Configurer le proxy en amont dans l'appliance Web sécurisée

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configuration du proxy en amont

- Étape 2. (Facultatif) Créez un profil d'identification à utiliser pour le proxy en amont
- Étape 3. Création du proxy en amont
- Étape 4. (Facultatif) Téléchargez le certificat de déchiffrement
- Étape 5 : configuration de la politique de routage
- Étape 6. (Facultatif) Configuration des paramètres de délai d'attente de non-réponse du proxy en amont

Journalisation

- Journaux d'accès
- Proxylogs

Autres informations utiles

Introduction

Ce document décrit les étapes pour configurer le proxy en amont dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA
- Protocoles réseau et proxy de base

Cisco recommande d'installer les outils suivants :

- SWA physique ou virtuel

- Accès administratif à l'interface utilisateur graphique (GUI) de SWA
- Accès administratif à l'interface de ligne de commande (CLI) SWA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration du proxy en amont

Suivez ces étapes pour configurer un proxy en amont dans SWA :

Étapes	Étapes
Étape 1. (Facultatif) Créez une catégorie d'URL personnalisée pour les URL Remarque : Si vous préférez définir le proxy en amont pour tout le trafic, vous pouvez ignorer cette étape.	Étape 1.1. Dans l'interface graphique, sélectionnez Web Security Manager, puis cliquez sur Custom and External URL Categories. Étape 1.2. Cliquez sur Ajouter une catégorie pour ajouter une catégorie d'URL personnalisée. Étape 1.3. Attribuer un nom de catégorie unique. Étape 1.4. (Facultatif) Ajoutez une description. Étape 1.5. Dans Ordre des listes, choisissez la première catégorie sur laquelle vous souhaitez vous positionner. Étape 1.6. Dans la liste déroulante Type de catégorie, sélectionnez Catégorie personnalisée locale. Étape 1.7. Ajoutez les URL souhaitées dans la section Sites. Étape 1.8. Envoyer.

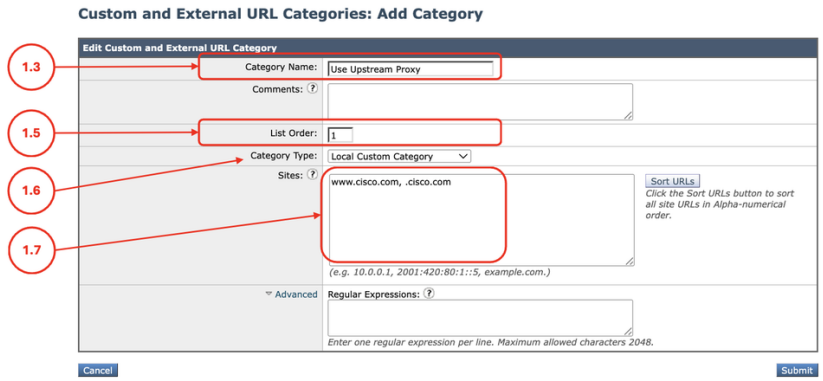


Image - Créer une catégorie d'URL personnalisée

Étape 2. (Facultatif) Créez un profil d'identification à utiliser pour le proxy en amont

Remarque : Si vous préférez définir le proxy en amont pour tout le trafic, vous pouvez ignorer cette étape.

Étape 2.1. Dans l'interface utilisateur graphique, sélectionnez Web Security Manager, puis cliquez sur Profils d'identification.
Étape 2.2. Cliquez sur Add Profile pour ajouter un profil.
Étape 2.3. Utilisez la case à cocher Activer le profil d'identification pour activer le profil ou le désactiver rapidement sans le supprimer.
Étape 2.4. Attribution d'un nom de profil unique.
Étape 2.5. (Facultatif) Ajoutez une description.
Étape 2.6. Dans la liste déroulante Insérer au-dessus, choisissez l'emplacement du profil dans le tableau.

Étape 2.7. Si vous ne souhaitez pas authentifier les utilisateurs qui appliquent cette stratégie, dans la section User Identification Method, choisissez Exempt from authentication/identification, sinon configurez les paramètres d'authentification.

Étape 2.8. Dans le champ Define Members by Subnet (Définir les membres par sous-réseau), laissez ce champ vide pour inclure toutes les adresses IP client, sauf si vous voulez transmettre le trafic pour certaines adresses IP.

Étape 2.9. (Facultatif : si vous devez utiliser un proxy en amont pour des utilisateurs spécifiques accédant à certains sites Web, effectuez cette étape). Dans la section Avancé, choisissez Catégories d'URL personnalisées et ajoutez la catégorie d'URL personnalisée qui a été créée à l'étape 1.

Étape 2.10. Envoyer.

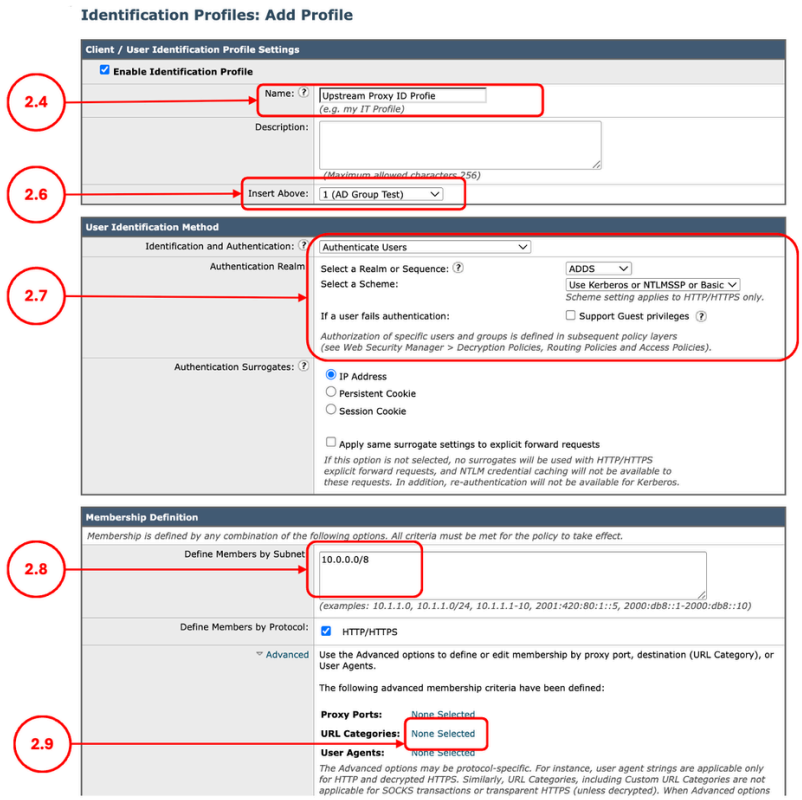


Image - Créer un profil d'identification

Étape 3. Création du proxy en amont	Étape 3.1. Dans l'interface utilisateur graphique, sélectionnez Network, puis cliquez sur Upstream Proxy. Étape 3.2. Cliquez sur Add Group. Étape 3.3. Attribuer un nom unique. Étape 3.4. Définition de l'adresse proxy et du numéro de port. Étape 3.5. (Facultatif) Si vous disposez de plusieurs Proxy en amont, cliquez sur Ajouter une ligne pour définir le Proxy suivant. Étape 3.6. (Facultatif) Si vous avez saisi plusieurs Proxy en amont dans la section Équilibrage de charge, définissez la méthode d'équilibrage de charge souhaitée : • None (Failover) : le proxy Web dirige les transactions vers un proxy externe dans le groupe. Il tente de connecter les proxys dans l'ordre dans lequel ils sont répertoriés. Si un proxy n'est pas accessible, le proxy Web tente de se connecter au proxy suivant de la liste. • Le plus petit nombre de connexions : le proxy Web effectue le suivi du nombre de demandes actives avec différents proxys dans le groupe et dirige une

transaction vers le proxy qui traite actuellement le moins de connexions.

- Basé sur le hachage (le moins récemment utilisé) : le proxy Web dirige une transaction vers le proxy qui a reçu une transaction le moins récemment si tous les proxys sont actuellement actifs. Ce paramètre est similaire au round robin, sauf que le proxy Web prend également en compte les transactions qu'un proxy a reçues (membre) et qui se trouvent dans un groupe de proxies différent. En d'autres termes, si un proxy est répertorié dans plusieurs groupes de proxies, l'option « le moins récemment utilisé » est moins susceptible de surcharger ce proxy.
- Round-Robin : le proxy Web effectue des cycles de transactions égaux entre tous les proxys du groupe dans l'ordre indiqué.

Étape 3.7. Choisissez l'option Failure Handling qui correspond à votre stratégie interne.

- Connect Directly : Envoie les requêtes directement à leurs serveurs de destination.
- Drop Requests : ignorez les demandes sans les transférer.

Étape 3.8. Envoyer.

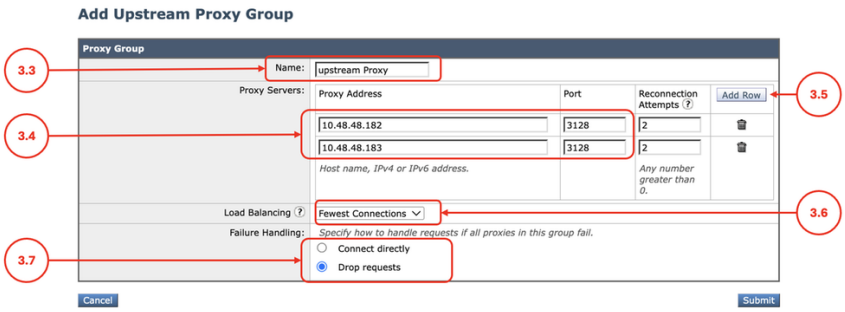


Image - Ajouter un groupe de proxys en amont

Étape 4. (Facultatif) Téléchargez le certificat de déchiffrement

Remarque : Si le proxy en amont ne déchiffre pas le

Étape 4.1. Dans l'interface utilisateur graphique, sélectionnez Network, puis cliquez sur Certificate Management.

Étape 4.2. Dans la section Certificate Management, cliquez sur Manage Trusted Root Certificates.

trafic ou si son serveur d'autorité de certification (CA) est déjà approuvé dans le SWA, vous pouvez ignorer cette étape.

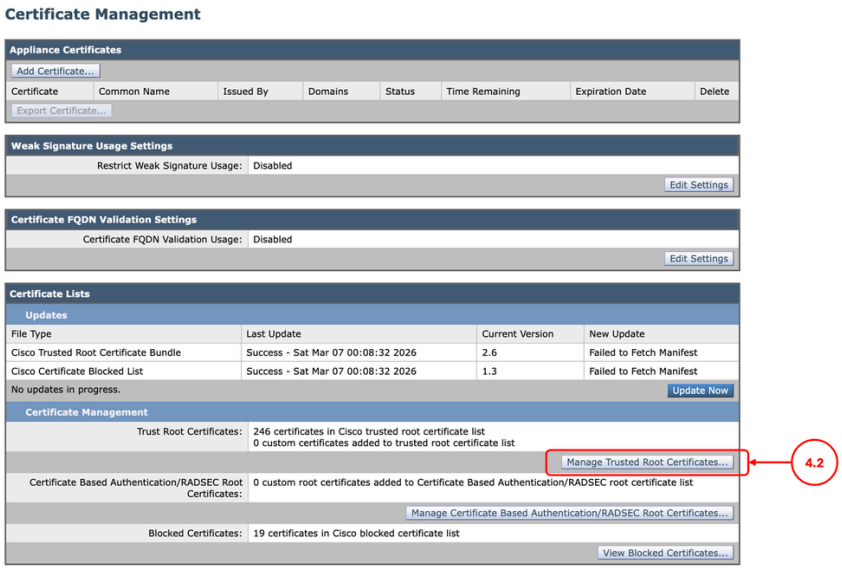


Image - Gérer le certificat racine de confiance

Étape 4.3. Soumettre et valider les modifications

Attention : si les certificats d'autorité de certification racine et intermédiaire sont requis, téléchargez d'abord le certificat d'autorité de certification racine, puis cliquez sur Submit and Commit. Une fois la validation terminée, importez le certificat d'autorité de certification intermédiaire, puis soumettez et validez à nouveau les modifications.

Étape 5 : configuration de la politique de routage

Étape 5.1. Dans l'interface graphique, choisissez Web Security Manager, puis cliquez sur Routing Policy.

Étape 5.2. (Facultatif) Si vous souhaitez utiliser le proxy en amont pour des utilisateurs ou des sites Web spécifiques, cliquez sur Ajouter une stratégie, puis sélectionnez le profil d'identification que vous avez créé à l'étape 2.

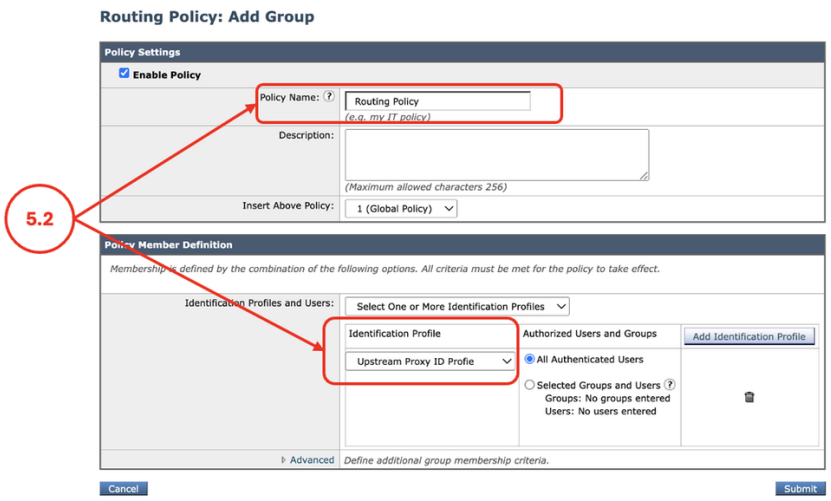


Image - Ajout d'un profil ID à la stratégie de routage

Étape 5.3. Pour les paramètres requis que vous préférez dans le proxy en amont, cliquez sur le lien Destination de routage et sélectionnez le groupe de proxy en amont que vous avez créé à l'étape 3.

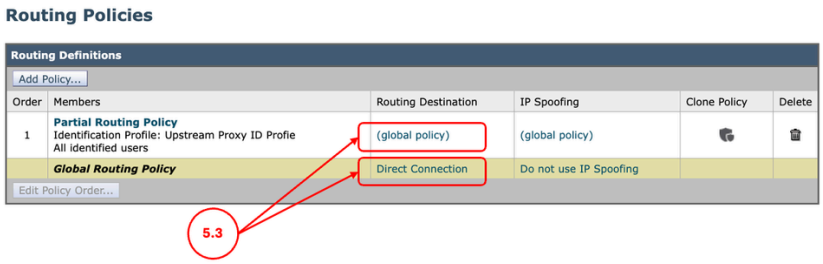


Image : configuration de la destination de routage

Remarque : Si vous préférez que tout le trafic utilise le proxy en amont, dans la Stratégie de routage globale, sélectionnez le proxy en amont souhaité.

Étape 5.4. Soumettre et valider les modifications

Étape 6. (Facultatif) Configuration des paramètres de délai d'attente de non-réponse du proxy en amont

Conseil : il est recommandé de ne pas modifier ces valeurs à moins que vous ne

Étape 6.1. Connectez-vous à l'interface de ligne de commande et exécutez advanced proxyconfig.

Étape 6.2. Sélectionnez DIVERS.

Étape 6.3. Appuyez sur Entrée jusqu'à ce que la fenêtre Entrer le délai d'inactivité minimum pour vérifier le proxy en amont qui ne répond pas (en secondes) s'affiche. Vous pouvez configurer la durée minimale pendant laquelle SWA attend pour réessayer le proxy en amont qui a été

compreniez parfaitement leur comportement et leur impact potentiel.	précédemment déclaré Inactif. La valeur par défaut est de 10 secondes. Étape 6.4. Appuyez sur Entrée pour passer au paramètre suivant. Lors de la définition du délai d'inactivité maximal pour la vérification d'un proxy en amont qui ne répond pas, notez que si cette valeur de délai d'attente est atteinte avant que le nombre configuré de tentatives de reconnexion soit épuisé (étape 3), le SWA considère le proxy en amont hors ligne. Étape 6.5. Continuez à appuyer sur Entrée, jusqu'à ce que vous quittiez l'assistant, exécutez commit pour enregistrer les modifications.

Journalisation

Journaux d'accès

Dans les journaux d'accès, le trafic acheminé vers le proxy en amont est affiché comme DEFAULT_PARENT suivi par le nom du proxy en amont. Voici un exemple :

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

Proxylogs

À partir des journaux de proxy, vous pouvez vérifier l'état de santé des proxys en amont.

Conseil : Vous pouvez filtrer les homologues pour examiner les journaux associés au proxy en amont.

Voici quelques exemples de ce qui a été configuré à deux reprises avec les tentatives de reconnexion de l'étape 3. Après la deuxième panne de connexion au proxy en amont, le proxy en amont est déclaré inactif et SWA supprime ce proxy en amont de la liste jusqu'à ce que le processus de proxy soit redémarré :

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

Remarque : Si le proxy en amont ne répond pas aux requêtes SYN TCP, ne renvoie pas de code de réponse HTTP ou renvoie une réponse HTTP 504 (Gateway Timeout) ; SWA considère que le proxy en amont n'est pas disponible et change son état de Healthy à Sick.

Conseil : Le SWA considère qu'un proxy en amont est sain s'il renvoie un en-tête VIA.

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance
- Configurer des catégories d'URL personnalisées dans Secure Web Appliance - Cisco
- Comment exempter le trafic Office 365 de l'authentification et du déchiffrement sur l'appareil de sécurité Web Cisco (WSA) - Cisco
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco
- Bloquer le trafic dans l'appliance Web sécurisée
- Bloquer le trafic de téléchargement dans l'appliance Web sécurisée
- Bloquer le téléchargement de fichiers exécutables dans SWA
- Contourner le trafic des mises à jour Microsoft dans l'appliance Web sécurisée
- Contourner l'authentification dans l'appareil Web sécurisé - Cisco

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.