

Configuración del Proxy upstream en el dispositivo web seguro

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración del Proxy Upstream](#)

[Paso 2. \(Opcional\) Crear un perfil de identificación para utilizar el proxy upstream](#)

[Paso 3. Crear el proxy upstream](#)

[Paso 4. \(Opcional\) Cargue el certificado de descifrado](#)

[Paso 5. Configuración de la Política de Ruteo](#)

[Paso 6. \(Opcional\) Configuración de los Valores de Tiempo de Espera de Respuesta de Proxy Upstream](#)

[Registro](#)

[Registros de acceso](#)

[Registros de proxy](#)

[Información Relacionada](#)

Introducción

En este documento se describen los pasos para configurar el proxy upstream en el dispositivo web seguro (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.
- Protocolos básicos de red y proxy.

Cisco recomienda tener instaladas estas herramientas:

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

Configuración del Proxy Upstream

Utilice estos pasos para configurar un Proxy upstream en SWA.



Pasos	Pasos
Paso 1. (Opcional) Crear una categoría de URL personalizada para las URL	Paso 1.1. Desde GUI, Elegir Administrador de seguridad web y, a continuación, haga clic en Categorías de URL externas y personalizadas.
 Nota: Si desea definir el proxy upstream para todo el tráfico, puede omitir este paso.	Paso 1.2. Haga clic en Agregar categoría para agregar una categoría de URL personalizada.
	Paso 1.3. Asignar un CategoryName único.
	Paso 1.4. (Opcional) Agregar descripción.
	Paso 1.5. En Orden de la lista, elija la primera categoría que desee colocar en la parte superior.
	Paso 1.6. En la lista desplegable Tipo de categoría, elija Categoría personalizada local.
	Paso 1.7. Agregue las URL deseadas en la Sección Sitios.
	Paso 1.8. Enviar.

Imagen: creación de una categoría de URL personalizada

Paso 2. (Opcional) Crear un perfil de identificación para utilizar el proxy upstream

 Nota: Si desea definir el proxy upstream para todo el tráfico, puede omitir este paso.

Paso 2.1. Desde GUI, Elegir Administrador de seguridad web y, a continuación, haga clic en Perfiles de identificación.

Paso 2.2. Haga clic en Agregar perfil para agregar un perfil.

Paso 2.3. Utilice la casilla de verificación Enable Identification Profile para habilitar este perfil o para deshabilitarlo rápidamente sin eliminarlo.

Paso 2.4. Asignar un profileName único.

Paso 2.5. (Opcional) Agregar descripción.

Paso 2.6. En la lista desplegable Insertar arriba, elija dónde debe aparecer este perfil en la tabla.

Paso 2.7. Si desea no autenticar a los usuarios que llegan a esta política, en la sección Método de identificación de usuarios, elija Exento de autenticación/ identificación; de lo contrario, configure los parámetros de autenticación.

Paso 2.8. En el campo Define Members by Subnet, deje este campo en blanco para incluir todas las direcciones IP del cliente a menos que desee pasar a través del tráfico para una dirección IP determinada.

Paso 2.9. (Opcional: Si necesita utilizar un proxy upstream para usuarios específicos que acceden a ciertos sitios web, complete este paso). En la sección Advanced, elija Custom URL Categories y Add the Custom URL Category que se creó en el Paso 1

Paso 2.10. Enviar.

Identification Profiles: Add Profile

The screenshot shows the 'Client / User Identification Profile Settings' page. It is divided into three main sections: 'Client / User Identification Profile Settings', 'User Identification Method', and 'Membership Definition'. Red circles with numbers 2.4 through 2.9 and arrows point to specific fields: 2.4 points to the 'Name' field containing 'Upstream Proxy ID Profile'; 2.6 points to the 'Insert Above' dropdown menu; 2.7 points to the 'Authentication Method' section, specifically the 'Authenticate Users' dropdown and the 'Select a Scheme' options; 2.8 points to the 'Define Members by Subnet' text input field containing '10.0.0.0/8'; 2.9 points to the 'Advanced' membership criteria section, specifically the 'Proxy Ports', 'URL Categories', and 'User Agents' dropdowns.

Imagen - Crear un perfil de identificación

Paso 3. Crear el proxy upstream

Paso 3.1. From GUI, Choose Network y luego haga clic en Upstream Proxy.

Paso 3.2. Haga clic en Agregar grupo.

Paso 3.3. Asignar un uniqueName.

Paso 3.4. Defina la dirección del proxy y el número de puerto.

Paso 3.5. (Opcional) Si tiene más de un proxy upstream, haga clic en Agregar fila para definir el siguiente proxy.

Paso 3.6. (Opcional) Si ingresó más de un Proxy Upstream desde la sección Balanceo de Carga, defina el método de Balanceo de Carga deseado,

- Ninguno (conmutación por error): el proxy web dirige las transacciones a un proxy externo del grupo. Intenta conectarse a los proxies en el orden en que aparecen en la lista. Si no se puede alcanzar un proxy, el proxy web intenta conectarse al siguiente de la lista.
- Menor número de conexiones: el proxy web realiza un seguimiento del número de solicitudes activas con los diferentes proxies del grupo y dirige una transacción al proxy que actualmente atiende el menor número de conexiones.

- Basado en Hash: menos utilizado recientemente. El proxy web dirige una transacción al proxy que recibió la transacción menos recientemente si todos los proxies están activos actualmente. Esta configuración es similar a la operación por turnos, excepto en que el proxy web también tiene en cuenta las transacciones que ha recibido un proxy al ser miembro de un grupo de proxy diferente. Es decir, si un proxy aparece en varios grupos de proxy, es menos probable que la opción "menos utilizada recientemente" sobrecargue ese proxy.
- Turnos rotatorios: el proxy de web procesa las transacciones por igual entre todos los proxies del grupo en el orden enumerado.

Paso 3.7. Elija la opción Gestión de Fallos en función de su política interna.

- Conectar directamente: Envíe las solicitudes directamente a sus servidores de destino.
- Solicitudes de descarte: descarte las solicitudes sin reenviarlas.

Paso 3.8. Enviar.

Add Upstream Proxy Group

Proxy Group

Name: upstream Proxy

Proxy Servers:	Proxy Address	Port	Reconnection Attempts (?)	Add Row
	10.48.48.182	3128	2	
	10.48.48.183	3128	2	

Host name, IPv4 or IPv6 address.

Load Balancing ? Fewest Connections

Failure Handling: Specify how to handle requests if all proxies in this group fail.

Connect directly

Drop requests

Cancel Submit

Imagen - Agregar grupo de proxy upstream

Paso 4. (Opcional) Cargue el certificado de descifrado

Nota: Si el proxy upstream no descifra el tráfico o si su servidor de la CA ya es de confianza en el SWA, puede omitir este paso

Paso 4.1. Desde GUI, Choose Network y luego haga clic en Certificate Management.

Paso 4.2. En la sección Administración de certificados, haga clic en Administrar certificados raíz de confianza.

Certificate Management

Appliance Certificates

Add Certificate...

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete
Export Certificate...							

Weak Signature Usage Settings

Restrict Weak Signature Usage: Disabled [Edit Settings](#)

Certificate FQDN Validation Settings

Certificate FQDN Validation Usage: Disabled [Edit Settings](#)

Certificate Lists

Updates

File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Sat Mar 07 00:08:32 2026	2.6	Failed to Fetch Manifest
Cisco Certificate Blocked List	Success - Sat Mar 07 00:08:32 2026	1.3	Failed to Fetch Manifest

No updates in progress. [Update Now](#)

Certificate Management

Trust Root Certificates: 246 certificates in Cisco trusted root certificate list
0 custom certificates added to trusted root certificate list [Manage Trusted Root Certificates...](#)

Certificate Based Authentication/RADSEC Root Certificates: 0 custom root certificates added to Certificate Based Authentication/RADSEC root certificate list [Manage Certificate Based Authentication/RADSEC Root Certificates...](#)

Blocked Certificates: 19 certificates in Cisco blocked certificate list [View Blocked Certificates...](#)

4.2

Imagen - Administrar certificado raíz de confianza

Paso 4.3. Enviar y registrar cambios.



Precaución: Si se requieren certificados de CA raíz e intermedia, cargue primero el certificado de CA raíz y, a continuación, haga clic en Enviar y confirmar. Una vez completada la confirmación, importe el certificado de CA intermedio y vuelva a enviar y confirme los cambios.

Paso 5. Configuración de la Política de Ruteo

Paso 5.1. Desde GUI, Elija Web Security Manager y haga clic en Política de enrutamiento.

Paso 5.2. (Opcional) Si desea utilizar el proxy upstream para usuarios o sitios web específicos, haga clic en Agregar directiva y seleccione el perfil de identificación que creó en el paso 2.

Routing Policy: Add Group

Policy Settings

Enable Policy

Policy Name: (e.g., my IT policy)

Description:

Insert Above Policy:

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:

Identification Profile:

Authorized Users and Groups

All Authenticated Users

Selected Groups and Users (?)

Groups: No groups entered

Users: No users entered

[Add Identification Profile](#)

[Cancel](#) [Submit](#)

5.2

Imagen - Agregando perfil de ID a la política de enrutamiento

Paso 5.3. Para las condiciones deseadas, que desea utilizar el proxy upstream, haga clic en el enlace Destino de Ruteo y seleccione el Grupo de Proxy Upstream que creó en el Paso 3.

Routing Policies

Order	Members	Routing Destination	IP Spoofing	Clone Policy	Delete
1	Partial Routing Policy Identification Profile: Upstream Proxy ID Profile All identified users	(global policy)	(global policy)		
	Global Routing Policy	Direct Connection	Do not use IP Spoofing		

5.3

Imagen - Configuración del Destino de Ruteo



Nota: Si desea que todo el tráfico utilice el proxy upstream, en la Política de routing global, seleccione el proxy upstream deseado.

Paso 5.4. Enviar y registrar los cambios.

Paso 6. (Opcional) Configuración de los Valores de Tiempo de Espera sin Respuesta del Proxy Upstream



Sugerencia: se recomienda no modificar estos valores a menos que comprenda completamente su comportamiento y su impacto potencial.

Paso 6.1. Inicie sesión en la CLI y ejecute `advanced proxyconfig`

Paso 6.2. Seleccione MISCELLANEOUS

Paso 6.3. Presione Enter hasta que vea Enter minimum idle timeout for check unresponse upstream proxy (en segundos). Si puede configurar la cantidad mínima de tiempo, SWA espera para reintentar el proxy upstream que se declaró anteriormente como Enfermo. El valor predeterminado es 10 segundos.

Paso 6.4. Pulse Intro para continuar con la siguiente configuración. Al definir el tiempo de espera inactivo máximo para verificar un proxy upstream que no responde, tenga en cuenta que si se alcanza este valor de tiempo de espera antes de que se agote el número configurado de intentos de reconexión (Paso 3), el SWA considerará el proxy upstream fuera de línea.

Paso 6.7. Siga presionando Enter, hasta que salga del asistente, ejecute `commit` para guardar los cambios.

Registro

Registros de acceso

En los registros de acceso, el tráfico que se enrutó al proxy upstream se muestra como DEFAULT_PARENT seguido del nombre del proxy upstream. aquí hay un ejemplo:

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

Registros de proxy

Desde los proxylogs, puede verificar el estado de salud de los proxies upstream.



Consejo: Puede filtrar por peer para revisar los registros relacionados con el proxy upstream.

Aquí hay algunos ejemplos, ya que configuramos los Intentos de Reconexión en el Paso 3 dos veces, después de dos fallas de conexión al proxy upstream, el proxy upstream se declara add y SWA elimina este proxy upstream de la lista hasta que se reinicie el proceso proxy.

```
Thu Apr 2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr 2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr 2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr 2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```



Nota: Si el proxy upstream no responde a las solicitudes SYN de TCP, no puede devolver un código de respuesta HTTP o devuelve una respuesta HTTP 504 (tiempo de espera de gateway), SWA considera que el proxy upstream no está disponible y cambia su estado de Correcto a Enfermo.



Consejo: El SWA considera un proxy upstream saludable si devuelve un encabezado VIA.

Información Relacionada

- [Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance](#)
- [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](#)
- [Uso de las prácticas recomendadas de los dispositivos web seguros: Cisco](#)
- [Bloqueo del tráfico en el dispositivo web seguro](#)
- [Bloquear la carga de tráfico en el dispositivo web seguro](#)
- [Bloquear la descarga de archivos ejecutables en SWA](#)
- [Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro](#)
- [Omitir autenticación en dispositivo web seguro - 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).