Contenu

Introduction

Ce document décrit comment employer le Transport Layer Security (TLS) pour sécuriser des réponses du service d'enveloppe recommandée de Cisco (CRES), qui permet à un utilisateur pour ne pas avoir besoin de les déchiffrer, en association avec l'appliance de sécurité du courrier électronique de Cisco (ESA).

Comment est-ce que j'emploie le TLS pour sécuriser des réponses décryptées CRES ?

Par défaut, des réponses à un email sécurisé sont chiffrées par CRES et en fonction envoyées à votre mail gateway. Ils traversent alors à vos serveurs de messagerie chiffrés pour que l'utilisateur s'ouvre avec leurs qualifications CRES.

Afin d'éviter le besoin de l'utilisateur d'authentifier avec CRES pour ouvrir la réponse sécurisée, CRES livre sous une forme « décryptée » pour envoyer par mail les passerelles qui prennent en charge le TLS. Dans la plupart des cas le mail gateway est l'ESA, et cet article est applicable.

Cependant, s'il y a un autre mail gateway qui se repose devant l'ESA tel qu'un filtre externe de Spam, là n'est aucun besoin de certificate/TLS/mail circulent la configuration sur votre ESA. Dans ce cas, vous pouvez ignorer les étapes 1 3 dans la partie Solution de ce document. Pour que les réponses décryptées fonctionnent dans cet environnement, le filtre externe de Spam (mail gateway) est l'appliance qui doit prendre en charge le TLS. S'ils prennent en charge le TLS, vous pouvez faire confirmer CRES ceci et vous obtenir installez pour des réponses « décryptées » afin de sécuriser des emails.

Solution

1. Obtenez et installez un certificat signé et le certificat intermédiaire sur l'ESA. Remarque: Il est important vous obtiennent le certificat intermédiaire de votre autorité de signature comme certificat de démonstration qui est livré sur l'appliance fait échouer le processus de vérification CRES.
2. Créez une nouvelle stratégie de flux de courrier : Du GUI, choisissez les **stratégies de messagerie > les stratégies de flux de courrier > ajoutent la stratégie….**Écrivez un nom et laissez tout le reste au par défaut excepté des *fonctionnalités de sécurité : TLS.* Placez ceci à **requis**.
3. Créez un nouveau groupe d'expéditeur : Du GUI, choisissez les **stratégies de messagerie > l'aperçu de CHAPEAU > ajoutent le groupe d'expéditeur….**Écrivez un nom et placez le numéro de commande à #1. Vous pouvez également écrire un commentaire facultatif.

Choisissez la stratégie de flux de courrier que vous avez créé dans le congé d'étape 2. tout autrement blanc.Cliquez sur Submit **et ajoutez les expéditeurs >>**.
4. Dans le domaine d'expéditeur, entrez dans ces plages et adresses Internet IP :
5. Soumettez et commettez les modifications.
6. Après que vous soyez sûr l'ESA est préparé pour le TLS des serveurs CRES, suivent les étapes dedans afin d'inviter les serveurs CRES à commencer à utiliser le TLS.

Informations connexes

- FOIRE AUX QUESTIONS ESA : Quels sont les IPS et les adresses Internet du CRES introduisent des serveurs ?
- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems