

Configuration VPN routeur site à site

1. Activation et configuration des modules

On active les fonctions crypto du routeur :

```
(config)#crypto isakmp enable
```

Nous allons configurer la police qui détermine quelles encryptions on utilise, quelle Hash, quel type d'authentification, etc.

```
(config)#crypto isakmp policy 100
(config-isakmp)#authentication pre-share
(config-isakmp)#encryption des
(config-isakmp)#hash md5
(config-isakmp)#group 1
(config-isakmp)#lifetime 86400
(config-isakmp)#exit
```

lifetime : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

2. Configuration de la connexion

Ensuite, on configure la clef:

```
(config)#crypto isakmp key root address <IPdistant>
```

On configure maintenant les options de chiffrement des données:

```
(config)#crypto ipsec transform-set TEST esp-aes 128 esp-md5-hmac
```

esp : Signifie Encapsulation Security Protocol

Encryption : aes; **hash** : md5

On fixe ensuite une valeur de Lifetime :

```
(config)#crypto ipsec security-association lifetime seconds 1800
```

On crée une ACL qui va déterminer le trafic autorisé.

```
(config)#ip access-list extended VPN
(config-ext-nacl)#permit ip <Réseau> <masqueInverse> <Réseau>
<masqueInverse>
(config-ext-nacl)#exit
```

On configure maintenant la crypto map qui va associer l'access-list, le trafic, et la destination:

```
(config)#crypto map VPN 10 ipsec-isakmp
(config-crypto-map)#set peer <IPdistant>
(config-crypto-map)#set transform-set TEST
(config-crypto-map)#match address VPN
(config-crypto-map)#exit
```

3. Activation de la connexion

Enfin, on applique la crypto map sur l'interface de sortie :

```
(config)#interface <interface>
(config-if)#crypto map VPN
```