VPN

今回はインターネット VPN の設定。また、LAN 同士の接続に IPSecVPN を使う。
モードはトランクモードを使用する。
VPN 装置＝ルータで設置

■設定手順
1.ACL の作成(誰から誰あてが VPN の対象)
拡張 ACL で設定する。
ex.
Router(config)#access-list 100 permit ip host 172.17.0.1 host 172.17.10.1

2.IKE ポリシー設定(鍵の交換用)
フェーズ 1 の暗号化、認証の設定を行う。
Router(config)#crypto isakmp policy 番号
Router(config-isakmp)#authentication pre-share　・・・認証モード(事前共有キー)
Router(config-isakmp)#encryption 3des　・・・暗号化アルゴリズム
Router(config-isakmp)#group 番号　・・・Deffie-Hellman のグループ(1,2,5)、送信時の暗号、数値が多いほど暗号化強度は強い。
Router(config-isakmp)#hash sha　・・・認証のアルゴリズム
Router(config-isakmp)#lifetime 秒　・・・SA の有効期限

3.鍵と IP アドレスの関連付け
対向ルータの IP アドレスとパスワードの関連付け
Router(config)#crypto isakmp key パスワード address IP アドレス(物理インターフェイス)

4.トランスフォームセット設定
IPSec での通信モードを設定
Router(config)#crypto ipsec transform-set 名前 {オプション}
ex.
Router(config)#crypto ipsec transform-set TS_HIGE esp-3des esp-sha-hmc
＊モードの指定(Packet Tracer ではない)
Router(config-crypto-trans)#mode {tunnel | transport}

5.IPSec ポリシー
map の定義・・・ACL との関連付けを行う
Router(config)#crypto map マップ名 シーケンス番号 ipsec-isakmp
Router(config-crypto-map)#match address ACL
Router(config-crypto-map)#set peer IP アドレス(対向ルータ)
Router(config-crypto-map)#set transform-set 名前(使用するトランスフォームセット)
Router_B(config-crypto-map)#set security-association lifetime seconds 秒・・・IPSecSA の生存時間

6.ポリシーをインタフェースに適応(インターフェイスモード)
Router(config-if)#crypto map 名前

7.デフォルトルート、スタティックルートの設定は必要

設定例(show running-config の抜粋)
```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
```

```
crypto isakmp key higechan address 200.1.1.2
!
!
!
crypto ipsec transform-set TS_HIGE esp-3des esp-sha-hmac
!
crypto map MAP_HIGE 1 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set TS_HIGE
 match address 100
!
!
interface FastEthernet0/0
 ip address 172.17.0.254 255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 ip address 200.1.1.1 255.255.255.252
 clock rate 2000000
 crypto map MAP_HIGE
!
!
ip classless
ip route 172.17.10.0 255.255.255.0 Serial0/0/0
!
access-list 100 permit ip 172.17.0.0 0.0.0.255 172.17.10.0 0.0.0.255
!
```

■OSPF でルーティング情報を交換しなさいとのこと。
　Cisco の IPSecVPN では、ブロードキャストやマルチキャストの通信はできない。ベンダーによってはできるらしい。そのため GRE でカプセル化して送る。そのためトンネルを掘る必要がある。
設定は基本的には変わりないが、若干異なるところがある。

■変更点
1.拡張 ACL
GRE(Generic Routing Encapsulation)を許可する。
Router(config)#access-list 100 permit gre host 200.1.1.1 host 200.1.1.2
＊IP アドレスは物理インターフェイスのもの
2～6 までは同じ。

7.GRE トンネルの作成
Router(config)#int tunnel 番号
Router(config-if)#ip address IP アドレス サブネットマスク　・・・トンネル用
Router(config-if)#tunnel source IP アドレス　・・・送信元物理インタフェース
Router(config-if)#tunnel destination IP アドレス　・・・宛先物理インタフェース
Router(config-if)#crypto map マップ名

8.OSPF の設定
Router(config)#router ospf 1
Router(config-router)#network IP アドレス ワイルドカードマスク area エリア ID
　　＊指定はトンネル、LAN を指定する。物理インタフェースは指定しない。

＊ルータにはデフォルトルートを設定する。
＊物理インターフェイスをプロトコルに設定しない。
http://www.cisco.com/c/ja_jp/support/docs/security-vpn/ipsec-negotiation-ike-protocols/ipsec-lantolan.html
http://moblog.absgexp.net/ikev1main/
http://www.network-engineer.info/cisco/cisco-greoveripsec%E3%81%AE%E8%A8%AD%E5%AE%9A%E6%96%B9%E6%B3%95/