在Cisco VPN集中器、Cisco IOS和PIX裝置之間重新協商LAN到LAN配置

目錄

簡介

本檔案將報告各種情況下(例如VPN裝置重新啟動、重新設定金鑰和手動終止IPSec安全關聯(SA))之間不同Cisco VPN產品之間的IP安全(IPSec)LAN到LAN通道重新交涉的實驗室測試結果。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

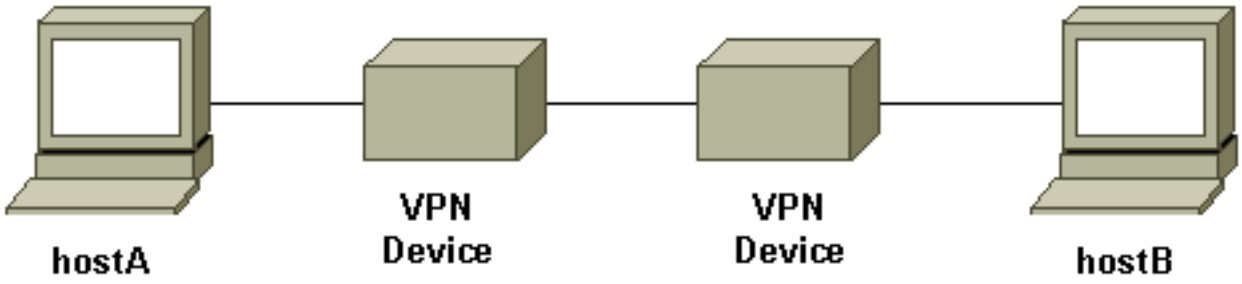
- Cisco IOS®軟體版本12.1(5)T8
- Cisco PIX軟體版本6.0(1)
- Cisco VPN 3000 Concentrator軟體版本3.0(3)A
- Cisco VPN 5000 Concentrator軟體版本5.2(21)

此測試中使用的IP流量是主機A和主機B之間的雙向網際網路控制訊息通訊協定(ICMP)封包。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

這是測試台的概念圖。



VPN裝置代表Cisco IOS路由器、Cisco Secure PIX防火牆、Cisco VPN 3000集中器或Cisco VPN 5000集中器。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

測試方案

測試了三種常見方案。以下是測試方案的簡要定義：

- **手動終止IPSec SA** — 使用者登入到VPN裝置並使用命令列介面(CLI)或圖形使用者介面(GUI)手動清除IPSec SA。
- **Rekey** — 當定義的生存期到期時，正常IPSec階段I和階段II重新生成金鑰。在本測試中，兩個VPN終端裝置配置了相同的I階段和II階段壽命。
- **VPN裝置重新**引導 — 已重新引導VPN隧道的任一端終止點以模擬服務中斷。

注意：對於使用VPN 5000集中器的LAN到LAN隧道，使用主模式和隧道響應器配置集中器。

測試結果

設定	手動終止IPSec SA	重新生成金鑰	VPN裝置重新啟動
IOS到PIX	• 在任一端清除階段I或階段II SA後重新建立隧道 • 測試流量工作	• 在第一階段或第二階段重新生成金鑰後，測試流量仍然可以正常工作	• 在兩台裝置上啟用IKE保持連線後，隧道重新建立 • 測試流量1在通道恢復後工作
IOS到VPN3000	• 在任一端清除階段I或階段II SA後重新建立隧道 • 測試流量工作	• 在第一階段或第二階段重新生成金鑰後，測試流量仍然可以正常工作	• 在兩台裝置上啟用IKE保持連線後，隧道重新建立 • 測試流量1在通道恢復後工作
IO	• 在IOS上	• 第II階段重新生	• 重新引導任

S到VPN5000	：在第II階段SA清除後，測試流量仍可工作階段ISA清除時，VPN隧道關閉測試流量停止工作 • 在VPN 5000上：手動清除SA後，通道無法恢復必須清除IOS上的I階段和II階段SA才能重新建立隧道	成金鑰後，測試流量仍可正常工作 • 第一階段重新生成金鑰使隧道關閉 • 測試流量停止工作 • 必須手動清除SA才能恢復隧道	一VPN裝置（具有雙向測試流量）後，通道無法恢復 • 測試流量停止工作 • 必須手動清除未重新啟動的裝置上的SA才能恢復隧道
PIX到VPN3000	• 在任一端清除階段I或階段IISA後重新建立隧道 • 測試流量工作	• 在第一階段或第二階段重新生成金鑰後，測試流量仍然可以正常工作	• 測試流量1在通道恢復後工作 • 使用失效對等體檢測(DPD)[2]（預設情況下啟用），重新建立通道
PIX到VPN5000	• 在PIX上：在第II階段SA清除後，測試流量仍可工作階段ISA清除時，VPN隧道關閉測試流量停止工作 • 在VPN 5000上：手動清除	• 第II階段重新生成金鑰後，測試流量仍可正常工作 • 第一階段重新生成金鑰使隧道關閉 • 測試流量停止工作 • 必須手動清除SA才能恢復隧道	• 重新引導任一VPN裝置（具有雙向測試流量）後，通道無法恢復 • 測試流量停止工作 • 必須手動清除未重新啟動的裝置上的SA才能恢復隧道

	SA後，通道無法恢復必須清除PIX上的I階段和II階段SA才能重建隧道		
VPN 3000到VPN 5000	• 在VPN 3000上：手動清除作業階段後通道即可復原流量仍然有效 • 在VPN 5000上：手動清除通道後通道無法復原測試流量停止工作必須清除VPN 3000上的SA才能重建隧道	• 在第一階段或第二階段重新生成金鑰後，測試流量仍然可以正常工作	• 重新引導任一VPN裝置後，通道無法恢復（使用雙向測試流量） • 測試流量停止工作 • 必須手動清除未重新啟動的裝置上的SA才能恢復隧道

[1] 如上所述，使用的測試流量是主機A和主機B之間的雙向ICMP封包。在VPN裝置重新開機測試中，也會測試單向流量來模擬最糟糕的情況（其中流量僅來自未重新開機的VPN裝置之後的主機重新開機至重新開機的VPN裝置）。 從表中可以看到，使用IKE keepalive或使用DPD協定時，VPN隧道可以從最壞的情況中恢復。

[2] DPD是Unity協定的一部分。目前，此功能僅在軟體版本為3.0及更高版本的Cisco VPN 3000 Concentrator和軟體版本為6.0(1)及更高版本的PIX防火牆上可用。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- Cisco VPN 5000集中器支援頁
- PIX支援頁
- IPSec支援頁面
- 技術支援與文件 - Cisco Systems