

Configurar a cadeia de proxy entre o Secure Web Appliance e o Umbrella SWG

Contents

[Introdução](#)

[Overview](#)

[Configuração de política do Secure Web Appliance](#)

[Para implantação transparente de proxy](#)

[Configuração da política da Web do SWG no painel Umbrella](#)

Introdução

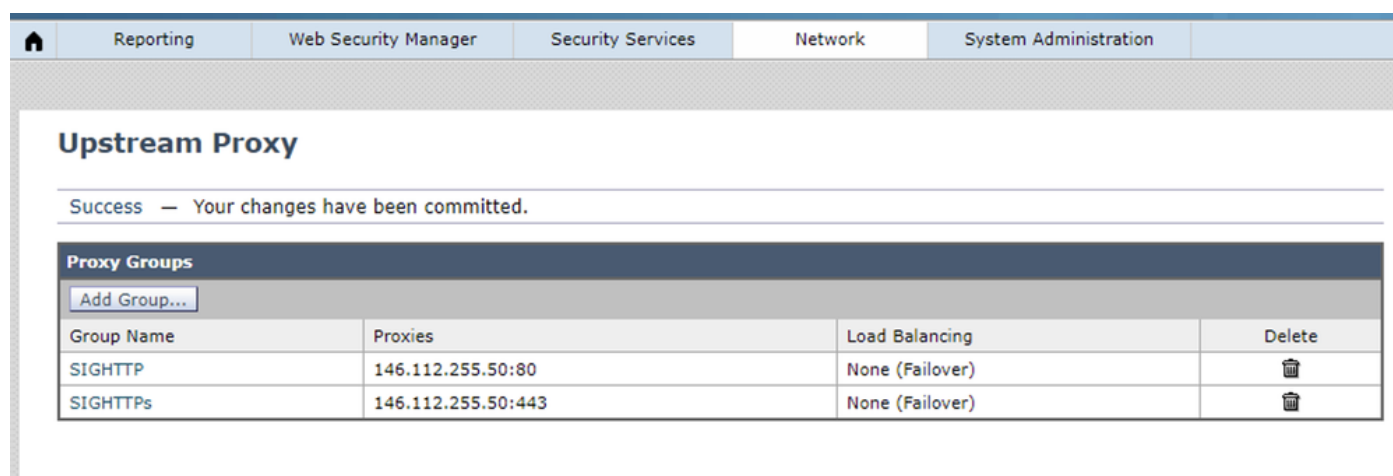
Este documento descreve como configurar a cadeia de proxy entre o Secure Web Appliance e o Umbrella Secure Web Gateway (SWG).

Overview

O Umbrella SIG suporta a cadeia de proxy e pode lidar com todas as solicitações HTTP/HTTPS do servidor proxy downstream. Este é um guia abrangente para implementar a cadeia de proxy entre o [Cisco Secure Web Appliance \(antigo Cisco WSA\)](#) e o [Umbrella Secure Web Gateway \(SWG\)](#), incluindo a configuração para o Secure Web Appliance e o SWG.

Configuração de política do Secure Web Appliance

1. Configure os links SWG HTTP e HTTPS como o Proxy de Upstream via Rede>Proxy de 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. Crie uma política de desvio através do Web Security Manager>Routing Policy para rotear todos

os URLs sugeridos diretamente para a Internet. Todos os URLs ignorados podem ser encontrados em nossa documentação: [Guia do usuário do Cisco Umbrella SIG: Gerenciar Encadeamento de Proxy](#)

- Comece criando uma nova "Categoria Personalizada" navegando até Web Security Manager>Categorias de URL Personalizadas e Externas, conforme mostrado aqui. A política de desvio é baseada na "Categoria Personalizada".

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

- Em seguida, crie uma nova política de desvio de roteamento navegando até Web Security Manager>Routing Policy. Certifique-se de que esta política seja a primeira, pois o Secure Web Appliance corresponde à política com base na ordem da 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. Crie uma nova política de roteamento para todas as solicitações HTTP.

- Na definição de membro da política de roteamento do Secure Web Appliance, as opções de protocolo são HTTP, FTP sobre HTTP, FTP nativo e "Todos os outros", enquanto "Todos os perfis de identificação" são selecionados. Como não há opção para HTTPs, crie a política de roteamento para solicitações HTTPs individualmente após implementar essa política de roteamento para todas as solicitações 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. Crie a política de roteamento para solicitações HTTPs com base no "Perfil de Identificação". Tenha cuidado com a sequência do "Perfil de identificação" definido, pois o Secure Web Appliance corresponde à "Identificação" da primeira correspondência. Neste exemplo, o perfil de identificação "win2k8" é uma identidade baseada em IP interno.

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles

Client / User Identification Profiles

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)	Delete

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

360050700091

5. Configurações finais para as Políticas de Roteamento do Secure Web Appliance:

- Tenha em mente que o Secure Web Appliance avalia as identidades e acessa as políticas usando uma abordagem de processamento de regras "de cima para baixo". Isso significa que a primeira correspondência feita em qualquer ponto no processamento resulta na ação tomada pelo Secure Web Appliance.
- Além disso, as identidades são avaliadas primeiro. Quando o acesso de um cliente corresponde a uma identidade específica, o Secure Web Appliance verifica todas as políticas de acesso configuradas para usar a identidade que corresponde ao acesso do 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	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

Note: A configuração de política mencionada é aplicável somente para Implantação de proxy explícito.

Para implantação transparente de proxy

No caso de HTTPS transparente, o AsyncOS não tem acesso às informações nos cabeçalhos do cliente. Portanto, o AsyncOS não pode aplicar políticas de roteamento se qualquer política de roteamento ou perfil de identificação depender das informações nos cabeçalhos do cliente.

1. Transações HTTPS redirecionadas de forma transparente só correspondem às Políticas de roteamento se:
 - O Grupo de Política de Roteamento não tem um critério de participação de política definido, como categoria de URL, Agente de Usuário etc.
 - O perfil de identificação não tem critérios de participação em políticas, como categoria de URL, agente de usuário etc. definidos.
2. Se qualquer Perfil de identificação ou Política de roteamento tiver uma categoria de URL personalizada definida, todas as transações HTTPS transparentes corresponderão ao Grupo de política de roteamento padrão.
3. Evite configurar a Política de Roteamento com Todos os Perfis de Identificação, pois isso pode fazer com que transações HTTPS transparentes correspondam ao Grupo de Política de Roteamento Padrão.

1. Cabeçalho X-Encaminhado-Para

- para implementar a política da Web baseada em IP interna no SWG. Certifique-se de habilitar o cabeçalho "X-Forwarded-For" no Secure Web Appliance via Security Services > Proxy Settings.

	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 raiz confiável para descriptografia de HTTPs.

- Se a descriptografia de HTTPs estiver habilitada em Web Policy no painel Umbrella, baixe "Cisco Root Certificate" do Umbrella dashboard> Deployments> Configuration e importe-o para os certificados raiz confiáveis do 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)

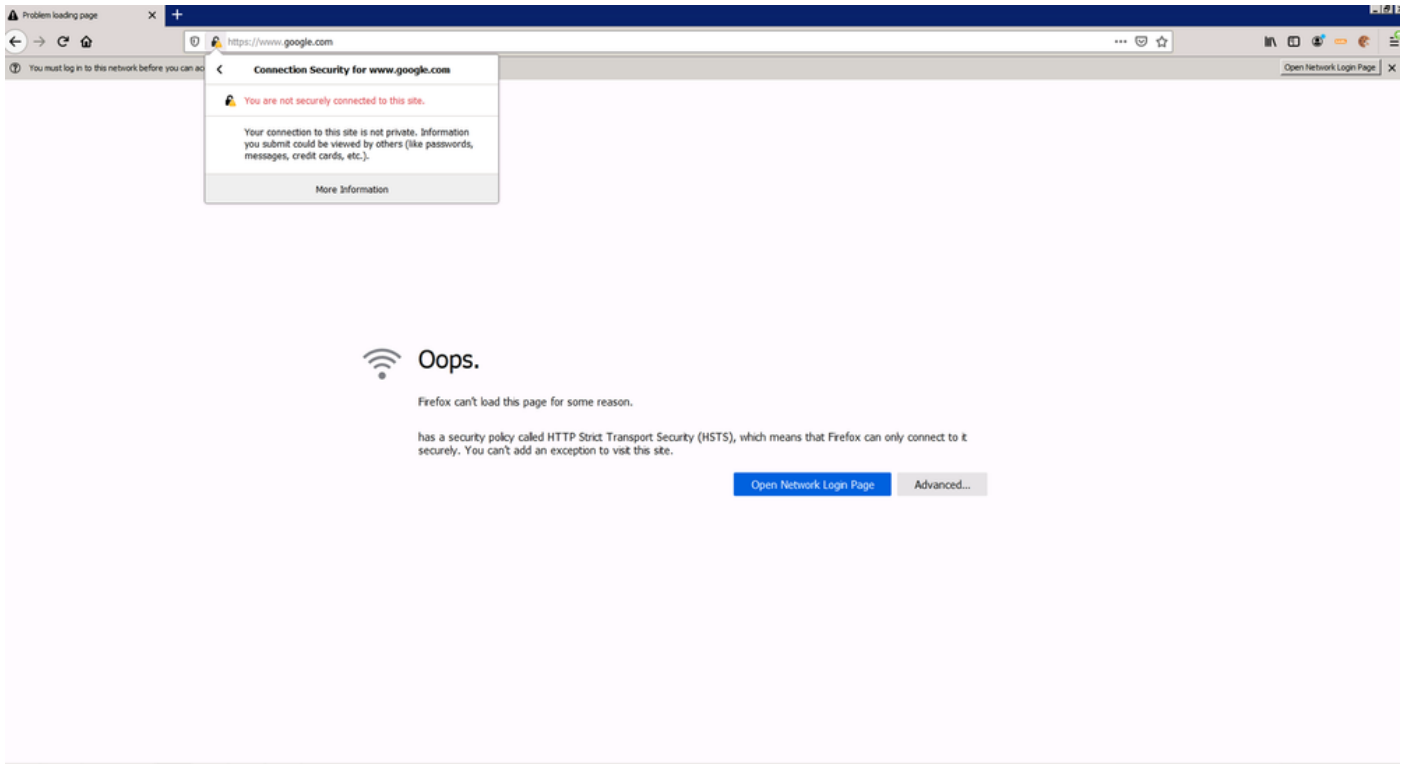
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

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	☐

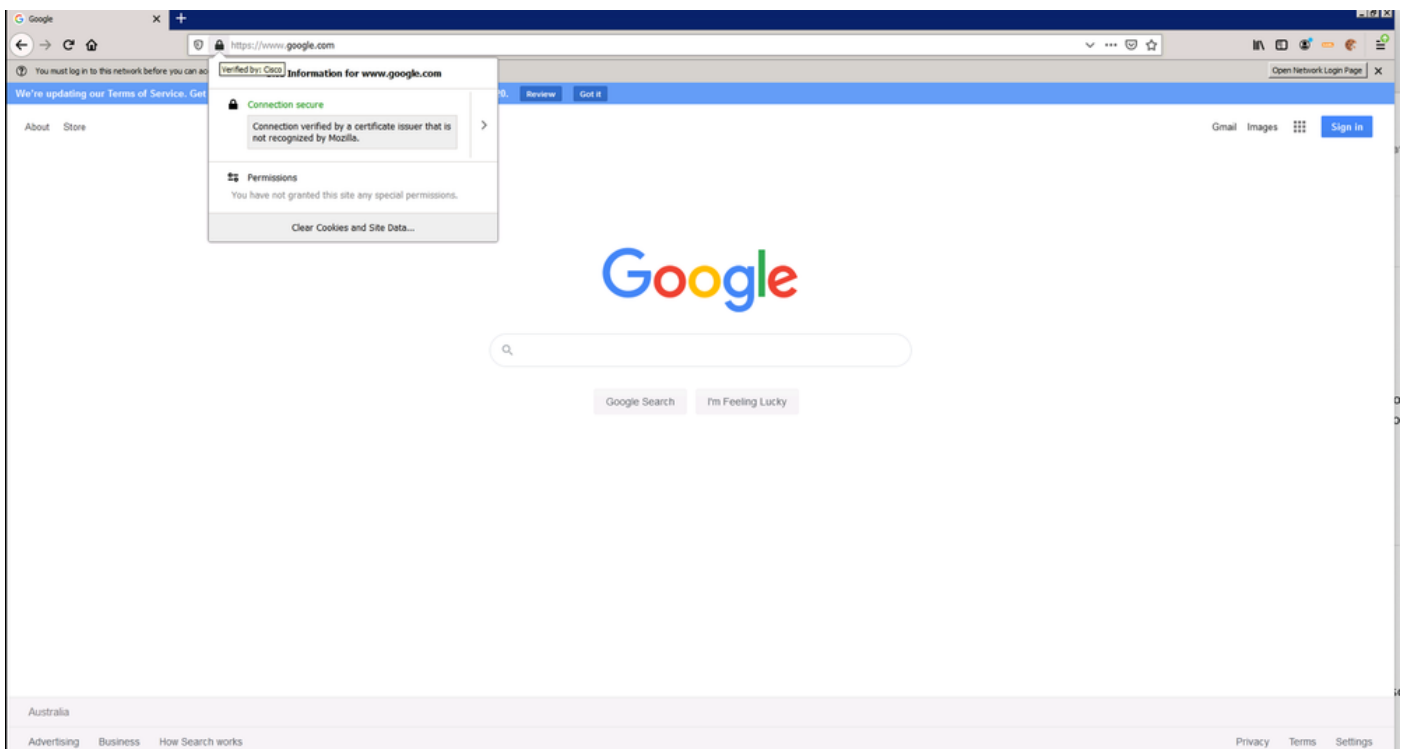
360050589612

- Se o "Certificado raiz da Cisco" não tiver sido importado para o Secure Web Appliance enquanto a descriptografia de HTTPs estiver habilitada na SWG Web Policy, o usuário final receberá um erro semelhante a este exemplo:
 - "Opa. (navegador) não pode carregar esta página por algum motivo. A tem uma política de segurança chamada HTTP Strict Transport Security (HSTS), o que significa que o (navegador) só pode se conectar a ele com segurança. Você não pode adicionar uma exceção para visitar este site."
 - "Você não está conectado com segurança a este site."



360050700171

- Este é um exemplo dos HTTPs descriptografados pelo Umbrella SWG. O certificado é verificado pelo "Certificado raiz da Cisco" chamado "Cisco".



360050700191

Configuração da política da Web do SWG no painel Umbrella

Política da Web do SWG baseada em IP interno:

- Certifique-se de habilitar o cabeçalho "X-Forwarded-For" no Secure Web Appliance, pois o SWG conta com ele para identificar o IP interno.
- Registre o IP de saída do Secure Web Appliance em Deployment > Networks.
- Crie um IP interno da máquina cliente em Deployment > Configuration > Internal Networks. Selecione o IP de saída registrado do Secure Web Appliance (Etapa 1) depois de marcar/selecionar "Mostrar redes".
- Crie uma nova Política da Web com base no IP interno criado na Etapa 2.
- Verifique se a opção "Habilitar SAML" está desabilitada na Política da Web.

Política da Web do SWG baseada em usuário/grupo do AD:

- Verifique se todos os usuários e grupos do AD foram provisionados no painel do Umbrella.
- Crie uma nova política da Web com base no IP de saída registrado do Secure Web Appliance com a opção "Enable SAML" ativada.
- Crie outra nova política da Web com base no usuário/grupo do AD com a opção "Habilitar SAML" desabilitada. Também é necessário posicionar essa política da Web antes da Política da Web criada na Etapa 2.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.