Problème de certificat de serveur Unified Mobility Advantage avec ASA

Contenu

Introduction

Ce document décrit comment échanger des certificats auto-signés entre le dispositif de sécurité adaptatif (ASA) et le serveur Cisco Unified Mobility Advantage (CUMA) et vice versa. Il explique également comment résoudre les problèmes courants qui se produisent lors de l'importation des certificats.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme Cisco ASA 5500
- Serveur Cisco Unified Mobility Advantage 7

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Scénarios de déploiement

Il existe deux scénarios de déploiement pour le **proxy TLS** utilisé par la solution **Cisco Mobility Advantage**.

Remarque : dans les deux cas, les clients se connectent à partir d'Internet.

1. Le dispositif de sécurité adaptatif fonctionne à la fois comme pare-feu et proxy TLS.
2. Le dispositif de sécurité adaptatif fonctionne uniquement en tant que proxy TLS.

Dans les deux scénarios, vous devez exporter le **certificat de serveur Cisco UMA** et la **paire de clés** au **format PKCS-12** et l'importer dans le dispositif de sécurité adaptatif. Le certificat est utilisé lors de la connexion avec les clients Cisco UMA.

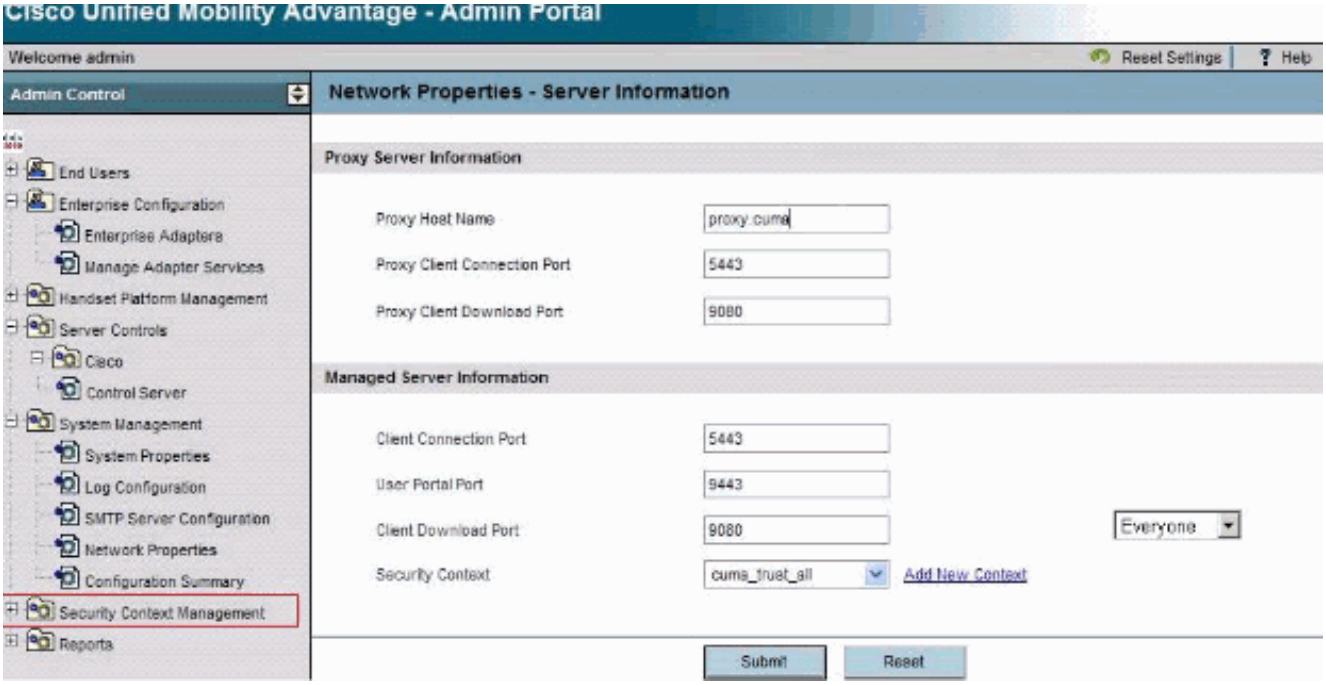
L'installation du certificat auto-signé du serveur Cisco UMA dans le magasin de confiance de l'appareil de sécurité adaptatif est nécessaire pour que l'appareil de sécurité adaptatif authentifie le serveur Cisco UMA pendant la connexion entre le proxy de l'appareil de sécurité adaptatif et le serveur Cisco UMA.

Installer le certificat auto-signé du serveur Cisco UMA

Tâches à effectuer sur le serveur CUMA

Ces étapes doivent être effectuées sur le serveur CUMA. Avec ces étapes, vous créez un certificat auto-signé sur CUMA pour échanger avec l'ASA avec CN=portal.aipc.com. Il doit être installé sur le magasin d'approbation ASA. Procédez comme suit :

1. Créez un certificat auto-signé sur le serveur CUMA.Connectez-vous au portail d'administration de Cisco Unified Mobility Advantage.Sélectionnez le **[+]** en regard de Security Context
   Management.



Choisissez **Contextes de sécurité**.Choisissez **Ajouter un contexte**.Entrez les informations suivantes :

```
Do you want to create/upload a new certificate? create
Context Name "cuma"
Description "cuma"
Trust Policy "Trusted Certificates"
Client Authentication Policy "none"
Client Password "changeme"
Server Name cuma.ciscodom.com
Department Name "vsec"
Company Name "cisco"
City "san jose"
State "ca"
Country "US"
```

2. Téléchargez les certificats auto-signés depuis Cisco Unified Mobility Advantage. Effectuez les étapes suivantes afin d'accomplir la tâche :Sélectionnez le **[+]** en regard de Security Context Management.Choisissez **Contextes de sécurité**.Choisissez **Gérer le contexte** en regard du contexte de sécurité qui contient le certificat à télécharger.Sélectionnez **Télécharger le certificat**.**Remarque :** si le certificat est une chaîne et comporte des certificats racine ou intermédiaire associés, seul le premier certificat de la chaîne est téléchargé. Cela suffit pour les certificats auto-signés.Enregistrez le fichier.
3. L'étape suivante consiste à ajouter le certificat auto-signé de Cisco Unified Mobility Advantage à l'ASA. Exécutez ces étapes sur l'ASA :Ouvrez le certificat auto-signé de Cisco Unified Mobility Advantage dans un éditeur de texte.Importez le certificat dans le magasin d'approbation de Cisco Adaptive Security Appliance :

```
cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert
cuma-asa(config-ca-trustpoint)# enrollment terminal
cuma-asa(config-ca-trustpoint)# crypto ca authenticate
cuma-server-id-cert
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

----BEGIN CERTIFICATE----
** paste the contents from wordpad **
----END CERTIFICATE----
```

4. Exporter le certificat auto-signé ASA sur le serveur CUMA. Vous devez configurer Cisco Unified Mobility Advantage pour exiger un certificat de l'appareil de sécurité adaptatif Cisco.

Complétez ces étapes afin de fournir le certificat auto-signé requis. Ces étapes doivent être effectuées sur l'ASA.Générer une nouvelle paire de clés :

```
cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024

INFO: The name for the keys will be: asa-id-key

Keypair generation process begin. Please wait...
```

Ajouter un nouveau point de confiance :

```
cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert

cuma-asa(config-ca-trustpoint)# keypair asa-id-key

cuma-asa(config-ca-trustpoint)# enrollment self
```

Inscrivez le point de confiance :

```
cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert
% The fully-qualified domain name in the certificate will be:
cuma-asa.cisco.com
% Include the device serial number in the subject name? [yes/no]: n
Generate Self-Signed Certificate? [yes/no]: y
```

Exporter le certificat dans un fichier texte.

```
cuma-asa(config)# crypto ca export asa-self-signed-id-cert
identity-certificate
The PEM encoded identity certificate follows:

-----BEGIN CERTIFICATE-----

Certificate data omitted

-----END CERTIFICATE-----
```

5. Copiez la sortie précédente dans un fichier texte et ajoutez-la au magasin d'approbation du serveur CUMA et utilisez la procédure suivante :Sélectionnez le **[+]** en regard de Security Context Management.Choisissez **Contextes de sécurité**.Choisissez **Gérer le contexte** en regard du contexte de sécurité dans lequel vous importez le certificat signé.Sélectionnez **Importer** dans la barre Certificats approuvés.Collez le texte du certificat.Nommez le certificat.Choisissez **Importer**.**Remarque :** pour la configuration de la destination distante, appelez le téléphone de bureau afin de déterminer si le téléphone portable sonne en même temps. Cela confirmerait que la connexion mobile fonctionne et qu'il n'y a aucun problème avec la configuration de la destination distante.

Problème d'ajout de la demande de certificat CUMA à d'autres autorités de certification

Problème 1

De nombreuses installations de démonstration/prototypes où il est utile si la solution CUMC/CUMA fonctionne avec des certificats de confiance sont auto-signés ou obtenus d'*autres autorités de certification*. Les certificats Verisign sont chers et il faut beaucoup de temps pour obtenir ces certificats. Il est bon que la solution prenne en charge les certificats auto-signés et les certificats d'autres autorités de certification.

Les certificats actuellement pris en charge sont GeoTrust et Verisign. Ceci est documenté dans l'ID de bogue Cisco CSCta62971 (clients enregistrés uniquement)

Erreur : Impossible de se connecter

Lorsque vous essayez d'accéder à la page du portail utilisateur, par exemple `https://<hôte>:8443`, le message d'erreur `Impossible de se connecter` apparaît.

Solution

Ce problème est documenté dans l'ID de bogue Cisco CSCsm26730 (clients enregistrés uniquement). Pour accéder à la page du portail utilisateur, procédez comme suit :

La cause de ce problème est le caractère dollar, donc évitez le caractère dollar avec un autre caractère dollar dans le **fichier server.xml** du serveur géré. Par exemple, modifiez /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

En ligne : **keystorePass=« pa$word »** maxSpareThreads=« 15 »

Remplacez le caractère `$` par `$$`. Il ressemble à **keystorePass=« pa$$word »** maxSpareThreads=« 15 ».

Certaines pages du portail d'administration CUMA ne sont pas accessibles

Ces pages ne peuvent pas être affichées dans le **portail d'administration CUMA** :

- activer/désactiver l'utilisateur
- recherche/maintenance

Si l'utilisateur clique sur l'une des deux pages ci-dessus dans le menu de gauche, le navigateur semble indiquer qu'il charge une page, mais rien ne se passe (seule la page précédente qui était dans le navigateur est visible).

Solution

Afin de résoudre ce problème lié à la page utilisateur, modifiez le port utilisé pour Active Directory sur **3268** et redémarrez CUMA.

Informations connexes

- Configuration pas à pas du proxy ASA-CUMA
- Présentation de tous les ASR5000 v1
- Mise à niveau de Cisco Unified Mobility Advantage
- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Support et documentation techniques - Cisco Systems