Come generare e installare un certificato in un SMA

Sommario

Introduzione

In questo documento viene descritto come generare e installare un certificato per la configurazione e l'utilizzo in una appliance Cisco Security Management (SMA).

Prerequisiti

Per eseguire il comando **openssl** localmente, è necessario disporre dell'accesso.

Ènecessario disporre dell'accesso come account amministratore a Email Security Appliance (ESA) e dell'accesso come amministratore alla CLI dello SMA.

Ènecessario disporre dei seguenti elementi in formato .pem:

- certificato X.509
- Chiave privata corrispondente al certificato
- Tutti i certificati intermedi forniti dall'Autorità di certificazione (CA)

Come generare e installare un certificato in un SMA

> **Suggerimento**: È consigliabile che un certificato sia firmato da una CA attendibile. Cisco sconsiglia di utilizzare una CA specifica. A seconda della CA con cui si sceglie di lavorare, è possibile ricevere il certificato firmato, la chiave privata e il certificato intermedio (se applicabile) in vari formati. Ricercare o discutere direttamente con l'autorità di certificazione il formato del file fornito prima di installare il certificato.

Al momento, l'SMA non supporta la generazione di un certificato localmente. È invece possibile

generare un certificato autofirmato sull'ESA. È possibile utilizzare questa soluzione per creare un certificato per l'SMA da importare e configurare.

Creazione ed esportazione di certificati da un'ESA

1. Dalla GUI ESA, creare un certificato autofirmato da **Rete > Certificati > Aggiungi certificato**. Quando si crea il certificato autofirmato, è importante che "Nome comune (CN)" utilizzi il nome host dell'SMA e non dell'ESA, in modo che il certificato possa essere utilizzato correttamente.
2. Inviare e confermare le modifiche.
3. Esporta il certificato creato da **Rete > Certificati > Esporta certificati**. Sono disponibili due opzioni: (1) esportare e salvare/utilizzare come certificato autofirmato oppure (2) scaricare la richiesta di firma del certificato (se è necessario che il certificato sia firmato esternamente): Salva/Usa come certificato autofirmato: Scegli **certificati di esportazione**Assegnare al certificato un nome file (ad esempio mycert.pfx) e una passphrase da utilizzare per la conversione del certificato.Verrà richiesto automaticamente di salvare il file localmente.Procedere a "Converti il certificato esportato".Scarica richiesta di firma certificato **Rete > Certificati**Fare clic sul nome del certificato creato.Nella sezione "Firma rilasciata da" fare clic su **Scarica richiesta di firma certificato...**Salvare il file .pem localmente e inviarlo alla CA.

Converti il certificato esportato

Il certificato creato ed esportato dall'ESA sarà in formato .pfx. L'SMA supporta solo il formato .pem per l'importazione, pertanto sarà necessario convertire il certificato. Per convertire un certificato dal formato PFX al formato PEM, utilizzare il seguente esempio di comando **openssl**:

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

Verrà richiesta la passphrase utilizzata durante la creazione del certificato dall'ESA. Il file con estensione pem creato nel comando OpenSSL conterrà sia il certificato che la chiave in formato pem. Il certificato è pronto per essere configurato nell'SMA. Procedere alla sezione "Installazione del certificato" di questo articolo.

Crea certificato con OpenSSL

In alternativa, se si dispone dell'accesso locale per eseguire **openssl** dal PC/workstation, è possibile utilizzare il seguente comando per generare il certificato e salvare il file .pem e la chiave privata necessari in due file separati:

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

Il certificato è pronto per essere configurato nell'SMA. Procedere alla sezione "Installazione del certificato" di questo articolo.

Opzione aggiuntiva, Esportazione di un certificato da un'ESA

Anziché convertire il certificato da .pfx in .pem, come accennato in precedenza, è possibile salvare un file di configurazione senza nascondere le password sull'ESA. Aprire il file di configurazione

.xml ESA salvato e cercare il tag <certificate>. Il certificato e la chiave privata saranno già in formato .pem. Copiare il certificato e la chiave privata per importarli nello SMA come descritto nella sezione "Installare il certificato" riportata di seguito.

> **Nota:** Questa opzione è valida solo per gli accessori con AsyncOS versione 11.1 e precedenti, in cui il file di configurazione può essere salvato utilizzando l'opzione 'plain passphrase'. Nelle versioni più recenti di AsyncOS è disponibile solo l'opzione di mascherare la passphrase o crittografare la passphrase. Entrambe le opzioni crittografano la chiave privata necessaria per l'opzione di importazione o incolla del certificato.

> **Nota:** Se si è optato per il numero 2, "Scarica richiesta di firma del certificato", e il certificato è stato firmato da una CA, sarà necessario importare il certificato firmato nuovamente nell'ESA da cui è stato creato il certificato prima di salvare il file di configurazione per creare una copia del certificato e della chiave privata. È possibile eseguire l'importazione facendo clic sul nome del certificato sulla GUI ESA e utilizzando l'opzione " Upload Signed Certificate" (Carica certificato firmato).

Installare il certificato nell'SMA

Èpossibile utilizzare un singolo certificato per tutti i servizi oppure un singolo certificato per ognuno dei quattro servizi seguenti:

- TLS in ingresso
- TLS in uscita
- HTTPS
- LDAPS

SMA, accedere tramite la CLI e completare i seguenti passaggi:

1. Eseguire **certconfig**.
2. Scegliere l'opzione **setup**.
3. Sarà necessario scegliere se utilizzare lo stesso certificato per tutti i servizi o se utilizzare certificati distinti per ogni singolo servizio: Quando viene visualizzato il messaggio "Si desidera utilizzare un solo certificato/chiave per la ricezione, la consegna, l'accesso alla gestione HTTPS e LDAPS?", rispondendo "Y" si richiede di immettere il certificato e la chiave una sola volta, quindi si assegna il certificato a tutti i servizi.Se si sceglie di immettere "N", sarà necessario immettere il certificato, la chiave e il certificato intermedio (se applicabile) per ogni servizio quando richiesto: In entrata, In uscita, HTTPS e Gestione
4. Quando richiesto, incollare il certificato o la chiave.
5. Termina con '.' in una riga specifica per ogni voce per indicare che non è necessario incollare l'elemento corrente. Vedere la sezione "Esempio".
6. Se si dispone di un certificato intermedio, assicurarsi di immetterlo quando richiesto.
7. Una volta completato, premere **Invio** per tornare al prompt CLI principale dello SMA.
8. Eseguire il comando **commit** per salvare la configurazione.

Nota: non uscire dal comando certconfig con CTRL+C poiché le modifiche vengono annullate immediatamente.

Esempio

```
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
```

Verificare il certificato importato e configurato nell'SMA

1. Connettersi all'SMA tramite GUI utilizzando HTTPS (https://<SMA IP or hostname>) e immettere le credenziali di accesso.
2. Accanto all'URL nella barra degli indirizzi del browser, fare clic sull'icona a forma di lucchetto o sull'icona delle informazioni per verificare la validità del certificato, la scadenza, ecc. A seconda del browser utilizzato, le azioni e i risultati possono variare.
3. Fare clic sul Percorso certificazione per controllare la catena di certificati.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems