目次

概要

このドキュメントでは、VPN ゲートウェイ デバイスが IKE ネゴシエーションで常に応答側として機能するように設定する方法について説明します。 デバイスは、そのピアによって開始されたすべての暗号ネゴシエーションに応答します。

前提条件

要件

このドキュメントに関する固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くものです。

- Cisco IOS® ソフトウェアリリース 12.4(24)T およびそれ以降が付いている Ciscoルータ
- バージョン 7.0 以降が稼働する Cisco 適応型セキュリティ アプライアンス (ASA)

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- ソフトウェア バージョン 7.0 以降が稼働する Cisco PIX Firewall

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。

背景説明

暗号ネゴシエーションでは、発信側と応答側という 2 つの参加者がそれぞれの役割を演じます。発信側は、暗号化、認証アルゴリズム、キー再生成オプション、ライフタイム値などに関するさまざまなパラメータが含まれている暗号提案を応答側に送信します。 応答側が正しい提案を選択すると、暗号セッションが確立します。 エンド デバイスが果たした役割は、次のコマンド出力で表示できます。

```
Router#show crypto isakmp sa1    IKE Peer: XX.XX.XX.XX     Type     : L2L              Role     :
initiator     Rekey    : no               State    : MM_ACTIVEASA(config)#show crypto isakmp sa
detailIKE Peer     Type  Dir    Rky    State       Encrypt     Hash  Auth       Lifetime1
209.165.200.225 User  Resp  No   AM_Active    3des       SHA   preshrd     86400
```

IKE 応答側専用モード機能の利点

（対象トラフィックがあるかないかにかかわらず）同時双方向 IKE ネゴシエーションを可能にするバーチャル プライベート ネットワーク（VPN）の出現以来、重複する IKE SA からのデータの処理および回復に伴う問題が発生してきました。 プロトコルとしての IKE には、IKE ネゴシエーションどうしを比較して、対象となる 2 つのピア間に既存のまたは処理中のネゴシエーションがすでに存在しているかどうかを判断する機能はありません。 このような重複するネゴシエーションは、リソースの観点から言っても、ルータ管理者に混乱をもたらすという観点から言っても、コストが高くつく可能性があります。 デバイスを応答側専用デバイスとして設定すると、IKE メイン、アグレッシブ、またはクイック モード（IKE および IPSec SA の確立用）が開始されず、IKE および IPSec SA のキー再生成も行われません。 そのため、SA が重複する可能性が低くなります。

この機能のその他の利点は、ロードバランス シナリオだけにおける一方向のネゴシエーション接続の制御されたサポートが可能になることです。 サーバやハブによってクライアントまたはスポークに対する VPN 接続を開始することは推奨できません。これらのデバイスはすべて、ロードバランサを介してアドバタイズされる単一方向 IP アドレスによってアクセスされるからです。ハブが接続を開始する場合、それらのハブでは、同処理に個々の IP アドレスが使用されます。その結果、ロード バランサの利点がなくなります。 ロード バランサの背後にあるハブまたはサーバから送信されるキー再生成要求についても同様です。

暗号ネゴシエーションで応答側専用デバイスとして設定されるルータ

Cisco IOS ソフトウェア リリース 12.4(24)T で、ピアによって開始された IKE ネゴシエーションに常に応答するルータの機能が導入されました。 主な制限は、この機能が IPSec プロファイルでしか設定できず、仮想インターフェイス シナリオにしか関係しないということです。 スタティックまたはダイナミック暗号マップ シナリオはサポートされません。

ルータを応答側専用に設定するには、次の手順を実行します。

```
enable configure terminal crypto ipsec profile <name>    responder-only
```

暗号ネゴシエーションで応答側専用デバイスとして設定される ASA

一般的な IPsec LAN 間接続では、ASA が発信側または応答側として機能できます。 IPsec クライアント/LAN 間接続では、ASA が応答側としてのみ機能します。 ASA は LAN 間 VPN 接続の応答専用デバイスとして設定できます。 ただし、VPN トンネルの反対側に設置するデバイスを次のいずれかにしなければならないという制限があります。

- Cisco ASA 5500 シリーズ アプライアンス
- Cisco VPN 3000 シリーズ コンセントレータ
- 7.0 ソフトウェア以降を実行している Cisco PIX 500 シリーズ ファイアウォール

ASA を応答側専用デバイスに設定するには、次のコマンドを発行します。

hostname(config)# crypto map mymap 10 set connection-type answer-only

注複数の VPN ピアが終端する VPN ゲートウェイ デバイスを応答側専用として設定することをお勧めします。

関連情報

- IKE アグレッシブ モードを開始するルータを使用する Router-to-Router LAN-to-LAN トンネルの設定
- Cisco ASA の設定例とテクニカル ノート
- テクニカルサポートとドキュメント - Cisco Systems