Erstellen und Installieren eines Zertifikats auf einer SMA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein Zertifikat für die Konfiguration und Verwendung auf einer Cisco Security Management Appliance (SMA) generieren und installieren.

Voraussetzungen

Sie benötigen Zugriff, um den Befehl **openssl** lokal auszuführen.

Sie benötigen Administratorkontozugriff auf Ihre E-Mail Security Appliance (ESA) und Administratorzugriff auf die CLI Ihrer SMA.

Folgende Elemente müssen im .pem-Format verfügbar sein:

- X.509-Zertifikat
- Privater Schlüssel, der mit Ihrem Zertifikat übereinstimmt
- Alle Zwischenzertifikate Ihrer Zertifizierungsstelle (Certificate Authority, CA)

Erstellen und Installieren eines Zertifikats auf einer SMA

> **Tipp**: Es wird empfohlen, ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu signieren. Cisco empfiehlt keine spezifische Zertifizierungsstelle. Abhängig von der CA, mit der Sie arbeiten möchten, können Sie das signierte Zertifikat, den privaten Schlüssel und das Zwischenzertifikat (falls zutreffend) in verschiedenen Formaten zurückerhalten. Recherchieren Sie direkt mit der Zertifizierungsstelle das Format der Datei, die Sie erhalten, bevor Sie das Zertifikat installieren.

Derzeit unterstützt SMA das lokale Generieren eines Zertifikats nicht. Stattdessen ist es möglich, ein selbstsigniertes Zertifikat auf der ESA zu generieren. Dies kann als Problemumgehung zum Erstellen eines Zertifikats für SMA verwendet werden, um importiert und konfiguriert zu werden.

Erstellen und Exportieren von Zertifikaten aus einer ESA

1. Erstellen Sie über die ESA-GUI ein selbstsigniertes Zertifikat von **Network > Certificates > Add Certificate**. Beim Erstellen des selbstsignierten Zertifikats ist es wichtig, dass "Common Name (CN)" den Hostnamen der SMA und nicht der ESA verwendet, damit das Zertifikat ordnungsgemäß verwendet werden kann.
2. Änderungen senden und bestätigen.
3. Exportieren Sie das Zertifikat, das über **Netzwerk > Zertifikate > Exportzertifikate** erstellt wurde. Sie haben zwei Optionen: (1) Exportieren und speichern/als selbstsigniertes Zertifikat verwenden oder (2) Anfordern zum Signieren von Zertifikaten herunterladen (falls Sie das Zertifikat extern signieren müssen): Speichern/Verwenden als selbst signiertes Zertifikat: **Exportzertifikate** auswählenGeben Sie ihm einen Dateinamen (z. B. mycert.pfx) und eine Passphrase, die bei der Umwandlung des Zertifikats verwendet werden.Dadurch werden Sie automatisch aufgefordert, die Datei lokal zu speichern.Fahren Sie mit "Konvertieren des exportierten Zertifikats" fort.Zertifikatssignaturanforderung herunterladen **Netzwerk > Zertifikate**Klicken Sie auf den von Ihnen erstellten Zertifikatsnamen.Klicken Sie im Abschnitt "Signatur ausgestellt von" auf **Zertifikatsanforderung herunterladen...**Speichern Sie die .pem-Datei lokal und senden Sie sie an die CA.

Konvertieren des exportierten Zertifikats

Das von der ESA erstellte und exportierte Zertifikat ist im PFX-Format. SMA unterstützt nur das .pem-Format für den Import, daher muss dieses Zertifikat konvertiert werden. Um ein Zertifikat aus dem PFX-Format in das .pem-Format zu konvertieren, verwenden Sie das folgende **openssl-**Befehlsbeispiel:

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

Sie werden aufgefordert, die Passphrase einzugeben, die beim Erstellen des Zertifikats von der ESA verwendet wird. Die im OpenSSL-Befehl erstellte .pem-Datei enthält sowohl das Zertifikat als auch den Schlüssel im .pem-Format. Das Zertifikat kann jetzt für SMA konfiguriert werden. Fahren Sie mit dem Abschnitt "Zertifikat installieren" in diesem Artikel fort.

Zertifikat mit OpenSSL erstellen

Wenn Sie über lokalen Zugriff verfügen, um **openssl** von Ihrem PC/Ihrer Workstation aus auszuführen, können Sie den folgenden Befehl ausgeben, um das Zertifikat zu generieren und die benötigte .pem-Datei und den privaten Schlüssel in zwei separate Dateien zu speichern:

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

Das Zertifikat kann jetzt für SMA konfiguriert werden. Fahren Sie mit dem Abschnitt "Zertifikat installieren" in diesem Artikel fort.

Zusätzliche Option zum Exportieren eines Zertifikats von einer ESA

Anstatt das Zertifikat wie oben erwähnt von .pfx in .pem zu konvertieren, können Sie eine Konfigurationsdatei speichern, ohne die Kennwörter auf der ESA zu maskieren. Öffnen Sie die gespeicherte ESA .xml-Konfigurationsdatei, und suchen Sie nach dem <certificate>-Tag. Das Zertifikat und der private Schlüssel sind bereits im .pem-Format. Kopieren Sie das Zertifikat und den privaten Schlüssel zum Importieren desselben in die SMA, wie im Abschnitt "Installation des Zertifikats" unten beschrieben.

Hinweis: Diese Option ist nur für Appliances gültig, auf denen AsyncOS 11.1 und älter ausgeführt wird, auf denen die Konfigurationsdatei mit der Option 'Nur Passphrase' gespeichert werden kann. Neuere Versionen von AsyncOS bieten nur die Möglichkeit, die Passphrase zu maskieren oder die Passphrase zu verschlüsseln. Beide Optionen verschlüsseln den privaten Schlüssel, der für den Zertifikatsimport oder die Einfügen-Option erforderlich ist.

Hinweis: Wenn Sie sich für die Nummer 2 oben, "Download Certificate Signing Request" (Zertifikatsanforderung herunterladen) entschieden haben und das Zertifikat von einer Zertifizierungsstelle signiert haben, müssen Sie das signierte Zertifikat zurück an die ESA importieren, aus der das Zertifikat vor dem Speichern der Konfigurationsdatei erstellt wurde, um eine Kopie des Zertifikats und des privaten Schlüssels zu erstellen. Der Import kann erfolgen, indem Sie auf den Zertifikatsnamen in der ESA-GUI klicken und die Option "Signiertes Zertifikat hochladen" verwenden.

Installieren des Zertifikats auf der SMA

Für alle Services kann ein einziges Zertifikat verwendet werden, oder es kann ein individuelles Zertifikat für jeden der vier Services verwendet werden:

- Eingehendes TLS
- Outbound-TLS
- HTTPS
- LDAPS

Melden Sie sich auf dem SMA über die CLI an, und führen Sie die folgenden Schritte aus:

1. Führen Sie **certconfig aus**.
2. Wählen Sie die **Setup-**Option aus.
3. Sie müssen festlegen, ob für alle Services dasselbe Zertifikat verwendet oder für jeden einzelnen Dienst separate Zertifikate verwendet werden sollen: Wenn "Möchten Sie ein Zertifikat/einen Schlüssel für Empfang, Zustellung, HTTPS-Management-Zugriff und LDAPS verwenden?" angezeigt wird, müssen Sie bei der Beantwortung von "Y" das Zertifikat und den Schlüssel nur einmal eingeben und dieses Zertifikat dann allen Services zuweisen.Wenn Sie "N" eingeben, müssen Sie ggf. das Zertifikat, den Schlüssel und das Zwischenzertifikat für jeden Dienst eingeben, wenn Sie dazu aufgefordert werden: Eingehend, Ausgehend, HTTPS und Verwaltung
4. Fügen Sie bei Aufforderung das Zertifikat oder den Schlüssel ein.

5. Beenden Sie mit ". in der eigenen Zeile für jeden Eintrag anzugeben, dass Sie mit dem Einfügen des aktuellen Elements fertig sind. (Siehe Abschnitt "Beispiel".)
6. Wenn Sie über ein Zwischenzertifikat verfügen, geben Sie es ein, wenn Sie dazu aufgefordert werden.
7. Drücken Sie nach Abschluss die **Eingabetaste**, um zur Haupt-CLI-Eingabeaufforderung des SMA zurückzukehren.
8. Führen Sie **Commit** aus, um die Konfiguration zu speichern.

Hinweis: Beenden Sie den Befehl **certconfig** nicht mit Strg+C, da Ihre Änderungen sofort abgebrochen werden.

Beispiel

```
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+aqYB7IE1fgnqpEXek8xFlfcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
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
J2SLKy0KHeDxZOZ4CwF5sRGsmMofILbK0OuHjMirQ5U9HFLpcINt11VWwhOiZZ5l
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
```

Überprüfen des importierten und konfigurierten Zertifikats für die SMA

1. Stellen Sie über die GUI eine Verbindung mit dem SMA her (https://<SMA IP or hostname>), und geben Sie Ihre Anmeldeinformationen ein.
2. Klicken Sie neben der URL in der Adressleiste Ihres Browsers auf das Sperrsymbol oder Informationssymbol, um die Gültigkeit des Zertifikats, das Ablaufdatum usw. zu überprüfen. Je nachdem, welchen Browser Sie verwenden, können Ihre Aktionen und Ergebnisse variieren.
3. Klicken Sie auf den Zertifizierungspfad, um die Zertifikatskette zu überprüfen.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems