

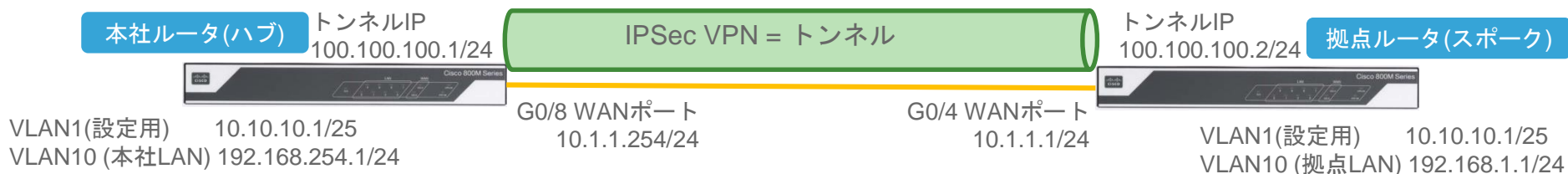


CCP Express 3.3 DMVPN簡単設定ガイド

※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?

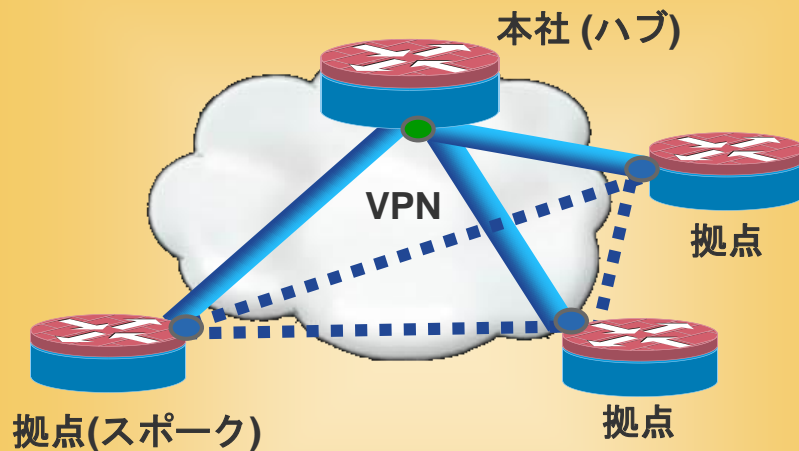
DMVPN(Dynamic Multipoint VPN):

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)

自動的に必要な拠点間トンネルを張るDMVPN



- ■ ■ ■ DMVPN トンネル
- ■ ■ ■ 従来からのスタティックなトンネル
- 固定設定のIPアドレス
- 動的に配布されるIPアドレス

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

クイックセットアップウィザード

基本 プライマリWAN バックアップWAN LAN セキュリティ&アプリ エクスプレスリエン

概要

基本	プライマリWAN	バックアップWAN	LAN	セキュリティ&アプリ エクスプレスリエン
<ul style="list-style-type: none">ルータ名:HONSHA-Routerドメインネーム:cisco.comタイムゾーン:(GMT+09:00)大阪, 札幌, 東京DNSサーバー:スタティック(1.1.1.1)NTPサーバー:無効	<ul style="list-style-type: none">WANインターフェイス: GigabitEthernet0/8Ipv4:スタティック(10.1.1.254)Ipv6:未設定NAT:有効PPPoE:無効	未設定	<ul style="list-style-type: none">プール名: ccp-poolLANネットワーク: 10.10.10.0サブネットマスク: 255.255.255.128デフォルトゲートウェイ: Vlan1 (10.10.10.1)新規LANネットワーク	<ul style="list-style-type: none">WANゾーン:GigabitEthernet0/8 ports GigabitEthernetLANゾーン:Vlan 1 with switchデフォルトポリシーの作成:許可シスコ推奨のセキュリティ設定:有効Application Visibility and Control (AVC):有効

拠点ルータ

クイックセットアップウィザード

基本 プライマリWAN バックアップWAN LAN セキュリティ&アプリ エクスプレスリエン

概要

基本	プライマリWAN	バックアップWAN	LAN	セキュリティ&アプリ エクスプレスリエン
<ul style="list-style-type: none">ルータ名:KYOTEN-1ドメインネーム:cisco.comタイムゾーン:(GMT+09:00)大阪, 札幌, 東京DNSサーバー:スタティック(1.1.1.1)NTPサーバー:無効	<ul style="list-style-type: none">WANインターフェイス: GigabitEthernet0/4Ipv4:スタティック(10.1.1.1)Ipv6:未設定NAT:有効PPPoE:無効	未設定	<ul style="list-style-type: none">プール名: ccp-poolLANネットワーク: 10.10.10.0サブネットマスク: 255.255.255.128デフォルトゲートウェイ: Vlan1 (10.10.10.1)新規LANネットワーク	<ul style="list-style-type: none">WANゾーン:GigabitEthernet0/4 ports GigabitEthernetLANゾーン:Vlan 1 with switchデフォルトポリシーの作成:許可シスコ推奨のセキュリティ設定:有効Application Visibility and Control (AVC):有効

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

The screenshot displays the main menu of the Cisco Configuration Assistant (CCA) interface. It features a grid of icons and text for various configuration tasks:

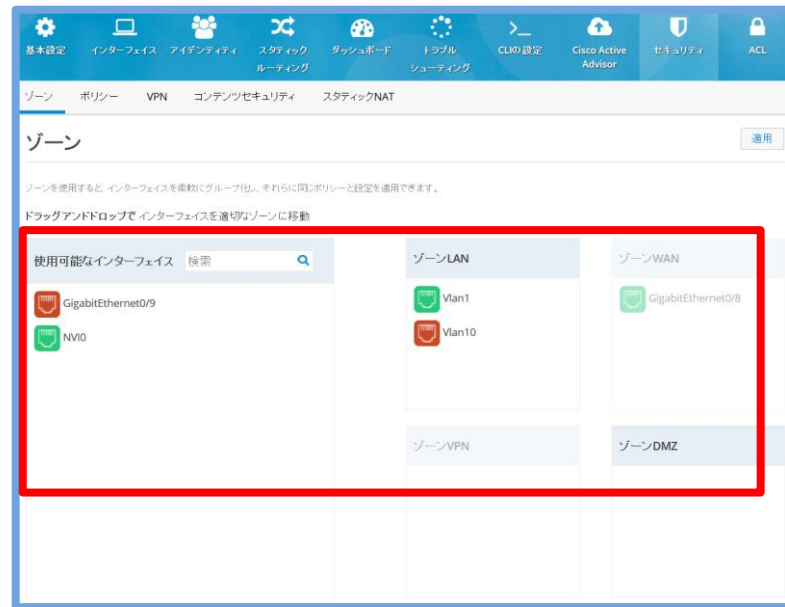
- 基本設定 (Basic Settings):** デバイスのホスト名、ドメイン名、タイムゾーン、NTP、DNSサーバ、IPv4 DHCPプールとDNSプロキシを設定します。
- インターフェイスと接続 (Interfaces and Connections):** LAN/WANインターフェイスを含む、デバイスのすべてのインターフェイスを設定します。DSL、イーサネット、3Gまたは4GのWANリンクをセットアップするか、VLANやループバックのインターフェイスを作成してインターフェイス属性を設定します。
- クイックセットアップウィザード (Quick Setup Wizard):** ウィザードにより、WAN/LANの接続が即座に建立されます。初期設定状態では、ルータに対してクイックセットアップウィザードを使用すると設定問題が生じることがあるため推奨しません。
- ダッシュボード (Dashboard):** ソフトウェアバージョンや詳細情報、インターフェイス、ラッシュやCPU使用率など、基本的な診断情報を表示します。セキュリティおよびApplication Visibility and Controlの情報は、デバイスのサポートに基づいて表示されます。
- アイデンティティ (Identity):** デバイスの新規ユーザを必要な権限レベルで設定し、グループを作成してから、これらのユーザをグループに移動します。認証パラメータを設定します。
- スタティックルーティング (Static Routing):** IPv4とIPv6のスタティックルートを設定します。
- Cisco Active Advisor:** ハードウェアおよびソフトウェア製品の使用情報をシスコに送信します。
- 任意のCLI (Arbitrary CLI):** IOS CLIコマンドを設定します。showコマンドを実行し、その出力をコピー/ダウンロードします。
- トラブルシューティング (Troubleshooting):** PingまたはTracerouteを使用して、IPv4またはIPv6の接続をトラブルシューティングします。
- セキュリティ (Security):** ファイアウォール、侵入防御、VPN、およびコンテナセキュリティ機能など、脅威防御の主要コンポーネントを含んでいる包括的なソリューションです。
- ACL (Access Control Lists):** アクセスコントロールリストを使うと、基本的なトラフィックフィルタリングとIPネットワークへのアクセス制御が可能になります。

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

基本設定 インターフェイス デフォルト値 スタック ルーティング ダッシュボード トラブル CLMの設定 Cisco Active Advisor セキュリティ ACL

インターフェイス

ループバックの追加 VLANの作成 編集 削除

プライマリ/WAN:GigabitEthernet0/8 バックアップ/WAN:未設定

*注: 複数選択できません

インターフェイス	IPv4アドレス	IPv6アドレス	管理ステータス	動作ステータス	説明	アクション
設定可能なインターフェイス						
<input type="checkbox"/> GigabitEthernet0/0			🟢	起動中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/1			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/2			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/3			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/4			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/5			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/6			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/7			🟢	停止中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/8	10.1.1.254		🟢	起動中		🔗 🗑
<input type="checkbox"/> GigabitEthernet0/9			🟡	停止中		🔗 🗑
<input type="checkbox"/> Vlan1	10.10.10.1		🟢	起動中	SETH_LANS	🔗 🗑
<input type="checkbox"/> Vlan10	192.168.254.1		🟢	停止中		🔗 🗑
読み取り専用のインターフェイス						
<input type="checkbox"/> NV10	10.10.10.1		🟢	起動中		🗑

GigabitEthernet0/8 インターフェイスの編集

プライマリ/バックアップインターフェイス

なし

プライマリ/WANインターフェイス

バックアップ/WANインターフェイス

WANゾーンへの移動

接続 & ルーティング

IPv4アドレス

IPv6アドレス

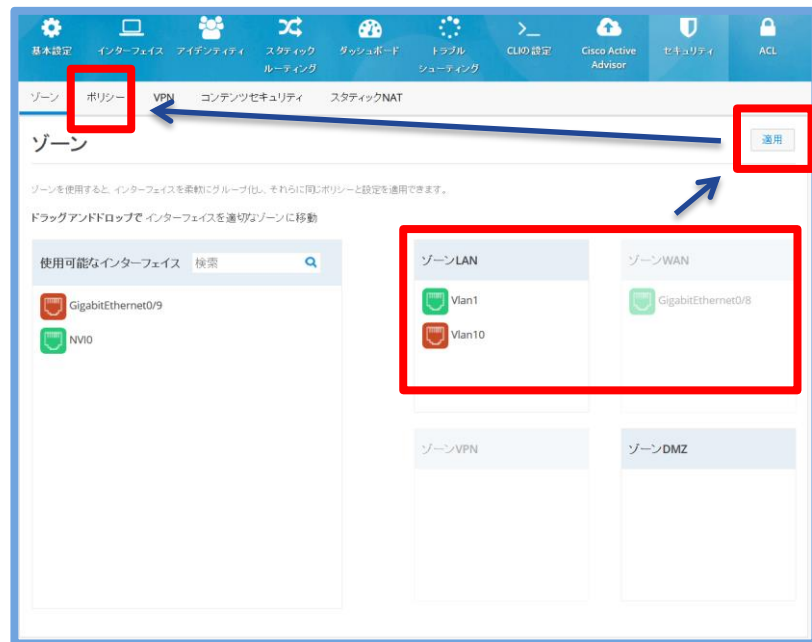
認証

OK キャンセル

ステップ3: ゾーン設定内容の確認

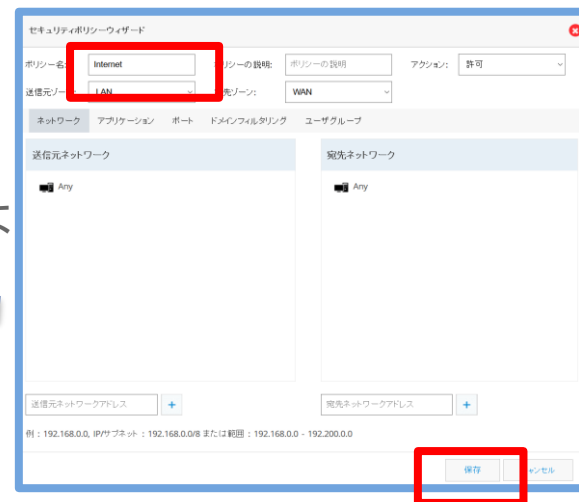
- 本ガイドの例では、本社ルータはG0/8, 拠点ルータはG0/4をゾーンWANにVlan1, Vlan10をゾーンLANに設定し、適用ボタンをクリックします
- ゾーン設定後、ポリシータブをクリックします

	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、ゾーン間のファイアーウォール機能(ゾーンベースファイアーウォール、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

The screenshot shows the Cisco configuration interface. The top navigation bar includes icons for various settings: 基本設定 (Basic Settings), インターフェイス (Interfaces), アイデンティティ (Identity), スタティックルーティング (Static Routing), ダッシュボード (Dashboard), トラブルシューティング (Troubleshooting), CLIの設定 (CLI Configuration), Cisco Active Advisor, セキュリティ (Security), and ACL. Below this, a sub-navigation bar shows 'ゾーン' (Zones), 'ポリシー' (Policies), 'VPN' (highlighted with a red box), 'コンテンツセキュリティ' (Content Security), and 'スタティックNAT' (Static NAT). The main content area is titled 'ポリシー' (Policy) and includes a 'ダッシュボード' (Dashboard) icon and buttons for '追加' (Add), '編集' (Edit), and '削除' (Delete). A note explains that firewall rules are created based on interface contexts. A table lists policies with columns: 'ポリシー名' (Policy Name), '説明' (Description), 'ユーザ' (User), '送信元ネットワーク' (Source Network), '宛先ネットワーク' (Destination Network), '送信元ポート' (Source Port), '宛先ポート' (Destination Port), 'アプリケーション' (Application), 'ドメイン' (Domain), 'ポリシーアクション' (Policy Action), and 'アクション' (Action). The first row, 'internet', is highlighted with a red box.

ポリシー名	説明	ユーザ	送信元ネットワーク	宛先ネットワーク	送信元ポート	宛先ポート	アプリケーション	ドメイン	ポリシーアクション	アクション
internet	-	Any	Any	Any	Any	Any	Any	Any	許可	📄 🗑️

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

- 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

The screenshot shows the Cisco VPN configuration interface. The top navigation bar includes options like '基本設定', 'インターフェイス', 'アイデンティティ', 'スタック ルーティング', 'ダッシュボード', 'トップ シューティング', 'CLIの設定', 'Cisco Active Advisor', 'セキュリティ', and 'ACL'. The main menu has 'ゾーン', 'ポリシー', 'VPN', 'コンテンツセキュリティ', and 'スタティックNAT'. The current page is titled '仮想プライベートネットワーク' (Virtual Private Network) and features a 'ダッシュボード' (Dashboard) link.

Below the title, there is a descriptive paragraph about VPN configurations. The main configuration area shows 'VPNの設定' (VPN Configuration) set to 'DMVPNハブ' (DMVPN Hub). A checkbox labeled 'DMVPNハブの有効化' (Enable DMVPN Hub) is checked. Below this, the 'ピア' (Peer) tab is selected, and the 'ハブ' (Hub) configuration is visible. The 'トンネルIP*' (Tunnel IP) field is set to '100.100.100.1' and the 'トンネルマスク*' (Tunnel Mask) field is set to '255.255.255.0'. At the bottom right, the '次へ' (Next) button is highlighted with a red box. Blue arrows point from the 'DMVPNハブ' dropdown, the 'DMVPNハブの有効化' checkbox, and the 'トンネルIP*' field to the '次へ' button.

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。

仮想プライベートネットワーク

VPNの設定: DMVPN/Hub

DMVPN/Hubの有効化

キー交換

キー交換方式: IKEv1 IKEv2

事前共有キー:

次へ

仮想プライベートネットワーク

VPNの設定: DMVPN/Hub

DMVPN/Hubの有効化

EIGRP AS番号: 100

ローカルLANサブネット: トンネルIP

ワイルドカードマスク: ワイルドカードマスク

+

終了

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

仮想プライベートネットワーク

VPNの設定: DMVPNスポーク

DMVPNスポークの有効化

スポーク	ハブ
トンネルIP:	トランスポートアドレス:
100.100.100.2	10.1.1.254
トンネルマスク:	リモートトンネルアドレス:
255.255.255.0	100.100.100.1

次へ

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。

仮想プライベートネットワーク

VPNの設定: DMVPNスポーク

DMVPNスポークの有効化

キー交換

キー交換方式: IKEv1 IKEv2

事前共有キー:

次へ

仮想プライベートネットワーク

VPNの設定: DMVPNスポーク

DMVPNスポークの有効化

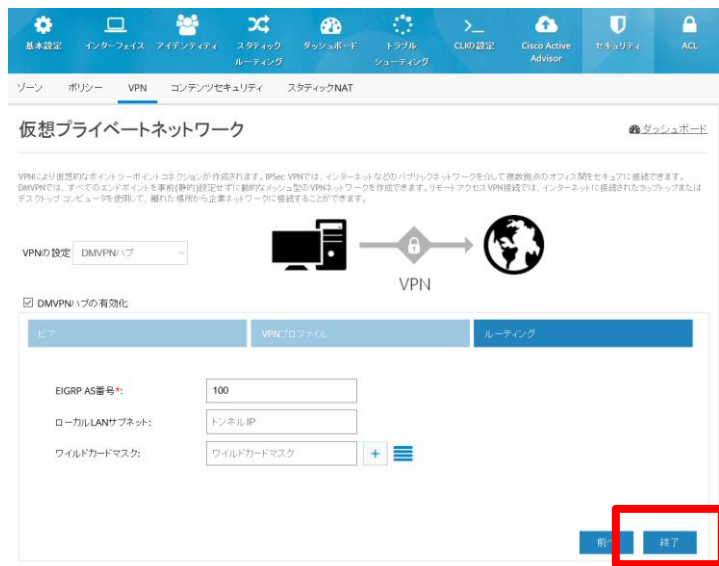
EIGRP AS番号: 100

ローカルLANサブネット: トンネルIP

Wildcard Mask: ワイルドカードマスク

完了

DMVPN設定バグ：ワークアラウンド



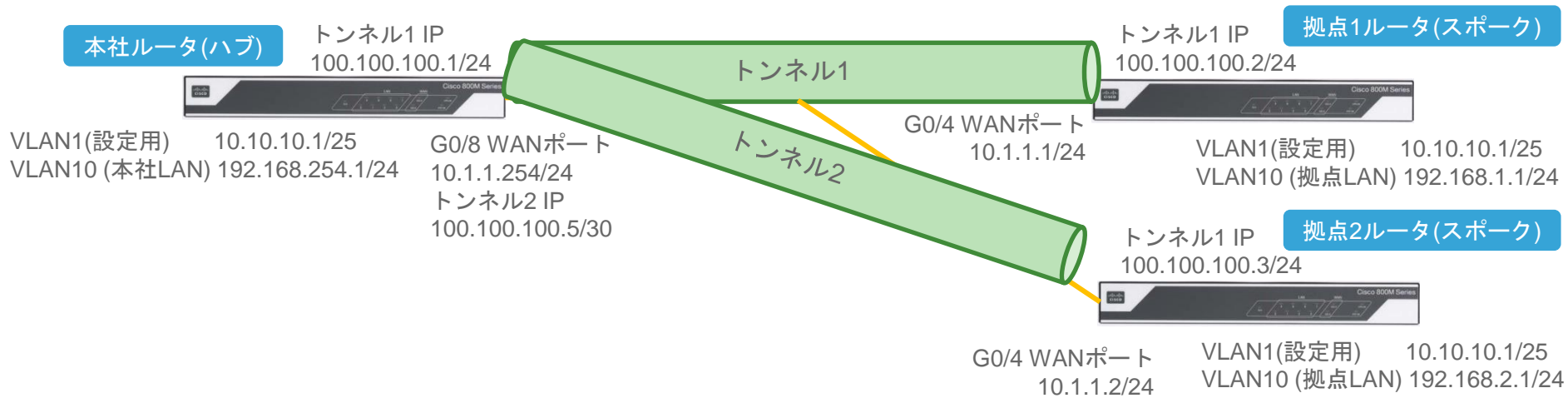
- 終了ボタンクリック後、終了せずにピアの設定に戻りますが、設定内容は反映されていますので他の設定機能をクリックして設定を継続してください
- ルーティングのローカルLANサブネットの設定を行いますが、Ver3.3ではすべてのインターフェイスのサブネットがすべて自動的に入力されます。不要なEIGRP Helloを送信したくない場合にはCLI設定から以下のコマンドで設定を消してください。

```
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。

