Configurar categorías de URL personalizadas en el dispositivo web seguro

Contenido

Introducción

Este documento describe la estructura de las categorías de localizador uniforme de recursos (URL) personalizado en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo funciona el proxy.
- Administración de Secure Web Appliance (SWA).

Cisco recomienda que tenga:

- Dispositivo web seguro (SWA) físico o virtual instalado.
- Licencia activada o instalada.
- El asistente de configuración ha finalizado.

- 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.

Categorías de URL personalizadas

El motor de filtro de URL permite filtrar las transacciones en las políticas de acceso, descifrado y seguridad de datos. Al configurar las categorías de URL para los grupos de políticas, puede configurar acciones para las categorías de URL personalizadas, si hay alguna definida, y las categorías de URL predefinidas.

Puede crear categorías de URL de transmisión en directo personalizadas y externas que describan nombres de host y direcciones de protocolo de Internet (IP) específicos. Además, puede editar y eliminar categorías de URL.

Cuando incluye estas categorías de URL personalizadas en el mismo grupo de acceso, descifrado o directiva de seguridad de datos de Cisco y asigna diferentes acciones a cada categoría, la acción de la categoría de URL personalizada más alta incluida tiene prioridad.

Nota: si el sistema de nombres de dominio (DNS) resuelve varias IP en un sitio web y si una de esas IP es una lista de bloqueadas personalizada, el dispositivo de seguridad web bloquea el sitio web para todas las IP, independientemente de que no aparezcan en la lista de bloqueadas personalizadas.

Categorías de URL de transmisión en directo

Las categorías de fuentes activas externas se utilizan para obtener la lista de direcciones URL de un sitio específico, por ejemplo, para obtener las direcciones URL de Office 365 de Microsoft.

Si selecciona Categoría de fuente activa externa para el tipo de categoría al crear y editar categorías de URL personalizadas y externas, debe seleccionar el formato de fuente (formato de fuente de Cisco o formato de fuente de Office 365) y, a continuación, proporcionar una dirección

URL al servidor de archivos de fuente adecuado.
A continuación se muestra el formato esperado para cada archivo de fuente:

- Formato de fuente de Cisco: debe ser un archivo de valores separados por comas (.csv); es decir, un archivo de texto con la extensión .csv. Cada entrada del archivo .csv debe estar en una línea independiente, con formato de dirección/coma/dirección (por ejemplo: www.cisco.com,site o ad2.*\.com,regex). Los tipos de dirección válidos son site y regex.

Este es un extracto de un archivo .csv con formato de fuente de Cisco:

```
www.cisco.com,site
\.xyz,regex
ad2.*\.com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Formato de fuente de Office 365: se trata de un archivo XML ubicado en un servidor de Microsoft Office 365 o en un servidor local en el que guardó el archivo. Lo proporciona el servicio de Office 365 y no se puede modificar.

Las direcciones de red del archivo están encerradas por etiquetas XML, esta estructura: products > product > address list > address. En la implementación actual, un "tipo de lista de direcciones" puede ser IPv6, IPv4 o URL [que puede incluir dominios y patrones de expresiones regulares (regex)].

A continuación se muestra un fragmento de un archivo de fuente de Office 365:

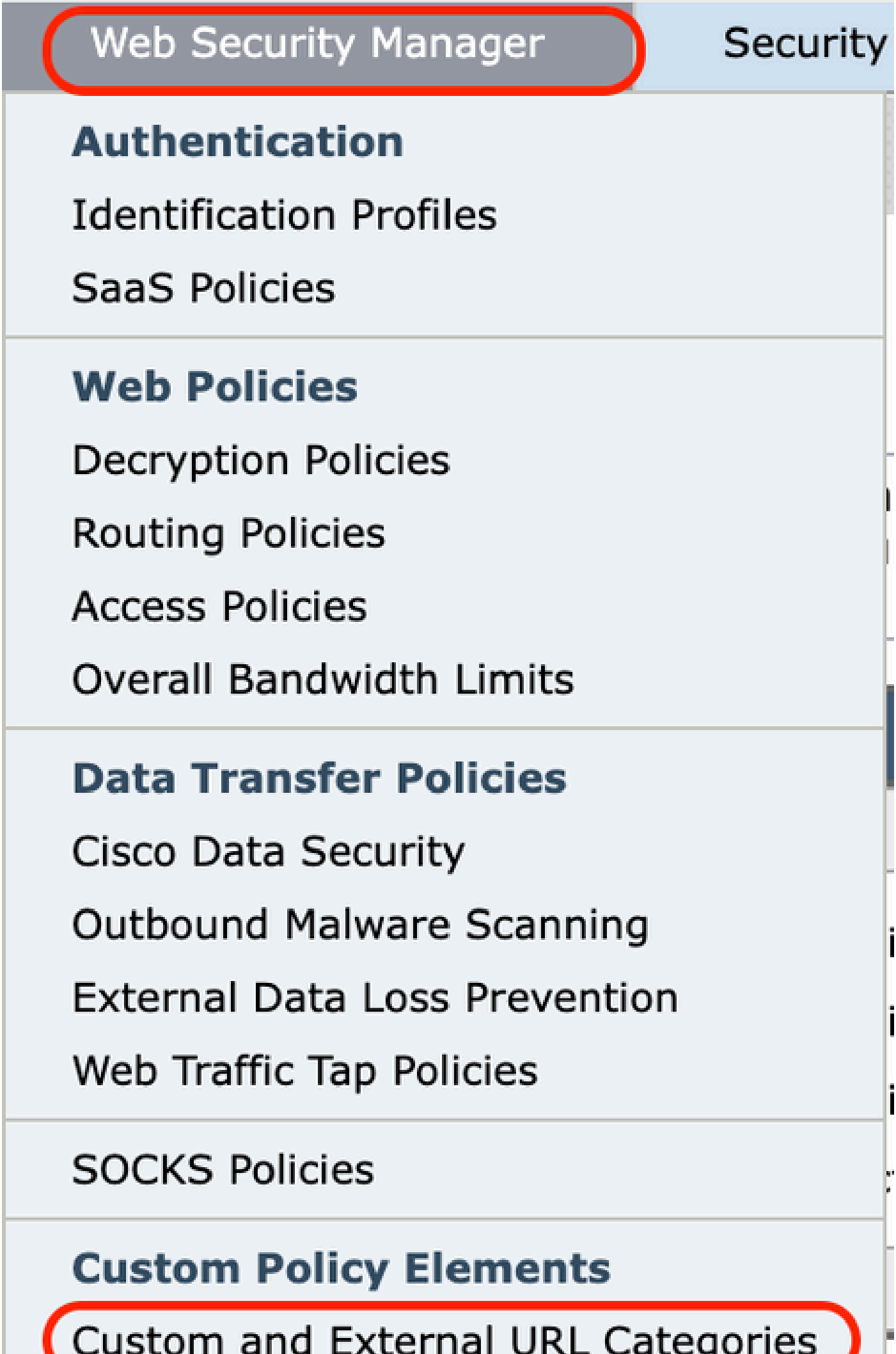
```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
```

```
</product>
</products>
```

Nota: No incluya http:// o https:// como parte de ninguna entrada de sitio en el archivo, ya que de lo contrario se producirá un error. En otras palabras, www.cisco.com se analiza correctamente, mientras que http://www.cisco.com produce un error

Pasos para crear categorías de URL personalizadas

Paso 1. Seleccione Administrador de seguridad web > Categorías de URL externas y personalizadas.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

: introduzca un identificador para esta categoría de URL. Este nombre aparece cuando se configura el filtro de URL para los grupos de políticas.

- Orden de la lista: especifique el orden de esta categoría en la lista de categorías de URL personalizadas. Introduzca "1" para la primera categoría de URL de la lista.
  El motor de filtro de URL evalúa una solicitud de cliente en función de las categorías de URL personalizadas en el orden especificado.

Nota: Cuando el motor de filtro de URL hace coincidir una categoría de URL con la URL de una solicitud de cliente, primero evalúa la URL con las categorías de URL personalizadas incluidas en el grupo de políticas. Si la URL de la solicitud no coincide con una categoría personalizada incluida, el motor de filtro de URL la compara con las categorías de URL predefinidas. Si la URL no coincide con ninguna de las categorías de URL predefinidas o personalizadas incluidas, la solicitud no se clasifica.

- Tipo de categoría: elija Categoría personalizada local o Categoría de transmisión en directo externa.
- Tabla de enrutamiento: elija Gestión o Datos. Esta opción sólo está disponible si está habilitado el "enrutamiento dividido"; es decir, no está disponible con categorías personalizadas locales.

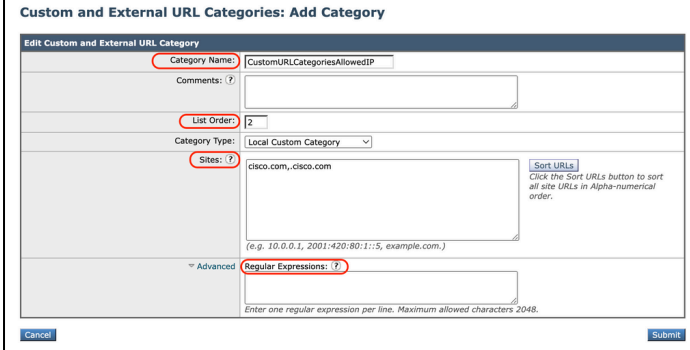
<table>
<tr>
<td> 

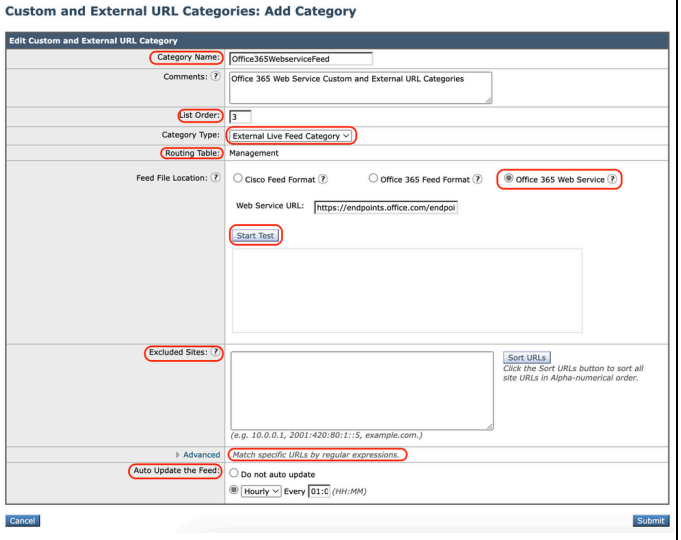
image: categoría de URL personalizado local</td>
<td> 

Imagen- Categoría de URL personalizada para configurar fuentes</td>
</tr>
<tr>
<td>Categoría personalizada local</td>
<td>Categoría de transmisión en directo externa</td>
</tr>
</table>

Definir expresiones regulares de uso

Secure Web Appliance utiliza una sintaxis de expresión regular que difiere ligeramente de la sintaxis de expresión regular utilizada por otras implementaciones del motor de coincidencia de patrones Velocity.

Además, el dispositivo no admite una barra diagonal inversa para escapar de una barra diagonal.

Si necesita utilizar una barra diagonal en una expresión regular, simplemente escriba la barra diagonal sin barra diagonal inversa.

Nota: Técnicamente, AsyncOS para Web utiliza el analizador de expresiones regulares Flex

Para probar sus expresiones regulares puede utilizar este enlace: flex lint - Regex Tester/Debugger

Precaución: las expresiones regulares que devuelven más de 63 caracteres producen un error de entrada no válida. Asegúrese de formar expresiones regulares que no tengan la posibilidad de devolver más de 63 caracteres

Precaución: las expresiones regulares que realizan coincidencias amplias de caracteres consumen recursos y pueden afectar al rendimiento del sistema. Por esta razón, las expresiones regulares se pueden aplicar con precaución.

Puede utilizar expresiones regulares en las siguientes ubicaciones:
· Categorías de URL personalizadas para las políticas de acceso. Al crear una categoría de URL personalizada para utilizarla con los grupos de directivas de acceso, puede utilizar expresiones regulares para especificar varios servidores web que coincidan con el modelo que especifique.
· Agentes de usuario personalizados para bloquear. Al editar las aplicaciones que se van a bloquear para un grupo de directivas de acceso, puede utilizar expresiones regulares para introducir agentes de usuario específicos que se van a bloquear.

Sugerencia: no puede establecer la omisión del proxy web para expresiones regulares.

A continuación se muestra la lista de clases de caracteres de una expresión regular flexible

Clases de caracteres	
.	cualquier carácter excepto línea nueva
\w \d \s	palabra, dígito, espacio en blanco
\W \D \S	sin palabra, dígito, espacio en blanco
[abc]	cualquiera de a, b o c
[^abc]	no a, b o c
[a-g]	carácter entre a & g
Anclas	
^abc$	inicio / fin de la cadena
\b	límite de palabra
Caracteres escapados	
\. * \\	caracteres especiales de escape
\t \n \r	tabulación, avance de línea, retorno de carro

\u00A9	unicode escaped ©
Grupos y Lookaround	
(abc)	grupo de captura
\1	referencia al grupo #1
(?:abc)	grupo sin captura
(?=abc)	visión positiva hacia el futuro
(?!abc)	mirada negativa hacia el futuro
Cuantificadores y alternancia	
a* a+ a?	0 o más, 1 o más, 0 o 1
a{5} a{2,}	exactamente cinco, dos o más
a{1,3}	entre uno y tres
a+? a{2,}?	coincidir lo menos posible
ab|cd	match ab o cd

⚠ Precaución: Ten cuidado con los puntos sin escape en los patrones largos, y especialmente en el medio de los patrones más largos y ten cuidado con este meta-carácter (Estrella *), especialmente en conjunción con el carácter de punto. Cualquier patrón contiene un punto sin escape que devuelve más de 63 caracteres después de deshabilitar el punto.
Siempre escape *(estrella) y . (punto) con \ (barra invertida) como * y \.
Si usamos .cisco.local en la expresión regular, el dominio Xcisco.local también coincide.
El carácter no escapado afecta al rendimiento y crea lentitud durante la navegación web.
Esto se debe a que el motor de coincidencia de patrones debe pasar por miles o millones de posibilidades hasta encontrar una coincidencia para la entrada correcta. También puede tener algunas preocupaciones de seguridad con respecto a las URL similares para las políticas permitidas

Puede utilizar la opción de la interfaz de línea de comandos (CLI) advanced proxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex, para habilitar o deshabilitar la conversión regex predeterminada a minúsculas para las coincidencias que no distinguen entre mayúsculas y minúsculas. Utilícelo si tiene problemas con la distinción entre mayúsculas y minúsculas.

Limitaciones y problemas de diseño

- No puede utilizar más de 30 archivos externos de transmisión en directo en estas definiciones de categoría de URL y cada archivo no debe contener más de 5000 entradas.
- Si aumenta el número de entradas de fuentes externas, se reduce el rendimiento.
- Es posible utilizar la misma dirección en varias categorías de URL personalizadas, pero el orden en el que se muestran las categorías es relevante.

Si incluye estas categorías en la misma política y define diferentes acciones para cada una, se aplica la acción definida para la categoría que aparece más arriba en la tabla de categorías de URL personalizadas.

- Cuando una solicitud de protocolo de transferencia de archivos (FTP) nativa se redirige de forma transparente al proxy FTP, no contiene información de nombre de host para el servidor FTP, sólo su dirección IP.

Debido a esto, algunas categorías de URL predefinidas y filtros de reputación web que sólo tienen información de nombre de host no coinciden con las solicitudes FTP nativas, incluso si las solicitudes están destinadas a esos servidores.

Si desea bloquear el acceso a estos sitios, debe crear categorías de URL personalizadas para que puedan utilizar sus direcciones IP.

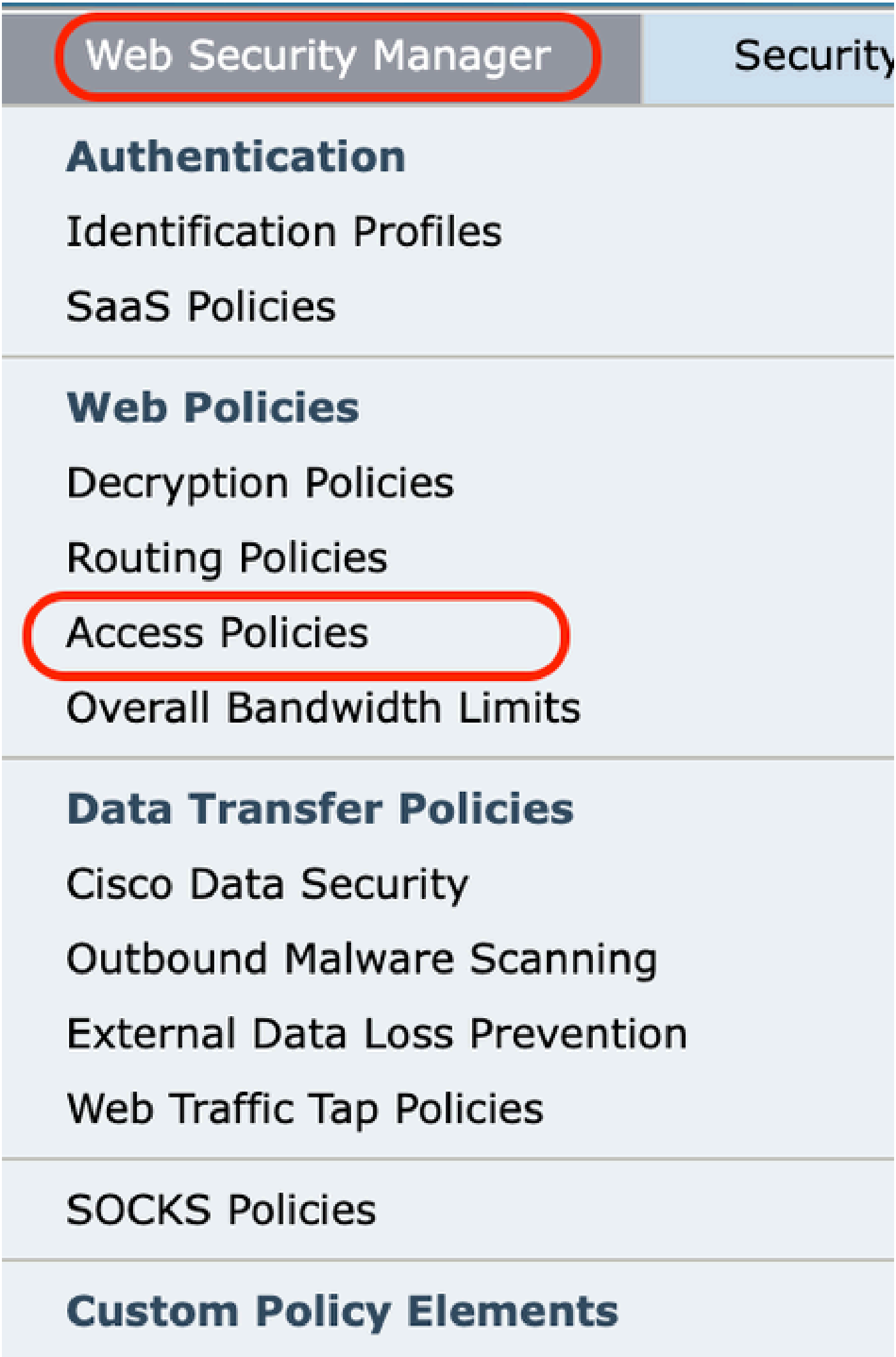
- Una URL no clasificada es una URL que no coincide con ninguna categoría de URL predefinida o categoría de URL personalizada incluida

Usar categorías de URL personalizadas en políticas

El motor de filtro de URL permite filtrar las transacciones en las políticas de acceso, descifrado y seguridad de datos. Al configurar las categorías de URL para los grupos de políticas, puede configurar acciones para las categorías de URL personalizadas, si hay alguna definida, y las categorías de URL predefinidas.

Pasos Para Configurar Los Filtros De URL Para La Política De Acceso

Paso 1. Elija Administrador de seguridad web > Políticas de acceso.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

Haga clic en el enlace de la tabla de directivas en la columna Filtro de URL del grupo de directivas que desea editar.

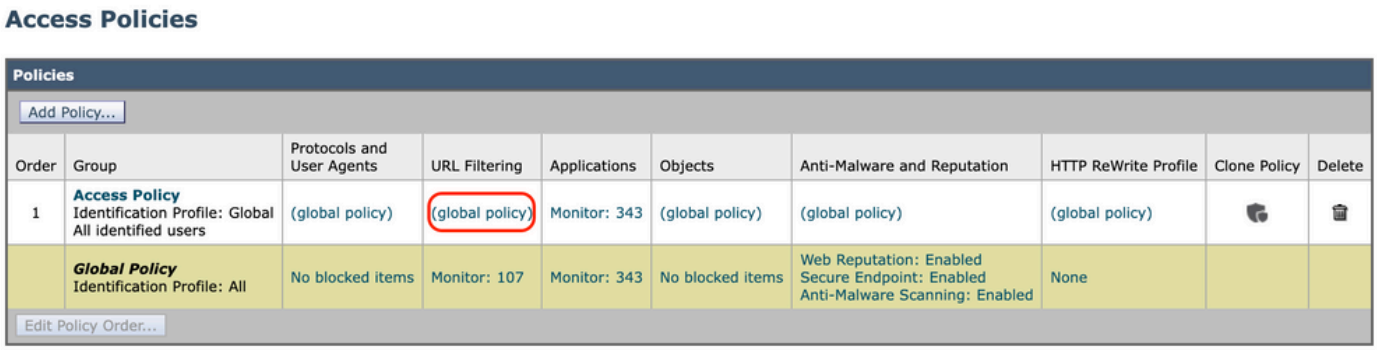
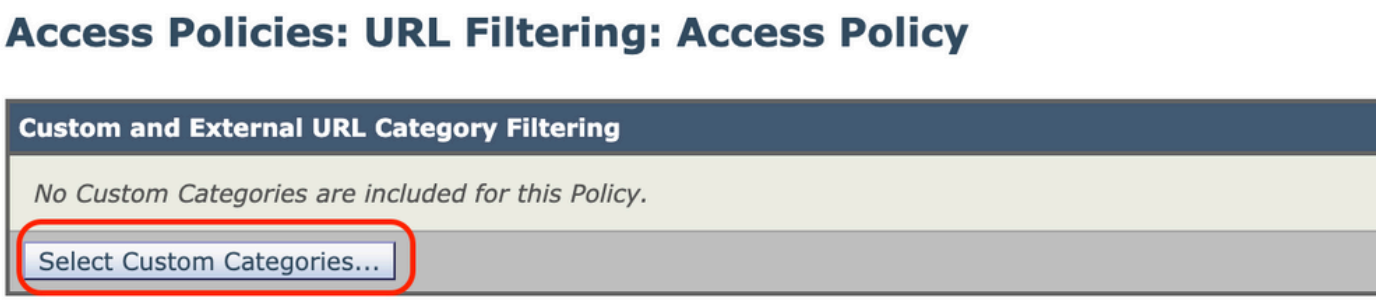


Imagen- Agregar categoría personalizada a la política de acceso

Paso 3. (Opcional) En la sección Filtrado de Categoría de URL Personalizado, puede agregar categorías de URL personalizadas sobre las que realizar acciones en esta política:

a) Haga clic en Seleccionar categorías personalizadas.



Categoría de URL personalizada de selección de imagen

b) Elija las categorías de URL personalizadas que desea incluir en esta política y haga clic en Apply.

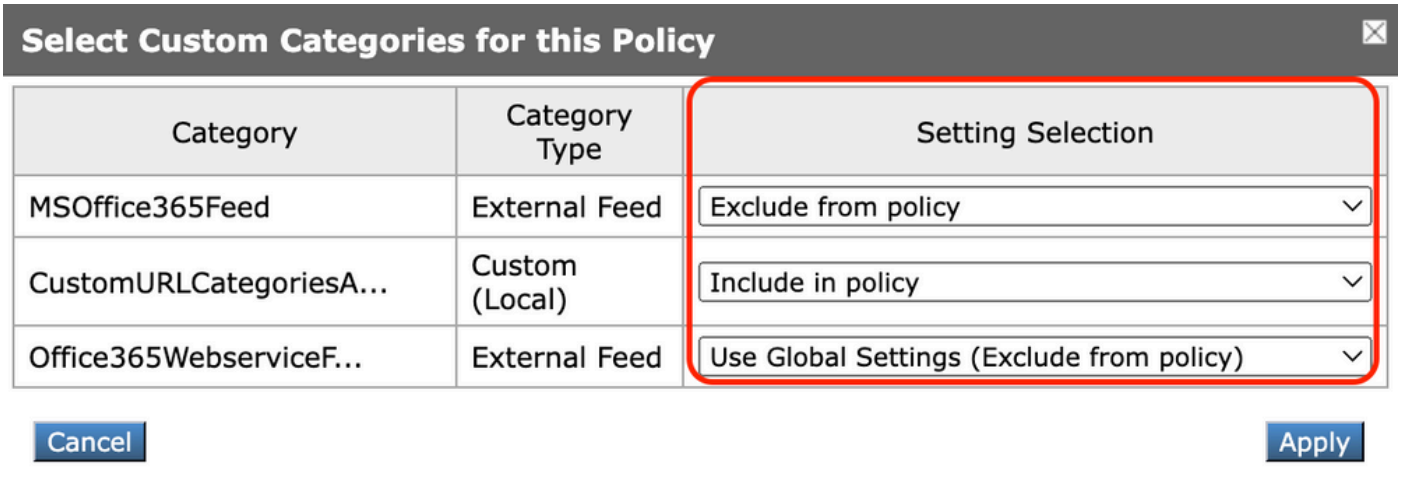


Imagen: seleccione las categorías personalizadas que desea incluir en la política

Elija las categorías de URL personalizadas con las que el motor de filtro de URL debe comparar la solicitud del cliente.

El motor de filtro de URL compara las solicitudes del cliente con las categorías de URL personalizadas incluidas e ignora las categorías de URL personalizadas excluidas.

El motor de filtro de URL compara la URL de una solicitud de cliente con las categorías de URL personalizadas incluidas antes que las categorías de URL predefinidas.

Las categorías de URL personalizadas incluidas en la política aparecen en la sección Filtrado de categoría de URL personalizado.

Paso 4. En la sección Filtrado personalizado de categoría de URL, elija una acción para cada categoría de URL personalizada incluida.

Imagen- Elegir acción para categoría personalizada

Acción	Descripción
Usar configuración global	Utiliza la acción para esta categoría en el Grupo de políticas globales. Esta es la acción predeterminada para los grupos de políticas definidas por el usuario. Sólo se aplica a grupos de directivas definidos por el usuario.
Bloqueo	El proxy web deniega las transacciones que coinciden con esta configuración.
Redireccionar	Redirige el tráfico destinado originalmente a una dirección URL de esta categoría a la ubicación que especifique. Al elegir esta acción, aparece el campo Redirigir a. Introduzca una URL a la que redirigir todo el tráfico.
Permiso	Permite siempre las solicitudes de los clientes para los sitios Web de esta categoría. Las solicitudes permitidas omiten el resto de filtros y escaneos de Malware. Utilice esta configuración sólo para sitios Web de confianza. Puede utilizar esta configuración para sitios internos.
Monitor	El proxy de Web no permite ni bloquea la solicitud. En su lugar, continúa evaluando la solicitud del cliente frente a otras configuraciones de control de grupo de políticas, como el filtro de reputación web.

Acción	Descripción
Avisar	El proxy web bloquea inicialmente la solicitud y muestra una página de advertencia, pero permite al usuario continuar haciendo clic en un enlace de hipertexto de la página de advertencia.
Basado en cuotas	Cuando un usuario individual se aproxima a las cuotas de volumen o de tiempo especificadas, se muestra una advertencia. Cuando se alcanza una cuota, se muestra una página de bloqueo. .
Basado en tiempo	El proxy de Web bloquea o supervisa la solicitud durante los intervalos de tiempo especificados.

Paso 5. En la sección Filtro de categoría de URL predefinido, elija una de estas acciones para cada categoría:

- Usar configuración global
- Monitor
- Avisar
- Bloqueo
- Basado en tiempo
- Basado en cuotas

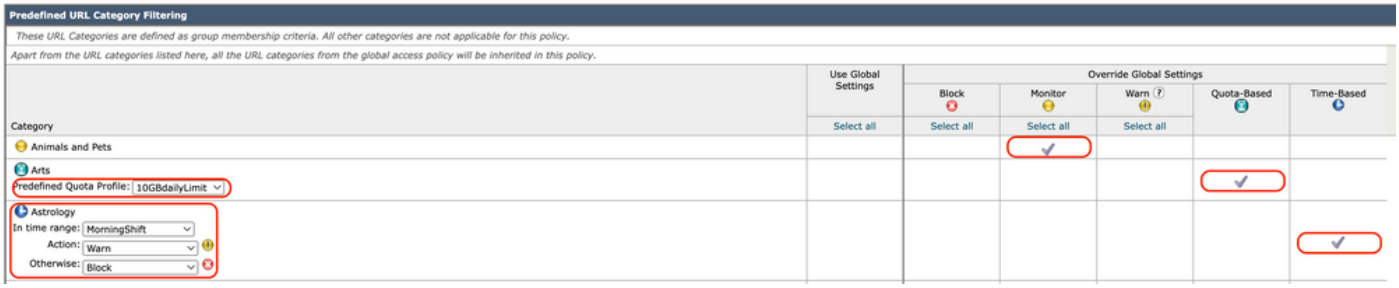


Imagen- Seleccionar acción para categoría predefinida

Paso 6. En la sección Uncategorized URLs, elija la acción a tomar para las solicitudes del cliente a los sitios web que no caen en una categoría de URL predefinida o personalizada. Esta configuración también determina la acción predeterminada para las categorías nuevas y combinadas resultantes de las actualizaciones del conjunto de categorías de URL.

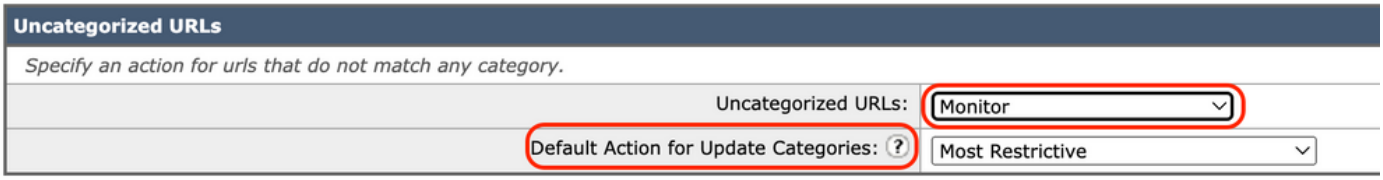
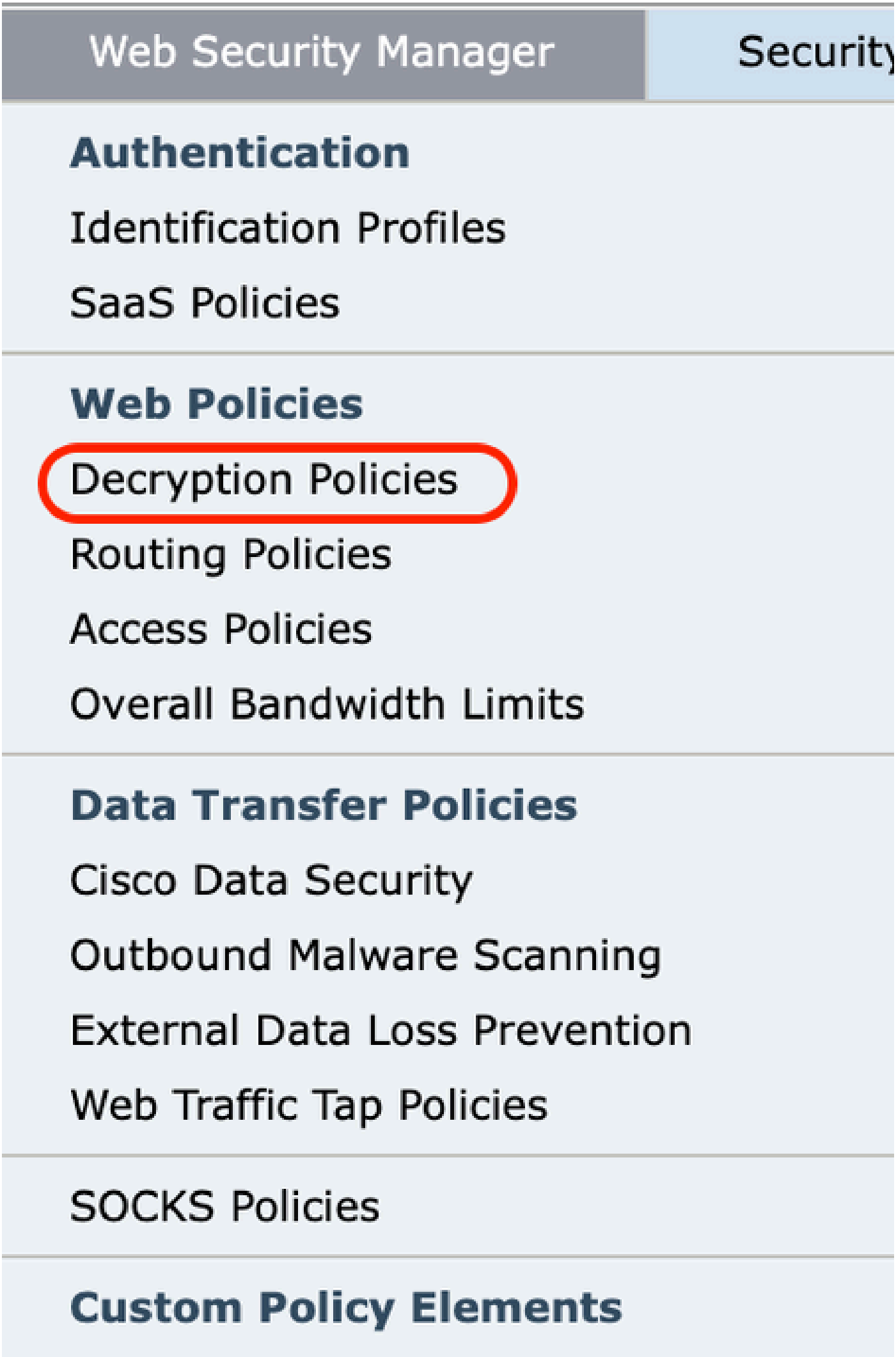


Imagen: elija la acción para la URL no clasificada

Paso 7. Enviar y registrar cambios.

Pasos Para Configurar Los Filtros De URL Para La Política De Descifrado

Paso 1. Elija Administrador de seguridad web > Políticas de descifrado.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements

Haga clic en el enlace de la tabla de directivas de la columna Filtrado de URL del grupo de directivas que desea editar.

Imagen - Elegir filtro de URL

Paso 3. (Opcional) En la sección Custom URL Category Filtering (Filtrado de categorías de URL personalizadas), puede agregar categorías de URL personalizadas sobre las que realizar acciones en esta política:

a. Haga clic en Seleccionar categorías personalizadas.

Imagen - Elegir categorías personalizadas

b. Elija las categorías de URL personalizadas que desea incluir en esta política y haga clic en Aplicar.

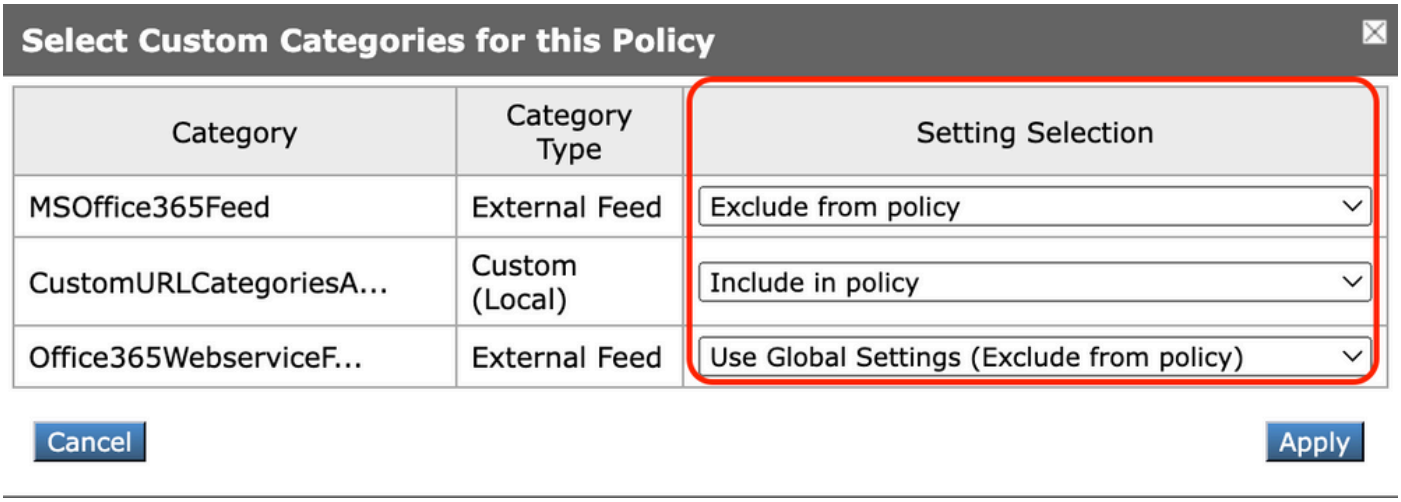


Imagen: seleccione las categorías personalizadas que desea incluir en la política

Elija las categorías de URL personalizadas con las que el motor de filtro de URL debe comparar la solicitud del cliente.

El motor de filtro de URL compara las solicitudes del cliente con las categorías de URL personalizadas incluidas e ignora las categorías de URL personalizadas excluidas.

El motor de filtro de URL compara la URL de una solicitud de cliente con las categorías de URL personalizadas incluidas antes que las categorías de URL predefinidas.

Las categorías de URL personalizadas incluidas en la política aparecen en la sección Filtrado de categoría de URL personalizado.

Paso 4. Elija una acción para cada categoría de URL personalizada y predefinida.

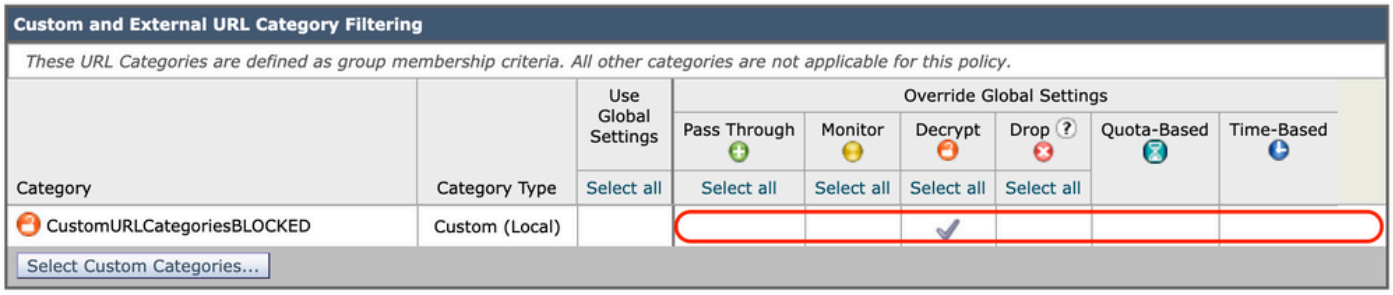


Imagen - Elegir Acción Para La Política De Descifrado

Acción	Descripción
Utilizar configuración global	Utiliza la acción para esta categoría en el grupo de directivas de descifrado global. Esta es la acción predeterminada para los grupos de políticas definidas por el usuario. Sólo se aplica a grupos de directivas definidos por el usuario. Cuando una categoría de URL personalizada se excluye en la política de descifrado global, la acción predeterminada para las categorías de URL personalizadas incluidas en las políticas de descifrado definidas por el usuario es Supervisar en lugar de Utilizar configuración global. No puede elegir Usar configuración global cuando una categoría de URL personalizada está excluida en la directiva de descifrado global.
Paso a través	Pasa a través de la conexión entre el cliente y el servidor sin inspeccionar el contenido del tráfico.
Monitor	El proxy de Web no permite ni bloquea la solicitud. En su lugar, continúa evaluando la solicitud del cliente frente a otras configuraciones de control de grupo de políticas, como el filtro de reputación web.
Descifrar	Permite la conexión, pero inspecciona el contenido del tráfico. El dispositivo

Acción	Descripción
	descifra el tráfico y aplica las directivas de acceso al tráfico descifrado como si se tratara de una conexión de protocolo de transferencia de hipertexto (HTTP) de texto sin formato. Cuando se descifran las conexiones y se aplican las políticas de acceso, puede analizar el tráfico en busca de malware.
Abandonar	Descarta la conexión y no pasa la solicitud de conexión al servidor. El dispositivo no notifica al usuario que ha interrumpido la conexión.

Paso 5. En la sección Uncategorized URLs, elija la acción a tomar para las solicitudes del cliente a los sitios web que no caen en una categoría de URL predefinida o personalizada.

Esta configuración también determina la acción predeterminada para las categorías nuevas y combinadas resultantes de las actualizaciones del conjunto de categorías de URL.

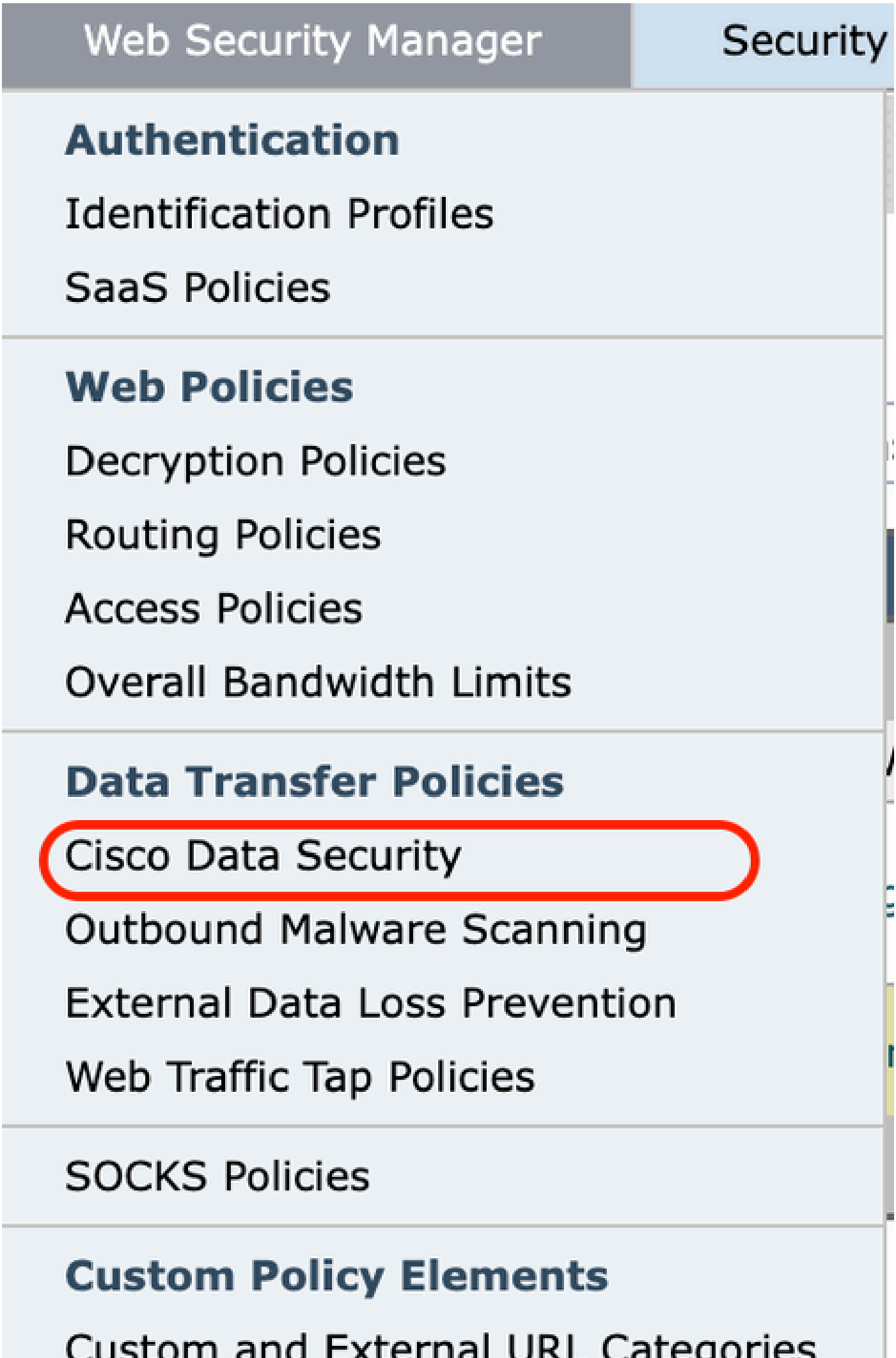
Imagen - Política de descifrado sin categorizar

Paso 6. Enviar y registrar cambios.

⚠ Precaución: si desea bloquear una categoría de URL concreta para solicitudes de protocolo de transferencia de hipertexto seguro (HTTPS), descifre esa categoría de URL en el grupo de políticas de descifrado y, a continuación, bloquee la misma categoría de URL en el grupo de políticas de acceso.

Pasos Para Configurar Filtros De URL Para Grupos De Políticas De Seguridad De Datos

Paso 1. Elija Web Security Manager > Cisco Data Security.


Web Security Manager
Security
Authentication
Identification Profiles
SaaS Policies
Web Policies
Decryption Policies
Routing Policies
Access Policies
Overall Bandwidth Limits
Data Transfer Policies
Cisco Data Security
Outbound Malware Scanning
External Data Loss Prevention
Web Traffic Tap Policies
SOCKS Policies
Custom Policy Elements
Custom and External URL Categories

Haga clic en el enlace de la tabla de directivas de la columna Filtrado de URL del grupo de directivas que desea editar.

Imagen - Seguridad de datos elija el filtro de URL

Paso 3. (Opcional) En la sección Custom URL Category Filtering (Filtrado de categorías de URL personalizadas), puede agregar categorías de URL personalizadas sobre las que realizar acciones en esta política:

a. Haga clic en Seleccionar categorías personalizadas.

Imagen - Seleccionar campo personalizado

b. Elija las categorías de URL personalizadas que desea incluir en esta política y haga clic en Aplicar.

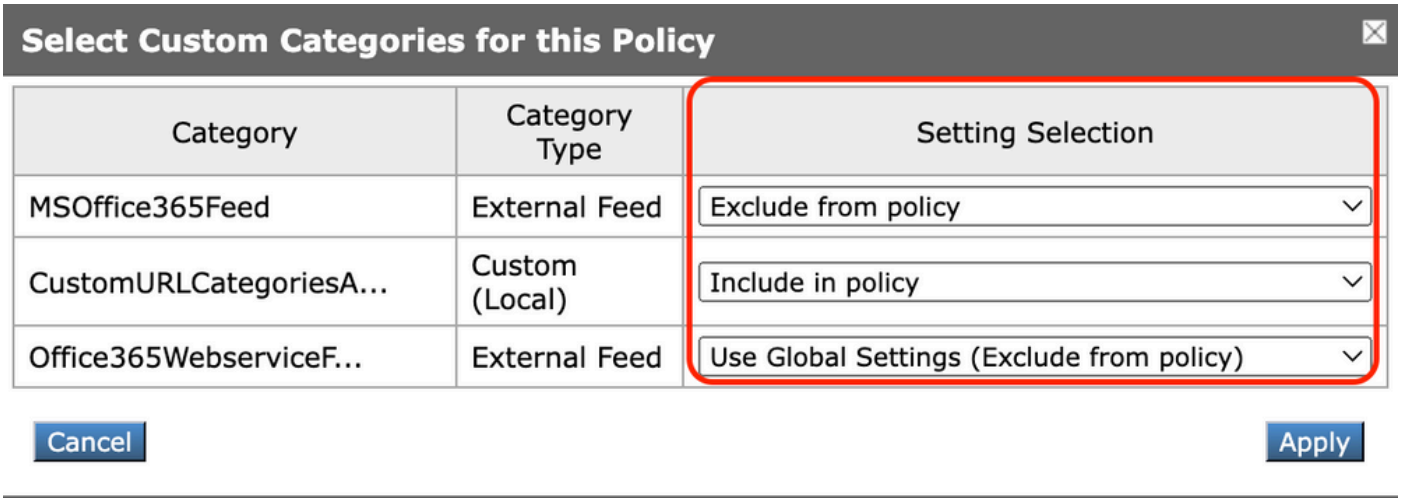


Imagen: seleccione las categorías personalizadas que desea incluir en la política

Elija las categorías de URL personalizadas con las que el motor de filtro de URL debe comparar la solicitud del cliente.

El motor de filtro de URL compara las solicitudes del cliente con las categorías de URL

personalizadas incluidas e ignora las categorías de URL personalizadas excluidas.

El motor de filtro de URL compara la URL de una solicitud de cliente con las categorías de URL personalizadas incluidas antes que las categorías de URL predefinidas.

Las categorías de URL personalizadas incluidas en la política aparecen en la sección Filtrado de categoría de URL personalizado.

Paso 4. En la sección Filtrado personalizado de categorías de URL, elija una acción para cada categoría de URL personalizada.

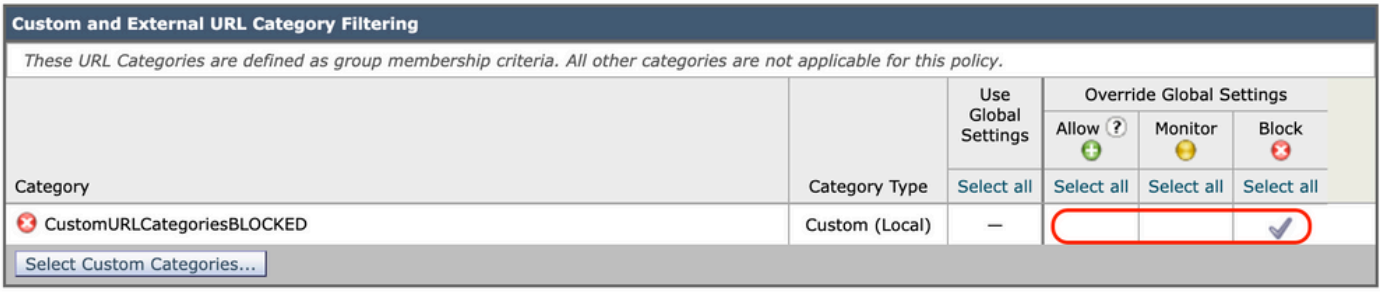


Imagen - Seguridad de datos Elegir acción

Acción	Descripción
Utilizar configuración global	Utiliza la acción para esta categoría en el Grupo de políticas globales. Esta es la acción predeterminada para los grupos de políticas definidas por el usuario. Sólo se aplica a grupos de directivas definidos por el usuario. Cuando una categoría de URL personalizada se excluye en la política de seguridad de datos de Cisco global, la acción predeterminada para las categorías de URL personalizadas incluidas en las políticas de seguridad de datos de Cisco definidas por el usuario es Supervisar en lugar de Usar configuración global. No puede elegir Usar configuración global cuando una categoría de URL personalizada está excluida en la política de seguridad de datos de Cisco global.
Permiso	Permite siempre las solicitudes de carga de sitios web de esta categoría. Se aplica sólo a categorías de URL personalizadas. Las solicitudes permitidas omiten todas las demás exploraciones de seguridad de datos y la solicitud se evalúa con las directivas de acceso. Utilice esta configuración sólo para sitios Web de confianza. Puede utilizar esta configuración para sitios internos.

Acción	Descripción
Monitor	El proxy de Web no permite ni bloquea la solicitud. En su lugar, continúa evaluando la solicitud de carga frente a otras configuraciones de control de grupo de políticas, como el filtro de reputación web.
Bloqueo	El proxy web deniega las transacciones que coinciden con esta configuración.

Paso 5. En la sección Filtrado Predefinido de Categorías de URL, elija una de estas acciones para cada categoría:

- Usar configuración global
- Monitor
- Bloqueo

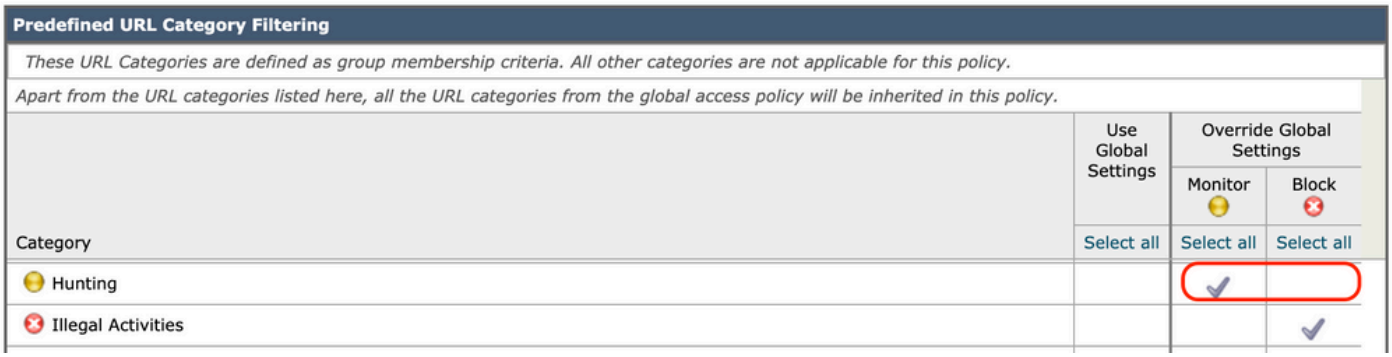


Imagen: acción de selección de URL predefinida de seguridad de datos

Paso 6. En la sección Uncategorized URLs, elija la acción a tomar para cargar solicitudes a sitios web que no caen en una categoría de URL predefinida o personalizada.

Esta configuración también determina la acción predeterminada para las categorías nuevas y combinadas resultantes de las actualizaciones del conjunto de categorías de URL.

Imagen - Seguridad De Datos Sin Categorizar

Paso 7. Enviar y registrar cambios.

⚠ Precaución: si no deshabilita la limitación de tamaño máximo de archivo, Web Security Appliance continúa validando el tamaño máximo de archivo cuando se seleccionan las opciones Permitir o Supervisar en el filtrado de URL.

Pasos para configurar el control de las solicitudes de carga con categorías de URL personalizadas

Cada solicitud de carga se asigna a un grupo de políticas de "escaneo de malware saliente" y hereda la configuración de control de ese grupo de políticas.

Una vez que el proxy web recibe los encabezados de solicitud de carga, dispone de la información necesaria para decidir si debe analizar el cuerpo de la solicitud.

El motor DVS analiza la solicitud y devuelve un veredicto al proxy web. La página de bloqueo aparece para el usuario final, si procede.

<table>
<tr><td>Paso 1</td><td>Elija Administrador de seguridad web > Escaneo de malware saliente.</td></tr>
<tr><td>Paso 2</td><td>En la columna Destinos, haga clic en el enlace del grupo de políticas que desea configurar.</td></tr>
<tr><td>Paso 3</td><td>En la sección Edit Destination Settings, seleccione "Define Destinations Scanning Custom Settings" en el menú desplegable.</td></tr>
<tr><td>Paso 4</td><td>En la sección Destinos a analizar, seleccione uno de estos:
<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>No buscar ninguna carga</td><td>El motor DVS no explora las solicitudes de carga. Todas las solicitudes de carga se evalúan según las políticas de acceso</td></tr>
<tr><td>Buscar todas las cargas</td><td>El motor DVS escanea todas las solicitudes de carga. La solicitud de carga se bloquea o evalúa según las políticas de acceso, según el veredicto del análisis del motor DVS</td></tr>
<tr><td>Buscar cargas en las categorías de URL personalizadas especificadas</td><td>El motor DVS analiza las solicitudes de carga que pertenecen a categorías de URL personalizadas específicas. La solicitud de carga se bloquea o evalúa en función de las políticas de acceso, según el veredicto del análisis del motor DVS.

Haga clic en Editar lista de categorías personalizadas para seleccionar las categorías de URL que desea</td></tr>
</table>
</td></tr>
</table>

	Opción	Descripción
		analizar
Paso 5	Envíe los cambios.	
Paso 6	En la columna Anti-Malware Filtering, haga clic en el enlace del grupo de políticas.	
Paso 7	En la sección Anti-Malware Settings, seleccione Define Anti-Malware Custom Settings.	
Paso 8	En la sección Configuración Anti-Malware DVS de Cisco, seleccione qué motores de análisis anti-malware activar para este grupo de políticas.	
Paso 9	En la sección Categorías de malware, elija si desea supervisar o bloquear las distintas categorías de malware. Las categorías enumeradas en esta sección dependen de los motores de exploración que active.	
Paso 10	Enviar y registrar cambios.	

Pasos para configurar el control de las solicitudes de carga en políticas DLP externas

Una vez que el proxy web recibe los encabezados de la solicitud de carga, dispone de la información necesaria para decidir si la solicitud puede dirigirse al sistema DLP externo para su análisis.

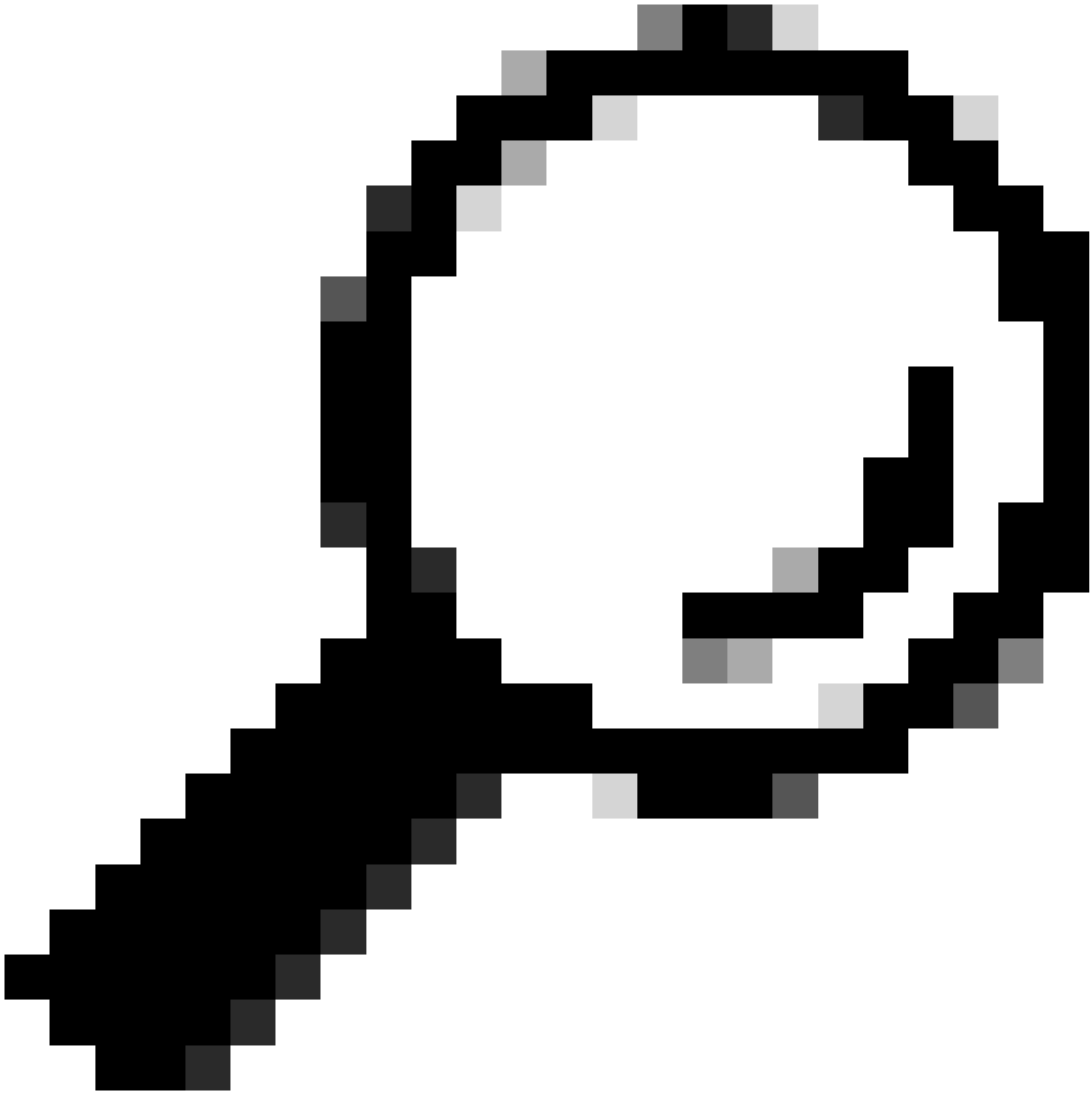
El sistema DLP analiza la solicitud y devuelve un veredicto al proxy web, ya sea para bloquearla o supervisarla (evalúe la solicitud según las políticas de acceso).

Paso 1	Elija Web Security Manager > External Data Loss Prevention.
Paso 2	Haga clic en el enlace de la columna Destinos del grupo de políticas que desea configurar.

Paso 3	En la sección Edit Destination Settings, elija "Define Destinations Scanning Custom Settings."
Paso 4	En la sección Destino para escanear, elija una de estas opciones: • No buscar ninguna carga. No se envían solicitudes de carga a los sistemas de prevención de pérdida de datos (DLP) configurados para su análisis. Todas las solicitudes de carga se evalúan según las políticas de acceso. • Analiza todas las cargas. Todas las solicitudes de carga se envían a los sistemas DLP configurados para su análisis. La solicitud de carga se bloquea o evalúa según las políticas de acceso, según el veredicto de los análisis del sistema DLP. • Buscar cargas excepto para las categorías de URL externas y personalizadas especificadas. Las solicitudes de carga que se incluyen en categorías de URL personalizadas específicas se excluyen de las políticas de análisis de DLP. Haga clic en Editar lista de categorías personalizadas para seleccionar las categorías de URL que desea analizar.
Paso 5	Enviar y registrar cambios.

URL de desvío y paso a través

Puede configurar Secure Web Appliance en la implementación de proxy transparente para omitir las solicitudes HTTP o HTTPS de clientes concretos o de destinos concretos.



Sugerencia: puede utilizar el paso a través para aplicaciones que requieran que el tráfico pase a través del dispositivo, sin necesidad de realizar ninguna modificación o comprobaciones de certificados de los servidores de destino

⚠ Precaución: la función Domain Map funciona en el modo transparente de HTTPS. Esta función no funciona en el modo explícito ni para el tráfico HTTP.

- La categoría personalizada local debe configurarse para permitir que el tráfico utilice esta función.
- Cuando esta función está habilitada, modifica o asigna el nombre del servidor según el nombre del servidor configurado en el mapa de dominio, incluso si la información de indicación de nombre de servidor (SNI) está disponible.

- Esta función no bloquea el tráfico basado en el nombre de dominio si dicho tráfico coincide con el mapa de dominio y corresponde a la categoría personalizada, se configuran la política de descifrado y la acción de paso a través.
- La autenticación no funciona con esta función de transferencia. La autenticación requiere descifrado, pero el tráfico no se descifra en este caso.
- no se supervisa el tráfico. Debe configurar el tráfico UDP para que no llegue a Web Security Appliance , sino que debe pasar directamente a través del firewall a Internet para aplicaciones como WhatsApp, Telegram, etc.
- WhatsApp, Telegram y Skype funcionan en modo Transparente. Sin embargo, algunas aplicaciones como WhatsApp no funcionan en modo explícito debido a las restricciones en la aplicación.

Asegúrese de que tiene una política de identificación definida para los dispositivos que requieren tráfico de paso a servidores específicos. En concreto, debe:

- Elija Exento de autenticación/identificación.
- Especifique las direcciones a las que debe aplicarse este perfil de identificación. Puede utilizar direcciones IP, bloques de enrutamiento entre dominios sin clase (CIDR) y subredes.

Paso 1	Habilitar Proxy HTTPS.
Paso 2	Elija Web Security Manager > Domain Map. a. Elija Agregar dominio. b. Introduzca el nombre de dominio o el servidor de destino. c. Elija el orden de la prioridad si hay algunos dominios especificados. d. Introduzca las direcciones IP. e. Haga clic en Submit (Enviar).
Paso 3	Elija Administrador de seguridad web > Categorías de URL externas y personalizadas. a. Elija Agregar categoría. b. Proporcione esta información.

<table>
<tr><td></td><td>
<table>
<tr><th>Configuración</th><th>Descripción</th></tr>
<tr><td>Nombre de categoría</td><td>Introduzca un identificador para esta categoría de URL. Este nombre aparece cuando se configura el filtro de URL para los grupos de políticas.</td></tr>
<tr><td>Orden de lista</td><td>Especifique el orden de esta categoría en la lista de categorías de URL personalizadas. Introduzca "1" para la primera categoría de URL de la lista.

El motor de filtro de URL evalúa una solicitud de cliente en función de las categorías de URL personalizadas en el orden especificado.</td></tr>
<tr><td>Tipo de categoría</td><td>Elija Categoría personalizada local.</td></tr>
<tr><td>Avanzado</td><td>Puede introducir expresiones regulares en esta sección para especificar conjuntos adicionales de direcciones.

Puede utilizar expresiones regulares para especificar varias direcciones que coincidan con los patrones que especifique.</td></tr>
</table>
c. Envíe y confirme los cambios.
</td></tr>
<tr><td>Paso 4</td><td>Elija Administrador de seguridad web > Políticas de descifrado.

a. Cree una nueva política de descifrado.

b. Elija el perfil de identificación que ha creado para omitir el tráfico HTTPS para aplicaciones específicas.

c. En el panel Avanzadas, haga clic en el enlace de las categorías de URL.

d. En la columna Add, haga clic para agregar la categoría de URL personalizada creada en el paso 3.

e. Elija Finalizado.

f. En la página Políticas de descifrado, haga clic en el enlace Filtrado de URL.

g. Elija Pass Through.</td></tr>
</table>

	h. Envíe y confirme los cambios. (Opcional) Puede utilizar el especificador de formato %(para ver la información del registro de acceso.

Configuración De La Omisión De Proxy Web Para Solicitudes Web

Una vez agregadas las categorías de URL personalizadas a la lista de omisión de proxy, se omiten todas las direcciones IP y los nombres de dominio de las categorías de URL personalizadas tanto para el origen como para el destino.

Paso 1	Elija Web Security Manager > Bypass Settings.
Paso 2	Haga clic en Editar configuración de omisión.
Paso 3	Introduzca las direcciones para las que desea omitir el proxy web. Nota: cuando configura /0 como máscara de subred para cualquier IP de la lista de desvío, el dispositivo omite todo el tráfico web. En este caso, el dispositivo interpreta la configuración como 0.0.0.0/0.
Paso 4	Elija las categorías de URL personalizadas que desea agregar a la lista de omisión de proxy.
Paso 5	Envíe y confirme los cambios.

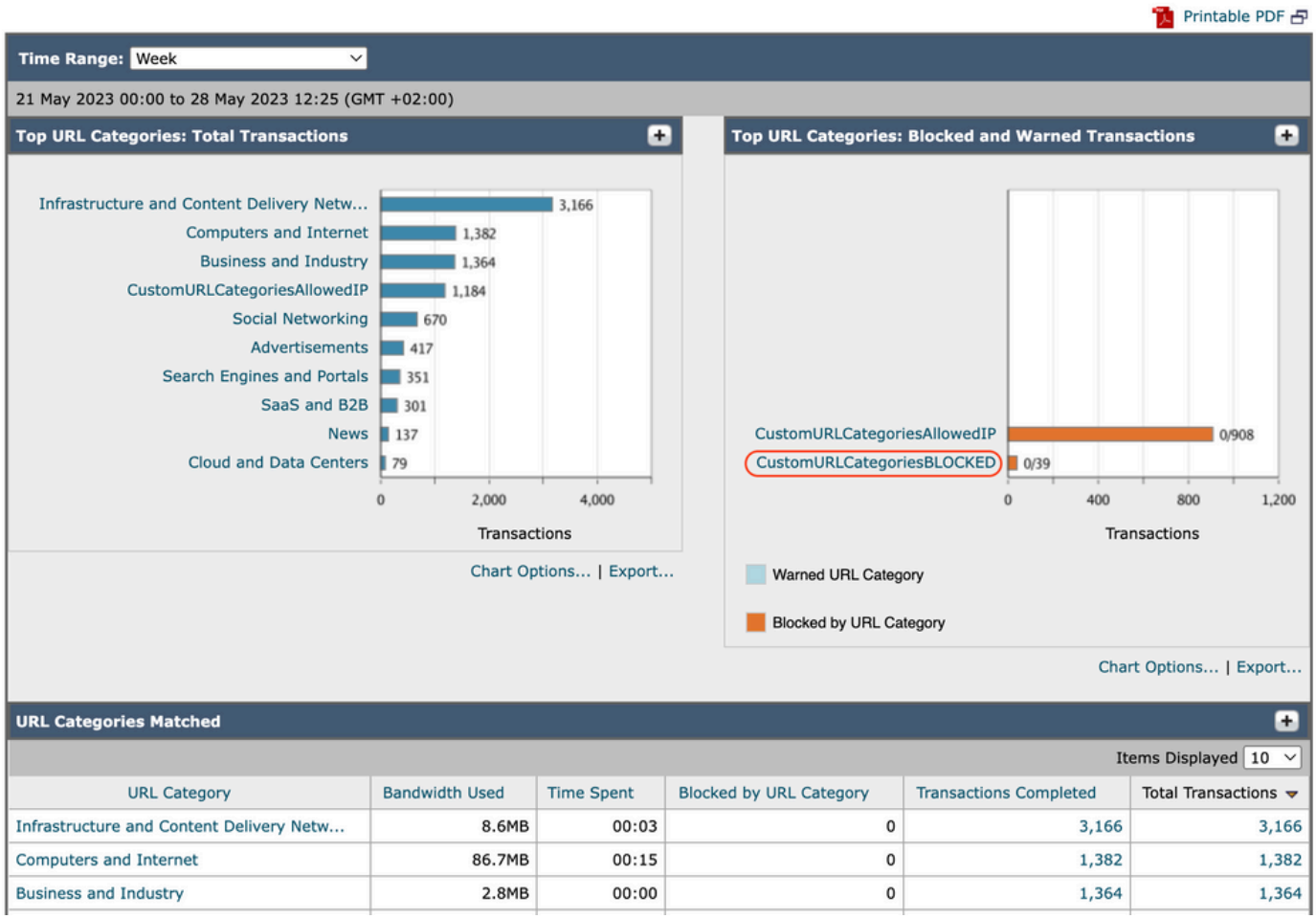
Precaución: no puede establecer la omisión del proxy web para expresiones regulares.

Informes

En la página "Informes" > Categorías de URL" se proporciona una visualización colectiva de las estadísticas de URL que incluye información sobre las principales categorías de URL coincidentes y las principales categorías de URL bloqueadas.

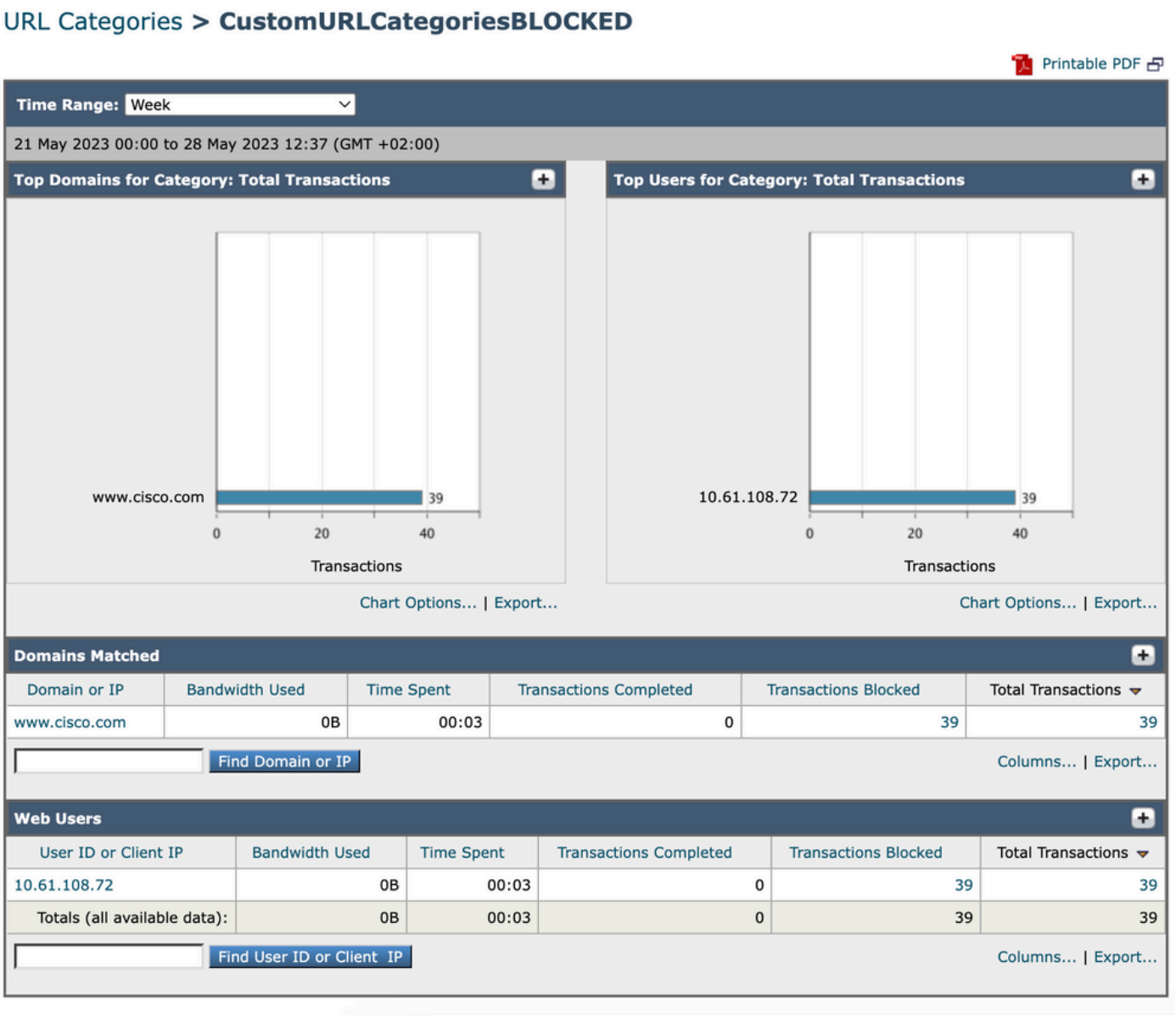
Esta página muestra datos específicos de categorías para el ahorro de ancho de banda y las transacciones web.

Sección	Descripción
Intervalo de tiempo (lista desplegable)	Seleccione el rango de tiempo del informe.
Categorías principales de URL por transacciones totales	Esta sección enumera las principales categorías de URL que se visitan en el sitio en un formato de gráfico.
Categorías principales de URL por transacciones bloqueadas y con advertencias	Muestra la dirección URL principal que ha activado una acción de bloqueo o advertencia por transacción en formato de gráfico.
Categorías de URL coincidentes	Muestra la disposición de las transacciones por categoría de URL durante el rango de tiempo especificado, más el ancho de banda utilizado y el tiempo empleado en cada categoría. Si el porcentaje de URL no categorizadas es superior al 15-20%, tenga en cuenta estas opciones: • En el caso de direcciones URL localizadas específicas, puede crear categorías de URL personalizadas y aplicarlas a usuarios o políticas de grupo específicos. • Puede informar sobre URL y URL no clasificadas y clasificadas erróneamente a Cisco para su evaluación y actualización de la base de datos. • Compruebe que el filtro de reputación web y el filtro anti-malware están activados.



Informe de categoría de URL de imagen

Puede hacer clic en cualquier nombre de categoría para ver más detalles relacionados con esa categoría, como Dominios coincidentes o lista de usuarios.



Página Imagen: Informe detallado

El conjunto de categorías de URL predefinidas se puede actualizar periódicamente de forma automática en su dispositivo de seguridad web .

Cuando se producen estas actualizaciones, los nombres de categorías antiguos siguen apareciendo en los informes hasta que los datos asociados a las categorías anteriores son demasiado antiguos para incluirlos en los informes.

Los datos de informe generados tras la actualización de un conjunto de categorías de URL utilizan las nuevas categorías, por lo que se pueden ver las categorías antiguas y las nuevas en el mismo informe.

En las estadísticas de URL de la página Categorías de URL de los informes, es importante comprender cómo interpretar estos datos:

Tipo de datos	Descripción
Filtrado de URL omitido	Representa la política, el puerto y el agente de usuario administrador bloqueados, lo que

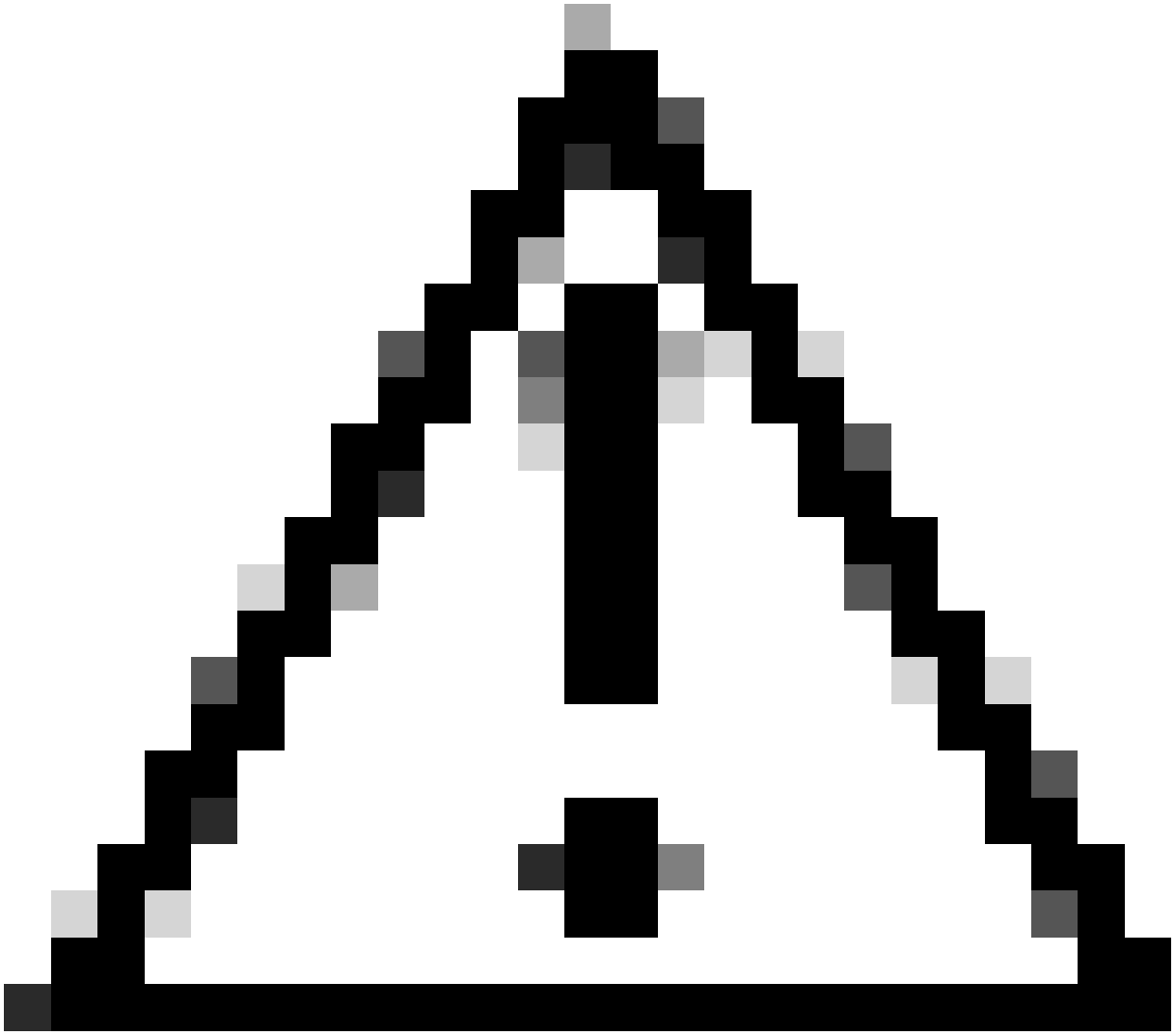
	ocurre antes del filtrado de URL.
URL sin categoría	Representa todas las transacciones para las que se consulta el motor de filtrado de URL, pero no coincide ninguna categoría.

Ver Categorías De URL Personalizadas En El Registro De Acceso

El dispositivo web seguro utiliza los primeros cuatro caracteres de los nombres de categoría de URL personalizados precedidos de "c_" en los registros de acceso.

En este ejemplo, el nombre de la categoría es CustomURLCategoriesBLOCKED y en los registros de acceso puede ver C_Cust :

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



Precaución: tenga en cuenta el nombre de categoría de URL personalizado si utiliza Sawmill para analizar los registros de acceso. Si los primeros cuatro caracteres de la categoría de URL personalizada incluyen un espacio, Sawmill no puede analizar correctamente la entrada del registro de acceso. En su lugar, utilice sólo caracteres admitidos en los primeros cuatro caracteres.

Sugerencia: si desea incluir el nombre completo de una categoría de URL personalizada en los logs de acceso, agregue el especificador de formato %XF a los logs de acceso.

Cuando un grupo de políticas de acceso a la Web tiene una categoría de URL personalizada establecida en Monitor y algún otro componente (como los filtros de reputación de Web o el motor de análisis de diferentes veredictos (DVS)) toma la decisión final de permitir o bloquear una solicitud de URL en la categoría de URL personalizada, la entrada del registro de acceso de la solicitud muestra la categoría de URL predefinida en lugar de la categoría de URL personalizada.

Para obtener más información sobre cómo configurar campos personalizados en Access Logs,

visite: Configure Performance Parameter in Access Logs - Cisco

Troubleshoot

Categoría no coincidente

En los registros de acceso puede ver la solicitud a la que pertenece la categoría de URL personalizado, si la selección no es la esperada:

- Si la solicitud se clasifica en otras categorías de URL personalizadas, compruebe si hay URL duplicada o una expresión regular coincidente en otras categorías o mueva la categoría de URL personalizado al principio y vuelva a comprobarlo. es mejor inspeccionar cuidadosamente la categoría de URL personalizado coincidente.

- Si la solicitud se clasifica en categorías predefinidas, compruebe las condiciones de la categoría de URL personalizado existente; si todas coinciden, intente agregar la dirección IP y compruebe o asegúrese de que se utiliza el error tipográfico y la expresión regular correcta, si existe.

Las Categorías Predefinidas No Están Actualizadas

Si las categorías predefinidas no están actualizadas, o en los registros de acceso ve "err" en la sección de categorías de URL, asegúrese de que TLSv1.2 esté habilitado para Updater.

Para cambiar la configuración SSL del actualizador, siga estos pasos de la GUI:

Paso 1. En Administración del sistema, elija Configuración SSL

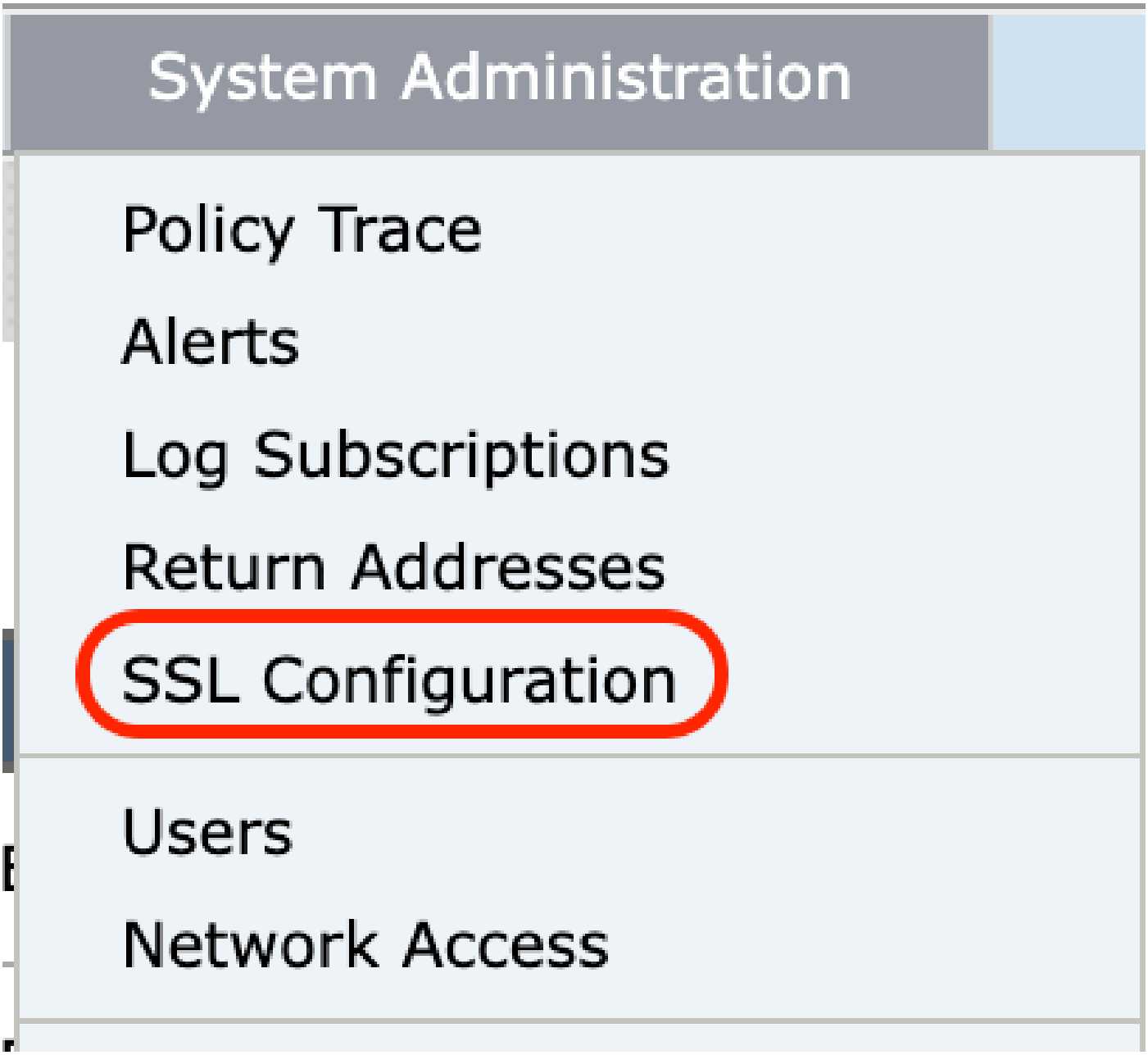


Imagen- configuración ssl

Paso 2. Seleccione Editar configuración.

Paso 3. En la sección Actualizar servicio, elija TLSv1.2

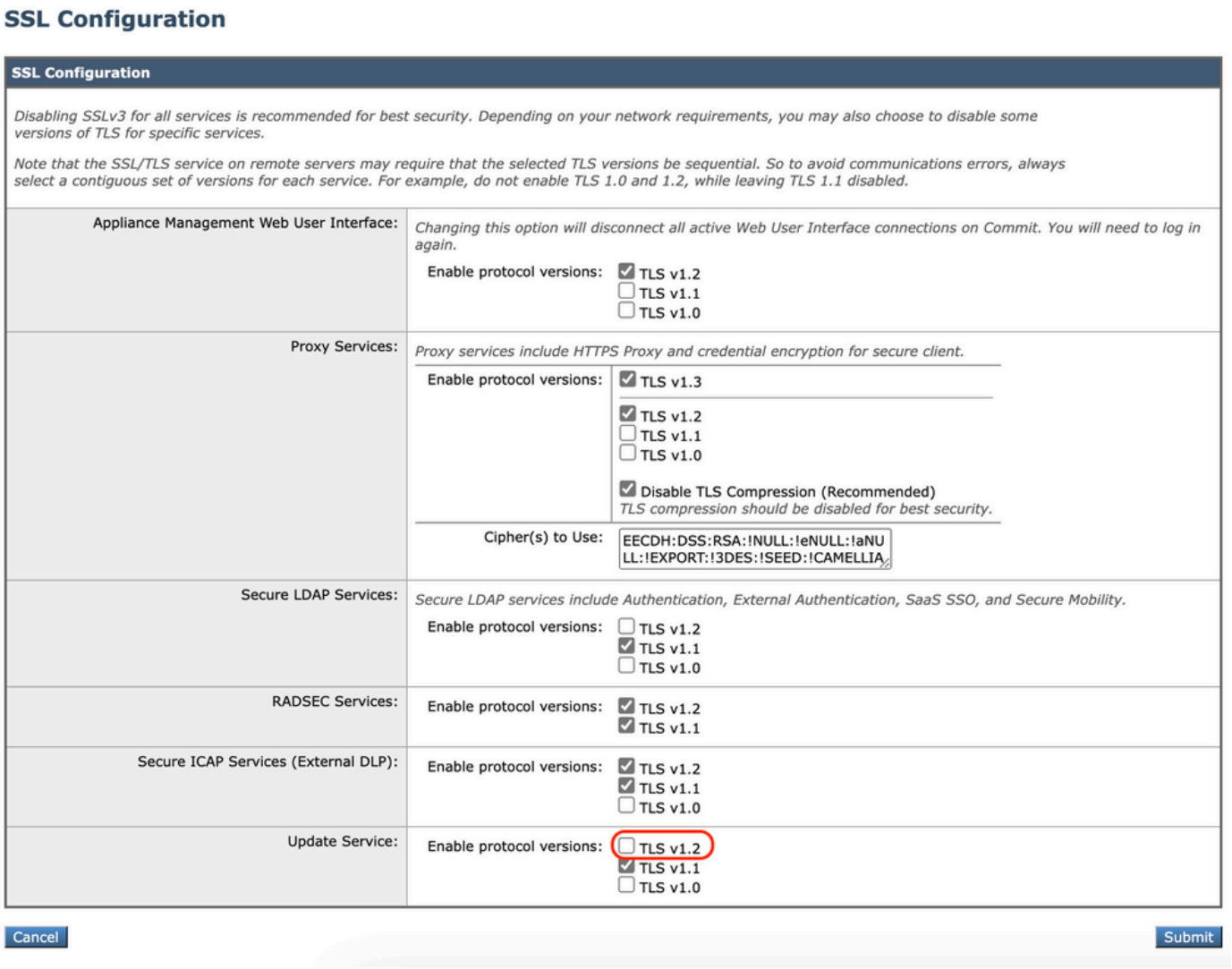


Imagen - Servicio de actualización TLSv1.2

Paso 4. Enviar y confirmar cambios

Para cambiar la configuración SSL del actualizador, siga estos pasos de la CLI:

Paso 1. Desde CLI, ejecute sslcofig

Paso 2. Escriba version y pulse intro

Paso 3. Elija Updater

Paso 4. Elija TLSv1.2

Paso 5. Pulse Intro para salir del asistente

Paso 6. Realice los cambios.

```
SWA_CLI> sslconfig

Disabling SSLv3 is recommended for best security.
```

```
Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequentia
1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:
- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.
[]> versions

SSL/TLS versions may be enabled or disabled for the following services:

        LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secu
        Updater - Update Service
        WebUI - Appliance Management Web User Interface
        RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
        SICAP - Secure ICAP Service
        Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

         LDAPS  Updater  WebUI   RADSEC  SICAP   Proxy
TLSv1.0    N       N       N      N/A      N       N
TLSv1.1    Y       Y       N       Y       Y       N
TLSv1.2    N       N       Y       Y       Y       Y
TLSv1.3   N/A     N/A     N/A     N/A     N/A      Y

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services
[]> 2


Currently enabled protocol(s) for Updater are TLSv1.1.


To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
[]> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y


Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.
```

Referencia

Directrices sobre prácticas recomendadas de Cisco Web Security Appliance: Cisco

BRKSEC-3303 (CiscoLive)

Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance - GD (implementación general) - Conexión, instalación y configuración [Cisco Secure Web Appliance] - 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).