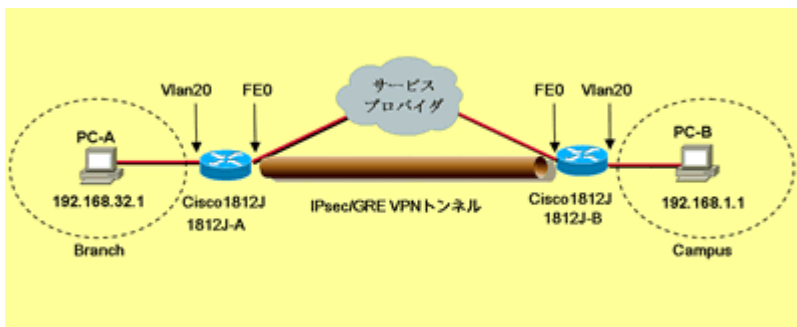


GRE over IPSecVPN を用いた LAN-to-LAN 接続 設定例

2006 年 7 月 31 日 更新
2006 年 1 月 27 日 初版

- [1. ネットワーク構成図](#)
- [2. システムの前提条件](#)
- [3. 想定する環境](#)
- [4. 必要なハードウェア / ソフトウェア要件](#)
- [5. サンプルコンフィギュレーション](#)
- [6. キーとなるコマンドの解説](#)
- [7. 設定に際しての注意点](#)

1. ネットワーク構成図



※ 画像をクリックすると、大きく表示されます。 [🔗](#)

2. システムの前提条件

2つの拠点それぞれ、PPPoE方式を利用するブロードバンド回線接続を提供するサービスにて、Cisco ISR サービス統合型ルータを使用し、インターネットに接続します。

また二つの拠点間にてインターネット上でIPSec VPNを設定し、かつそのトンネル上にてルーティングプロトコルを動作させる為の設定を行います。

3. 想定する環境

それぞれの拠点に設置しているルータには、サービスプロバイダより固定のIPアドレスを提供されています。二つの拠点間の通信をインターネット上にてセキュアに行う為に、各ルータにIPSec VPNの設定を行う設定をします。また各拠点間の経路交換の為にOSPFを使用します。ルーティングプロトコルを動作させる為に拠点間にてGREトンネルを設定します。IPSec VPNに関するパラメータは以下のものを設定します。

(1) IKE に関するパラメータ

パラメータ名	1812J-A (Branch)	1812J-B (Campus)
暗号化アルゴリズム	3DES	3DES
ハッシュアルゴリズム	MD5	MD5
認証方式	Pre-shared key	Pre-shared key
DH グループ	2 (1024bit)	2 (1024bit)
Pre-shared key	cisco	cisco

(2) IPSec に関するパラメータ

パラメータ名	1812J-A (Branch)	1812J-B (Campus)
ポリシーマップ名	GRE-IPSEC_to_campus	GRE-IPSEC_to_branch
リモート IPSec ピア	64.104.2.1	64.2.2.14
トランスフォームセット名	IPSEC	IPSEC
ESP トランスフォーム	3DES (168bit) / ESP-MD5-HMAC	3DES (168bit) / ESP-MD5-HMAC
保護すべきトラフィック	ACL# 100	ACL# 100

4. 必要なハードウェア/ソフトウェア要件

Cisco ISR サービス統合型ルータ シリーズは全てオンボードにて 2FE (もしくは 2GE) を具備します。Cisco ISR シリーズにて本構成が実現可能なハードウェア/ソフトウェアの組み合わせは下記になります。

プラットフォーム	Tトレイン	メイントレイン
871	12.4 (2) T 以上	N/A
1812J	12.4 (2) T 以上	N/A
1841	12.3 (8) T 以上	12.4 (1) 以上
2800 シリーズ (2801/2811/2821/2851)	12.3 (8) T 以上	12.4 (1) 以上
3800 シリーズ (3825/3845)	12.3 (11) T 以上	12.4 (1) 以上

本設定例においては、2つの拠点にて Cisco1812J、IOS12.4 (2) T2 を使用しています

。

5. サンプルコンフィグレーション

1. 1812J-A

```
hostname 1812J-A
!
ip cef
!
crypto isakmp policy 1
encr 3des
```

```
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 64.104.2.1
crypto isakmp keepalive 30
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!
crypto map GRE-IPSEC_to_campus 1 ipsec-isakmp
set peer 64.104.2.1
set transform-set IPSEC
match address 100
!
interface Tunnel0
ip address 192.168.100.1 255.255.255.0
ip mtu 1372
tunnel source Dialer1
tunnel destination 64.104.2.1
!
interface Loopback0
ip address 64.2.2.14 255.255.255.255
!
interface FastEthernet0
no ip address
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet3
switchport access vlan 20
!
interface Vlan20
ip address 192.168.32.254 255.255.255.0
ip tcp adjust-mss 1332
!
interface Dialer1
ip unnumbered Loopback0
ip mtu 1454
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname Flet's@cisco.com
ppp chap password 0 cisco
crypto map GRE-IPSEC_to_campus
!
router ospf 1
log-adjacency-changes
network 192.168.100.0 0.0.0.255 area 0
network 192.168.32.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
```

```
access-list 1 permit any
access-list 100 permit gre host 64.2.2.14 host 64.104.2.1
dialer-list 1 protocol ip permit
!
end
```

2. 1812J-B

```
hostname 1812J-B
!
ip cef
!
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 64.2.2.14
crypto isakmp keepalive 30
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!
crypto map GRE-IPSEC_to_branch 1 ipsec-isakmp
set peer 64.2.2.14
set transform-set IPSEC
match address 100
!
interface Tunnel0
ip address 192.168.100.2 255.255.255.0
ip mtu 1372
tunnel source Dialer1
tunnel destination 64.2.2.14
!
interface Loopback0
ip address 64.104.2.1 255.255.255.255
!
interface FastEthernet0
no ip address
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet3
switchport access vlan 20
!
interface Vlan20
ip address 192.168.1.254 255.255.255.0
ip tcp adjust-mss 1332
!
interface Dialer1
ip unnumbered Loopback0
```

```
ip mtu 1454
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname Flet's@cisco.com
ppp chap password 0 cisco
crypto map GRE-IPSEC_to_branch
!
router ospf 1
log-adjacency-changes
network 192.168.100.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 permit any
access-list 100 permit gre host 64.104.2.1 host 64.2.2.14
dialer-list 1 protocol ip permit
!
end
```

6. キーとなるコマンドの解説

"crypto isakmp policy 1"

<コマンド種別>

グローバルコンフィギュレーションコマンド

<コマンドの機能>

IKE ネゴシエーション時に使用される IKE ポリシーを作成します。プライオリティ番号の範囲は 1~10000 で、プライオリティが最も高いのが 1 です。

また、Internet Security Association Key and Management Protocol (ISAKMP) ポリシー コンフィギュレーション モードを開始します。

"encryption 3des"

<コマンド種別>

ISAKMP ポリシー コンフィギュレーション モード

<コマンドの機能>

IKE ポリシーに使用される暗号化アルゴリズムを指定します。des (DES 56ビット)、3des (3DES 168ビット)、aes (AES) が選択可能です。

デフォルトでは、56 ビット DES を使用します。

"hash md5"

<コマンド種別>

ISAKMP ポリシー コンフィギュレーション モード

<コマンドの機能>

IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。

この例では、Message Digest 5 (MD5) アルゴリズムを指定します。デフォルトは、Secure Hash 標準 (SHA-1) です。

"authentication pre-share"

<コマンド種別>
ISAKMP ポリシー コンフィギュレーション モード
<コマンドの機能>
IKE ポリシーに使用される認証方式を指定します。
この例では、事前共有キーを使用します。

"group 2"

<コマンド種別>
ISAKMP ポリシー コンフィギュレーション モード
<コマンドの機能>
IKE ポリシーに使用される Diffie-Hellman グループを指定します。

"lifetime seconds"

<コマンド種別>
ISAKMP ポリシー コンフィギュレーション モード
<コマンドの機能>
IKE Security Association (SA;セキュリティ アソシエーション) のライフタイム (60~86400秒) を指定します。

"crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac"

<コマンド種別>
グローバルコンフィギュレーションコマンド
<コマンドの機能>
トランスフォーム セット (IPSec セキュリティ プロトコルとアルゴリズムの有効な組み合わせ) を定義します。

"crypto map GRE-IPSEC_to_branch 1 ipsec-isakmp"

<コマンド種別>
グローバルコンフィギュレーションコマンド
<コマンドの機能>
暗号マップ プロファイルを作成します。
また、暗号マップコンフィギュレーションコマンドを開始します。

"set peer 64.2.2.14"

<コマンド種別>
暗号マップコンフィギュレーションコマンド
<コマンドの機能>
トラフィックの暗号化 / 復号化を許可するピアを指定します。

"set transform-set IPSEC"

<コマンド種別>
暗号マップコンフィギュレーションコマンド
<コマンドの機能>
暗号マップ エントリに使用できるトランスフォーム セットを指定します。

"match address 100"

<コマンド種別>
暗号マップコンフィギュレーションコマンド
<コマンドの機能>

暗号マップ エントリに適用するトラフィックを識別するためのアクセスリストを指定します。

"crypto isakmp key cisco address 64.2.2.14"

<コマンド種別>

グローバルコンフィグレーションコマンド

<コマンドの機能>

リモートピアの IP アドレスと、そのピアに対するIKE事前共有キーを指定します。

"crypto isakmp keepalive 30"

<コマンド種別>

グローバルコンフィグレーションコマンド

<コマンドの機能>

IKE キープアライブを送信する間隔を指定します。

上記の設定を行ったときは、デフォルトの振る舞いとして、On-Demand (上記のように、ESP パケットの送受信状況をモニタし、必要時だけ送信) が選択されます。

"crypto map GRE-IPSEC_to_branch"

<コマンド種別>

インタフェースコンフィグレーションコマンド

<コマンドの機能>

インターフェイスに暗号マップを適用します。本設定ではダイアラーインターフェイスに指定します。

"interface Tunnel0"

<コマンド種別>

グローバルコンフィグレーションコマンド

<コマンドの機能>

GRE トンネル インターフェイスを作成します。

"ip address 192.168.100.1 255.255.255.0"

<コマンド種別>

インタフェースコンフィグレーションコマンド

<コマンドの機能>

GRE トンネルに IP アドレスを割り当てます。

"tunnel source Dialer1"

<コマンド種別>

インタフェースコンフィグレーションコマンド

<コマンドの機能>

GRE トンネルにルータの送信元を指定します。

"tunnel destination 64.104.2.1"

<コマンド種別>

インタフェースコンフィグレーションコマンド

<コマンドの機能>

GRE トンネルにルータの宛先を指定します。

"access-list 100 permit gre host 64.2.2.14 host 64.104.2.1"

<コマンド種別>

グローバルコンフィグレーションコマンド

<コマンドの機能>

アクセスリストにより暗号化対象トラフィックを定義します。本設定ではアドレスに GRE トンネルのエンドポイントを指定し、プロトコルを GRE に指定しています。

7. 設定に際しての注意点

PPPoE 使用時の MTU サイズは、通常時よりも小さくなります。(フレッツでは、1454 バイトを推奨) また本設定例では IPSec Tunnel モードのオーバーヘッド (36byte+trailer) も考慮し、MTU サイズ、TCP の MSS (最大セグメントサイズ) の値をそれに合わせて調整することが必要となる点に注意してください。

PPPoE インターフェース上での `ip route 0.0.0.0 0.0.0.0 Dialer1` と指定した際にはファーストスイッチとなります。PPPoE にてより高速な CEF スイッチを実現する為にはサービスプロバイダーの BAS アドレスが PPP ネゴシエーション時にルータにインストールされている必要があります。インストールされている様であれば、dialer インターフェースにて `ppp ipcp route default` を設定し、再度 PPPoE セッション確立してください。PPP ネゴシエーション終了時に BAS アドレスを nexthop としたデフォルトルートが作成されます。本設定に関しては実際のトラフィックは OSPF により学習されたルートを選択する為、あまり考慮する必要がありません。

サービスプロバイダーに対しての無駄なトラフィックを防ぐ為にも、OSPF の `network` コマンドは Tunnel インターフェースおよび LAN 側インターフェースのみに適用し、WAN 側インターフェースには適用しないでください。

以前 IOS では PPPoE クライアントにおいて、下記のコマンドが必要でしたが、現在の IOS では必要ありません。またこのコマンドを設定する事により PPPoE サーバの機能が有効になり、WAN 側の同一セグメントにおいて、PPPoE クライアントが存在する際には、broadcast で送られる PADI に対し、PADO を返してしまいます。**設定は行わないで下さい。**

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
```

1812J や 871 の様な SW 内蔵のプラットフォームまたは HWIC-4ESW/HWIC-9DESW などのスイッチモジュールを使用し、vlan を使用する際には、vlan database コマンドにて追加する vlan を指定する必要があります。

実際に導入し、運用される際には障害解析などの観点により下記の様なコマンドも追加する事を推奨いたします。

```
service timestamps debug datetime localtime msec
service timestamps log datetime localtime msec
clock timezone JST 9
!
logging buffered 512000 debugging
!
```

全ての Cisco ISR サービス統合型ルータでは、HW 暗号化アクセラレータがオンボードにて提供されています。1841/2800/3800 にてより高速でスケラビリティのある拡張暗号化モジュールが必要な際には下記モジュールをご購入下さい。

プラットフォーム

1841

2800シリーズ

(2801/2811/2821/2851)

3800シリーズ

(3825/3845)

Updated: Jul 31, 2006

拡張暗号化モジュール

AIM-VPN/BPII-PLUS

AIM-VPN/EPII-PLUS

3825 : AIM-VPN/EPII-PLUS

3845 : AIM-VPN/HPII-PLUS

Document ID: jtac_20060127_7