Cisco VPN 集中器、Cisco IOS 和 PIX 设备之间 LAN 到 LAN 配置的重新协商

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[网络图](#)
[规则](#)
[测试方案](#)
[测试结果](#)
[相关信息](#)

简介

本文档报告不同Cisco VPN产品之间在不同场景(如VPN设备重启、密钥重新生成和IPSec安全关联(SA)手动终止)下IP安全(IPSec)LAN到LAN隧道重新协商的实验测试结果。

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：

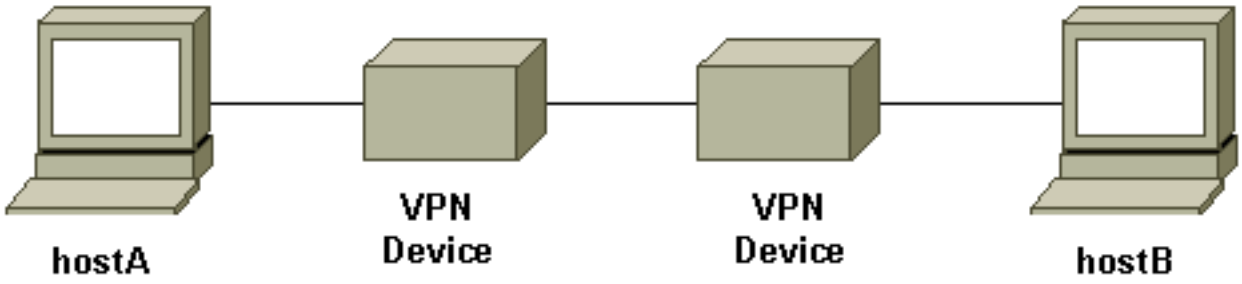
- 思科IOS®软件版本12.1(5)T8
- 思科PIX软件版本6.0(1)
- 思科VPN 3000集中器软件版本3.0(3)A
- Cisco VPN 5000 集中器软件版本 5.2(21)

本测试中使用的IP流量是主机A和主机B之间的双向互联网控制消息协议(ICMP)数据包。

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。

网络图

这是试验台的概念图。



VPN设备代表Cisco IOS路由器、Cisco Secure PIX防火墙、Cisco VPN 3000集中器或Cisco VPN 5000集中器。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

测试方案

测试了三种常见场景。以下是测试场景的简要定义：

- **手动终止IPSec SA** — 用户登录VPN设备并使用命令行界面(CLI)或图形用户界面(GUI)手动清除IPSec SA。
- **Rekey** — 当定义的生命期到期时，正常IPSec阶段I和阶段II重新生成密钥。在本测试中，两个VPN终端设备配置了相同的阶段I和阶段II寿命。
- **VPN device reboot** - VPN隧道终止点的任一端已重新启动以模拟服务中断。

注意：对于使用VPN 5000集中器的LAN到LAN隧道，使用MAIN模式和隧道响应器配置集中器。

测试结果

设置	手动终止IPSec SA	重新生成密钥	VPN设备重新启动
IOS到PIX	• 在两端清除第I阶段或第II阶段SA后重新建立隧道 • 测试流量工作	• 测试流量在第I阶段或第II阶段重新生成密钥后仍然有效	• 在两台设备上启用IKE保持连接后，隧道将重新建立 • 在隧道恢复后测试流量[1]工作
IOS到VPN3000	• 在两端清除第I阶段或第II阶段SA后重新建立隧道 • 测试流量工作	• 测试流量在第I阶段或第II阶段重新生成密钥后仍然有效	• 在两台设备上启用IKE保持连接后，隧道将重新建立 • 在隧道恢复后测试流量[1]工作
IOS到	• 在IOS上：在清除第II阶段SA后	• 在第II阶段重新生成密钥后	• 在重新启动任一VPN设备（具有双向测

VPN 5000	，测试流量仍然有效清除阶段I SA时，VPN隧道关闭测试流量停止工作 • 在VPN 5000上：手动清除SA后，隧道无法恢复必须清除IOS上的第I阶段和第II阶段SA，才能重新建立隧道	，测试流量仍然有效 • I阶段重新生成密钥，使隧道关闭 • 测试流量停止工作 • 必须手动清除SA才能恢复隧道	试流量）后，隧道无法恢复 • 测试流量停止工作 • 必须手动清除未重新启动的设备上的SA，才能恢复隧道
PIX到VPN 3000	• 在两端清除第I阶段或第II阶段SA后重新建立隧道 • 测试流量工作	• 测试流量在第I阶段或第II阶段重新生成密钥后仍然有效	• 在隧道恢复后测试流量[1]工作 • 使用失效对等体检测(DPD)[2]（默认启用），隧道已重新建立
PIX到VPN 5000	• 在PIX上：在清除第II阶段SA后，测试流量仍然有效清除阶段I SA时VPN隧道关闭测试流量停止工作 • 在VPN 5000上：手动清除SA后，隧道无法恢复必须清除PIX上的第I阶段和第II SA阶段，才能重新建立隧道	• 在第II阶段重新生成密钥后，测试流量仍然有效 • I阶段重新生成密钥，使隧道关闭 • 测试流量停止工作 • 必须手动清除SA才能恢复隧道	• 在重新启动任一VPN设备（具有双向测试流量）后，隧道无法恢复 • 测试流量停止工作 • 必须手动清除未重新启动的设备上的SA，才能恢复隧道
VPN	• 在VPN 3000上：手动清除会话	• 测试流量在第I阶段或第II阶段	• 重新启动任一VPN设备（具有双向测试流

3000到VPN5000	后，隧道将恢复流量仍然有效 • 在VPN 5000上： 手动清除隧道后，隧道无法恢复测试流量停止工作必须清除VPN 3000上的SA才能重新建立隧道	重新生成密钥后仍然有效	量）后，隧道无法恢复 • 测试流量停止工作 • 必须手动清除未重新启动的设备上的SA，才能恢复隧道

[1]如上所述，使用的测试流量是主机A和主机B之间的双向ICMP数据包。在VPN设备重启测试中，还测试单向流量以模拟最坏情况（其中流量仅来自VPN设备后面的主机，而不是重新启动到VPN设备的主机）。 从表中可以看到，使用IKE保活或DPD协议时，VPN隧道可以从最坏情况下恢复。

[2] DPD是Unity协议的一部分。目前，此功能仅在软件版本为3.0及更高版本的Cisco VPN 3000集中器和软件版本为6.0(1)及更高版本的PIX防火墙上可用。

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 5000 集中器支持页
- PIX 支持页
- IPSec 支持页面
- 技术支持和文档 - Cisco Systems