Contenu

Introduction

Beaucoup d'administrateurs réseau choisissent d'implémenter le Cisco Unified Communications Manager Express (CME) avec la Sécurité. Au lieu de l'autorité de certification intégrée IOS (IOS-CA), les administrateurs réseau peuvent choisir d'intégrer CME sécurisé avec leur infrastructure existante d'Infrastructure à clés publiques (PKI). Ce document décrit comment configurer CME sécurisé pour fonctionner avec la signalisation sécurisée, et des medias, par l'intermédiaire des Certificats de tiers.

Conditions préalables

Conditions requises

Ce document suppose que le Cisco Unified Communications Manager Express (CME) dans votre environnement s'exécute et entièrement - fonctionnel. Tous les téléphones qui doivent être opérationnels sur le besoin de Cisco Unified CME Secure de pouvoir s'enregistrer d'abord avec succès à CME. Référez-vous au guide d'administrateur système de Cisco Unified Communications Manager Express pour les informations sur la façon dont configurer CME.

Ce document suppose également que la Voix et les fonctionnalités de sécurité sont activées.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Unified Communications Manager Express (CME).

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.

Configurez

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Étapes récapitulatives de configuration

1. Créez l'exemple IOS-CA.
2. Créez les points de confiance pour tenir les Certificats CA de tiers.
3. Générez les demandes de signature de certificat (CSRs) des points de confiance.
4. Signez CSRs avec l'utilisation d'authentification de serveur, et obtenez la certification CA.
5. Authentifiez les points de confiance avec le certificat de CA, et importez les certificats d'identité respectifs.
6. Validez les points de confiance de certificat de tiers.
7. Créez le point de confiance IOS CA CME.
8. Configurez le client de la liste de confiance de certificat (CTL).
9. Configurez le serveur de la fonction de proxy d'autorité de certification (CAPF).
10. Configurez le service téléphonique.
11. Configurez le téléphone de test.
12. Vérifiez.

Exemple de configuration détaillée

1. Créez l'exemple IOS-CA. L'exemple IOS-CA produit le certificat auto-signé qui est utilisé pour signer le téléphone localement - le certificat significatif (LSC).
2. Créez les points de confiance qui génèreront le CSRs pour la signature de tiers. Ces points de confiance tiennent par la suite le certificat de CA de tiers, aussi bien que les certificats d'identité, qui sont un résultat du CSRs.

3. Générez CSRs des points de confiance. La commande de **crypto pki enroll** produit le CSR qui est fourni au tiers CA pour signer.

   Exemple 1 :
   Exemple 2 :
4. Employez les deux CSRs afin de générer des Certificats avec des autorisations d'authentification de serveur.
   Notes : Il est essentiel que la pleine chaîne de certificat soit obtenue pour un des deux Certificats du CA. La chaîne de certificat fournit le CA et le certificat d'identité du CA de signature.Assurez-vous que les Certificats sont téléchargés dans le format de la base 64.Il est très important que le certificat de CA soit utilisé pour l'authentification pour chaque point

de confiance et que les certificats d'identité sont importés dans chaque point de confiance, dans cette commande.

5. Authentifiez les points de confiance avec les Certificats CA, et importez les certificats d'identité SAST.

   Exemple 1 :

   Exemple 2 :
6. Une fois que le CA et des certificats d'identité sont chargés dans les points de confiance respectifs, validez la chaîne de certificat pour chaque point de confiance. Cette étape s'assure que les étapes précédentes ont été avec succès terminées.

7. Créez le point de confiance IOS CA CME.

   Puisque le point de confiance IOS-CA ne peut pas être utilisé pour l'authentification client connexion de niveau de degré de sécurité de transport ((TLS) avec des téléphones), vous devez créer un autre point de confiance et mettre le certificat IOS-CA dans lui.

   Ce point de confiance est utilisé pour autoriser seulement la demande du téléphone IP d'une connexion de TLS (ainsi eux peut s'enregistrer correctement).

8. Configurez le client CTL.

   Remarque: Assurez-vous que le fichier CTL a été créé avec succès :
9. Configurez le serveur CAPF.

10. Configurez le service téléphonique.

11. Configurez le téléphone de test (ephone) afin d'améliorer son certificat et mode chiffré par utilisation. Une fois que la configuration est complète, remettez à l'état initial le téléphone et attendez-le pour s'enregistrer.

    Remarque: Avant que le téléphone soit remis à l'état initial, assurez-vous qu'il n'y a aucun présent de configuration de sécurité déjà. Si une configuration de sécurité est présente, elle doit être manuellement retirée ou se terminer une réinitialisation aux paramètres d'usine du téléphone de test avant l'enregistrement pour sécuriser le Cisco Unified CME.

    Pour remettre à l'état initial le téléphone, exécutez ces commandes :Une fois le téléphone a reçu le LSC mis à jour, la commande de **chaîne null d'authentique-mode de mise à jour de CERT-exécution** est retiré.
12. Vérifiez que le téléphone s'est inscrit à l'authentification et au cryptage.

Le Cisco Unified CME sécurisé devrait être entièrement - fonctionnel avec des Certificats de tiers.

Informations connexes

- Guide d'administrateur système de Cisco Unified Communications Manager Express
- Voix sécurisée sur Cisco TAC Wiki
- Support et documentation techniques - Cisco Systems