

Configuración de la cadena de proxy entre el dispositivo web seguro y el SWG de Umbrella

Contenido

[Introducción](#)

[Overview](#)

[Configuración de la política de Secure Web Appliance](#)

[Para una implementación de proxy transparente](#)

[Configuración de la política web de SWG en el panel de Umbrella](#)

Introducción

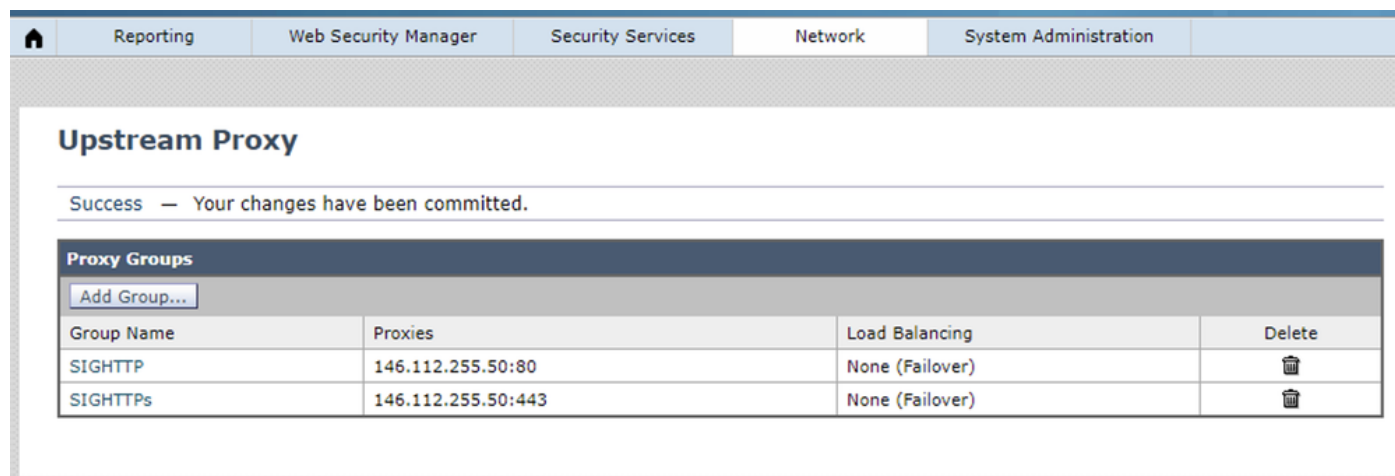
En este documento se describe cómo configurar la cadena de proxy entre Secure Web Appliance y Umbrella Secure Web Gateway (SWG).

Overview

Umbrella SIG soporta la cadena de proxy y puede manejar todas las solicitudes HTTP/HTTPS del servidor proxy de flujo descendente. Esta es una guía completa para implementar la cadena de proxy entre [Cisco Secure Web Appliance \(anteriormente Cisco WSA\)](#) y [Umbrella Secure Web Gateway \(SWG\)](#), incluida la configuración tanto para Secure Web Appliance como para SWG.

Configuración de la política de Secure Web Appliance

1. Configure los links HTTP y HTTPS SWG como el Proxy Upstream vía Red>Proxy Upstream.



Group Name	Proxies	Load Balancing	Delete
SIGHTTP	146.112.255.50:80	None (Failover)	
SIGHTTps	146.112.255.50:443	None (Failover)	

360079596451

2. Cree una política de desvío a través de Web Security Manager>Política de enrutamiento para enrutar todas las URL sugeridas a Internet directamente. Todas las URL omitidas se pueden

encontrar en nuestra documentación: [Guía del usuario de Cisco Umbrella SIG: Administrar encadenamiento de proxy](#)

- Comience creando una nueva "Categoría personalizada" navegando hasta Administrador de seguridad web>Categorías de URL externas y personalizadas como se muestra aquí. La política de omisión se basa en la "Categoría personalizada".

Reporting

Web Security Manager

Security Services

Network

System Administration

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:

ProxyChainBypassList

List Order:

1

Category Type:

Local Custom Category

Sites: ?

.cisco.com, .isrg.trustid.ocsp.identrust.com,
.login.microsoftonline.com, .ocsp.int-x3.letsencrypt.org,
.okta.com, .oktacdn.com, .opendns.com, .pingidentity.com,
.secure.aadcdn.microsoftonline-p.com, .umbrella.com

Sort URLs
Click the Sort URLs
button to sort all site
URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced

Regular Expressions: ?

Enter one regular expression per line.

Cancel

Submit

360050592552

- A continuación, cree una nueva política de enrutamiento de omisión navegando hasta Administrador de seguridad web>Política de enrutamiento. Asegúrese de que esta política es la primera, ya que el dispositivo web seguro coincide con la política basada en el orden de la política.

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: BypassProxyChain

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:

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

☒ Advanced Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:

Protocols:

Proxy Ports:

Subnets:

Time Range:

URL Categories:

User Agents:

360050703131

3. Cree una nueva política de enrutamiento para todas las solicitudes HTTP.

- En la definición de miembro de la política de routing de Secure Web Appliance, las opciones de protocolo son HTTP, FTP sobre HTTP, FTP nativo y "Todos los demás", mientras que se selecciona "Todos los perfiles de identificación". Dado que no hay ninguna opción para HTTP, cree la política de enrutamiento para la solicitud de HTTP individualmente después de implementar esta política de enrutamiento para todas las solicitudes HTTP.

Reporting Web Security Manager Security Services Network System Administration

Routing Policies: Policy "SIGALLHTTP": Membership by Protocol

Advanced Membership Definition: Protocols

Policy membership can be defined to apply to one or more protocols. Leave all protocols unselected if membership by protocol is not desired.

Protocols: ☒ HTTP ☐ FTP over HTTP ☐ Native FTP ☐ All others

Note: Policy membership by HTTPS is not available when the HTTPS proxy is enabled.

360050592772

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: SIGALLHTTP

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:

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP
 Proxy Ports: None Selected
 Subnets: None Selected
 Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)
 URL Categories: None Selected
 User Agents: None Selected

Cancel **Submit**

360050589572

4. Cree la política de enrutamiento para las solicitudes HTTP basándose en el "perfil de identificación". Tenga cuidado con la secuencia del "perfil de identificación" definido, ya que el dispositivo web seguro coincide con la "identificación" para la primera coincidencia. En este ejemplo, el perfil de identificación "win2k8" es una identidad interna basada en IP.

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles

Client / User Identification Profiles

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	win2k8 Subnets: 192.168.0.212 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	

360050703971

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: Win2k8HTTps

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	
win2k8	No authentication required	Add Identification Profile

☒ Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile win2k8
Proxy Ports: None Selected
Subnets: None Selected
Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories: None Selected
User Agents: None Selected

"Protocols" can't be selected for the individual "Identification Profile"

Cancel Submit

360050700091

5. Configuraciones finales de las políticas de routing de dispositivos web seguros:

- Tenga en cuenta que Secure Web Appliance evalúa las identidades y las políticas de acceso mediante un enfoque de procesamiento de reglas "descendente". Esto significa que la primera coincidencia realizada en cualquier punto del procesamiento tiene como resultado la acción realizada por Secure Web Appliance.
- Además, las identidades se evalúan primero. Una vez que el acceso de un cliente coincide con una identidad específica, Secure Web Appliance comprueba todas las políticas de acceso configuradas para utilizar la identidad que coincide con el acceso del cliente.

Routing Policies

Routing Definitions			
Add Policy...			
Order	Members	Routing Destination	Delete
1	BypassProxyChain Identification Profile: All URL Categories: ProxyChainBypassList	Direct Connection	
2	SIGALLHTTPs (disabled) Identification Profile: All Protocols: All others	SIGHTTPs proxy.sig.umbrella.com:443	
3	SIGALLHTTP Identification Profile: All Protocols: HTTP	SIGHTTP proxy.sig.umbrella.com:80	
4	Win2k8HTTPs Identification Profile: win2k8 All identified users	SIGHTTPs proxy.sig.umbrella.com:443	
5	Win2016ProxyChainHTTPs Identification Profile: Win2016 All identified users	SIGHTTPs proxy.sig.umbrella.com:443	

360050700131

Nota: La configuración de directiva mencionada sólo se aplica a la implementación de proxy explícito.

Para una implementación de proxy transparente

En el caso de HTTPS transparente, AsyncOS no tiene acceso a la información de los encabezados de cliente. Por lo tanto, AsyncOS no puede aplicar directivas de enrutamiento si alguna directiva de enrutamiento o perfil de identificación depende de la información de los encabezados de cliente.

1. Las transacciones HTTPS redirigidas de forma transparente sólo coinciden con las políticas de enrutamiento si:
 - El grupo de políticas de enrutamiento no tiene definidos criterios de pertenencia a políticas como la categoría de URL, el agente de usuario, etc.
 - El perfil de identificación no tiene definidos criterios de pertenencia a políticas como la categoría de URL, el agente de usuario, etc.
2. Si algún perfil de identificación o política de enrutamiento tiene definida una categoría de URL personalizada, todas las transacciones HTTPS transparentes coinciden con el grupo de políticas de enrutamiento predeterminado.
3. En la medida de lo posible, evite configurar la política de routing con todos los perfiles de identificación, ya que esto podría hacer que las transacciones HTTPS transparentes coincidieran con el grupo de políticas de routing predeterminado.

1. Encabezado X-Forwarded-For

- para implementar la política web interna basada en IP en SWG. Asegúrese de habilitar el encabezado "X-Forwarded-For" en Secure Web Appliance mediante Servicios de seguridad > Configuración de proxy.

Reporting

Web Security Manager

Security Services

Network

System Administration

Proxy Settings

Web Proxy Settings

Basic Settings

Proxy:	Enabled
HTTP Ports to Proxy:	80, 3128
Caching:	Disabled Clear Cache
Proxy Mode:	Transparent
IP Spoofing:	Not Enabled

Advanced Settings

Persistent Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
In-Use Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
Simultaneous Persistent Connections:	Server Maximum Number: 2000
Generate Headers:	X-Forwarded-For: Send Request Side VIA: Send Response Side VIA: Send
Use Received Headers:	Identification of Client IP Addresses using X-Forwarded-For: Disabled
Range Request Forwarding:	Disabled

Edit Settings...

360050700111

2. Certificado raíz de confianza para el descifrado de HTTPs.

- Si el descifrado de HTTPs está habilitado en Web Policy en el panel de Umbrella, descargue "Cisco Root Certificate" desde el panel de Umbrella> Deployments> Configuration e impórtelo en los certificados raíz de confianza de Secure Web Appliance.

Manage Trusted Root Certificates

Custom Trusted Root Certificates

[Import...](#)

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
▸ Cisco Umbrella Root CA	Jun 28 15:37:53 2036 GMT	No	

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

Cisco Trusted Root Certificate List (332 entries, 0 overridden)

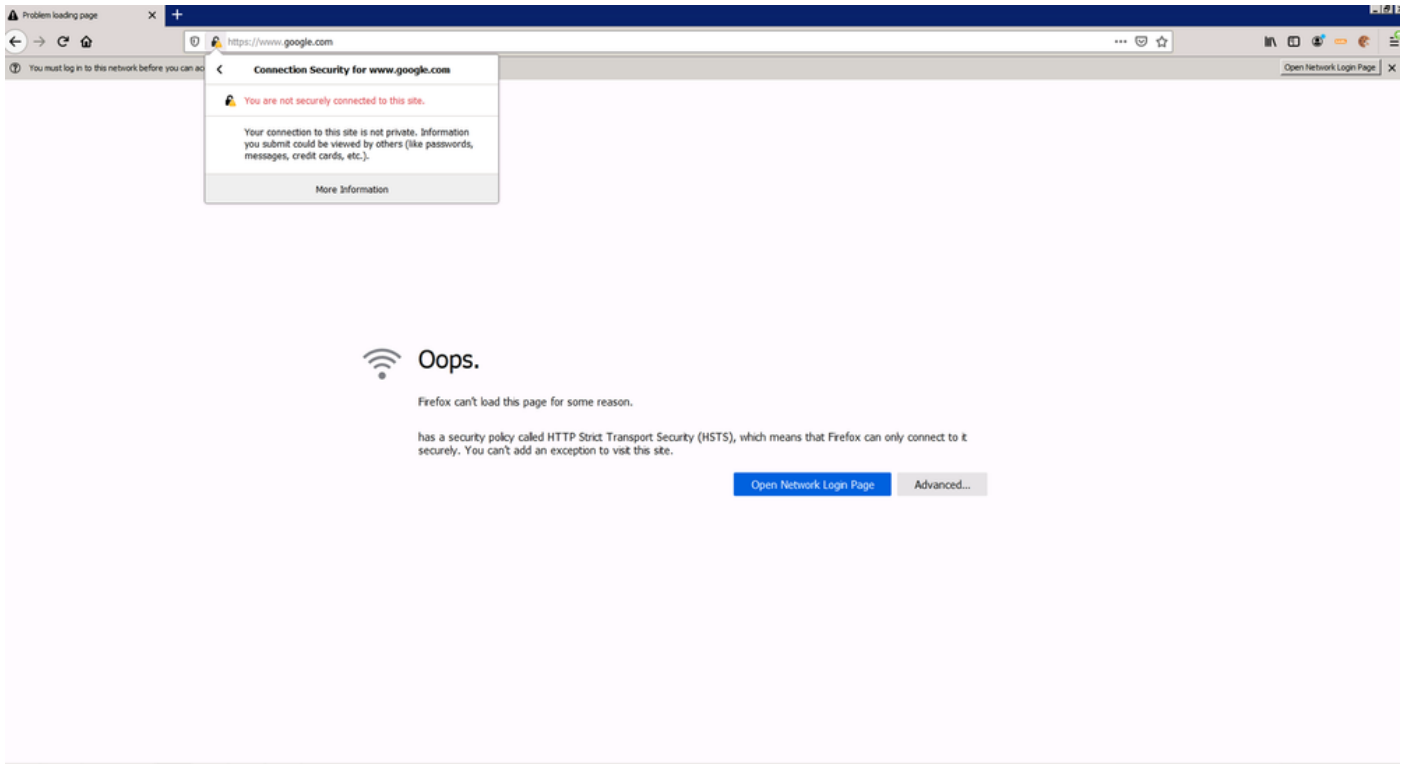
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

Use the checkboxes to override entries. If an entry on the list is overridden, it will not be treated as a trusted root certificate authority.

Certificate	Expiration Date	Override Trust ?
▸ (c) 1998 VeriSign, Inc. - For authorized use only	Aug 1 23:59:59 2028 GMT	☐
▸ A-Trust-nQual-03	Jul 23 08:38:29 2025 GMT	☐
▸ A-Trust-Qual-02	Jul 1 09:23:33 2024 GMT	☐
▸ A-Trust-Root-05	Sep 20 11:24:11 2023 GMT	☐
▸ AAA Certificate Services	Dec 31 23:59:59 2028 GMT	☐

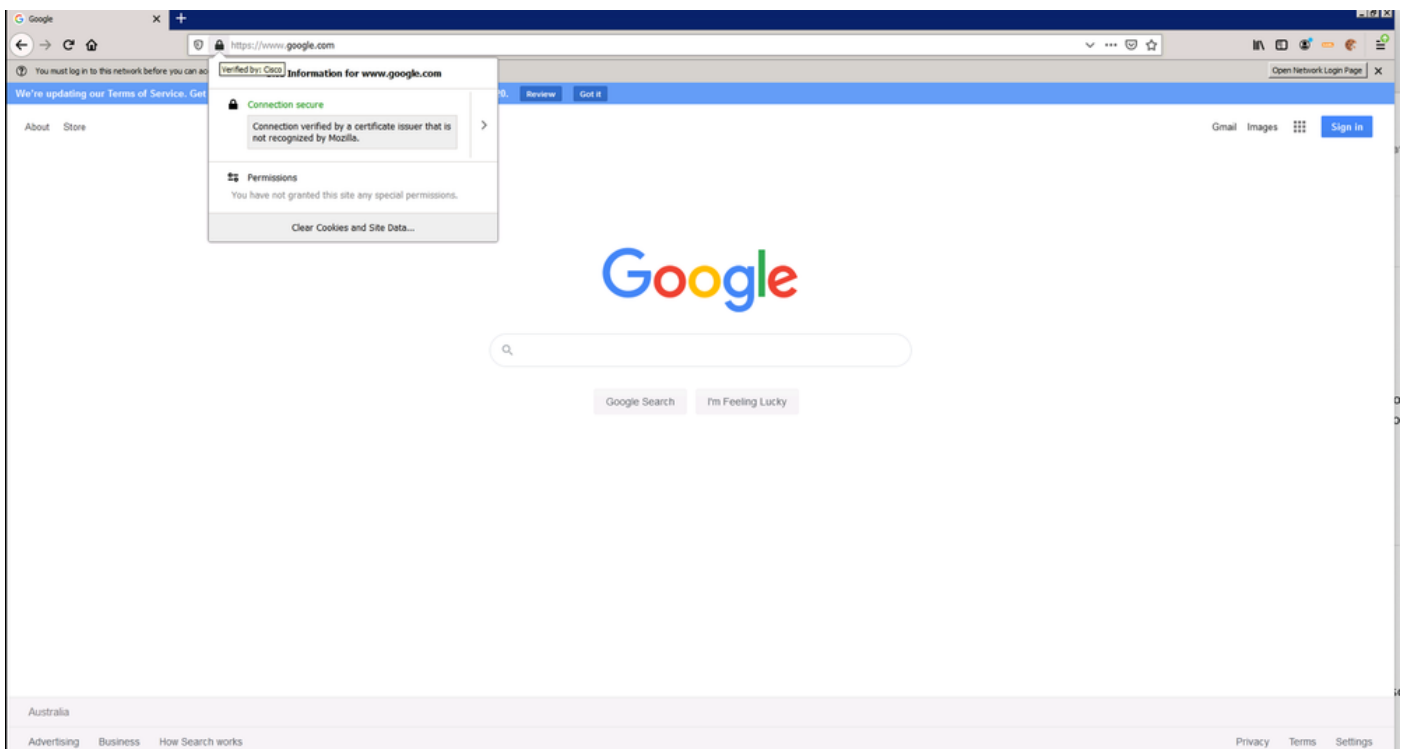
360050589612

- Si el "certificado raíz de Cisco" no se ha importado al dispositivo web seguro mientras el descifrado de HTTPs está habilitado en la política web de SWG, el usuario final recibe un error similar a este ejemplo:
 - "Uy. (navegador) no puede cargar esta página por algún motivo. cuenta con una política de seguridad denominada seguridad de transporte estricta HTTP (HSTS), lo que significa que (navegador) solo puede conectarse a ella de forma segura. No puede agregar una excepción para visitar este sitio."
 - "No está conectado de forma segura a este sitio."



360050700171

- Este es un ejemplo de los HTTP descifrados por Umbrella SWG. El certificado se verifica mediante el "certificado raíz de Cisco" denominado "Cisco".



360050700191

Configuración de la política web de SWG en el panel de Umbrella

Política web SWG basada en IP interna:

- Asegúrese de habilitar el encabezado "X-Forwarded-For" en el dispositivo web seguro, ya que SWG se basa en eso para identificar la IP interna.
- Registre la IP de salida del dispositivo web seguro en Implementación > Redes.
- Cree una IP interna del equipo cliente en Implementación > Configuración > Redes internas. Seleccione la IP de salida del dispositivo web seguro registrado (paso 1) después de marcar/seleccionar "Mostrar redes".
- Cree una nueva política web basada en la IP interna creada en el paso 2.
- Asegúrese de que la opción "Enable SAML" (Activar SAML) esté desactivada en la política web.

Política web SWG basada en usuario/grupo AD:

- Asegúrese de que todos los usuarios y grupos de AD se aprovisionan en el panel de Umbrella.
- Cree una nueva política web basada en la IP de salida registrada del dispositivo web seguro con la opción "Enable SAML" (Activar SAML) activada.
- Cree otra nueva política web basada en el usuario/grupo de AD con la opción "Activar SAML" desactivada. También debe colocar esta política web por delante de la política web creada en el paso 2.

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).