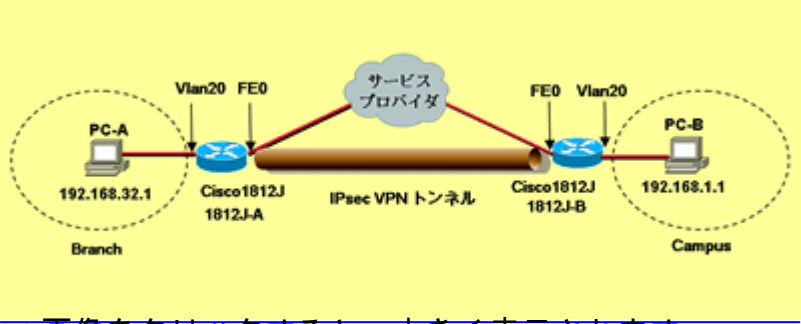
IPSec VPN を用いた LAN-to-LAN 接続設定例

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. サンプルコンフィグレーション
6. キーとなるコマンドの解説
7. 設定に際しての注意点
8. IPSec の設定手順

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 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。IPSecVPN 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	map_to_campus	map_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 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 periodic
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!

crypto map map_to_campus 1 ipsec-isakmp
set peer 64.104.2.1
set transform-set IPSEC
match address 100
!
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 1356
!
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 map_to_campus
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 100 permit ip 192.168.32.0 0.0.0.255 192.168.1.0 0.0.0.255
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 periodic
!
crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
!

crypto map map_to_branch 1 ipsec-isakmp
set peer 64.2.2.14
set transform-set IPSEC
match address 100
!
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 1356
!
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 map_to_branch
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.32.0 0.0.0.255
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。

"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 map_to_branch 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 64.2.2.14"
<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 periodic"
＜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 が選択されます。
ダイナミックルーティングなどと併用しない際には、定期的に DPD を送出する Periodic を選択する事を推奨します。

"crypto map map_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＞
すでに定義されているインターフェイスに暗号マップを適用します。

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 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。
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。**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。
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.IPSec の設定手順

IOS にて既知共有鍵方式による LAN-to-LAN IPSecVPN の設定手順は、以下のようになります。

1. トンネル対象トラフィックの指定
2. IKE ポリシ設定
3. 既知共有鍵設定
4. トランスフォームセットの設定
5. IPSec ポリシ設定
6. インタフェースへのIPSec ポリシの適用

以下に本設定例における 1812J-A 設定について設定手順にそって説明します。

1. トンネル対象トラフィックの指定

```
access-list 100 permit ip 192.168.32.0 0.0.0.255 192.168.1.0 0.0.0.255
```

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。暗号化で保護する IP トラフィックを permit で指定します。この暗号アクセスリストは crypto map エントリの中で IPSec ポリシとして利用されます。尚、IPSec ピア間では相互のミラーイメージのアクセスリスト利用を推奨します。

2. IKE ポリシ設定

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
```

IKE フェーズ 1 認証における各種パラメータを定義します。暗号化アルゴリズム、ハッシュアルゴリズム、認証方式、Diffie-Hellman グループ識別子を指定します。ポリシの後に指定する数値はポリシ優先度を示し、小さい数値のものが最優先、つまり 1 が最優先されます。本設定では暗号化アルゴリズム：DES、ハッシュアルゴリズム：MD5、認証方式：pre-shared key、Diffie-Hellman グループ識別子：2 を指定しています。

3. 既知共有鍵設定

crypto isakmp key cisco address 64.104.2.1
ピアに対しての既知共有鍵の設定を行います。本設定では共有鍵として"cisco"を指定しています。このキーは IPSec ピア間で一致する必要があり、またアドレスは互いのピアを指定します。

4. トランスフォームセットの設定

crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac
利用する IPSec トランスフォームを指定します。指定したトランスフォーム名は crypto map エントリの中で IPSec ポリシとして利用されます。本設定ではESP暗号として esp-3des、ESP 認証として esp-md5-hmac を指定しています。またモードはデフォルトでトンネルモードが指定されています。

5. IPSecポリシ設定

crypto map map_to_campus 1 ipsec-isakmp
 set peer 64.104.2.1
 set transform-set IPSEC
 match address 100
crypto map エントリを設定します。crypto map 名はインタフェースに適用する crypto map として利用されます。crypto map エントリのシーケンス番号は数値が小さいほど優先されるポリシとなります。（1 つのインタフェースに適用できる crypto map は1つです）本設定では ISAKMP を利用したIPSecとしてcrypto map を定義しています。またピア IP アドレスの指定、トランスフォームセットの指定、暗号アクセスリストの指定を行います。

6. インタフェースへの IPSec ポリシの適用

interface Dialer1
crypto map map_to_campus
最後にインタフェースにどの crypto map エントリを定義するか指定します。本設定ではアウトバウンド IP インタフェース "Dialer1" に指定します。crypto map のインタフェースへの適用によりトラフィックを監視し、暗号アクセスリストに該当したトラフィックは暗号化されます。
以上により IOS にて既知共有鍵方式による LAN-to-LAN IPSec VPN を利用することが可能になります。設定に際してはピアルータとの各種パラメータ（暗号化、ハッシュアルゴリズム、認証方式、共有鍵など）に誤りがないか注意する必要があります。