Contenu

Introduction

Ce document décrit le type de certificat qui devrait être utilisé pour le déchiffrement HTTPS sur une appliance de sécurité Web de Cisco (WSA).

Aperçu de certificat

Le WSA a la capacité d'utiliser un certificat valable et une clé privée pour l'usage avec le déchiffrement HTTPS. Cependant, il pourrait y avoir confusion au sujet du type de certificat qui devrait être utilisé, puisque non tous les Certificats x.509 fonctionnent.

Il y a deux types importants de Certificats : **Certificats** et **certificats racine de serveur**. Tous les Certificats x.509 contiennent des contraintes de base mettent en place, qui identifie le type de certificat :

- **Entité soumise de Type=End** - Certificat de serveur
- **Type=CA soumis** - Certificat racine

> Remarque: Vous devez utiliser un certificat racine, également visé comme un Autorité de certification (CA) signant le certificat, pour le déchiffrement HTTPS sur le WSA.

Certificats racine

Un certificat racine est spécifiquement créé afin de signer des Certificats de serveur. Vous pouvez créer et actionner votre propre CA et signer vos propres Certificats de serveur.

> Remarque: Puisqu'un certificat racine signe seulement d'autres Certificats, il ne peut pas être utilisé sur un web server afin d'exécuter le cryptage et le déchiffrement HTTPS.

Le WSA doit employer un certificat racine afin de générer activement des Certificats de serveur

pour le déchiffrement HTTPS. Il y a deux options disponibles pour l'utilisation de certificat racine :

- Générez un certificat racine sur le WSA. Le WSA crée son propres certificat racine et clé privée, et il emploie cette paire de clés afin de signer des Certificats de serveur.

- Vous pouvez télécharger un certificat racine en cours et sa clé privée dans le WSA. Le champ commun du nom (NC) dans un certificat racine identifie l'entité (typiquement un nom de société) cette des confiances tous les Certificats de serveur qui contiennent sa signature.

  Remarque: Avant qu'un certificat de serveur puisse êtes de confiance, il doit être signé par un certificat racine qui a une clé publique actuelle dans le navigateur Web.

Certificats de serveur

Un certificat de serveur est spécifiquement créé afin de pour être utilisé dans le cryptage et le déchiffrement HTTPS et afin de vérifier l'authenticité d'un serveur spécifique. Des Certificats de serveur sont signés par un CA avec l'utilisation du certificat racine CA. Un exemple classique d'un CA est Verisign ou Thawte.

Remarque: Un certificat de serveur ne peut pas être utilisé afin de signer d'autres Certificats ; donc, le déchiffrement HTTPS ne fonctionne pas si un certificat de serveur est installé sur le WSA.

Le champ NC dans un certificat de serveur spécifie l'hôte pour lequel le certificat est destiné pour être utilisé. Par exemple, **https://www.verisign.com** utilise un certificat de serveur avec une NC de **www.verisign.com**.

Informations connexes

- Utilisation de certificat des appareils de sécurité Web (WSA) (déchiffrement HTTPS, procédure de connexion GUI, cryptage de créance)
- Étapes pour activer le proxy HTTPS en WSA et option de la demande de signature de certificat (CSR)
- Étapes pour activer le proxy HTTPS en fonction (WSA) et téléchargeant la racine/option intermédiaire de certificat
- Support et documentation techniques - Cisco Systems