目录

简介

及时有效期有构件的所有数字证书在登记期间，由发出的Certificate Authority (CA)服务器分配的证书。当数字证书使用ISAKMP时VPN IPSec认证，有通信设备的证书到期时间和系统时间的自动校验在设备(VPN终端)。这保证使用的证书有效和未超时。也是您为什么*必须*设置在每个VPN终端(路由器)的内部时钟。如果网络时间协议(NTP) (或简单网络时间协议[SNTP])不是可能的在VPN crypto路由器，则请使用**set clock命令的**指南。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据运行该各自平台的镜像的所有路由器。

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。

被认为超时的数字证书或什么时候没有超时？

- 证书超时(无效)，如果系统时间是在证书到期时间之后或在证书前的发出的时期。
- 证书没有超时(有效)，如果系统时间在或在证书的发出的时间和超时的证书的之间时间。

自动注册功能的目的将提供CA管理员机制允许一个当前登记的路由器用其在路由器证书的寿命的一已配置的百分比的CA服务器自动地再登记。这是证书的可管理性/支持能力的一个重要功能作为控制机制。如果使用特定CA潜在发行证书到千位有一个一年寿命的分组VPN路由器(没有自动注册)，则在正确地一年发出的时间，所有证书超时，并且所有分组通过IPSec丢失连接。或者，如果自动注册功能设置“自动登记70"，正如在此示例，然后在70%已签发证书(1年)的寿命中，每个路由器

自动地发出一新的注册请求到在信任点列出的Cisco IOS CA服务器。

注意： 对自动注册功能的一例外是，如果设置到*小于或等于10*，然后是以分钟。如果它*比10极大*，则它是百分比证书的寿命。

有Cisco IOS CA管理员需要知道与自动注册的一些警告。管理员需要执行重新登记的这些操作能是成功的：

1. (除非“授予自动”在Cisco IOS CA服务器使用)，请手工同意或拒绝在Cisco IOS CA服务器的每重新登记请求。Cisco IOS CA服务器还是需要授权或拒绝其中每一个请求(假设Cisco IOS CA没有“”启用的授予自动)。然而，在登记的路由器的管理行为没有要求开始重新登记进程。
2. 保存在重新注册VPN路由器的新的重新登记的证书，如果适当。如果没有待定未获救的配置更改在路由器，则新证书自动地保存对非易失性RAM。新证书在NVRAM写入，并且上一个证书删除。如果有待定未获救的配置更改，则您必须发出**copy run start命令**在登记的路由器为了保存配置更改和新的重新登记的证书到NVRAM。一旦**copy run start命令**完成，然后新证书在NVRAM写入，并且上一个证书删除。**注意：** 当一新的重新登记是成功的时，那不废除那的上一个证书在CA服务器的登记的设备。当VPN设备连通时，他们互相发送证书序号(唯一号码)。**注意：** 例如，如果是在70%证书的寿命，并且VPN分组是再登记与CA，该CA有该主机名的两证书。然而，登记的路由器只有一(更新一个)。如果选择对，您能管理性废除旧有证书，或者请允许它通常超时。**注意：** 自动注册功能的更新的代码版本有一个选项“重新生成”用于登记的密钥对。此选项是重新生成密钥对的“不是”默认。如果此选项选择，请注意Cisco Bug ID CSCea90136。此bug修复允许在临时文件将放置的新的密钥对，当新证书登记在发生使用旧有密钥对)的一个现有IPSec隧道时(。自动注册有选项生成新建的密钥在证明更新时间。目前，在采取获取新证书时候，这导致一项丧失服务。这是因为有新密钥，但是匹配它的没有证书。此功能保留旧有密钥和证书，直到新证书是可用的。自动密钥生成为手动注册也实现。密钥为自动或手动注册生成(当必要时)。找到的版本- 12.3PIH03是的版本修复的12.3T版本应用对-12.3PI03集成无其他信息，联系方式思科技术支持。

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems