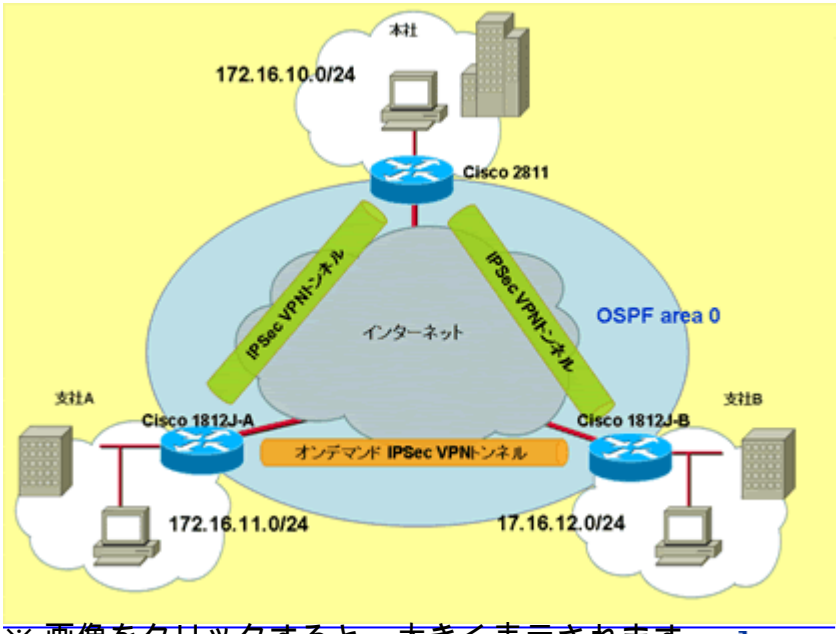
DMVPNを用いたフルメッシュIPSec VPN接続設定例

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

3 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、CiscoISR ルータを使用し、インターネットに接続します。
これら 3 つの拠点を、DMVPN (Dynamic Multipoint VPN) を利用することによりオンデマンドで支社間にも IPSec VPN トンネルをはり、全拠点間のフルメッシュ IPSec VPN 環境を構築する設定を行います。

3.想定する環境

それぞれの拠点に設置しているルータは、サービスプロバイダより IP アドレスを提供されています。本社は固定の IP アドレスを付与されており、各支社は端末型払い出し方式により、ダイナミックに IP アドレスを付与されています。
これら 3 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の設定を行います。

支社側のダイナミックなアドレス環境をサポートする為、支社−本社間に Multipoint GRE を設定し、その上に IPSec VPN および NHRP の設定を行います。
また、各拠点間の経路交換の為に OSPF を使用します。

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	2811 (本社)	1812J-A (支社A)	1812J-B (支社B)
暗号化アルゴリズム	3DES	3DES	3DES
ハッシュアルゴリズム	MD5	MD5	MD5
認証方式	Pre-shared key	Pre-shared key	Pre-shared key
DH グループ	2 (1024bit)	2 (1024bit)	2 (1024bit)
Pre-shared key	cisco	cisco	cisco

(2) IPsec に関するパラメータ

パラメータ名	2811 (本社)	1812J-A (支社A)	1812J-B (支社B)
プロファイル名	dmprofile	dmprofile	dmprofile
トランスフォームセット名	dmvpnset	dmvpnset	dmvpnset
ESP トランスフォーム	3DES (168bit) / ESP-MD5-HMAC	3DES (168bit) / ESP-MD5-HMAC	3DES (168bit) / ESP-MD5-HMAC

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、Cisco1812J : IOS12.4 (2) T2、Cisco2811: 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) 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 0.0.0.0 0.0.0.0
crypto isakmp keepalive 30
!
crypto ipsec transform-set dmvpnset esp-3des esp-md5-hmac
!
crypto ipsec profile dmprofile
set transform-set dmvpnset
!
interface Tunnel0
ip address 172.31.255.2 255.255.255.0
no ip redirects
ip mtu 1368
ip nhrp authentication dmcisco
ip nhrp map multicast 64.100.1.100
ip nhrp map 172.31.255.1 64.100.1.100
ip nhrp network-id 99
ip nhrp holdtime 300
ip nhrp nhs 172.31.255.1
ip ospf network broadcast
ip ospf priority 0
tunnel source Dialer1
tunnel mode gre multipoint
tunnel key 10
tunnel protection ipsec profile dmprofile
!
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 172.16.11.1 255.255.255.0
ip tcp adjust-mss 1328
!
interface Dialer1
ip address negotiated
ip mtu 1454
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication pap callin
ppp chap hostname Flet's@cisco.com
ppp chap password 0 cisco
!
router ospf 1
log-adjacency-changes
network 172.16.11.0 0.0.0.255 area 0
```

network 172.31.255.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
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 0.0.0.0 0.0.0.0
crypto isakmp keepalive 30
!
crypto ipsec transform-set dmvpnset esp-3des esp-md5-hmac
!
crypto ipsec profile dmprofile
set transform-set dmvpnset
!
interface Tunnel0
ip address 172.31.255.3 255.255.255.0
no ip redirects
ip mtu 1368
ip nhrp authentication dmcisco
ip nhrp map multicast 64.100.1.100
ip nhrp map 172.31.255.1 64.100.1.100
ip nhrp network-id 99
ip nhrp holdtime 300
ip nhrp nhs 172.31.255.1
ip ospf network broadcast
ip ospf priority 0
tunnel source Dialer1
tunnel mode gre multipoint
tunnel key 10
tunnel protection ipsec profile dmprofile
!
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 172.16.12.1 255.255.255.0
ip tcp adjust-mss 1328
!
interface Dialer1
ip address negotiated
ip mtu 1454
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication pap callin
ppp chap hostname Flet's@cisco.com
ppp chap password 0 cisco
!
router ospf 1
log-adjacency-changes
network 172.16.12.0 0.0.0.255 area 0
network 172.31.255.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
dialer-list 1 protocol ip permit
!
end
```

(3) 2811

```
hostname C2811
!
ip cef
!
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 30
!
crypto ipsec transform-set dmvpnset esp-3des esp-md5-hmac
!
crypto ipsec profile dmprofile
set transform-set dmvpnset
!
interface Tunnel0
ip address 172.31.255.1 255.255.255.0
no ip redirects
ip mtu 1368
ip nhrp authentication dmcisco
ip nhrp map multicast dynamic
```

```
ip nhrp network-id 99
ip nhrp holdtime 300
ip ospf network broadcast
tunnel source Dialer1
tunnel mode gre multipoint
tunnel key 10
tunnel protection ipsec profile dmprofile
!
interface Loopback0
ip address 64.100.1.100 255.255.255.0
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet0/1
ip address 172.16.10.1 255.255.255.0
ip tcp adjust-mss 1328
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@cisco.com
ppp chap password 0 cisco
!
router ospf 1
log-adjacency-changes
network 172.16.10.0 0.0.0.255 area 0
network 172.31.255.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 Dialer1
!
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＞
ISAKM P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 isakmp key **cisco** address **0.0.0.0 0.0.0.0**"
＜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＞
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 ipsec transform-set **dmvpnset 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"dmvpnset"（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 ipsec profile **dmprofile**"
＜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＞
IPSec パラメータをプロファイル名 "dmprofile" の中で指定します。

"set transform-set **dmvpnset**"
＜コマンド種別＞
IPSec プロファイルコンフィグレーションコマンド
＜コマンドの機能＞
使用できるトランスフォーム セットを指定します。"crypto ipsec transform-set" コマンドで設定済のトランスフォームセット名を指定します。

"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 **172.31.255.2 255.255.255.0**"
＜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。

"ip nhrp authentication **dmcisco**"
＜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＞
Next Hop Resolution Protocol（NHRP）を利用しているインターフェースに認証用ストリング "dmcisco" を設定します。

"ip nhrp map **172.31.255.1 64.100.1.100**"
＜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＞
NBMA ネットワークに接続された宛先となる HUB ルータのアドレスを静的に IP-to-NBMA アドレスとしてマッピングします。この例では "172.31.255.1" が HUBルータの Tunnel IP アドレス、"64.100.1.100" が HUB ルータの物理 IP アドレスとなります。

"ip nhrp map multicast **64.100.1.100**"

＜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＞
Spoke-Hub 間でダイナミックルーティングプロトコルの使用を有効にします。また、Hub ルータ "64.100.1.100" へのマルチキャストパケット送信を有効にします。

"ip nhrp map multicast **dynamic**"
＜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＞
マルチキャスト NHRP マッピングに自動的に Spoke ルータを追加することを有効にします。

"ip nhrp network-id **99**"
＜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＞
インターフェース上で NHRP を有効にします。network-id "99" は同一の論理 NBMA ネットワークにおいて一意のものを指定する必要があります。

"ip nhrp holdtime **300**"
＜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＞
NHRP NBMA アドレスの有効時間（秒）を設定します。デフォルトは 7200 秒となります。

"ip nhrp nhs **172.31.255.1**"
＜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＞
NHRP ネクストホップサーバとして Hub ルータのアドレス"172.31.255.1" を指定します。

"ip ospf network **broadcast**"
＜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＞
OSPF ネットワークタイプを "broadcast"に指定します。

"ip ospf priority **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＞
OSPF DR の選出の為にインターフェースの OSPF プライオリティを指定します。Hub ルータを DR に選出する為、Spoke 側に "0" を設定します。

"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 mode **gre multipoint**"
＜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＞
トンネルモードを multipoint GRE（mGRE）に指定します。

"tunnel key **10**"
＜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＞
トンネルインターフェース用IDキーを指定します。

"tunnel protection ipsec profile **dmprofile**"
＜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＞
トンネルインターフェースと IPSec プロファイルを関連付けます。指定されるプロファイル名は "crypto ipsec profile" で作成されたプロファイルと同一のものである必要があります。

"ip tcp adjust-mss **1328**"
＜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＞
このインタフェースを通過する TCP セッションは、TCP の最大セグメントサイズが 1330 バイトでネゴシエーションが行われるようになります。

"ip mtu **1454**"
＜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＞
パケットの最大送信サイズを定義します。この事例では、Dialer1 インタフェースから送信されるパケットの最大サイズは 1454 バイトに調整されます。

7.設定に際しての注意点

OSPF 使用時には Tunnel インターフェースにてデフォルトの Point-to-Point ネットワークタイプより、**" ip ospf network broadcast "**などにてネットワークタイプを変更する必要があります。
OSPF 使用時には HUB ルータが必ず DR になるように、Spoke ルータにて、**" ip ospf priority 0 "**を使用してください。
ディスタンスベクタープロトコルではデフォルトにてSplit-horizon が有効になっており、この為、経路を学習したインターフェースにはその経路をアドバタイズしません。EIGRPを使用する際には、HUB ルータの Tunnel インターフェースにて" no ip split-horizon eigrp AS 番号"にて Split-horizon を無効にして下さい。また RIP および IGRP においても同様に" no ip split-horizon"を使用して下さい。
EIGRP では経路を広告する際に nexthop を変更します。Spoke-to-Spoke の直接通信を行なう際には HUB ルータの Tunnel インターフェースにて" no ip next-hop-self eigrp AS 番号"コマンドを使用してください。
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 mGRE オーバヘット（Tunnel key 分 4byte+GRE ヘッダ 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、

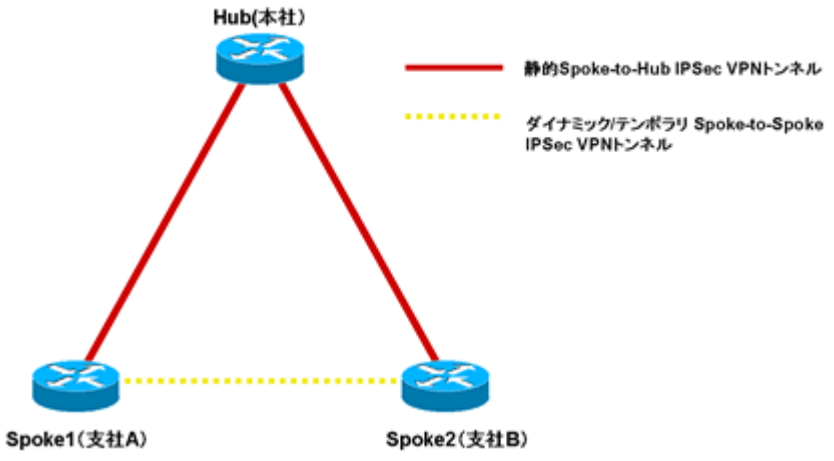
再度PPPoEセッション確立してください。PPPネゴシエーション終了時にBASアドレスをnexthopとしたデフォルトルートが作成されます。本設定に関しては実際のトラフィックはOSPFにより学習されたルートを選択する為、あまり考慮する必要がありません。

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

8.DMVPNについて

DMVPN（Dynamic Multipoint VPN）はIPSecとmGREを組み合わせることにより、スケーラブルなIPSec VPN環境を構築することを可能にします。DMVPNが提供するダイナミックなSpoke-to-Spoke IPSec VPNトンネルの構築により、HUBに経由によるネットワークの遅延や暗号化による遅延を減らすことが可能になります。
DMVPNはmGREおよびNHRPを二つの主要な機能として利用します。
複数のSpokeとHub間を接続する為にmGREインターフェースが利用されます。DMVPN環境下ではトンネルインターフェース上に"tunnel destination"を指定する必要がなく、Hub側ではNHRP（Next Hop Resolution Protocol）を利用してSpokeの宛先トンネルアドレスを取得します。その為、Spoke側でFTTHやADSLといったサービスを利用してダイナミックにアドレスを取得する場合でも、NHRPによりIP-to-NBMAのアドレスマッピングが自動的に行われ、Spoke-to-HubのIPSec VPNトンネルを構築することが可能です。



※ 画像をクリックすると、大きく表示されます。
Spoke-to-HubのIPSec VPNトンネルの構築後Spoke-to-Spokeの通信が発生した際、NHRPを利用することによりHub側から対向のSpokeのNBMAアドレスを取得し、Spoke-to-SpokeのIPSec

VPNトンネルをオンデマンドに構築することができます。
Jun 21, 2006 Document ID: jtac_20060621_6