

Configure the Proxy Chain Between the Secure Web Appliance and the Umbrella SWG

Contents

[Introduction](#)

[Overview](#)

[Secure Web Appliance Policy Configuration](#)

[For Transparent Proxy Deployment](#)

[SWG Web Policy Configuration in Umbrella Dashboard](#)

Introduction

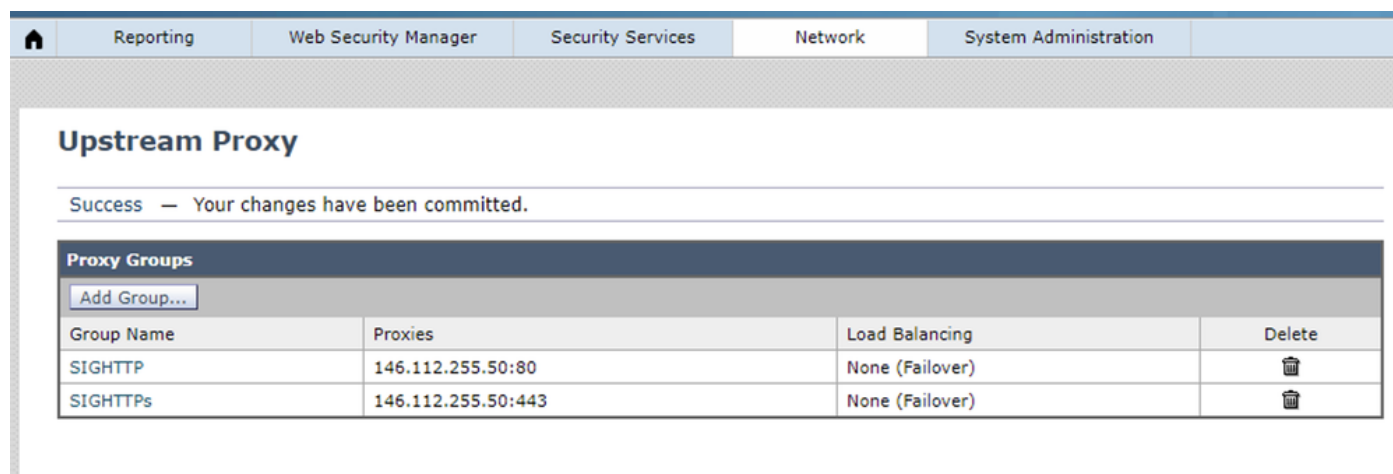
This document describes how to configure the proxy chain between the Secure Web Appliance and the Umbrella Secure Web Gateway (SWG).

Overview

The Umbrella SIG supports the proxy chain and can handle all the HTTP/HTTPS requests from the downstream proxy server. This is a comprehensive guide to implement the proxy chain between [Cisco Secure Web Appliance \(formerly Cisco WSA\)](#) and the [Umbrella Secure Web Gateway \(SWG\)](#), including the configuration for both Secure Web Appliance and SWG.

Secure Web Appliance Policy Configuration

1. Configure the SWG HTTP and HTTPS links as the Upstream Proxy via **Network>Upstream Proxy**.



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

360079596451

2. Create a bypass policy via **Web Security Manager>Routing Policy** to route all suggested URLs to the internet directly. All bypassed URLs can be found in our documentation: [Cisco Umbrella SIG User Guide: Manage Proxy Chaining](#)

- Start by creating a new "Custom Category" by navigating to **Web Security Manager>Custom and**

External URL Categories as shown here. The bypass policy is based on the "Custom Category."

Home	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

- Next, create a new bypass routing policy by navigating to **Web Security Manager>Routing Policy**. Please make sure this policy is the first one as Secure Web Appliance matches the policy based on the policy order.

Home	Reporting	Web Security Manager	Security Services	Network	System Administration
------	-----------	----------------------	-------------------	---------	-----------------------

Routing Policy: BypassProxyChain

Policy Settings

☒ Enable Policy

Policy Name: ?

BypassProxyChain
(e.g. my IT policy)

Description:

Insert Above Policy:

1 (SIGALLHTTPs)

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:

All Identification Profiles

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:

None Selected

Proxy Ports:

None Selected

Subnets:

None Selected

Time Range:

No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories:

ProxyChainBypassList

User Agents:

None Selected

Cancel

Submit

360050703131

3. Create a new routing policy for all HTTP requests.

- In the Secure Web Appliance routing policy member definition, the protocol options are HTTP, FTP over HTTP, Native FTP, and "All others" while "All Identification Profiles" are selected. Since there is no option for HTTPs, create the routing policy for HTTPs request individually after implementing this routing policy for all HTTP requests.

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.

Cancel Done

360050592772

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: SIGALLHTTP

Policy Settings

☒ Enable Policy

Policy Name: ? SIGALLHTTP
(e.g. my IT policy)

Description:

Insert Above Policy: 3 (Win2k8HTTps)

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: All Identification Profiles

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. Create the routing policy for HTTPs requests based on the "Identification Profile." Please be careful with the sequence of the defined "Identification Profile," since the Secure Web Appliance matches the "Identification" for the first match. In this example, the Identification Profile "win2k8" is an internal IP based identity.

Reporting	Web Security Manager	Security Services	Network	System Administration										
Identification Profiles Client / User Identification Profiles Add Identification Profile... <table> <tr> <th>Order</th><th>Transaction Criteria</th><th>Authentication / Identification Decision</th><th>End-User Acknowledgement</th><th>Delete</th></tr> <tr> <td>1</td><td> win2k8 Subnets: 192.168.0.212 Protocols: HTTP/HTTPS </td><td>Exempt from Authentication / User Identification</td><td>(global profile)</td><td></td></tr> </table>					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)	
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: Win2k8HTTps
(e.g. my IT policy)

Description:

Insert Above Policy: 4 (Win2016ProxyChainHTTps)

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:
Select One or More Identification Profiles

Identification Profile	Authorized Users and Groups	Add Identification Profile
win2k8	No authentication required	

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"

360050700091

5. Final configurations for the Secure Web Appliance Routing Policies:

- Be mindful that Secure Web Appliance evaluates the identities and access policies using a "top down" rule processing approach. This means that the first match made at any point in the processing results in the action taken by Secure Web Appliance.
- Additionally, identities are evaluated first. Once a client's access matches a specific identity, Secure Web Appliance checks all access policies that are configured to use the identity that matches the client's access.

Routing Policies

1. Bypass SWG always be the top

2. Then one for all HTTP requests

~~3 Individual one for the HTTPs~~

360050700131

Note: The mentioned Policy Configuration is applicable for Explicit Proxy Deployment only.

For Transparent Proxy Deployment

In the case of transparent HTTPS, AsyncOS does not have access to information in the client headers. Therefore, AsyncOS cannot enforce routing policies if any routing policy or identification profile relies on the information in the client headers.

1. Transparently redirected HTTPS transactions only matches Routing Policies if:
 - Routing Policy Group does not have a policy membership criteria like URL category, User Agent, and so on defined.
 - Identification Profile does not have a policy membership criteria like URL category, User Agent, and so on defined.
2. If any Identification Profile or Routing Policy has a custom URL category defined, then all the transparent HTTPS transactions matches the Default Routing Policy Group.
3. As much as possible, avoid configuring Routing Policy with All Identification Profiles as this might cause transparent HTTPS transactions to match the Default Routing Policy Group.

1. X-Forwarded-For Header

- to implement the internal IP based Web Policy in SWG. Make sure to enable the "X-Forwarded-For" header in Secure Web Appliance via **Security Services > Proxy Settings**.

Home	Reporting	Web Security Manager	Security Services	Network	System Administration																														
Proxy Settings <table border="1"><thead><tr><th colspan="2">Web Proxy Settings</th></tr><tr><th colspan="2">Basic Settings</th></tr></thead><tbody><tr><td>Proxy:</td><td>Enabled</td></tr><tr><td>HTTP Ports to Proxy:</td><td>80, 3128</td></tr><tr><td>Caching:</td><td>Disabled Clear Cache</td></tr><tr><td>Proxy Mode:</td><td>Transparent</td></tr><tr><td>IP Spoofing:</td><td>Not Enabled</td></tr><tr><th colspan="2">Advanced Settings</th></tr><tr><td>Persistent Connection Timeout:</td><td>Client Side: 300 Seconds Server Side: 300 Seconds</td></tr><tr><td>In-Use Connection Timeout:</td><td>Client Side: 300 Seconds Server Side: 300 Seconds</td></tr><tr><td>Simultaneous Persistent Connections:</td><td>Server Maximum Number: 2000</td></tr><tr><td>Generate Headers:</td><td>X-Forwarded-For: Send Request Side VIA: Send Response Side VIA: Send</td></tr><tr><td>Use Received Headers:</td><td>Identification of Client IP Addresses using X-Forwarded-For: Disabled</td></tr><tr><td>Range Request Forwarding:</td><td>Disabled</td></tr><tr><td colspan="2">Edit Settings...</td></tr></tbody></table>						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...	
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...																																			

2. Trusted Root Certificate for HTTPs decryption.

- If the HTTPs decryption is enabled at **Web Policy** in the Umbrella dashboard, download "Cisco Root Certificate" from the **Umbrella dashboard**> **Deployments**> **Configuration** and import it into the Secure Web Appliance trusted root certificates.

 Cisco S000V
Web Security Virtual Appliance

Web Security Appliance is getting a new look.

Home

Reporting

Web Security Manager

Security Services

Network

System Administration

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)

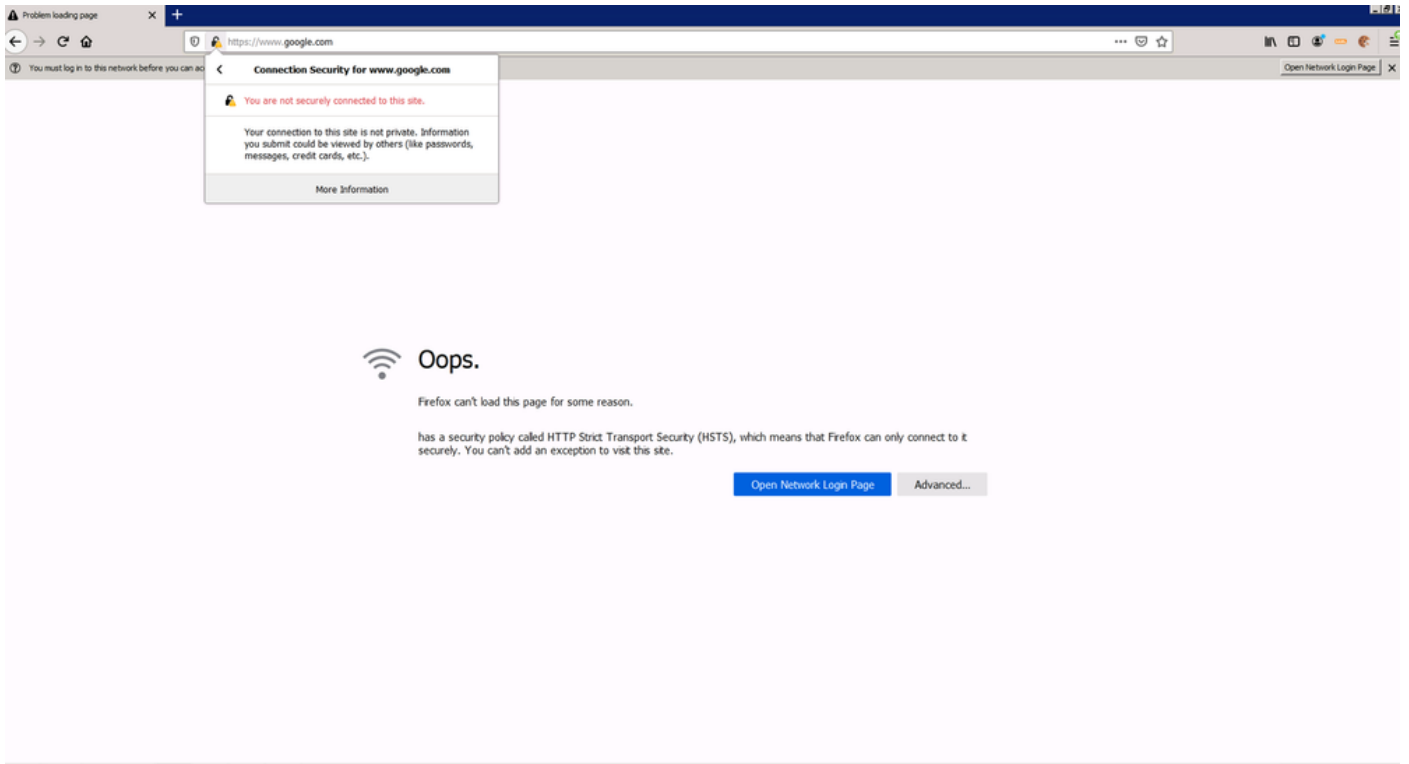
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

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	☐

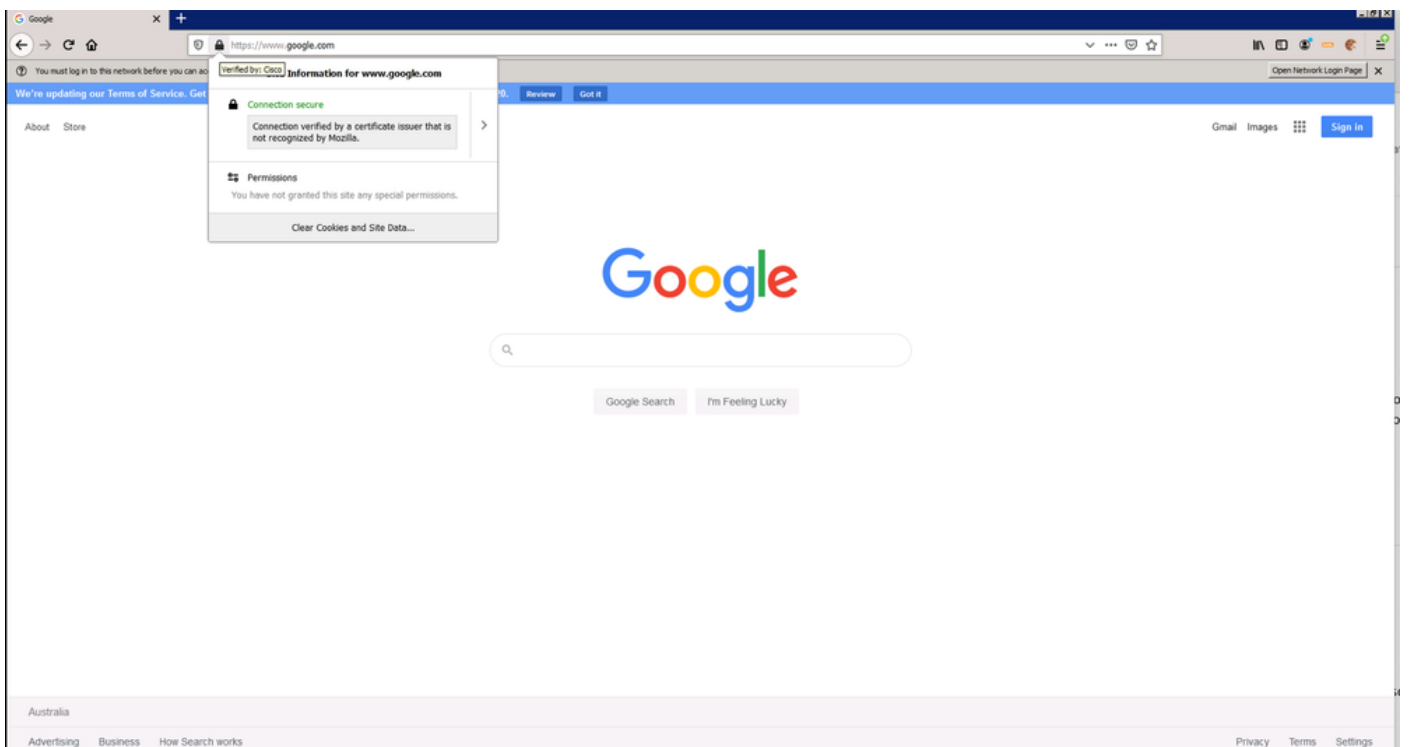
360050589612

- If the "Cisco Root Certificate" has not been imported to the Secure Web Appliance while the HTTPs decryption is enabled at SWG Web Policy, the end-user receives an error similar to this example:
 - "Oops. (browser) cannot load this page for some reason. has a security policy called HTTP Strict Transport Security (HSTS), which means that (browser) can only connect to it securely. You cannot add an exception to visit this site."
 - "You are not securely connected to this site."



360050700171

- This is an example of the HTTPs decrypted by Umbrella SWG. The certificate is verified by the "Cisco Root Certificate" named "Cisco."



360050700191

SWG Web Policy Configuration in Umbrella Dashboard

SWG Web Policy based on internal IP:

- Make sure to enable the "X-Forwarded-For" Header in the Secure Web Appliance, since SWG relies on that to identify the internal IP.
- Register the egress IP of the Secure Web Appliance in **Deployment > Networks**.
- Create an internal IP of the client machine in **Deployment > Configuration > Internal Networks**. Please select the registered Secure Web Appliance egress IP (Step 1) after ticking/selecting "Show Networks."
- Create a new Web Policy based on the internal IP created in Step 2.
- Make sure the "Enable SAML" option is disabled in the Web Policy.

SWG Web Policy based on AD user/group:

- Make sure all AD users and groups are provisioned to the Umbrella dashboard.
- Create a new web policy based on the registered egress IP of the Secure Web Appliance with the "Enable SAML" option enabled.
- Create another new web policy based on the AD user/group with the "Enable SAML" option disabled. Also need to place this web policy ahead of the Web Policy created at Step 2.