Créez une demande de signature de certificat sur un ESA

Contenu

Introduction

Ce document décrit comment créer une demande de signature de certificat (CSR) sur une appliance de sécurité du courrier électronique (ESA).

Créez un CSR sur un ESA

En date d'AsyncOS 7.1.1, l'ESA peut créer un certificat auto-signé pour votre propre utiliser-et génèrent un CSR pour soumettre à une autorité de certification et pour obtenir le certificat public. L'autorité de certification renvoie un certificat public de confiance signé par une clé privée. Employez la page de **réseau > de Certificats** dans le GUI ou la commande de **certconfig** dans le CLI afin de créer le certificat auto-signé, générer le CSR, et installer le certificat public de confiance.

Si vous saisissez ou créez un certificat pour la première fois, recherchez l'Internet pour « des Certificats de serveur SSL de services d'autorité de certification » et choisissez le service que ce meilleur répond aux besoins de votre organisation. Suivez les instructions du service afin d'obtenir un certificat.

Étapes de configuration sur le GUI

1. Afin de créer un certificat auto-signé, cliquez sur Add le **certificat à la** page de réseau > de Certificats dans le GUI (ou la commande de **certconfig** dans le CLI). À la page de certificat d'ajouter, choisissez **créent le certificat Auto-signé**.
2. Écrivez ces informations pour le certificat auto-signé : Nom commun - Le nom de domaine complet.Organisation - Le nom juridique précis de l'organisation.Unité organisationnelle - Section de l'organisation.Ville (localité) - Ville où l'organisation est légalement localisée.État (province) - L'état, le pays, ou la région où l'organisation est légalement localisée.Pays - L'abréviation à deux lettres de l'organisation internationale de normalisation (OIN) du pays où l'organisation est légalement localisée.Durée avant expiration - Le nombre de jours avant le certificat expire.Taille de clé privée - Taille de la clé privée à se produire pour le CSR.

Seulement 2048-bit et 1024-bit sont pris en charge.
3. Cliquez sur Next afin de visualiser le certificat et les informations de signature.
4. Écrivez un nom pour le certificat. AsyncOS assigne le nom commun par défaut.
5. Si vous voulez soumettre un CSR pour le certificat auto-signé à une autorité de certification, cliquez sur Download la **demande de signature de certificat** afin de sauvegarder le CSR dans le format du Privacy Enhanced Mail (PEM) à des gens du pays ou à un ordinateur du réseau.
6. Cliquez sur Submit afin de sauvegarder le certificat et commettre vos modifications. Si vous laissez les modifications non engagées, la clé privée obtiendra perdu et le certificat signé ne peut pas être installé.

Quand l'autorité de certification renvoie le certificat public de confiance signé par une clé privée, cliquez sur le nom du certificat à la page de Certificats et entrez dans le chemin au fichier sur votre ordinateur local ou réseau afin de télécharger le certificat. Assurez-vous que le certificat public de confiance que vous recevez est dans le format PEM ou un format que vous pouvez convertir en PEM avant qu'il soit téléchargé à l'appliance. Des outils pour se terminer ceci sont inclus avec OpenSSL, logiciel gratuit disponible chez http://www.openssl.org.

Si vous téléchargez le certificat de l'autorité de certification, le certificat existant est remplacé. Vous pouvez également télécharger un certificat intermédiaire lié au certificat auto-signé. Vous pouvez utiliser le certificat avec un auditeur public ou privé, les services HTTPS d'une interface IP, l'interface de Protocole LDAP (Lightweight Directory Access Protocol), ou toutes les connexions sortantes de Transport Layer Security (TLS) aux domaines de destination.

Informations connexes

- Guide complet d'installation pour le TLS sur l'ESA
- Support et documentation techniques - Cisco Systems