# 用于 Cisco VPN 5000集中器系列的 虚拟专用网和互联网密钥交换

## 目录



## 简介

互联网密钥交换(IKE)是用于安排安全、经过身份验证的通信的标准方法。Cisco VPN 5000集中器使用IKE设置IPSec隧道。这些IPSec隧道是此产品的主干。

## 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：

- VPN 5000系列集中器

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。

# IKE 任务

IKE处理以下任务：

- 身份验证
- 会话协商
- 密钥交换
- IPSec 隧道协商和配置

## 身份验证

身份验证是IKE完成的最重要任务，也是最复杂的任务。无论何时，只要你谈判某件事，就必须知道你与谁谈判。IKE 可以使用若干方法之一对协商各方进行彼此验证。

- **共享密钥** - IKE使用散列技术来确保只有拥有相同密钥的人才能发送IKE数据包。
- **数字签名标准(DSS)或Rivest、Shamir、Adelman(RSA)数字签名** - IKE使用公钥数字签名加密来验证每个方是否都自称是谁。
- **RSA加密**- IKE使用两种方法之一来加密足够的协商，以确保只有具有正确私钥的一方才能继续协商。

会话协商
在会话协商期间，IKE 允许各方协商他们将如何进行认证以及如何保护未来的协商（即 IPSec 隧道协商）。 这些项目经协商：

- **身份验**证方法 — 这是本文档“身份验证”部分列出的方法之一。
- **密钥交换算**法 — 这是一种通过公共介质(Diffie-Hellman)安全交换加密密钥的数学技术。 这些密钥用于加密算法和数据包签名算法中。
- **加密算**法 — 数据加密标准(DES)或三重数据加密标准(3DES)。
- **数据包签**名算法 — 消息摘要5(MD5)和安全散列算法1(SHA-1)。

## 密钥交换

IKE使用协商的密钥交换方法(请参阅本文档的会话协商部分)来创建足够位的加密密钥材料，以保护将来的事务。此方法确保每个IKE会话都使用新的安全密钥集进行保护。

身份验证、会话协商和密钥交换构成IKE协商的第一阶段。对于VPN 5000集中器，这些属性在IKE策略部分**中通过**Protection关键字进行配置。此关键字是包含三个部分的标签：身份验证算法、加密算法和密钥交换算法。这些片段用下划线分隔。标签MD5_DES_G1表示使用MD5进行IKE数据包身份验证，使用DES进行IKE数据包加密，并使用Diffie-Hellman组1进行密钥交换。有关详细信息，请参阅为IPSec隧道安全配置IKE策略。

## IPSec 隧道协商和配置

在IKE完成协商用于交换信息的安全方法（第1阶段）后，IKE用于协商IPSec隧道。这是使用IKE第2阶段完成的。在此交换中，IKE为IPSec隧道创建新密钥材料以供使用（将IKE第1阶段密钥用作基础或执行新密钥交换）。 其间还协商此通道的加密算法和认证算法。

IPSec隧道使用VPN Client隧道的VPN Group(以前称为Secure Tunnel Establishment Protocol(STEP)Client)部分和LAN到LAN隧道的Tunnel Partner部分进行配置。“**VPN用户**”部分存储

每个用户的身份验证方法。这些部分在为IPSec隧道安全配置IKE策略中有说明。

## VPN 5000集中器IKE扩展

- **RADIUS** - IKE不支持RADIUS身份验证。RADIUS身份验证在VPN客户端的第一个IKE数据包之后发生的特殊信息交换中执行。如果需要密码身份验证协议(PAP)，则需要特殊的RADIUS身份验证密钥。有关详细信息，请参阅配置IPSec隧道安全的IKE策略中的NoCHAP和PAPAuthSecret文档。RADIUS身份验证经过身份验证和加密。PAP交换受PAPuthSecret保护。但是，整个IntraPort只有一个此类密钥，因此保护与任何共享密码一样弱。
- **SecurID** - IKE当前不支持SecurID身份验证。SecurID身份验证在第一阶段和第二阶段之间的特殊信息交换中执行。此交换由第1阶段协商的IKE安全关联(SA)完全保护。
- **安全隧道访问管理协议(STAMP)** - VPN客户端连接在IKE过程中与IntraPort交换信息。在最后两个IKE数据包期间，以私有负载发送信息，例如，保存机密（要隧道的IP网络）或是否隧道网际数据包交换(IPX)流量等信息是否正确。这些负载仅发送到兼容的VPN客户端。

## ISAKMP 和 Oakley

互联网安全关联和密钥管理协议(ISAKMP)是一种用于在互联网上（例如，使用IP协议）进行协商的语言。 Oakley是用于进行经过验证的加密密钥材料交换的方法。IKE将两者放在一个包中，这允许在不安全的互联网上建立安全连接。

## STEP 和 STAMP

安全隧道建立协议(STEP)是VPN系统的以前名称。在IKE之前的日子里，STAMP用于协商IPSec连接。早于3.0的VPN客户端版本使用STAMP与IntraPort建立连接。

## 相关信息

- **Cisco VPN 5000 系列集中器终止销售公告**
- **配置路由器到 VPN 5000 系列集中器的 LAN 到 LAN 隧道**
- **Cisco VPN 5000集中器产品支持页**
- **Cisco VPN 5000客户端产品支持页**
- **IPSec协商/IKE协议技术支持**
- **技术支持和文档 - Cisco Systems**