在CLI管理的ASA上安装和更新证书

目录

简介

本文档介绍如何在通过CLI管理的Cisco ASA软件上请求、安装、信任和续订特定类型的证书。

先决条件

要求

- 验证自适应安全设备(ASA)具有正确的时钟时间、日期和时区。对于证书身份验证，建议使用网络时间协议 (NTP) 服务器同步 ASA 上的时间。检查相关信息以供参考。
- 要请求使用证书签名请求(CSR)的证书，需要访问受信任的内部或第三方证书颁发机构(CA)。第三方CA供应商的示例包括（但不限于）Entrust、Geotrust、GoDaddy、Thawte和VeriSign。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASAv 9.18.1
- 创建PKCS12时，使用OpenSSL。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

此文档处理的证书类型为自签名证书、第三方证书颁发机构签名的证书或内部CA，位于通过命令行界面(CLI)管理的思科自适应安全设备软件上。

证书安装

自签名证书注册

1. （可选）创建具有特定密钥大小的命名密钥对。

> 注意：默认情况下，使用名称为Default-RSA-Key且大小为2048的RSA密钥；但是，建议为每个证书使用唯一的名称，以便它们不使用相同的专用/公共密钥对。

```
<#root>

ASAv(config)#

crypto key generate rsa label

 SELF-SIGNED-KEYPAIR

modulus

 2048
INFO: The name for the keys will be: SELF-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...
```

使用命令可查看生成的密钥对 **show crypto key mypubkey rsa**.

```
<#root>

ASAv#

show crypto key mypubkey rsa

(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022

Key name:

 SELF-SIGNED-KEYPAIR
Usage: General Purpose Key

Key Size

 (bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
```

```
af020301 0001
```

2. 创建具有特定名称的信任点。自行配置注册类型。
<#root>

```
ASAv(config)#
```

crypto ca trustpoint

```
 SELF-SIGNED
ASAv(config-ca-trustpoint)#
```

enrollment self

3. 配置完全限定域名(FQDN)和主题名称。

⚠ 注意：FQDN参数必须与证书使用的ASA接口的FQDN或IP地址匹配。此参数设置证书的主题备用名称(SAN)。

<#root>

```
ASAv(config-ca-trustpoint)#
```

fqdn

```
 asavpn.example.com
ASAv(config-ca-trustpoint)#
```

subject-name

CN=

```
asavpn.example.com,O=Example Inc,C=US,St=California,L=San Jose
```

4. （可选）配置步骤1中创建的密钥对名称。如果使用默认密钥对，则不需要此项。
<#root>

```
ASAv(config-ca-trustpoint)#
```

keypair

```
 SELF-SIGNED-KEYPAIR
ASAv(config-ca-trustpoint)# exit
```

5. 注册信任点并生成证书。
<#root>

```
ASAv(config)#
```

crypto ca enroll

```
 SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
```

```
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]:

yes

% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]:

no

Generate Self-Signed Certificate? [yes/no]:

yes

ASAv(config)#

exit
```

6. 完成后，可以使用命令查看新的自签名证书 **show crypto ca certificates**

.

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:
start date: 15:00:58 CEDT Jul 15 2022
end date: 15:00:58 CEDT Jul 12 2032
Storage: config
Associated Trustpoints: SELF-SIGNED
```

通过证书签名请求(CSR)进行注册

1. （可选）创建具有特定密钥大小的命名密钥对。

> 注意：默认情况下，使用名称为Default-RSA-Key且大小为2048的RSA密钥；但是，建议为每个证书使用唯一的名称，以便它们不使用相同的专用/公共密钥对。

<#root>

ASAv(config)#

crypto key generate rsa label

CA-SIGNED-KEYPAIR

modulus

2048
INFO: The name for the keys will be: CA-SIGNED-KEYPAIR
Keypair generation process begin. Please wait...

使用命令可查看生成的密钥对 **show crypto key mypubkey rsa**.

<#root>

ASAv#

show crypto key mypubkey rsa

(...)
Key pair was generated at: 14:52:49 CEDT Jul 15 2022

Key name:

CA-SIGNED-KEYPAIR
Usage: General Purpose Key

Key Size

(bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
...
59dcd7d7 c3ee77f5 bbd0988d 515e390e b8d95177 dfaf6b94 a9df474b 1ec3b4a4
af020301 0001

2. 创建具有特定名称的信任点。配置注册类型终端。

```
ASAv(config)# crypto ca trustpoint CA-SIGNED
ASAv(config-ca-trustpoint)# enrollment terminal
```

3. 配置完全限定域名和主题名称。FQDN和主题CN参数必须与使用证书的服务的FQDN或IP地址匹配。

```
ASAv(config-ca-trustpoint)# fqdn asavpn.example.com
ASAv(config-ca-trustpoint)# subject-name CN=asavpn.example.com,O=Example Inc,C=US,St=California,L=
```

4. （可选）配置步骤1中创建的密钥对名称。

```
ASAv(config-ca-trustpoint)# keypair CA-SIGNED-KEYPAIR
```

5. （可选）使用证书撤销列表(CRL)或在线证书状态协议(OCSP)配置证书撤销检查方法。默认情况下，证书撤销检查处于禁用状态。

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

6. （可选）对信任点进行身份验证，并安装将身份证书签名为受信任的CA证书。如果在此步骤中未安装CA证书，则可以稍后与身份证书一起安装。

```
ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

ASAv(config)# crypto ca authenticate CA-SIGNED
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0xNTAyMDYxNDEwMDBaFw0zMDAyMDYxNDEwMDBaMEUx
CzAJBgNVBAYTAlBMMQ8wDQYDVQQKEwZ3dy12cG4xDDAKBgNVBAsTA2xhYjEXMBUG
A1UEAxMOY2EuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDI6pth5KFFTB29LynOg9/CTiOGYa+WFTcZXSLHZA6WTUzLYM19IbSFHWa6
gTeBnHqToLRnQoB51QlxEA45ArL2G98aew8BMDO8GXkxWayforwLA3U9WZVTZsVN
4noWaXH1boGGD7+5vk0esJfL2B7pEhGodLh7Gki1T4KoqL/lDM9LqkzOctZkCT7f
SkXvFik1Z1cZEGn6b2umnIqaVZ81ewIuTHOX48ls3uxTPH8+B5QG0+d1waOsbCWk
oK5sEPpHZ3IQuVxGiirp/zmomzxl4G/tel6eyMOpjpnVtDYjQ9HNkQdQT5LKwRsX
Oj9xKnYCbPfg3p2FdH7wJh1lK3prAgMBAAGjUDBOMAwGA1UdEwQFMAMBAf8wHQYD
VR0OBBYEFE55kZsbra9b9tLFV52U47em9uXaMB8GA1UdIwQYMBaAFE55kZsbra9b
9tLFV52U47em9uXaMA0GCSqGSIb3DQEBCwUAA4IBAQArsXlFwK3jlNBwOsYh5mqT
cGqeyDMRhs3Rs/wD25M2wkAF4AYZHgN9gK9VCK+ModKMQZy4X/uhj65NDU7oFf6f
z9kqaRijsx153jV/YLk8E9oAIatnA/fQfX6V+h74yqucfF1js3d1FjyV14odRPwM
OjRyjalH56BFlackNc7KRddtVxYB9sfEbFhN8odlBvnUedxGAJFHqxEQKmBE+h4w
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----

quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

7. 注册证书并生成可复制并发送到CA进行签名的CSR。CSR包括信任点使用的密钥对中的公钥。签名证书只能由具有该密钥对的设备使用。

注意：签署CSR和创建签名身份证书时，CA可以更改信任点中定义的FQDN和主题名称参数。

```
ASAv(config)# crypto ca enroll CA-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor

% The fully-qualified domain name in the certificate will be: asavpn.example.com

% Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
OPFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2Bg0KOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmAOpDWL9z
Duu8BQnBGuNO8T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
lOApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

8. 导入身份证书。签署CSR后，提供身份证书。

```
ASAv(config)# crypto ca import CA-SIGNED certificate
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.




Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIIKbLY8Qt8N5gwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
kzAihRuFqmYYUeQP2Byp/S5fNqUcyZfAczIHt8BcPmVO9l6iSF/ULGlzXMSOUX6N
```

```
d/LHXwrcTpc1zU+7qx3TpVDZbJlwwF+BWTBlxgM0BosJx65u/n75KnbBhGUE75jV
HX2eRzuhnnSVExCoeyed7DLiezD8
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

9. 验证证书链。完成后，可以使用命令查看新的身份证书和CA证书 **show crypto ca certificates** .

```
ASAv# show crypto ca certificates CA-SIGNED
CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: CA-SIGNED

Certificate
Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

PKCS12注册

使用从您的CA接收的PKCS12文件，该文件包含密钥对、身份证书和（可选）CA证书链。

1. 创建具有特定名称的信任点。

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12
ASAv(config-ca-trustpoint)# exit
```

> 注意：导入的密钥对以信任点名称命名。

2. （可选）使用证书撤销列表(CRL)或在线证书状态协议(OCSP)配置证书撤销检查方法。默认情况下，证书撤销检查处于禁用状态。

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. 从PKCS12文件导入证书。

> 注意：PKCS12文件需要采用base64编码。如果在文本编辑器中打开文件时看到可打印字符，则该文件是base64编码的。若要将二进制文件转换为base64编码形式，可使用openssl。

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiKOc
wqE3Tm0CAggAgIIH0NjxmJBuoPRuYl1VxTiawHzsL8kIl03lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/hqoKcwECD05
dnxCNJx6
quit

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.
```

4. 验证安装的证书。

```
ASAv# show crypto ca certificates TP-PKCS12

Certificate
Status: Available
```

```
Certificate Serial Number: 2b368f75e1770fd0
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
CN=asavpnpkcs12chain.example.com
O=Example Inc
L=San Jose
ST=California
C=US
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023
Storage: config
Associated Trustpoints: TP-PKCS12

CA Certificate
Status: Available
Certificate Serial Number: 0ccfd063f876f7e9
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Validity Date:
start date: 15:10:00 CEST Feb 6 2015
end date: 15:10:00 CEST Feb 6 2030
Storage: config
Associated Trustpoints: TP-PKCS12
```

在上一个示例中，PKCS12包含身份和CA证书 — 两个条目 — 证书和CA证书。否则，仅存在证书。

5. （可选）验证信任点。

如果PKCS12不包含CA证书，并且CA证书是以PEM格式单独获得的，则可以手动安装。

```
ASAv(config)# crypto ca authenticate TP-PKCS12
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
```

```
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes

WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

证书续订

续订自签名证书

1. 检查当前证书到期日期。
   <#root>

```
# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16084
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:00:58 CEDT Jul 15 2022

end date: 15:00:58 CEDT Jul 12 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

2. 重新生成证书。

```
ASAv# conf t
ASAv(config)# crypto ca enroll SELF-SIGNED
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

WARNING: Trustpoint TP has already enrolled and has
a device cert issued to it.
If you successfully re-enroll this trustpoint,
the current certificate will be replaced.
Do you want to continue with re-enrollment? [yes/no]: yes
% The fully-qualified domain name in the certificate will be: asa.example.com
% Include the device serial number in the subject name? [yes/no]: no
Generate Self-Signed Certificate? [yes/no]: yes
ASAv(config)# exit
```

3. 验证新证书。

<#root>

```
ASAv# show crypto ca certificates SELF-SIGNED
Certificate
Status: Available
Certificate Serial Number: 62d16085
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Subject Name:
unstructuredName=asa.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asa.example.com
Validity Date:

start date: 15:09:09 CEDT Jul 20 2022

end date: 15:09:09 CEDT Jul 17 2032

Storage: config
Associated Trustpoints: SELF-SIGNED
```

使用证书签名请求(CSR)注册续订证书

注意：如果需要更改新证书的任何新证书元素（subject/fqdn、密钥对），则创建新证书。请参阅使用证书签名请求(CSR)注册部分。下一个过程只是刷新证书到期日期。

1. 检查当前证书到期日期。
<#root>

```
ASAv# show crypto ca certificates CA-SIGNED


Certificate

Status: Available
Certificate Serial Number: 29b2d8f10b7c3798
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 15:33:00 CEDT Jul 15 2022
end date: 15:33:00 CEDT Jul 15 2023

Storage: config
Associated Trustpoints: CA-SIGNED

Certificate
Subject Name:
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 790aa617 c30c6894 0bdc0327 0d60b032
Associated Trustpoint: CA-SIGNED
```

2. 注册证书。生成可复制的CSR并发送到CA进行签名。CSR包括信任点使用的密钥对中的公钥 — 签名的证书只能由具有该密钥对的设备使用。

> 注意：签署CSR和创建签名身份证书时，CA可以更改信任点中定义的FQDN和主题名称参数。

> 注意：对于同一信任点，在不更改主题/fqdn和密钥对配置的情况下，后续注册与初始注册提供相同的CSR。

```
ASAv# conf t
ASAv(config)# crypto ca enroll CA-SIGNED

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes
```

```
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=asavpn.example.com,O=Example Inc,C=US,St=Califor
% The fully-qualified domain name in the certificate will be: asavpn.example.com
% Include the device serial number in the subject name? [yes/no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDHzCCAgcCAQAwgYsxGzAZBgNVBAMMEmFzYXZwbi5leGFtcGxlLmNvbTEUMBIG
A1UECgwLRXhhbXBsZSBJbmMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9y
bmlhMREwDwYDVQQHDAhTYW4gSm9zZTEhMB8GCSqGSIb3DQEJAgwSYXNhdnBuLmV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5cvZVr1j
Me8Mz4T3vgT1Z8DAAR0avs/TBdYiqGdjyiV/3K92IIT/0r8cuAUe5rR4sjTvaXYC
SycSbwKc4kZbr3x120ss8Itd5g4kBdrUSCprl+VMiTphQgBTAqRPk0vFX4rC8k/T
0PFDE+2gjT1wMn9reb92jYrolGK4MWZdCzqowLPjEj5cCwu8Pv5h4hqTpudms+v4
g3R1OODmeyv4uEMYLS/noPxZXZ8YiQMiG2EP2Bg0KOT3FzxOmVuekonQtRhiZt+c
zyyfSRoqyBSakEZBwABod8q1Eg5J/pH13OJlitOUJEyIlFoVHqv3jL7zfA9ilInu
NaHkir062VQNXwIDAQABoE4wDwYJKoZIhvcNAQkHMQITADA7BgkqhkiG9w0BCQ4x
LjAsMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJhc2F2cG4uZXhhbXBsZS5jb20w
DQYJKoZIhvcNAQELBQADggEBAM3Q3zvp9G3MWP7R4wkpnBOH2CNUmPENIhHNjQjH
Yh08EOvWyoo9FaLfHKVDLvFXh0vn5osXBmPLuVps6Ta4sBRUNicRoAmmA0pDWL9z
Duu8BQnBGuNO8T/H3ydjaNoPJ/f6EZ8gXY29NXEKb/+A2Tt0VVUTsYreGS+84Gqo
ixFOtW8R50IXg+afAVOAh81xVUFOvuAi9DsiuvufMb4wdngQSOel/B9Zgp/BfGMl
l0ApgejACoJAGmyrn9Tj6Z/6/lbpKBKpf4VE5UXdj7WLAjw5JF/X2NrH3/cQsczi
G2Yg2dr3WpkTIY2W/kVohTiohVRkgXOMCecUaMlYxJyLTRQ=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

3. 导入身份证书。签署CSR后，提供身份证书。

```
ASAv(config)# crypto ca import CA-SIGNED certificate

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.
Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be: asavpn.example.com

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIMA+aIxCtNtMwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
YS5leGFtcGxlLmNvbTAeFw0yMjA3MjAxNDA5MDBaFw0yMzA3MjAxNDA5MDBaMIGL
MRswGQYDVQQDDBJhc2F2cG4uZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUg
SW5jMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTERMA8GA1UEBwwI
U2FuIEpvc2UxITAfBgkqhkiG9w0BCQIMEmFzYXZwbi5leGFtcGxlLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOXL2Va9YzHvDM+E974E9WfAwAEd
Gr7P0wXWIqhnY8olf9yvdiCE/9K/HLgFHua0eLI072l2AksnEm8CnOJGW698ddtL
LPCLXeYOJAXa1Egqa5flTIk6YUIAUwKkT5NLxV+KwvJP09DxQxPtoIO9cDJ/a3m/
do2K6JRiuDFmXQs6qMCz4xI+XAsLvD7+YeIak6bnZrPr+INOdTjg5nsr+LhDGC0v
56D8WV2fGIkDIhthD9gYNCjk9xc8dJlbnpKJOLUYYmbfnM8snOkaKsgUmpBGQcAA
aHfKtRIOSf6R9d9CZYrTlCRMiJRaFR6r94y+83wPYpSJ7jWh5Iq9OtlUDV8CAwEA
AaMuMCwwCwYDVR0PBAQDAgWgMB0GA1UdEQQWMBSCEmFzYXZwbi5leGFtcGxlLmNv
bTANBgkqhkiG9w0BAQsFAAOCAQEAfQUchY4UjhjkySMJAh7NT3TT5JJ4NzqW8qHa
wNq+YyHR+sQ6G3vn+6cYCU87tqWlY3fXC27TwweREwMbq8NsJrr8OhsChYby8kwE
LnTkrN7dJBl7u5OVQ3DRjfmFrJ9LEUaYZx1HYvcS1kAeEeVB4VJwVzeujWepcmEM
```

```
p7cB6veTcF9rulDVRImdOKYEOx+HYav2INT2udcOG1yDwml/mqdfO/ON2SpBBpnE
gtiKshtsST/NAw25WjkrDIfN8uR2z5xpzxnEDUBoHOipGlgb1I6G1ARXWO+LwfBl
n1QD5b/RdQOUbLCpfKNPdE/9wNnoXGDlJ7qfZxrO4T7ld2Idug==
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
```

4. 验证新证书到期日期。
   <#root>

```
ASAv# show crypto ca certificates CA-SIGNED
Certificate
Status: Available
Certificate Serial Number: 300f9a2310ad36d3
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: RSA-SHA256
Issuer Name:
CN=ca.example.com
OU=lab
O=ww-vpn
C=PL
Subject Name:
unstructuredName=asavpn.example.com
L=San Jose
ST=California
C=US
O=Example Inc
CN=asavpn.example.com
Validity Date:
start date: 16:09:00 CEDT Jul 20 2022
end date: 16:09:00 CEDT Jul 20 2023
Storage: config
Associated Trustpoints: CA-SIGNED
```

PKCS12续订

无法在使用PKCS12文件注册的信任点中续订证书。要安装新证书，需要创建新的信任点。

1. 创建具有特定名称的信任点。

```
ASAv(config)# crypto ca trustpoint Trustpoint-PKCS12-2022
ASAv(config-ca-trustpoint)# exit
```

2. （可选）使用证书撤销列表(CRL)或在线证书状态协议(OCSP)配置证书撤销检查方法。默认情况下，证书撤销检查处于禁用状态。

```
ASAv(config-ca-trustpoint)# revocation-check ocsp
```

3. 从PKCS12文件导入新证书。

注意：PKCS12文件需要采用base64编码。如果在文本编辑器中打开文件时看到可打印字符，则该文件是base64编码的。要将二进制文件转换为base64编码形式，可以使用openssl。

```
openssl enc -base64 -in asavpnpkcs12chain.example.com.pfx -out asavpnpkcs12chain.example.com.
```

```
ASAv(config)# crypto ca import TP-PKCS12-2022 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
BqCCCAgwgggEAgEAMIIH/QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIiKOc
wqE3Tm0CAggAgIIHONjxmJBuoPRuYl1VxTiawHzsL8kIlO3lOj7tcWmECBwzsKKq
(...)
PXowMwYJKoZIhvcNAQkUMSYeJABhAHMAYQB2AHAAbgAuAGUAeABhAG0AcABsAGUA
LgBjAG8AbTAtMCEwCQYFKw4DAhoFAAQUPXZZtBeqlh98wQljHW7J/hqoKcwECDO5
dnxCNJx6
quit

Trustpoint CA certificate accepted.
WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

INFO: Import PKCS12 operation completed successfully.
```

注意：如果新的PKCS12文件包含与旧证书使用的密钥对相同的身份证书，则新的信任点引用旧密钥对名称。
示例：

<#root>

```
ASAv(config)# crypto ca import
```

TP-PKCS12-2022

```
 pkcs12 cisco123

Enter the base 64 encoded pkcs12. End with the word "quit" on a line by itself:

MIIN4gIBAzCCDawGCSqGSIb3DQEHAaCCDZ0Egg2ZMIINlTCCCBcGCSqGSIb3DQEH
...
dnxCNJx6
quit
```

WARNING: Identical public key already exists as TP-PKCS12

```
ASAv(config)# show run crypto ca trustpoint

TP-PKCS12-2022

crypto ca trustpoint TP-PKCS12-2022


keypair TP-PKCS12

 no validation-usage crl configure
```

4. 验证安装的证书。
<#root>

```
ASAv# show crypto ca certificates TP-PKCS12-2022


Certificate

 Status: Available
 Certificate Serial Number: 2b368f75e1770fd0
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: RSA-SHA256
 Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Subject Name: unstructuredName=asavpn.example.com CN=asavpnpkcs12chain.example.com O=Example Inc
 Validity Date:
 start date: 15:33:00 CEDT Jul 15 2022
 end date: 15:33:00 CEDT Jul 15 2023
 Storage: config
 Associated Trustpoints: TP-PKCS12-2022


CA Certificate

 Status: Available
 Certificate Serial Number: 0ccfd063f876f7e9
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: RSA-SHA256
 Issuer Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Subject Name: CN=ca.example.com OU=lab O=ww-vpn C=PL
 Validity Date:
 start date: 15:10:00 CEST Feb 6 2015
 end date: 15:10:00 CEST Feb 6 2030
 Storage: config
 Associated Trustpoints: TP-PKCS12-2022
```

在上一个示例中，PKCS12包含身份证书和CA证书，因此，在导入后可以看到两个条目：证书和CA证书。否则，仅存在证书条目。

5. （可选）验证信任点。

如果PKCS12不包含CA证书，并且CA证书是以PEM格式单独获得的，则可以手动安装。

```
ASAv(config)# crypto ca authenticate TP-PKCS12-2022
Enter the base 64 encoded CA certificate.
```

```
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDXDCCAkSgAwIBAgIIDM/QY/h29+kwDQYJKoZIhvcNAQELBQAwRTELMAkGA1UE
BhMCUEwxDzANBgNVBAoTBnd3LXZwbjEMMAoGA1UECxMDbGFiMRcwFQYDVQQDEw5j
(...)
gW8YnHOvMO8svyTXSLlJfOUCdmAY+lGOgqhUlSlkFBtLRt6Z2uCotOONoMHIOhh5
dcVcovOi/PAxnrAlJ+Ng2jrWFN3MXWZO4S3CHYMGkWqHkaHChlqDOx9badgfsyzz
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: e9ad165c 2673424c 6e7e0c5f b30b4a02
Do you accept this certificate? [yes/no]: yes

WARNING: CA certificates can be used to validate VPN connections,
by default. Please adjust the validation-usage of this
trustpoint to limit the validation scope, if necessary.

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

6. 重新配置ASA以使用新信任点而不是旧信任点。

示例：

```
ASAv# show running-config ssl trust-point
ssl trust-point TP-PKCS12
ASAv# conf t
ASAv(config)#ssl trust-point TP-PKCS12-2022
ASAv(config)#exit
```

注意：信任点可用于不同的配置元素。检查使用旧信任点的配置。

相关信息

如何在ASA上配置时间设置。

有关在ASA上正确设置时间和日期所需的步骤，请参阅《思科ASA系列常规操作CLI配置指南9.18》。https://www.cisco.com/c/en/us/td/docs/security/asa/asa918/configuration/general/asa-918-general-config/basic-hostname-pw.html#ID-2130-000001bf

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。