配置Cisco VPN 3000集中器4.7.x获得数字证书和SSL证书

目录

简介

本文包括关于如何的逐步指导配置Cisco VPN 3000系列集中器验证与使用数字或身份证书和SSL证书。

注意： 在VPN集中器中，必须禁用负载均衡，在您生成另一SSL证书前，因为这防止证书生成。

请参阅如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书，以便了解有关 PIX/ASA 7.x 中的相同方案的详细信息。

参考的Cisco IOS证书登记使用增强版登记Configuration命令示例为了学习更加大致同样的方案用Cisco IOS平台。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

运行版本4.7的本文档中的信息根据Cisco VPN 3000集中器。

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。

在VPN集中器的安装数字证书

完成这些步骤：

1. 选择**Administration > Certificate Management > Enroll**为了选择数字或身份证书请求。
2. 选择**Administration > Certificate Management > Enrollment > Identity Certificate**并且单击**通过PKCS10 Request(Manual)登记。**
3. 填写请求的字段，然后单击**登记。**这些字段在本例中填写。**公用名称**— altiga30**组织单位**— IPSECCERT (OU应该匹配已配置的IPsec组名)**组织**— Cisco系统**现场**— RTP**州/省**—北卡罗来纳**国家**—美国**完全限定域名**— (没使用这里)**密钥大小**— 512**注意：** 使用简单认证登记协议(SCEP)，如果请求SSL证书或身份证书，这些是可用唯一的RSA的选项。RSA 512位RSA 768位RSA 1024位RSA 2048位DSA 512位DSA 768位DSA 1024位
4. 在您单击后请**登记**，几windows出现。第一个窗口确认您请求证书。一个新的浏览器窗口也打开并且显示您的PKCS请求文件。
5. 在您的认证机构(CA)服务器上，请突出显示请求并且粘贴它在您的CA服务器为了提交您的请求。单击 **Next。**
6. 选择**Advanced请求**并且**其次**单击。
7. **使用a base64 encoded PKCS -7 file，**选择**提交证书请求使用a base64 encoded PKCS -10 file或续订请求**，**其次**然后单击。
8. 剪贴您的PKCS文件到文本字段在Saved Request部分下。然后请点击**提交。**
9. 发行在CA服务器的身份证书。
10. 下载根和身份证书。在您的CA服务器上，请选择**在一待定证书的检查**，并且**其次**单击。
11. 选择**编码的Base64**，并且点击在CA服务器的**下载CA证书。**
12. 保存在您的本地驱动器的身份证书。
13. 在CA服务器上，请选择**获取CA证书或证书撤销列表**为了获得根证明。然后，单击**下一步。**
14. 保存在您的本地驱动器的根证明。
15. 安装根和身份证书在VPN 3000集中器。为了执行此，选择**通过登记获取的Administration > Certificate Manager > Installation > Install证书。**在登记状态下，请点击**安装。**
16. 点击**从工作站的上传文件。**
17. 单击**浏览**并且选择该根证明的文件您保存到您的本地驱动器。选择**安装**安装在VPN集中器的身份证书。管理|证书管理窗口出现作为确认，并且您新的身份证书在Identity Certificates表出现。**注意：** 如果证书发生故障，请完成这些步骤生成新证书。选择 **Administration > Certificate Management。**点击在Action选择框的**删除**SSL证书列表的。选择**管理**>System**重新启动。**选择**保存活动配置在重新启动的时期**，**当前**选择，并且单击**应用。**在重新加载完成后，您当前能生成新证书。

安装在VPN集中器的SSL证书

如果使用您的浏览器和VPN集中器之间的一个安全连接， VPN集中器要求SSL证书。您也需要一SSL证书在您使用管理VPN集中器和WebVPN的接口和终止WebVPN通道的每个接口的。

接口SSL证书，如果不存在，自动地生成，当VPN 3000集中器重新启动时，在您升级VPN 3000集中器软件后。由于自签名证书自生，此证书不是可核实的。没有认证机关保证其标识。使用浏览器，但是此证书允许您做初始联系用VPN集中器。如果要用另一自已签署的SSL证书替换它，请完成这些步骤：

1. 选择**Administration > Certificate Management**。
2. 单击**生成**为了显示新证书在SSL证书表里和替换存在的一个。此窗口允许您配置VPN集中器自动地生成的SSL证书的字段。这些SSL证书是为接口和为负载均衡。如果要获取一可核实的SSL证书(即a发出的一认证机关)，请参阅在本文的VPN集中器部分的安装数字证书为了使用您使用获取身份证书的同一个步骤。但是这次，在**Administration > Certificate Management > Enroll**窗口，点击**SSL证书**(而不是身份证书)。**注意：** *参考管理*/VPN 3000 Concentrator Reference Volume II*证书管理部分*：管理和监听版本4.7关于数字证书和SSL证书的全部信息。

更新在VPN集中器的SSL证书

此部分描述如何更新SSL证书：

如果这是为SSL生成的证书由VPN集中器，请去在SSL部分的**Administration > Certificate Management**。点击**更新**选项，并且那更新SSL证书。

如果这是为外部CA服务器授权的证书，请完成这些步骤：

1. 选择**Administration > Certificate Management >Delete**在*SSL证书*下为了删除从公共接口的过期的证书。点击**是**为了确认SSL证书的删除。
2. 选择**Administration > Certificate Management >生成**为了生成新的SSL证书。公共接口的新的SSL证书出现。

相关信息

- Cisco VPN 3000 系列集中器支持页
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems