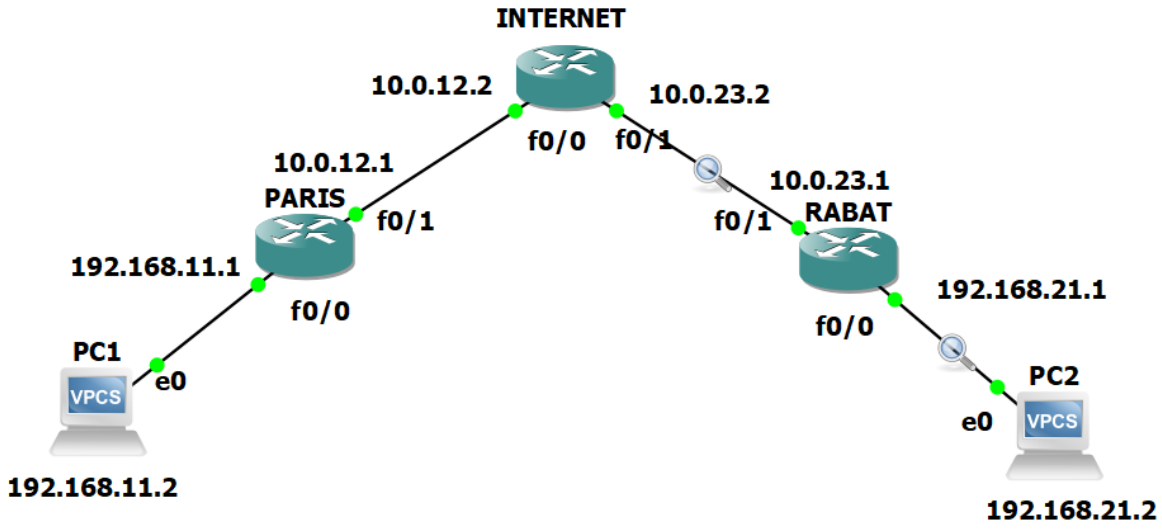
VPN IPsec CISCO de site à site

Création d'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.

Ce compte rendu 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.

La topologie utilisée pour le lab



Les routeurs utilisés sont des Cisco 7200.

Configuration des routeurs

```
PARIS(config)#interface fastEthernet 0/0
PARIS(config-if)#
PARIS(config-if)#ip add
PARIS(config-if)#ip address 192.168.11.1 255.255.255.0
PARIS(config-if)#no s
PARIS(config-if)#no sh
PARIS(config-if)#no shutdown
PARIS(config-if)#
*Mar 20 11:17:24.147: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
o up
*Mar 20 11:17:25.147: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEther
et0/0, changed state to up
PARIS(config-if)#exit
PARIS(config)#
PARIS(config)#int f
PARIS(config)#int fastEthernet 0/1
PARIS(config-if)#
PARIS(config-if)#
PARIS(config-if)#ip add
PARIS(config-if)#ip address 10.0.12.1 255.255.255.0
PARIS(config-if)#no sh
PARIS(config-if)#no shutdown
```

```
RABAT(config)#int fastEthernet 0/0
RABAT(config-if)#ip add
RABAT(config-if)#ip address 192.168.21.1 255.255.255.0
RABAT(config-if)#no shutdown
RABAT(config-if)#
*Mar 20 11:26:07.871: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar 20 11:26:08.871: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
RABAT(config-if)#exit
RABAT(config)#int fa
RABAT(config)#int fastEthernet 0/1
RABAT(config-if)#ip add
RABAT(config-if)#ip address 10.0.23.1 255.255.255.0
RABAT(config-if)#no shutdown
RABAT(config-if)#
*Mar 20 11:27:20.227: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar 20 11:27:21.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
```

```
INTERNET(config)#int fastEthernet 0/0
INTERNET(config-if)#ip add
INTERNET(config-if)#ip address 10.0.12.2 255.255.255.0
INTERNET(config-if)#no sh
INTERNET(config-if)#no shutdown
INTERNET(config-if)#
*Mar 20 11:22:34.791: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
o up
*Mar 20 11:22:35.791: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEther
et0/0, changed state to up
INTERNET(config-if)#exit
INTERNET(config)#int fa
INTERNET(config)#int fastEthernet 0/1
INTERNET(config-if)#ip add
INTERNET(config-if)#ip address 10.0.23.2 255.255.255.0
INTERNET(config-if)#no shutdown
INTERNET(config-if)#
*Mar 20 11:23:16.723: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state
o up
*Mar 20 11:23:17.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEther
et0/1, changed state to up
```

Mise en place du routage statique sur les routeurs (moins gourmand en ressource que le routage dynamique) :

```
PARIS(config)#ip route 10.0.23.0 255.255.255.0 10.0.12.2
PARIS(config)#ip route 192.168.21.0 255.255.255.0 10.0.12.2
```

```
INTERNET(config)#router eigrp 1
INTERNET(config-router)#network 0.0.0.0
```

Mise en place du tunnel VPN IPsec

Configuration de la négociation des clés (phase 1)

Détail de la configuration sur Routeur1

L'objectif est de 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
- 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 valeur par défaut (86400 secondes)

```
PARIS(config)#crypto isakmp policy 1
PARIS(config-isakmp)#encryption aes 128
PARIS(config-isakmp)#authentication pre-share
PARIS(config-isakmp)#group 2
PARIS(config-isakmp)#hash sha
PARIS(config-isakmp)#exit
```

On indique ensuite la clé partagée et l'adresse du routeur pair que l'on souhaite contacter (pour nous int fa0/1 du routeur rabat)

```
PARIS(config)#crypto isakmp key CLESECRETE address 10.0.23.1
```

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.

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 PARIS, ce sera le trafic d'origine 192.168.11.0/24 à destination de 192.168.21.0/24.)

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

Voici le détail de la configuration sur PARIS

1.
```
PARIS(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
PARIS(cfg-crypto-trans)#exit
```
2.
```
PARIS(config)#ip access-list extended VPN
PARIS(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 192.168.21.0 0.0.0.255
PARIS(config-ext-nacl)#exit
```
3.
```
PARIS(config)#crypto map MAPVPN 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
PARIS(config-crypto-map)#match address VPN
PARIS(config-crypto-map)#set peer 10.0.23.1
PARIS(config-crypto-map)#set transform-set VPNLABO
PARIS(config-crypto-map)#exit
```

Il faut maintenant appliquer la crypto-map à l'interface f0/1 du routeur PARIS.

```
PARIS(config)#int f0/1
PARIS(config-if)#crypto map MAPVPN
PARIS(config-if)#
*Mar 20 12:30:15.063: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
PARIS(config-if)#end
PARIS#
*Mar 20 12:30:36.359: %SYS-5-CONFIG_I: Configured from console by console
PARIS#write
Building configuration...
[OK]
```

Voici le détail de la configuration sur Routeur2

La configuration est similaire à celle du routeur 1, il suffit d'adapter les adresses des réseaux à filtrer et préciser l'adresse du routeur pair.

```
RABAT(config)#crypto isakmp policy 1
RABAT(config-isakmp)#encryption aes 128
RABAT(config-isakmp)#authentication pre-share
RABAT(config-isakmp)#group 2
RABAT(config-isakmp)#hash sha
RABAT(config-isakmp)#exit
```

```
RABAT(config)#crypto isakmp key CLESECRETE address 10.0.12.1
```

```
RABAT(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
RABAT(cfg-crypto-trans)#exit
```

(la commande est bien “permit ip 192.168.21.0.....” on ne voit pas le debut)

```
RABAT(config)#ip access-list extended VPN
RABAT(config-ext-nacl)#$92.168.21.0 0.0.0.255 192.168.11.0 0.0.0.255
RABAT(config-ext-nacl)#exit
```

```
RABAT(config)#crypto map MAPVPN 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RABAT(config-crypto-map)#match address VPN
RABAT(config-crypto-map)#set peer 10.0.12.1
RABAT(config-crypto-map)#set transform-set VPNLABO
RABAT(config-crypto-map)#exit
```

```
RABAT(config)#int fa0/1
RABAT(config-if)#crypto map MAPVPN
RABAT(config-if)#
*Mar 20 12:41:06.219: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
RABAT(config-if)#end
RABAT#
*Mar 20 12:41:15.147: %SYS-5-CONFIG_I: Configured from console by console
RABAT#write
Building configuration...
[OK]
```

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

- PAR#show crypto isakmp policy

```
PARIS#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

- PARIS#show crypto isakmp sa

```
PARIS#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.0.23.1       10.0.12.1       QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

- PARIS#show crypto ipsec sa

```
PARIS#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: MAPVPN, local addr 10.0.12.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.21.0/255.255.255.0/0/0)
   current_peer 10.0.23.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.12.1, remote crypto endpt.: 10.0.23.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)
     PFS (Y/N): N, DH group: none
```