

配置一个 Cisco IOS 路由器并将其注册到配置为 CA 服务器的另一个 Cisco IOS 路由器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[规则](#)

[为证书服务器生成并导出 RSA 密钥对](#)

[导出生成的密钥对](#)

[验证生成的密钥对](#)

[在路由器上启用 HTTP 服务器](#)

[在路由器上启用并配置 CA 服务器](#)

[配置第二个 IOS 路由器 \(R2\) 并向证书服务器进行注册](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍了如何配置 Cisco IOS® 路由器以用作证书颁发机构 (CA) 服务器。此外还阐述了如何注册另一个 Cisco IOS 路由器，以便从 CA 服务器上获取一个根和 ID 证书，以进行 IPsec 身份验证。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS 软件版本 12.3(4)T3 的两个 Cisco 2600 系列路由器。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[网络图](#)

本文档使用以下网络设置：

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[为证书服务器生成并导出 RSA 密钥对](#)

第一步是生成供 Cisco IOS CA 服务器使用的 RSA 密钥对。在路由器 (R1) 上，按照此输出所示生成 RSA 密钥：

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable The name for the keys
will be: cisco1 Choose the size of the key modulus in the range of 360 to 2048 for your General
Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in
the modulus [512]: % Generating 512 bit RSA keys ...[OK] R1(config)# *Jan 22 09:51:46.116: %SSH-
5-ENABLED: SSH 1.99 has been enabled
```

注意：对于计划为证书服务器使用的密钥对，您必须采用相同的名称 (*key-label*) (通过稍后介绍的 `crypto pki server cs-label` 命令)。

[导出生成的密钥对](#)

将密钥导出到非易失性 RAM (NVRAM) 或 TFTP 中 (根据您的配置而定)。在本示例中，使用 NVRAM。根据您的实施情况，为了存储证书信息，您可能希望使用单独的 TFTP 服务器。

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123 % Key name: cisco1 Usage:
General Purpose Key Exporting public key... Destination filename [cisco1.pub]? Writing file to
nvram:cisco1.pub Exporting private key... Destination filename [cisco1.prv]? Writing file to
nvram:cisco1.prv R1(config)#
```

如果使用 TFTP 服务器，您可以根据此命令所示重新导入生成的密钥对：

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

注意：如果不希望密钥可以从您的证书服务器上导出，您可以先将密钥导出为不可导出的密钥对，然后再将其重新导入到证书服务器上。这样，这些密钥就不可以再次导出了。

[验证生成的密钥对](#)

要验证生成的密钥对，请发出 `show crypto key mypubkey rsa` 命令。

[命令输出解释程序 \(仅限注册用户\)](#) (OIT) 支持某些 `show` 命令。使用 OIT 可查看对 `show` 命令输出的分析。

```
R1#show crypto key mypubkey rsa % Key pair was generated at: 09:51:45 UTC Jan 22 2004 Key name:
cisco1 Usage: General Purpose Key Key is exportable. Key Data: 305C300D 06092A86 4886F70D
01010105 00034B00 30480241 00CC2DC8 ED26163A B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83
F7B2BD56 126E0F11 50552843 7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001 %
Key pair was generated at: 09:51:54 UTC Jan 22 2004 Key name: cisco1.server Usage: Encryption
Key Key is exportable. Key Data: 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578
025D3066 72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698 EBD02905
FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1 C1607433 5C7BC549 D532D18C
```

[在路由器上启用 HTTP 服务器](#)

Cisco IOS CA 服务器仅支持通过简单证书注册协议 (SCEP) 进行的注册。因此，为了能够执行此操作，路由器必须运行内置的 Cisco IOS HTTP 服务器。要启用该服务器，请使用 `ip http server` 命令：

```
R1(config)#ip http server
```

[在路由器上启用并配置 CA 服务器](#)

完成这些步骤：

1. 证书服务器必须与您刚才手动生成的密钥对使用相同的名称，记住这一点非常重要。其标签与生成的密钥对标签相匹配：`R1(config)#crypto pki server cisco1` 启用证书服务器之后，您可以使用预配置的默认值或通过 CLI 指定其他值，以便证书服务器能够正常运行。
2. `database url` 命令可指定写出 CA 服务器的所有数据库条目时使用的位置。如果未指定此命令，所有数据库条目将写入闪存中。`R1(cs-server)#database url nvram` **注意**：如果使用 TFTP 服务器，则 URL 应为 `ftp://<ip_address>/directory`。
3. 配置数据库级别：`R1(cs-server)#database level minimum` 此命令控制证书注册数据库中存储的数据类型：**Minimum** - 存储足够的信息仅为在不发生冲突的情况下继续签发新证书。这是默认值。**Names** - 除了 minimal 级别中提供的信息外，还包括每个证书的序列号和主题名称。**Complete** - 除了 minimal 级别和 names 级别中提供的信息外，还将签发的每个证书写入数据库中。**注意**：**complete** 关键字会生成大量信息。如果使用此关键字，您还应通过 `database url` 命令指定在其中存储数据的外部 TFTP 服务器。
4. 将 CA 颁发者名称配置为指定的 DN 字符串。在本示例中，使用的 CN (公用名称) 为 `cisco1.cisco.com`，L (位置) 为 `RTP`，C (国家/地区) 为 `美国`：`R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US`
5. 以天数为单位指定 CA 证书或其他一般证书的有效期。有效值范围自 1 天到 1825 天。默认的 CA 证书有效期是三年，默认的证书有效期是一年。证书有效期的最长期限比 CA 证书有效期短一个月。例如：`R1(cs-server)#lifetime ca-certificate 365 R1(cs-server)#lifetime certificate 200`
6. 以小时为单位定义证书服务器使用的 CRL 的有效期。有效期的最大值为 336 小时 (两周)。默认值是 168 小时 (一周)。`R1(cs-server)#lifetime crl 24`
7. 定义由证书服务器签发的证书中使用的证书撤销列表分配点 (CDP)。URL 必须是 HTTP URL。例如，假设我们的服务器 IP 地址为 `172.18.108.26`：`R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl`
8. 要启用 CA 服务器，请发出 `no shutdown` 命令。`R1(cs-server)#no shutdown` **注意**：仅在您已经完全配置好证书服务器之后才能发出此命令。

[配置第二个 IOS 路由器 \(R2\) 并向证书服务器进行注册](#)

遵循该步骤。

1. 在 R2 上配置主机名、域名并生成 RSA 密钥。要将路由器的主机名配置为 R2，请使用 `hostname` 命令：`Router(config)#hostname R2 R2(config)#` 请注意，在您输入 `hostname` 命令之后，路由器的主机名立即发生了更改。要在路由器上配置域名，请使用 `ip domain-name` 命令：`R2(config)#ip domain-name cisco.com` 要生成 R2 密钥对，请使用 `crypto key generate rsa` 命

令 : R2(config)#**crypto key generate rsa** The name for the keys will be: R2.cisco.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA keys ...[OK]

2. 在全局配置模式中使用以下命令，以便向 CA 表明路由器应该使用（本示例中的 Cisco IOS CA）并为信任点 CA 指定特性：

crypto ca trustpoint cisco enrollment retry count 5 enrollment retry period 3 enrollment url http://14.38.99.99:80 revocation-check none 注意：**crypto ca trustpoint** 命令结合了现有的 **crypto ca identity** 命令和 **crypto ca trusted-root** 命令，从而能够以单个命令提供组合功能。

3. 使用 **crypto ca authenticate cisco** 命令（cisco 是信任点标签），以便从 CA 服务器检索根证书：R2(config)#**crypto ca authenticate cisco**

4. 使用 **crypto ca enroll cisco** 命令（cisco 是信任点标签），以便注册并生成：R2(config)#**crypto**

ca enroll cisco 成功向 Cisco IOS CA 服务器进行注册之后，使用 **show crypto ca certificates** 命令应该就可以看到所签发的证书。这是命令的输出。该命令显示了详细的证书信息，与 Cisco IOS CA 服务器中配置的参数对应：R2#**show crypto ca certificates** Certificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer: **cn=cisco1.cisco.com l=RTP c=US** Subject: Name: **R2.cisco.com** hostname=**R2.cisco.com** CRL Distribution Point: **http://172.18.108.26/cisco1cdp.cisco1.crl** Validity Date: start date: 15:41:11 UTC Jan 21 2004 end date: 15:41:11 UTC Aug 8 2004 renew date: 00:00:00 UTC Jan 1 1970 Associated Trustpoints: **cisco** CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer: **cn=cisco1.cisco.com l=RTP c=US** Subject: **cn=cisco1.cisco.com l=RTP c=US** Validity Date: start date: 15:39:00 UTC Jan 21 2004 end date: 15:39:00 UTC Jan 20 2005 Associated Trustpoints: **cisco**

5. 要将密钥保存到永久闪存中，请输入以下命令：**hostname(config)#write memory**

6. 要保存配置，请输入以下命令：**hostname#copy run start**

验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序](#)（[仅限注册用户](#)）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 **show** 命令输出的分析。

- **show crypto ca certificates** - 显示证书。
- **show crypto key mypubkey rsa** - 显示密钥对。!% Key pair was generated at: 09:28:16 EST Jan 30 2004

```
!Key name: ese-ios-ca
! Usage: General Purpose Key
! Key is exportable.
! Key Data:
! 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198
! C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060
! E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B
! ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE
! 9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
!% Key pair was generated at: 09:28:17 EST Jan 30 2004
!Key name: ese-ios-ca.server
! Usage: Encryption Key
! Key is exportable.
! Key Data:
! 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
! 0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
! 18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
! 3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```

- **crypto pki server ese-ios-ca info crl** - 显示证书撤销列表 (CRL)。! Certificate Revocation

List:

```
! Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
! This Update: 09:58:27 EST Jan 30 2004
! Next Update: 09:58:27 EST Jan 31 2004
! Number of CRL entries: 0
! CRL size: 300 bytes
```

- **crypto pki server ese-ios-ca info requests** - 显示挂起的注册请求。! Enrollment Request

Database:

```
! ReqID State Fingerprint SubjectName
! -----
```

- **show crypto pki server** - 显示当前的 Public Key Infrastructure (PKI) 服务器状态。! Certificate

Server status: enabled, configured

```
! Granting mode is: manual
! Last certificate issued serial number: 0x1
! CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
! CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
! Current storage dir: nvram:
! Database Level: Names - subject name data written as .cnm
```

- **crypto pki server cs-label grant { all|transaction-id }** - 同意所有或特定的 SCEP 请求。
- **crypto pki server cs-label reject {全部|transaction-id }** - 拒绝所有或特定的 SCEP 请求。
- **crypto pki server cs-label password generate [minutes]** - 为某个 SCEP 请求生成一个在一段时间 (minutes - 以分钟为单位的时间长度) 内有效的一次性口令 (OTP)。有效范围自 1 分钟到 1440 分钟。默认时间为 60 分钟。**注意**：一次仅有一个 OTP 有效。如果生成另一个 OTP，之前的 OTP 就不再有效。
- **crypto pki server cs-label revoke certificate-serial-number** - 根据序列号撤销证书。
- **crypto pki server cs-label request pkcs10 {URL URL|terminal} [pem]** - 向请求数据库中添加 base64 或 PEM PKCS10 证书注册请求。
- **crypto pki server cs-label info crl** - 显示有关当前 CRL 状态的信息。
- **crypto pki server cs-label info request** - 显示所有未解决的证书注册请求。

有关其他验证信息，请参阅本文档中[验证生成的密钥对](#)部分。

故障排除

有关故障排除信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

注意：大多数情况下，删除并重新定义 CA 服务器就可以解决问题。

相关信息

- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)