Question de certificat de serveur de Cisco Unified Mobility Advantage avec l'ASA

Contenu

Introduction

Ce document décrit comment permuter les Certificats auto-signés entre l'appliance de sécurité adaptable (ASA) et le serveur du Cisco Unified Mobility Advantage (CUMA) et vice versa. Il explique également comment dépanner les problèmes courants qui se produit tandis que vous importez les Certificats.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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 y a deux scénarios de déploiement pour le **proxy de TLS** utilisé par la solution d'**avantage de mobilité Cisco**.

Remarque: Dans les deux scénarios, les clients se connectent de l'Internet.

1. L'appliance de sécurité adaptable fonctionne comme Pare-feu et proxy de TLS.
2. L'appliance de sécurité adaptable fonctionne comme proxy de TLS seulement.

Dans les deux scénarios, vous devez exporter le **certificat** et la **paire de clés de serveur d'UMA de Cisco** dans le format **PKCS-12** et l'importer à l'appliance de sécurité adaptable. Le certificat est utilisé pendant la prise de contact avec les clients d'UMA de Cisco.

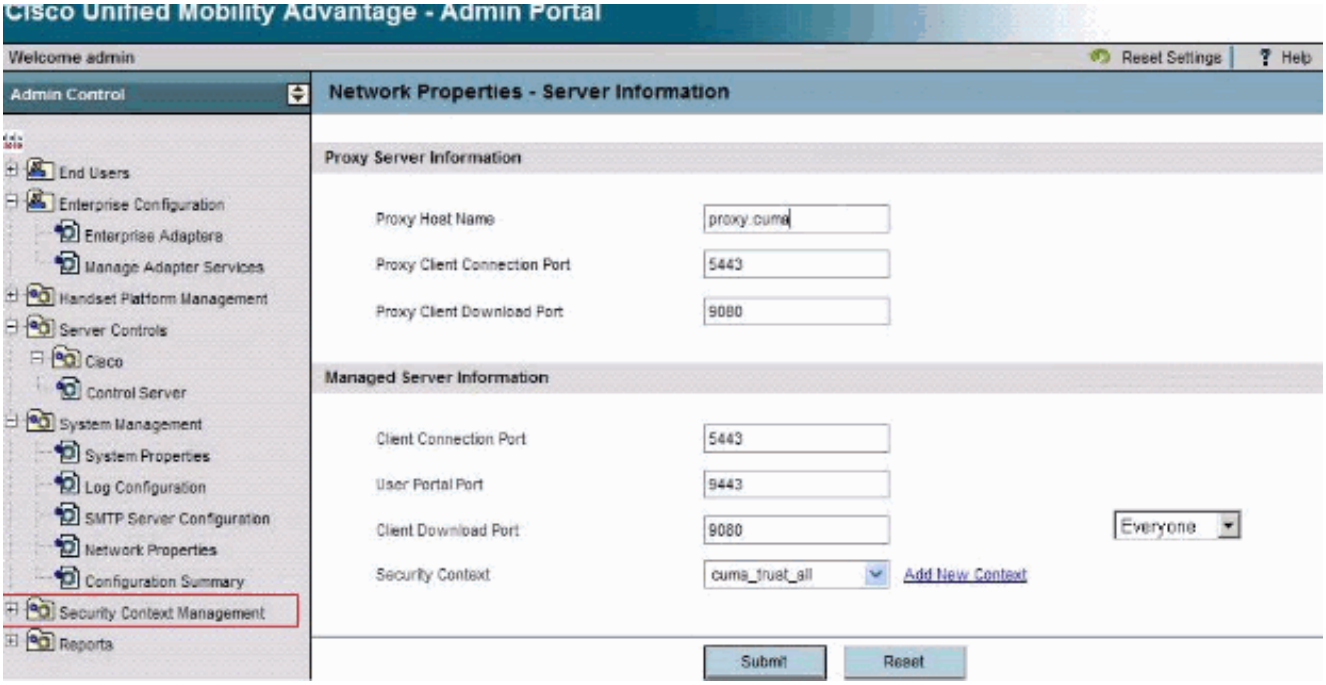
L'installation du certificat auto-signé par serveur d'UMA de Cisco dans le truststore d'appliance de sécurité adaptable est nécessaire pour que l'appliance de sécurité adaptable authentifie le serveur d'UMA de Cisco pendant la prise de contact entre le proxy d'appliance de sécurité adaptable et le serveur d'UMA de Cisco.

Installez le certificat Auto-signé par serveur d'UMA de Cisco

Tâches d'être fait sur le serveur CUMA

Ces étapes doivent être faites sur le serveur CUMA. Avec ces étapes, vous créez un certificat auto-signé sur CUMA pour permuter avec l'ASA avec CN=portal.aipc.com. Ceci doit être installé sur la mémoire de confiance ASA. Procédez comme suit :

1. Créez un CERT auto-signé sur le serveur CUMA.Connectez-vous au portail d'admin de Cisco Unified Mobility Advantage.Choisissez **[+]** près de la Gestion de contexte de sécurité.



Choisissez les **contextes de sécurité**.Choisissez **ajoutent le 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 du Cisco Unified Mobility Advantage. Terminez-vous ces étapes afin d'accomplir la tâche :Choisissez **[+]** près de la Gestion de contexte de sécurité.Choisissez les **contextes de sécurité**.Choisissez **gèrent le contexte** près du contexte de sécurité qui tient le certificat pour le télécharger.Choisissez le **certificat de téléchargement**.**Remarque:** Si le certificat est une chaîne, et a associé des Certificats de racine ou d'intermédiaire, seulement le premier certificat dans la chaîne est téléchargé. C'est suffisant pour les Certificats auto-signés.Enregistrez le fichier.
3. L'étape suivante est d'ajouter le certificat auto-signé du Cisco Unified Mobility Advantage sur l'ASA. Terminez-vous ces étapes sur l'ASA :Ouvrez le certificat auto-signé du Cisco Unified Mobility Advantage dans un éditeur de texte.Importez le certificat dans la mémoire de confiance d'appliance de sécurité adaptable Cisco :`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. Certificat auto-signé par ASA d'exportation sur le serveur CUMA. Vous devez configurer le Cisco Unified Mobility Advantage pour avoir besoin d'un certificat de l'appliance de sécurité adaptable Cisco. Terminez-vous ces étapes afin de fournir le certificat auto-signé requis. Ces étapes doivent être faites sur l'ASA.Générez 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...`Ajoutez 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-vous 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`Exportez le certificat à 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 sur un fichier texte et ajoutez-la à la mémoire de confiance de serveur CUMA et utilisez cette procédure :Choisissez **[+]** près de la Gestion de contexte de sécurité.Choisissez les **contextes de sécurité**.Choisissez **gèrent le contexte** près du contexte de sécurité dans lequel vous importez le certificat signé.Choisissez l'**importation** dans la barre de Certificats de confiance.Collez le texte de certificat.Nommez le certificat.Choisissez l'**importation**.**Remarque:** Pour la configuration de destination distante, appel dans le téléphone de bureau afin de déterminer si le téléphone portable sonne en même temps. Ceci confirmerait que le mobile connectent des travaux et qu'il n'y a aucune question avec la configuration de destination distante.

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

Problème 1

Beaucoup installations de démonstration/prototype où il aide si les travaux de solution CUMC/CUMA avec les Certificats de confiance auto-sont signés ou obtenus d'*autres autorités de certification*. Les certificats Verisign sont chers et cela prend un longtemps d'obtenir ces Certificats. Il est bon si les prises en charge des solutions auto-signaient des Certificats et des Certificats de l'autre CAs.

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

Erreur : Incapable de se connecter

Quand vous essayez d'accéder à la page du portail d'utilisateur, par exemple, `https://<host>:8443`, l'`incapable de connecter le` message d'erreur apparaît.

Solution

Cette question est documentée dans l'ID de bogue Cisco CSCsm26730 (clients enregistrés seulement). Afin d'accéder à la page du portail d'utilisateur, terminez-vous ce contournement :

La cause de cette question est le caractère du dollar, ainsi échappez au caractère du dollar avec un autre caractère du dollar dans le **fichier server.xml du** serveur géré**. Par exemple**, éditez /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml.

Dans la ligne : **keystorePass= " pa$word »** maxSpareThreads="15"

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

Quelques pages dans le portail d'admin CUMA ne sont pas accessibles

Ces pages ne peuvent pas être visualisées dans le **portail d'admin CUMA** :

- lancez/retirez du service actif l'utilisateur
- recherche/maintenance

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

Solution

Afin de résoudre ce problème a associé à la page utilisateur, change le port utilisé pour le Répertoire actif à **3268** et redémarre le CUMA.

Informations connexes

- Configuration de pas à pas de proxy ASA-CUMA
- AI ASR5000 v1 d'Introduccion
- Évolution du 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