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

本文在各种情况下报告IP安全区别Cisco VPN产品之间的LAN-to-LAN隧道重新协商实验室测试结果，例如VPN设备重新启动，重新生成密钥和手工终止IPSec安全关联(SAS)。

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：

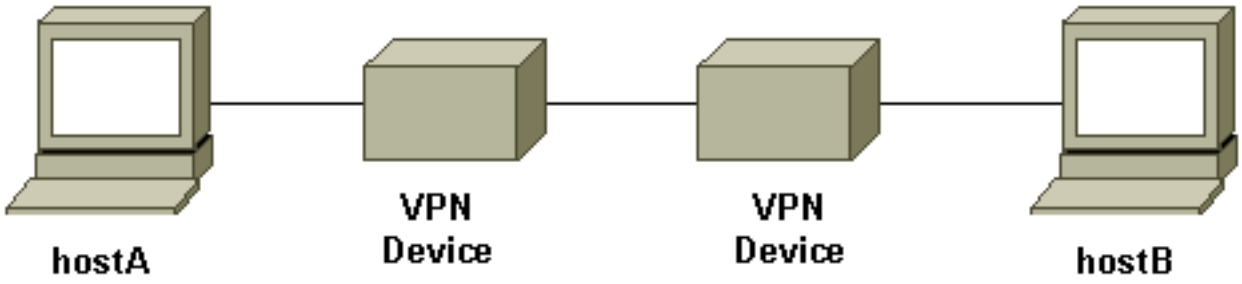
- Cisco IOS软件版本12.1(5)T8
- Cisco PIX软件版本6.0(1)
- Cisco VPN 3000集中器软件版本3.0(3)A
- Cisco VPN 5000集中器软件版本5.2(21)

用于此测验的IP数据流是在玉簪属植物和hostB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

这是测试平台的概念图。



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

三常见情况测试了。下列是测试方案的一个简要定义：

- **IPSec SAS手工终止**—使用命令行界面(CLI)或图形用户界面(GUI)，用户注册到VPN设备和手工清除IPSec SAS。
- **重新生成密钥**—，当定义的寿命超时，正常IPSec阶段我和第II阶段重新生成密钥。在此测验中，两VPN终端设备有同一个相位配置的我和第II阶段寿命。
- **VPN设备重新启动**— VPN隧道终止点的任一个末端重新启动模拟服务中断。

注意： 使用主模式和通道响应方，对于VPN 5000集中器使用的LAN-to-LAN隧道，集中器配置。

测试结果

设置	IPSec SAS的手工终止	重新生成密钥	VPN设备重新启动
对PIX的IOS	• 在相位之后被重建的通道在任何一方清除我或SA第II阶段 • 测试流量工作	• 在相位我或第II阶段重新生成密钥后，测试流量仍然运作	• 当IKE Keepalive启用在两个设备，被重建的通道 • 在被恢复的通道以后的测试流量[1]工作
对VPN3000的IOS	• 在相位之后被重建的通道在任何一方清除我或SA第II阶段 • 测试流量	• 在相位我或第II阶段重新生成密钥后，测试流量仍然运作	• 当IKE Keepalive启用在两个设备，被重建的通道 • 在被恢复的通道以后的测试流量[1]工

	工作		作
对VPN5000的IOS	• 在IOS ：在清除后，测试流量仍然运作SA第II阶段当相位SA清除时，VPN通道去在下我测试流量终止工作 • 在VPN5000 ：通道不能在手工清除SA以后恢复必须清除在IOS的相位我和SA第II阶段重建通道	• 在第II阶段重新生成密钥后，测试流量仍然运作 • 我重新生成密钥减少通道的相位 • 测试流量终止工作 • 必须手工带来通道上一步的清楚SAS	• 通道不能在重新启动以后恢复任一个VPN设备(与双向测试数据流) • 测试流量终止工作 • 手工必须清楚在未重新启动带来通道上一步的设备的SA
对VPN3000的PIX	• 在相位之后被重建的通道在任何一方清除我或SA第II阶段 • 测试流量工作	• 在相位我或第II阶段重新生成密钥后，测试流量仍然运作	• 在被恢复的通道以后的测试流量[1]工作 • 当对端死机检测(DPD) [2] (默认情况下启用)，被重建的通道
对VPN5000的PIX	• 在PIX ：在清除后，测试流量仍然运作SA第II阶段当相位SA清除时，VPN通道去在下我测试流量终止工作 • 在VPN5000	• 在第II阶段重新生成密钥后，测试流量仍然运作 • 我重新生成密钥减少通道的相位 • 测试流量终止工作 • 必须手工带来通道	• 通道不能在重新启动以后恢复任一个VPN设备(与双向测试数据流) • 测试流量终止工作 • 手工必须清楚在未重新启动带来通道上一步的设备的SA

	：在手工清除SA后，通道不能恢复必须清除在PIX的相位我和SA第II阶段重建通道	上一步的清楚SAS	
对VPN5000的VPN3000	• 在VPN3000：通道在清楚以后手工被恢复会话仍然流量工作 • 在VPN5000：通道不能在清楚以后手工恢复通道测试流量终止工作必须清除在VPN3000的SA重建通道	• 在相位我或第II阶段重新生成密钥后，测试流量仍然运作	• 通道不能在任一个VPN设备以后重新启动恢复(与双向测试数据流) • 测试流量终止工作 • 手工必须清楚在未重新启动带来通道上一步的设备的SA

[1]如上所述，使用的测试流量是在玉簪属植物和hostB之间的双向ICMP数据包。在VPN设备重新启动测验中，单向数据流也测试模拟最坏的情况(其中流量仅是从主机在没有重新启动到VPN设备重新启动)的VPN设备背后。象能看到从表，与IKE Keepalive或在DPD协议， VPN通道可以从最坏的情况恢复。

[2] DPD是Unity协议的一部分。目前此功能只是可用的在Cisco VPN 3000集中器有软件版本的3.0和在和在与软件版本6.0(1)的以上PIX防火墙上。

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