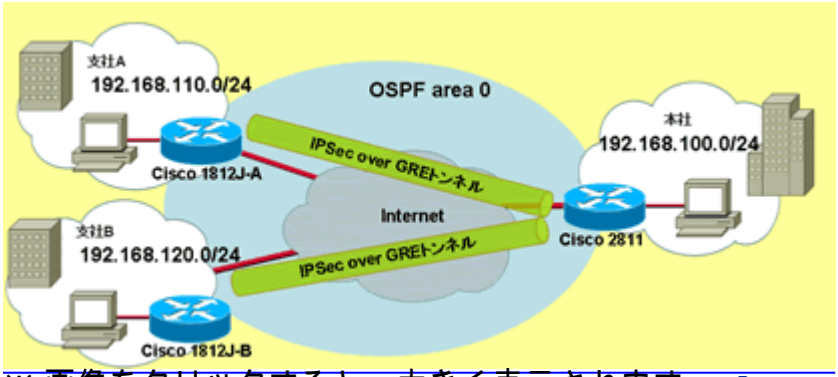
GRE over IPsec VPNとDynamic Routingを用いた複数拠点接続設定例

2006 年 7 月 31 日 更新
2006 年 6 月 21 日 初版

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

三つの拠点がそれぞれ、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 ルータを使用し、インターネットに接続します。
この三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。
三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	Router (2811/1812J)
暗号化アルゴリズム	3DES
ハッシュアルゴリズム	MD5

認証方式	Pre-shared key
DHグループ	2（1024bit）
Pre-shared key	cisco

（2）IPsec に関するパラメータ

パラメータ名	1812J-A（Branch A）	1812J-B（Branch B）	2811（Campus）
ポリシーマップ名	GRE-IPSEC	GRE-IPSEC	GRE-IPSEC
リモート IPsec ピア	64.100.1.101	64.100.1.101	64.100.2.101 64.100.3.101
トランスフォームセット名	IPSEC	IPSEC	IPSEC
ESP トランスフォーム	3DES（168bit）/ ESP-MD5-HMAC	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	ACL# 100, 101

4.必要なハードウェア/ソフトウェア

ISR 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。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。

プラットホーム	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、支社側にて Cisco1812J : IOS12.4（6）T、本社側にて Cisco 2811 : IOS12.4（5a）を使用しています。

5.サンプルコンフィグレーション

（1）2811

```
hostname C2811
!
ip cef
!
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 64.100.2.101
crypto isakmp key cisco address 64.100.3.101
crypto isakmp keepalive 30
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!
```

```
crypto map GRE-IPSEC 1 ipsec-isakmp
set peer 64.100.2.101
set transform-set IPSEC
match address 100
crypto map GRE-IPSEC 2 ipsec-isakmp
set peer 64.100.3.101
set transform-set IPSEC
match address 101
!
interface Tunnel0
description to 1812J-A
ip address 192.168.1.1 255.255.255.0
ip mtu 1372
tunnel source Dialer1
tunnel destination 64.100.2.101
!
interface Tunnel1
description to 1812J-B
ip address 192.168.2.1 255.255.255.0
ip mtu 1372
tunnel source Dialer1
tunnel destination 64.100.3.101
!
interface Loopback0
ip address 64.100.1.101 255.255.255.0
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet0/1
ip address 192.168.100.254 255.255.255.0
ip tcp adjust-mss 1332
duplex auto
speed auto
!
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-a@cisco.com
ppp chap password 0 cisco
crypto map GRE-IPSEC
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
```

network 192.168.2.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 100 permit gre host 64.100.1.101 host 64.100.2.101
access-list 101 permit gre host 64.100.1.101 host 64.100.3.101
dialer-list 1 protocol ip permit
!
end

(2) 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 64.100.1.101
crypto isakmp keepalive 30
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!
crypto map GRE-IPSEC 1 ipsec-isakmp
set peer 64.100.1.101
set transform-set IPSEC
match address 100
!
interface Tunnel0
description to 2811
ip address 192.168.1.2 255.255.255.0
ip mtu 1372
tunnel source Dialer1
tunnel destination 64.100.1.101
!
interface Loopback0
ip address 64.100.2.101 255.255.255.0
!
interface FastEthernet0
no ip address
duplex auto
speed auto
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet3
switchport access vlan 20
!

```
interface Vlan20
ip address 192.168.110.254 255.255.255.0
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-b@cisco.com
ppp chap password 0 cisco
crypto map GRE-IPSEC
!
router ospf 1
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
network 192.168.110.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 100 permit gre host 64.100.2.101 host 64.100.1.101
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 64.100.1.101
crypto isakmp keepalive 30
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!
crypto map GRE-IPSEC 1 ipsec-isakmp
set peer 64.100.1.101
set transform-set IPSEC
match address 100
!
interface Tunnel0
description to 2811
ip address 192.168.2.2 255.255.255.0
ip mtu 1372
```

```
tunnel source Dialer1
tunnel destination 64.100.1.101
!
interface Loopback1
ip address 64.100.3.101 255.255.255.0
!
interface FastEthernet0
no ip address
duplex auto
speed auto
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet3
switchport access vlan 20
!
interface Vlan20
ip address 192.168.120.254 255.255.255.0
ip tcp adjust-mss 1332
!
interface Dialer1
ip unnumbered Loopback1
ip mtu 1454
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname Flet's-c@cisco.com
ppp chap password 0 cisco
crypto map GRE-IPSEC
!
router ospf 1
log-adjacency-changes
network 192.168.2.0 0.0.0.255 area 0
network 192.168.120.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 100 permit gre host 64.100.3.101 host 64.100.1.101
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グ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。

"crypto isakmp key cisco address 64.100.2.101"
<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。

"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グ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 1 ipsec-isakmp"
＜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＞
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 64.100.1.101"
＜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。

"access-list 100 permit gre host 64.100.1.101 host 64.100.2.101"
＜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。
デフォルトの振る舞いとして、On-Demand（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"
＜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フェースに指定します。

"interface Tunnel 0"
＜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 192.168.1.1 255.255.255.0"
＜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 64.100.2.101"
＜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 64.100.1.101 host 64.100.2.101"
＜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 GRE オーバヘット（24byte）ならび IPSec Tunnel モードのオーバヘッド（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。
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 では必要がありません。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。**こちらの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 内臓のプラットホームまたは 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。
全ての ISR 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ーラビリティのある拡張暗号化モジュールが必要の際には下記モジュールをご購入下さい。

プラットホーム	拡張暗号化モジュール
1841	AIM-VPN/BPII-PLUS
2800 シリーズ （2801/2811/2821/2851）	AIM-VPN/EPII-PLUS
3800 シリーズ （3825/3845）	3825：AIM-VPN/EPII-PLUS 3845：AIM-VPN/HPII-PLUS

事前共有キーの設定はユーザ個別もしくはグループ事前共有で行います。ユーザ個別の場合、各IPSec ピアで個別に事前共有キーの設定を行います。グループ事前共有キーを設定する場合、下記のようにグループ内で同一の事前共有キーを設定します。

crypto isakmp key 0 cisco address 0.0.0.0 0.0.0.0

上記設定では全ての IP アドレスからの IPSec のネゴシエーションを許容する為に、セキュリティレベルは落ちる事を注意してください。
Cisco VPN Client ソフトウェアにて接続時にも PPPoE 接続時などは MTU を考慮する必要があります。Cisco System VPN Client->Set MTU にて適切なMTUに設定をして下さい。

Jul 31, 2006 Document ID: jtac_20060621_3