Cisco VPN Concentrator、Cisco IOS および PIXデバイス間のLAN-to-LAN構成の再ネゴシエーション

内容

概要

このドキュメントでは、異なる Cisco VPN 製品の間における IP Security (IPSec) LAN-to-LAN トンネル再ネゴシエーションに関する、VPN デバイスのリブート、キー再生成、および IPSec セキュリティ アソシエーション（SA）の手動での終了など、さまざまなシナリオでのラボ試験結果を報告します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS®ソフトウェアリリース12.1(5)T8
- Cisco PIXソフトウェアリリース6.0(1)
- Cisco VPN 3000コンセントレータソフトウェアバージョン3.0(3)A
- Cisco VPN 5000 コンセントレータ ソフトウェア バージョン 5.2(21)

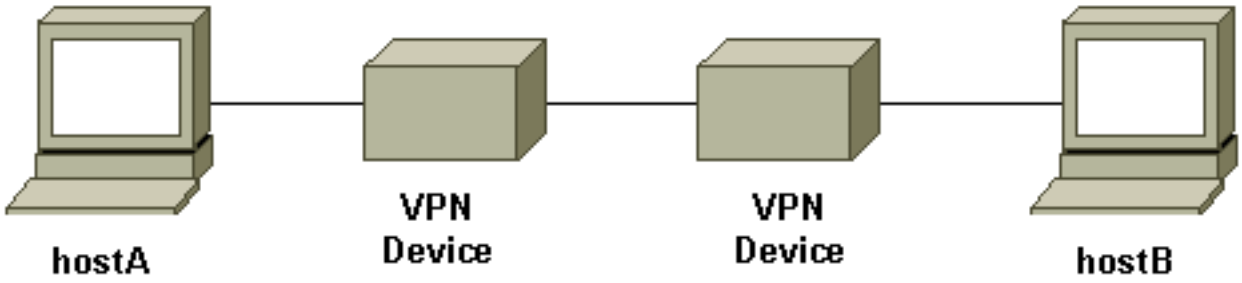
このテストで使用されるIPトラフィックは、ホストAとホストBの間の双方向インターネット制御メッセージプロトコル(ICMP)パケットです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

これは、テストベッドの概念図です。



VPNデバイスは、Cisco IOSルータ、Cisco Secure PIX Firewall、Cisco VPN 3000コンセントレータ、またはCisco VPN 5000コンセントレータを表します。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

テストシナリオ

3つの一般的なシナリオがテストされました。次に、テストシナリオの簡単な定義を示します。

- **IPSec SAの手動終了**：ユーザはVPNデバイスにログオンし、コマンドラインインターフェイス(CLI)またはグラフィカルユーザインターフェイス(GUI)を使用してIPSec SAを手動でクリアします。
- **キー再生成**：定義されたライフタイムが期限切れになると、通常のIPSecフェーズIおよびフェーズIIキー再生成が行われます。このテストでは、2台のVPN終端デバイスに同じフェーズIおよびフェーズIIライフタイムが設定されています。
- **VPNデバイスのリブート**：サービス停止をシミュレートするために、VPNトンネルの終端のいずれかの端がリブートされました。

注：VPN 5000コンセントレータを使用するLAN-to-LANトンネルの場合、コンセントレータはMAINモードとトンネルレスポンダを使用して設定されます。

テスト結果

セットアップ	IPSec SAの手動終了	キー再生成	VPNデバイスのリブート
IO	• フェーズIまた	• テストトラフィックは、フ	• 両方のデバイスでIKEキープア

SからPIX	はフェーズII SAが両側でクリアされた後、トンネルが再確立される • テストトラフィックが動作する	ェーズIまたはフェーズIIのキー再生成の後も引き続き動作します	ライブが有効になっている場合、トンネルが再確立されます • テストトラフィック[1]は、トンネルが回復した後に動作します
IOSからVPN3000	• フェーズIまたはフェーズII SAが両側でクリアされた後、トンネルが再確立される • テストトラフィックが動作する	• テストトラフィックは、フェーズIまたはフェーズIIのキー再生成の後も引き続き動作します	• 両方のデバイスでIKEキープアライブが有効になっている場合、トンネルが再確立されます • テストトラフィック[1]は、トンネルが回復した後に動作します
IOSからVPN5000	• IOS: テストトラフィックは、フェーズII SAがクリアされた後も引き続き動作しますフェーズI SAがク	• テストトラフィックは、フェーズIIのキー再生成後も引き続き動作します • フェーズ1のキー再生成がトンネルをダウンしました • テストトラフィックが動作しなくなる • トンネルを復旧するには、	• いずれかのVPNデバイス（双方向テストトラフィック）をリブートした後、トンネルが回復しない • テストトラフィックが動作しなくなる • トンネルを復旧するために、リブートされなかったデバイスのSAを手動でク

	リアされると、VPNトンネルがダウンしますテストトラフィックが動作しなくなる • VPN 5000: SAを手動でクリアした後、トンネルが回復しないトンネルを再確立するには、IOSのフェーズIとフェーズII SAの両方をクリアする必要があります	SAを手動でクリアする必要があります	リアする必要があります
PIXからVPN3000	• フェーズIまたはフェーズII SAが両側でクリアされた後、トンネルが再確立	• テストトラフィックは、フェーズIまたはフェーズIIのキー再生成の後も引き続き動作します	• テストトラフィック[1]は、トンネルが回復した後に動作します • Dead Peer Detection(DPD)[2]（デフォルトで有効）では、トンネルが再確立されます

	されるテストトラフィックが動作する		
PIXからVPN5000	• PIX: テストトラフィックは、フェーズII SAがクリアされた後も引き続き動作しますフェーズI SAがクリアされると、VPNトンネルがダウンしたテストトラフィックが動作しなくなる • VPN 5000: SAを手動でクリアした後、トンネルが回復しないトンネルを再確立するには、	• テストトラフィックは、フェーズIIのキー再生成後も引き続き動作します • フェーズ1のキー再生成がトンネルをダウンしました • テストトラフィックが動作しなくなる • トンネルを復旧するには、SAを手動でクリアする必要があります	• いずれかのVPNデバイス（双方向テストトラフィック）をリブートした後、トンネルが回復しない • テストトラフィックが動作しなくなる • トンネルを復旧するために、リブートされなかったデバイスのSAを手動でクリアする必要があります

	PIXのフェーズIとフェーズII SAの両方をクリアする必要があります		
VPN3000からVPN5000	• VPN 3000: トンネルは、セッションを手動でクリアした後に回復されますトラフィックはまだ動作している • VPN 5000: トンネルを手動でクリアした後、トンネルが回復しないテストトラフィックが動作しなくなるトンネルを再確立するには	• テストトラフィックは、フェーズIまたはフェーズIIキー再生成の後も引き続き動作します	• いずれかのVPNデバイスのリブート後にトンネルが回復しない（双方向テストトラフィックがある） • テストトラフィックが動作しなくなる • トンネルを復旧するために、リブートされなかったデバイスのSAを手動でクリアする必要があります

	、VPN 3000のSAをクリアする必要があります		

[1]上記のように、使用されるテストトラフィックは、hostAとhostBの間の双方向ICMPパケットです。VPNデバイスのリブートテストでは、単方向トラフィックもテストされ、最悪のケースのシナリオをシミュレートします（トラフィックはVPNデバイスの背後にあるホストからリブートされたVPNデバイスに対してのみ行われます）。 表から分かるように、IKEキープアライブまたはDPDプロトコルを使用して、VPNトンネルを最悪のシナリオから回復できます。

[2] DPDはUnityプロトコルの一部です。現在、この機能は、ソフトウェアバージョン3.0以降が稼働するCisco VPN 3000コンセントレータと、ソフトウェアバージョン6.0(1)以降が稼働するPIX Firewallでのみ使用できます。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 5000 コンセントレータに関するサポートページ
- PIX に関するサポート ページ
- IPSec に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems