Comment installer un certificat SSL chaîné au module CSS SSL

Contenu

Introduction

Une chaîne de certificat est un ordre des Certificats, où chaque certificat dans la chaîne est signé par le certificat ultérieur. Le but de la chaîne de certificat est d'établir une chaîne de confiance d'un certificat de pair à un certificat de confiance de l'autorité de certification (CA). Le CA garantit pour l'identité dans le certificat de pair en le signant. Si le CA est un au lequel vous faites confiance (indiqué par la présence d'une copie du certificat de CA dans votre répertoire de certificat racine), ceci vous implique peut faire confiance au certificat signé de pair aussi bien.

Souvent, les clients ne reçoivent pas les Certificats parce qu'ils n'ont pas été créés par un CA connu. Le client déclare typiquement que la validité du certificat ne peut pas être vérifiée. C'est le cas quand le certificat est signé par un intermédiaire CA, qui n'est pas connu au navigateur de client. En pareil cas, il est nécessaire d'utiliser un certificat ssl enchaîné ou de délivrer un certificat le groupe. Ce document discute comment installer correctement un certificat enchaîné de Protocole SSL (Secure Socket Layer) sur un module SSL CSS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Module SSL CSS11506 (cryptage fort) - CSS 506-SSL-K9
- Module SSL CSS11501 (cryptage fort) - CSS 501-SSL-K9
- Seulement module de commutation CSS11506 - CSS 506-SM
- WebNS 7.10 et 7.20

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 des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Instructions pas à pas

Cette section affiche comment installer un certificat enchaîné sur le module SSL CSS avec le CSS 11500.

Si le certificat enchaîné est dans des plusieurs fichiers, utilisez la procédure tracée les grandes lignes ci-dessous.

1. Convertissez tous les Certificats en même format. Si les Certificats sont distincts et pas dans le format du Privacy Enhanced Mail (PEM), vous devez les convertir en format PEM et puis concaténer.
2. Concaténez tous les Certificats dans un fichier ; assurez-vous qu'ils sont concaténés pendant qu'ils apparaissent dans la chaîne. Le certificat de serveur devrait être le premier dans la chaîne, suivie des intermédiaires (des Certificats de serveur et des Certificats CA intermédiaires).
3. Importez le fichier du certificat concaténé dans le CSS.
4. Associez le certificat au SSL-serveur.
5. Appliquez le CA du SSL-serveur dans la SSL-proxy-liste.

Si tous ces Certificats sont enchaînés dans un fichier PKCS#12 (autant de des Certificats PKCS#12 soyez), vous devriez importer le certificat enchaîné comme PKCS#12, et l'associé/l'appliquent en tant que normale. PKCS#12 ne sont pas capables d'être concaténé.

Remarque: Les formats distingués de la règle de codage (DER) ne prennent en charge pas des chaînes, ainsi ceci ne devrait pas être une question.

Pour vérifier, la clé qui doit être utilisée est la clé qui a généré le fichier de la demande de signature de certificat (CSR) pour créer le certificat de serveur. Il y a seulement une clé pour un certificat, que ce soit enchaîné ou militaire de carrière. Veillez à vérifier le certificat et la clé après qu'ils soient importés. Vous pouvez émettre la commande affichée ci-dessous.

```
(config)# ssl verify myrsacert1 myrsakey1 Certificate and key match
```

Informations connexes

- Guide de configuration avancée CSS
- Sécurisez/installation d'ID de serveur site de commerce pro - accélérateur de commerce électronique d'Intel NetStructure 7110
- Support produit de Services de mise en réseau d'applications
- Support et documentation techniques - Cisco Systems