配置一台Cisco IOS路由器並將其註冊到另一台配置為CA伺服器的Cisco IOS路由器

目錄

簡介

本檔案將說明如何將Cisco IOS®路由器設定為憑證授權單位(CA)伺服器。此外，還說明了如何註冊另一個Cisco IOS路由器，以便從CA伺服器獲取IPsec身份驗證的根證書和ID證書。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 兩台執行Cisco IOS軟體版本12.3(4)T3的Cisco 2600系列路由器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

生成並匯出證書伺服器的RSA金鑰對

第一步是生成Cisco IOS CA伺服器使用的RSA金鑰對。在路由器(R1)上生成RSA金鑰，如以下輸出所示：

```
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：對於計畫用於證書伺服器的金鑰對(*key-label*)，您必須使用相同的名稱(通過**crypto pki server *cs-label* 命令)。**

匯出生成的金鑰對

將金鑰匯出到非易失性RAM(NVRAM)或TFTP（基於您的配置）。 在此範例中，使用NVRAM。根據您的實作，您可能要使用單獨的TFTP伺服器來儲存憑證資訊。

```
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伺服器，可以重新匯入產生的金鑰對，如下命令所示：

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

注意：如果不希望金鑰從證書伺服器匯出，請在匯出為不可匯出的金鑰對後將其匯入證書伺服器。如此一來，金鑰就無法再被拿掉。

驗證生成的金鑰對

發出**show crypto key mypubkey rsa**命令，以驗證生成的金鑰對。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

```
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 DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

在路由器上啟用HTTP伺服器

Cisco IOS CA伺服器僅支援透過簡單憑證註冊通訊協定(SCEP)完成的註冊。 因此，為使這一點成為可能，路由器必須運行內建的Cisco IOS HTTP伺服器。使用**ip http server**命令以啟用它：

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

在路由器上啟用和配置CA伺服器

請完成以下步驟：

1. 請務必記住，憑證伺服器必須與您剛才手動產生的金鑰對使用相同的名稱。該標籤與生成的金鑰對標籤匹配：
   ```
   R1(config)#crypto pki server cisco1
   ```
   啟用證書伺服器後，可以使用預配置的預設值或通過CLI指定證書伺服器的功能值。
2. **database url**命令指定CA伺服器的所有資料庫條目的寫入位置。如果未指定此命令，則所有資

料庫條目都將寫入快閃記憶體。

```
R1(cs-server)#database url nvram:
```

注意：如果使用TFTP伺服器，則URL需要為**tftp://<ip_address>/directory**。

3. 配置資料庫級別：

```
R1(cs-server)#database level minimum
```

此命令控制證書註冊資料庫中儲存的資料型別：**Minimum** — 僅儲存足夠的資訊，以繼續頒發新證書而不會發生衝突。預設值。**Names** — 除了最小級別中提供的資訊外，每個證書的序列號和主題名稱也包含在內。**Complete** — 除了最小和名稱級別中提供的資訊外，每個已頒發的證書都將寫入資料庫。**注意：**complete關鍵字可生成大量資訊。如果發出，您還應指定通過**database url**命令儲存資料的外部TFTP伺服器。

4. 將CA頒發者名稱配置為指定的DN字串。在本示例中，使用了cisco1.cisco.com的CN（通用名稱）、RTP的L（位置）和US的C（國家/地區）：

```
R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. 指定CA證書或證書的生存期（以天為單位）。有效值範圍為*1天到1825天*。預設CA證書有效期為三年，預設證書有效期為一年。最大證書生命期*比CA證書*的生命期短一個月。例如：

```
R1(cs-server)#lifetime ca-certificate 365
R1(cs-server)#lifetime certificate 200
```

6. 定義證書伺服器使用的CRL的生存時間（小時）。最大生存時間值**為336**小時（兩週）。 預設值為**168小時**（一週）。

```
R1(cs-server)#lifetime crl 24
```

7. 定義證書撤銷清單分發點(CDP)，用於由證書伺服器頒發的證書。URL必須是HTTP URL。例如，我們的伺服器的IP地址為172.18.108.26:

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. 發出**no shutdown**命令以啟用CA伺服器：

```
R1(cs-server)#no shutdown
```

注意：僅在完成證書伺服器配置後發出此命令。

配置第二台IOS路由器(R2)並將其註冊到證書伺服器

請按照以下步驟操作。

1. 在R2上配置主機名、域名並生成RSA金鑰。使用**hostname**命令將路由器的主機名配置為R2:

```
Router(config)#hostname R2
R2(config)#
```

請注意，輸入**hostname**命令後，路由器的主機名立即發生了更改。使用**ip domain-name**命令在路由器上配置域名：

```
R2(config)#ip domain-name cisco.com
```

使用**crypto key generate rsa**命令生成R2金鑰對：

```
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. 在全域性配置模式下使用以下命令以向CA宣告您的路由器應使用（在本示例中為Cisco IOS CA）並指定信任點CA的特徵：

```
crypto ca trustpoint cisco
 enrollment retry count 5
 enrollment retry period 3
 enrollment url http://14.38.99.99:80
 revocation-check none
```

註：crypto ca trustpoint命令將現有的crypto ca identity 命令和crypto ca trusted-root 命令統一起來，從而在一個命令下提供組合功能。

3. 使用**crypto ca authenticate cisco**命令（cisco是信任點標籤）從CA伺服器檢索根證書：

```
R2(config)#crypto ca authenticate cisco
```

4. 使用**crypto ca enroll cisco**命令（cisco是信任點標籤）以註冊和生成：

```
R2(config)#crypto ca enroll cisco
```

成功註冊到Cisco IOS CA伺服器後，您應該使用**show crypto ca certificates**命令來檢視頒發的證書。這是命令的輸出。命令會顯示詳細的證書資訊，這些資訊與Cisco IOS CA伺服器中配置的引數相對應：

```
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. 輸入以下命令可將金鑰儲存到永久快閃記憶體：

```
hostname(config)#write memory
```

6. 輸入以下命令可儲存組態：

```
hostname#copy run start
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show crypto ca certificates** — 顯示證書。
- **show crypto key mypubkey rsa** — 顯示金鑰對。

```
!% 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** — 顯示證書吊銷清單(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** — 顯示掛起的註冊請求。

```
! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------------
```

- **show crypto pki server** — 顯示當前公鑰基礎架構(PKI)伺服器狀態。

```
! 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* }** — 授予所有或特定SCEP請求。
- **crypto pki server *cs-label* reject { all | *transaction-id* }** — 拒絕所有或特定SCEP請求。
- **crypto pki server cs-label password generate [*minutes*]** — 為SCEP請求生成一次性密碼(OTP)(分鐘 — 密碼有效的時間長度（以分鐘為單位）。有效範圍為1至1440分鐘。預設值為

60分鐘。**注意**：一次只有一個OTP有效。如果產生第二個OTP，則先前的OTP不再有效。
- crypto pki server *cs-label* ***revoke*** *certificate-serial-number* ***— 根據證書的序列號撤銷證書。***
- **crypto pki server *cs-label* request *pkcs10* {url *url* | *terminal*} [pem]** — 手動將base64或PEM PKCS10證書註冊請求新增到請求資料庫。
- **crypto pki server *cs-label* info crl** — 顯示有關當前CRL狀態的資訊。
- **crypto pki server *cs-label* info request** — 顯示所有未完成的證書註冊請求。

如需其他驗證資訊，請參閱本檔案的驗證產生的金鑰對一節。

疑難排解

如需疑難排解資訊，請參閱IP安全性疑難排解 — 瞭解和使用debug命令。

注意：在許多情況下，刪除並重新定義CA伺服器可以解決這些問題。

相關資訊

- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems