Configure and Enroll a Cisco VPN 3000 Concentrator to a Cisco IOS Router as a CA Server

Document ID: 50281

Contents

Introduction

This document describes how to configure a Cisco IOS® Router as a Certificate Authority (CA) server. Additionally, it illustrates how to enroll a Cisco VPN 3000 Concentrator to the Cisco IOS router to obtain a root and ID certificate for IPSec authentication.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

  - Cisco 2600 Series Router that runs Cisco IOS Software Release 12.3(4)T3
  - Cisco VPN 3030 Concentrator Version 4.1.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:

VPN 3000 Concentrator
172.18.124.130/24

Cisco IOS CA Server
14.38.99.99/16

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Generate and Export the RSA Key Pair for the Certificate Server

The first step is to generate the RSA key pair which the Cisco IOS CA server uses. On the Router (R1), generate the RSA keys as seen here:

```
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
```

Note: You must use the same name for the key pair (*key−label*) that you plan to use for the certificate server (via the **crypto pki server** *cs−label* command covered later).

Export the Generated Key Pair

The keys then need to be exported to Non−Volatile RAM (NVRAM) or TFTP (based on your configuration). In this example, NVRAM is used. Based on your implementation, you might potentially want to use a separate TFTP server to store your certificate information.

```
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)#
```

If you use a TFTP server, you can re−import the generated key pair as seen here:

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

Note: If you do not want the key to be exportable from your certificate server, import it back to the certificate server after it has been exported as a non–exportable key pair. Therefore, the key cannot be taken off again.

Verify the Generated Key Pair

You can verify the generated key pair by invoking the **show crypto key mypubkey rsa** command:

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

```
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
```

Enable the HTTP Server on the Router

The Cisco IOS CA Server only supports enrollments done via Simple Certificate Enrollment Protocol (SCEP). Consequently, in order to make this possible, the router must run the built–in Cisco IOS HTTP server. To enable it, use the **ip http server** command:

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

Enable and Configure the CA Server on the Router

Follow this procedure.

1. It is very important to remember that the certificate server must use the same name as the key pair you just manually generated. The label matches the generated key pair label:

```
R1(config)#crypto pki server cisco1
```

After you have enabled a certificate server, you can use the preconfigured default values or specify values via CLI for the functionality of the certificate server.

2. The **database url** command specifies the location where all database entries for the CA server are written out.

If this command is not specified, all database entries are written to Flash.

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

Note: If you use a TFTP server, the URL needs to be **tftp://<ip_address>/directory**.

3. Configure the database level:

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

This command controls what type of data is stored in the certificate enrollment database.

- **Minimum** Enough information is stored only to continue issuing new certificates without conflict; the default value.
- **Names** In addition to the information given in the minimal level, the serial number and subject name of each certificate.
- **Complete** In addition to the information given in the minimal and names levels, each issued certificate is written to the database.

Note: The **complete** keyword produces a large amount of information. If it is issued, you also need to specify an external TFTP server in which to store the data via the **database url** command.

4. Configure the CA issuer name to the specified DN–string. In this example, the CN (Common Name) of cisco1.cisco.com, L (Locality) of RTP, and C (Country) of US are used:

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

5. Specify the lifetime, in days, of a CA certificate or a certificate.

Valid values range from *1 day to 1825 days*. The default CA certificate lifetime is **3 years** and the default certificate lifetime is **1 year**. The maximum certificate lifetime is *1 month less* than the lifetime of the CA certificate. For example:

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

6. Define the lifetime, in hours, of the CRL that is used by the certificate server. The maximum lifetime value is **336 hours** (2 weeks). The default value is **168 hours** (1 week).

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

7. Define a Certificate–Revocation–List Distribution Point (CDP) to be used in the certificates that are issued by the certificate server. The URL must be an HTTP URL.

For example, the IP address of our server is 172.18.108.26.

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

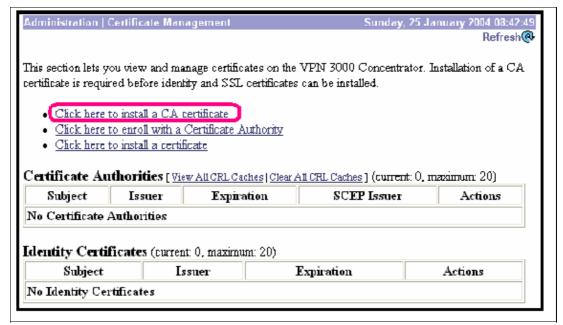8. Enable the CA server by issuing the **no shutdown** command.

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

Note: Issue this command only after you have completely configured your certificate server.

Configure and Enroll the Cisco VPN 3000 Concentrator

Follow this procedure.

1. Selecting **Administration** > **Certificate Management** and choose **Click here to install a CA certificate** to retrieve the root certificate from the Cisco IOS CA Server.
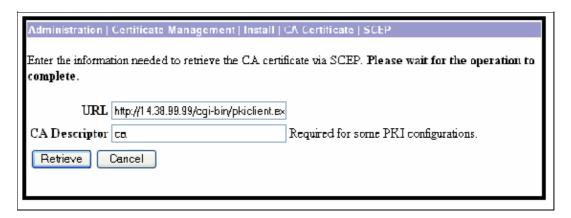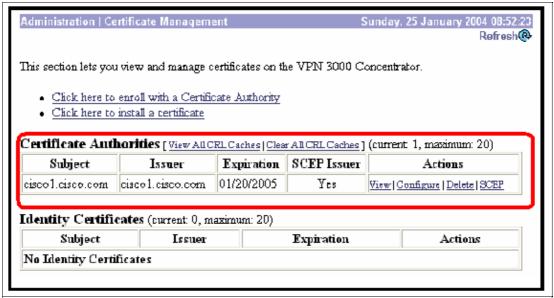
2. Select **SCEP** as the method of installation.

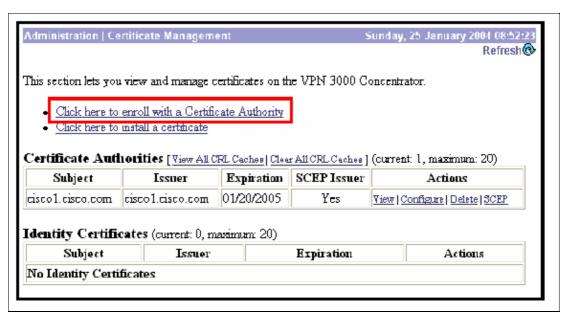3. Enter the URL of the Cisco IOS CA Server, a CA descriptor, and click **Retrieve**.

   Note: The correct URL in this example is http://14.38.99.99/cgi−bin/pkiclient.exe (you must include the full path of /cgi−bin/pkiclient.exe).

   Select **Administration** > **Certificate Management** to verify that the root certificate has been installed. This figure illustrates the root certificate details.

4. Select **Click here to enroll with a Certificate Authority** to obtain the ID certificate from the Cisco IOS CA Server.

5. Select **Enroll via SCEP at cisco1.cisco.com** (cisco1.cisco.com is the CN of the Cisco IOS CA Server).

6. Complete the enrollment form by entering all the information to be included within the certificate request.

After completion of the form, click **Enroll** to begin the enrollment request to the CA server.

After you click Enroll, the VPN 3000 Concentrator displays "A certificate request has been generated".

Note: The Cisco IOS CA Server can be configured to automatically grant the certificates with the Cisco IOS CA Server subcommand **grant automatic**. This command is used for this example. To see the details of the ID certificate, select **Administration** > **Certificate Management**. The certificate displayed is similar to this.

Verify

See the Verify the Generated Key Pair section for verification information.

Troubleshoot

For troubleshooting information, refer to either Troubleshooting Connection Problems on the VPN 3000 Concentrator or IP Security Troubleshooting – Understanding and Using debug Commands.

Related Information

- **Cisco VPN 3000 Series Concentrator Support Page**
- **Cisco VPN 3000 Series Client Support Page**
- **IPSec Support Page**
- **Technical Support – Cisco Systems**