为 VPN 设备访问控制配置基于 DN 的加密映射

目录

简介

本文档介绍如何配置基于可分辨名称(DN)的加密映射以提供访问控制，以便VPN设备可以与Cisco IOS®路由器建立VPN隧道。在本文档示例中，Rivest、Shamir和Adelman(RSA)签名是IKE身份验证的方法。除标准证书验证外，基于DN的加密映射还尝试将对等体的ISAKMP身份与其证书中的某些字段(如X.500可分辨名称或完全限定域名(FQDN))匹配。

先决条件

要求

此功能是在Cisco IOS软件版本12.2(4)T中首次引入的。您必须在此版本或更高版本中才能进行此配置。

还测试了思科IOS软件版本12.3(5)。但是，基于DN的加密映射由于Cisco Bug ID CSCed45783(仅限注册的客户)而失败。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 7200 路由器
- 思科IOS软件版本12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

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。

背景信息

以前，在使用RSA签名方法进行IKE身份验证期间，在认证验证和可选证书撤销列表(CRL)检查之后，Cisco IOS继续进行IKE快速模式协商。除加密对等体的IP地址限制外，它没有提供阻止远程VPN设备与任何加密接口通信的方法。

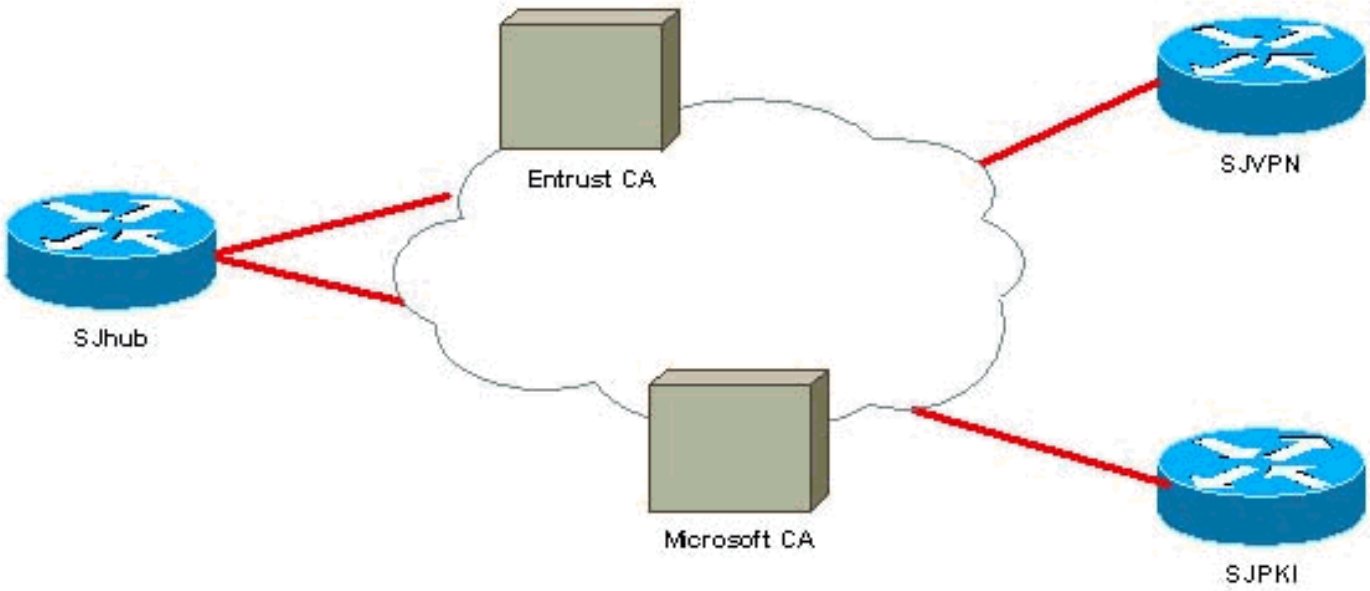
现在，通过基于DN的加密映射，Cisco IOS可以限制远程VPN对等体仅访问具有特定证书的选定接口。特别是具有某些DN或FQDN的证书。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用此图所示的网络设置。



配置

本文档使用此处所示的配置。

在本例中，使用简单的网络设置来演示该功能。SJhub路由器有两个身份证书，一个来自Entrust证书颁发机构(CA)，另一个来自Microsoft CA。请参阅相关信息