2 つの ASA 間の動的なサイト間 IKEv2 VPN トンネルの設定例

目次

概要

1 ASA にダイナミックIPアドレスがあり、他に静的IP アドレスがあるところこの資料に 2 間のサイト間のバージョン 2 （ IKEv2 ） VPN トンネルを Internet Key Exchange （ IKE ）設定する方法を適応型セキュリティ アプライアンス （ ASA ）記述されています （ ASA ）。

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。

- ASA バージョン 5505
- ASA バージョン 9.1(5)

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

この設定が設定することができること 2 つの方法があります:

- DefaultL2LGroup トンネル グループを使って
- ネームド トンネル グループを使って

2 つのシナリオ間の最も大きいコンフィギュレーションの差はリモート ASA によって使用される Internet Security Association and Key Management Protocol（ISAKMP） ID です。 DefaultL2LGroup がスタティック ASA で使用されるとき、ピアの ISAKMP ID はアドレスでなければなりません。 ただしネームド トンネル グループが使用されれば、ピアの ISAKMP ID はこのコマンドを使用して同じでなければなりませんトンネル グループ名前:

```
crypto isakmp identity key-id <tunnel-group_name>
```

スタティック ASA のネームド トンネル グループを事前共有キーが含まれている使用する長所は DefaultL2LGroup が使用されるときこと、リモート ダイナミック ASA の設定同一でなければならないであり、ポリシーのセットアップの多くの細かさを可能にしません。

ネットワーク図

設定

このセクションはによってどのソリューションを使用することにするか各 ASA の設定を説明します。

ソリューション 1 - DefaultL2LGroup の使用

これは 1 ASA がアドレスを動的に取得するとき 2 ASA 間の LAN-to-LAN な（L2L）トンネルを設定する最も簡単な方法です。 DefaultL2L グループは ASA の前もって構成されたトンネル グループであり、明示的に 特定 の トンネル グループを一致するすべての接続はこの接続で落ちます。 ダイナミック ASA が持っていないので定数は特定のトンネル グループの接続を可能にするために admin が Statis ASA を設定できないことを IP アドレスを、それ意味します前もって決定しました。 この場合、DefaultL2L グループはダイナミック 接続を許可するために使用することができます。

> **ヒント**： この方式によって、マイナス面は 1 つの事前共有キーだけトンネル グループ 1人あたりに定義することができ、同位すべてが同じ DefaultL2LGroup トンネル グループに接続するのですべての同位に同じ事前共有キーがあることです。

静的な ASA 設定

```
crypto isakmp identity key-id <tunnel-group_name>
```

Adaptive Security Device Manager （ASDM）で、ここに示されているように DefaultL2LGroup を設定できます:

ダイナミック ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

ASDM で、適切な接続プロファイルを設定するために標準ウィザードを使用できますまたは新しい接続を単に追加し、標準手続 きに従うことができます。

ソリューション 2 -ユーザが定義するトンネル グループを作成して下さい

この方式はより多くの設定を slighly 必要としますが、より多くの細かさを可能にします。 各ピアは自身の別のポリシーおよび事前共有キーがある場合があります。 ここにダイナミック ピアの ISAKMP ID を変更することは重要どんなにでもそれが IP アドレスの代りに名前を使用するように。 これはスタティック ASA が着信 ISAKMP 初期化要求を右のトンネル グループに一致させ、右のポリシーを使用するようにします。

静的な ASA 設定

```
crypto isakmp identity key-id <tunnel-group_name>
```

ASDM で、接続プロファイル名前はデフォルトで IP アドレスです。 従ってそれを作成するとき、スクリーン ショットに示すようにそれに名前をここにつけるためにそれを変更して下さい:

ダイナミック ASA 設定

ダイナミック ASA はここに示されているように 1 コマンドの付加でほとんど設定されて両方のソリューションの同じ方法:

```
crypto isakmp identity key-id DynamicSite2Site1
```

以前に記述されているように、デフォルトで ASA は VPN トンネルが ISAKMP キー ID としてにマッピング される インターフェイスの IP アドレスを使用します。 ただしこの場合、ダイナミック ASA のキー ID はスタティック ASA のトンネル グループの名前と同じです。 従って各ダイナミック ピアで、キー ID は異なって、対応するトンネル グループは右の名前でスタティック ASA で作成する必要があります。

ASDM で、これはこのスクリーン ショットに示すように設定することができます:

確認

このセクションでは、設定が正常に機能していることを確認します。

スタティック ASA

提示暗号 IKEv2 sa det コマンドの結果はここにあります:

```
crypto isakmp identity key-id DynamicSite2Site1
```

show crypto ipsec sa **コマンド**の結果はここにあります:

```
crypto isakmp identity key-id DynamicSite2Site1
```

ダイナミック ASA

提示暗号 IKEv2 sa detail **コマンド**の結果はここにあります:

```
crypto isakmp identity key-id DynamicSite2Site1
```

show crypto ipsec sa **コマンド**の結果はここにあります:

```
crypto isakmp identity key-id DynamicSite2Site1
```

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **deb 暗号 IKEv2 パケット**
- **内部 deb 暗号 IKEv2**