目录

简介

本文为动态LAN提供一配置示例给在Cisco IOS路由器之间的LAN VPN该使用数字证书，当使用IOS Certificate Authority (CA)功能时。本文档演示如何在配置 Cisco IOS 路由器以及如何配置 IOS CA 服务器以便通过自动注册获得身份证书。

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 12.4(6) T 的 Cisco 2851 路由器
- 运行 Cisco IOS 软件版本 12.3(14)YT1 的 Cisco 871 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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- 在路由器上配置 IOS CA 服务器
- 身份验证并注册到 IOS CA 服务器
- 中心配置
- 分支配置

在路由器上配置 IOS CA 服务器

要在路由器上配置 IOS CA 服务器，请完成以下步骤：

1. 发出 **crypto pki server 命令**以便输入 IOS CA 服务器配置的参数。在本例中，赋予 IOS CA 服务器配置的标签是 **cisco**。该标签可以是您喜欢的任何名称。`HubIOSCA(config)#crypto pki server cisco`
2. 发出 **issuer-name** 子命令以便定义证书信息。在这种情况下，共同名称(CN)、现场(l)，状态(ST)和国家代码(c)定义作为显示此处：`HubIOSCA(cs-server)#issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US`
3. 发出 **grant** 命令。在本例中，IOS 服务器自动向客户端授予证书。`HubIOSCA(cs-server)#grant auto`
4. 发出 **no shut** 命令以便启用 IOS CA 服务器。`HubIOSCA(cs-server)#no shut`在您输入此命令后，系统提示您输入密码短语以保护私有密钥。在生成 CA 证书以后，有些服务器设置无法进行更改。输入密码短语以保护私有密钥，或输入 **Return** 退出。`HubIOSCA(cs-server)#no shut`

身份验证并注册到 IOS CA 服务器

证书服务器也有一个自动生成的同名信任点。该信任点存储证书服务器的证书。当路由器检测到正在使用某个信任点存储证书服务器的证书之后，该信任点将会锁定，无法对其进行修改。

1. 在您配置证书服务器之前，您可以发出 **crypto pki trustpoint** 命令以便手工创建和设置此信任点。这样，您就可以指定一个备用 RSA 密钥对（使用 **rsakeypair** 命令）。**注意：** 自动生成的信任点和证书服务器证书不能用于证明证书服务器设备的身份。所以，所有命令行界面(CLI)，例

如**IP HTTP安全信任点**命令，使用指定CA信任点获取证书和验证客户端的连接的证书必须指向在证书服务器设备配置的一另外的信任点。如果服务器是根证书服务器，则它使用 RSA 密钥对和几个其他属性生成自签名证书。相关的 CA 证书具有以下密钥扩展用途：数字签名证书签名证书撤销列表(CRL)符号在本例中，HubIOSCA 路由器使用其他信任点凭借证书进行登记以便能与分支路由器建立 VPN 隧道。按照下面所示定义一个信任点（iosca 是为这个新信任点指定的名称）：HubIOSCA(config)#**crypto pki trustpoint iosca**

2. 输入注册 URL，如下所示：HubIOSCA(ca-trustpoint)#**enrollment url http://1.1.1.1:80**在本例中，未进行 CRL 撤销检查。HubIOSCA(ca-trustpoint)#**revocation-check none**
3. 发出 **crypto ca authenticate iosca** 命令以便接收根证书。HubIOSCA(config)#**crypto ca authenticate iosca**该证书具有以下属性：Fingerprint MD5: 441446A1 CA3C32B6 3B680204 452A00B2 Fingerprint SHA1: 6C09E064 E4B09087 DDFFADCD 2E9C6853 1669BF39Do you accept this certificate? [yes/no]: **yes**Trustpoint CA certificate accepted.
4. 发出 **crypto ca enroll iosca** 命令以便获取身份证书。Start certificate enrollment... Create a challenge password. You need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons, your password is not saved in the configuration. Please make a note of it.Password:Re-enter password: The subject name in the certificate includes: HubIOSCA.cisco.com Include the router serial number in the subject name? [yes/no]: **no** Include an IP address in the subject name? [no]: **no** Request certificate from CA? [yes/no]: **yes** Certificate request sent to Certificate Authority The **show crypto ca certificate iosca verbose** command shows the fingerprint.
5. 发出 **show crypto pki cert** 命令以便验证已安装了证书。HubIOSCA#**show crypto pki cert**Certificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: Name: HubIOSCA.cisco.com hostname=HubIOSCA.cisco.com Validity Date: start date: 19:11:55 UTC Aug 11 2006 end date: 19:11:55 UTC Aug 11 2007 Associated Trustpoints: iosca CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Validity Date: start date: 19:01:54 UTC Aug 11 2006 end date: 19:01:54 UTC Aug 10 2009 Associated Trustpoints: iosca cisco**注意：** 因为 CA 服务器也是一个 IPSec 对等体，所以中心路由器需要身份验证并注册到同一路由器上的 CA 服务器。

中心配置

中心配置

```
HubIOSCA#show crypto pki certCertificate Status: Available
Certificate Serial Number: 02 Certificate Usage: General
Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject: Name: HubIOSCA.cisco.com
hostname=HubIOSCA.cisco.com Validity Date: start date:
19:11:55 UTC Aug 11 2006 end date: 19:11:55 UTC Aug 11
2007 Associated Trustpoints: iosca CA Certificate Status:
Available Certificate Serial Number: 01 Certificate Usage:
Signature Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Validity
Date: start date: 19:01:54 UTC Aug 11 2006 end date:
19:01:54 UTC Aug 10 2009 Associated Trustpoints: iosca cisco
```

分支配置

分支配置

```
HubIOSCA#show crypto pki certCertificate Status: Available
Certificate Serial Number: 02 Certificate Usage: General
Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject: Name: HubIOSCA.cisco.com
hostname=HubIOSCA.cisco.com Validity Date: start date:
```

```
19:11:55 UTC Aug 11 2006    end   date: 19:11:55 UTC Aug 11
2007  Associated Trustpoints: iosca CA Certificate  Status:
Available  Certificate Serial Number: 01  Certificate Usage:
Signature  Issuer:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US  Validity
Date:    start date: 19:01:54 UTC Aug 11 2006    end   date:
19:01:54 UTC Aug 10 2009  Associated Trustpoints: iosca cisco
```

验证

当前没有可用于此配置的验证过程。

故障排除

证书验证为L2L通道失效。

有时，当您使用一个有效CA证书ISAKMP验证时， IPsec协商可能发生故障。因为预先共享密钥是确实小数据包， VPN隧道协商与预先共享密钥一起使用。如果证书验证需要发送整个证书，被分段的这创建大数据包。分段防止适当地验证的证书在设备之间。

降低MTU并且换成全双工为了解决此问题。设置MTU值为不必须被分段的大小：

```
Router(config)#interface type [slot_#/]port_#Router(config-if)#ip mtu MTU_size_in_bytes
```

相关信息

- 技术支持和文档 - Cisco Systems