# L2L トンネルを介した ASA VPN クライアント接続の設定例

## 内容



## 概要

このドキュメントでは、Lan-to-Lan(L2L)ピアアドレスからのリモートVPNクライアント接続を許可するようにCisco適応型セキュリティアプライアンス(ASA)を設定する方法について説明します。

## 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 VPN

### 使用するコンポーネント

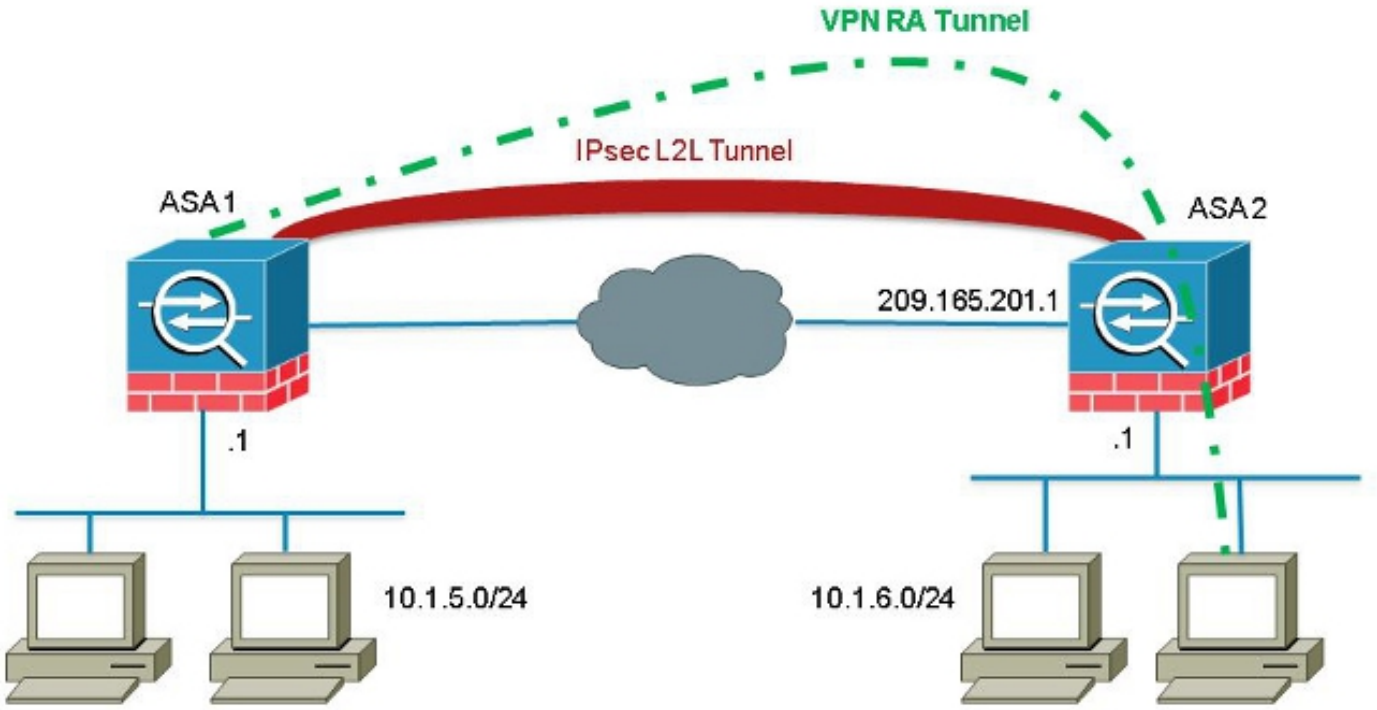
このドキュメントの情報は、ソフトウェアバージョン8.4(7)が稼働するCisco 5520シリーズASAに基づくものです。

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。

# 背景説明

VPNクライアントがL2Lトンネルを介して接続を確立しようとするシナリオは一般的ではありませんが、管理者は、特定のリモートユーザに特定の権限またはアクセス制限を割り当て、これらのリソースへのアクセスが必要な場合にソフトウェアクライアントを使用します。

> **注**：このシナリオは以前は動作していましたが、ヘッドエンドASAをバージョン8.4(6)以降にアップグレードすると、VPNクライアントは接続を確立できなくなります。




Cisco Bug ID CSCuc75090で動作の変更が導入されました。以前は、Private Internet Exchange(PIX)では、Internet Protocol Security(IPSec)プロキシが暗号マップのアクセスコントロールリスト(ACL)と一致しなかった場合、リストの下のエントリをさらにチェックし続けました。この例では、ピアが指定されていないダイナミック暗号マップと一致しています。

これは、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にリモート管理者がアクセスする可能性があるため、脆弱性と見なされていました。

ピアに一致するマップエントリがすでにチェックされている場合に、ピアのないcrypto-mapエントリとの一致を防ぐためにチェックを追加した修正が作成されました。ただし、このドキュメントで説明されているシナリオは、これに該当します。具体的には、L2Lピアアドレスから接続しようとするリモートVPNクライアントは、ヘッドエンドに接続できません。

# 設定

このセクションでは、L2LピアアドレスからのリモートVPNクライアント接続を許可するようにASAを設定します。

### 新しいダイナミックエントリの追加

L2Lピアアドレスからのリモートvpn接続を許可するには、同じピアIPアドレスを含む新しいダイナミックエントリを追加する必要があります。

> **注**：また、インターネット上のクライアントも接続できるように、ピアのない別のダイナミックエントリを残す必要があります。

前のダイナミック暗号マップの動作設定の例を次に示します。

```
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
```

新しいダイナミックエントリが設定されたダイナミック暗号マップの設定を次に示します。

```
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。

# トラブルシュート

現在、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。