Contourner l'authentification dans l'appliance Web sécurisée

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Authentification Exempt](#)

[Méthodes d'exemption d'authentification dans Cisco SWA](#)

[Étapes pour contourner l'authentification](#)

[Autres informations utiles](#)

Introduction

Ce document décrit comment contourner l'authentification dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.

Cisco recommande d'installer les outils suivants :

- SWA physique ou virtuel
- Accès administratif à l'interface utilisateur graphique (GUI) de 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.

Authentification Exempt

L'exemption de l'authentification pour certains utilisateurs ou systèmes dans Cisco SWA peut être essentielle pour maintenir l'efficacité opérationnelle et répondre à des exigences spécifiques. Premièrement, certains utilisateurs ou systèmes nécessitent un accès ininterrompu à des ressources ou services critiques qui pourraient être entravés par les processus d'authentification. Par exemple, les systèmes automatisés ou les comptes de service effectuant des mises à jour ou des sauvegardes régulières ont besoin d'un accès transparent sans les retards ou les défaillances potentielles induites par les mécanismes d'authentification.

En outre, il existe des scénarios dans lesquels le fournisseur de services Web recommande de ne pas utiliser de proxy pour accéder à son service. Dans de tels cas, l'exemption d'authentification garantit la conformité aux directives du fournisseur et maintient la fiabilité du service. En outre, pour bloquer efficacement le trafic de certains utilisateurs, il est souvent nécessaire de les exempter d'abord de l'authentification, puis d'appliquer les stratégies de blocage appropriées. Cette approche permet un contrôle précis des autorisations d'accès.

Dans certains cas, le service Web auquel vous accédez est approuvé et universellement acceptable, comme les mises à jour Microsoft. L'exemption d'authentification pour ces services simplifie l'accès pour tous les utilisateurs. En outre, il existe des situations où le système d'exploitation ou l'application utilisateur ne prend pas en charge le mécanisme d'authentification configuré dans le SWA, nécessitant un contournement pour assurer la connectivité.

Enfin, les serveurs avec des adresses IP fixes qui n'ont pas de connexion utilisateur et ont un accès Internet sécurisé et limité ne nécessitent pas d'authentification, car leurs modèles d'accès sont prévisibles et sécurisés.

En exemptant l'authentification de manière stratégique dans ces cas, les entreprises peuvent équilibrer les besoins en sécurité et l'efficacité opérationnelle.

Méthodes d'exemption d'authentification dans Cisco SWA

L'exemption de l'authentification dans SWA peut être réalisée par le biais de diverses méthodes, chacune étant adaptée à des scénarios et des exigences spécifiques. Voici quelques méthodes

courantes de configuration des exemptions d'authentification :

- Adresse IP ou masque de sous-réseau : L'une des méthodes les plus simples consiste à exempter de l'authentification des adresses IP spécifiques ou des sous-réseaux entiers. Cela est particulièrement utile pour les serveurs avec des adresses IP fixes ou des segments de réseau approuvés qui nécessitent un accès ininterrompu à Internet ou à des ressources internes. En spécifiant ces adresses IP ou masques de sous-réseau dans la configuration SWA, vous pouvez vous assurer que ces systèmes contournent le processus d'authentification.

- Ports proxy : Vous pouvez configurer le SWA pour exempter le trafic en fonction de ports proxy spécifiques. Cela est utile lorsque certaines applications ou certains services utilisent des ports désignés pour communiquer. En identifiant ces ports, vous pouvez configurer le SWA pour contourner l'authentification pour le trafic sur ces ports, assurant un accès transparent pour les applications ou services concernés.

- Catégories d'URL : Une autre méthode consiste à exempter l'authentification en fonction des catégories d'URL. Il peut s'agir à la fois de catégories Cisco prédéfinies et de catégories d'URL personnalisées que vous définissez en fonction des besoins spécifiques de votre entreprise. Par exemple, si certains services Web, tels que les mises à jour Microsoft, sont considérés comme fiables et universellement acceptables, vous pouvez configurer le SWA pour contourner l'authentification pour ces catégories d'URL spécifiques. Cela garantit que tous les utilisateurs peuvent accéder à ces services sans avoir besoin d'authentification.

- Agents utilisateurs : L'exemption de l'authentification basée sur les agents utilisateur est utile lorsque vous traitez avec des applications ou des périphériques spécifiques qui ne prennent pas en charge les mécanismes d'authentification configurés. En identifiant les chaînes d'agent utilisateur de ces applications ou périphériques, vous pouvez configurer le SWA pour contourner l'authentification pour le trafic provenant d'eux, assurant ainsi une connectivité transparente.

Étapes pour contourner l'authentification

Voici les étapes à suivre pour créer un profil d'identification à exempter de l'authentification :

Étape 1. Dans l'interface graphique utilisateur, choisissez Web Security Manager, puis cliquez sur Identification Profiles.
Étape 2. Cliquez sur Add Profile pour ajouter un profil.
Étape 3. Utilisez la case à cocher Activer le profil d'identification pour activer ce profil ou pour le désactiver rapidement sans le supprimer.
Étape 4. Attribuez un nom de profil unique.
Étape 5. (Facultatif) Ajoutez une description.

Étape 6. Dans la liste déroulante Insérer au-dessus, choisissez l'emplacement de ce profil dans le tableau.



Remarque : Positionner les profils d'identification qui ne nécessitent pas d'authentification en haut de la liste. Cette approche réduit la charge sur le SWA, réduit la file d'attente d'authentification et accélère l'authentification des autres utilisateurs.

Étape 7. Dans la section User Identification Method, sélectionnez Exempt from authentication/ identification.

Étape 8. Dans la zone Define Members by Subnet, saisissez les adresses IP ou les sous-réseaux auxquels s'applique ce profil d'identification. Vous pouvez utiliser des adresses IP, des blocs CIDR (Classless Inter-Domain Routing) et des sous-réseaux.

Étape 9. (Facultatif) Cliquez sur Avancé pour définir des critères d'appartenance supplémentaires, tels que Ports proxy, Catégories d'URL ou Agents utilisateur.



Mise en garde : Dans un déploiement de proxy transparent, SWA ne peut pas lire les agents utilisateur ou l'URL complète pour le trafic HTTPS à moins que le trafic ne soit décrypté. Par conséquent, si vous configurez le profil d'identification à l'aide d'agents utilisateur ou d'une catégorie d'URL personnalisée avec des expressions régulières, ce trafic ne correspond pas au profil d'identification.

Pour plus d'informations sur la façon de configurer la catégorie d'URL personnalisée, consultez : Configurer des catégories d'URL personnalisées dans Appareil Web sécurisé - Cisco

---



Conseil : La stratégie utilise une logique AND, ce qui signifie que toutes les conditions doivent être remplies pour que le profil d'ID corresponde. Lorsque les options avancées sont définies, chaque condition doit être satisfaite pour que la stratégie s'applique.

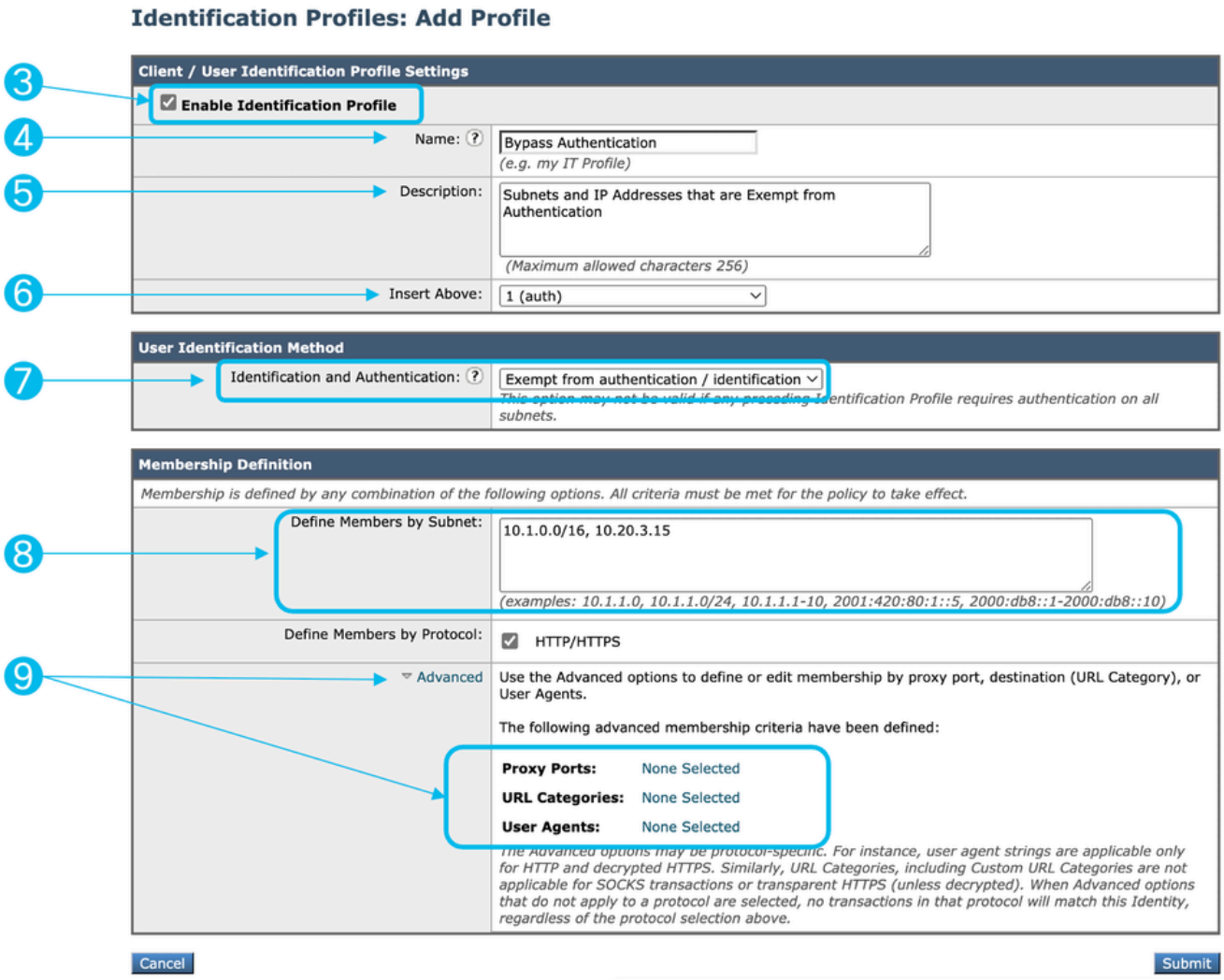


Image - Étapes de création du profil d'ID pour contourner l'authentification

Étape 10. Soumettre et valider les modifications

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - GD(General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco
- 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

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.