配置并且登记Cisco VPN 3000集中器到Cisco IOS路由器作为CA服务器

目录

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，还阐述了如何将 Cisco VPN 3000 集中器注册到 Cisco IOS 路由器，以获取根证书和 ID 证书，用于进行 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 Cisco 2600 系列路由器
- Cisco VPN 3030 集中器版本 4.1.2

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 Cisco IOS CA 服务器使用的 RSA 密钥对。在路由器 (R1) 上生成 RSA 密钥，如下所示：

```
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： 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

然后将该密钥导出到非易失性 RAM (NVRAM) 或 TFTP（根据您的配置）。在本示例中，使用 NVRAM。根据实施情况，您可能希望使用单独的 TFTP 服务器来存储证书信息。

```
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，您可以按如下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，密钥就不能再次导出了。

验证生成的密钥对

您可以通过调用 **show crypto key mypubkey rsa** 命令来验证生成的密钥对：

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 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 DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

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。要启用它，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

遵循该步骤。

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 **tftp:// <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的类型。**Minimum** — 存储足以在不发生冲突的情况下继续签发新证书的最少信息；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。如果发出此命令，您还需要通过 **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 证书有效期为 **3 年**，默认的证书有效期为 **1 年**。最大证书有效期比 CA 证书有效期*短 1 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）。默认值为 **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 Certificate-Revocation-List 分发点 (CDP)。URL 必须是 HTTP URL。例如，我们的服务器的 IP 地址为 172.18.108.26。
```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. 可通过发出 **no shutdown** 命令来启用 CA 服务器。
```
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。

配置和注册 Cisco VPN 3000 集中器

遵循该步骤。

1. 选择 **Administration > Certificate Management**，然后选择 **Click here to install a CA certificate**，以便从 Cisco IOS CA 服务器取回根证书。
2. 选择 **SCEP** 作为安装方法。
3. 输入 Cisco IOS CA 服务器的 URL（一个 CA 描述符），然后单击 **Retrieve**。**注意：** 本例中的正确 URL 应为 http://14.38.99.99/cgi-bin/pkiclient.exe（必须包括 /cgi-bin/pkiclient.exe 的完整路径）。选择 **Administration > Certificate Management** 以验证根证书是否已安装。此图说明了根证书的详细信息。
4. 选择 **Click here to enroll with a Certificate Authority**，以便从 Cisco IOS CA 服务器获取 ID 证书。
5. 选择 **Enroll via SCEP at cisco1.cisco.com**（cisco1.cisco.com 是 Cisco IOS CA 服务器的 CN）。
6. 输入证书申请中包含的所有信息，以完成注册表。完成注册表后，单击 **Enroll** 开始对 CA 服务器的注册请求。单击“Enroll”之后，VPN 3000 集中器将显示“A certificate request has been generated”。**注意：** 可使用 Cisco IOS CA 服务器子命令 **grant automatic** 将 Cisco IOS CA 服务器配置为自动授予证书。本例中使用了此命令。要查看 ID 证书的详细信息，请选择 **Administration > Certificate Management**。显示的证书类似于以下内容。

验证

有关验证信息，请参阅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 VPN 3000 集中器连接问题故障排除疑难解答或 IP 安全故障排除 - 了解和使用 debug 命令。

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPSec 支持页面
- 技术支持 - Cisco Systems