Travaux pratiques
VPN IPsec CISCO de site à site

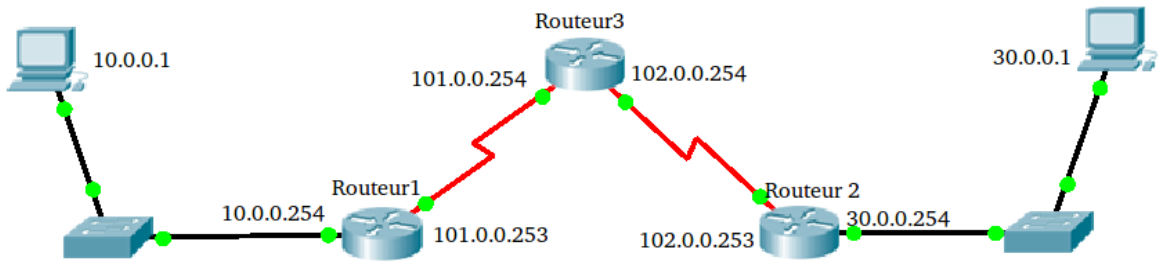
Je vais vous ici montrer comment créer une liaison d'interconnexion site à site, au travers d'un réseau non sécurisé, tel qu'Internet.

Cette liaison est un tunnel VPN IPsec utilisé afin de sécuriser une connexion entre deux sites.

Afin de mieux comprendre le principe du fonctionnement des VPN IPsec, je vous renvoi à la lecture du mémo IPsec que je vous avais remis.

Le TP vise à montrer la configuration de base pour l'établissement du VPN IPsec site à site (de routeur à routeur), reposant sur le protocole ISAKMP avec secret partagé.
Chaque site reproduit l'image d'un petit réseau local accédant à internet via un routeur NAT avec fonction "overload".

La topologie utilisée pour la maquette



Les routeurs utilisés sont des Cisco 2811.

Configuration de base de routeur1

```
Router>enable
Router#configure terminal
Router(config)#hostname Routeur1
Routeur1(config)#interface FastEthernet 0/0
Routeur1(config-if)#no shutdown
Routeur1(config-if)#ip address 10.0.0.254 255.0.0.0
Routeur1(config-if)#ip nat inside
Routeur1(config-if)#exit
Routeur1(config)#interface Serial 0/0/0
Routeur1(config-if)#no shutdown
Routeur1(config-if)#ip address 101.0.0.253 255.0.0.0
Routeur1(config-if)#ip nat outside
Routeur1(config-if)#exit
Routeur1(config)#ip route 0.0.0.0 0.0.0.0 101.0.0.254
Routeur1(config)#do wr
```

Mise en place de la fonction NAT sur Routeur1

```
Routeur1(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255
Routeur1(config)#access-list 100 permit ip 10.0.0.0 0.255.255.255 any
Routeur1(config)#ip nat inside source list 100 interface Serial 0/0/0 overload
Routeur1(config)#do wr
```

Configuration de base de routeur2

```
Router>enable
Router#configure terminal
Router(config)#hostname Routeur2
Routeur2(config)#interface FastEthernet 0/0
Routeur2(config-if)#no shutdown
Routeur2(config-if)#ip address 30.0.0.254 255.0.0.0
Routeur2(config-if)#ip nat inside
Routeur2(config-if)#exit
Routeur2(config)#interface Serial 0/0/0
Routeur2(config-if)#no shutdown
Routeur2(config-if)#ip address 102.0.0.253 255.0.0.0
Routeur2(config-if)#ip nat outside
Routeur2(config-if)#exit
Routeur2(config)#ip route 0.0.0.0 0.0.0.0 102.0.0.254
Routeur2(config)#do wr
```

Mise en place de la fonction NAT sur Routeur2

```
Routeur2(config)#access-list 100 deny ip 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
Routeur2(config)#access-list 100 permit ip 30.0.0.0 0.255.255.255 any
Routeur2(config)#ip nat inside source list 100 interface Serial 0/0/0 overload
Routeur2(config)#do wr
```

Configuration de base de routeur3 (le routeur central)

```
Router>enable
Router#configure terminal
Router(config)#hostname Routeur3
Router3(config)#interface Serial 0/0/0
Router3(config-if)#clock rate 2000000
Routeur3(config-if)#no shutdown
Routeur3(config-if)#ip address 101.0.0.254 255.0.0.0
Routeur3(config-if)#exit
Router3(config)#interface Serial 0/0/1
Router3(config-if)#clock rate 2000000
Routeur3(config-if)#no shutdown
Routeur3(config-if)#ip address 102.0.0.254 255.0.0.0
Routeur3(config-if)#exit
Routeur3(config)#ip route 10.0.0.0 255.0.0.0 101.0.0.253
Routeur3(config)#ip route 30.0.0.0 255.0.0.0 102.0.0.253
Routeur3(config-if)#do wr
```

Mise en place du tunnel VPN IPsec

Configuration de la négociation des clés (phase 1)

Détail de la configuration sur Routeur1

L'objectif est d'activer le protocole 'IKE', configurer le protocole 'ISAKMP' qui gère l'échange des clés et établir une stratégie de négociation des clés et d'établissement de la liaison VPN.

La clé pré partagée (PSK) sera définie avec pour valeur 'CLESECRETE'.

On va ici utiliser les paramètres suivants:

- Encryptage AES
- Mode de secret partagé PSK
- Authentification par clé pré-partagées
- Algorithme de hachage SHA (valeur par défaut)
- Méthode de distribution des clés partagées DH-2 (clés Diffie-Hellman groupe 2 - 1024bits)
- Durée de vie 86400 secondes (valeur par défaut)

On spécifie le protocole de hash utilisé, le type et la durée de validité des clés de sessions.

On indique ensuite si le routeur 'peer' (celui situé au bout du tunnel) est identifié par un nom ou son adresse.

```
Routeur1(config)#crypto isakmp enable                  → active IKE
Routeur1(config)#crypto isakmp policy 10               → active une politique IKE
Routeur1(config-isakmp)# encryption aes                → fixe l'algorithme de cryptage
Routeur1(config-isakmp)# authentication pre-share      → fixe la méthode d'authentification
Routeur1(config-isakmp)# hash sha                      → fixe l'algorithme de hachage
Routeur1(config-isakmp)# group 2                       → définit le groupe Diffie Hellman
Routeur1(config-isakmp)# lifetime 86400                → fixe la durée de vie de la SA
Routeur1(config-isakmp)#exit
Routeur1(config)# crypto isakmp key CLESECRETE address 102.0.0.253 → indique la clé partagée et
l'adresse du routeur pair qui doit être contacté
```

Configuration de la méthode de chiffrage des données (phase 2)

Il faut établir l'opération en trois phases

1. Créer la méthode de cryptage (transform-set) que je nomme "VPNLABO", avec "esp-aes" comme méthode de cryptage et "esp-sha-hmac" comme méthode d'authentification.

   On définit la durée de vie de la clé soit en durée (secondes).

2. Je créé ensuite une liste de contrôle d'accés (access-list) que je nomme "VPN", servant à identifier le trafic à traiter par le tunnel VPN. Pour Routeur1, ce sera le trafic d'origine 10.0.0.0/8 à destination de 30.0.0.0/8.

3. Je déclare finalement une carte de cryptage (crypto-map) que j'appelle "CARTEVPN", servant à spécifier le pair distant, le 'transform set' et l'access list.

Voici le détail de la configuration sur Routeur1

```
Routeur1(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeur1(config)#crypto ipsec security-association lifetime seconds 86400

Routeur1(config)#ip access-list extended VPN
Routeur1(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255
Routeur1(config-ext-nacl)#exit

Routeur1(config)#crypto map CARTEVPN 10 ipsec-isakmp
Routeur1(config-crypto-map)# match address VPN
Routeur1(config-crypto-map)#set peer 102.0.0.253
Routeur1(config-crypto-map)#set transform-set  VPNLABO
Routeur1(config-crypto-map)#exit
```

Il faut maintenant appliquer la crypto-map à l'interface WAN de Routeur1.

```
Routeur1(config)# interface serial 0/0/0
Routeur1(config-if)#crypto map CARTEVPN
Routeur1(config-if)#do wr
```

Le Routeur1 est prêt, il reste à faire l'équivalent sur Routeur2.

Voici le détail de la configuration sur Routeur2

La configuration est très similaire, il suffit d'adapter les adresses des réseaux à filtrer et préciser l'adresse du routeur pair.

```
Routeur2(config)#crypto isakmp enable
Routeur2(config)#crypto isakmp policy 10
Routeur2(config-isakmp)# encryption aes
Routeur2(config-isakmp)#authentication pre-share
Routeur2(config-isakmp)#hash sha
Routeur2(config-isakmp)#group 2
Routeur2(config-isakmp)#lifetime 86400
Routeur2(config-isakmp)#exit

Routeur2(config)# crypto isakmp key CLESECRETE address 101.0.0.253


Routeur2(config)# crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeur2(config)# crypto ipsec security-association lifetime seconds 86400
Routeur2(config)# ip access-list extended VPN
Routeur2(config-ext-nacl)# permit ip 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
Routeur2(config-ext-nacl)# exit

Routeur2(config)# crypto map CARTEVPN 10 ipsec-isakmp
Routeur2(config-crypto-map)# match address VPN
Routeur2(config-crypto-map)#set peer 101.0.0.253
Routeur2(config-crypto-map)#set transform-set  VPNLABO
Routeur2(config-crypto-map)#exit

Routeur2(config)# interface serial 0/0/0
Routeur2(config-if)#crypto map CARTEVPN
Routeur2(config-if)#do wr
```

Vérification du fonctionnement tunnel VPN

Pour établir la liaison VPN et vérifier le fonctionnement, il faut envoyer du trafic au travers du tunnel, on faisant un ping entre les stations.

Une fois le tunnel configuré, plusieurs commandes permettent de vérifier si le tunnel fonctionne

- Routeur1#show crypto isakmp policy
- Routeur1#show crypto isakmp sa
- Routeur1#show crypto ipsec sa