

Renegotiating LAN-to-LAN Configurations Between Cisco VPN Concentrators, Cisco IOS, and PIX Devices

Document ID: 14111

Contents

Introduction

Prerequisites

Requirements

Components Used

Network Diagram

Conventions

Test Scenarios

Test Results

Related Information

Introduction

This document reports the lab test results of IP Security (IPSec) LAN-to-LAN tunnel renegotiation between different Cisco VPN products in various scenarios, such as VPN device reboot, rekey, and the manual termination of IPSec security associations (SAs).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

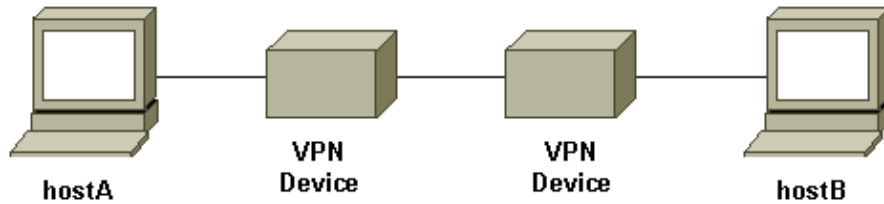
- Cisco IOS® Software Release 12.1(5)T8
- Cisco PIX Software Release 6.0(1)
- Cisco VPN 3000 Concentrator software version 3.0(3)A
- Cisco VPN 5000 Concentrator software version 5.2(21)

The IP traffic used in this test is bi-directional Internet Control Message Protocol (ICMP) packets between hostA and hostB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This is a concept diagram of the test bed.



VPN devices represent a Cisco IOS router, a Cisco Secure PIX Firewall, a Cisco VPN 3000 Concentrator or a Cisco VPN 5000 Concentrator.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Test Scenarios

Three common scenarios were tested. The following is a brief definition of the test scenarios:

- **Manual termination of IPSec SAs** User logs on to the VPN devices and manually clears the IPSec SAs using the command line interface (CLI) or the graphical user interface (GUI).
- **Rekey** Normal IPSec phase I and phase II rekey when defined lifetime expires. In this test, the two VPN termination devices have the same phase I and phase II lifetime configured.
- **VPN device reboot** Either end of the VPN tunnel termination points was rebooted to simulate service outage.

Note: For LAN-to-LAN tunnels where the VPN 5000 Concentrator is used, the concentrator is configured using the MAIN mode and tunnel responder.

Test Results

Setup	Manually Termination of IPSec SAs	Rekey	VPN Device Reboot
IOS to PIX	<ul style="list-style-type: none"> • Tunnel reestablished after phase I or phase II SA is cleared on either side • Test traffic works 	<ul style="list-style-type: none"> • Test traffic still works after phase I or 	<ul style="list-style-type: none"> • With IKE keepalive enabled on both devices, tunnel reestablished
IOS to VPN 3000	<ul style="list-style-type: none"> • Tunnel reestablished after phase I or 	<ul style="list-style-type: none"> • Test traffic still works 	<ul style="list-style-type: none"> • Test traffic works after tunnel recovered • With IKE keepalive enabled on both

	<p>phase II SA is cleared on either side</p> <ul style="list-style-type: none"> • Test traffic works 	<p>after phase I or phase II rekey</p>	<p>devices, tunnel reestablished</p> <ul style="list-style-type: none"> • Test traffic¹ works after tunnel recovered
<p>IOS to VPN 5000</p>	<ul style="list-style-type: none"> • On IOS: <ul style="list-style-type: none"> ◆ Test traffic still works after phase II SA is cleared ◆ VPN tunnel goes down when phase I SA is cleared ◆ Test traffic stops working • On VPN 5000: <ul style="list-style-type: none"> ◆ Tunnel fails to recover after manually clearing the SA ◆ Must clear both phase I and phase II 	<ul style="list-style-type: none"> • Test traffic still works after phase II rekey • Phase I rekey brought down the tunnel • Test traffic stops working • Must manually clear SAs to bring the tunnel back 	<ul style="list-style-type: none"> • Tunnel fails to recover after reboot either VPN device (with bi-directional test traffic) • Test traffic stops working • Must manually clear the SA on the device which was not rebooted to bring the tunnel back

		SA on IOS to reestablish tunnel	
PIX to VPN 3000	<ul style="list-style-type: none"> • Tunnel reestablished after phase I or phase II SA is cleared on either side • Test traffic works 	<ul style="list-style-type: none"> • Test traffic still works after phase I or phase II 	<ul style="list-style-type: none"> • Test traffic¹ works after tunnel recovered • With Dead Peer Detection (DPD)² (enabled by default),
PIX to VPN 5000	<ul style="list-style-type: none"> • On PIX: <ul style="list-style-type: none"> ◆ Test traffic still works after phase II SA is cleared ◆ VPN tunnel went down when phase I SA is cleared ◆ Test traffic stops working • On VPN 5000: <ul style="list-style-type: none"> ◆ Tunnel fails to recover after manually 	<ul style="list-style-type: none"> • Test traffic still works after phase II rekey • Phase I rekey brought down the tunnel • Test traffic stops working • Must manually clear SAs to bring the tunnel back 	<ul style="list-style-type: none"> • Tunnel fails to reestablish after reboot either VPN device (with bi-directional test traffic) • Test traffic stops working • Must manually clear the SA on the device which was not rebooted to bring the tunnel back

		<p>clears SA</p> <ul style="list-style-type: none"> ◆ Must clear both phase I and phase II SA on PIX to reestablish tunnel 	
VPN 3000 to VPN 5000	<ul style="list-style-type: none"> • On VPN 3000: <ul style="list-style-type: none"> ◆ Tunnel is recovered after manually clear the session ◆ Traffic still works • On VPN 5000: <ul style="list-style-type: none"> ◆ Tunnel fails to recover after manually clear the tunnel ◆ Test traffic stops working ◆ Must clear SA on VPN 3000 to reestablish 	<ul style="list-style-type: none"> • Test traffic still works after either phase I or phase II rekey 	<ul style="list-style-type: none"> • Tunnel fails to recover after reboot of either VPN device (with bi-directional test traffic) • Test traffic stops working • Must manually clear the SA on the device which was not rebooted to bring the tunnel back

	tunnel	
--	--------	--

¹ As described above, the test traffic used is bi-directional ICMP packets between hostA and hostB. In the VPN device reboot test, unidirectional traffic is also tested to simulate the worst case scenario (where traffic is only from the host behind the VPN device which is not rebooted to the VPN device which is rebooted). As can be seen from the table, with IKE keepalive or with DPD protocol, the VPN tunnel can be recovered from the worst case scenario.

² DPD is part of the Unity protocol. Currently this feature is only available on the Cisco VPN 3000 Concentrator with software version 3.0 and above and on the PIX Firewall with software version 6.0(1) and above.

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 5000 Concentrator Support Page](#)
- [PIX Support Page](#)
- [IPSec Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 02, 2006

Document ID: 14111
