

Cisco Start Router

設定マニュアル サイト間インターネット IPsec-VPN Cisco 841M J

2016 年 5 月 31 日

第 1.1 版



www.networld.co.jp

株式会社ネットワールド



Networld



改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016 年 1 月 29 日	ネットワーク	● 新規
1.1	2016 年 5 月 31 日	ネットワーク	<ul style="list-style-type: none">● 「1. はじめに」章の対象外構成で動的 IP アドレスを使用した構成の“VPN レスポンダー”を“VPN イニシエーター”に変更● 「1. はじめに」章の対象外構成に MP LS-VPN と IPsec-VPN のマッピング（VRF-Aware IPsec）を追加● 「2. システム構成」章の「図 2 サイト間インターネット IPsec-VPN の設定で構成するシステム」のリモートサイトの製品の LAN 側インターフェースの誤った IP アドレスの“.1”を“.129”に変更● 「3.1 ゾーンの設定」節のリード文からポリシーと IPsec-VPN トンネルの関係性の説明を削除● 「3.3 VPN の設定」節の手順にリモートサブネット宛のスタティックルートの説明を追加● 「3.3 VPN の設定」節の手順に複数の IPsec-VPN トンネル設定時の VPN OK LED の説明を追加● 「3.3 VPN の設定」節のリード文で製品を通過するトラフィックが IPsec-VPN トンネルを使用するかどうかを決定する基準を“ポリシーベース”から“ルーティングベース”に変更● 「4. 設定ファイル」章の設定にリモートサブネット宛のスタティックルートを追加



免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワーク（以下 弊社）が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではありません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではありません。



表記規則

表記	表記の意味
「」(括弧記号)	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold (ボールド文字)	入力または選択するシステム定義値
<i><italic></i> (イタリック文字)	入力または選択するユーザー定義値
□ (囲み線)	入力または選択するオブジェクト
"" (二重引用符記号)	表示されるメッセージ
■ (蛍光マーカー)	確認するメッセージ

表記の例)

(1) 「Exec」ラジオボタンを選択します。

(2) テキストボックスに以下のコマンドを入力します。

copy running-config <file name>

(3) 「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に「[OK]」が表示されます。

Destination filename [startup-config]?

Building configuration...

[OK]

CLIによる設定

CLI機能はルータのコマンドプロンプトで実行可能な設定や、全てのIOS CLIコマンドを入力できます

1
2
3

☒ Exec
☐ Configure

copy running-config startup-config

コマンドを実行

クリア

Destination filename [startup-config]?
Building configuration...
[OK]



目次

1. はじめに.....	1
1.1 対象製品.....	2
1.2 CCP Express のシステム要件.....	2
1.3 クイックリンク.....	2
2. システム構成.....	4
2.1 設定値	4
2.1.1 ユーザー定義値.....	4
2.1.2 システムの既定値.....	5
2.2 使用した機材	6
3. 設定手順	7
3.1 ゾーンの設定	7
3.1.1 WAN ゾーンの設定	7
3.1.2 LAN ゾーンの設定	9
3.2 ルーティングの設定	11
3.3 VPN の設定.....	14
3.4 ポリシーの設定	17
4. 設定ファイル.....	20



1. はじめに

本書は、Cisco Configuration Professional Express（以下 CCP Express）のアドバンスドセットアップを使用してCisco 841M Jシリーズのサイト間インターネットIPsec-VPNの設定を実行する手順を説明した資料です。本書では暗号化、およびカプセル化（トンネリング）共にIPsecを使用したVPNゲートウェイとして、製品を設定します。CCP Expressは、Web UIを備えた組み込みのデバイス管理ツールです。CCP Expressのアドバンスドセットアップを使用すると、WAN、LAN、およびセキュリティなど、製品の詳細設定を簡単に実行できます。サイト間インターネットIPsec-VPNの設定が完了すると、ローカルサイトとリモートサイトがインターネット上で安全に接続できるようになります。

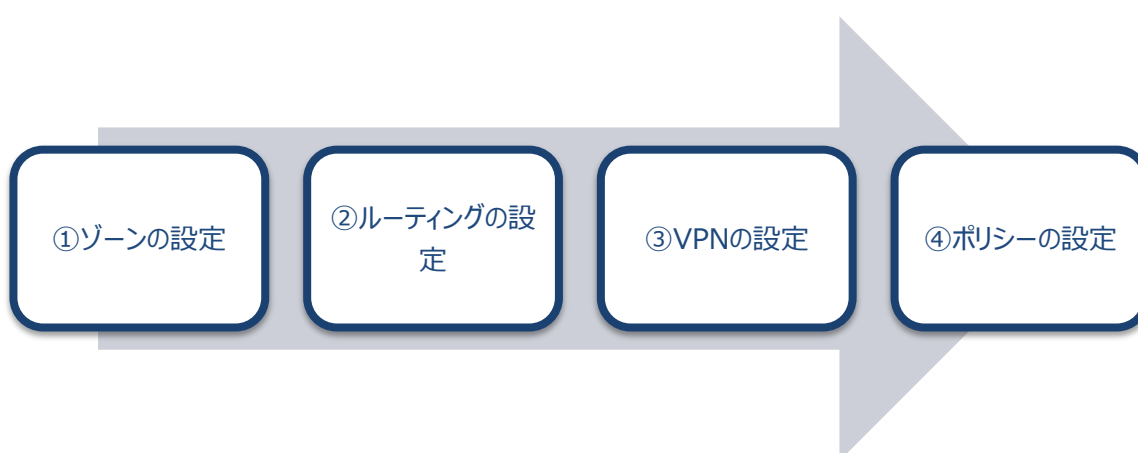


図 1 本書で実行する設定

なお、CCP Expressでは以下のような構成のサイト間インターネットIPsec-VPNの設定を実行できません。必要に応じてCisco Systems（以下Cisco）社が提供するマニュアルを参照して、CLIで設定してください。

- 複数サイトをVPNで接続する場合
- WAN側IPアドレスが動的に変更されるVPNイニシエーターを使用する場合
- カプセル化にGREなどのIPsec以外のプロトコルを使用する場合
- トランスポートモードでVPNトラフィックを転送する場合
- VPNゲートウェイ間にNATデバイスが構成されている場合
- VPNゲートウェイ間がIPv6ネットワークで構成されている場合
- VPNトンネルを冗長化する場合
- 鍵管理、暗号化、認証などの、IKEの詳細なパラメーター設定を必要とする場合
- MPLS-VPNにIPsec-VPNをマッピングする場合



1.1 対象製品

本書を使用してサイト間インターネット IPsec-VPN の設定を実行できる製品は、以下のとおりです。

表 1 本書の対象製品

C841M-4X-JSEC/K9	C841M-4X-JAIS/K9	C841M-8X-JAIS/K9
<input checked="" type="checkbox"/> (最大 20 トンネル)	<input checked="" type="checkbox"/> (最大 20 トンネル)	<input checked="" type="checkbox"/> (最大 100 トンネル)

1.2 CCP Express のシステム要件

CCP Express を使用できる Cisco IOS および Web ブラウザーは、次のとおりです。なお、本書では CCP Express のセキュリティ機能（ゾーン、ポリシー、VPN などのセキュリティ設定）を使用するため、製品にバージョン 15.5(1)T 以上の Cisco IOS がインストールされている必要があります。

- Cisco IOS 15.2(4)M2～、または 15.3(1)T～、セキュリティ機能は 15.5(1)T～
- Microsoft Internet Explorer 10
- Google Chrome 17～
- Mozilla Firefox 10～

1.3 クイックリンク

Cisco 841M J シリーズの公式の情報は、以下の URL から入手できます。

- Cisco Start Router ホーム:
<http://www.cisco.com/web/JP/smb/c800m/index.html>
- 製品カタログ:
http://www.cisco.com/web/JP/product/catalog/pdf/1082_en_start_catalog.pdf
- データシート:
http://www.cisco.com/web/JP/smb/c800m/docs/c800mj_data_sheet_c78-732678.pdf
- サポートコミュニティ:
<https://supportforums.cisco.com/ja/start>



Cisco Start Router

設定マニュアル サイト間インターネット IPsec-VPN Cisco 841M J



- よくある質問:
<http://www.cisco.com/web/JP/smb/c800m/c800m-faq.html>
- サポート窓口:
<http://www.cisco.com/web/JP/smb/c800m/c800m-support.html>



2. システム構成

サイト間インターネット IPsec-VPN の設定の手順は、以下の構成で説明します。

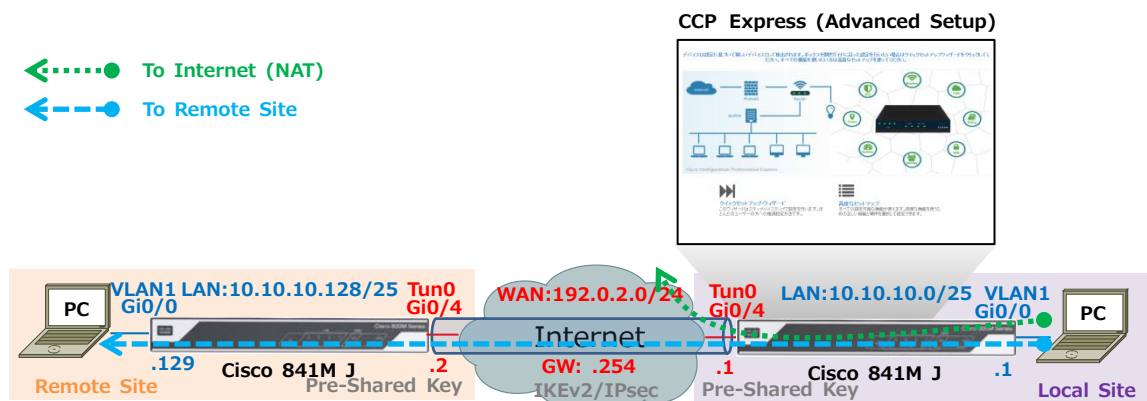


図 2 サイト間インターネット IPsec-VPN の設定で構成するシステム

ローカルサイトとリモートサイトの製品は、固定のパブリック IP アドレスを割り当てた WAN 側インターフェースを使用して互いにポイントツーポイントの IPsec-VPN トンネルをインターネット上に確立します。各サイトは、製品の IPsec ポリシーによって確立された IPsec-VPN トンネルを使用して、オリジナルの送信元 IP アドレスで対向サイトのネットワークに接続します。インターネット接続を含むその他の通信は、IPsec-VPN トンネルを使用せず、送信元 IP アドレスを変換して送出されます。なお、本書ではリモートサイトの製品の設定はすでに完了しているものとし、ローカルサイトの製品に対する設定のみを説明の対象としています。また、ローカルサイトの製品についても、クイックセットアップウィザードを使用したインターフェースや VLAN などの LAN 側の基本設定、PPPoE、デフォルトルート、NAT などの WAN 側の基本設定、およびインターネット接続用の標準的なファイアウォール設定が完了しているものとします。クイックセットアップウィザードを使用した製品の初期セットアップについては、クイックスタートガイドをご参照ください。

- Cisco Start Router 設定マニュアル クイックスタートガイド Cisco 841M J:
http://www.networkworld.co.jp/download_file/4574/7266/

2.1 設定値

本書でを使用した VPN 関連の設定値について説明します。

2.1.1 ユーザー定義値

CCP Express を使用して設定できる VPN 関連の設定値は、以下のとおりです。



表 2 CCP Express を使用して設定できる VPN 関連の設定値

項目	値	備考
VPN 接続形態	サイト間	
鍵交換プロトコル	IKEv2	
ローカルサイトの VPN トンネルの IP アドレス	192.0.2.1	
ローカルサイトの VPN トンネルのサブネットマスク	255.255.255.0	
リモートサイトの VPN トンネルの IP アドレス	192.0.2.2	
事前共有鍵	passphrase	
リモートサイトの LAN 側のネットワークアドレス	10.10.10.128/25	

2.1.2 システムの既定値

CCP Express を使用してサイト間インターネット IPsec-VPN を設定した場合、ほとんどの設定に既定値が適用されます。CCP Express によって自動的に適用される VPN 関連の設定値は、以下のとおりです。

表 3 CCP Express によって自動的に適用される VPN 関連の設定値

項目	値	備考
セキュリティプロトコル	IPsec	
トンネリングプロトコル	IPsec	
VPN ロール	イニシエーター	
IPsec SA グラニュラリティ	ネットワーク	
IKE フェーズ 1: メッセージ交換方式	メインモード	
IKE フェーズ 1: 鍵管理方式	Diffie-Hellman Group 5/2	プロポーザルの優先順
IKE フェーズ 1: 暗号化方式	AES 256/192/128bit	プロポーザルの優先順
IKE フェーズ 1: ハッシュ方式	SHA-2 512/384/256bit, SHA-1 96bit, MD5 96bit	プロポーザルの優先順
IKE フェーズ 1: 認証方式	HMAC-SHA-1 160bit	事前共有鍵
IKE フェーズ 1: SA ライフタイム	86,400 秒	
IKE フェーズ 2: カプセル化方式	トンネルモード (ESP)	
IKE フェーズ 2: メッセージ交換方式	クイックモード	
IKE フェーズ 2: 鍵管理方式	なし	
IKE フェーズ 2: 暗号化方式	AES 128bit	
IKE フェーズ 2: 認証方式	HMAC-SHA-1 160bit	
IKE フェーズ 2: SA ライフタイム	3,600 秒	



2.2 使用した機材

本書で使用した機材は、以下のとおりです。

表 4 本書で使用した機材

機材	製品型番または名称	備考
Cisco 841M J シリーズ	C841M-4X-JAIS/K9 15.5(3)M	各サイト共通
デバイス管理ツール	CCP Express 3.1.2	各サイト共通
PC	Windows 7 x64 Professional SP1	各サイト共通
Web ブラウザー	Internet Explorer x64 11.0.9600.18163	各サイト共通



3. 設定手順

Cisco 841M J シリーズのサイト間インターネット IPsec-VPN の設定を実行します。

3.1 ゾーンの設定

既定の WAN ゾーンと LAN ゾーンに、VPN 接続で使用するインターフェースを割り当てます。ゾーンはポリシーの前提条件で、ポリシーはゾーンのペアに対して適用されます。ゾーンに対してポリシーが割り当てられていない場合、既定ですべてのトラフィックが破棄（Drop）されます。

3.1.1 WAN ゾーンの設定

既定の WAN ゾーンに、VPN 接続で使用する WAN 側インターフェースを割り当てます。

(1) インターフェースの設定画面に移動します。「インターフェイスと接続」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「インターフェイス」ボタンをクリックしてください。



図 3 CCP Express のホーム（インターフェイスと接続）



図 4 CCP Express のショートカット（ホームとインターフェイス）

(2) WAN 側インターフェースを編集します。「GigabitEthernet0/4」ラベル内の「編集」ボタンをクリックします。

インターフェイス

ループバックの追加

VLAN の追加

編集

削除


 プライマリ WAN: GigabitEthernet0/4(Dialer1)


 バックアップ WAN: 未構成

[ゾーン](#)

*注意: 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	管理状態	操作状態	説明	アクション
構成可能なインターフェイス						
<input type="checkbox"/> GigabitEthernet0/0			↑	up		 
<input type="checkbox"/> GigabitEthernet0/1			↑	down		 
<input type="checkbox"/> GigabitEthernet0/2			↑	down		 
<input type="checkbox"/> GigabitEthernet0/3			↑	down		 
<input type="checkbox"/> GigabitEthernet0/4			↑	up		 
<input type="checkbox"/> GigabitEthernet0/5			↓	down		 
<input type="checkbox"/> Vlan1	10.10.10.1		↑	up	\$ETH_LAN\$	 
読み取り専用のインターフェイス						
<input type="checkbox"/> NVI0			↑	up		
<input type="checkbox"/> Virtual-Access1			↑	up		
<input type="checkbox"/> Virtual-Access2			↑	up		
<input type="checkbox"/> Dialer1	192.0.2.1		↑	up		

図 5 インターフェイスの編集

(3) WAN 側インターフェースを既定の WAN ゾーンに割り当てます。「WAN ゾーンに移動」チェックボックスにチェックを入れます。「はい」ボタンをクリックします。この設定はプライマリ WAN インターフェイスの既定の設定のため、ほとんどの場合、当該インターフェースはすでに WAN ゾーンに割り当てられています。



編集 GigabitEthernet0/4 インターフェイス

▼ プライマリセカンダリインターフェイス

☐ 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

1 ☒ WANゾーンに移動

▶ 接続
▶ IPv4 アドレス
▶ IPv6 アドレス
▶ 認証

2 はい キャンセル

図 6 インターフェイスの編集（詳細）

3.1.2 LAN ゾーンの設定

既定の LAN ゾーンに、VPN 接続で使用する LAN 側インターフェイスを割り当てます。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。



図 7 CCP Express のホーム（セキュリティ）



図 8 CCP Express のショートカット（ホームとセキュリティ）

(2) LAN 側インターフェースを既定の LAN ゾーンに割り当てます。「使用可能なインターフェース」リスト内の「GigabitEthernet0/0」ラベルをドラッグし、「ゾーン LAN」リストにドロップします。同様の手順で「Vlan1」ラベルをドラッグアンドドロップで「ゾーン LAN」リストに移動します。「適用する」ボタンをクリックします。この設定は初期セットアップにクイックセットアップウィザードを使用した場合の既定の設定のため、ほとんどの場合、当該インターフェースはすでに LAN ゾーンに割り当てられています。

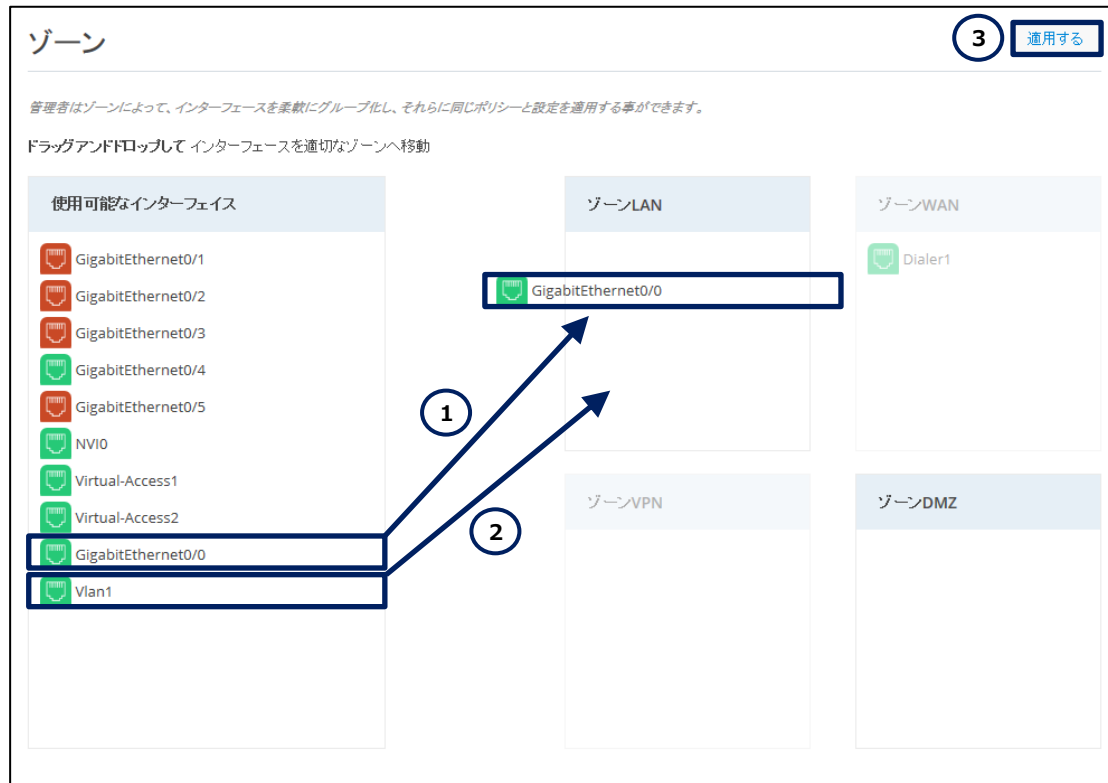


図 9 セキュリティの編集 (ゾーン)

3.2 ルーティングの設定

リモートサイトの製品のトンネルエンドポイントになる WAN 側インターフェースのスタティックルートを設定します。この設定は、製品がローカルサイトのトンネルエンドポイントとして使用される WAN 側インターフェース自体を使用して、リモートサイトのトンネルエンドポイント宛にルーティングされることによって起こる、再帰的ルーティングの問題を防止します。

- リモートサイトのトンネルエンドポイントの WAN 側インターフェースに対してローカルサイトの IPsec-VPN トンネルを使用する場合、再帰的ルーティングが起こり、IPsec-VPN トンネルは確立と切断を繰り返す

```
S* 0.0.0.0/0 is directly connected, Dialer1
S 0.0.0.0/32 is directly connected, Tunnel0
10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C 10.10.10.0/25 is directly connected, Vlan1
L 10.10.10.1/32 is directly connected, Vlan1
S 10.10.10.128/25 is directly connected, Tunnel0
C 192.0.2.1/32 is directly connected, Dialer1
```




```
C      192.0.2.254/32 is directly connected, Dialer1
*Jan 28 08:10:35.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to up
*Jan 28 08:10:35.975: %ADJ-5-PARENT: Midchain parent maintenance for IP
midchain out of Tunnel0 - looped chain attempting to stack
*Jan 28 08:10:45.975: %TUN-5-RECURDOWN: Tunnel0 temporarily disabled due
to recursive routing
*Jan 28 08:10:45.975: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to down
*Jan 28 08:11:45.979: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to up
*Jan 28 08:11:45.979: %ADJ-5-PARENT: Midchain parent maintenance for IP
midchain out of Tunnel0 - looped chain attempting to stack
*Jan 28 08:11:55.979: %TUN-5-RECURDOWN: Tunnel0 temporarily disabled due
to recursive routing
  ● リモートサイトのトンネルエンドポイントの WAN 側インターフェースに対してローカルサイトの WAN
    側インターフェースを使用する場合、再帰的ルーティングが解決し、IPsec-VPN トンネルは正常
    に確立する
S*    0.0.0.0/0 is directly connected, Dialer1
S      0.0.0.0/32 is directly connected, Tunnel0
      10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
C      10.10.10.0/25 is directly connected, Vlan1
L      10.10.10.1/32 is directly connected, Vlan1
S      10.10.10.128/25 is directly connected, Tunnel0
C      192.0.2.0/24 is directly connected, Tunnel0
C      192.0.2.1/32 is directly connected, Tunnel0
      is directly connected, Dialer1
S      192.0.2.2/32 is directly connected, Dialer1
C      192.0.2.254/32 is directly connected, Dialer1
```

(1) 静的ルーティングの設定画面に移動します。「静的ルーティング」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「静的ルーティング」ボタンをクリックしてください。



図 10 CCP Express のホーム（静的ルーティング）



図 11 CCP Express のショートカット（ホームと静的ルーティング）

(2) スタティックルートを追加します。「追加」ボタンをクリックします。

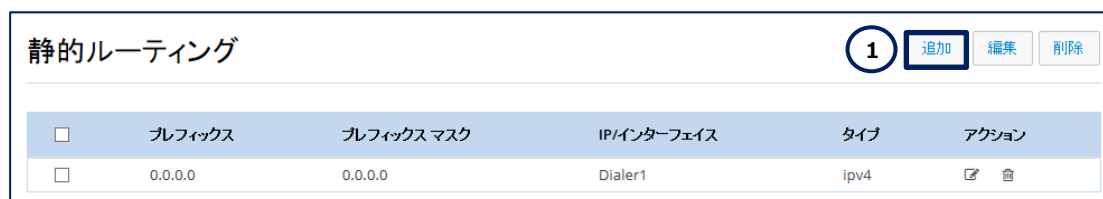


図 12 静的ルーティングの編集

(3) リモートサイトの製品の WAN 側インターフェイス宛のスタティックルートを追加します。

- ① 「プレフィックス」テキストボックスにリモートサイトの製品の WAN 側インターフェイスの IP アドレスを入力します。本書では、表 2 のとおり、**192.0.2.2** を使用しています。



- ② 「プレフィックスマスク」テキストボックスに **255.255.255.255** を入力します。
- ③ 「インターフェイス」ラジオボタンをクリックします。
- ④ 「フォーワーディングインターフェイス」ドロップダウンリストで **Dialer1** を選択します。
- ⑤ 「はい」ボタンをクリックします。

静的ルートの追加

IPv4 アドレス

接続先のアドレス

プレフィックス

192.0.2.2

1

プレフィックス マスク

255.255.255.255

2

ネクストホップ IP

☒ インターフェイス
☐ IP
☐ DHCP

フォーワーディングインターフェイス

Dialer1

4

3

IPv6 アドレス

5

はい

キャンセル

図 13 静的ルーティングの編集（詳細）

3.3 VPN の設定

IPsec-VPN の暗号化とトンネリングを設定します。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。



図 14 CCP Express のホーム（セキュリティ）



図 15 CCP Express のショートカット（ホームとセキュリティ）

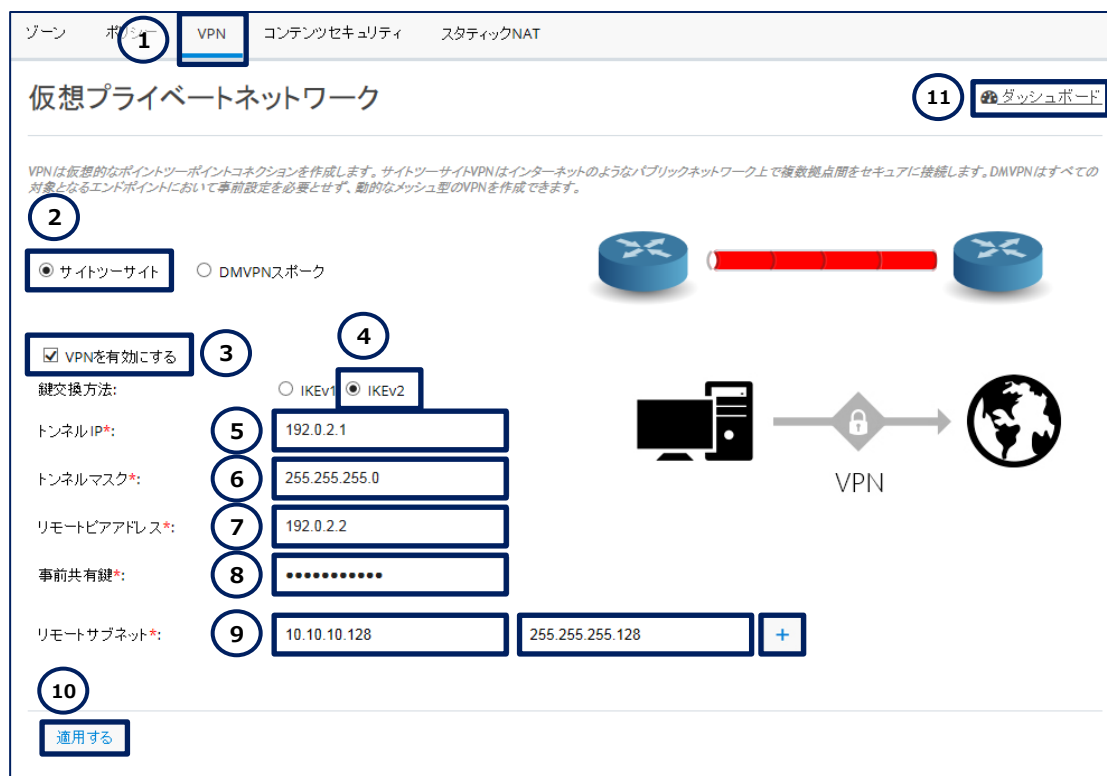
(2) VPN の設定を実行します。「*」ラベルが記載された設定は、必須の設定です。

- ① 「VPN」タブをクリックします。
- ② 「サイトツーサイト」ラジオボタンをクリックします。
- ③ 「VPN を有効にする」チェックボックスにチェックを入れます。
- ④ 「IKEv2」ラジオボタンをクリックします。IKEv2 は IKEv1 と比べて、攻撃に対する復元性の向上、さまざまなデバイスとの相互接続性の向上、プロトコルのオーバーヘッドの減少、鍵再生時間の短縮など、性能面の優位性があります。なお、IKEv2 と IKEv1 の間に相互接続性はありせん。
- ⑤ 「トンネル IP」テキストボックスに製品の WAN 側インターフェースの IP アドレスを入力します。本書では、表 2 のとおり、**192.0.2.1** を使用しています。
- ⑥ 「トンネルマスク」テキストボックスに製品の WAN 側インターフェースのサブネットマスクを入力し



ます。本書では、表 2 のとおり、**255.255.255.0** を使用しています。

- ⑦ 「リモートピアアドレス」テキストボックスにリモートサイトの製品の WAN 側インターフェースの IP アドレスを入力します。本書では、表 2 のとおり、**192.0.2.2** を使用しています。
- ⑧ 「事前共有鍵」テキストボックスにリモートサイトの製品と共通の、IPsec 暗号化用のパスフレーズを入力します。本書では、表 2 のとおり、**passphrase** を使用しています。
- ⑨ 「リモートサブネット」テキストボックスにリモートサイトの LAN 側インターフェースのネットワークアドレスとサブネットマスクを入力し、「+」ボタンをクリックします。複数のリモートサブネットがある場合は、同様の手順を繰り返します。ここで入力したリモートサブネットは、IPsec-VPN トンネルをネクストホップとしたスタティックルートとしてルーティングテーブルに追加されます。また、リモートサブネット宛のトラフィックは、NAT されずに送出されます。本書では、表 2 のとおり、**10.10.10.128/25** を使用しています。
- ⑩ 「適用する」ボタンをクリックします。
- ⑪ 「ダッシュボード」リンクラベルをクリックします。



ゾーン ボタン 1 VPN コンテンツセキュリティ スタティックNAT

仮想プライベートネットワーク 11 ダッシュボード

VPNは仮想的なポイントツーポイントコネクションを作成します。サイトツーサイトVPNはインターネットのようなパブリックネットワーク上で複数拠点間をセキュアに接続します。DMVPNはすべての対象となるエンドポイントにおいて事前設定を必要とせず、動的なメッシュ型のVPNを作成できます。

2

② サイトツーサイト DMVPNスボーク

③ ④

⑤ ⑥ ⑦ ⑧ ⑨

⑩ ⑪

VPNを有効にする

鍵交換方法: IKEv1 IKEv2

トンネルIP*: 192.0.2.1

トンネルマスク*: 255.255.255.0

リモートピアアドレス*: 192.0.2.2

事前共有鍵*:

リモートサブネット*: 10.10.10.128 255.255.255.128 +

適用する

図 16 セキュリティの編集 (VPN)

(3) IPsec-VPN トンネルが確立していることを確認します。

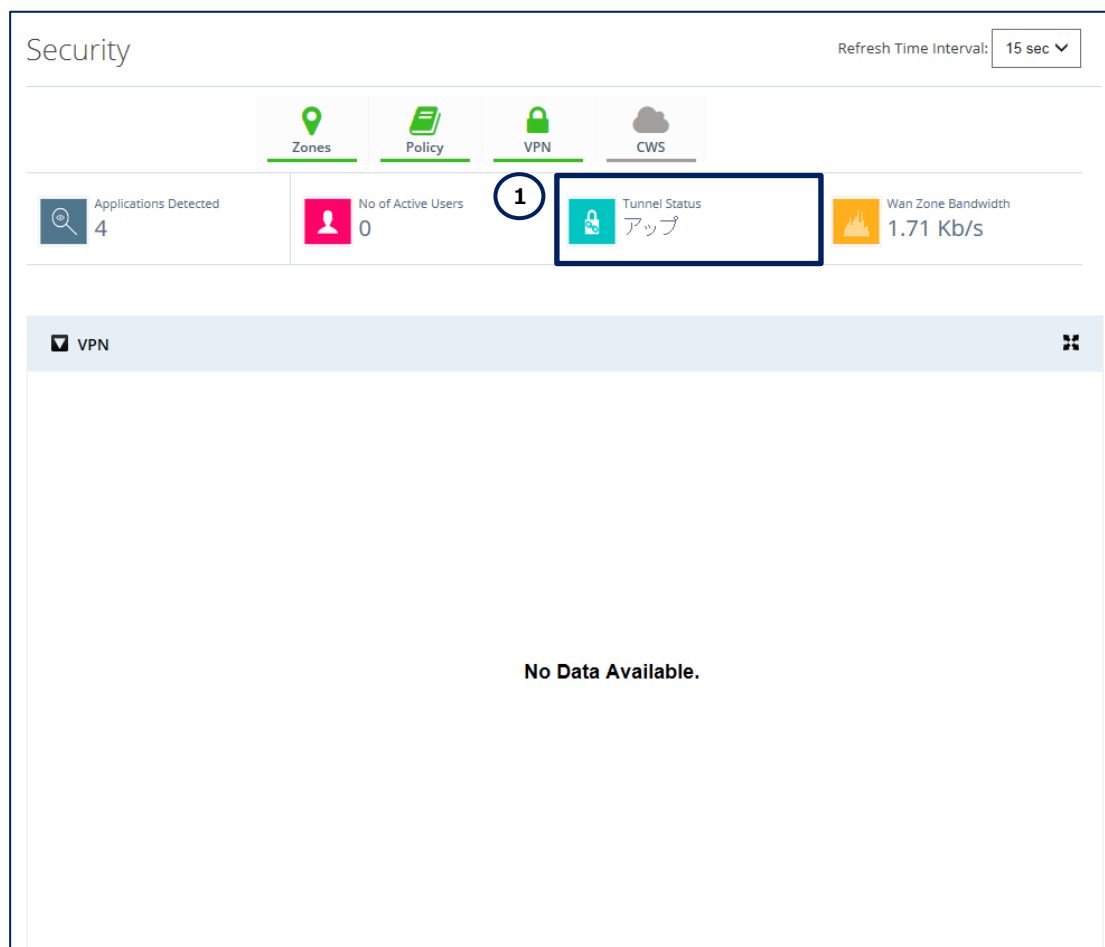


図 17 ダッシュボード（セキュリティ）

(4) IPsec-VPN トンネルが正常に確立された場合、「VPN OK」LED が緑点灯します。なお、複数の IPsec-VPN トンネルを設定している場合、いずれかの IPsec-VPN トンネルが正常に確立されていれば、他の IPsec-VPN トンネルの状態に係わらず「VPN OK」LED は緑点灯します。



図 18 VPN OK LED（緑点灯）（C841M-8X-JAIS/K9 の場合）

3.4 ポリシーの設定

Cisco 841M J シリーズの IPsec-VPN は、ルーティングベースの VPN です。製品を通過するトラフィックが IPsec-VPN トンネルを使用するかどうかは、ポリシーではなく、ルーティングテーブルのエントリによって決定されます。ただし、トラフィックが IPsec-VPN トンネルを通過できるかどうかは、ポリシーによって決定されます。ここでは、リモートサイト宛のすべてのトラフィックが IPsec-VPN トンネルを通過できるように、ポリシ



ーを設定します。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。



図 19 CCP Express のホーム（セキュリティ）

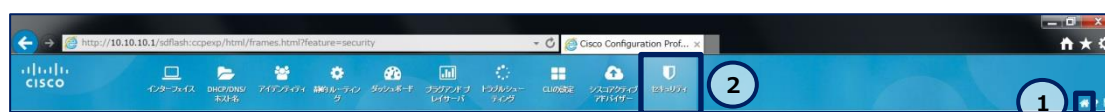


図 20 CCP Express のショートカット（ホームとセキュリティ）

(2) ポリシーを追加します。

- ① 「ポリシー」タブをクリックします。
- ② 「追加」ボタンをクリックします。




ポリシー名	説明	ユーザー	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
LAN-WAN ポリシー										
↓ Web	-	Any	Any	Any	Any	Any	http	Any	許可	
↓ Others	-	Any	Any	Any	Any	Any	https, smtp, ...	Any	許可	

図 21 ポリシーの編集

(3) 既定の LAN ゾーンから既定の VPN ゾーンに向かうトラフィックに対するポリシーを設定します。

- ① 「ポリシー名」テキストボックスにポリシー名を入力します。
- ② 「送信元ゾーン」ドロップダウンリストで **LAN** を選択します。
- ③ 「宛先ゾーン」ドロップダウンリストで **VPN** を選択します。
- ④ 「セーブ」ボタンをクリックします。



セキュリティポリシーウィザード

ポリシー名: **LANtoVPN** ポリシーの説明: アクション: 許可

送信元ゾーン: **LAN** 宛先ゾーン: **VPN**

ネットワーク アプリケーション ポート ドメインフィルタリング ユーザグループ

送信元ネットワーク: Any

宛先ネットワーク: Any

送信元ネットワークアドレス: 宛先ネットワークアドレス:

例: 192.168.0.0, IP /サブネット: 192.168.0.0/8 または範囲: 192.168.0.0 - 192.200.0.0

セーブ キャンセル

図 22 ポリシーの編集（詳細）

設定は以上です。Ping 等を使用して、ローカルサイトの PC がリモートサイトの PC とインターネットに接続できることを確認してください。



4. 設定ファイル

本書で追加または変更される設定（クイックスタートガイドを使用した設定との差分）は、以下のとおりです。

```
001: object-group network lantovpn_dst_net
002: any
003: object-group network lantovpn_src_net
004: any
005: object-group service lantovpn_svc
006: ip
007: object-group network local_lan_subnets
008: 10.10.10.0 255.255.255.128
009: object-group network vpn_remote_subnets
010: 10.10.10.128 255.255.255.128
011: crypto ikev2 authorization policy authpolicy1
012: route set interface GigabitEthernet0/0
013: route set interface Vlan1
014: crypto ikev2 proposal default
015: encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
016: integrity sha512 sha384 sha256 sha1 md5
017: group 5 2
018: crypto ikev2 policy default
019: match fvrnf any
020: proposal default
021: crypto ikev2 keyring key
022: peer SITE-KEY
023: address 192.0.2.2
024: identity address 192.0.2.2
025: pre-shared-key passphrase
026: crypto ikev2 profile prof
027: match identity remote address 192.0.2.2 255.255.255.255
028: authentication remote pre-share
029: authentication local pre-share
030: keyring local key
031: aaa authorization group psk list local-group-author-list authpolicy1
```



```
032: crypto ikev2 dpd 10 2 periodic
033: class-map type inspect match-all lantovpn
034: match access-group name lantovpn_acl
035: policy-map type inspect LAN-WAN-POLICY
036: class type inspect INTERNAL_DOMAIN_FILTER
037: inspect
038: class class-default
039: drop log
040: policy-map type inspect LAN-VPN-POLICY
041: class type inspect lantovpn
042: inspect
043: class type inspect INTERNAL_DOMAIN_FILTER
044: inspect
045: zone security VPN
046: zone-pair security LAN-VPN source LAN destination VPN
047: service-policy type inspect LAN-VPN-POLICY
048: crypto ipsec transform-set test_trans esp-aes esp-sha-hmac
049: mode tunnel
050: crypto ipsec profile test_profile
051: set transform-set test_trans
052: set ikev2-profile prof
053: interface Tunnel0
054: ip address 192.0.2.1 255.255.255.0
055: zone-member security VPN
056: tunnel source Dialer1
057: tunnel mode ipsec ipv4
058: tunnel destination 192.0.2.2
059: tunnel protection ipsec profile test_profile
060: interface GigabitEthernet0/0
061: zone-member security LAN
062: ip tcp adjust-mss 1412
063: interface Vlan1
064: zone-member security LAN
065: ip tcp adjust-mss 1412
066: ip route 10.10.10.128 255.255.255.128 Tunnel0
067: ip route 192.0.2.2 255.255.255.255 Dialer1
```



```
068: ip access-list extended INTRANET-WHITELIST
069: permit ip any 10.10.10.128 0.0.0.127
070: ip access-list extended lantovpn_acl
071: permit object-group lantovpn_svc object-group lantovpn_src_net object-group lantovpn_dst_net
072: ip access-list extended nat-list
073: deny ip object-group local_lan_subnets object-group vpn_remote_subnets
```

お問い合わせ

Q 製品のご購入に関するお問い合わせ

<https://info-networld.smartseminar.jp/public/application/add/152>

Q ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q 製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

本書に記載されているロゴ、会社名、製品名、サービス名は、一般に各社の登録商標または商標です。
本書では、®、™、©マークを省略しています。

www.networld.co.jp

株式会社ネットワーク

