

# H3C MSRルーター

## Ipsec VPN設定ガイド

New h3c Technologies Co.,Ltd.<http://www.h3c.com>

Document version: 6W103-20200507

Product version: R5426P02

**Copyright © 2020, New H3C Technologies Co., Ltd. and its licensors**

## **All rights reserved**

本書のいかなる部分も、New H3C Technologies Co., Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または更新することはできません。

## **商標**

New H3C Technologies Co., Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の商標または登録商標です。

## **注意**

本書に記載されている情報は、予告なしに変更されることがあります。このドキュメントに記載されているすべての内容(記述、情報、推奨事項を含む)は、正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提供されています。H3Cは、本書に含まれている技術的または編集上の誤りまたは脱落に対して責任を負わないものとします。

## 内容

はじめに.....	1
前提条件 .....	1
使用されているソフトウェアのバージョン .....	1
例:メインモードIPsec VPNの設定.....	2
ネットワーク構成.....	2
解析.....	2
制限事項およびガイドライン .....	2
手順.....	3
ルータAの設定 .....	3
ルータBの設定 .....	8
設定の確認.....	13
例:アグレッシブモードIPsec VPNの設定 .....	14
ネットワーク構成.....	14
解析.....	14
制限事項およびガイドライン .....	14
手順.....	15
ルータAの設定 .....	15
ルータBの設定 .....	20
設定の確認.....	24

# はじめに

次に、次のモードでのIKE交換に基づくIPsec VPNの設定例を示します。

- **メインモード:**本社と支店のゲートウェイルータの両方のWANインターフェイスで固定パブリックアドレスが使用されているシナリオに適用できます。
- **アグレッシブモード:**本社または支店のゲートウェイルータ上のWANインターフェイスがダイナミックパブリックアドレス(DHCPによって割り当てられたIPアドレスなど)を使用するシナリオに適用されます。

実際のネットワークに合わせてIPsec VPNを設定するには、このドキュメントのメインモードまたはアグレッシブモードの設定例を参照してください。

## 前提条件

この例の手順と情報は、ルータのソフトウェアバージョンまたはハードウェアバージョンによって若干異なる場合があります。

設定例はラボ環境で作成および検証され、すべてのデバイスは工場出荷時のデフォルト設定で起動されました。ライブネットワークで作業している場合は、すべてのコマンドがネットワークに与える潜在的な影響を理解していることを確認してください。

次の情報は、IPsec VPNIに関する基本的な知識があることを前提としています。

## 使用されているソフトウェアのバージョン

設定例は、MSR 3600-10 HIルータのリリース6728P22およびMSR 830-28-G-DPルータのリリース6728P22で作成および検証されています。

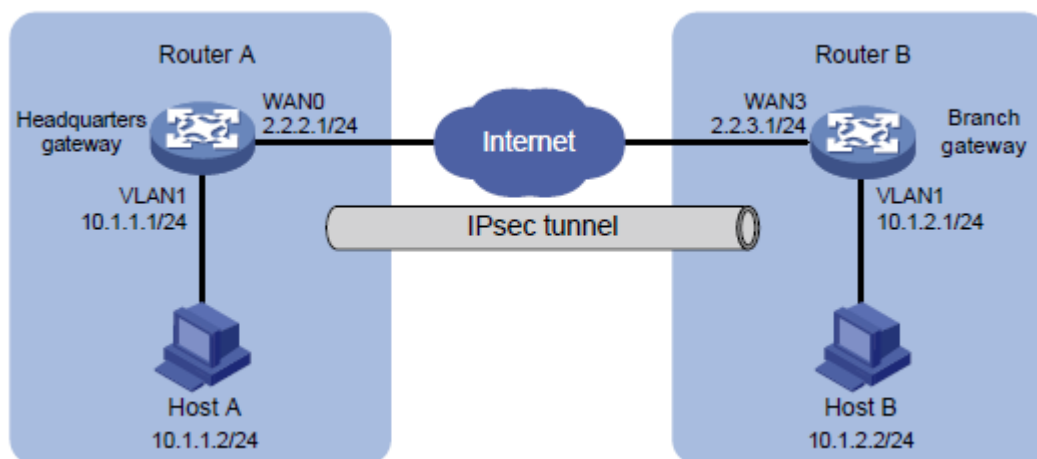
# 例:メインモードIPsec VPNの設定

## ネットワーク構成

図1に示すように、本社のゲートウェイルータAと支店のゲートウェイルータBは、それぞれ固定のパブリックアドレスを持つ単一のWANインターフェイスを使用してインターネットに接続します。本社と支店は、インターネットを介して相互に通信します。本社と支店間のデータフローを保護するには、ゲートウェイルータ間にIPsecトンネルを確立します。ネットワークを次のように設定します。

- 認証に事前共有キー**123456 TESTplat&!**を使用するように、ルータAとルータBを設定します。
- カプセル化モードをトンネルに、セキュリティプロトコルをESPに指定します。
- 暗号化アルゴリズムを3DES-CBCに、認証アルゴリズムをMD5に指定します。

図1 ネットワークダイアグラム



## 解析

IPsec VPNを設定するには、ルータAおよびルータBで次の設定を完了します。

1. WANおよびLANの基本的な設定を行います。
  - a. 各ルータのWANインターフェイスのIPアドレスとゲートウェイを指定します。
  - b. 各ルータのVLAN 1のデフォルトIPアドレスを変更します。
2. IPsecポリシーを追加します。

各ルータのWANインターフェイスは固定IPアドレスを使用してインターネットに接続するため、フェーズ1のIKEネゴシエーションにメインモードを使用するようにIPsecポリシーを設定します。

## 制限事項およびガイドライン

VLAN 1のデフォルトIPアドレスを変更すると、Web接続が失敗します。変更したIPアドレスを使用して、Webインターフェイスに再度ログインする必要があります。

ネットワークでデュアルWANまたはマルチWANアクセスを使用している場合は、各ルータにスタティックルートを設定して、ピア内部ネットワーク宛てのトラフィックをIPsecポリシーで指定されたWANインターフェイスに転送します。この例では、ルータはシングルWANアクセスを使用します。スタティックルートの設定は必要ありません。ルータはデフォルトルートを生成し、すべてのトラフィックを出力ゲートウェイに転送します。

IPsecトンネルの両側で、同じ事前共有キー、セキュリティプロトコル、暗号化アルゴリズム、認証アルゴリズム、およびカプセル化モードが使用されていることを確認します。

## 手順

### ルータAの設定

#### VLAN 1のIPアドレスの変更

#VLAN 1のVLANインターフェイスIPアドレスを10.1.1.1/24に変更します。

1. Webインターフェイスにログインします。ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. VLAN 1の**Operation**カラムで**Edit**アイコンをクリックします。
3. **Interface IP address**フィールドに、10.1.1.1と入力します。
4. **Subnet mask**フィールドに、255.255.255.0と入力します。
5. その他のパラメータには既定の設定を使用し、**Apply**をクリックします。

図2 VLAN 1の変更

Field	Value	Range/Default
VLAN ID *	1	(1-4094)
Interface IP address *	10.1.1.1	
Subnet mask *	255.255.255.0	
TCP MSS	1280	(128-1460bytes)
MTU	1500	(46-1500bytes)
Enable DHCP	<input checked="" type="checkbox"/>	
Start address of pool	10.1.1.1	
End address of pool	10.1.1.254	
Forbidden address ?	10.1.1.1	
Gateway address	10.1.1.1	
DNS1	10.1.1.1	
DNS2		
Address lease	1440	minute(range:1-11520,default:1440)

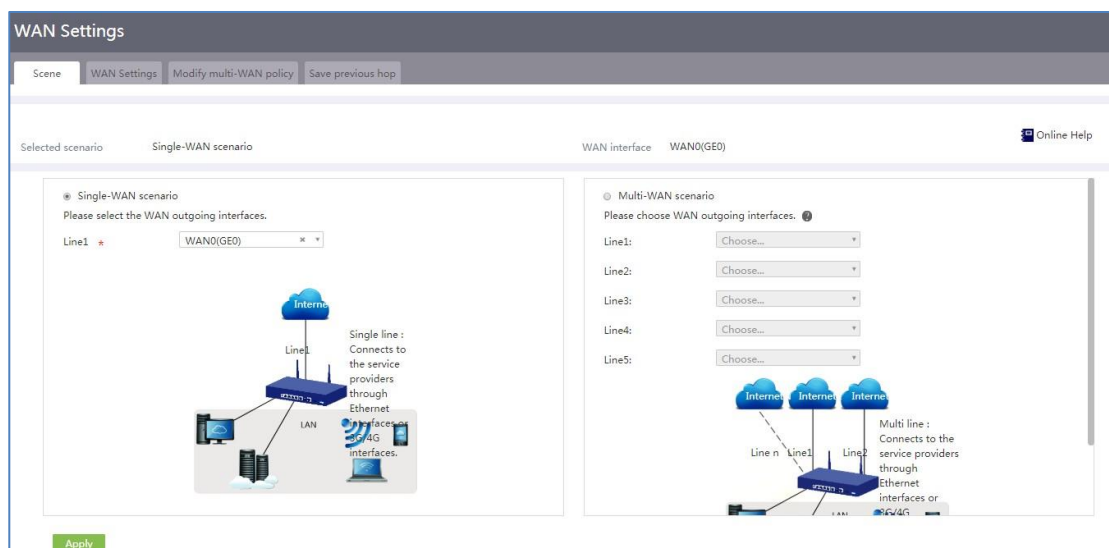
#### インターネットに接続するためのWANインターフェイス(WAN0)の設定

# 固定IPアドレスを使用して、単一のWANインターフェイスを設定します。

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。

- 表示された**Scene**ページで、**Single-WAN scenario**を選択し、**Line1**フィールドで**WAN0(GE0)**を選択します。
- Apply**をクリックします。

図3 WAN構成のシナリオ



- WAN Settings**タブをクリックします。
- WAN0(GE0)の**Operation**カラムにある**Edit**アイコンをクリックします。
- Connection mode**フィールドで、**Fixed IP**を選択します。
- IP address**フィールドに、2.2.2.1と入力します。
- Subnet mask**フィールドに、255.255.255.0と入力します。
- Gateway**フィールドに、2.2.2.254と入力します。
- その他のパラメータには既定の設定を使用し、**Apply**をクリックします。

図4 WAN設定の変更

Modify WAN configuration

WAN interface	WAN0(GE0)
Connection mode	Fixed IP
IP address *	2.2.2.1
Subnet mask *	255.255.255.0
Gateway	2.2.2.254
DNS1	
DNS2	
MAC	<input checked="" type="radio"/> Using the interface to the default MAC( 1C-AB-34-C7-CF-34 ) <input type="radio"/> Using the specified MAC
NAT function	Enable
	<input type="checkbox"/> Use Address Pool for Translation Please Choose Address Pool
TCP MSS	1280 (128-1610bytes)
MTU	1500 (46-1650bytes)
Link detection	Disable
Detection address	
Detection interval	(1-10s)

Apply Cancel

## IPsecポリシーの構成

#ネットワークモードを本社ゲートウェイとして指定し、IKEネゴシエーションモードをメインモードとして指定します。

1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **Add**をクリックします。
3. 開いたページで、次のパラメータを設定します。
  - **map1**という名前を指定します。
  - **Interface**フィールドで**WAN0(GE0)**を選択します。
  - **Network mode**フィールドで**Headquarters gateway**を選択します。
  - **Preshared key**フィールドに**123456 TESTplat&!**と入力します。



図5 IPsecポリシーの追加

4. **Show advanced settings**をクリックします。表示されたページで、次のパラメータを構成します。

- **Negotiation mode**フィールドで、**Main mode**を選択します。
- **Local ID**フィールドで、**IP address**を選択し、2.2.2.1と入力します。
- **DPD**フィールドで、**Enable**を選択し、DPD試行間隔を30に指定します。  
この機能は、デフォルトではディセーブルになっています。IPsecトンネルの可用性をタイムリーに監視するには、この機能をイネーブルにします。
- **Algorithm suite**フィールドで、**Customize**を選択します。
- **Authentication algorithm**フィールドで、**MD5**を選択します。
- **Encryption algorithm**フィールドで、**3DES-CBC**を選択します。
- その他のパラメータには、デフォルト設定を使用します。

図6 IKEの詳細設定

5. **IPsec settings**タブをクリックし、次のパラメータを設定します。
  - **Algorithm combination**フィールドで、**Customize**を選択します。
  - **Security protocol**フィールドで、**ESP**を選択します。
  - **ESP authentication algorithm**フィールドで、**MD5**を選択します。
  - **ESP encryption algorithm**フィールドで、**3DES-CBC**を選択します。
  - **Encapsulation mode**フィールドで、**Tunnel**を選択します。
  - その他のパラメータには、デフォルト設定を使用します。

図7 IPsecの詳細設定

Advanced settings	IKE settings	IPsec settings
Algorithm combination	Customize ▼	
Security protocol *	ESP ▼	
ESP authentication algorithm *	MD5 ▼	
ESP encryption algorithm *	3DES-CBC ▼	
Encapsulation mode *	<input type="radio"/> Transport <input checked="" type="radio"/> Tunnel	
PFS	▼	
Time-based SA lifetime	3600	seconds (180-604800. Default: 3600)
Traffic-based SA lifetime	1843200	Kilobytes (2560-4294967295. Default: 1843200)
<a href="#">Back to basic settings</a>		

6. **Back to basic settings**をクリックして、**Add IPsec Policy**ページに戻ります。
7. **Apply**をクリックします。

# ルータBの設定

## VLAN 1のIPアドレスの変更

#VLAN 1のVLANインターフェイスIPアドレスを10.1.2.1/24に変更します。

1. Webインターフェイスにログインします。
2. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
3. VLAN 1の**Operation**カラムで**Edit**アイコンをクリックします。
4. **Interface IP address**フィールドに、10.1.2.1と入力します。
5. **Subnet mask**フィールドに、255.255.255.0と入力します。
6. その他のパラメータには既定の設定を使用し、**Apply**をクリックします。

図8 VLAN 1の変更

The screenshot shows a 'Modify LAN' configuration window with the following fields and values:

VLAN ID *	1	(1-4094)
Interface IP address *	10.1.2.1	
Subnet mask *	255.255.255.0	
TCP MSS	1280	(128-1460bytes)
MTU	1500	(46-1500bytes)
<input checked="" type="checkbox"/> Enable DHCP		
Start address of pool	10.1.2.1	
End address of pool	10.1.2.254	
Forbidden address ?	10.1.2.1	
Gateway address	10.1.2.1	
DNS1	10.1.2.1	
DNS2		
Address lease	1440	minute(range:1-11520,default:1440)

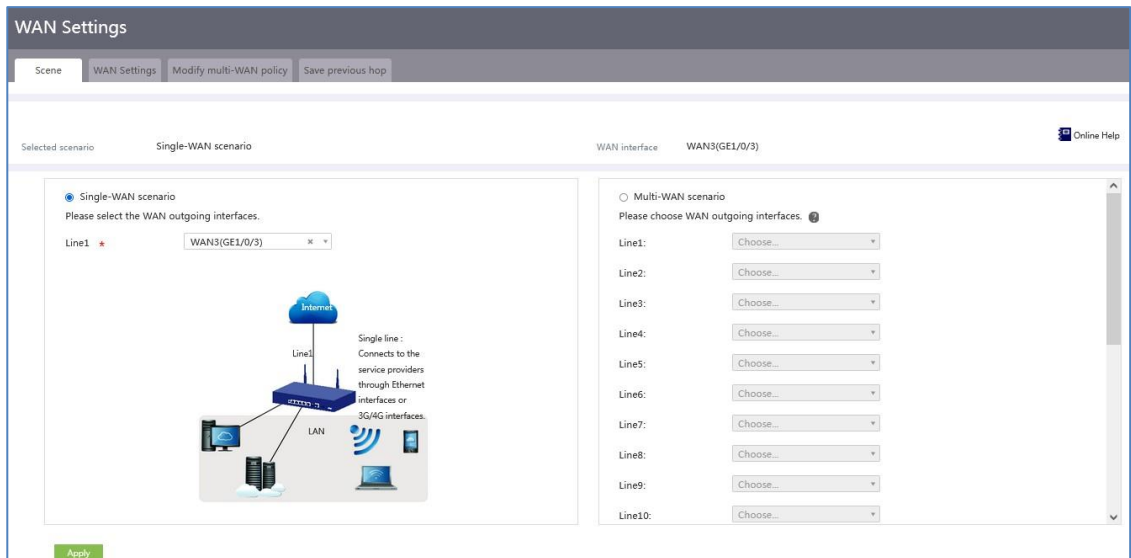
Buttons: Apply (green), Cancel (red)

## インターネットに接続するためのWANインターフェイス(WAN3)の設定

#固定IPアドレスを使用して、単一のWANインターフェイスを設定します。

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。
2. 表示された**Scene**ページで、**Single-WAN scenario**を選択し、次に**WAN3(GE1/0/3)**を選択します。のフィールドに表示されます。
3. **Apply**をクリックします。

図9 WANシナリオの設定



4. WAN Settingsタブをクリックします。
5. WAN3(GE1/0/3)のOperationカラムにあるEditアイコンをクリックします。
6. Connection modeフィールドで、Fixed IPを選択します。
7. IP addressフィールドに、2.2.3.1と入力します。
8. Subnet maskフィールドに、255.255.255.0と入力します。
9. Gatewayフィールドに、2.2.3.254と入力します。
10. その他のパラメータには既定の設定を使用し、Applyをクリックします。

図10 WAN設定の変更

Modify WAN configuration

WAN interface: WAN3(GE1/0/3)

Connection mode: Fixed IP

IP address \*: 2.2.3.1

Subnet mask \*: 255.255.255.0

Gateway: 2.2.3.254

DNS1: 114.114.114.114

DNS2: 223.5.5.5

MAC:
 

- Using the interface to the default MAC( EC-DA-59-4E-48-6D )
- Using the specified MAC

NAT function: Enable
 

- Use Address Pool for Translation

TCP MSS: 1280 (128-1610bytes)

MTU: 1500 (46-1650bytes)

Link detection: Disable

Detection address:

Detection interval: (1-10s)

Apply Cancel

## IPsecポリシーの構成

#ネットワークモードをブランチゲートウェイとして指定し、IKEネゴシエーションモードをメインモードとして指定します。


1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **Add**をクリックします。
3. 開いたページで、次のパラメータを設定します。
  - **map1**という名前を指定します。
  - **Interface**フィールドで**WAN3(GE1/0/3)**を選択します。
  - **Network mode**フィールドで**Branch gateway**を選択し、ピアゲートウェイアドレスを2.2.2.1に指定します。
  - **Preshared key**フィールドに**123456 TESTplat&!**と入力します。
  - **Protected data flows**領域で、保護するプロトコルとして**IP**を選択し、**Local subnet/mask**フィールドに**10.1.2.0/255.255.255.0**、**Peer subnet/mask**フィールドに**10.1.1.0/255.255.255.0**と入力して、アイコン  をクリックします。

図11 IPsecポリシーの追加

Add IPsec Policy
✕

---

**Add IPsec Policy**

Name \*  (1-33 chars)

Interface \*

Network mode  Branch gateway ?  Headquarters gateway ?

Peer gateway address \*  (Example: 1.1.1.1)

Authentication method

Preshared key \*  (1-128 chars)

**Protected data flows \***

ID	Protocol	Local subnet/mask	Local port	Peer subnet/mask	Peer port
1	IP	10.1.2.0/255.255.255.0		10.1.1.0/255.255.255.0	🗑
<input type="text"/>	<input type="text" value="IP"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>

[Show advanced settings...](#)

4. **Show advanced settings**をクリックします。表示されたページで、次のパラメータを構成します。

- **Negotiation mode**フィールドで、**Main mode**を選択します。
- **Local ID**フィールドで、**IP address**を選択し、2.2.3.1と入力します。
- **Remote ID**フィールドで、**IP address**を選択し、2.2.2.1と入力します。
- **DPD**フィールドで、**Enable**を選択し、DPD試行間隔を30に指定します。
- **Algorithm suite**フィールドで、**Customize**を選択します。
- **Authentication algorithm**フィールドで、**MD5**を選択します。
- **Encryption algorithm**フィールドで、**3DES-CBC**を選択します。
- その他のパラメータには、デフォルト設定を使用します。

図12 IKEの詳細設定

Advanced settings	IKE settings	IPsec settings
Negotiation mode	Main mode ▼	
Local ID	IP address ▼	2.2.3.1 (Example: 1.1.1.1)
Remote ID *	IP address ▼	2.2.2.1 (Example: 1.1.1.1)
DPD	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
	DPD retry interval *	30 seconds (1-300)
Algorithm suite	Customize ▼	
Authentication algorithm *	MD5 ▼	
Encryption algorithm *	3DES-CBC ▼	
PFS *	DH group 1 ▼	
SA lifetime	86400 seconds (60-604800. Default: 86400.)	
<a href="#">Back to basic settings</a>		

5. IPsec settingsタブをクリックし、次のパラメータを設定します。
- **Algorithm combination**フィールドで、**Customize**を選択します。
  - **Security protocol**フィールドで、**ESP**を選択します。
  - **ESP authentication algorithm**フィールドで、**MD5**を選択します。
  - **ESP encryption algorithm**フィールドで、**3DES-CBC**を選択します。
  - **Encapsulation mode**フィールドで、**Tunnel**を選択します。
  - その他のパラメータには、デフォルト設定を使用します。

図13 IPsecの詳細設定の構成

Advanced settings	IKE settings	IPsec settings
Algorithm combination	Customize ▼	
Security protocol *	ESP ▼	
ESP authentication algorithm *	MD5 ▼	
ESP encryption algorithm *	3DES-CBC ▼	
Encapsulation mode *	<input type="radio"/> Transport <input checked="" type="radio"/> Tunnel	
PFS	▼	
Time-based SA lifetime	3600	seconds (180-604800. Default: 3600)
Traffic-based SA lifetime	1843200	Kilobytes (2560-4294967295. Default: 1843200)
Trigger mode	Flow trigger ▼	
<a href="#">Back to basic settings</a>		

6. **Back to basic settings**をクリックして、**Add IPsec Policy**ページに戻ります。
7. **Apply**をクリックします。

## 設定の確認

1. ホストAがホストBに対して正常にpingできることを確認します。  
C:\Users\abc>ping 10.1.2.2  
Ping 10.1.2.2 (10.1.2.2): 56 data bytes, press CTRL\_C to break  
56 bytes from 10.1.2.2: icmp\_seq=0 ttl=254 time=2.137 ms  
56 bytes from 10.1.2.2: icmp\_seq=1 ttl=254 time=2.051 ms  
56 bytes from 10.1.2.2: icmp\_seq=2 ttl=254 time=1.996 ms  
56 bytes from 10.1.2.2: icmp\_seq=3 ttl=254 time=1.963 ms  
56 bytes from 10.1.2.2: icmp\_seq=4 ttl=254 time=1.991 ms  
--- Ping statistics for 10.1.2.2 ---  
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss  
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms  
C:\Users\abc>
2. Webインターフェイスで**Virtual Network > IPsec VPN > Monitor Information**をクリックして、次のことを確認します。  
IPsecトンネルが正常に確立されます。Status Activeは、IPsecトンネルが正常に確立されたことを示します。



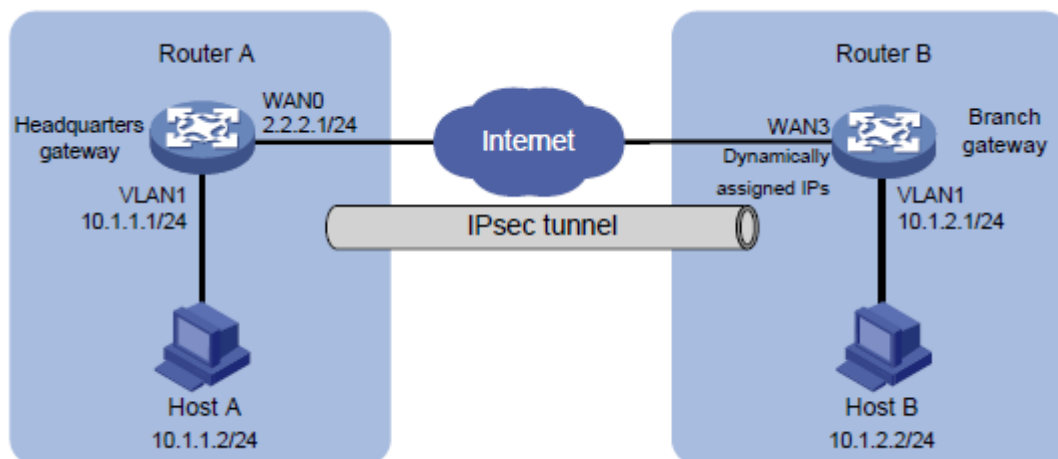
# 例:アグレッシブモードIPsec VPNの設定

## ネットワーク構成

図14に示すように、本社ゲートウェイルータAは、固定パブリックアドレスを持つ単一のWANインターフェイスを使用してインターネットに接続します。支店ゲートウェイルータBは、DHCPによって割り当てられたIPアドレスを使用してインターネットに接続します。本社と支店は、インターネットを介して相互に通信します。本社と支店間のデータフローを保護するには、ルータ間にIPsecトンネルを確立します。ネットワークを次のように設定します。

- 認証に事前共有キー**123456 TESTplat&!**を使用するように、ルータAとルータBを設定します。
- カプセル化モードをトンネルに、セキュリティプロトコルをESPに指定します。
- 暗号化アルゴリズムを3DES-CBCに、認証アルゴリズムをMD5に指定します。

図14 ネットワークダイアグラム



## 解析

IPsec VPNを設定するには、ルータAおよびルータBで次の設定を完了します。

1. WANおよびLANの基本的な設定を行います。
  - a. 各ルータのWANインターフェイスのIPアドレスとゲートウェイを指定します。
  - b. 各ルータのVLAN 1のデフォルトIPアドレスを変更します。
2. IPsecポリシーを追加します。

IPsecトンネルの片側(ルータB)はDHCPで割り当てられたIPアドレスを使用するため、IPsecトンネルを正常に設定するには、フェーズ1のIKEネゴシエーションにアグレッシブモードを使用するようにIPsecポリシーを設定します。

## 制限事項およびガイドライン

VLAN 1のデフォルトIPアドレスを変更すると、Web接続が失敗します。変更したIPアドレスを使用して、Webインターフェイスに再度ログインする必要があります。

ネットワークでデュアルWANまたはマルチWANアクセスを使用している場合は、各ルータにスタティックルートを設定して、ピア内部ネットワーク宛てのトラフィックをIPsecポリシーで指定されたWANインターフ

エイズに転送します。この例では、ルータはシングルWANアクセスを使用します。スタティックルートの設定は必要ありません。ルータはデフォルトルートを生成し、すべてのトラフィックを出力ゲートウェイに転送します。

IPsecトンネルの両側で、同じ事前共有キー、セキュリティプロトコル、暗号化アルゴリズム、認証アルゴリズム、およびカプセル化モードが使用されていることを確認します。

## 手順

### ルータAの設定

#### VLAN 1のIPアドレスの変更

#VLAN 1のVLANインターフェイスIPアドレスを10.1.1.1/24に変更します。

1. Webインターフェイスにログインします。ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. VLAN 1の**Operation**カラムで**Edit**アイコンをクリックします。
3. **Interface IP address**フィールドに、10.1.1.1と入力します。
4. **Subnet mask**フィールドに、255.255.255.0と入力します。
5. その他のパラメータには既定の設定を使用し、**Apply**をクリックします。

図15 VLAN 1の変更

The screenshot shows a 'Modify LAN' configuration window with the following fields and values:

Field	Value	Range/Unit
VLAN ID *	1	(1-4094)
Interface IP address *	10.1.1.1	
Subnet mask *	255.255.255.0	
TCP MSS	1280	(128-1460bytes)
MTU	1500	(46-1500bytes)
<input checked="" type="checkbox"/> Enable DHCP		
Start address of pool	10.1.1.1	
End address of pool	10.1.1.254	
Forbidden address ?	10.1.1.1	
Gateway address	10.1.1.1	
DNS1	10.1.1.1	
DNS2		
Address lease	1440	minute(range:1-11520,default:1440)

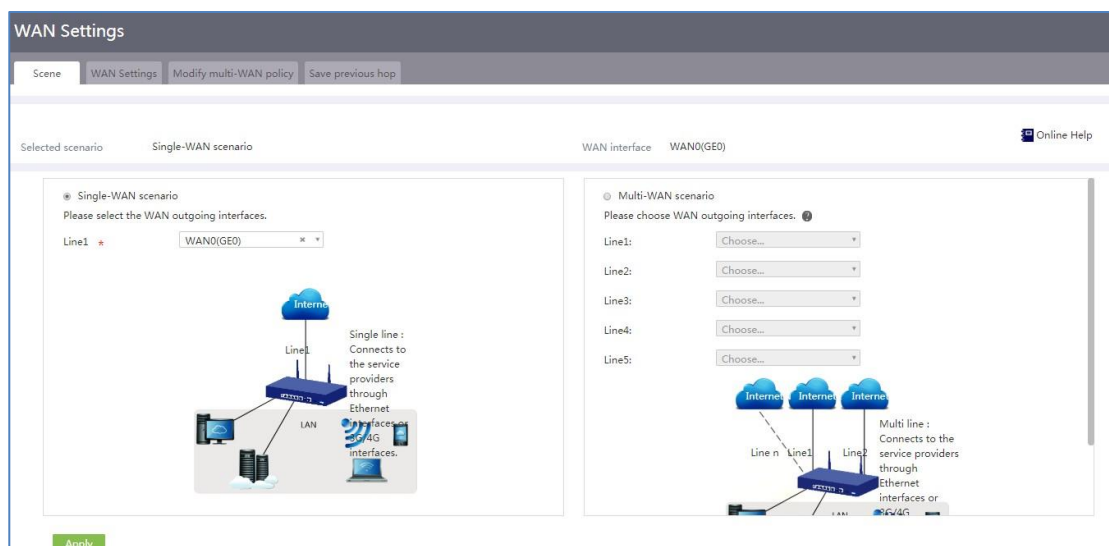
Buttons: Apply (green), Cancel (red)

## インターネットに接続するためのWANインターフェイス(WAN 0)の設定

# 固定IPアドレスを使用して、単一のWANインターフェイスを設定します。

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。
2. 表示された**Scene**ページで、**Single-WAN scenario**を選択し、**Line1**フィールドで**WAN0(GE0)**を選択します。
3. **Apply**をクリックします。

図16 WAN構成のシナリオ



4. **WAN Settings**タブをクリックします。
5. **WAN0(GE0)**の**Operation**カラムにある**Edit**アイコンをクリックします。
6. **Connection mode**フィールドで、**Fixed IP**を選択します。
7. **IP address**フィールドに、2.2.2.1と入力します。
8. **Subnet mask**フィールドに、255.255.255.0と入力します。
9. **Gateway**フィールドに、2.2.2.254と入力します。
10. その他のパラメータには既定の設定を使用し、**Apply**をクリックします。

図17 WAN設定の変更

WAN interface	WAN0(GE0)	
Connection mode	Fixed IP ▼	
IP address *	2.2.2.1	
Subnet mask *	255.255.255.0	
Gateway	2.2.2.254	
DNS1		
DNS2		
MAC	<input checked="" type="radio"/> Using the interface to the default MAC( 1C-AB-34-C7-CF-34 ) <input type="radio"/> Using the specified MAC <input type="text"/>	
NAT function	Enable ▼	
	<input type="checkbox"/> Use Address Pool for Translation	<input type="text" value="Please Choose Address Pool ▼"/>
TCP MSS	1280	(128-1610bytes)
MTU	1500	(46-1650bytes)
Link detection	Disable ▼	
Detection address	<input type="text"/>	
Detection interval	<input type="text"/>	(1-10s)

### IPsecポリシーの構成

# ネットワークモードを本社ゲートウェイとして指定し、IKEネゴシエーションモードをアグレッシブモードとして指定します。

1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **Add**をクリックします。
3. 開いたページで、次のパラメータを設定します。
  - **map1**という名前を指定します。
  - **Interface**フィールドで**WAN0(GE0)**を選択します。
  - **Network mode**フィールドで**Headquarters gateway**を選択します。
  - **Preshared key**フィールドに**123456 TESTplat&!**と入力します。

図18 IPsecポリシーの追加

4. **Show advanced settings**をクリックします。表示されたページで、次のパラメータを構成します。

- **Negotiation mode**フィールドで、**Aggressive mode**を選択します。
- **Local ID**フィールドで、**FQDN**を選択し、FQDN名(たとえば**www.test.com**を参照)。
- **DPD**フィールドで、**Enable**を選択し、DPD試行間隔を30に指定します。  
この機能は、デフォルトではディセーブルになっています。IPsecトンネルの可用性をタイムリーに監視するには、この機能をイネーブルにします。
- **Algorithm suite**フィールドで、**Customize**を選択します。
- **Authentication algorithm**フィールドで、**MD5**を選択します。
- **Encryption algorithm**フィールドで、**3DES-CBC**を選択します。
- その他のパラメータには、デフォルト設定を使用します。

図19 IKEの詳細設定

5. **IPsec settings**タブをクリックし、次のパラメータを設定します。

- **Algorithm combination**フィールドで、**Customize**を選択します。
- **Security protocol**フィールドで、**ESP**を選択します。
- **ESP authentication algorithm**フィールドで、**MD5**を選択します。
- **ESP encryption algorithm**フィールドで、**3DES-CBC**を選択します。
- **Encapsulation mode**フィールドで、**Tunnel**を選択します。
- その他のパラメータには、デフォルト設定を使用します。

図20 IPsecの詳細設定

Advanced settings	IKE settings	IPsec settings
Algorithm combination	Customize ▼	
Security protocol *	ESP ▼	
ESP authentication algorithm *	MD5 ▼	
ESP encryption algorithm *	3DES-CBC ▼	
Encapsulation mode *	<input type="radio"/> Transport <input checked="" type="radio"/> Tunnel	
PFS	▼	
Time-based SA lifetime	3600	seconds (180-604800, Default: 3600)
Traffic-based SA lifetime	1843200	Kilobytes (2560-4294967295, Default: 1843200)
<a href="#">Back to basic settings</a>		

6. **Back to basic settings**をクリックして、**Add IPsec Policy**ページに戻ります。
7. **Apply**をクリックします。

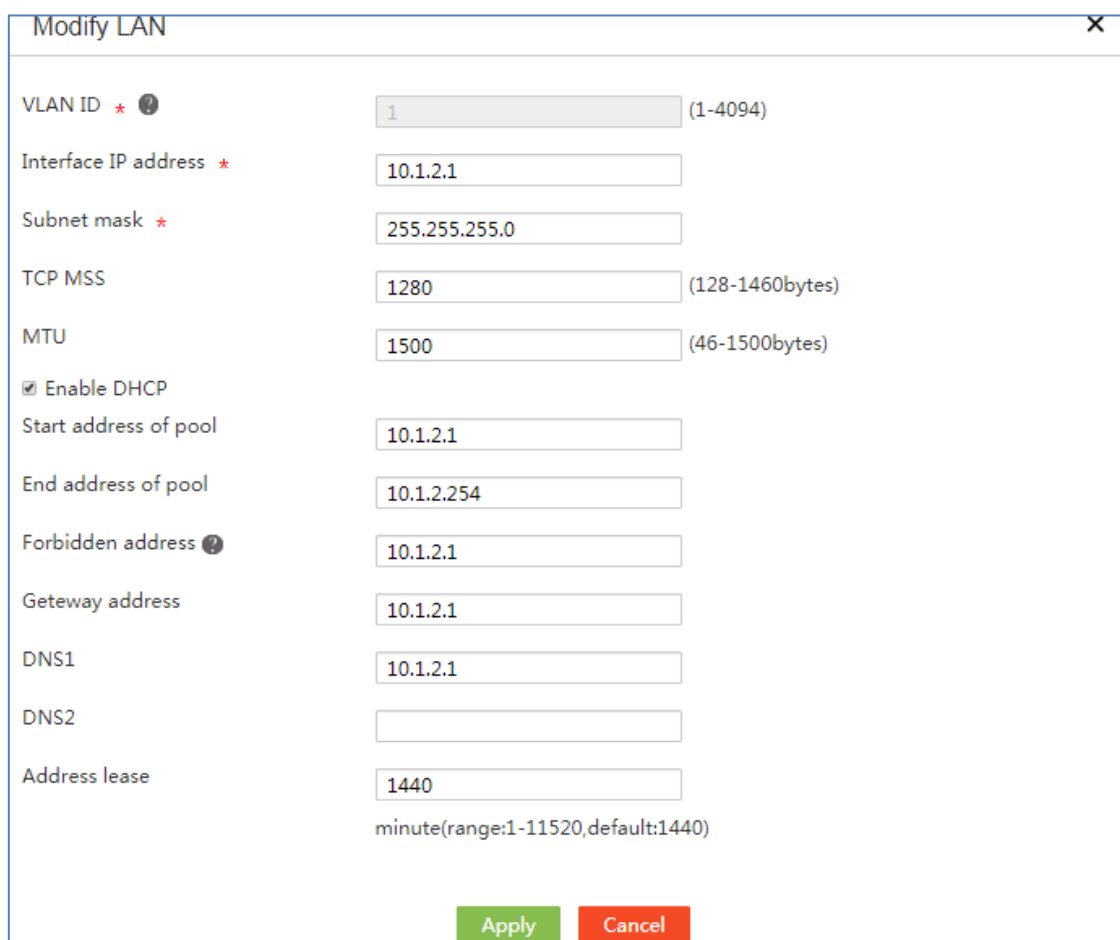
# ルータBの設定

## VLAN 1のIPアドレスの変更

#VLAN 1のVLANインターフェイスIPアドレスを10.1.2.1/24に変更します。

1. Webインターフェイスにログインします。
2. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
3. VLAN 1の**Operation**カラムで**Edit**アイコンをクリックします。
4. **Interface IP address**フィールドに、10.1.2.1と入力します。
5. **Subnet mask**フィールドに、255.255.255.0と入力します。
6. その他のパラメータには既定の設定を使用し、**Apply**をクリックします。

図21 VLAN 1の変更



VLAN ID *	1	(1-4094)
Interface IP address *	10.1.2.1	
Subnet mask *	255.255.255.0	
TCP MSS	1280	(128-1460bytes)
MTU	1500	(46-1500bytes)
<input checked="" type="checkbox"/> Enable DHCP		
Start address of pool	10.1.2.1	
End address of pool	10.1.2.254	
Forbidden address ?	10.1.2.1	
Geteway address	10.1.2.1	
DNS1	10.1.2.1	
DNS2		
Address lease	1440	minute(range:1-11520,default:1440)

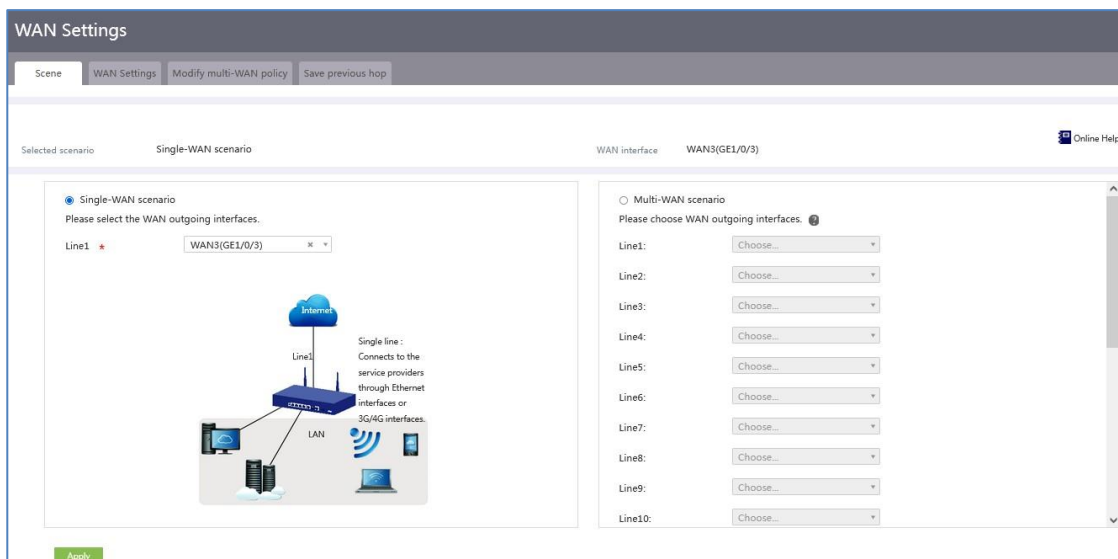
Apply Cancel

## インターネットに接続するためのWANインターフェイス(WAN 3)の設定

# DHCPで割り当てられたIPアドレスを使用して、単一のWANインターフェイスを設定します。

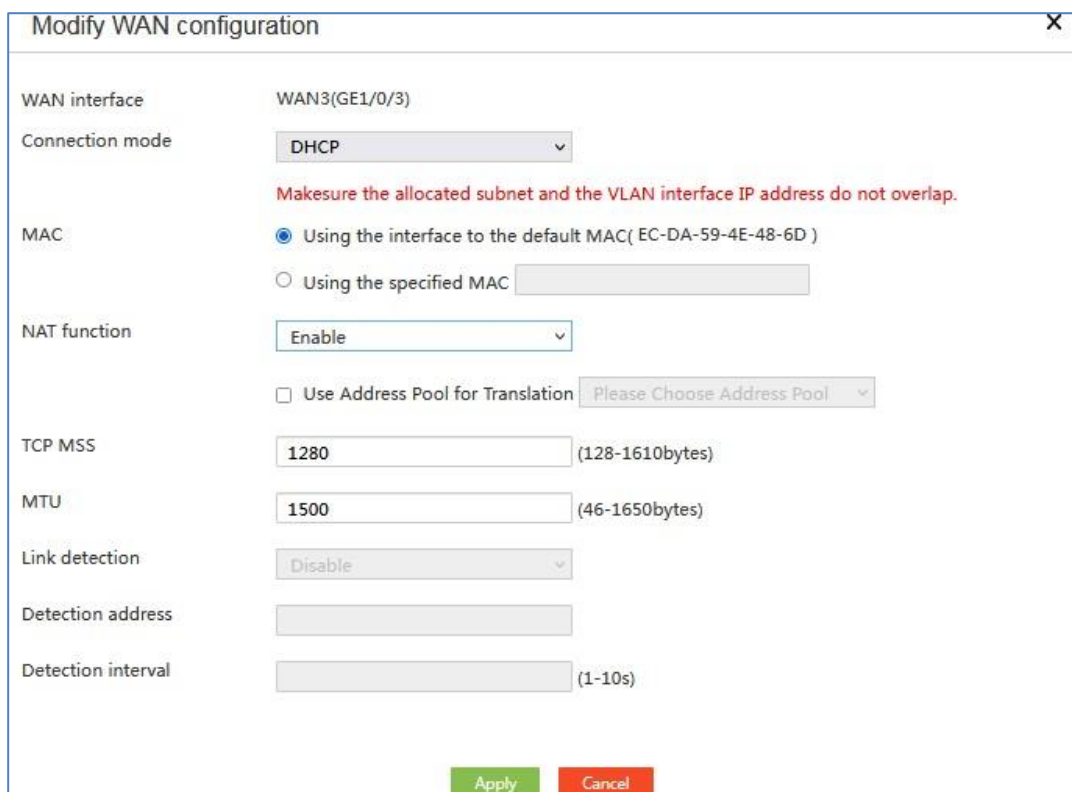
1. ナビゲーションペインで、**Network > WAN Settings**を選択します。
2. 表示された**Scene**ページで、**Single-WAN scenario**を選択し、次に**WAN3(GE1/0/3)**を選択します。のフィールドに表示されます。
3. **Apply**をクリックします。

図22 WAN構成のシナリオ



4. WAN Settingsタブをクリックします。
5. WAN3(GE1/0/3)のOperationカラムにあるEditアイコンをクリックします。
6. Connection modeフィールドで、DHCPを選択します。
7. その他のパラメータには既定の設定を使用し、Applyをクリックします。

図23 WAN設定の変更



## IPsecポリシーの構成

#ネットワークモードをブランチゲートウェイとして指定し、IKEネゴシエーションモードをアグレッシブモード



として指定します。


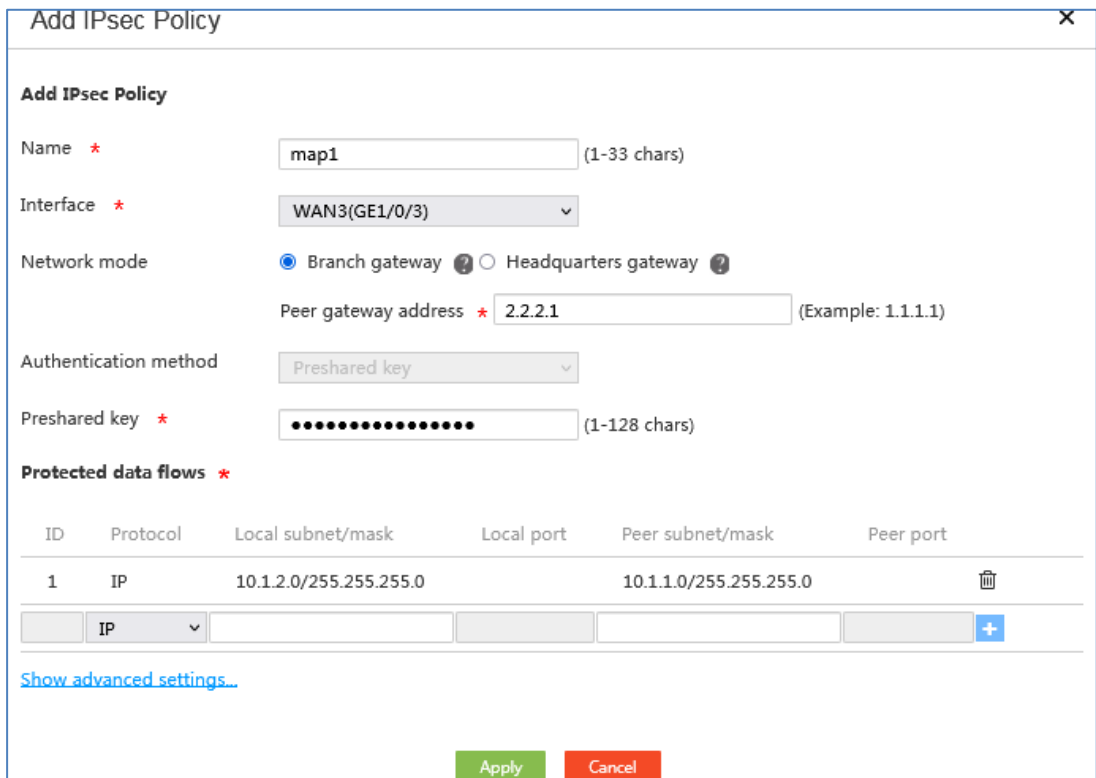
1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **Add**をクリックします。
3. 開いたページで、次のパラメータを設定します。
  - **map1**という名前を指定します。
  - **Interface**フィールドで**WAN3(GE1/0/3)**を選択します。
  - **Network mode**フィールドで**Branch gateway**を選択し、ピアゲートウェイアドレスを2.2.2.1に指定します。
  - **Preshared key**フィールドに**123456 TESTplat&!**と入力します。
  - **Protected data flows**領域で、保護するプロトコルとして**IP**を選択し、**Local subnet/mask**フィールドに**10.1.2.0/255.255.255.0**、**Peer subnet/mask**フィールドに**10.1.1.0/255.255.255.0**と入力して、アイコン  をクリックします。

図24 IPsecポリシーの追加



Add IPsec Policy

**Add IPsec Policy**

Name \*  (1-33 chars)

Interface \*


Network mode  Branch gateway  Headquarters gateway

Peer gateway address \*  (Example: 1.1.1.1)

Authentication method

Preshared key \*  (1-128 chars)

**Protected data flows \***

ID	Protocol	Local subnet/mask	Local port	Peer subnet/mask	Peer port
1	IP	10.1.2.0/255.255.255.0		10.1.1.0/255.255.255.0	

[Show advanced settings...](#)

4. **Show advanced settings**をクリックします。表示されたページで、次のパラメータを構成します。
  - **Negotiation mode**フィールドで、**Main mode**を選択します。
  - **Local ID**フィールドで、**FDQN**を選択し、FQDN名(たとえば**www.test1.com**を参照)。
  - **Remote ID**フィールドで、**FDQN**を選択し、FQDN名として**www.test.com**と入力します。
  - **DPD**フィールドで、**Enable**を選択し、DPD再試行間隔を30に指定します。
  - **Algorithm suite**フィールドで、**Customize**を選択します。
  - **Authentication algorithm**フィールドで、**MD5**を選択します。
  - **Encryption algorithm**フィールドで、**3DES-CBC**を選択します。
  - その他のパラメータには、デフォルト設定を使用します。

図25 IKEの詳細設定

Advanced settings	IKE settings	IPsec settings
Negotiation mode	Aggressive mode ▼	
Local ID	FQDN ▼	www.test1.com (1-255 chars)
Remote ID *	FQDN ▼	www.test.com (1-255 chars)
DPD	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
	DPD retry interval *	30 seconds (1-300)
Algorithm suite	Customize ▼	
Authentication algorithm *	MD5 ▼	
Encryption algorithm *	3DES-CBC ▼	
PFS *	DH group 1 ▼	
SA lifetime	86400	seconds (60-604800. Default: 86400.)
<a href="#">Back to basic settings</a>		

5. IPsec settingsタブをクリックし、次のパラメータを設定します。
- **Algorithm combination**フィールドで、**Customize**を選択します。
  - **Security protocol**フィールドで、**ESP**を選択します。
  - **ESP authentication algorithm**フィールドで、**MD5**を選択します。
  - **ESP encryption algorithm**フィールドで、**3DES-CBC**を選択します。
  - **Encapsulation mode**フィールドで、**Tunnel**を選択します。
  - その他のパラメータには、デフォルト設定を使用します。

図26 IPsecの詳細設定

Advanced settings	IKE settings	IPsec settings
Algorithm combination	Customize ▼	
Security protocol *	ESP ▼	
ESP authentication algorithm *	MD5 ▼	
ESP encryption algorithm *	3DES-CBC ▼	
Encapsulation mode *	<input type="radio"/> Transport <input checked="" type="radio"/> Tunnel	
PFS	▼	
Time-based SA lifetime	3600	seconds (180-604800. Default: 3600)
Traffic-based SA lifetime	1843200	Kilobytes (2560-4294967295. Default: 1843200)
Trigger mode	Flow trigger ▼	
<a href="#">Back to basic settings</a>		

6. **Back to basic settings**をクリックして、**Add IPsec Policy**ページに戻ります。
7. [適用]をクリックします。

## 設定の確認

1. ホストAがホストBに対して正常にpingできることを確認します。  
C:\Users\abc>ping 10.1.2.2  
Ping 10.1.2.2 (10.1.2.2): 56 data bytes, press CTRL\_C to break  
56 bytes from 10.1.2.2: icmp\_seq=0 ttl=254 time=2.137 ms  
56 bytes from 10.1.2.2: icmp\_seq=1 ttl=254 time=2.051 ms  
56 bytes from 10.1.2.2: icmp\_seq=2 ttl=254 time=1.996 ms  
56 bytes from 10.1.2.2: icmp\_seq=3 ttl=254 time=1.963 ms  
56 bytes from 10.1.2.2: icmp\_seq=4 ttl=254 time=1.991 ms  
--- Ping statistics for 10.1.2.2 ---  
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss  
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms  
C:\Users\abc>
2. Webインターフェイスで**Virtual Network > IPsec VPN > Monitor Information**をクリックして、IPsecトンネルが正常に確立されたことを確認します。Status **Active**は、IPsecトンネルが正常に確立されたことを示します。