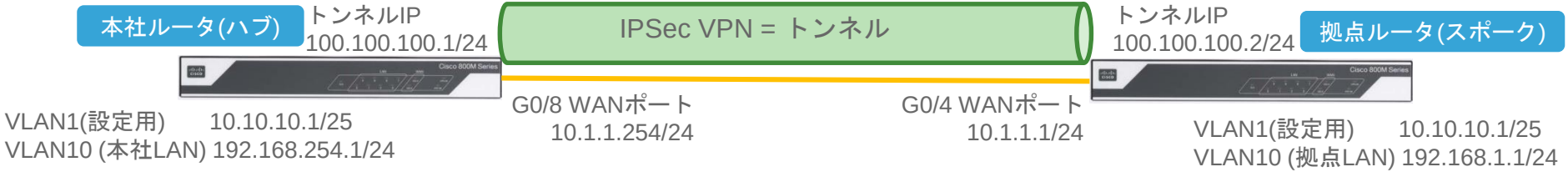
CCP Express 3.3
DMVPN簡単設定ガイド

※本資料は2017/02現在のハードウェア/ソフトウェアにおけるガイドです

はじめに

- 以下のサンプル構成における設定方法です
- WAN/LANの設定に関しては、同梱資料またはhttp://www.cisco.com/jp/go/c800m ”Cisco Configuration Professional（CCP）Express 3.3 による Cisco 841M J シリーズ初期設定ガイド”をご覧ください（以降の説明は初期設定がされていることが前提となっています）



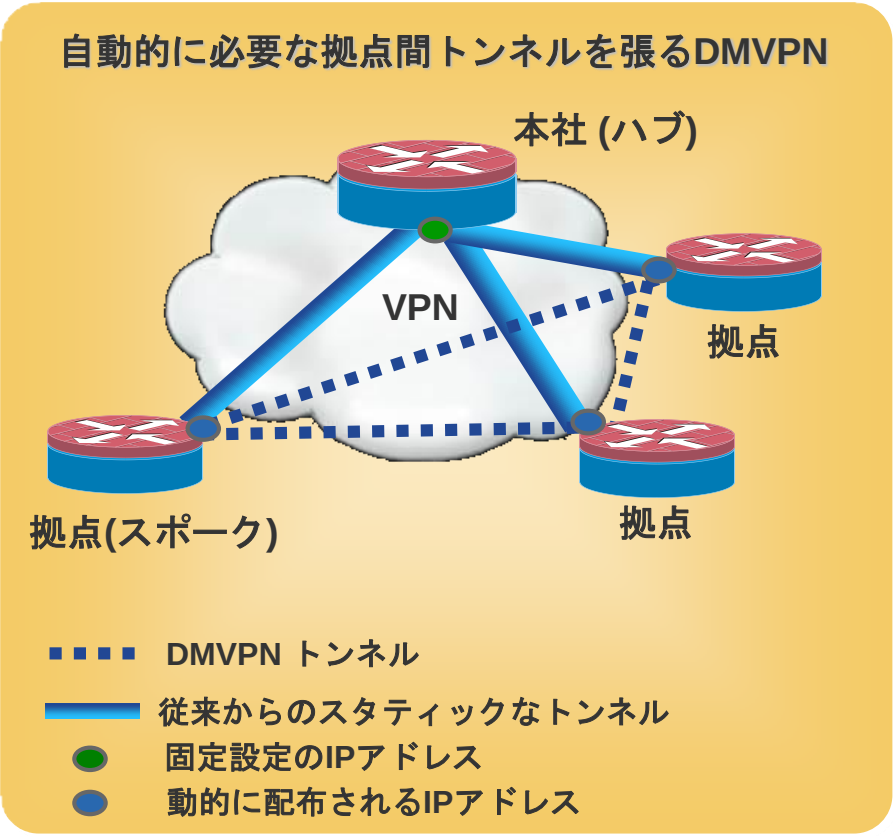
注) 本ガイドでは初期出荷時の管理VLAN1 10.10.10.0/25に設定端末をそれぞれ繋いで設定を行っています。VLAN1は”クイックセットアップウィザード”や”インターフェイスと接続”を使って追加/削除することも可能です。

DMVPNとは?

DMVPN(Dynamic Multipoint VPN):

VPN接続を行う技術の1つ
プロバイダの契約により、拠点では固定的なアドレスが指定出来ない場合があります。通常VPN接続には相互にIPアドレスを指定する設定が必要ですが、DMVPNではその必要がありません。拠点ルータは本社の固定IPアドレスを指定するだけで、自身のIPアドレスを考慮することなくVPN接続を構築することが可能です。

※本社側は固定IPアドレスが必須です
(CLIによる設定の場合DDNSも利用できます)



はじめに (参考)

- 以下のクイックセットアップウィザード設定時の概要画面です

本社ルータ

拠点ルータ

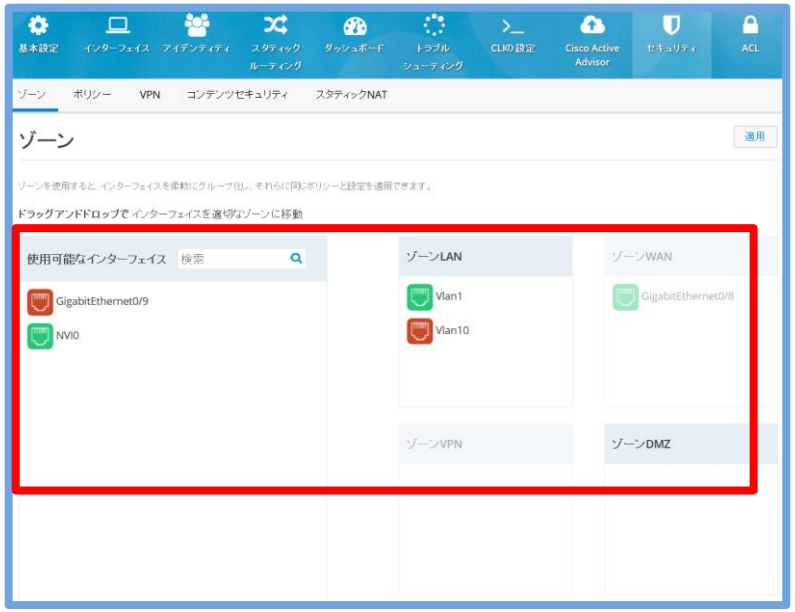
ステップ1：CCP Expressへのアクセス

- PCのブラウザを立ち上げ、”10.10.10.1”へアクセスして下さい
- 設定済みのユーザ名/パスワードを入力して下さい

ステップ2:ゾーンの設定

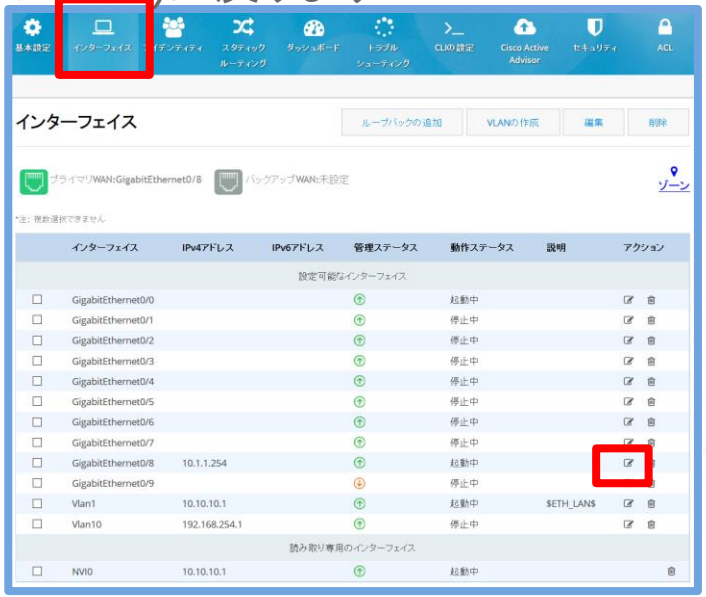
- CCP ExpressでVPNを使う場合、初めにゾーンの設定が必要です
- トップページから、セキュリティを選択して下さい
- ゾーン画面では使用可能インターフェイスをドラッグ&ドロップでゾーンLAN, DMZにあてはめることができます

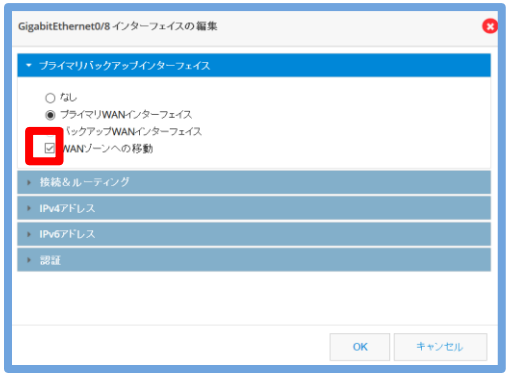
セキュリティ



ステップ2 (オプション):ゾーンWANの設定

- ゾーンWANに利用しているWANインターフェイスが入っていない場合は左上のインターフェイスボタンをクリックしてWANに使っているポート(本ガイドの例ではGigabitEthernet0/8)の編集ボタンをクリックしてください
- ポップアップした編集ボックスで"WANゾーンに移動"をクリックし、セキュリティ設定(ゾーン設定)に戻ります

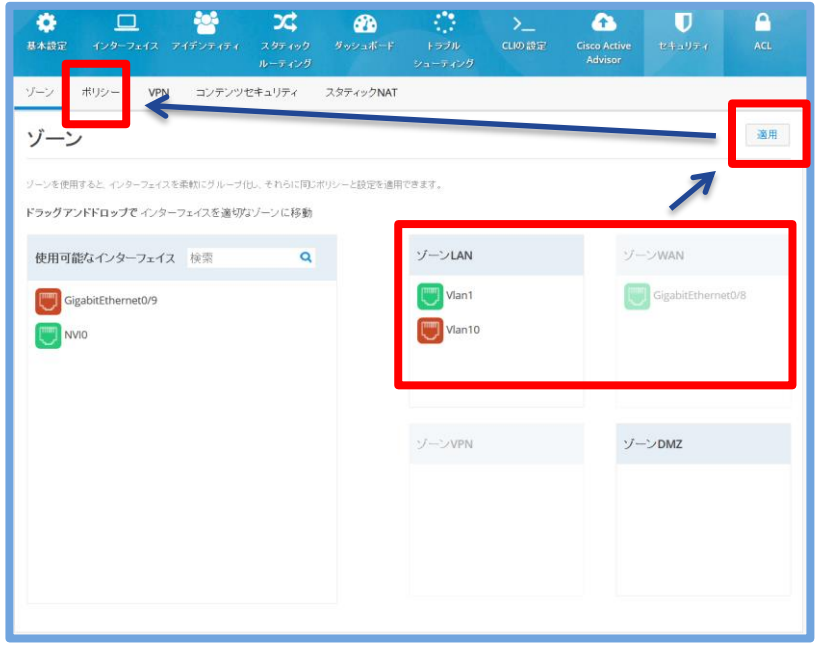




ステップ3:ゾーン設定内容の確認

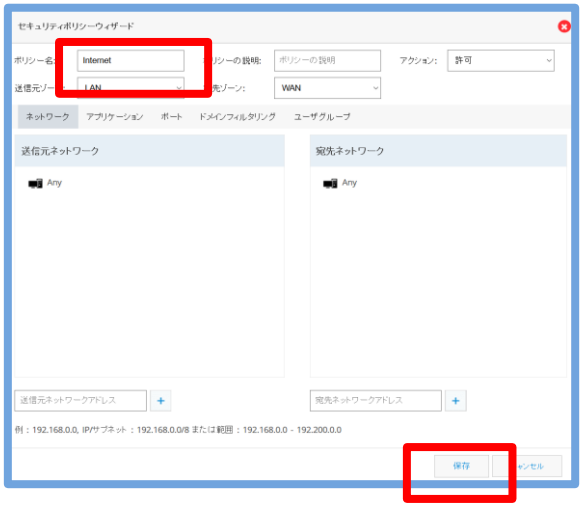
- 本ガイドの例では、本社ルータはG0/8, 拠点ルータはG0/4をゾーンWANにVlan1, Vlan10をゾーンLANに設定し、適用ボタンをクリックします
- ゾーン設定後、ポリシータブをクリックします

	ゾーンWAN	ゾーンLAN
本社ルータ	G0/8	VLAN1 VLAN10
拠点ルータ	G0/4	VLAN1 VLAN10



ステップ4：ポリシーの設定

- ポリシーを設定することで、ゾーン間のファイヤーウォール機能(ゾーンベースファイヤーウォール、ZBFW)を利用できます。
  クイックセットアップウィザードの設定方法によっては、ポリシー設定が全く行われず、全ての通信がドロップされる場合があります。
  今回の例では全てのIPトラフィックを通す設定を参考として追加します。（要件に応じて許可するトラフィックを設定して下さい）
- 右上の追加ボタンをクリックしてください
- セキュリティポリシーボックスが開いた後、
  ポリシー名(今回は”Internet”という名前)を入力し、他はデフォルトのまま保存します



ステップ5:ポリシー設定内容の確認

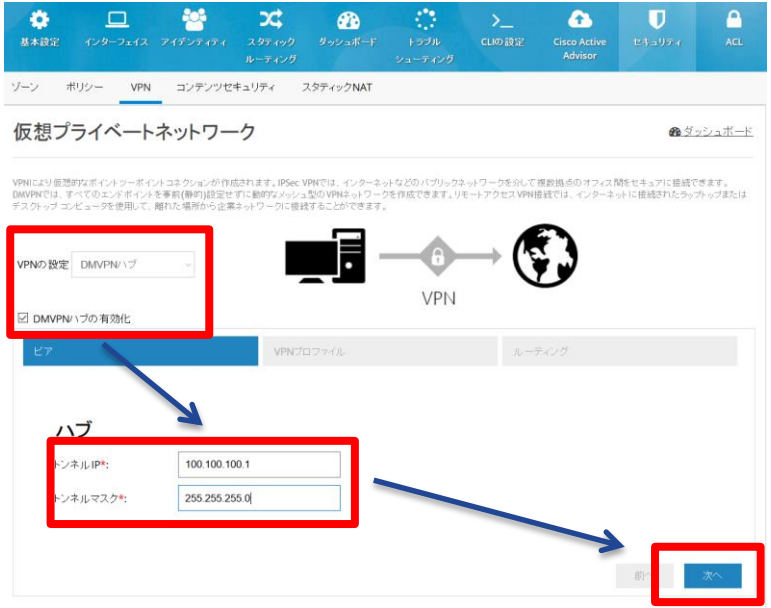
- ステップ4で設定した内容を確認の後、VPNタブをクリックします

注) ファイヤーウォール機能を使って必要なアプリケーションのみ通過させたい場合には、
全て許可 (Any / 許可)を設定せず、宛先やポート/アプリケーション別の許可を設定してください

ステップ6：仮想プライベートネットワークの設定

ハブルータ用
(本社ルータ)

- VPNの設定でDMVPNハブを選択し、「DMVPNハブの有効化」のチェックボックスにチェックを入れるとピアの設定が可能になります
- トンネルIPにはDMVPNハブのトンネルIPアドレスを、トンネルマスクにはサブネットマスクを入力して”次へ”をクリックします



ステップ6：仮想プライベートネットワークの設定

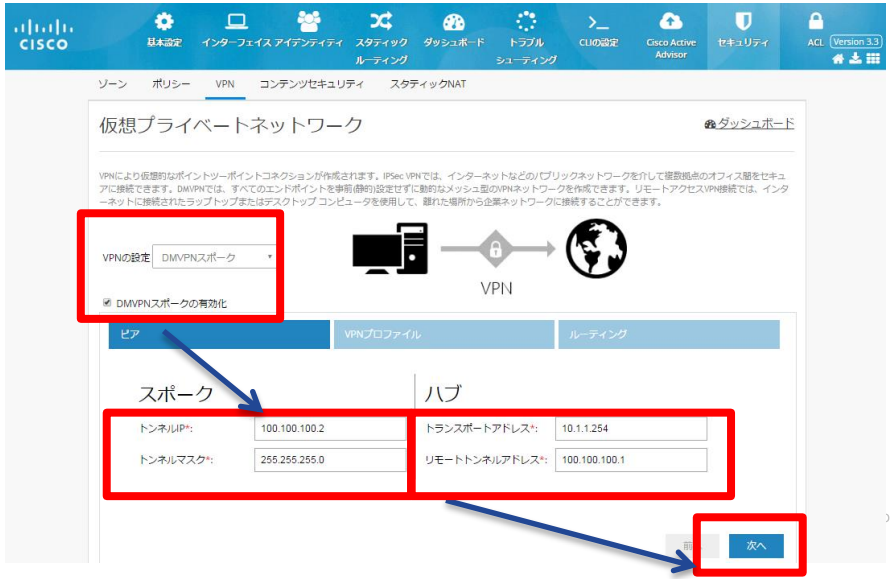
ハブルータ用
(本社ルータ)

- キー交換方式はデフォルト IKEv2です。IKEv1を使いたい場合には変更してください。事前共有キーはスポークルータと同じパスワードを入力します。次へをクリックします。
- ルーティングではEIGRP AS番号(DMVPN全体で利用する任意の数字)、LANセグメントのサブネットとワイルドカードマスクを入力し、+ボタンを押します。最後に終了をクリックします。

ステップ6：仮想プライベートネットワークの設定

スポークルータ用
(拠点ルータ)

- VPNの設定でDMVPNスポークを選択し、「DMVPNスポークの有効化」のチェックボックスにチェックを入れるとピアの設定が可能になります
- スポーク側のトンネルIPにはDMVPNスポークのトンネルIPアドレスを、トンネルマスクにはサブネットマスクを入力します
- ハブ側のトランスポートアドレスにはDMVPNハブのWANインターフェイスのIPアドレスを、リモートトンネルアドレスにはDMVPNハブのトンネルIPアドレスを入力して”次へ”をクリックします



ステップ6：仮想プライベートネットワークの設定

スポークルータ用
(拠点ルータ)

- キー交換方式はデフォルト IKEv2です。IKEv1を使いたい場合には変更してください。事前共有キーはスポークルータと同じパスワードを入力します。次へをクリックします。
- ルーティングではEIGRP AS番号(DMVPN全体で利用する任意の数字)、LANセグメントのサブネットとワイルドカードマスクを入力し、+ボタンを押します。最後に終了をクリックします。

DMVPN設定バグ：ワークアラウンド

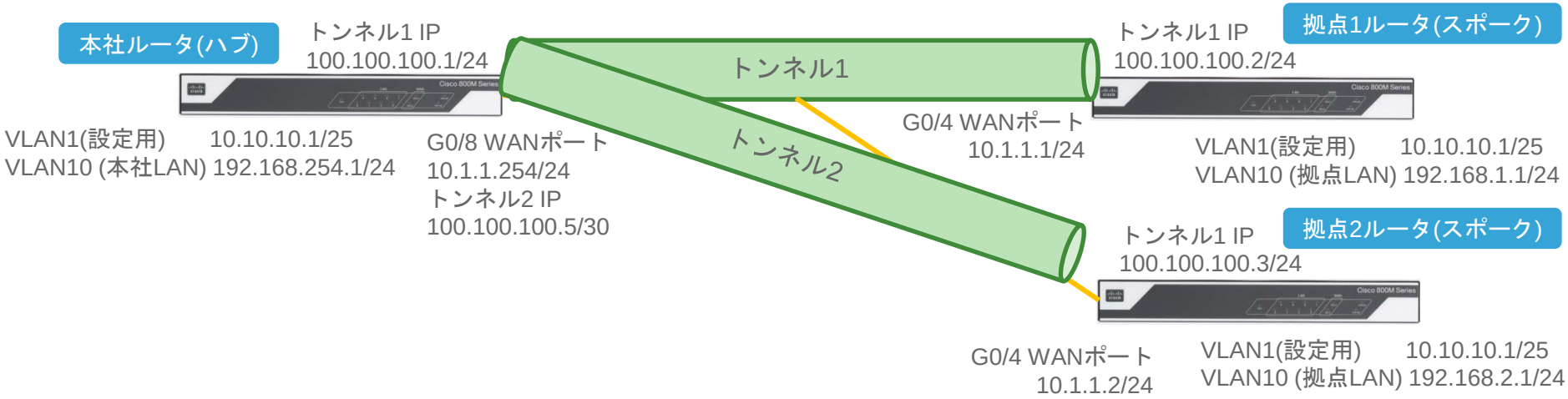
- 終了ボタンクリック後、終了せずにピアの設定に戻りますが、設定内容は反映されていますので他の設定機能をクリックして設定を継続してください
- ルーティングのローカルLANサブネットの設定を行いますが、Ver3.3ではすべてのインターフェイスのサブネットがすべて自動的に入力されます。
  不要なEIGRP Helloを送信したくない場合にはCLI設定から以下のコマンドで設定を消してください。

  router eigrp XXX (XXX:EIGRP AS番号)
  no network Y.Y.Y.Y (Y.Y.Y.Y 消したいネットワークアドレス)

ステップ7：仮想プライベートネットワーク接続完了

- ハブ/スポーク共に本Versionではピアの設定に戻りますが、設定終了している場合にはIPsecトンネルが自動的に張られます。
- 必要に応じてPingなどでご確認ください。

オプション例：拠点が追加された場合



- 本社ルータで追加の設定は必要ありません。
- 各拠点ルータはアドレスが違うだけで同様の設定方法となります。


CISCO