Comment générer et installer un certificat sur un SMA

Contenu

Introduction

Ce document décrit comment générer et installer un certificat pour la configuration et l'usage sur une appliance de Gestion de sécurité Cisco (SMA).

Conditions préalables

Vous devrez avoir accès pour exécuter l'**openssl de** commande localement.

Vous aurez besoin de l'accès de compte d'admin à votre appliance de sécurité du courrier électronique (ESA), et de l'accès d'admin au CLI de votre SMA.

Vous devez avoir ces éléments disponibles dans le format .pem :

- Certificat X.509
- Clé privée qui apparie votre certificat
- Tous Certificats intermédiaires fournis par votre Autorité de certification (CA)

Comment générer et installer un certificat sur un SMA

> **Conseil** : Il est recommandé pour faire signer un certificat par un CA de confiance Cisco ne recommande pas une particularité CA selon le CA que vous choisissez de travailler avec, vous peut recevoir de retour le certificat signé, la clé privée, et le certificat intermédiaire (le cas échéant) dans divers formats. Recherchez ou veuillez discutez directement avec le CA le format du fichier qu'ils te fournissent avant d'installer le certificat.

Actuellement, le SMA ne prend en charge pas générer un certificat localement. Au lieu de cela, il

est possible de générer un certificat auto-signé sur l'ESA. Ceci peut être utilisé comme contournement pour créer un certificat pour le SMA afin de pour être importé et configuré.

Créez et certificat d'exportation d'un ESA

1. Du GUI ESA, créez un certificat auto-signé de **réseau > de Certificats > ajoutent le certificat**. En créant le certificat auto-signé, il est important que « le nom commun (NC) » utilise l'adresse Internet du SMA et pas de l'ESA, de sorte que le certificat puisse être correctement utilisé.
2. Soumettez et commettez les modifications.
3. Exportez le certificat créé du **réseau > des Certificats > des Certificats d'exportation**. Vous avez deux options, (1) exportation et sauvegarde/utilisation comme certificat auto-signé, ou (2) demande de signature de certificat de téléchargement (si vous devez faire signer le certificat extérieurement) : Sauvegardez/utilisation comme un certificat Auto-signé : Choisissez les **Certificats d'exportation**Donnez-lui un nom du fichier (par exemple mycert.pfx) et le mot de passe qui seront utilisés quand convertissant le certificat.Ceci vous incitera automatiquement à sauvegarder le fichier localement.Poursuivez « pour convertir le certificat exporté ».Demande de signature de certificat de téléchargement **Réseau > Certificats**Cliquez sur en fonction le nom de certificat que vous avez créé.Dans la « signature émise par » la section, cliquez sur Download la **demande de signature de certificat…**Sauvegardez le fichier .pem localement et soumettez au CA.

Convertissez le certificat exporté

Le certificat créé et exporté de l'ESA sera dans le format .pfx. Le SMA prend en charge seulement le format .pem pour importer, ainsi ce certificat devra être converti. Afin de convertir un certificat de format .pfx en format .pem, utilisez s'il vous plaît l'exemple suivant de commande d'**openssl** :

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

Vous serez incité pour le mot de passe utilisé tout en créant le certificat de l'ESA. Le fichier créé .pem dans la commande d'OpenSSL contiendra le certificat et la clé dans le format .pem. Le certificat est maintenant prêt à être configuré sur le SMA. Veuillez poursuivre la section « installent certificat » de cet article.

Créez le certificat avec OpenSSL

Alternativement, si vous avez l'accès local pour exécuter l'**openssl de** votre PC/workstation, vous pouvez émettre la commande suivante de générer le certificat et de sauvegarder le fichier nécessaire .pem et la clé privée dans deux fichiers séparés :

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout sma_key.pem -out sma_cert.pem
```

Le certificat est maintenant prêt à être configuré sur le SMA. Veuillez poursuivre la section « installent certificat » de cet article.

Option supplémentaire, exportant un certificat d'un ESA

Au lieu de convertir le certificat de .pfx en .pem, comme mentionné ci-dessus, vous pouvez

sauvegarder un fichier de configuration sans masquer les mots de passe sur l'ESA. Ouvrez le fichier de configuration enregistré ESA .xml et recherchez la balise de <certificate>. Le certificat et la clé privée seront déjà dans le format .pem. Copiez le certificat et la clé privée pour importer la même chose dans le SMA comme a décrit section « installent certificat » ci-dessous.

> Remarque: Cette option est seulement valide pour des appliances exécutant AsyncOS 11.1 et plus vieux, où le fichier de configuration peut être enregistré utilisant l'option « de mot de passe ordinaire ». De plus nouvelles versions d'AsyncOS fournissent seulement l'option de masquer le mot de passe ou de chiffrer le mot de passe. Les deux options chiffrent la clé privée, qui est nécessaire pour l'importation de certificat ou l'option de regroupement.

> Remarque: Si vous optiez pour #2 ci-dessus, « téléchargez la demande de signature de certificat », et faites signer le certificat par un CA, vous devrez importer le certificat signé de nouveau à l'ESA que le certificat a été créé de avant d'enregistrer le fichier de configuration pour tirer une copie du certificat et de la clé privée. L'importation peut être faite en cliquant sur sur le nom de certificat sur le GUI ESA et utiliser l'option « certificat signé de téléchargement ».

Installez le certificat sur le SMA

Un certificat simple peut être utilisé pour tous les services, ou un certificat individuel peut être utilisé pour chacun des quatre services :

- TLS d'arrivée
- TLS sortant
- HTTPS
- LDAP

Sur le SMA, connectez-vous dans par l'intermédiaire du CLI et terminez-vous les étapes suivantes :

1. Exécutez le **certconfig**.
2. Choisissez l'**option de configuration**.
3. Vous devrez choisir si utiliser le même certificat pour tous les services ou utiliser les Certificats distincts pour chaque service individuel : Une fois présenté « faites vous veulent-ils utiliser une certificat/clé l'accès pour la réception, la livraison, HTTPS Gestion, et les LDAP ? », « Y de réponse » exigera seulement de vous d'entrer dans le certificat et de l'introduire une fois, et assignera alors ce certificat à tous les services.Si vous choisissez d'écrire « N », vous devrez entrer dans le certificat, la clé, et le certificat intermédiaire (le cas échéant) pour chaque service une fois incité : D'arrivée, sortant, HTTPS, et Gestion
4. Une fois incité, collez le certificat ou l'introduisez.
5. Extrémité avec « . » sur sa propre ligne pour chaque entrée afin d'indiquer que vous êtes fait collant l'élément actuel. (Voyez la section de « exemple ».)
6. Si vous avez un certificat intermédiaire, soyez sûr de l'entrer dans une fois incité à faire ainsi.
7. Une fois que terminé, appuyez sur **entrent** pour retourner à la demande principale CLI du

SMA.

8. Exécutez la validation à enregistrer la configuration.

   Remarque: Ne quittez pas la commande de certconfig avec Ctrl+C puisque ceci annule immédiatement vos modifications.

Exemple

```
mysma.local> certconfig

Currently using the demo certificate/key for receiving, delivery, HTTPS management access, and
LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
[]> setup

Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and
LDAPS? [Y]> y

paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAwIJAIXvIlkArow9MA0GCSqGSIb3DQEBBQUAMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzAeFw0xNzExMTAxNjA3MTRaFw0yNzExMDgxNjA3MTRaMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPz0perw3QA
ZH8xctOrvvjsnOPkItmSc+DUqtVKM6OOOkNHA2WY9XJ3+vESwkIdwexibj6VUQ85
K7NE6zOgRfpYdQsxmpIWhzYf9qCBOXuKsRw/9jonKk98DfHFM02J3BSmmgZ0MPp7
6EwA/sZAN+aqYB7IE1fgnqpEXek8xF1fcVnS2YTc7NXz781NK0jvXOtCVBrWFu0z
lEmZVpAj0AKkz1nujvzfOqEzed+tjauZr7nDIaiTrzhLKte4pJUm3T61q/PhegvN
Iy/WHN1xojP+FzjRAUlmtmjMzHyM2///dmq8JivUlaLXX9vUfdK3VViIOIz4zngG
Rz85QXO7ivcCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAM10zCcOOtqV1LDBmoDqd
4G2IhVbBESsbvZ/QmB6kpikT4pe5clQucskHq4D/xg1EZyfuXu+4auMie4B9Dym8
8pjbMDDi9hJPZ7j85nWMd6SfWhQUOPankdazpCycN6gNVzRBgPdR8tLOvt90vtV4
KCPmDYbwi6kfOl8tvjWHMh/wYicfvFRy0vPMpemtbCVGyC3cpquv8nFDutB6exym
skotn5wixCqErKlnHdUa3Z+zhutIAm/Q0sVWQQlbZZ+MIxBegyJ0ucTmBqqQHhhJ
pSO7PbevxwanYVXvNR8o2feAWs5LYkrwqdGRxLJmHjFnMV3PbkwRPgFWQ6AD1g12
34==
-----END CERTIFICATE-----
.
paste key in PEM format (end with '.'):
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCj89KXq8N0AGR/
MXLTq7747Jzj5CLZknPg1KrVSjOjjjpDRwNlmPVyd/rxEsJCHcHsYm4+lVEPOSuz
ROszoEX6WHULMZqSFoc2H/aggTl7irEcP/Y6JypPfA3xxTNNidwUppoGdDD6e+hM
AP7GQDfmqmAeyBNX4J6qRF3pPMRZX3FZ0tmE3OzV8+/JTStI71zrQlQa1hbtM5RJ
mVaQI9ACpM9Z7o783zqhM3nfrY2rma+5wyGok684SyrXuKSVJt0+tavz4XoLzSMv
1hzdcaIz/hc40QFJZrZozMx8jNv//3ZqvCYr1JWi11/b1H3St1VYiDiM+M54Bkc/
OUFzu4r3AgMBAAECggEAB9EFjsaZHGwyXmAIpe/PvIVnW3QSd0YEsUjiViXh/V+4
BmIZ1tuqhAkVVS38RfOuPatZrzEmOrASlcro3b6751oVRnHYeTOKwblXZEKU739m
vz6Lai1Y1o5HCepJbl5uuCtTN5CNjzueERWRD/ma0Kv5xi3qwitK1TpKMeb8Q3h2
YABmpk0TyJQ5ixLw3ch9ru1nqiO5zQ91GvIuDckudUu/bBnao+jV7D362lIPyLG8
03GqNviNZ6c3wjD0yQWg619g+ZmjM8DTtDR16zmzBvQ4TgZi22sUWrSSILRa69jW
q8XszQVRydl+gt666iUeN/ozmEMt5J8pu3i9vf3G2QKBgQDHyfv55rjZbWyf0eAT
Ch5T1YsjjMgMOtC9ivi5mMQCunWyRiyZ6qqSBME9Tper/YdAA07PoNtTpVPYyuVX
```

```
DDmyuWGHE04baf5QEmSgvQjXOSUPN5TI9hc5/mtvD8QjDO6rebUWxV3NJoR7YNrz
OmfARMXxaF+/mEj+6blSjZuGaQKBgQDSFKvYownPL6qTFhIH7B3kOLwZHk6cJUau
Zoaj7vTw7LrVJv1B0iLPmttEXeJgxzlFYR8tzfn0kTxGQlnhQxXkQ1kdDeqaiLvm
0TtmHMDupjDNKCNH8yBPqB+BIA4cB+/vo23W1HMHpGgqYWRRX/qremL72XFZSRnM
B8nRwK4aXwKBgB+hkwtVxB5ofLIxAFEDYRnUzVqrh2CoTzQzNH3t+dqUut2mzpjv
1mGX7yBNuSW51hgEbg3hYdg0bLn+JaFKhjgNsas5Gzyr41+6CcSJKUUp/vwRyLSo
gbTk2w2SaXNDMOZlNo6MYPWCC6edBg1MSfDe8pft9nrXGXeCeZzgXqdBAoGAQ6Iq
DQ24O76h0Ma7OVe36+CkFgYe0sBheAZD9IUa0HG2WKc7w7QORv4Y93KuTe/1rTNu
YUW94hHb8Natrwr1Ak74YpU3YVcB/3Z/BAnfxzUz4ui4KxLH5T1AH0cdo8KeaW0Z
EJ/HBL/WVUaTkGsw/YHiWiiQCGmzZ29edyvsIUsCgYEAvJtx0ZBAJ443WeHajZWm
J2SLKy0KHeDxZOZ4CwF5sRGsmMofILbK0OuHjMirQ5U9HFLpcINt11VWwhOiZZ51
k6o79mYhfrTMa4LlHOTyScvuxELqow82vdj6gqX0HVj4fUyrrZ28MiYOMcPw6Y12
34VjKaAsxgZIgN3LvoP7aXo=
-----END PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n

Currently using one certificate/key for receiving, delivery, HTTPS management access, and LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
- PRINT - Display configured certificates/keys.
- CLEAR - Clear configured certificates/keys.
[]>

mysma.local> commit

Please enter some comments describing your changes:
[]> Certificate installation

Changes committed: Fri Nov 10 11:46:07 2017 EST
```

Vérifiez le certificat importé et configuré sur le SMA

1. Connectez au SMA par l'intermédiaire du GUI utilisant HTTPS (IP de https:// <SMA ou hostname>) et entrez dans vos qualifications de procédure de connexion.
2. Àcôté de l'URL dans la barre d'adresses sur votre navigateur, cliquez sur l'icône de verrouillage ou l'icône de l'information pour vérifier la validité du certificat, de l'échéance, etc. Selon quel navigateur vous utilisez, vos actions et résultats peuvent varier.
3. Cliquez sur en fonction le chemin de certification pour vérifier la chaîne des Certificats.

Informations connexes

- Support et documentation techniques - Cisco Systems