear la carga de tráfico en el dispositivo web seguro

Contenido

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

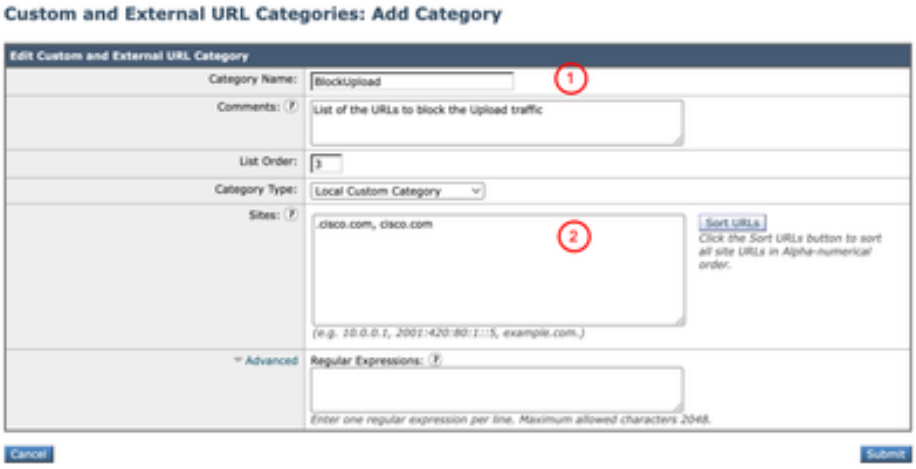
<table>
<tr>
<td>Paso 1. Crear una categoría de URL personalizada para el sitio web.</td>
<td>Paso 1.1. Desde la GUI vaya a Web Security Manager y elija Custom and External URL Categories.

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.

 
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</td>
</tr>
<tr>
<td>Paso 2. Descifrar el tráfico para la URL</td>
<td>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.</td>
</tr>
</table>

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

Paso 2.7. Haga clic en Enviar.

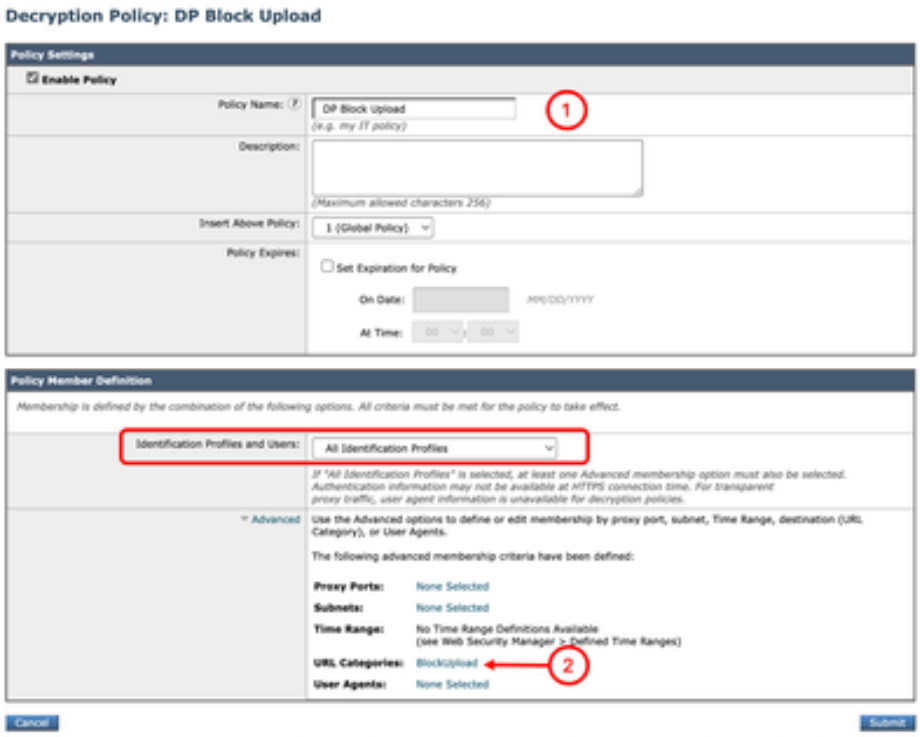


Imagen - Crear una política de descifrado

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

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.

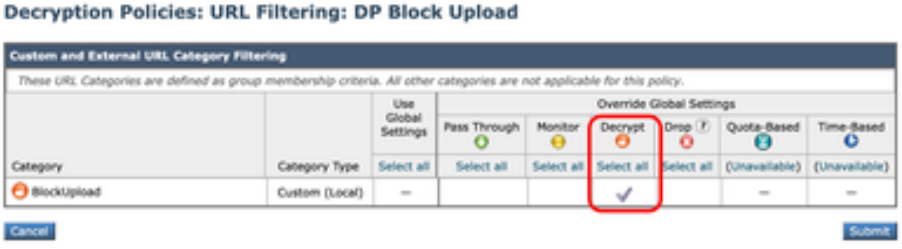


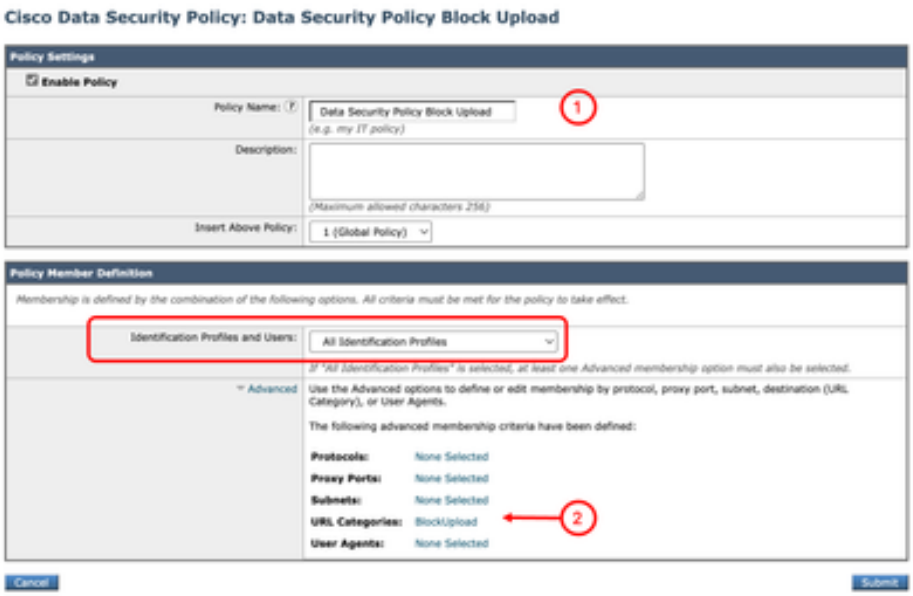
	Imagen - Establecer descifrado como acción
Paso 3. Bloqueo del tráfico de carga	Paso 3.1. Desde la GUI, navegue hasta Web Security Manager y elija Cisco Data Security. Paso 3.2. Haga clic en Agregar directiva. Paso 3.3. Introduzca Name para la nueva política. Paso 3.4. (Opcional) Seleccione el perfil 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.  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.

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.

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.

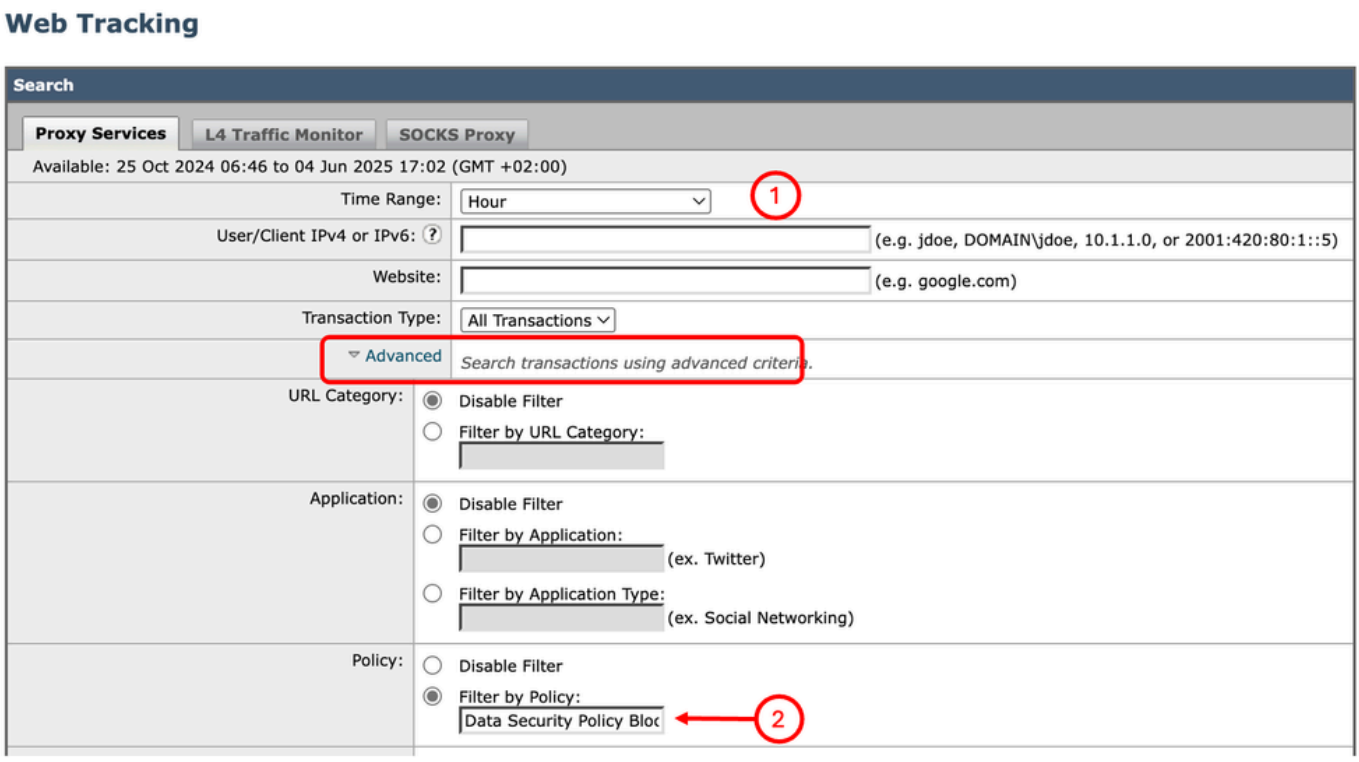


Imagen: filtrado de los informes de rastreo web

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).