

配置安全Web裝置和Umbrella SWG之間的代理鏈

目錄

[簡介](#)

[概觀](#)

[安全Web裝置策略配置](#)

[用於透明代理部署](#)

[Umbrella控制面板中的SWG Web策略配置](#)

簡介

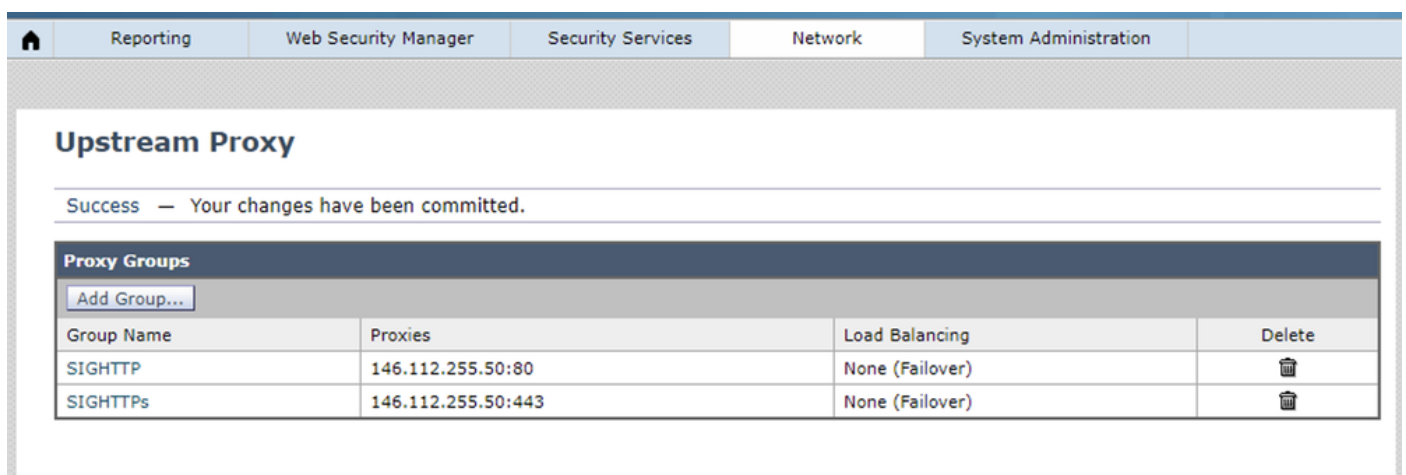
本檔案介紹如何在安全網路裝置和Umbrella安全網路閘道(SWG)之間設定代理鏈結。

概觀

Umbrella SIG支援代理鏈並可處理來自下游代理伺服器的所有HTTP/HTTPS請求。這是在[Cisco Secure Web Appliance \(前身為Cisco WSA \)](#)和[Umbrella Secure Web Gateway\(SWG\)](#)之間實施代理鏈的綜合指南，包括安全Web裝置和SWG的配置。

安全Web裝置策略配置

1.將SWG HTTP和HTTPS連結配置為通過Network>Upstream Proxy的上游代理。



The screenshot shows the Umbrella management console with the 'Network' tab selected. The 'Upstream Proxy' section displays a success message: 'Success — Your changes have been committed.' Below this is a table titled 'Proxy Groups' with an 'Add Group...' button. The table has four columns: 'Group Name', 'Proxies', 'Load Balancing', and 'Delete'. It contains two entries: 'SIGHTTP' with proxy '146.112.255.50:80' and 'SIGHTTps' with proxy '146.112.255.50:443'. Both have 'None (Failover)' for load balancing and a delete icon.

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

360079596451

2.通過Web Security Manager>Routing Policy建立繞過策略，將所有建議的URL直接路由到Internet。所有繞過的URL可在我們的文檔中找到：[Cisco Umbrella SIG使用手冊：管理代理連結](#)

- 首先建立一個新的「自定義類別」，導航到Web Security Manager>自定義和外部URL類別（如此處所示）。繞過策略基於「自定義類別」。

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

- 接下來，通過導航到Web Security Manager>Routing Policy來建立新的旁路路由策略。請確保此策略是第一個策略，因為安全網路裝置會根據策略順序匹配策略。

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.為所有HTTP請求建立新的路由策略。

- 在Secure Web Appliance路由策略成員定義中，協定選項為HTTP、FTP over HTTP、本地

FTP和「所有其他」，同時選擇了「所有標識配置檔案」。由於HTTP沒有選項，因此請在為所有HTTP請求實施此路由策略之後，分別為HTTPS請求建立路由策略。

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: (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.根據「標識配置檔案」為HTTPs請求建立路由策略。請注意定義的「標識配置檔案」的順序，因為安全網路裝置與第一個匹配項的「標識」匹配。在本示例中，標識配置檔案「win2k8」是基於IP的內部標識。

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

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	
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

Cancel Submit

360050700091

5.安全Web裝置路由策略的最終配置：

- 請注意，Secure Web Appliance使用「自上而下」的規則處理方法來評估標識和訪問策略。這意味著在處理過程中的任何時刻進行的第一個匹配都會導致Secure Web Appliance執行的操作。
- 此外，首先評估身份。一旦客戶端的訪問與特定身份匹配，安全網路裝置將檢查所有配置為使用與客戶端訪問匹配的身份的訪問策略。

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	SIGHTHTTps proxy.sig.umbrella.com:443	
3	SIGALLHTTP Identification Profile: All Protocols: HTTP	SIGHTHTTP proxy.sig.umbrella.com:80	
4	Win2k8HTTps Identification Profile: win2k8 All identified users	SIGHTHTTps proxy.sig.umbrella.com:443	
5	Win2016ProxyChainHTTps Identification Profile: Win2016 All identified users	SIGHTHTTps proxy.sig.umbrella.com:443	

360050700131

附註：上述策略配置僅適用於顯式代理部署。

用於透明代理部署

對於透明HTTPS，AsyncOS無權訪問客戶端報頭中的資訊。因此，如果任何路由策略或標識配置檔案依賴於客戶端報頭中的資訊，則AsyncOS無法實施路由策略。

- 在以下情況下，透明重定向的HTTPS事務僅與路由策略匹配：
 - 路由策略組沒有定義策略成員資格條件，如URL類別、使用者代理等。
 - 標識配置檔案沒有定義策略成員資格條件，如URL類別、使用者代理等。
- 如果任何標識配置檔案或路由策略定義了自定義URL類別，則所有透明HTTPS事務都與預設路由策略組匹配。
- 儘可能避免使用所有標識配置檔案配置路由策略，因為這樣可能會導致透明HTTPS事務與預設路由策略組匹配。

1. X-Forwarded-For Header

- 在SWG中實施基於IP的內部Web策略。確保通過Security Services > Proxy Settings在安全Web裝置啟用「X-Forwarded-For」標頭。

[Home](#) | [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...](#)

2. 用於HTTP解密的受信任根證書。

- 如果在Umbrella控制面板中的Web策略上啟用HTTP解密，請從Umbrella控制面板>部署>配置下載「思科根證書」，並將其匯入到安全Web裝置受信任的根證書中。

Cisco S000V Web Security Virtual Appliance

Web Security Appliance is getting a new look.

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

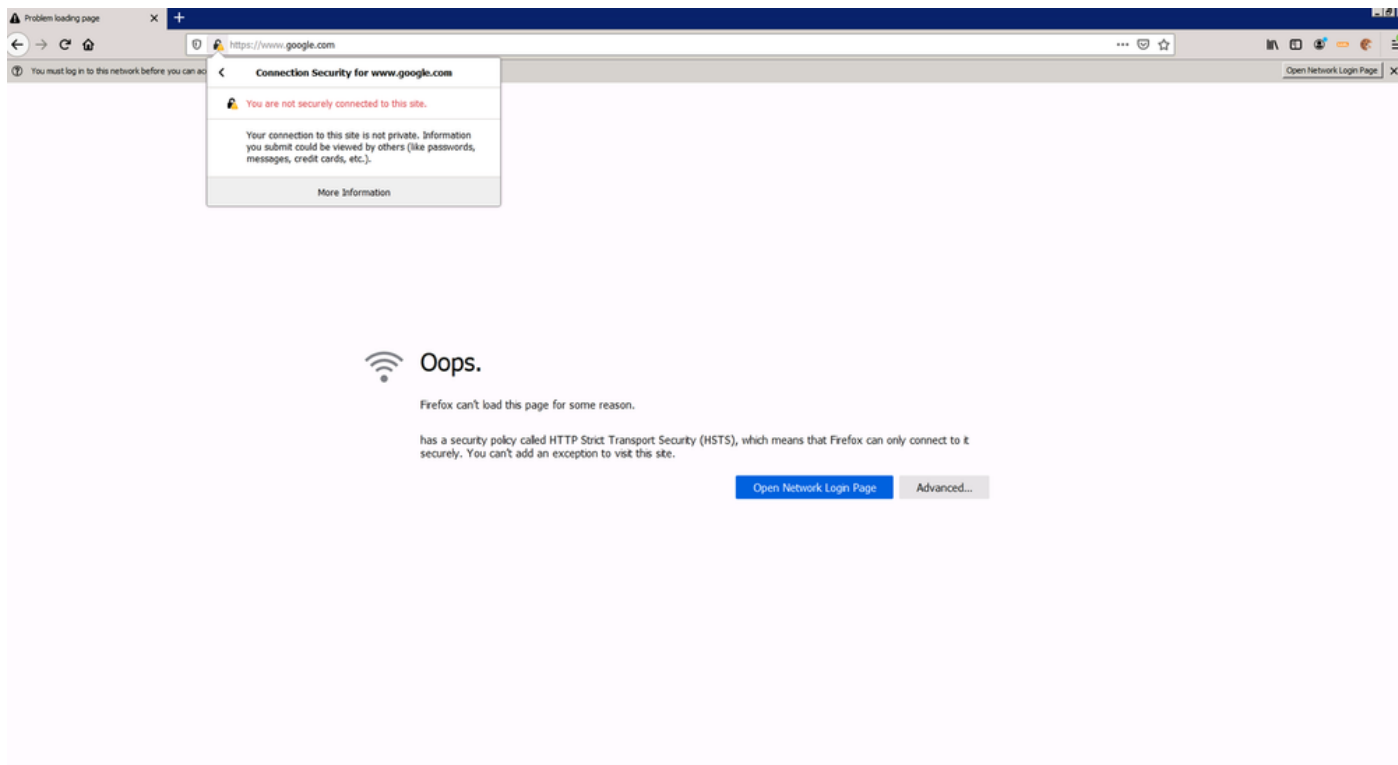
Cisco Trusted Root Certificate List (332 entries, 0 overridden)

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.

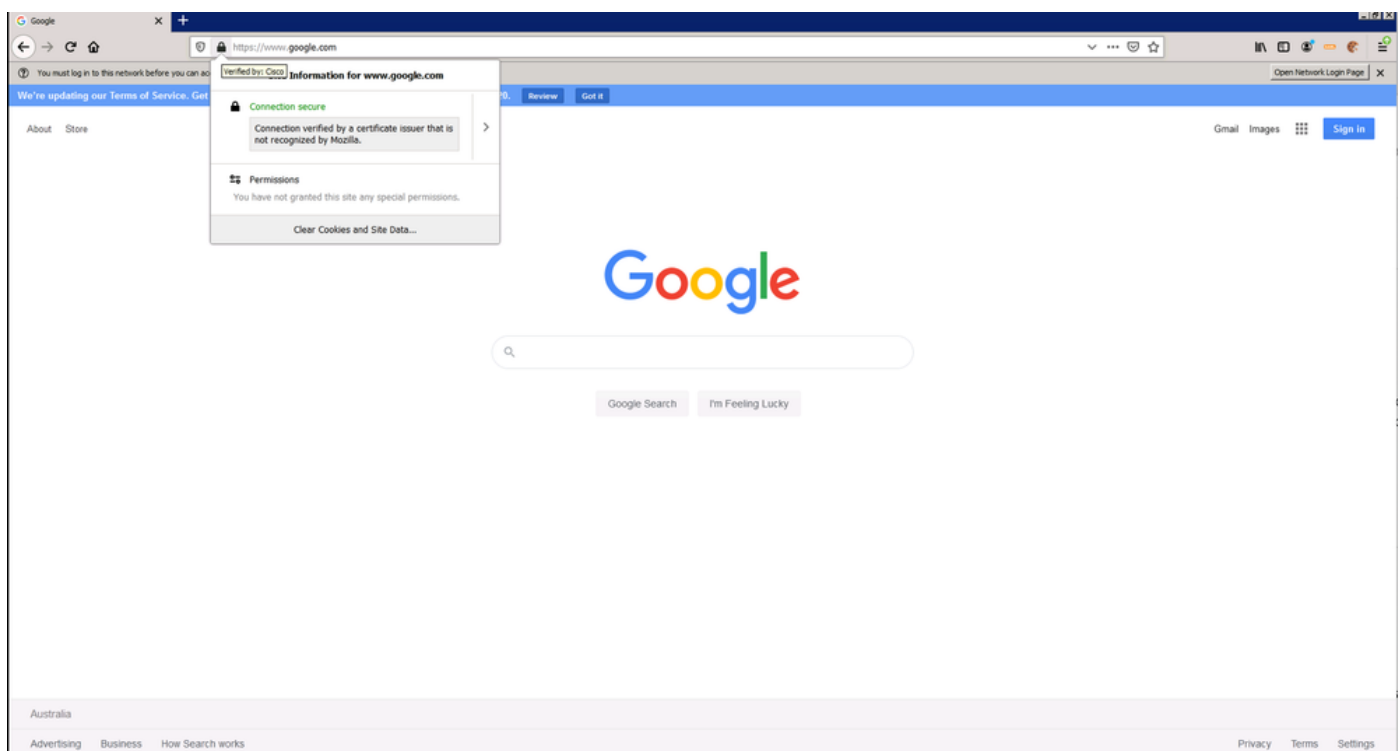
Certificate	Expiration Date	Override Trust ?
▸ (c) 1998 VeriSign, Inc. - For authorized use only	Aug 1 23:59:59 2028 GMT	☐
▸ A-Trust-nQual-03	Jul 23 08:38:29 2025 GMT	☐
▸ A-Trust-Qual-02	Jul 1 09:23:33 2024 GMT	☐
▸ A-Trust-Root-05	Sep 20 11:24:11 2023 GMT	☐
▸ AAA Certificate Services	Dec 31 23:59:59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

- 如果在SWG Web策略中啟用HTTPs解密時，「Cisco Root Certificate」（思科根證書）尚未匯入到安全Web裝置，則終端使用者會收到類似於以下示例的錯誤：
 - 「哎呀。（瀏覽器）由於某種原因無法載入此頁面。具有稱為HTTP Strict Transport Security(HSTS)的安全策略，這意味著（瀏覽器）只能安全連線到該策略。您不能新增例外來訪問此站點。」
 - 「您沒有安全連線到此站點。」



360050700171

- 以下是使用Umbrella SWG解密的HTTPs範例。憑證由名為「Cisco」的「Cisco Root Certificate」驗證。



360050700191

Umbrella控制面板中的SWG Web策略配置

基於內部IP的SWG Web策略：

- 確保啟用安全Web裝置中的「X-Forwarded-For」標頭，因為SWG依靠該標頭識別內部IP。
- 在Deployment > Networks中註冊安全Web裝置的輸出IP。
- 在部署>配置>內部網路中建立客戶端電腦的內部IP。在勾選/選擇「顯示網路」後，請選擇註冊的Secure Web Appliance出口IP（步驟1）。
- 根據步驟2中建立的內部IP建立新的Web策略。
- 確保Web策略中禁用了「啟用SAML」選項。

基於AD使用者/組的SWG Web策略：

- 確保所有AD使用者和組都調配到Umbrella控制面板。
- 在啟用「啟用SAML」選項的情況下，根據安全網路裝置的已註冊出口IP建立新的網路策略。
- 根據AD使用者/組建立另一個新的Web策略，並禁用「啟用SAML」選項。還需要將此Web策略置於第2步中建立的Web策略之前。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。