Installer un certificat sécurisé pour le Gestionnaire de châssis FXOS

Table des matières

Introduction

Ce document décrit comment générer un CSR et installer le certificat d'identité à utiliser avec le Gestionnaire de châssis pour FXOS sur les périphériques FP 4100/9300.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configurer le système d'exploitation extensible Firepower (FXOS) à partir de la ligne de commande
- Utiliser la demande de signature de certificat (CSR)
- Concepts d'infrastructure à clé privée (PKI)

Composants utilisés

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

- Matériel des gammes Firepower (FP) 4100 et 9300
- FXOS Versions 2.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Après la configuration initiale, un certificat SSL auto-signé est généré pour être utilisé avec l'application Web Gestionnaire de châssis. Comme ce certificat est auto-signé, il n'est pas automatiquement approuvé par les navigateurs clients. La première fois qu'un nouveau navigateur client accède à l'interface Web du Gestionnaire de châssis, le navigateur émet un avertissement SSL semblable à votre connexion, indiquant qu'il n'est pas privé et demandant à l'utilisateur d'accepter le certificat avant d'accéder au Gestionnaire de châssis. Ce processus permet l'installation d'un certificat signé par une autorité de certification approuvée, ce qui permet à un navigateur client d'approuver la connexion et d'afficher l'interface Web sans avertissement.

Configurer

Générer une requête de signature de certificat (CSR)

Procédez comme suit afin d'obtenir un certificat qui contient l'adresse IP ou le nom de domaine complet (FQDN) du périphérique (qui permet à un navigateur client d'identifier correctement le serveur) :

- Créez un porte-clés et sélectionnez la taille de module de la clé privée.

Remarque : le nom du trousseau peut être n'importe quelle entrée. Dans ces exemples, firepower_cert est utilisé.

Cet exemple crée un porte-clés avec une taille de clé de 1024 bits :

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
```

- Configurez les champs CSR. La CSR peut être générée avec des options de base comme un nom de sujet. Vous êtes également invité à saisir un mot de passe de demande de certificat.

Cet exemple crée et affiche une demande de certificat avec une adresse IPv4 pour un porte-clés, avec des options de base :

```
Firepower-chassis# scope security
```

```
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
```

- Le CSR peut également être généré avec des options plus avancées qui permettent d'intégrer des informations telles que les paramètres régionaux et l'organisation dans le certificat.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* #  set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
```

- Exportez le CSR à fournir à votre autorité de certification. Copiez le résultat qui commence par (et inclut) -----BEGIN CERTIFICATE REQUEST----- se termine par (et inclut) -----END CERTIFICATE REQUEST-----.

```
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/OOKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```

Importer la chaîne de certificats de l'autorité de certification

Remarque : tous les certificats doivent être au format Base64 pour être importés dans FXOS. Si le certificat ou la chaîne reçu de l'autorité de certification est dans un format différent, vous devez d'abord le convertir avec un outil SSL tel qu'OpenSSL.

- Créez un nouveau point de confiance pour contenir la chaîne de certificats.

Remarque : le nom du point de confiance peut être n'importe quelle entrée. Dans les exemples, firepower_chain est utilisé.

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl9O3O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

Remarque : pour une autorité de certification qui utilise des certificats intermédiaires, les certificats racine et intermédiaires doivent être combinés. Dans le fichier texte, collez le certificat racine en haut, suivi de chaque certificat intermédiaire de la chaîne (qui inclut tous les indicateurs BEGIN CERTIFICATE et END CERTIFICATE). Collez ensuite l'intégralité du fichier avant la délimitation ENDOFBUF.

Importer le certificat d'identité signé pour le serveur

- Associez le point de confiance créé à l'étape précédente au porte-clés créé pour le CSR.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
```

- Collez le contenu du certificat d'identité fourni par l'autorité de certification.

```
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
```

Configurer le gestionnaire de châssis pour utiliser le nouveau certificat

Le certificat a été installé, mais le service Web n'est pas encore configuré pour l'utiliser.

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
```

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- show https - Output affiche le trousseau de clés associé au serveur HTTPS. Il peut refléter le nom créé dans les étapes mentionnées précédemment. S'il affiche toujours la valeur par défaut, il n'a pas été mis à jour pour utiliser le nouveau certificat.

<#root>

```
Firepower-chassis /system/services #
show https
 Name: https Admin State: Enabled Port: 443 Operational port: 443 Key Ring: kring7984
 Cipher suite mode: Medium Strength Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HI
```

- show keyring <keyring_name> detail - Le résultat affiche le contenu du certificat importé et indique s'il est valide ou non.

<#root>

```
fp4120 /security #
scope security
fp4120 /security #
show keyring kring7984
 detail
 Keyring
kring7984
: RSA key modulus: Mod2048 Trustpoint CA: tPoint10

 Certificate status: Valid
 Certificate: Data: Version: 3 (0x2) Serial Number: 45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBg
-----END CERTIFICATE-----
 Zeroized: No
```

- Entrez https://<FQDN_or_IP>/ dans la barre d'adresse d'un navigateur Web, accédez au Gestionnaire de châssis Firepower et vérifiez que le nouveau certificat approuvé est présenté.

⚠ Avertissement : les navigateurs vérifient également le nom du sujet d'un certificat par rapport

---

à l'entrée dans la barre d'adresse. Par conséquent, si le certificat est délivré au nom de domaine complet, il doit être accessible de cette manière dans le navigateur. Si l'accès s'effectue via une adresse IP, une erreur SSL différente est générée (Nom commun non valide) même si le certificat approuvé est utilisé.

Dépannage

Il n’y a actuellement aucune information spécifique disponible pour dépanner cette configuration.

Informations connexes

- Accès à la CLI FXOS
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.