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

Internet Key Exchange (IKE)是用于的标准方法安排安全，已验证通信。设置IPSec隧道的Cisco VPN 5000集中器用途IKE。这些IPSec隧道是此产品的骨干网。

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处理这些任务：

- 验证
- 会话协商
- 密钥交换
- IPSec 隧道协商和配置

验证

验证是IKE完成的最重要的任务，并且是最复杂的。每当您协商某事，知道与是重要的谁您协商。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使用一散列方法保证拥有同一密钥仅的人能发送IKE数据包。
- **数字签字标准(DSS)或Rivest，非对称加密算法(RSA)数字签名**- IKE使用公共密钥数字签名加密算法验证每个当事人是谁他们声称是。
- **RSA加密**- IKE使用两个方法之一加密足够协商保证与正确专用密钥的仅一个当事人能继续协商。

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）。这些项目协商：

- **认证方法**-这是在本文的Authentication部分列出的其中一个方法。
- **密钥交换算法**-这是安全地交换加密密钥的一个数学技术在公共媒体(Diffie-Hellman)。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使用经过协商的密钥交换方法(请参阅本文的Session Negotiation部分)创建足够的位加密的发报材料获取将来处理。此方法保证每IKE会话保护与新，安全套密钥。

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 Policy部分**配置通过Protection关键字。此关键字是有三个片段的标签：验证算法、加密算法和密钥交换算法。片段由下划线分离。标签MD5_DES_G1含义IKE数据包验证的使用MD5， IKE数据包加密的使用DES和密钥交换的使用Diffie-Hellman group1。欲知更多信息，参考配置IPSec隧道安全的IKE策略。

IPSec 隧道协商和配置

在IKE完成协商交换的信息(第一阶段)后一个安全的方法， IKE用于协商IPSec隧道。这使用IKE相位两是实现的。在此交换， IKE创建IPSec隧道的新的密码资料能使用(使用IKE第一阶段密钥作为一个

基础或由执行新密钥交换)。其间还协商此通道的加密算法和认证算法。

使用VPN客户端通道的VPN组(以前安全隧道建立协议(STEP)客户端)部分和LAN-to-LAN隧道的，Tunnel Partner部分IPSec隧道配置。**VPN用户**部分是每个用户的认证方法存储的地方。这些部分在配置描述IPSec隧道安全的IKE策略。

VPN 5000集中器IKE扩展

- **RADIUS** - IKE没有RADIUS验证的支持。RADIUS验证在从VPN客户端的第一IKE数据包以后发生的特殊信息交换进行。如果密码认证协议要求，特殊RADIUS验证机密要求。欲知更多信息，参考NoCHAP和PAPAuthSecret的文档在配置IKE策略IPSec隧道安全的。RADIUS验证验证并且加密。PAP交换由PAPAuthSecret保护。然而，只有整个Intraport的一这样机密，因此保护是一样弱象其中任一共享的密码。
- **SecurID** - IKE当前没有SecurID验证的支持。SecurID验证在一个特殊信息性交换介于中间的第一阶段和相位两进行。此交换由在第一阶段协商的IKE安全关联(SA)充分地保护。
- **安全隧道访问管理协议(STAMP)** - VPN客户端连接与Intraport的交换信息在IKE进程中。信息例如，如果是所有权利保存秘密，在最后两IKE数据包期间，建立隧道的IP网络，或者以隧道传输互联网分组交换流量，是否在私有有效载荷发送。这些有效载荷只发送给兼容的VPN客户端。

ISAKMP 和 Oakley

互联网安全协会和密钥管理协议(ISAKMP)是用于的语言进行在互联网间的协商(例如，使用IP协议)。Oakley是进行的加密密钥材料已验证交换一个方法。IKE汇集两个到一个包，允许在不安全的互联网间将设置的安全连接。

STEP 和 STAMP

安全隧道建立协议(STEP)是VPN系统的上一个名称。在IKE前天， STAMP用于协商IPSec连接。VPN客户端版本早于3.0使用STAMP建立与Intraport的连接。

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 Client产品支持页
- IPSec协商/IKE协议技术支持
- 技术支持和文档 - Cisco Systems