如何生成和安装在SMA的一证书

目录

简介

本文描述如何生成和安装一证书为配置和使用在Cisco安全管理设备(SMA)。

先决条件

您将需要访问运行的命令**openssl**本地。

您将需要对您的电子邮件安全工具(ESA)的管理帐户访问和对您的SMA CLI的admin访问。

您必须有这些项目可用在.pem格式：

- X.509 证书
- 匹配您的证书的专用密钥
- 您的Certificate Authority (CA)提供的任何半成品证书

如何生成和安装在SMA的证书

> **提示**：推荐安排证书签字由委托CA.思科不根据您选择工作与的CA推荐特定CA.，您可能接收上一步签名证书、专用密钥和中间证书(哪里可适用)以多种格式。 直接地与CA请研究或讨论他们提供给您在安装证书之前文件的格式。

目前， SMA不支持生成证书本地。 反而，生成在ESA的一自签名证书是可能的。这可以用于作为应急方案创建SMA的一证书为了导入和配置。

创建和从ESA的出口许可证

1. 从ESA GUI，请创建从**网络>证书>Add的**一自签证书**证书**。 当创建自签名证书时，使用

SMA的主机名和不ESA “共同名称(CN)”是重要的，因此可以正确使用证书。
2. 提交并且确认更改。
3. 导出从**网络>证书>出口许可证**创建的证书。 (如果需要安排证书签字外部)，您有两个选项，(1)出口和保存/使用作为自签名证书或者(2)下载证书签名请求： 保存/使用作为自签名证书：选择**出口许可证**给它将使用，当转换证书时的文件名(即mycert.pfx)和密码短语。这将自动地提示您保存文件本地。继续“转换导出的证书”。下载证书签名请求 **网络>证书**点击您创建的验证名称。在”部分发出的“签名，请点击**下载证书签名请求...**保存.pem文件本地并且提交对CA。

转换导出的证书

从ESA创建和导出的证书在.pfx格式。导入的仅SMA支持.pem格式，因此此证书将需要转换。 为了转换证书从.pfx格式到.pem格式，请使用以下**openssl** example命令：

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

将提示对于使用的密码短语，当创建从ESA时的证书。 在openssl命令创建的.pem文件将包含证书和密钥在.pem格式。 证书当前准备配置在SMA。 请继续“安装此条款的证书”部分。

创建与Openssl的证书

或者，如果访问本地访问运行**openssl**从您的PC/workstation，您能发出以下命令生成证书和保存需要的.pem文件和专用密钥到两分离文件：

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

证书当前准备配置在SMA。 请继续“安装此条款的证书”部分。

其它选项，导出从ESA的证书

而不是转换从.pfx的证书到.pem里，如上所述，您能保存配置文件，无需屏蔽在ESA的密码。打开已保存ESA .xml配置文件和搜索<certificate>标记的。证书和专用密钥已经在.pem格式。复制证书和专用密钥导入的同样到SMA象描述“安装下面证书”部分。

> **Note**:如果选择了以上的#2， “请下载证书签名请求”，并且安排证书签字由CA，您将需要导入签名证书回到证书从在保存配置文件之前创建为进行证书和专用密钥的复制的ESA。导入可以由单击完成在ESA GUI和使用选项“加载签名证书”的验证名称。

安装在SMA的证书

单个证书可以用于所有服务，或者一单个证书可以用于四服务中的每一：

- 入站TLS
- 出站TLS
- HTTPS
- LDAP

在SMA，请通过CLI登录并且完成以下步骤：

1. 运行**certconfig**。
2. 选择**设置**选项。
3. 您是否将需要选择使用同一证书所有服务，或者使用分开的证书每项独立服务： 提交“什么时候要使用一证书/密钥接收，交付、HTTPS管理访问和LDAP ？”，回答“Y”在证书只将要求您输入和一次锁上和然后分配该证书到所有服务。如果选择输入“N”，您在证书、密钥和中间证书将需要输入(哪里可适用)每服务的，当提示：入站，出站， HTTPS和管理
4. 当提示，请粘贴证书或锁上。
5. 结束与‘。‘独自地每个条目的线路为了表明执行粘贴当前项目的您。 (请参阅“示例”部分。)
6. 如果有一中间证书，请务必输入它，当提示如此执行。
7. 一旦完成，请按回车返回到SMA的主CLI提示符。
8. 运行**进行**保存配置。

Note: 因为这立即取消您的更改，请勿退出与Ctrl+C的**certconfig**命令。

示例

```
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+aqYB7IE1fgnqpEXek8xF1fcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
lEmZVpAj0AKkz1nujvzfOqEzed+tjauZr7nDIaiTrzhLKte4pJUm3T61q/PhegvN
Iy/WHN1xojP+FzjRAUlmtmjMzHyM2///dmq8JivUlaLXX9vUfdK3VViIOIz4zngG
Rz85QXO7ivcCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAM10zCcOOtqV1LDBmoDqd
4G2IhVbBESsbvZ/QmB6kpikT4pe5clQucskHq4D/xg1EZyfuXu+4auMie4B9Dym8
8pjbMDDi9hJPZ7j85nWMd6SfWhQUOPankdazpCycN6gNVzRBgPdR8tLOvt90vtV4
KCPmDYbwi6kfOl8tvjWHMh/wYicfvFRy0vPMpemtbCVGyC3cpquv8nFDutB6exym
skotn5wixCqErKlnHdUa3Z+zhutIAm/Q0sVWQQlbZZ+MIxBegyJ0ucTmBqgQHhhJ
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
g8XszQVRydl+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
```

验证在SMA的已导入和已配置的证书

1. 连接对SMA通过GUI使用HTTPS (https:// <SMA IP或hostname>)并且输入在您的登录凭证。
2. 在地址栏的URL旁边在您的浏览器，请点击锁图标或信息图标检查证书、终止等等的正确性。根据哪个浏览器您使用，您的操作和结果可能变化。
3. 点击证书路径检查证书一系列。

相关信息

- 技术支持和文档 - Cisco Systems