

Configureer de proxyketen tussen de Secure Web Appliance en de overkoepelende SWG

Inhoud

[Inleiding](#)

[Overzicht](#)

[Beleidsconfiguratie voor veilige webapparaten](#)

[Voor transparante proxyimplementatie](#)

[Configuratie van SWG-webbeleid in overkoepelend dashboard](#)

Inleiding

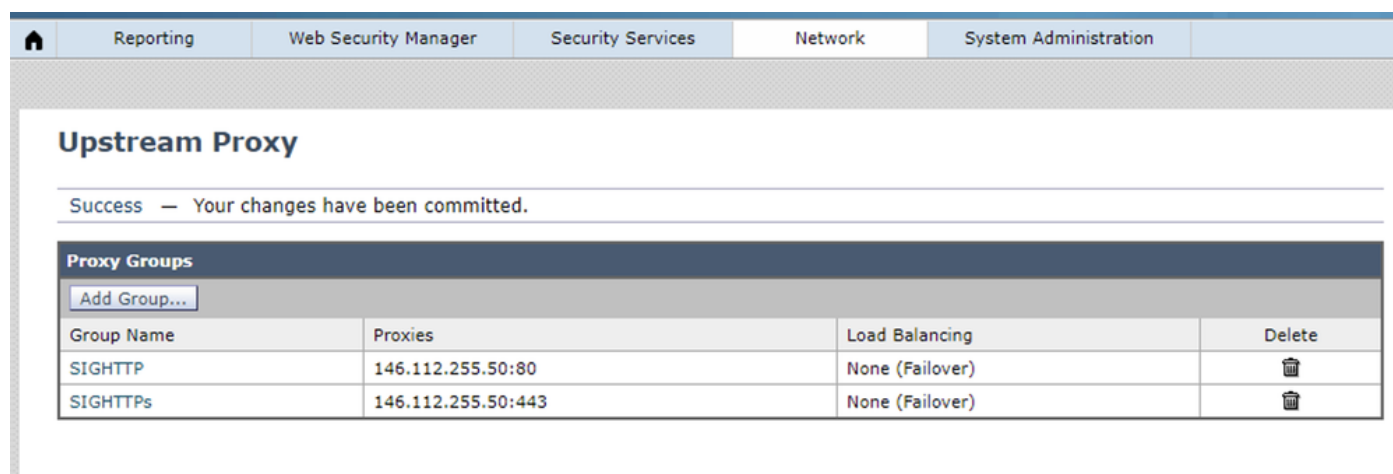
In dit document wordt beschreven hoe u de proxyketen tussen de Secure Web Appliance en de Umbrella Secure Web Gateway (SWG) configureert.

Overzicht

De Umbrella SIG ondersteunt de proxy-keten en kan alle HTTP / HTTP-verzoeken van de downstream-proxyserver afhandelen. Dit is een uitgebreide handleiding voor de implementatie van de proxyketen tussen [Cisco Secure Web Appliance \(voorheen Cisco WSA\)](#) en de [Umbrella Secure Web Gateway \(SWG\)](#), inclusief de configuratie voor zowel Secure Web Appliance als SWG.

Beleidsconfiguratie voor veilige webapparaten

1. Configureer de SWG HTTP- en HTTP-koppelingen als de 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)	

2. Maak een bypassbeleid via Web Security Manager>Routeringsbeleid om alle voorgestelde URL's rechtstreeks naar internet te routeren. Alle omzeilde URL's zijn te vinden in onze documentatie: [Cisco Umbrella SIG User Guide: Manage Proxy Chaining](#)

- Begin met het maken van een nieuwe "Aangepaste categorie" door te navigeren naar Web Security Manager>Aangepaste en Externe URL-categorieën zoals hier weergegeven. Het bypassbeleid is gebaseerd op de 'Aangepaste rubriek'.

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

- Maak vervolgens een nieuw bypass-routeringsbeleid door naar Web Security Manager>Routeringsbeleid te navigeren. Zorg ervoor dat dit beleid het eerste beleid is, aangezien Secure Web Appliance overeenkomt met het beleid op basis van de beleidsvolgorde.

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: 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:

User Agents: None Selected

Cancel Submit

360050703131

3. Maak een nieuw routeringsbeleid voor alle HTTP-verzoeken.

- In de leden definitie van het routeringsbeleid voor Secure Web Appliance zijn de protocolopties HTTP, FTP over HTTP, Native FTP en "All others", terwijl "All Identification Profiles" is geselecteerd. Aangezien er geen optie is voor HTTP's, maakt u het routeringsbeleid voor HTTP-aanvragen afzonderlijk nadat u dit routeringsbeleid voor alle HTTP-aanvragen hebt geïmplementeerd.

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

"Protocols" can only be selected while using "All Identification Profiles"

360050589572

4. Maak het routeringsbeleid voor HTTP-verzoeken op basis van het "Identificatieprofiel". Wees voorzichtig met de volgorde van het gedefinieerde "Identificatieprofiel", aangezien het Secure Web Appliance overeenkomt met de "Identificatie" voor de eerste match. In dit voorbeeld is het identificatieprofiel "win2k8" een interne op IP gebaseerde identiteit.

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

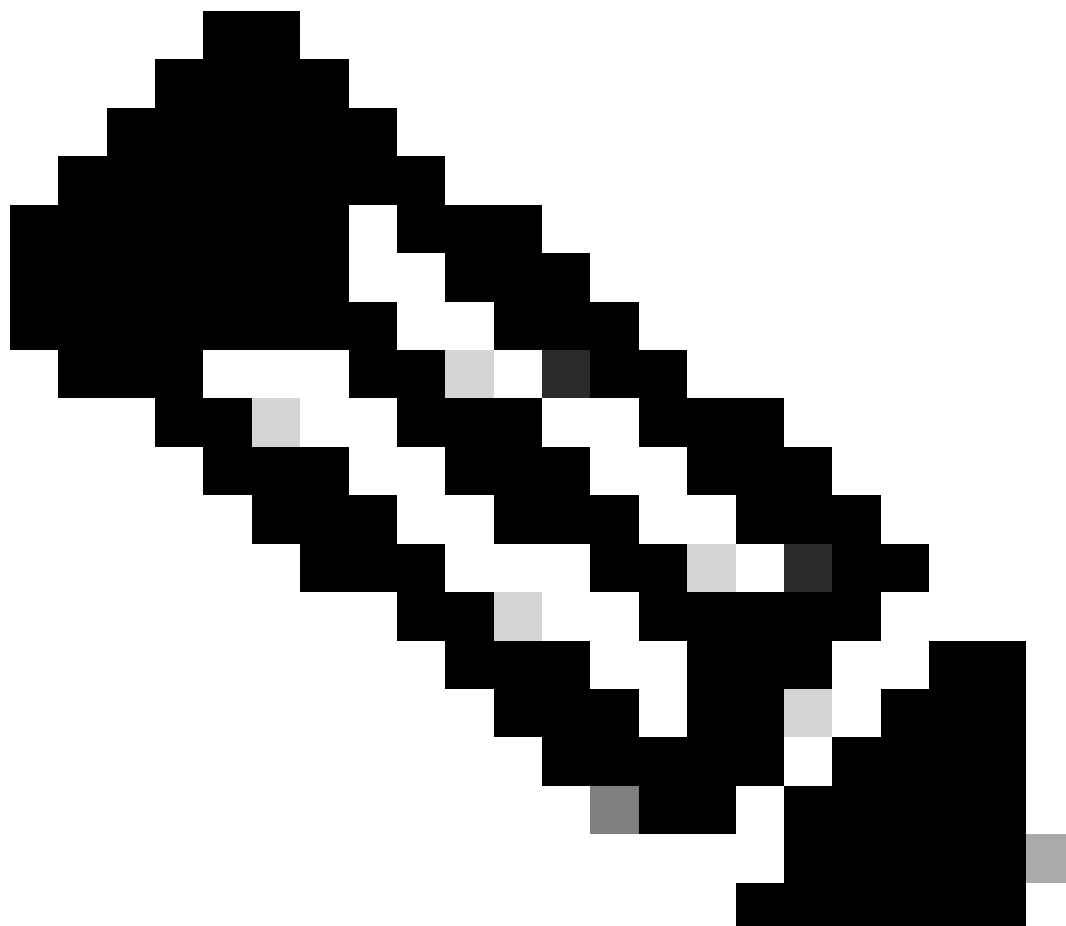
5. Definitieve configuraties voor het routeringsbeleid voor veilige webapparaten:

- Houd er rekening mee dat Secure Web Appliance de identiteit en het toegangsbeleid evalueert met behulp van een "top down"-regelverwerkingsaanpak. Dit betekent dat de eerste match die op enig moment in de verwerking wordt gemaakt, resulteert in de actie die door Secure Web Appliance wordt ondernomen.
- Identiteiten worden eerst beoordeeld. Zodra de toegang van een client overeenkomt met een specifieke identiteit, controleert Secure Web Appliance alle toegangsbeleidsregels die zijn geconfigureerd om de identiteit te gebruiken die overeenkomt met de toegang van de client.

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



Opmerking: de vermelde beleidsconfiguratie is alleen van toepassing voor de implementatie van expliciete proxy's.

Voor transparante proxyimplementatie

In het geval van transparante HTTPS heeft AsyncOS geen toegang tot informatie in de clientheaders. Daarom kan AsyncOS geen routeringsbeleid afdwingen als een routeringsbeleid of identificatieprofiel afhankelijk is van de informatie in de kopteksten van de client.

1. Transparant omgeleide HTTPS-transacties komen alleen overeen met het routeringsbeleid als:
 - Routing Policy Group heeft geen lidmaatschapscriteria voor beleid zoals URL-categorie, User Agent, enzovoort.
 - Identificatieprofiel heeft geen lidmaatschapscriteria voor beleid, zoals URL-categorie, User Agent, enzovoort.
2. Als in een identificatieprofiel of routeringsbeleid een aangepaste URL-categorie is gedefinieerd, komen alle transparante HTTPS-transacties overeen met de standaardgroep voor routeringsbeleid.
3. Vermijd zoveel mogelijk het configureren van het routeringsbeleid met alle identificatieprofielen, omdat dit ertoe kan leiden dat transparante HTTPS-transacties overeenkomen met de standaardgroep voor routeringsbeleid.

1. X-forwarding voor koptekst

- om het interne IP-gebaseerde webbeleid in SWG te implementeren. Zorg ervoor dat u de koptekst "X-Forwarding-For" inschakelt in Secure Web Appliance via Beveiligingsservices > Proxyinstellingen.

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...

360050700111

2. Vertrouwd basiscertificaat voor HTTP-decodering.

- Als de HTTP-decodering is ingeschakeld bij Webbeleid in het overkoepelende dashboard, downloadt u "Cisco Root Certificate" van het overkoepelende dashboard> Implementaties> Configuratie en importeert u het in de vertrouwde basiscertificaten van 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)

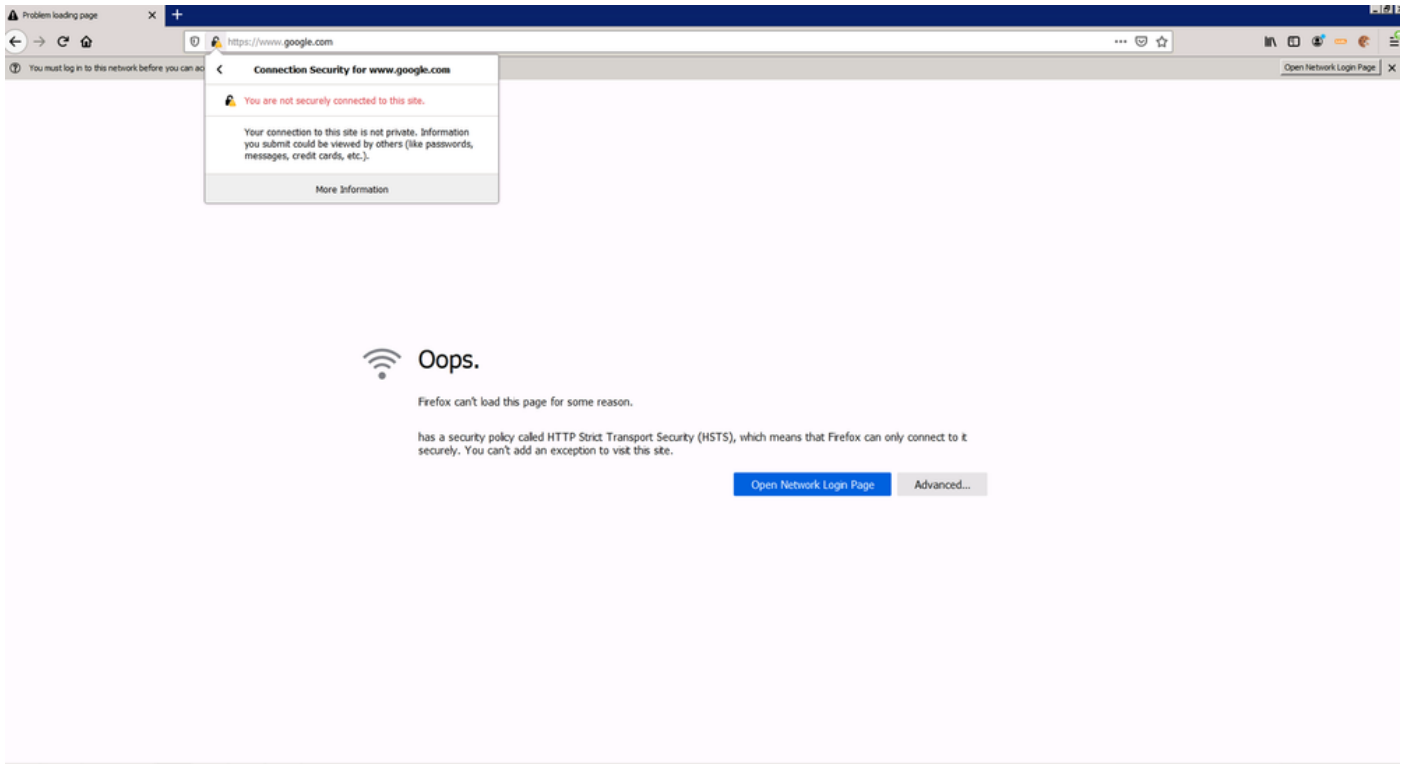
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

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	☐

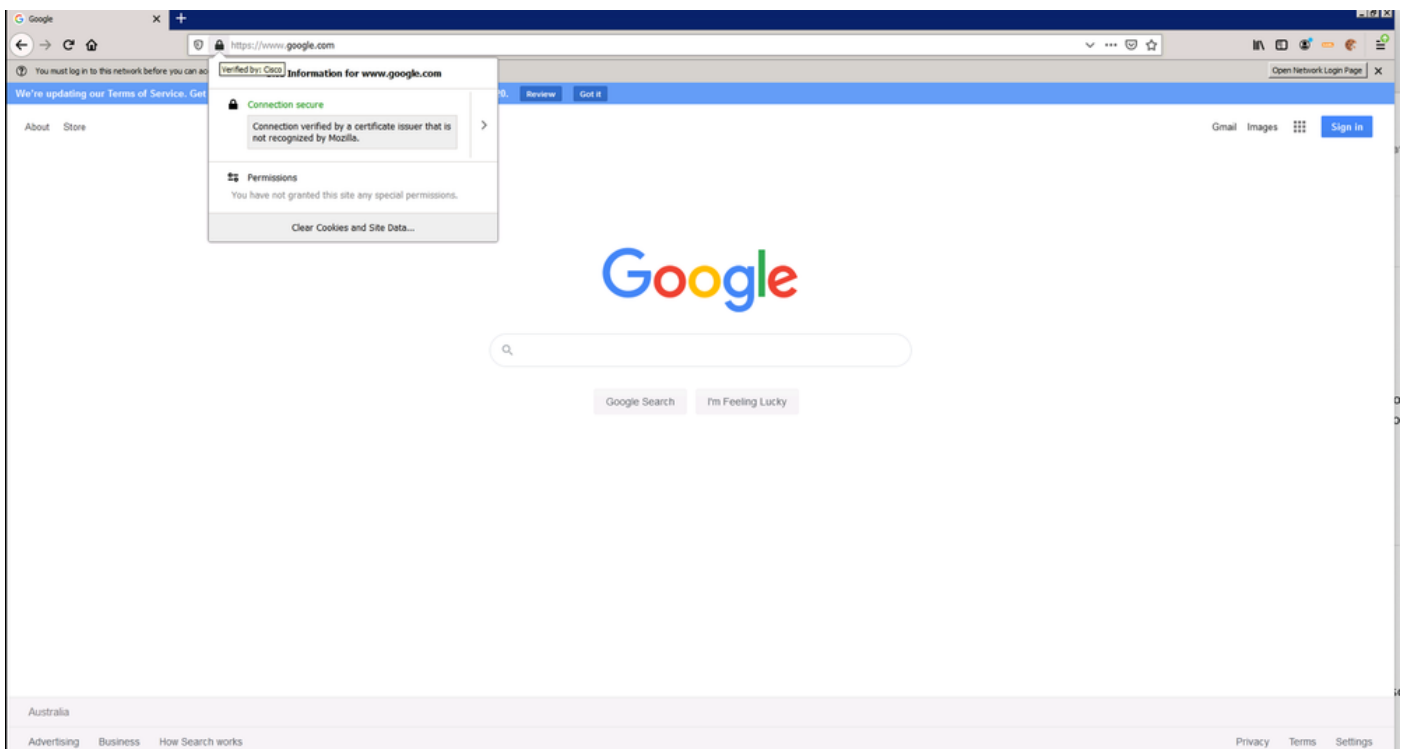
360050589612

- Als het "Cisco Root Certificate" niet is geïmporteerd in de Secure Web Appliance terwijl de HTTPS-decodering is ingeschakeld in SWG Web Policy, krijgt de eindgebruiker een fout die vergelijkbaar is met dit voorbeeld:
 - "Oeps. (browser) kan deze pagina om een of andere reden niet laden. heeft een beveiligingsbeleid genaamd HTTP Strict Transport Security (HSTS), wat betekent dat (browser) er alleen veilig verbinding mee kan maken. Je kunt geen uitzondering toevoegen om deze site te bezoeken."
 - "Je bent niet veilig verbonden met deze site."



360050700171

- Dit is een voorbeeld van de HTTP's die zijn gedecodeerd door Umbrella SWG. Het certificaat wordt geverifieerd door het "Cisco Root Certificate" met de naam "Cisco".



360050700191

Configuratie van SWG-webbeleid in overkoepelend dashboard

SWG-webbeleid op basis van interne IP:

- Zorg ervoor dat u de "X-Forwarding-For" -header inschakelt in de Secure Web Appliance, omdat SWG daarop vertrouwt om het interne IP-adres te identificeren.
- Registreer de IP-uitgang van de Secure Web Appliance in Implementatie > Netwerken.
- Maak een intern IP-adres van het clientsysteem in Implementatie > Configuratie > Interne netwerken. Selecteer de geregistreerde Secure Web Appliance-uitgang IP (stap 1) nadat u "Netwerken weergeven" hebt aangevinkt/geselecteerd.
- Maak een nieuw webbeleid op basis van het interne IP-adres dat in stap 2 is gemaakt.
- Zorg ervoor dat de optie "SAML inschakelen" is uitgeschakeld in het webbeleid.

SWG-webbeleid op basis van AD-gebruiker/groep:

- Zorg ervoor dat alle AD-gebruikers en -groepen zijn voorzien van het Umbrella-dashboard.
- Maak een nieuw webbeleid op basis van de geregistreerde IP-uitgang van de Secure Web Appliance met de optie "SAML inschakelen" ingeschakeld.
- Maak een ander nieuw webbeleid op basis van de AD-gebruiker/groep met de optie "SAML inschakelen" uitgeschakeld. U moet dit webbeleid ook vóór het webbeleid plaatsen dat in stap 2 is gemaakt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.