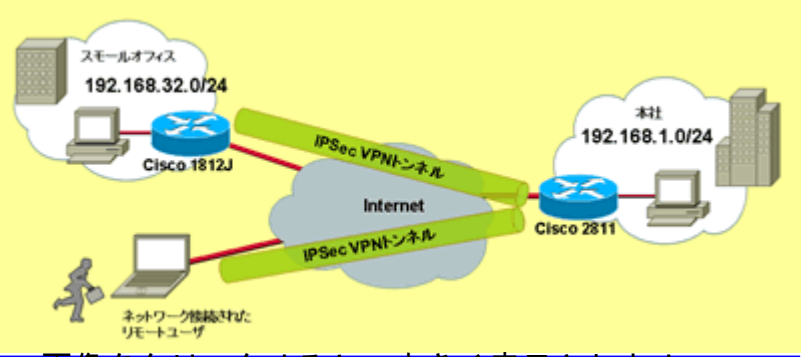
Cisco Easy VPN 接続設定例

2006 年 6 月 29 日 更新
2006 年 1 月 27 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

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。動的にアドレスを払い出されたスモールオフィスと本社を Cisco Easy VPN 機能を用いた IP Sec VPN を設定します。またインターネットに接続されたリモートユーザも本社と IPSec VPN を設定します。

3.想定する環境

本社ルータは、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。
スモールオフィスのルータおよびリモートユーザは、動的にIPアドレスが払い出されます。
本社ルータを Cisco Easy VPN サーバとして動作させます。
スモールオフィスのルータを Cisco Easy VPN リモート、リモートユーザでは Cisco VPN Client ソフトウェアを用いて、本社ルータとの間にてIPSec トンネルを設定し、セキュアな通信を行います。
VPNCisco クライアントは、クライアントモードで動作させ、スモールオフィスの LAN ネットワーク (192.168.32.0) は WAN 側に割り当てたられた IP アドレスで PAT され本社と通信します。

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。本社 Cisco Easy VPN サーバ機能およびスモールオフィスの Cisco Easy VPN リモート機能ともに提供が可能になります。

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、本社: Cisco2811 12.4（2）T2、リモートオフィス:Cisco 1812J 12.4（2）T2、リモートユーザに Cisco VPN Client バージョン 4.7.00.0053 for Windows 2000/XP 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

```
hostname 1812J
!
ip subnet-zero
!
ip cef
!
crypto isakmp keepalive 30 periodic
!
crypto ipsec client ezvpn 1812
connect auto
group VPNCLIENT key cisco
mode client
peer 64.104.2.100
username ezvpn password cisco
xauth userid mode local
!
!
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 192.168.32.254 255.255.255.0
ip tcp adjust-mss 1356
crypto ipsec client ezvpn 1812 inside
!
```

```
interface Dialer1
ip address negotiated
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 ipsec client ezvpn 1812
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
dialer-list 1 protocol ip permit
!
```

2. 2811

```
hostname IPSec
!
!
aaa new-model
!
!
aaa authentication login userauth local
aaa authorization network groupauth local
!
aaa session-id common
!
ip subnet-zero
!
!
ip cef
!
username ezvpn password 0 cisco
username remoteuser password 0 cisco
!
crypto isakmp keepalive 30 periodic
!
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp client configuration group VPNCLIENT
key cisco
dns 192.168.1.100
wins 192.168.1.200
domain cisco.com
pool ezvpn1
save-password
```

```
crypto isakmp profile vpnclient-profile
match identity group VPNCLIENT
client authentication list userauth
isakmp authorization list groupauth
client configuration address respond !
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto dynamic-map dynmap 1
set transform-set myset
set isakmp-profile vpnclient-profile
!
!
crypto map ezvpnmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Loopback0 ip address 64.104.2.100 255.255.255.0
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
pppoe enable
pppoe-client dial-pool-number 1
!
interface FastEthernet0/1
ip address 192.168.1.254 255.255.255.0
ip tcp adjust-mss 1356
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
crypto map ezvpnmap
!
ip local pool ezvpn1 192.168.10.1 192.168.10.100!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
!
!
dialer-list 1 protocol ip permit
!
```

6.キーとなるコマンドの解説

1. Cisco1812J - Cisco Easy VPN リモートの設定

"crypto ipsec client ezvpn 1812"
＜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＞
Cisco Easy VPN リモート コンフィギュレーション "1812" を作成します。

"connect auto"
＜コマンド種別＞
Cisco Easy VPN リモートコンフィグレーションコマンド
＜コマンドの機能＞
IPSec VPN トンネルを自動的に接続するコマンド。デフォルトで auto となっており、Cisco Easy VPN リモート機能が Interface に割り当てられた場合、自動的に接続を開始します。

"group VPNCLIENT key cisco"
＜コマンド種別＞
Cisco Easy VPN リモートコンフィグレーションコマンド
＜コマンドの機能＞
VPN 接続の IPSec グループおよび IPSec キー値を指定します。この例では group 名 VPNCLIENT、IPSec キー値が cisco となっています。

"mode client"
＜コマンド種別＞
Cisco Easy VPN リモートコンフィグレーションコマンド
＜コマンドの機能＞
VPN 動作モードを指定します。client モードと network extension モードがあります。

"peer 64.104.2.100"
＜コマンド種別＞
Cisco Easy VPN リモートコンフィグレーションサブコマンド
＜コマンドの機能＞
VPN 接続のピア IP アドレスまたはホスト名を指定します。この例では 64.104.2.100 が VPN 接続のピア IP アドレスとなります。

"username ezvpn password 0 cisco"
＜コマンド種別＞
Cisco Easy VPN リモートコンフィグレーションサブコマンド
＜コマンドの機能＞
サーバ側がパスワードの保存を許可している場合にのみ有効。Ｘａｕｔｈ（拡張認証）ユーザ名およびパスワードを設定します。
本設定例ではパスワードは簡略化のために暗号化なし（0）で記載しております。必要に応じ暗号化（7）にて設定してください。

"xauth userid mode local"
＜コマンド種別＞
Cisco Easy VPN リモートコンフィグレーションサブコマンド
＜コマンドの機能＞
Xauth リクエストに対する Cisco クライアントの対応方式を指定。この例では Local でセーブされたユーザー名 / パスワードを利用します。

"crypto ipsec client ezvpn 1812 [inside | outside] "

＜コマンド種別＞
インター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＞
インターフェースに Cisco Easy VPN リモートコンフィグレーションを適用します。
---

2. Cisco2811-Easy VPN サーバの設定

"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。

"encr 3des"
＜コマンド種別＞
ISAKMP ポリシーコンフィグレーションコマンド
＜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。この例では、168 ビット Data Encryption Standard（DES;データ暗号化規格）を指定します。

"hash md5"
＜コマンド種別＞
ISAKMP ポリシーコンフィグレーションコマンド
＜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。

"authentication pre-share"
＜コマンド種別＞
ISAKMP ポリシーコンフィグレーションコマンド
＜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、事前共有キーを指定します。

"group 2"
＜コマンド種別＞
ISAKMP ポリシーコンフィグレーションコマンド
＜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 client configuration group VPNCLIENT"
＜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＞
リモートクライアントにダウンロードされるアトリビュートを含む IKE ポリシーグループ "VPNCLIENT" を作成します。

"key cisco"
＜コマンド種別＞
ISAKMP グループポリシーコンフィギュレーションコマンド
＜コマンドの機能＞
グループ ポリシーの IKE 事前共有キーを指定します。

"dns 192.168.1.100"
＜コマンド種別＞
ISAKMP グループポリシーコンフィギュレーションコマンド
＜コマンドの機能＞
ポリシーグループ用プライマリおよびセカンダリ DNS サーバを指定します。

"wins 192.168.1.200"
＜コマンド種別＞
ISAKMP グループポリシーコンフィギュレーションコマンド
＜コマンドの機能＞
ポリシーグループ用プライマリおよびセカンダリ WINS サーバを指定します。

"domain cisco.com"
＜コマンド種別＞
ISAKMP グループポリシーコンフィギュレーションコマンド
＜コマンドの機能＞
ポリシーグループのドメイン名を指定します。

"pool ezvpn1"
＜コマンド種別＞
ISAKMP グループポリシーコンフィギュレーションコマンド
＜コマンドの機能＞
ローカルプールアドレスを定義します。この例では、プール名 "ezvpn1" で指定された IP アドレスプールが Cisco Easy VPN リモートクライアントに割り当てられるよう指定しています。

"save-password"
＜コマンド種別＞
ISAKMPグループポリシーコンフィギュレーションコマンド
＜コマンドの機能＞
Cisco Easy VPN リモートクライアントにパスワードをローカルにセーブする機能を許可する設定。この機能を有効にすることにより、リモートクライアントとなる PC やハードウェアクライアント上で、ユーザ名およびパスワードをセーブできるようになり、Xauth 中にユーザ名/パスワードが自動的にサーバ側に送信され、認証が行われます。

"ip local pool ezvpn1 192.168.10.1 192.168.10.100"
＜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＞
リモートピアがポイントツーポイントインターフェースに接続する際に使用される IP アドレスプールを指定します。この例では、 IP ローカルプール "ezvpn1" に IP アドレス 192.168.10.1 から 192.168.10.100 が割り当てられています。

"aaa new-model"
＜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＞
AAA アクセス制御モデルをイネーブルにします。

"aaa authentication login userauth local"
＜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＞

ユーザログイン時のAAA認証およびその認証方式を指定します。この例では、認証方式にローカル認証データベースを指定し、リスト名が"userauth" に設定されています。
この他に、認証データベースとして RADIUS サーバなどを設定することも可能です。

"aaa authorization network groupauth local"
＜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＞
PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定します。この例では、許可方式にローカル許可データベースを指定し、リスト名が"groupauth" に設定されています。
この他に、許可データベースとして RADIUS サーバなどを設定することも可能です。

"username ezvpn password 0 cisco"
"username remoteuser password cisco"
＜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＞
ユーザ名ベースの認証システムを確立します。
スモールオフィス 1812J 用に username ezvpn password cisco
リモートユーザ VPN クライアント用に username remoteuser password Cisco を設定します。
本設定例ではパスワードは簡略化のために暗号化なし（0）で記載しております。必要に応じ暗号化（7）にて設定してください。

"crypto ipsec transform-set myset 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 isakmp profile vpnclient-profile"
＜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＞
ISAKMP プロファイルを指定します。この例ではプロファイル名 "vpnclient-profile" を設定しています。

"match identity group VPNCLIENT"
＜コマンド種別＞
ISAKMP 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＞
ピアとの間で交換する識別子を ISAKMP プロファイルで指定します。交換する識別子がピア間で合致した場合、ISAKMP のプロファイルが引き出されます。その為、ISAKMP プロファイルに対して設定されている識別子は一意のものを利用する必要があります。この例では "VPNCLIENT" を識別子として指定しています。

"client authentication list userauth"
＜コマンド種別＞
ISAKMP 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＞
IKE Xauth の設定を指定します。リスト名は、AAA 認証設定部分で指定したリスト名と一致させる必要があります。この例ではリスト名 "userauth" を AAA 認証リストとして指定しています。

"isakmp authorization list groupauth"
＜コマンド種別＞
ISAKMP 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＞
アグレッシブモードでのトンネルアトリビュートに対して、AAA サーバからのグループ ポリシーのキールックアップ（IKE クエリ）を有効にします。リスト名は AAA 許可設定部分で指定したリスト名と一致させる必要があります。この例ではリスト名 "groupauth" を AAA 許可リストとして指定しています。

"client configuration address respond"
＜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＞
ルータの IKE モードを設定します。この例ではリモートクライアントからのモード設定要求にルータが応答するように設定しています。

"crypto dynamic-map dynmap 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＞
ダイナミック暗号マップエントリ "dynmap" を作成します。

"set transform-set myset"
＜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。この例ではトランスフォームセット "myset" を指定しています。

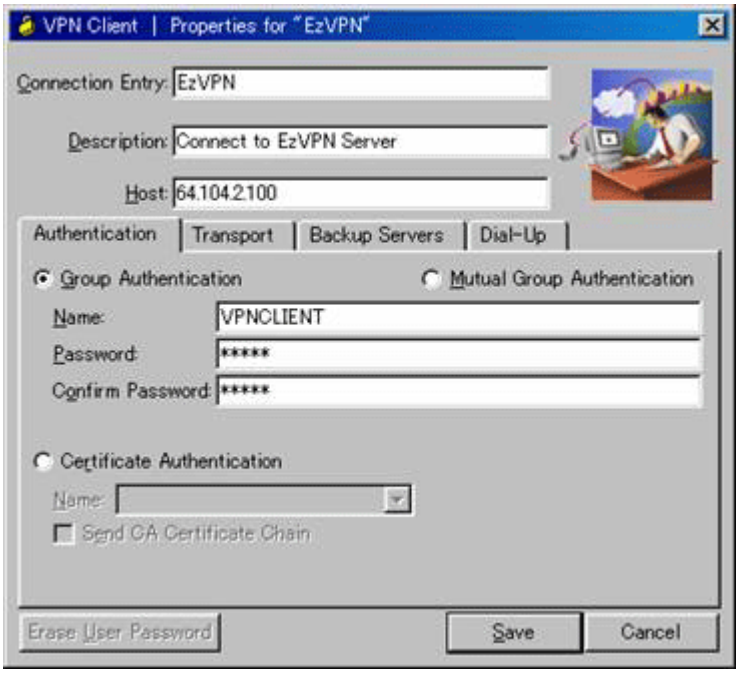
"set isakmp-profile vpnclient-profile"
＜コマンド種別＞
暗号マップコンフィギュレーションコマンド
＜コマンドの機能＞
IKE 交換の際に使用される ISAKMP プロファイルを指定します。この例では ISAKMP プロファイル "vpnclient-profile" を指定しています。

"crypto map ezvpnmap 1 ipsec-isakmp dynamic dynmap"
＜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。この例では暗号マップ "ezvpnmap" に対して IPSec SA の確立の為に IKE が使用され、設定されているダイナミック暗号マップ "dynmap" を参照するよう指定しています。ダイナミック暗号マップのポリシーテンプレートは IPSec リモートピアからのネゴシエーションリクエスト時に使用されます。

"crypto map ezvpnmap"
＜コマンド種別＞
インター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。この例では暗号マップ "ezvpnmap" を PPPoE セッションに利用するダイヤラーインターフェース 1 に適用します。
---

3. Cisco VPN Client ソフトウェアの設定

Cisco VPN Client ソフトウェア→ "New" より新しいコネクション用のエントリーを作成します。今回の例では Host (Cisco Easy VPN サーバ) のアドレスを "64.104.2.100"、Group Authentication 部分にグループ名 "VPNCLIENT"、パスワード "cisco" を指定し、コネクションエントリをセーブします。



＜VPN 接続時のユーザ認証＞
VPN 接続時、PC側では下記ユーザ認証用ポップアップの画面が表示されます。
ここでユーザ名 "remoteuser"、パスワード "cisco" を入力し、VPN サーバ側との認証を行います。

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。**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。
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

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
!
clock calendar-valid
Cisco Easy VPN サーバ側にて、複数のインターネットアクセスを保持してる際や接続しているクライアントのアドレスを他のルータに広報したい際には、サーバにて RRI（Reverse Route Injection）機能が必要になります。RRI を使用するとリモートユーザとの VPN 接続後、リモートユーザのインターフェースアドレスおよび LAN 側のネットワークアドレスが、サーバ側にインストールされます。サーバ側にて下記のような設定を追加してください。

!
crypto dynamic-map dynmap 1
reverse-route remote-peer
!

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。

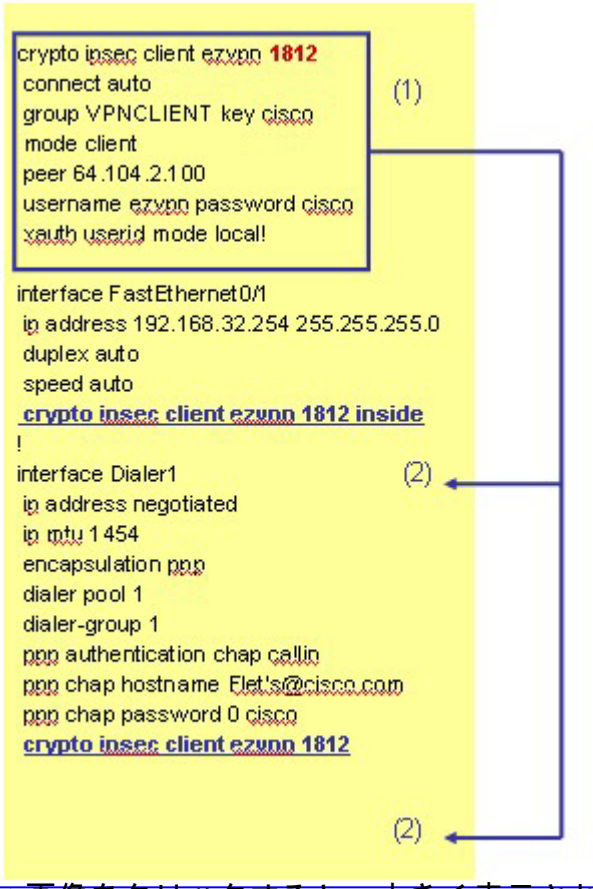
8.Cisco Easy VPN について

Cisco Easy VPN はスモールオフィスやテレワーカー、モバイルワーカーの為の Virtual Private Network（VPN）展開を容易にするソリューションです。Cisco Easy VPN ソリューションは VPN 接続に必要な設定をセンター側で一元管理し、今まで VPN 接続に必要だったリモート拠点における複雑な設定を最低限におさえることを可能にします。
Cisco ISR サービス統合型ルータシリーズ以外においても下記の様なプラットホームで Cisco

Easy VPN サーバの動作が可能です。
IOS ルータ 12.2 (8) T 以降
Cisco VPN 3000 シリーズ
PIX Firewall 6.0 以上
Cisco Easy VPN の設定手順を下記に本設定例を詳細に解説します。

1. Cisco Easy VPN リモートの設定

コンフィグ例と照らし合わせた形での手順を以下に示します。



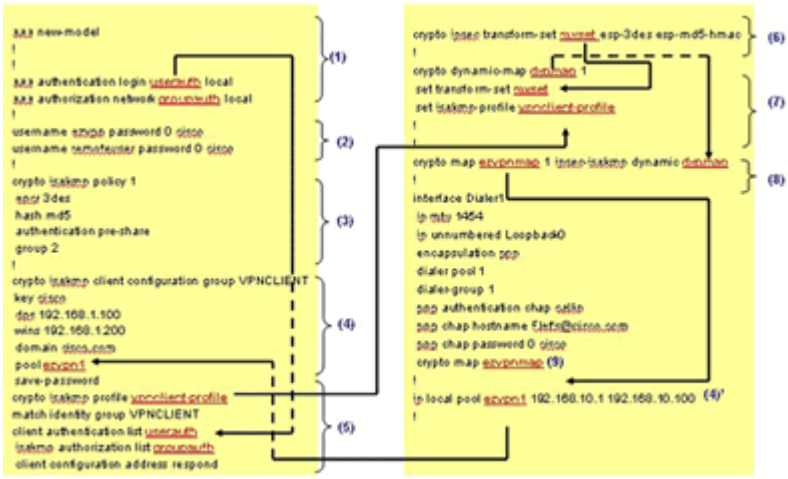
※ 画像をクリックすると、大きく表示されます。

詳細な手順については以下のとおりです。

1. Cisco Easy VPN リモートコンフィグレーションの設定
   センター側に VPN 接続を行う為のリモートコンフィグレーションを設定します。
2. リモートコンフィグレーションのインターフェースへの適用

2. Cisco Easy VPN サーバの設定

コンフィグ例と照らし合わせた形での手順を以下に示します。



※ 画像をクリックすると、大きく表示されます。

詳細な手順については以下のとおりです。

1. ポリシールックアップの有効化
   AAA コマンドによるポリシールックアップの有効化。AAA 認証および AAA 許可の設定を行います。
2. リモートクライアント認証用ユーザ名/パスワードの設定
3. IKE（Internet Key Exchange）ポリシーの設定
   リモートピアとの IKE ネゴシエーションの際使用される IKE ポリシーを設定します。暗号化 ハッシュアルゴリズム、認証方式などが含まれます。
4. グループポリシー情報の設定
   リモートクライアントがダウンロードするアトリビュートを含むグループポリシーを設定します。グループポリシーはリモートクライアント用 IP アドレスプール、DNS サーバや WINS サーバ、ドメイン名などの情報を含みます。
   この他に、リモートピア用 IP アドレスプールとして "ip local pool" の設定を行う必要があります。（（4）'）
5. ISAKMP プロファイルの設定
   ISAKMPプロファイルを設定します。ここでは"ポリシールックアップの有効化"で設定済の AAA 認証・許可の設定をひもづけます。
6. IPSec トランスフォームおよびプロトコルの設定
7. IPSec クリプト方式およびパラメータの設定
   IPSec クリプト方式を設定します。今回の例である、リモートクライアント側の WAN 側 IP アドレスが動的に変化するような環境の場合、ダイナミック暗号マップを利用した設定を行います。
   ダイナミック暗号マップエントリには、トランスフォームセットおよび ISAKMP プロファイルをひもづけます。
8. 暗号マップの作成 暗号マップを設定します。設定済のダイナミック暗号マップとひもづけます。
9. インターフェースへの暗号マップの適用

Updated: Jun 29, 2006 Document ID: jtac_20060127_4