为 VPN 设备访问控制配置基于 DN 的加密映射

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[配置](#)
[网络图](#)
[配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文描述如何配置特有名(DN) -基于加密映射提供访问控制，以便VPN设备能设立VPN通道用Cisco IOS路由器。在本文的示例中， Rivest、沙米尔和Adelman (RSA)签名是IKE验证的方法。除标准的证书确认之外，基于DN的加密映射设法匹配与某些字段的对等体的ISAKMP标识其证书的，例如X.500辨别名称或完全合格的域名(FQDN)。

先决条件

要求

此功能在Cisco IOS软件版本12.2(4)T首先介绍。您必须此版本或以后为此配置。

Cisco IOS软件版本12.3(5)也测试了。然而， DN根据加密映射失败的由于Cisco Bug ID CSCed45783 (仅限注册用户)。

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
- Cisco 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IKE验证时使用RSA签名方法和在证明的验证和检查可选的证书撤销列表(CRL)以后，Cisco IOS继续IKE快速模式协商。除在加密对等体的IP地址的限制之外它没有提供一个方法防止远程VPN设备通信与任何加密的接口。

现在与基于DN的加密映射， Cisco IOS能限制远程VPN对等体只访问与特定证书的所选接口。特别是，证书用某一Dns或FQDN。

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，简单网络设置用于展示功能。SJhub路由器有两身份证书，一从Entrust Certificate Authority (CA)和人一个从Microsoft CA。请参阅相关信息