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

Table des matières

Introduction

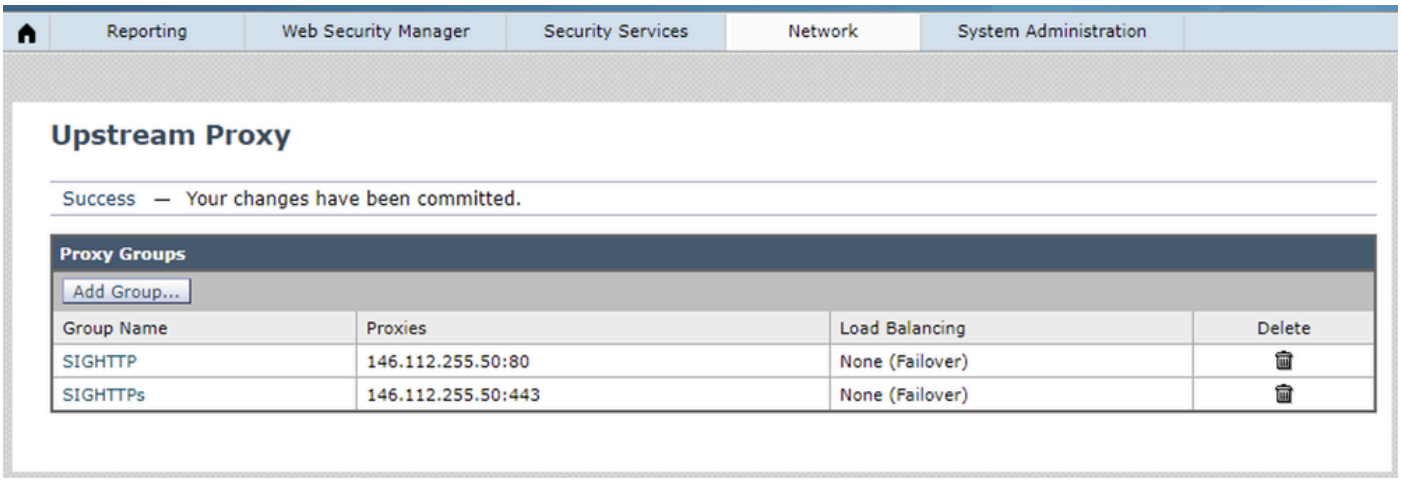
Ce document décrit comment configurer la chaîne proxy entre l'appareil Web sécurisé et la passerelle Web sécurisée (SWG) Umbrella.

Aperçu

Umbrella SIG prend en charge la chaîne proxy et peut gérer toutes les requêtes HTTP/HTTP 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 HTTP SWG en tant que proxy en amont via Réseau>Proxy en amont.

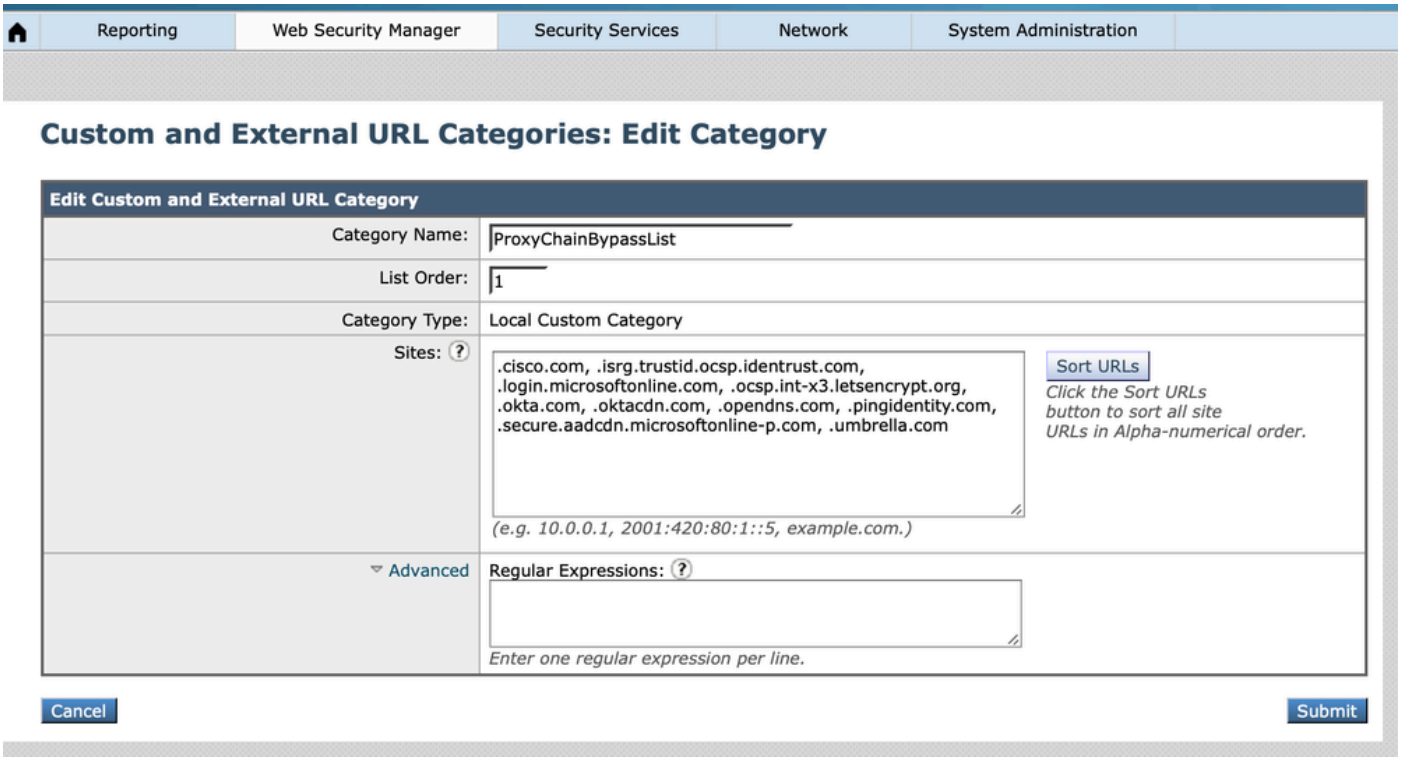


360079596451

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

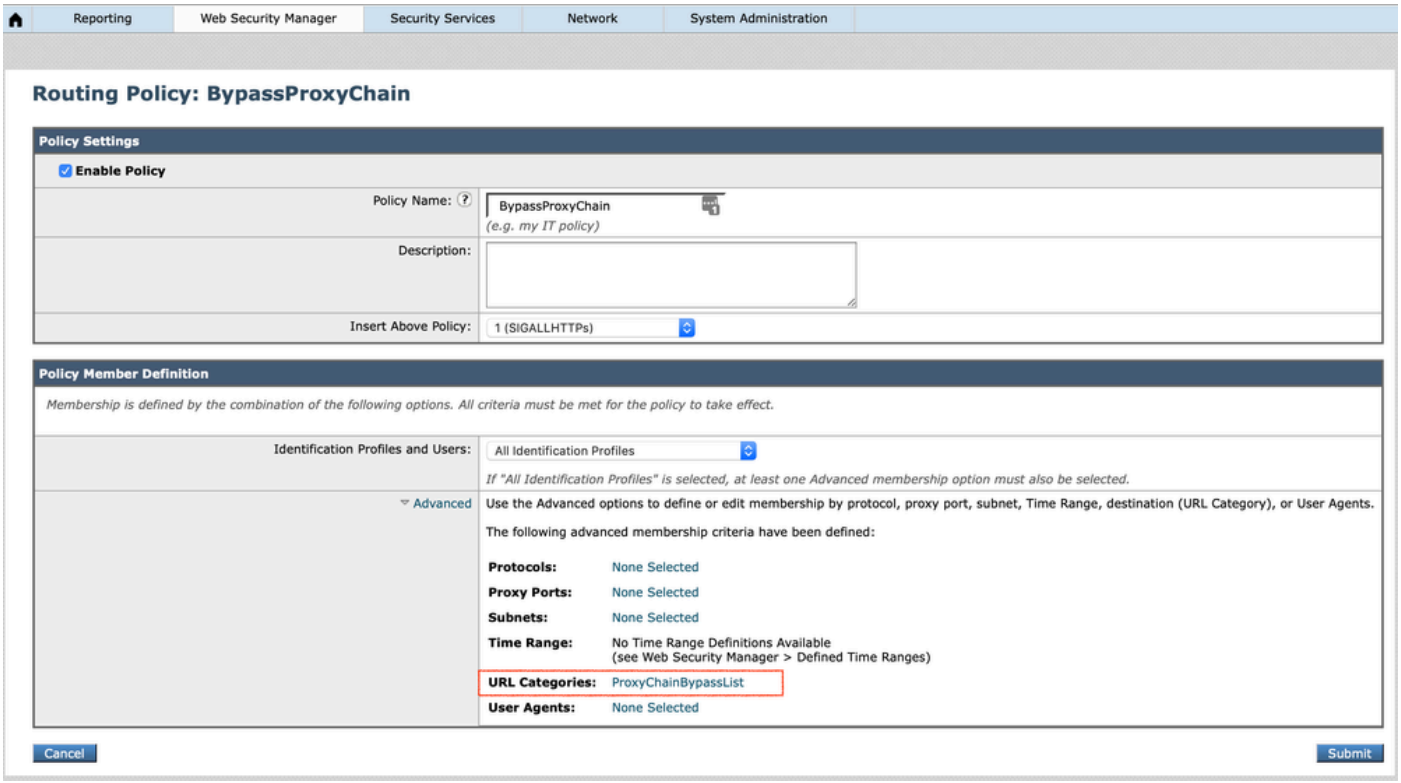
directement vers Internet toutes les URL suggérées. Toutes les URL contournées se trouvent dans notre documentation : [Guide de l'utilisateur de Cisco Umbrella SIG : Gérer le chaînage proxy]

- 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 ».



360050592552

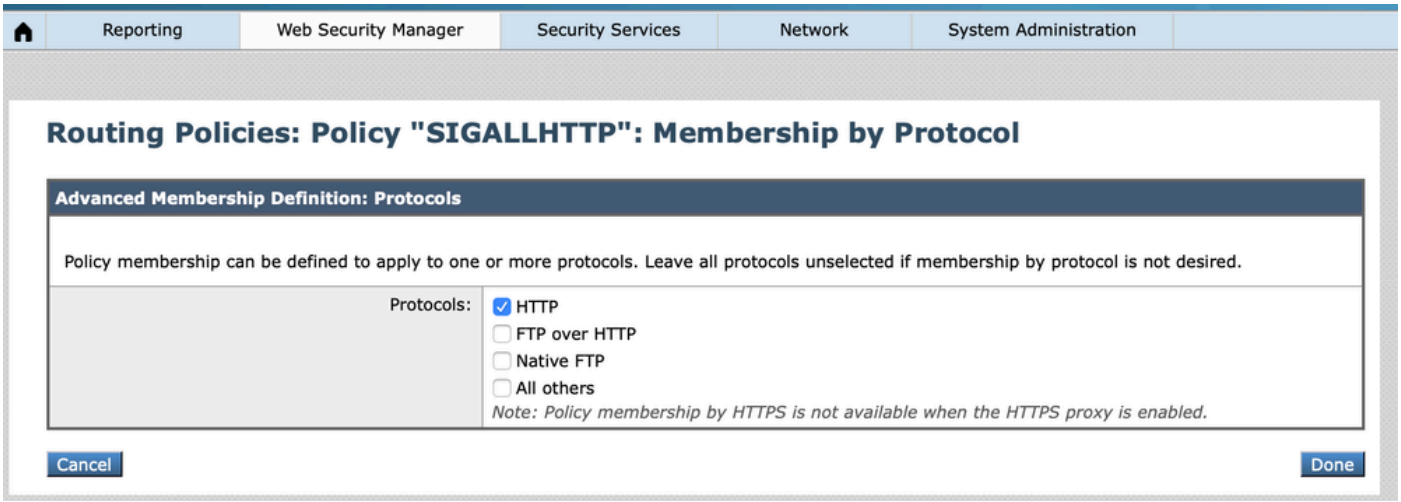
- Créez ensuite une nouvelle stratégie de routage de contournement en naviguant vers Gestionnaire de sécurité Web>Stratégie de routage. Assurez-vous que cette stratégie est la première car l'appliance Web sécurisée correspond à la stratégie basée sur l'ordre de la stratégie.



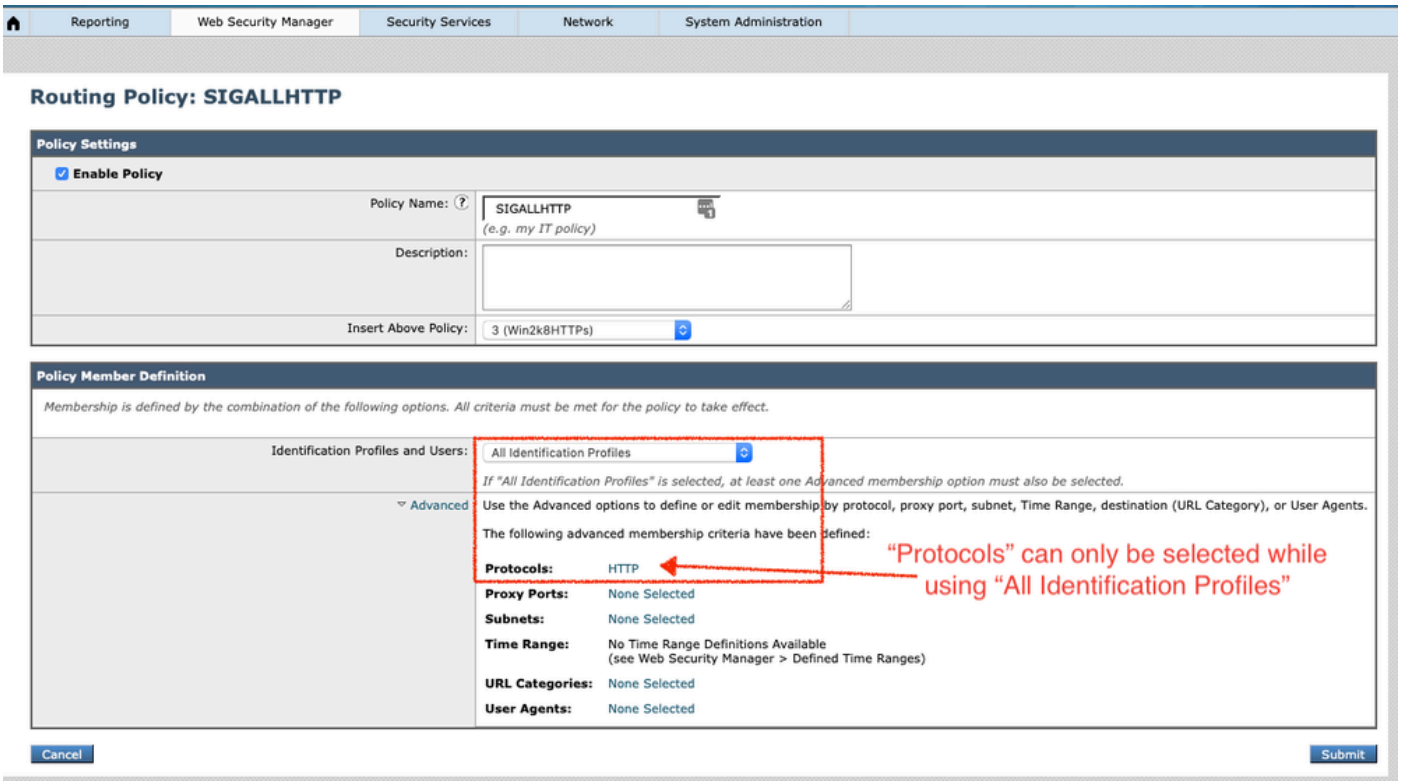
360050703131

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.

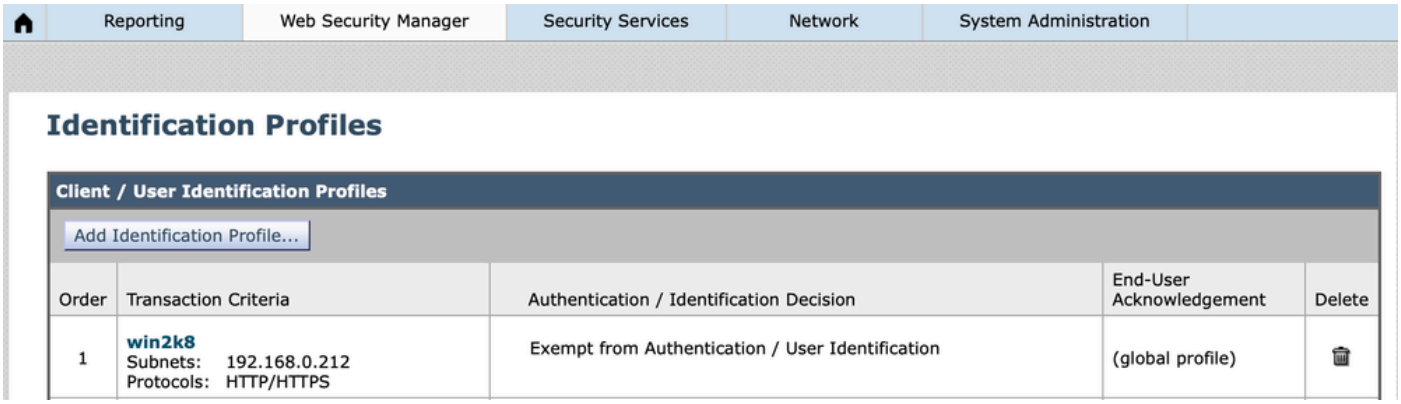


360050592772

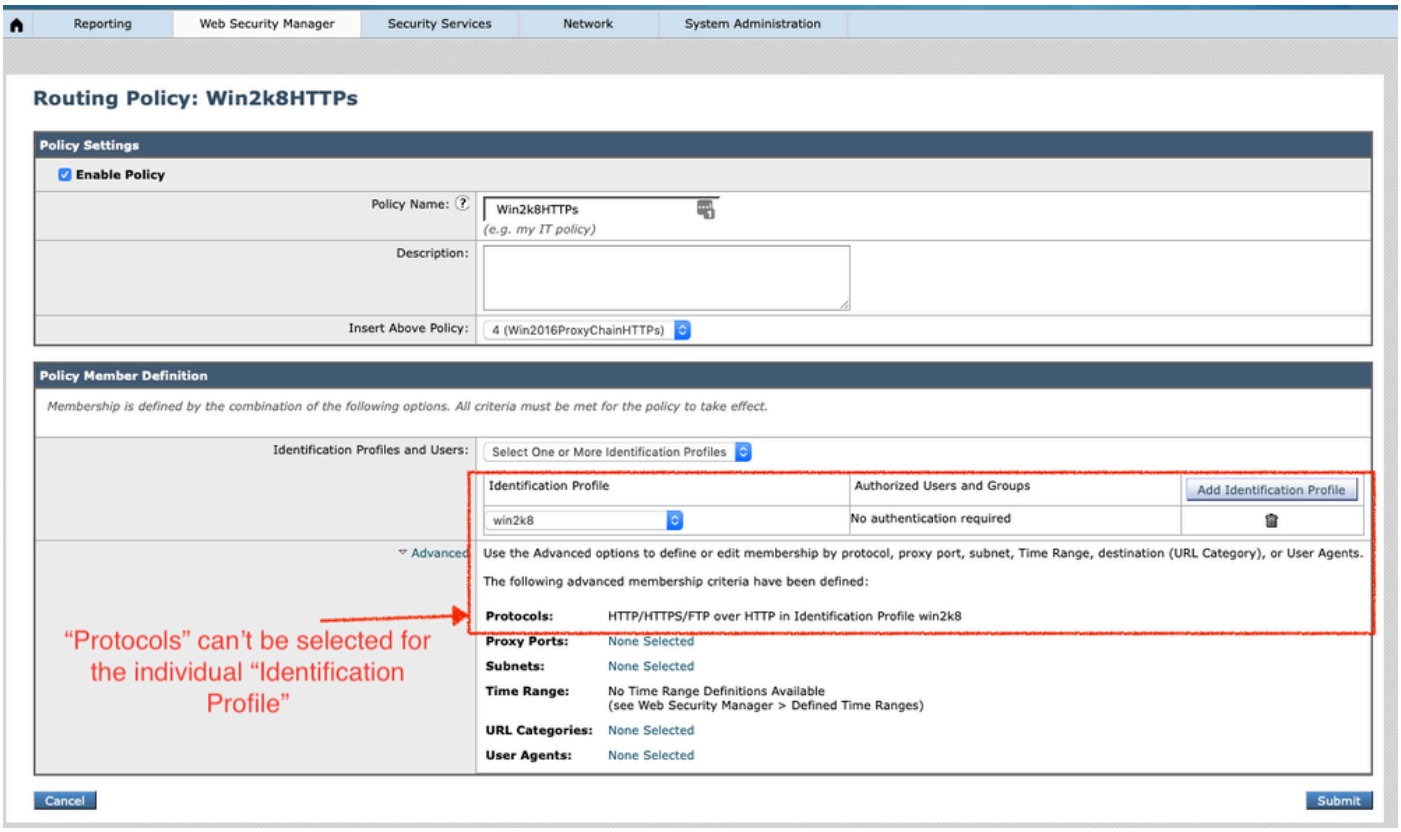


360050589572

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.



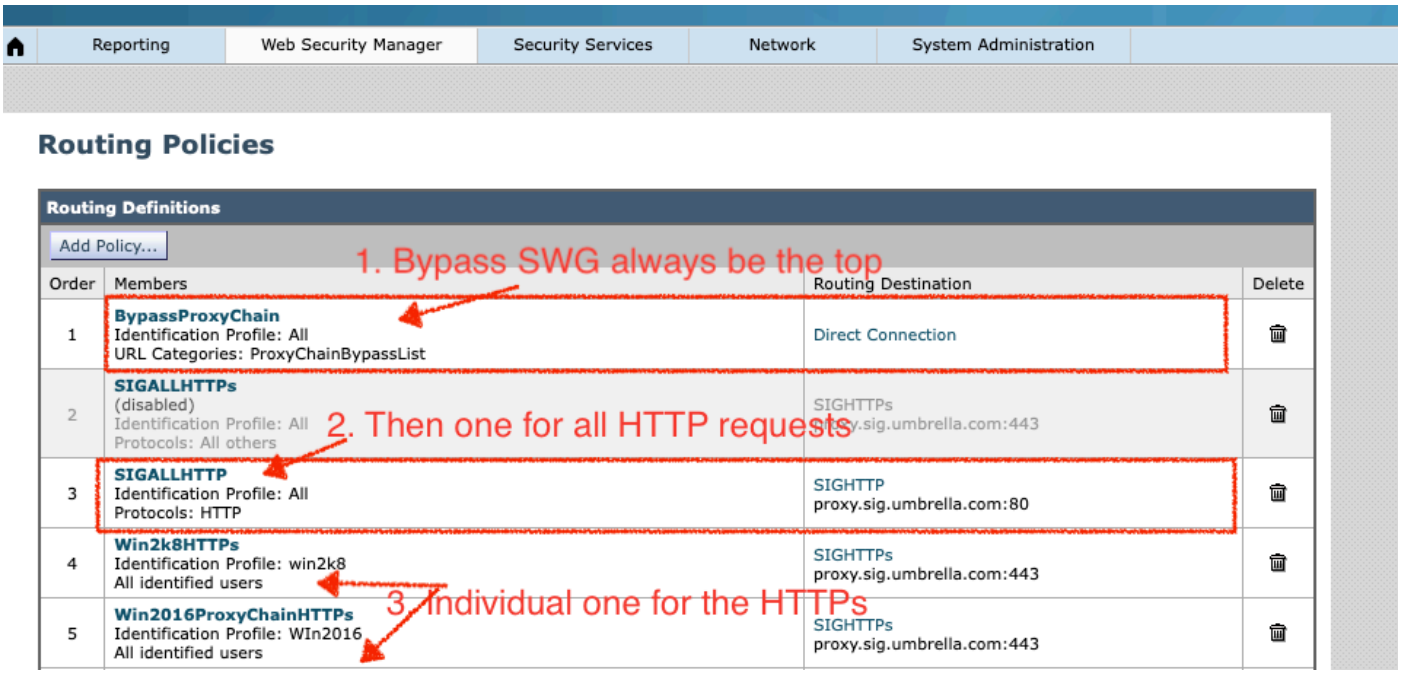
360050703971



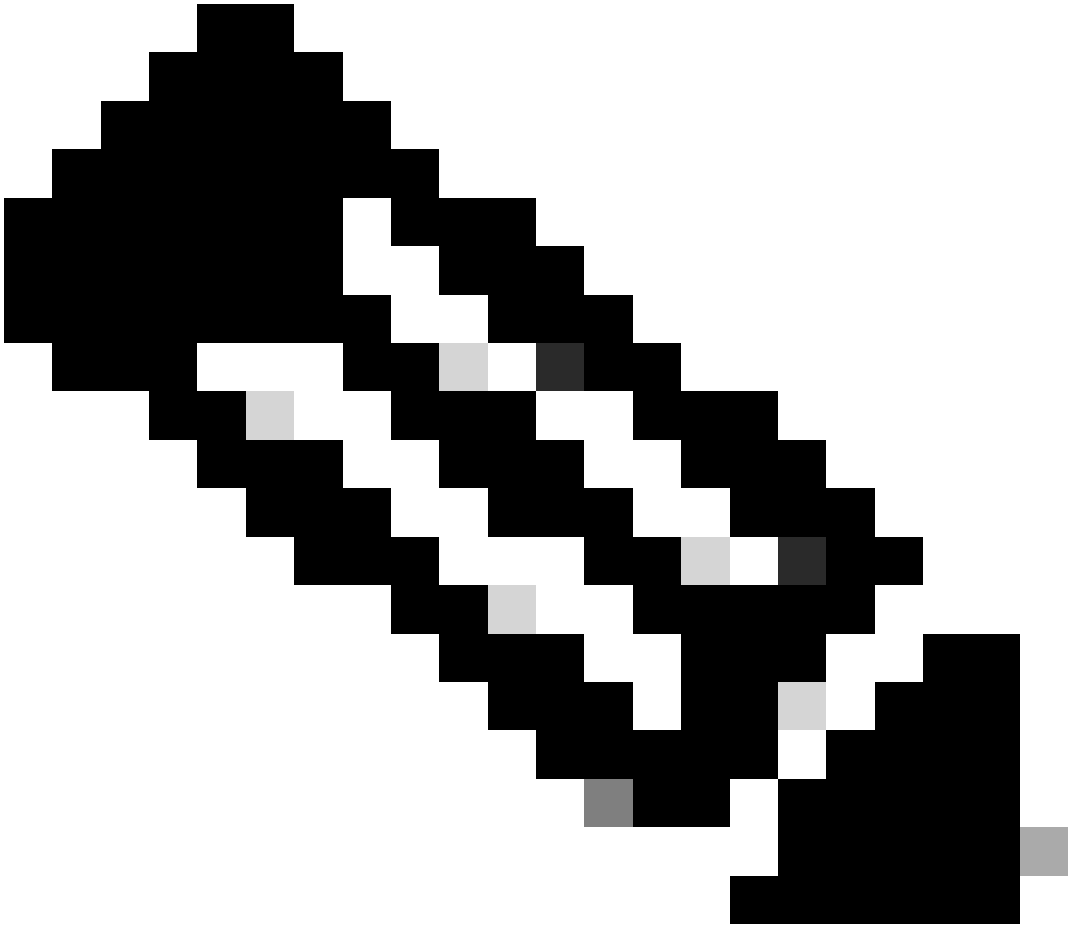
360050700091

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.



360050700131



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

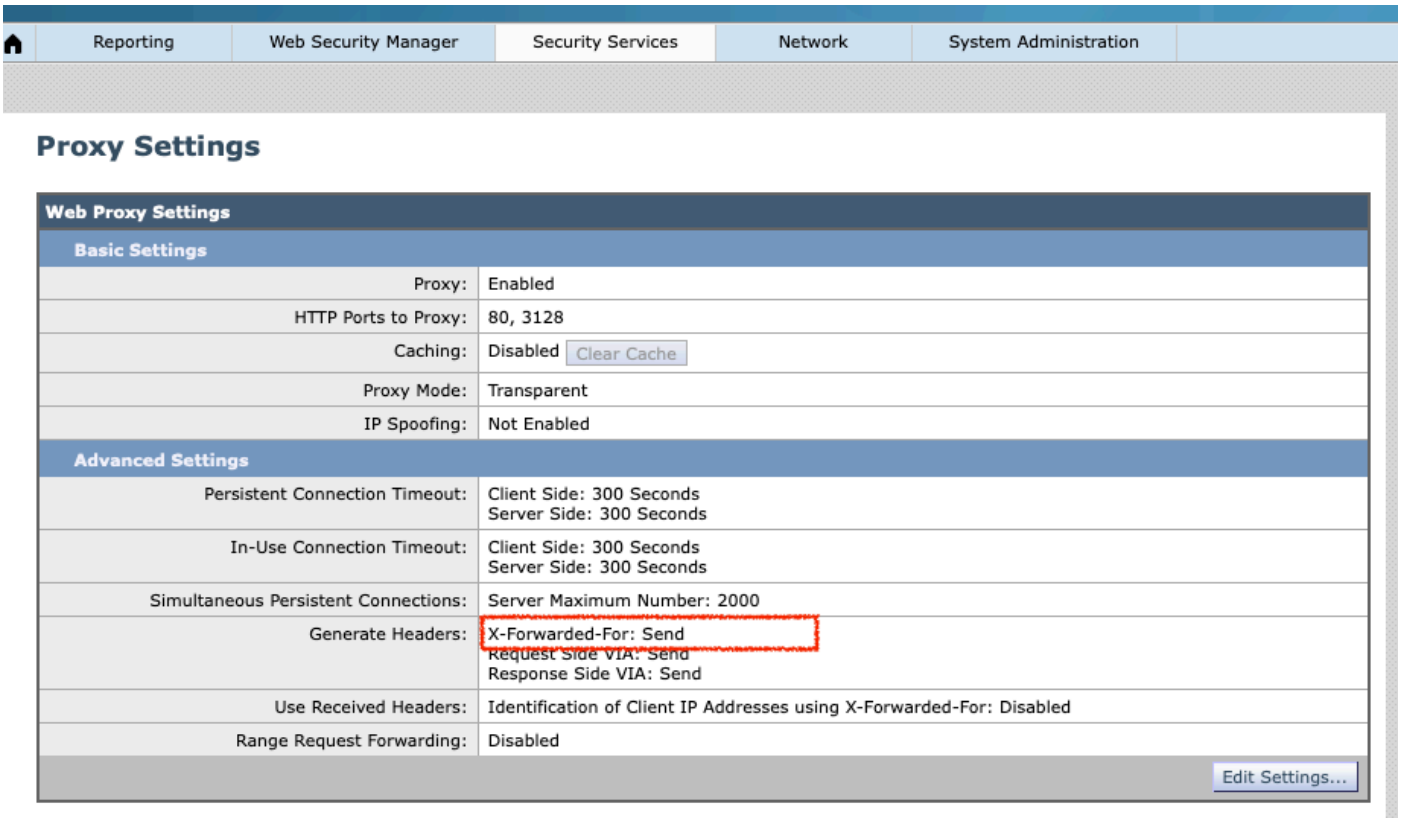
Pour un déploiement transparent du proxy

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

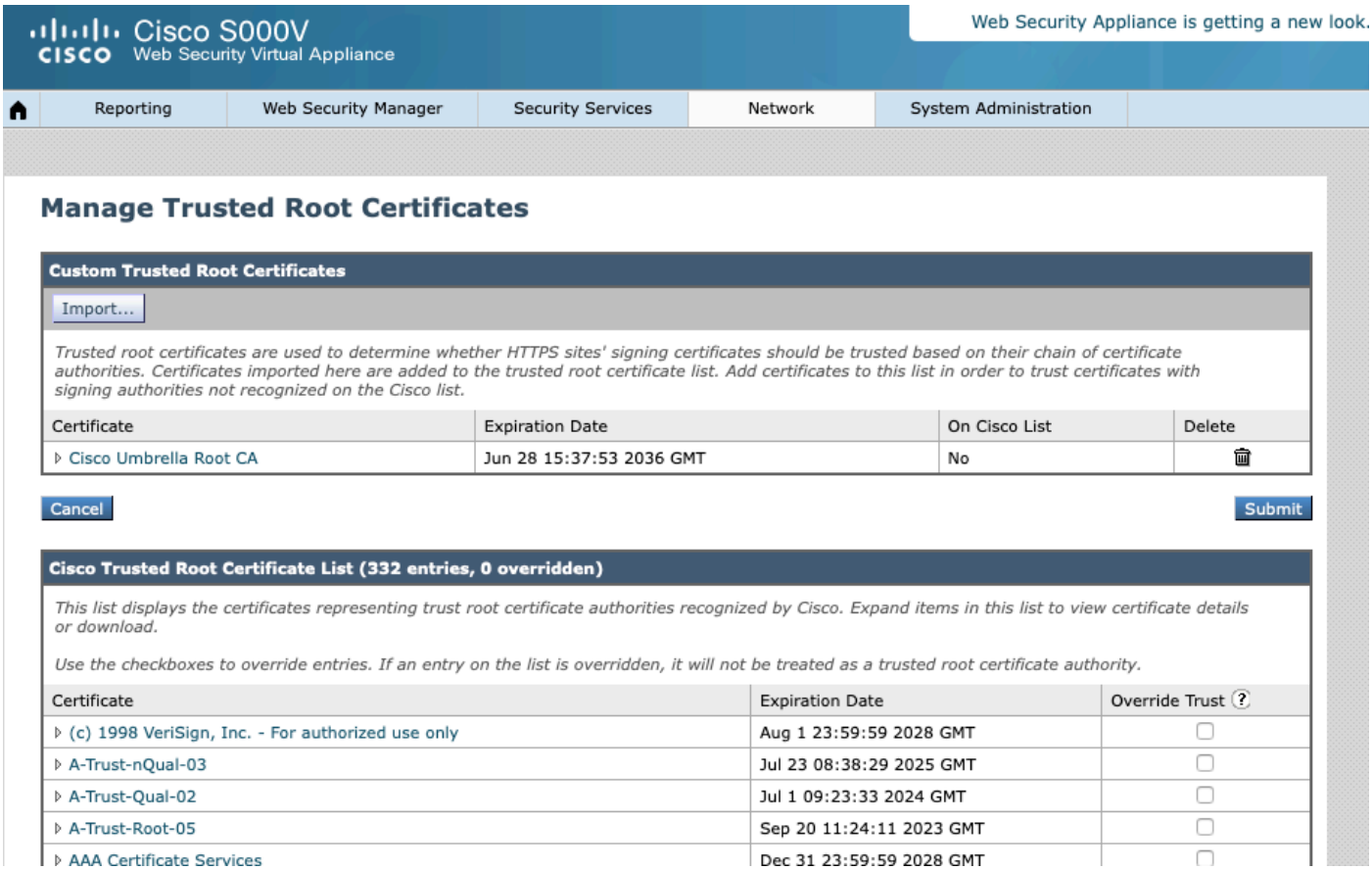
- pour implémenter la stratégie Web IP interne dans SWG.Assurez-vous d'activer l'en-tête « X-Forwarded-For » dans l'appliance Web sécurisé via Services de sécurité > Paramètres du proxy.



360050700111

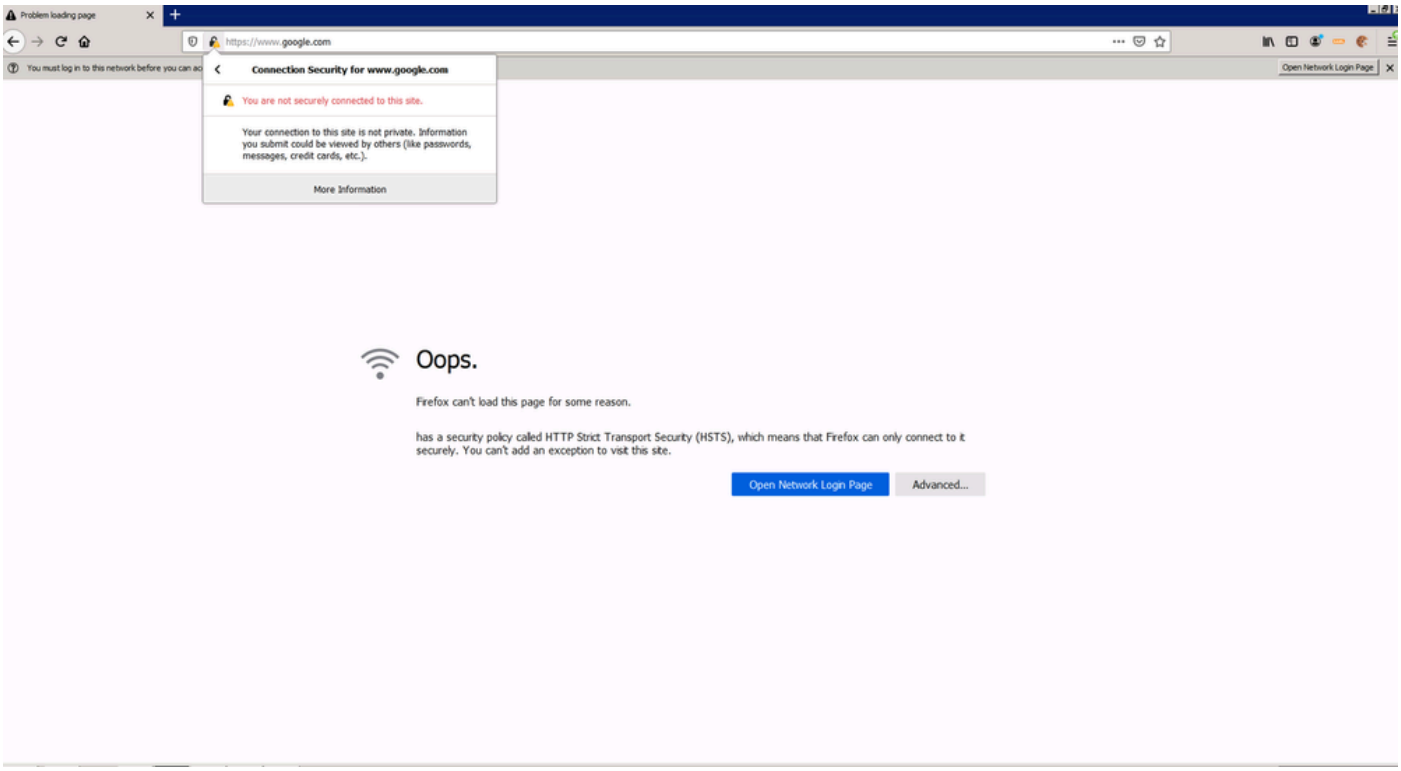
2. Certificat racine de confiance pour le déchiffrement HTTP.

- 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.



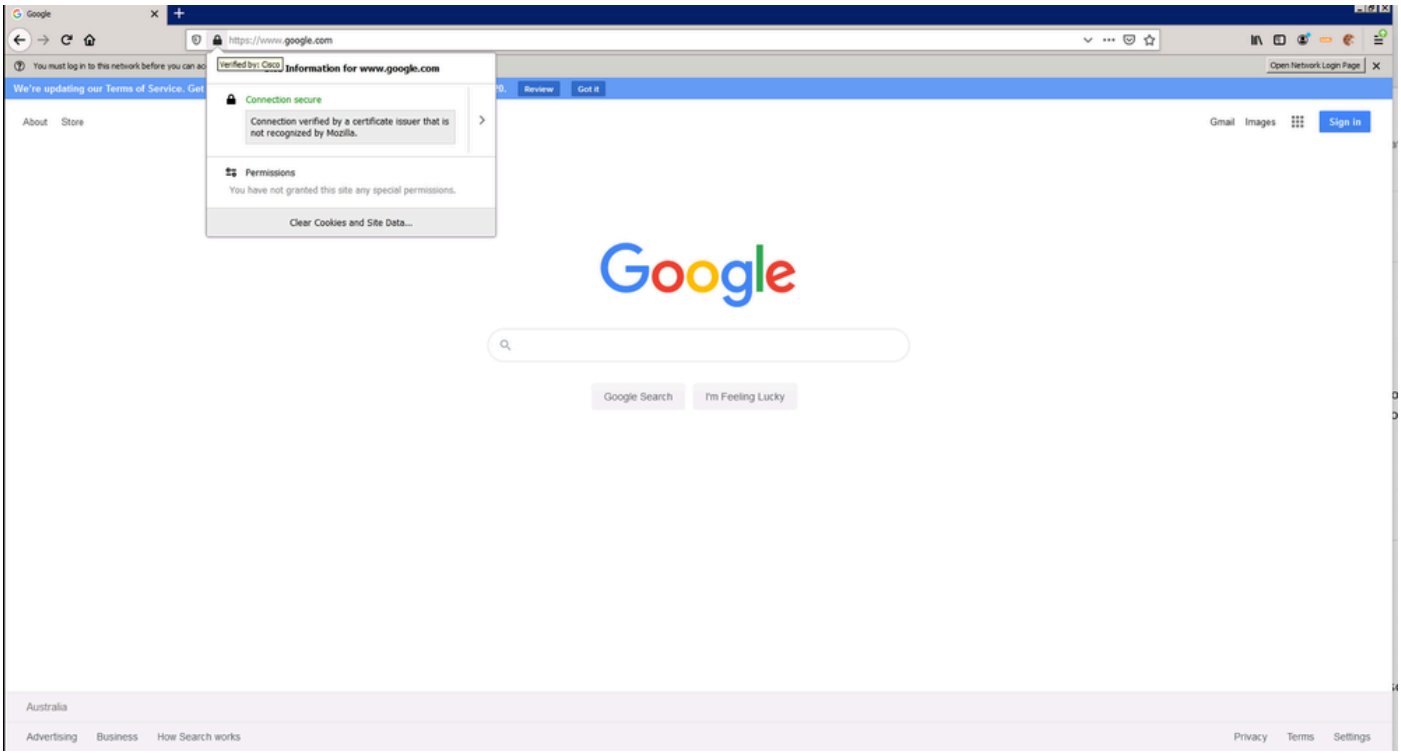
360050589612

- 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.