

Configuration de la chaîne proxy entre l'appliance Web sécurisée et le SWG Umbrella

Table des matières

[Introduction](#)

[Aperçu](#)

[Configuration de la stratégie Secure Web Appliance](#)

[Pour un déploiement transparent du proxy](#)

[Configuration de la stratégie Web SWG dans le tableau de bord Umbrella](#)

Introduction

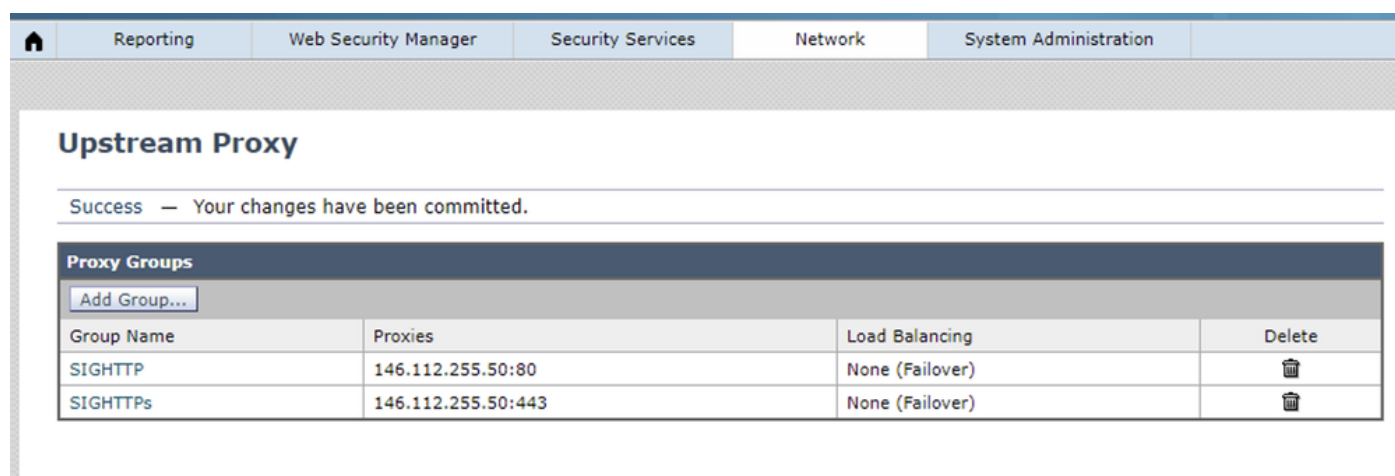
Ce document décrit comment configurer la chaîne proxy entre l'appareil Web sécurisé et la passerelle Web sécurisée (SWG) Umbrella.

Aperçu

Umbrella SIG prend en charge la chaîne proxy et peut gérer toutes les requêtes HTTP/HTTPS du serveur proxy en aval. Ce guide complet permet de mettre en oeuvre la chaîne de proxy entre l'[appareil Web sécurisé Cisco \(anciennement Cisco WSA\)](#) et la [passerelle Web sécurisée Umbrella \(SWG\)](#), y compris la configuration de l'appareil Web sécurisé et du SWG.

Configuration de la stratégie Secure Web Appliance

1. Configurez les liaisons HTTP et HTTPS SWG en tant que proxy en amont via Réseau>Proxy en amont.



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

360079596451

2. Créez une stratégie de contournement via Web Security Manager>Routing Policy pour router

directement vers Internet toutes les URL suggérées. Toutes les URL contournées se trouvent dans notre documentation : [Guide de l'utilisateur de Cisco Umbrella SIG : Gérer le chaînage proxy](#)

- Commencez par créer une nouvelle « Catégorie personnalisée » en accédant à Gestionnaire de sécurité Web>Catégories d'URL personnalisées et externes comme indiqué ici. La stratégie de contournement est basée sur la « Catégorie personnalisée ».

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

- Créez ensuite une nouvelle stratégie de routage de contournement en naviguant vers Gestionnaire de sécurité Web>Stratégie de routage. Assurez-vous que cette stratégie est la première car l'appliance Web sécurisée correspond à la stratégie basée sur l'ordre de la stratégie.

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. Créez une nouvelle stratégie de routage pour toutes les requêtes HTTP.

- Dans la définition de membre de stratégie de routage Secure Web Appliance, les options de protocole sont HTTP, FTP sur HTTP, Native FTP et « All others », tandis que « All Identification Profiles » est sélectionné. Puisqu'il n'y a pas d'option pour les requêtes HTTP, créez la stratégie de routage pour les requêtes HTTP individuellement après avoir implémenté cette stratégie de routage pour toutes les requêtes 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. Créez la stratégie de routage pour les demandes HTTP en fonction du « profil d'identification ». Soyez prudent avec la séquence du « profil d'identification » défini, car l'appareil Web sécurisé correspond à l'« identification » de la première correspondance. Dans cet exemple, le profil d'identification « win2k8 » est une identité IP interne.

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

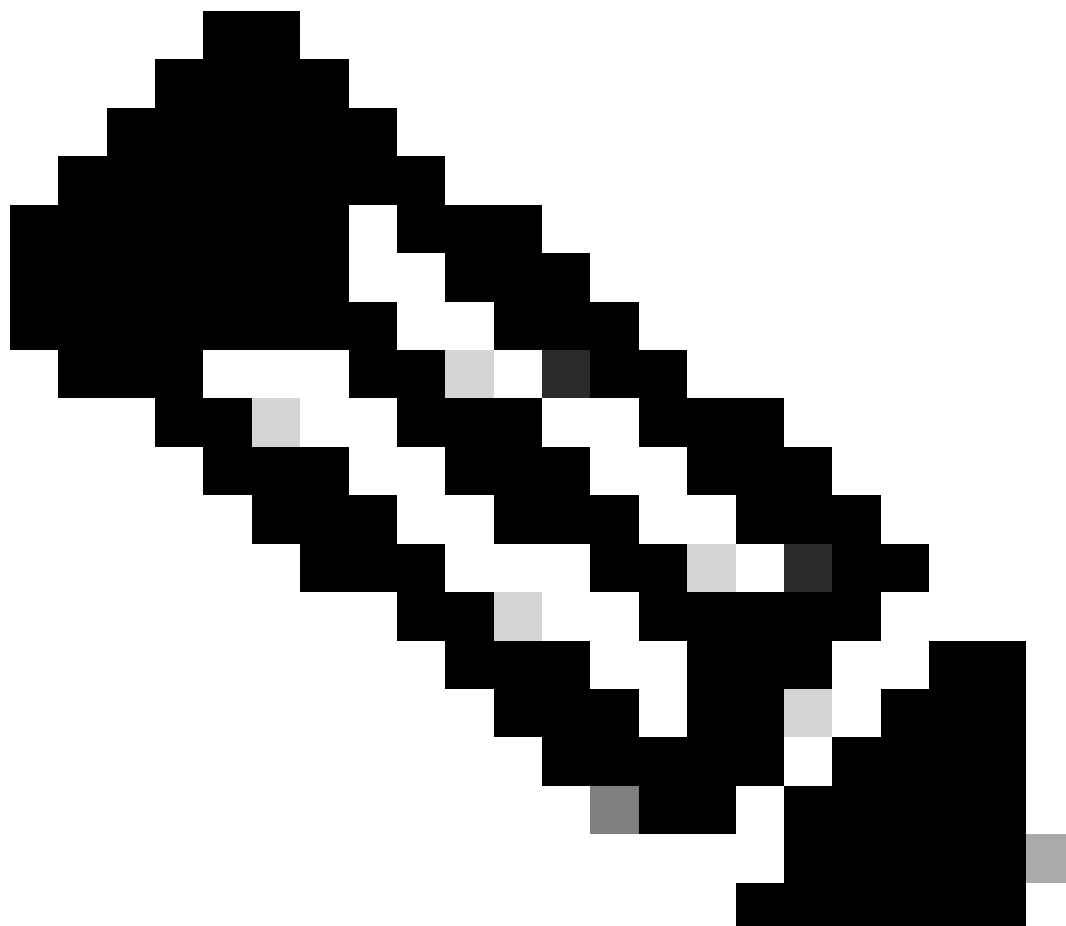
5. Configurations finales des politiques de routage de l'appliance Web sécurisé :

- Gardez à l'esprit que Secure Web Appliance évalue les identités et les stratégies d'accès à l'aide d'une approche de traitement de règle « descendante ». Cela signifie que la première correspondance effectuée à un point quelconque du traitement entraîne l'action entreprise par Secure Web Appliance.
- En outre, les identités sont évaluées en premier. Une fois que l'accès d'un client correspond à une identité spécifique, l'appliance Web sécurisée vérifie toutes les stratégies d'accès qui sont configurées pour utiliser l'identité qui correspond à l'accès du 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



Remarque : La configuration de stratégie mentionnée s'applique uniquement au déploiement de proxy explicite.

Pour un déploiement transparent du proxy

Dans le cas du protocole HTTPS transparent, AsyncOS n'a pas accès aux informations contenues dans les en-têtes client. Par conséquent, AsyncOS ne peut pas appliquer de stratégies de routage si une stratégie de routage ou un profil d'identification repose sur les informations contenues dans les en-têtes client.

1. Les transactions HTTPS redirigées de manière transparente correspondent uniquement aux politiques de routage si :
 - Le groupe de stratégies de routage n'a pas de critères d'appartenance à une stratégie tels que la catégorie d'URL, l'agent utilisateur, etc. définis.
 - Aucun critère d'appartenance à la stratégie, tel que la catégorie d'URL, l'agent utilisateur, etc., n'est défini pour le profil d'identification.
2. Si une catégorie d'URL personnalisée est définie pour un profil d'identification ou une stratégie de routage, toutes les transactions HTTPS transparentes correspondent au groupe de stratégies de routage par défaut.
3. Dans la mesure du possible, évitez de configurer la stratégie de routage avec tous les profils d'identification, car cela pourrait entraîner une correspondance entre les transactions HTTPS transparentes et le groupe de stratégie de routage par défaut.

1. En-Tête X-Forwarded-For

- pour implémenter la stratégie Web IP interne dans SWG. Assurez-vous d'activer l'en-tête « X-Forwarded-For » dans l'appliance Web sécurisé via Services de sécurité > Paramètres du 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. Certificat racine de confiance pour le déchiffrement HTTP.

- Si le déchiffrement HTTP est activé au niveau de la stratégie Web dans le tableau de bord Umbrella, téléchargez « Certificat racine Cisco » à partir du tableau de bord Umbrella > Déploiements > Configuration et importez-le dans les certificats racines de confiance de l'appliance Web sécurisée.

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)

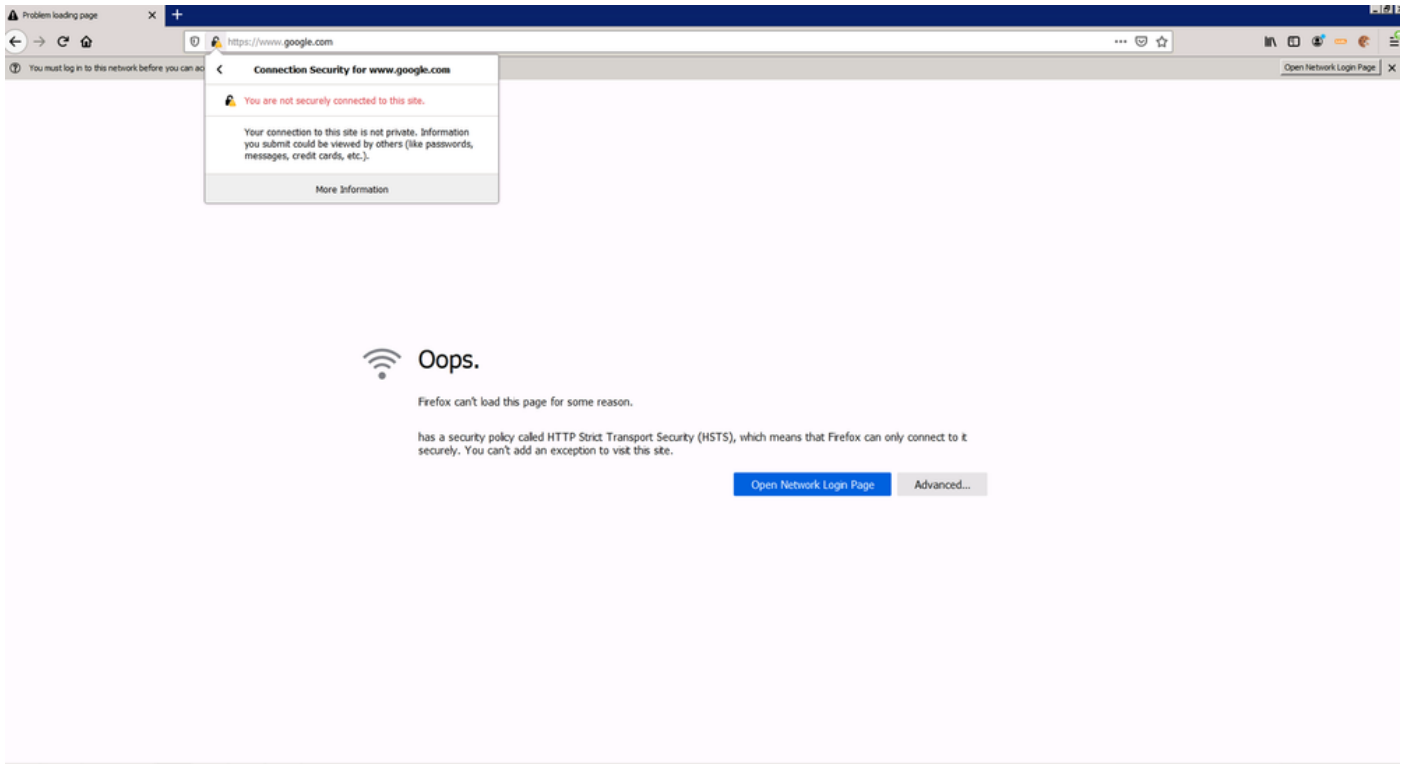
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

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	☐

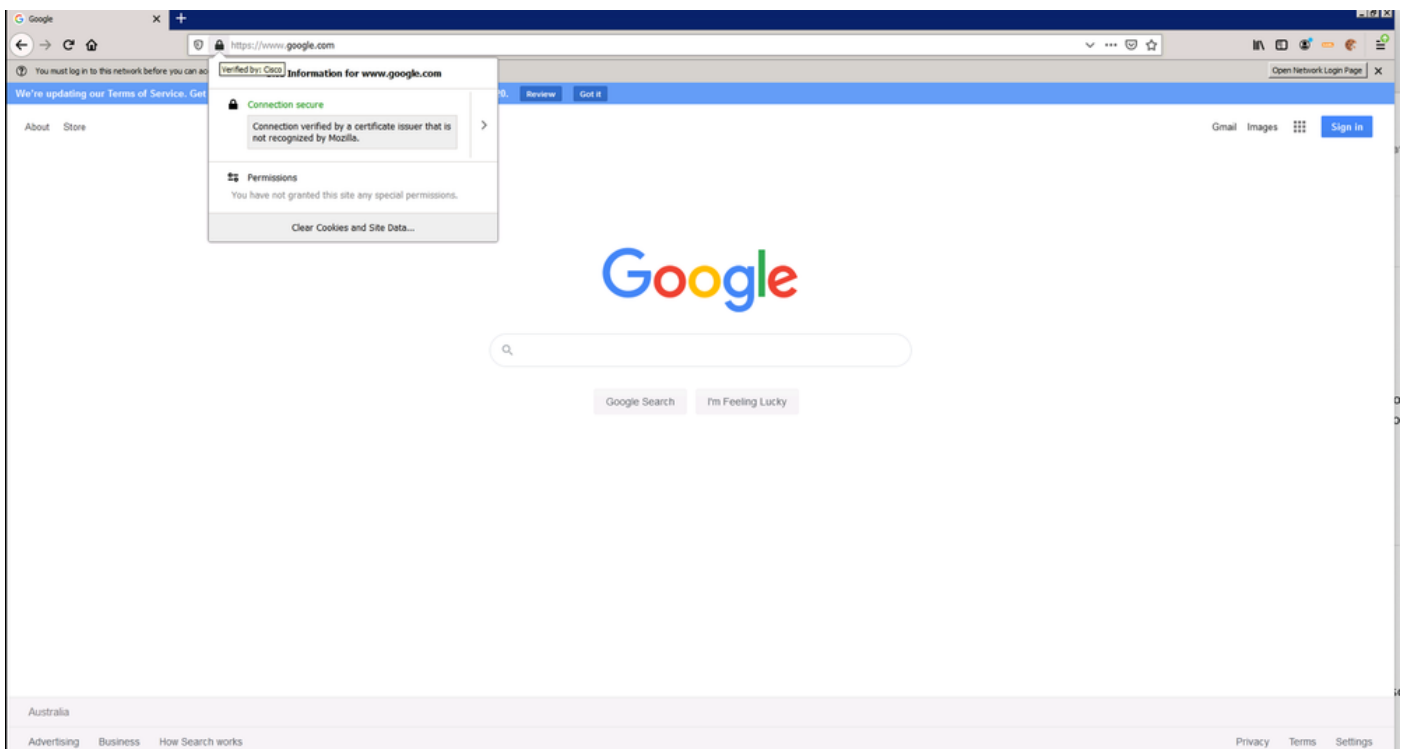
360050589612

- Si le « certificat racine Cisco » n'a pas été importé dans l'appareil Web sécurisé alors que le déchiffrement HTTP est activé au niveau de la stratégie Web SWG, l'utilisateur final reçoit une erreur semblable à celle de l'exemple suivant :
 - "Oups. (navigateur) ne peut pas charger cette page pour une raison quelconque. dispose d'une stratégie de sécurité appelée HTTP Strict Transport Security (HSTS), ce qui signifie que (navigateur) ne peut s'y connecter que de manière sécurisée. Vous ne pouvez pas ajouter d'exception pour visiter ce site."
 - "Vous n'êtes pas connecté à ce site de manière sécurisée."



360050700171

- Ceci est un exemple des HTTP déchiffrés par Umbrella SWG. Le certificat est vérifié par le « certificat racine Cisco » nommé « Cisco ».



360050700191

Configuration de la stratégie Web SWG dans le tableau de bord Umbrella

Politique Web SWG basée sur IP interne :

- Assurez-vous d'activer l'en-tête « X-Forwarded-For » dans l'appliance Web sécurisé, car SWG s'appuie sur ce dernier pour identifier l'adresse IP interne.
- Enregistrez l'adresse IP de sortie de l'appliance Web sécurisée dans Déploiement > Réseaux.
- Créez une adresse IP interne de l'ordinateur client dans Déploiement > Configuration > Réseaux internes. Sélectionnez l'adresse IP de sortie de l'appliance Web sécurisé enregistrée (étape 1) après avoir coché/sélectionné « Afficher les réseaux ».
- Créez une nouvelle stratégie Web basée sur l'adresse IP interne créée à l'étape 2.
- Assurez-vous que l'option « Activer SAML » est désactivée dans la stratégie Web.

Stratégie Web SWG basée sur l'utilisateur/le groupe AD :

- Assurez-vous que tous les utilisateurs et groupes AD sont provisionnés dans le tableau de bord Umbrella.
- Créez une nouvelle stratégie Web basée sur l'adresse IP de sortie enregistrée de l'appareil Web sécurisé avec l'option « Activer SAML » activée.
- Créez une autre stratégie Web basée sur l'utilisateur/groupe AD avec l'option « Activer SAML » désactivée. Vous devez également placer cette stratégie Web avant la stratégie Web créée à l'étape 2.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.