L2L トンネルを介した ASA VPN クライアント接続の設定例

目次

概要

この資料に Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア設定する方法を (ASA) LAN-to-LAN な (L2L) ピアアドレスからの遠隔 VPNクライアント接続を許可するために記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ASA
- リモートアクセス VPN
- LAN-to-LAN な VPN

使用するコンポーネント

この文書に記載されている情報はソフトウェア バージョン 8.4(7) を実行する ASA に Cisco 5520 シリーズ基づいています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

VPN クライアントが L2L トンネルによって接続を確立するように試みるシナリオに出会うためにそれがよくないが管理者はこれらのリソースへのアクセスが必要となるとき特定の特権かアクセス制限をある特定のリモートユーザに割り当て、ソフトウェアクライアントを使用するように指示したいと思うかもしれません。

> **注:** バージョン 8.4(6) または それ 以降へのヘッドエンド ASA のアップグレードが以前はたらく、このシナリオは VPN クライアントあった後、しかしもはや接続を確立できません。

Cisco バグ ID CSCuc75090 は動作変更をもたらしました。 以前はインターネット プロトコル セキュリティ（IPSec）プロキシがクリプト マップ Access Control List （ACL）を一致するときに、Private Internet Exchange （PIX）と、それはリストの下のエントリを更にチェックし続けました。 これは規定 された ピア無しでダイナミック暗号マップが付いている一致が含まれていました。

これはリモート管理者がスタティック L2L が設定されたときにヘッドエンド 管理者が意図しなかったリソースへのアクセス権を得る可能性があるので、脆弱性とみなされました。

ピアなしで既にピアと一致した Map エントリをチェックしたときに暗号マップエントリが付いているマッチを防ぐためにチェックを追加した修正は作成されました。 ただし、この資料で説明されているこれはシナリオに影響を与えました。 具体的には、L2L ピアアドレスから接続するように試みるリモート VPN クライアントはヘッドエンドに接続できません。

設定

ASA を L2L ピアアドレスからの遠隔 VPNクライアント接続を許可するために設定するためにこのセクションを使用して下さい。

新しい動的エントリを追加して下さい

L2L ピアアドレスからの遠隔 VPN 結合を許可するために、同じピアIP アドレスが含まれている新しい動的エントリを追加して下さい。

> **注:** インターネットからのどのクライアントでも同様に接続できるようにまたピアなしで別の動的エントリを残して下さい。

前のダイナミック暗号マップ 運用コンフィギュレーションの例はここにあります:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

新しい動的エントリが設定されているダイナミック暗号マップ 設定はここにあります:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。