ASA 8.x : Renouveler et installer le certificat SSL avec ASDM

Contenu

Introduction

La procédure dans ce document est un exemple et peut être utilisée comme instruction avec n'importe quel constructeur de certificat ou votre propre serveur de certificat racine. Des conditions requises spéciales de paramètre de certificat sont parfois exigées par votre constructeur de certificat, mais ce document est destiné pour fournir l'étape nécessaire générale pour renouveler un certificat ssl et pour l'installer sur une ASA qui utilise le logiciel 8.0.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Cette procédure concerne des versions 8.x ASA avec la version 6.0(2) ou ultérieures ASDM.

La procédure dans ce document est basée sur une configuration valide avec un certificat installé et utilisé pour l'accès de VPN SSL. Cette procédure n'affecte pas votre réseau tant que le certificat valable n'est pas supprimé. Cette procédure est un processus pas à pas sur la façon dont émettre un nouveau CSR pour un certificat valable avec le même certificat racine qui a émis la racine d'origine CA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. 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.

Procédure

Procédez comme suit :

1. Sélectionnez le certificat que vous voulez renouveler sous la configuration > la Gestion de périphériques > les certificats d'identité, et puis cliquez sur Add.**Figure 1**
2. Sous ajoutez le certificat d'identité, sélectionnez l'**ajouter une nouvelle** case d'option de **certificat d'identité**, et choisissez votre paire de clés du menu déroulant.**Remarque:** Il n'est pas recommandé pour utiliser le <Default-RSA-Key> parce que si vous régénérez votre ssh key, vous infirmez votre certificat. Si vous n'avez pas une clé RSA, complète fait un pas a et B. Autrement continuez à l'étape 3.**Figure 2** (Facultatif) terminez-vous ces étapes si vous ne faites pas configurer une clé RSA encore, autrement saut à l'étape 3.Cliquez sur New….Écrivez le nom de paire de clés dans la **nouvelle** zone d'**identification de paire de clés d'entrer**, et le clic **se produisent maintenant**.**Figure 3**
3. Clic **choisi**.
4. Écrivez les attributs appropriés de certificat suivant les indications de la figure 4. Une fois que terminé, cliquez sur OK. Cliquez sur Add alors le **certificat**.**Figure 4** CLI sorti :
```
crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec fqdn 5540-uwe
subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA enrollment terminal
crypto ca enroll ASDM_TrustPoint0
```
5. Dans la fenêtre contextuelle de **demande de certificat d'identité**, sauvegardez votre demande de signature de certificat (CSR) à un fichier texte, et cliquez sur OK.**Figure 5**
6. (Facultatif) vérifiez dans l'ASDM que le CSR est en suspens, suivant les indications de la figure 6.**Figure 6**
7. Soumettez la demande de certificat à l'administrateur de certificat, qui délivre le certificat sur le serveur. Ceci peut être par une interface web, courrier électronique, ou directement au serveur de la racine CA pour le processus de question de certificat.
8. Terminez-vous ces étapes afin d'installer le certificat renouvelé.Sélectionnez la demande en attente de certificat sous la configuration > la Gestion de périphériques > les certificats d'identité, suivant les indications de la figure 6, et le clic **installent**.Dans la fenêtre de certificat d'identité d'installer, sélectionnez la **pâte les données de certificat dans la** case d'option du **format base-64**, et le clic **installent le certificat**.**Remarque:** Alternativement, si le certificat est délivré dans un fichier de .cer plutôt puis un fichier ou un courrier électronique basé par texte, vous pouvez également sélectionner **installez à partir d'un fichier**, parcourez au fichier approprié sur votre PC, clic **installez le fichier du certificat d'ID** et puis cliquez sur **installez le certificat**.**Figure 7**CLI sorti :
```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated
wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```
9. Une fenêtre apparaît qui confirme le certificat est avec succès installée. Clic « CORRECT » pour confirmer.**Figure 8**

10. Assurez que votre nouveau certificat apparaît sous des certificats d'identité.**Figure 9**
11. Terminez-vous ces étapes afin de lier le nouveau certificat à l'interface :Choisissez la **configuration > la Gestion de périphériques > a avancé > des configurations SSL**, suivant les indications de la figure 10.Sélectionnez votre interface sous des Certificats, et cliquez sur Edit.**Figure 10**
12. Choisissez votre nouveau certificat du menu déroulant, cliquez sur OK, et cliquez sur Apply.`ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1`
    `ssl trust-point ASDM_TrustPoint0 outside`**Figure 11**
13. Sauvegardez votre configuration dans l'ASDM ou sur le CLI.

Vérifiez

Vous pouvez employer l'interface CLI afin de vérifier que le nouveau certificat est installé sur l'ASA correctement, suivant les indications de cette sortie témoin :

```
ASA(config)#show crypto ca certificates Certificate Status: Available Certificate Serial Number:
61bf707b000000000027 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=MS-CA Subject Name: cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems
st=CA c=US CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008
end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate
Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

Dépannez

(Facultatif) vérifiez sur le CLI que le certificat correct est appliqué à l'interface :

```
ASA(config)#show running-config ssl ssl trust-point ASDM_TrustPoint0 outside !--- Shows that the
correct trustpoint is tied to the outside interface that terminates SSL VPN. ASA(config)#
```

Comment copier des Certificats SSL d'une ASA à l'autre

Ceci peut être fait si vous aviez généré des clés exportables. Vous devez exporter le certificat à un fichier PKCS. Ceci inclut exporter toutes les clés associées.

Utilisez cette commande d'exporter votre certificat par l'intermédiaire du CLI :

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Remarque: Phrase de passe - utilisée pour protéger le fichier pkcs12.

Utilisez cette commande d'importer votre certificat par l'intermédiaire du CLI :

```
SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase>
```

Remarque: Ce mot de passe devrait être identique qu'utilisé en exportant le fichier.

Ceci peut également être fait par l'ASDM pour une paire de Basculement ASA. Terminez-vous ces étapes pour exécuter ceci :

1. Ouvrez une session à l'ASA primaire par l'intermédiaire de l'ASDM et choisissez les **outils--> configuration de sauvegarde**.
2. Vous pouvez sauvegarde tout ou juste les Certificats.
3. En état d'alerte, l'ASDM ouvert et choisissent des **outils --> a restauré la configuration**.

Informations connexes

- Page de support de l'appliance de sécurité adaptable Cisco (ASA)
- Exemple de configuration de l'installation manuelle de certificats de fournisseurs tiers dans ASA 8.x pour une utilisation avec WebVPN
- Support et documentation techniques - Cisco Systems