Configurer l'authentification unique Kerberos dans SWA

Table des matières

Introduction

Ce document décrit les étapes pour configurer les utilisateurs proxy pour avoir l'authentification SSO (Single-Sign-On) via Kerberos dans Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.
- Administration Active Directory 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 Active Directory.

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.

Avant de commencer

Si le client proxy tente d'accéder à un site Web et est invité à saisir manuellement les informations d'identification, procédez comme suit pour le dépannage.

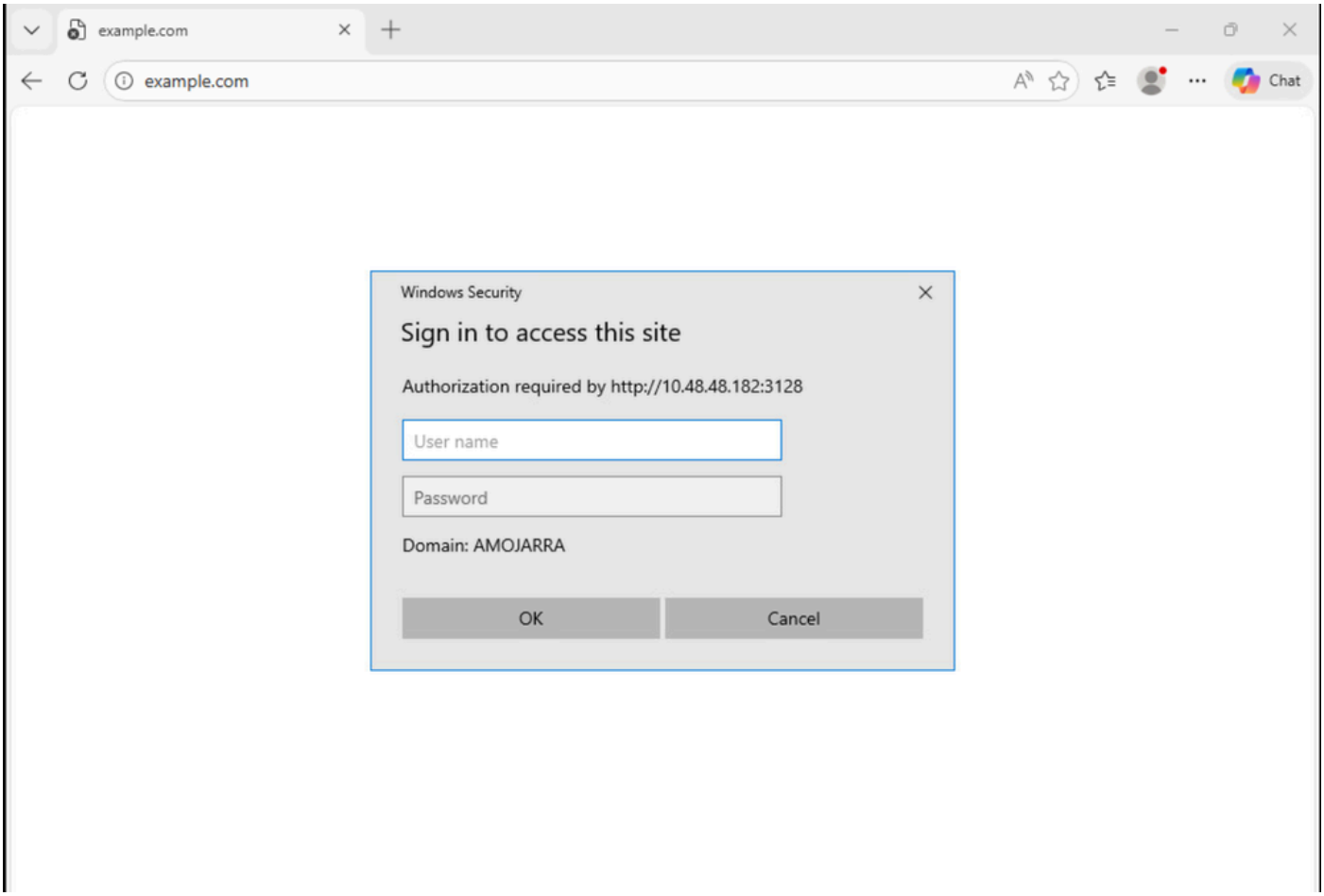


Image - Invite d'authentification utilisateur

Étape 1 : vérifiez les journaux d’accès associés au client.

Étape 1.1. Connectez-vous à l’interface de ligne de commande.

Étape 1.2. Exécutez grep.

Étape 1.3. Sélectionnez le numéro associé à l'. access logs.

Étape 1.4. Dans le champ Entrez l’expression régulière pour grep, tapez l’adresse IP du client.

Étape 1.5. Appuyez sur Entrée jusqu'à ce que Do you want to tail the logs, Tapez "Y" et appuyez sur Entrée jusqu'à ce que vous voyiez les journaux d'accès.

Étape 1.6. Reproduisez le problème en essayant d’accéder à n’importe quel site Web à partir du PC client.

Étape 1.7. Confirmez le profil d’identification que le trafic atteint.

Dans cet exemple, le profil d'identification est Auth_ID :

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

Étape 2 : vérification du profil d'identification

Étape 2.1. Connectez-vous à l'interface utilisateur graphique du SWA.

Étape 2.2. Dans le Gestionnaire de sécurité Web, sélectionnez Profils d'identification.

Étape 2.3. Cliquez sur le nom du profil d’identification que le trafic atteignait.

Étape 2.4 : vérifiez que le schéma d’authentification n’est pas défini sur Basic.

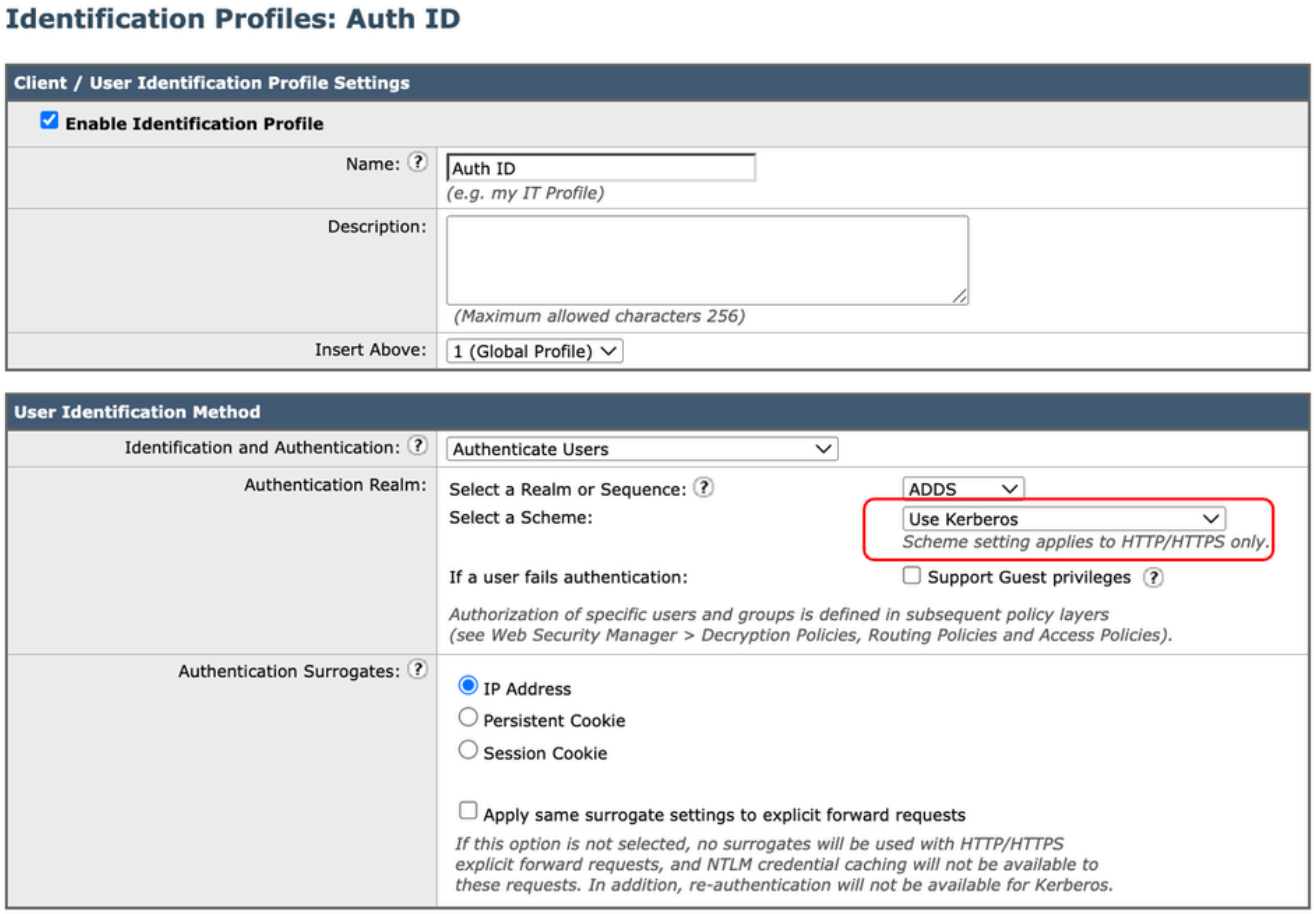


Image - Schéma d'authentification

Étape 3 : test de la connectivité SWA et Active Directory

Étape 3.1. Dans l’interface utilisateur graphique de SWA, accédez à Network et sélectionnez Authentication.

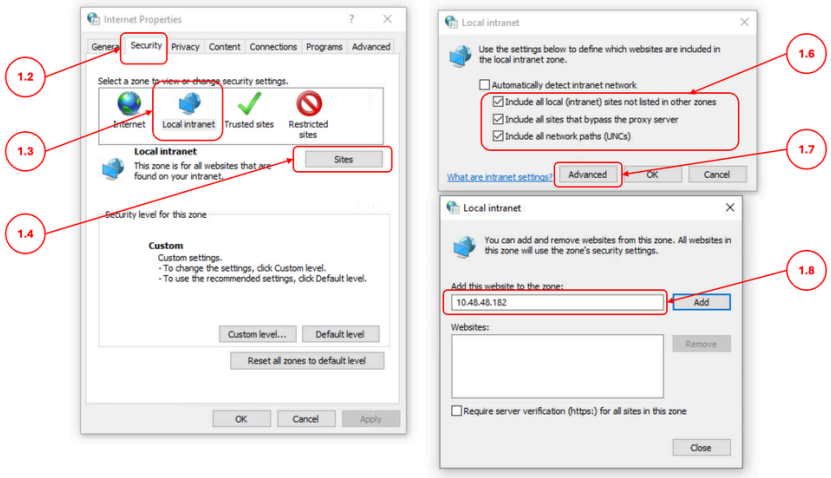
Étape 3.2. Cliquez sur le nom du domaine d’authentification.

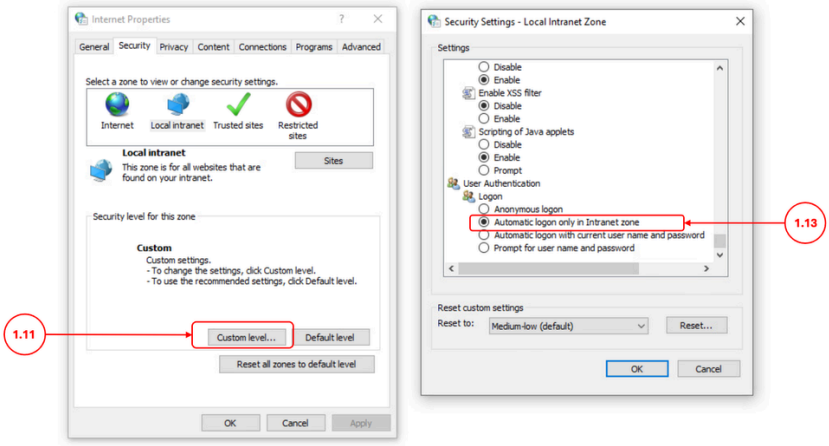
Étape 3.3. Cliquez sur Start Test (Démarrer le test) pour vérifier l'état de connectivité SWA et Active Directory.

Si aucune erreur n'est détectée, vérifiez la configuration de l'ordinateur client comme décrit dans cet article.

Configuration du PC client

Pour vérifier la configuration du PC client, procédez comme suit :

Étapes	Détails
Étape 1. Sites intranet locaux	Étape 1.1. Dans le menu Démarrer, tapez Internet Option, puis appuyez sur Entrée. Étape 1.2. Dans la fenêtre Propriétés Internet, cliquez sur l'onglet Sécurité. Étape 1.3. Sélectionnez Intranet local. Étape 1.4. Cliquez sur Sites. Étape 1.5. Assurez-vous que la case à cocher Détection automatique du réseau intranet n'est pas activée. Étape 1.6. Sélectionnez les trois options suivantes : • Inclure tous les sites locaux (intranet) non répertoriés dans d'autres zones • Inclure tous les sites qui contournent le serveur proxy • Inclure tous les chemins réseau (UNC) Étape 1.7. Cliquez sur Advanced. Étape 1.8. Entrez le nom de domaine complet (FQDN) ou l'adresse IP de votre SWA et ajoutez-le à la liste. Étape 1.9. (Facultatif) En fonction de vos stratégies de sécurité internes, vous pouvez désactiver l'option Require Server Verification.  Image : configuration des sites Internet locaux Étape 1.10. Cliquez sur Fermer et sur OK. Étape 1.11. Dans l'onglet Sécurité, cliquez sur Personnaliser

	le niveau. Étape 1.12. Faites défiler jusqu'à Authentification utilisateur. Étape 1.13. Assurez-vous que l'option Connexion automatique uniquement dans la zone Intranet est sélectionnée.  Image - Connexion automatique pour les utilisateurs de l'intranet
Étape 2. Collecte des journaux	Si l'étape 1 n'a pas corrigé l'authentification SSO via Kerberos : Étape 2.1. Remplacez les journaux d'authentification SWA par Trace et vérifiez les journaux. Étape 2.2. Ajouter [Auth-Method = %m] en tant que champ personnalisé aux journaux d'accès. pour plus d'informations, veuillez visiter : Configurez le paramètre Performance dans les journaux d'accès. Étape 2.3. Exécutez un filtre de capture de paquets pour l'adresse IP du client et l'adresse IP Active Directory et vérifiez que le PC client envoie le ticket de service Kerberos au SWA.

Remarque : Assurez-vous d'avoir configuré le nom de domaine complet du SWA dans les paramètres proxy de votre navigateur.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance

- Configurer le pare-feu pour l'appliance Web sécurisée
- Configurer la capture de paquets sur l'appliance de sécurité du contenu
- Configurer le paramètre de performance dans les journaux d'accès
- Accéder aux journaux de l'appliance Web sécurisée
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco
- 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.