Cisco IOS ルータの設定と CA サーバとして設定した別の Cisco IOS ルータへの登録

目次

概要

このドキュメントでは、Cisco IOS® ルータを Certificate Authority（CA; 認証局）サーバとして設定する方法について説明しています。 さらに、他の Cisco IOS ルータを登録して、CA サーバから IPSec 認証のためのルートと ID の証明書を取得する方法を解説しています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.3(4)T3 が稼働する 2 台の Cisco 2600 シリーズ ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく

必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

証明書サーバの RSA キー ペアの生成およびエクスポート

最初の手順では、Cisco IOS CA サーバで使用する RSA キー ペアを生成します。 ルータ（R1）で、次の出力に示すように RSA キーを作成します。

```
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: 証明書サーバで使用するキー ペア（*key-label*）に、同じ名前を使用する必要があります（後述の **crypto pki server cs-label** コマンドを使用します）。

生成したキー ペアのエクスポート

使用している構成に応じて、Non-Volatile RAM（NVRAM; 不揮発性 RAM）または TFTP にキーをエクスポートします。 この例では、NVRAM を使用します。 実装方法によっては、証明書情報を保存するために、独立した TFTP サーバを使用することができます。

```
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)#
```

TFTP サーバを使用する場合、次のコマンドで示すように、生成されたキー ペアを再インポートできます。

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

注: 証明書サーバからキーをエクスポートできないようにする場合は、エクスポートできないキー ペアとしてキーをエクスポートした後、そのキーを証明書サーバにインポートして戻します。 このようにすると、キーを再び取り出すことはできなくなります。

生成済キー ペアの検証

生成したキー ペアを確認するには、**show crypto key mypubkey rsa** コマンドを発行します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

```
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
```

ルータでの HTTP サーバの有効化

Cisco IOS CA サーバは、Simple Certificate Enrollment Protocol（SCEP）を使用して実行される登録だけをサポートしています。 さらに、これを可能にするには、ルータで組み込み Cisco IOS HTTP サーバが稼働している必要があります。 **ip http server** コマンドを使用すると、これが有効になります。

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

ルータでの CA サーバのイネーブル化および設定

次の手順を実行します。

1. 非常に重要なのは、証明書サーバでは手作業で生成したキー ペアに同じ名前を使用する必要があるということです。次のように、ラベルは生成済キー ペアのラベルに一致しています。`R1(config)#crypto pki server cisco1` 証明書サーバをイネーブルにした後、事前設定のデフォルト値を使用するか、CLI から証明書サーバの機能用に値を指定できます。
2. **database url** コマンドは、CA サーバのすべてのデータベース エントリを書き出す場所を指定します。 このコマンドを指定しない場合、すべてのデータベース エントリはフラッシュに書き込まれます。`R1(cs-server)#database url nvram:` **注:** TFTP サーバを使用する場合は、URL を **tftp://<ip_address>/directory** にする必要があります。
3. データベース レベルを次のように設定します。`R1(cs-server)#database level minimum` このコマンドは、証明書登録データベースに保存するデータの種類を制御します。**minimum**：競合しない新しい証明書を継続して発行するために十分な情報が保存されます。 デフォルト値です。**names**：minimum レベルで得られる情報のほか、各証明書のシリアル番号および主体者名。**complete**：minimum レベルおよび names レベルで得られる情報のほか、発行済みの各証明書がデータベースに書き込まれます。**注: complete** キーワードを指定すると、大量の情報が生成されます。 これが使用される場合は、さらに **database url** コマンドで、データを保存する外部 TFTP サーバを指定する必要があります。
4. 指定された DN 文字列に CA 発行者名を設定します。 この例では、CN（Common Name）に cisco1.cisco.com、L（Locality）に RTP、C（Country）に US を使用しています。`R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US`
5. CA 証明書または証明書のライフタイムを日単位で指定します。有効な値の範囲は *1 ~ 1825 日*です。 デフォルトの CA 証明書ライフタイムは 3 年で、デフォルトの証明書ライフタイムは 1 年です。 最長の証明書ライフタイムは、CA 証明書のライフタイムよりも *1 か月短くなります*。 次に、例を示します。`R1(cs-server)#lifetime ca-certificate 365 R1(cs-server)#lifetime certificate 200`
6. 証明書サーバで使用する CRL のライフタイムを時間単位で定義します。 最長のライフタイム値は **336 時間**（2 週間）です。 デフォルト値は **168 時間**（1 週間）です。`R1(cs-server)#lifetime crl 24`
7. 証明書サーバで発行された証明書で使用する Certificate-Revocation-List Distribution Point（CDP; 証明書失効リスト分散ポイント）を定義します。URL は HTTP URL である必要があります。 たとえば、このサーバの IP アドレスは 172.18.108.26 でした。`R1(cs-`

server)#**cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl**

8. CA サーバをイネーブルにするには、**no shutdown** コマンドを発行します。R1(cs-server)#**no shutdown** **注:** 証明書サーバの設定完了後だけ、このコマンドを発行します。

2 番目の IOS ルータ（R2）の設定および証明書サーバへの登録

次の手順に従います。

1. ホスト名、ドメイン名を設定し、R2 で RSA キーを生成します。ルータのホスト名が R2 になるように設定するには、**hostname** コマンドを使用します。Router(config)#**hostname R2** R2(config)# **hostname** コマンドを入力した後すぐに、ルータのホスト名が変更されることに注意してください。ルータでドメイン名を設定するには、**ip domain-name** コマンドを使用します。R2(config)#**ip domain-name cisco.com** R2 キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。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. ルータが使用する CA（ここでは、Cisco IOS CA）を宣言して、トラストポイント CA の特性を定義するには、グローバル設定モードで次のコマンドを使用します。**crypto ca trustpoint cisco enrollment retry count 5 enrollment retry period 3 enrollment url http://14.38.99.99:80 revocation-check none** **注:** **crypto ca trustpoint** コマンドは、既存の **crypto ca identity** コマンドと **crypto ca trusted-root** コマンドをまとめたものです。これにより、1 つのコマンドで一体化された機能を利用できます。
3. CA サーバからルート証明書を取得するには、**crypto ca authenticate cisco** コマンド（cisco はトラストポイント ラベルです）を使用します。R2(config)#**crypto ca authenticate cisco**
4. 登録および生成するには、**crypto ca enroll cisco** コマンド（cisco はトラストポイント ラベルです）を使用します。R2(config)#**crypto ca enroll cisco** Cisco IOS CA サーバへの登録が完了したら、**show crypto ca certificates** コマンドを使用して発行された証明書を確認できます。 このコマンドの出力を示します。 このコマンドにより、Cisco IOS CA サーバで設定されたパラメータに応じた、詳細な証明書情報が表示されます。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. キーを固定フラッシュ メモリに保存するには、次のコマンドを入力します。hostname(config)#**write memory**
6. 設定を保存するには、次のコマンドを使用します。hostname#**copy run start**

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto ca certificates**：証明書を表示します。

- **show crypto key mypubkey rsa**：キー ペアを表示します。
```
!% 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**：Certificate Revocation List（CRL; 証明書失効リスト）を表示します。
```
! 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**：保留中の登録要求を表示します。
```
! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------------
```
- **show crypto pki server**：現在の Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）サーバの状態を表示します。
```
! 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 | tranaction-id }**：すべてまたは特定の SCEP 要求を認可します。
- **crypto pki server cs-label reject { all | tranaction-id }**：すべてまたは特定の SCEP 要求を拒否します。
- **crypto pki server cs-label password generate [minutes]**：SCEP 要求の One-Time Password（OTP; ワンタイム パスワード）を生成します（minutes：パスワードが有効な期間（分単位））。 有効な範囲は 1 ~ 1440 分です。 デフォルトは 60 分です。**注:** 一度に有効な OTP は 1 つだけです。 次の OTP が生成されると、以前の OTP は無効になります。
- **crypto pki server cs-label revoke certificate-serial-number**：証明書をそのシリアル番号に基づいて無効にします。
- **crypto pki server cs-label request pkcs10 {url url | terminal} [pem]**：Base64 または PEM PKCS10 の証明書登録要求を要求データベースに手動で追加します。
- **crypto pki server cs-label info crl**：現在の CRL のステータスに関する情報を表示します。
- **crypto pki server cs-label info request**：未処理のすべての証明書登録要求を表示します。

その他の確認情報については、このドキュメントの「生成したキー ペアの確認」セクションを参照してください。

トラブルシューティング

トラブルシューティング情報については、『IP Security のトラブルシューティング：debug コマンドの説明と使用』を参照してください。

注: 多くの場合、CA サーバを削除してから再定義すると、問題を解決できます。

関連情報

- IPSec ネゴシエーション/IKE プロトコル
- テクニカルサポートとドキュメント - Cisco Systems