Configurer le certificat de déchiffrement dans l'appareil Web sécurisé

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Décryptage HTTPS
- Configurer le certificat de déchiffrement dans SWA
  - Télécharger un certificat racine et une clé
  - Générer un certificat et une clé pour le proxy HTTPS
- Importer un certificat
  - Importer un certificat de proxy en amont vers SWA
  - Importer un certificat SWA dans un autre SWA
  - Importer un certificat SWA dans un client Windows
  - Importer le certificat SWA dans le client Mac
  - Importer un certificat SWA dans Ubuntu/Debian
  - Importer un certificat SWA dans CentOS 6
  - Importer un certificat SWA dans CentOS 5
  - Importer un certificat SWA dans Mozilla Firefox
  - Importer un certificat SWA dans Google Chrome
  - Importer un certificat SWA dans Microsoft Edge/Internet Explorer
  - Importer un certificat SWA dans Safari
  - Importer un certificat SWA de la stratégie de groupe vers les clients
- Autres informations utiles

Introduction

Ce document décrit les étapes pour configurer les certificats de chiffrement HTTPS dans les appliances Web sécurisés (SWA) et les clients proxy.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès administratif à SWA
- Accès à l'interface graphique utilisateur (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.

Décryptage HTTPS

Le déchiffrement HTTPS (Hypertext Transfer Protocol Secure) SWA utilise des certificats racine et des fichiers de clé privée que vous téléchargez sur l'appliance pour chiffrer le trafic. Les fichiers de certificat racine et de clé privée que vous téléchargez vers l'appliance doivent être au format PEM.



Remarque : Format DER non pris en charge.

Vous pouvez également télécharger un certificat intermédiaire signé par une autorité de certification racine. Lorsque SWA crée un certificat qui représente le certificat du serveur, il envoie le certificat téléchargé avec le certificat imité à l'application cliente. Ainsi, tant que le certificat intermédiaire est signé par une autorité de certification racine à laquelle l'application cliente fait confiance, l'application fait confiance au certificat de serveur imité.

Configurer le certificat de déchiffrement dans SWA

Le SWA peut utiliser un certificat et une clé privée existants pour le déchiffrement HTTPS. Cependant, il peut y avoir confusion au sujet du type de certificat qui doit être utilisé, car tous les certificats x.509 ne fonctionnent pas.

Il existe deux types principaux de certificats : Certificats de serveur et Certificats racine. Tous les certificats x.509 contiennent un champ Contraintes de base, qui identifie le type de certificat :

- Subject Type=Entité finale - Certificat de serveur
- Subject Type=CA - Certificat racine

Télécharger un certificat racine et une clé

Étape 1. Dans l’interface utilisateur graphique, accédez à Security Services et sélectionnez HTTPS Proxy.
Étape 2. Cliquez sur Edit Settings.
Étape 3. Cliquez sur Use Uploaded Certificate and Key.
Étape 4. Cliquez sur Parcourir le champ Certificat pour accéder au fichier de certificat stocké sur l'ordinateur local.



Remarque : Si le fichier que vous téléchargez contient plusieurs certificats ou clés, le proxy Web utilise le premier certificat ou la première clé du fichier.

Étape 5. Cliquez sur Parcourir dans le champ Clé pour accéder au fichier de clé privée.



Remarque : La longueur de clé doit être de 512, 1 024 ou 2 048 bits.

Étape 6. Sélectionnez Key is Encrypted si la clé est chiffrée.
Étape 7. Cliquez sur Upload Files pour transférer les fichiers de certificat et de clé vers l'appliance Web sécurisée. Les informations de certificat téléchargées sont affichées sur la page Edit HTTPS Proxy Settings.
Étape 8. (Facultatif) Cliquez sur Download Certificate (Télécharger le certificat) pour transférer vers les applications clientes sur le réseau.

Étape 9. Soumettre et valider les modifications

Générer un certificat et une clé pour le proxy HTTPS

Étape 1. Dans l’interface utilisateur graphique, accédez à Security Services et sélectionnez HTTPS Proxy.
Étape 2. Cliquez sur Edit Settings.

Étape 3. Choisissez Utiliser le certificat et la clé générés.
Étape 4. Cliquez sur Generate New Certificate and Key.
Étape 5. Dans la boîte de dialogue Générer un certificat et une clé, entrez les informations à afficher dans le certificat racine. Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ Nom commun.
Étape 6. Cliquez sur Generate.
Étape 7. Les informations de certificat générées sont affichées sur la page Edit HTTPS Proxy Settings.
Étape 8. (Facultatif) Cliquez sur Download Certificate (Télécharger le certificat), afin de pouvoir le transférer vers les applications clientes sur le réseau.
Étape 9. (Facultatif) Cliquez sur le lien Download Certificate Signing Request, afin de pouvoir envoyer la demande de signature de certificat (CSR) à une autorité de certification.
Étape 10. (Facultatif) Téléchargez le certificat signé sur l'appareil Web sécurisé après l'avoir reçu de l'autorité de certification. Vous pouvez le faire à tout moment après avoir généré le certificat sur l'appliance.
Étape 11. Soumettre et valider les modifications

Importer un certificat

Importer un certificat de proxy en amont vers SWA

Si SWA est configuré pour utiliser un proxy en amont et que le proxy en amont est configuré pour le déchiffrement HTTPS, vous devez importer le certificat de chiffrement du proxy en amont vers SWA. Vous pouvez gérer la liste des certificats de confiance, y ajouter des certificats et en supprimer des certificats.

Étape 1. Dans l'interface utilisateur graphique, sélectionnez Network et choisissez Certificate Management.
Étape 2. Cliquez sur Gérer les certificats racines de confiance sur la page Gestion des certificats.
Étape 3. Pour ajouter un certificat racine approuvé personnalisé avec autorité de signature, ne figurant pas dans la liste reconnue par Cisco, cliquez sur Importer, puis envoyez le fichier de certificat.

Étape 4. Soumettre et valider les modifications

Importer un certificat SWA dans un autre SWA

Si vous avez téléchargé le certificat et la clé HTTPS dans un SWA pour le proxy HTTPS et que les fichiers d'origine sont accessibles, vous pouvez les importer dans un autre SWA à partir du fichier

de configuration.

Étape 1. Dans l'interface utilisateur graphique des deux SWA, sélectionnez System Administration et cliquez sur Configuration File.

Étape 2. Cliquez sur Download file sur l'ordinateur local pour afficher ou enregistrer.

Étape 3. Choisissez Encrypt passwords dans les fichiers de configuration.

Étape 4. (Facultatif) Choisissez Use a user-defined file name et ajoutez le nom souhaité au fichier de configuration.

Étape 5. Cliquez sur Submit sous Current Configuration pour télécharger le fichier configuration .xml.

Étape 6. Ouvrez les fichiers téléchargés avec des éditeurs de texte ou des éditeurs XML.

Étape 7. Copiez ces balises de SWA avec le certificat, copiez toutes les données à l'intérieur des balises et remplacez-les dans le fichier de configuration de l'autre SWA :

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

Étape 8 : enregistrement des modifications dans le fichier .xml du SWA de destination

Étape 9. Pour réimporter le fichier de configuration .xml modifié vers le SWA de destination, dans l'interface utilisateur graphique, sélectionnez System Administration et cliquez sur Configuration File.

Étape 10. Dans la section Load Configuration, cliquez sur Load a configuration file from local computer.

Étape 11. Cliquez sur Choose file et choisissez le fichier de configuration .xml modifié.

Étape 12. Cliquez sur Load pour importer le nouveau fichier de configuration avec le certificat et la clé.

Étape 13. Validez les modifications si le système vous y invite.

Importer un certificat SWA dans un client Windows

Pour importer le certificat SWA HTTPS Proxy comme étant approuvé sur les ordinateurs clients avec le système d'exploitation Microsoft Windows, procédez comme suit :

Étape 1. Cliquez sur Démarrer dans la barre des tâches et tapez Gérer les certificats des ordinateurs.
Étape 2. Sur la page Certificates-Local Computer, développez Trusted Root Certification et cliquez avec le bouton droit sur le dossier Certificates.
Étape 3. Cliquez sur All Tasks et choisissez Import.
Étape 4. Dans la page Assistant Importation de certificat, cliquez sur Suivant.
Étape 5. Pour importer le fichier de certificat SWA, cliquez sur Browse (Parcourir) et sélectionnez le certificat que vous avez téléchargé à partir de SWA.



Conseil : Pour télécharger le certificat SWA, reportez-vous à l'étape 8 de la section Upload a Root Certificate and Key ou à la section Generating a Certificate and Key for the HTTPS Proxy.

Étape 6. Cochez la case Placer tous les certificats dans le tableau suivant.
Étape 7. Sélectionnez Autorités de certification racines de confiance et cliquez sur Suivant.
Étape 8. Cliquez sur Finish.

Vous pouvez également exécuter cette commande pour importer le certificat vers les autorités de certification racine de confiance.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```



Remarque : Vous devez remplacer **<**Chemin d'accès à SWA Certificate/CertificateName.crt**>** par le chemin d'accès et le nom de fichier du certificat que vous avez téléchargés.

Importer le certificat SWA dans le client Mac

Étape 1 : téléchargement du certificat du proxy HTTPS de SWA vers le client Mac OS
Étape 2 : renommez l'extension de fichier en .crt.
Étape 3. Exécutez cette commande pour importer le certificat en tant que certificat approuvé :

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```



Remarque : Vous devez le remplacer par le chemin d'accès et le nom de fichier du certificat que vous avez téléchargés.

Importer un certificat SWA dans Ubuntu/Debian

Étape 1 : téléchargement du certificat du proxy HTTPS à partir de SWA
Étape 2. Ouvrez le fichier de certificat dans l'éditeur de texte et copiez tout son contenu.
Étape 3. Créez un nouveau fichier dans /usr/local/share/ca-certificates/ avec l'extension .crt.
Étape 4. Modifiez le fichier avec votre éditeur de texte souhaité et collez le texte copié dans le nouveau fichier, puis enregistrez.
Étape 5. Exécutez cette commande pour actualiser les certificats dans le système d'exploitation.

```
sudo update-ca-certificates
```



Conseil : Si vous avez le certificat stocké localement sur le client, vous pouvez copier le certificat dans /usr/local/share/ca-certificates/ et exécuter sudo update-ca-certificates.



Remarque : Dans certaines versions, vous devez installer le package ca-certificates avec cette commande : sudo apt-get install -y ca-certificates.

Importer un certificat SWA dans CentOS 6

Étape 1 : téléchargement du certificat du proxy HTTPS à partir de SWA
Étape 2. Ouvrez le fichier de certificat dans l'éditeur de texte et copiez tout le contenu du fichier.
Étape 3. Créez un nouveau fichier dans /etc/pki/ca-trust/source/anchors/ avec une extension .crt.
Étape 4. Modifiez le fichier avec l'éditeur de texte de votre choix et le texte copié précédemment dans le nouveau fichier, puis enregistrez.

Étape 5. Installez le package ca-certificates :

```
yum install ca-certificates
```

Étape 6. Exécutez cette commande pour actualiser les certificats dans le système d'exploitation :

```
update-ca-trust extract
```



Conseil : Si vous avez le certificat stocké localement sur le client, vous pouvez copier le certificat dans /etc/pki/ca-trust/source/anchors/ et exécuter update-ca-trust extraction après avoir installé les certificats ca.

Importer un certificat SWA dans CentOS 5

Étape 1 : téléchargement du certificat du proxy HTTPS à partir de SWA
Étape 2. Ouvrez le fichier de certificat dans l'éditeur de texte et copiez tout son contenu.
Étape 3. Créez un nouveau fichier dans le dossier actuel avec une extension .crt (par exemple, SWA.crt).
Étape 4. Modifiez le fichier /etc/pki/tls/certs/ca-bundle.crt avec l'éditeur de texte de votre choix, collez le texte copié à la fin du fichier et enregistrez.



Conseil : Si vous avez le certificat stocké localement sur le client (dans cet exemple, le nom de fichier est SWA.crt), vous pouvez ajouter le certificat avec cette commande : cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt.

Importer un certificat SWA dans Mozilla Firefox

Étape 1 : téléchargement du certificat de proxy HTTPS à partir de SWA
Étape 2 : renommez l'extension de fichier en .crt.
Étape 3. Ouvrez Firefox et cliquez sur le menu (trois barres dans le coin supérieur droit).
Étape 4. Sélectionnez Paramètres (dans certaines versions, il s'agit d'Options).
Étape 5. Cliquez sur Confidentialité et sécurité dans le menu de gauche et faites défiler jusqu'à Certificats.
Étape 6. Cliquez sur Afficher les certificats.

Étape 7. Cliquez sur l'onglet Autorités, puis sur Importer.
Étape 8. Choisissez le fichier de certificat et cliquez sur Ouvrir.
Étape 9. Cliquez sur OK.

Importer un certificat SWA dans Google Chrome

Étape 1 : téléchargement du certificat de proxy HTTPS à partir de SWA
Étape 2 : renommez l'extension de fichier en .crt.
Étape 3. Ouvrez Google Chrome et cliquez sur Personnaliser et contrôler Google Chrome (trois points en haut à droite).
Étape 4. Sélectionnez Settings.
Étape 5. Cliquez sur Privacy and Security dans le menu de gauche.
Étape 6. Sélectionnez Security.
Étape 7. Faites défiler la liste pour Gérer les certificats et cliquez sur le bouton à droite.
Étape 8. Sélectionnez l'onglet Autorités de certification racines de confiance et cliquez sur Importer.
Étape 9. Choisissez le fichier de certificat et cliquez sur Ouvrir.
Étape 10. Cliquez sur OK.



Remarque : Si vous installez le certificat SWA dans le système d'exploitation, Google Chrome fait confiance à ce certificat et il n'est pas nécessaire d'importer le certificat séparément dans votre navigateur.

Importer un certificat SWA dans Microsoft Edge/Internet Explorer

Microsoft Edge et Internet Explorer (IE) utilisent des certificats de système d'exploitation. Si vous installez le certificat SWA dans le système d'exploitation, il n'est pas nécessaire d'importer le certificat séparément dans votre navigateur.

Importer un certificat SWA dans Safari

Étape 1 : téléchargement du certificat du proxy HTTPS à partir de SWA
Étape 2 : renommez l'extension de fichier en .crt.
Étape 3. Dans le Launchpad, sélectionnez Keychain Access.
Étape 4. Dans le menu File, cliquez sur Add Keychain.
Étape 5. Choisissez le fichier de certificat SWA et cliquez sur Add.
Étape 6. Sélectionnez Security.
Étape 7. Faites défiler la liste pour Gérer les certificats et cliquez sur le bouton à droite.

Étape 8. Sélectionnez l'onglet Autorités de certification racines de confiance et cliquez sur Importer.
Étape 9. Choisissez le fichier de certificat et cliquez sur Ouvrir.
Étape 10. Cliquez sur OK.

Importer un certificat SWA de la stratégie de groupe vers les clients

Pour distribuer des certificats aux ordinateurs clients par la stratégie de groupe à partir d'Active Directory, procédez comme suit :

Étape 1 : téléchargement du certificat du proxy HTTPS à partir de SWA
Étape 2 : renommez l'extension de fichier en .crt.
Étape 3. Copiez le fichier de certificat sur votre contrôleur de domaine.
Étape 4. Sur le contrôleur de domaine, cliquez sur Démarrer et ouvrez le composant logiciel enfichable Gestion des stratégies de groupe.
Étape 5. Recherchez l'objet de stratégie de groupe (GPO) souhaité ou créez un nouvel objet de stratégie de groupe pour contenir le certificat SWA à importer vers le client.
Étape 6. Cliquez avec le bouton droit sur GPO, puis cliquez sur Modifier.
Étape 7. Dans le menu de gauche, accédez à Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique.
Étape 8. Cliquez avec le bouton droit sur les Autorités de certification racines de confiance, puis cliquez sur Importer.
Étape 9. Cliquez sur Next sur la page Welcome to the Certificate Import Wizard.
Étape 10. Choisissez le fichier de certificat SWA afin d'importer et cliquez sur Next.
Étape 11. Cliquez sur Placer tous les certificats dans le magasin suivant, puis cliquez sur Suivant.
Étape 12. Vérifiez que les informations fournies sont correctes, puis cliquez sur Finish.



Remarque : Dans certaines conditions, vous devez redémarrer le client ou exécuter gpupdate /force pour appliquer les modifications sur l'ordinateur client Active Directory.

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance - GD (General Deployment)
- Distribuer des certificats aux ordinateurs clients à l'aide de la stratégie de groupe | Microsoft Learn
- Assistance et documentation techniques - Cisco Systems

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.