Renouvelez un certificat sur une appliance de sécurité du courrier électronique

Contenu

Introduction

Ce document décrit comment renouveler un certificat expiré sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Renouvelez un certificat sur l'ESA

Si vous avez un certificat expiré sur votre ESA (ou un qui expirera bientôt), vous pouvez simplement mettre à jour le certificat valable :

1. Téléchargez le fichier de la demande de signature de certificat (CSR).

2. Fournissez le fichier CSR à votre Autorité de certification (CA) et demandez un Privacy Enhanced Mail (PEM) (X.509) certificat signé.

3. Mettez à jour votre certificat valable par l'intermédiaire d'une des méthodes qui sont décrites dans les sections qui suivent.

Mettez à jour le certificat par l'intermédiaire du GUI

Afin de commencer, naviguez vers le **réseau > les Certificats du** GUI d'appareils. Ouvrez votre certificat et téléchargez le fichier CSR par l'intermédiaire du lien qui est affiché dans la prochaine image. Si l'ESA est un membre d'une batterie, vous devez vérifier les autres Certificats de cluster member et utiliser la même méthode pour chaque ordinateur. Avec cette méthode, la clé privée demeure sur l'ESA. La dernière étape est de faire signer le certificat par votre CA.

Voici un exemple :

1. Fichier CSR de téléchargement à votre ordinateur local, suivant les indications de l'image précédente.

2. Fournissez le fichier CSR à votre CA et demandez un certificat formaté par **X.509**.

3. Une fois que vous recevez le fichier PEM, importez le certificat par l'intermédiaire de la section de *certificat signé de téléchargement*. En outre, téléchargez le certificat intermédiaire (si disponible) dans la section *facultative*.

4. Soumettez et commettez les modifications.

5. Revenez à la page principale de Certificats (**réseau > Certificats du** GUI).

6. Vérifiez que la nouvelle date d'expiration apparaît et que le certificat affiche comme **VALID/ACTIVE**.

7. Soumettez et commettez les modifications.

Mettez à jour le certificat par l'intermédiaire du CLI

Vous pouvez également mettre à jour le certificat par l'intermédiaire du CLI. Cette méthode pourrait sembler plus intuitive, comme les demandes sont dans le format de question/réponse.

Voici un exemple :

```
myexample.com> certconfig


Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate

List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
tarheel.r  myexample.com         myexample.com         Active          327 days
test       test                  test                  Valid          3248 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         1570 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]> edit

1. [myexample.com] C=US,CN=myexample.com,L=RTP,O=Cisco Inc.,ST=NC,OU=TAC
2. [test] C=US,CN=test,L=yanceyville,O=test,ST=NC,OU=another test

Select the certificate profile you wish to edit:
[]> 1

Would you like to update the existing public certificate? [N]> y
```

```
Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
FR3XlVd6h3cMPWNgHAeWGYlcMKMr5n2M3L9
DdeLZOOD0ekCqTxG7OD8tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+f
ajNHbf9lKRUFy9AHyMRsa+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V66
8caFN0A7tDyUt/6YCW1KFeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds
3ZDvi/oJBn5nCR8HuvkDVNO6z9NVIE06gP564n6RAgMBAAEwDQYJKoZIhvcNAQEF
BQADggEBAA/BTYiw+0wAh1q3z1yfW6oVyx03/bGEdeT0TE8U3naBBKM/Niu8zAwK
7yS4tkWK3b96HK98IKWuxOVSY0EivW8EUWSalK/2zsLEp5/iuZ/eAfdsHrJdQKn3
H541MuowGaQc6NGtLjIfFet5pQ7w7R44z+4oSWXYsT9FLH78/w5DdLf6Rk696c1p
hb9U9lg7SnKvDrwLZ6i4Sn0TA6bl/z0p9DuvVSwWTNEHcn3kCbmbFpsD2Hd6EWKD
70zXapUp6/xG79pc2gFXHfg0RcmsozcmHPCjXjnL4OjpUExonSjffB3HhSKDqjhf
A0uN6Psgar9yz8M/B3ego34Nq3a1/F4=
-----END CERTIFICATE-----
.
C=US,CN=myexample.com,L=RTP,O=Cisco Inc.,ST=NC,OU=TAC

Do you want to add an intermediate certificate? [N]> Y

Paste intermediate certificate in PEM format (end with '.'):
[Removed for simplicity]

Do you want to add another intermediate certificate? [N]>

Would you like to remove an intermediate certificate? [N]>

Do you want to view the CSR? [Y]>

-----BEGIN CERTIFICATE REQUEST-----
MIICpjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxFDASBgNVBAMTC3RhcmhlZWwucnRw
MQwwCgYDVQQHEwNSVFAxEzARBgNVBAoTCkNpc2NvIEluYy4xCzAJBgNVBAgTAk5D
MQwwCgYDVQQLEwNUQUMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
gnqxG/GgDsxfOB7iWpNkCZpedKC5Qj5UpOEuMMx/OsAUXUNblJNktGMmW7dq6p9Z
4zAofRMgQFR3XlVd6h3cMPWNgHAeWGYlcMKMr5n2M3L9DdeLZOOD0ekCqTxG7OD8
tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+fajNHbf9lKRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFN0A7tDyUt/6YCW1K
FeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VNO6z9NVIE06gP564n6RAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAOpN8fD+H
Wa7n+XTwAb1jyC7yrjp9Llo8bc6Viy4bolrS15DxqAkvTCqssK+xhAScX2j9hxq2
pHBp8D5wMEmSUR39Jw77HRWNKHltUauIJUc3wEOeZ3b6pOUJAlNQenMBZJby7Hgw
0wV9X42JmDfwNBpWUW+rEyZHm0N9AATdgxmpFGvKIeiOM+fA0BKNxc7p0MMdcaBw
cQr/+bSfF3dwR8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvjky1sYcn2USqupFn
WbhzArh0AQiSxolI+B6pgk/GE+50fNABOlIVqAYzzG41V76p17soBp6mXr7dxOGL
YM2lmN12Rq3BkQ==
-----END CERTIFICATE REQUEST-----
List of Certificates
Name       Common Name           Issued By             Status         Remaining
---------  --------------------  --------------------  -------------  ---------
tarheel.r  myexample.com           myexample.com           Active          327 days
test       test                  test                  Valid          3248 days
Demo       Cisco Appliance Demo  Cisco Appliance Demo  Active         1570 days

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>
```

```
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]>

>commit
```

Informations connexes

- Conditions requises pour l'installation de certificat ESA
- Installez un certificat ssl par l'intermédiaire du CLI sur un ESA
- Assurez-vous que votre certificat ESA peut être vérifié
- Ajoutez/certificat PKCS#12 d'importation nouveau sur le GUI de Cisco ESA
- Support et documentation techniques - Cisco Systems