CSTRSF TP N°4 : VPN, IPSec

Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau comme Internet. Il permet de faire transiter des informations, entre les différents membres de ce VPN, le tout de manière sécurisée.
On peut considérer qu'une connexion VPN revient à se connecter en réseau local mais en utilisant Internet. On peut ainsi communiquer avec les machines de ce réseau en prenant comme adresse de destination, l'adresse IP local de la machine que l'on veut atteindre.

Il existe plusieurs types de VPN fonctionnant sur différentes couches réseau, voici les VPN que nous pouvons mettre en place sur un serveur dédié ou à la maison :

- **PPTP** : Facile à mettre en place, mais beaucoup d'inconvénients liés à la lourdeur du protocole de transport GRE, le matériel réseau (routeur ADSL, wifi, doit être compatible avec le PPTP)
- **Ipsec** : Plus efficace que le PPTP en termes de performance, mais aussi très contraignant au niveau de la mise en place
- **OpenVPN** : La Rolls des VPN, il suffit de se prendre un peu la tête sur la mise en place, mais son utilisation est très souple.

Dans notre cas nous allons utiliser IPsec.

Configuration du VPN IPSEC

1.Activer ISAKMP : R1(config)#crypto isakmp enable

2.**Détermination de la politique ISAKMP**

Pour qu'il y ait communication IPSec possible, il faut que les 2 peers trouvent un accord sur une politique ISAKMP commune. Une politique ISAKM contient: l'Algorithme d'encryption, l'Algorithme de hachage,le groupe Diffie-Hellman et la durée de vie du chiffrement de la clé.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
```

3.Configuration de la clé : R1(config)# crypto isakmp key 12345 address 10.2.2.1

4.Création du Transform Set : *Le transform set est l'association d'une méthode de chiffrement et d'authentification. Cette phase va permettre durant l'établissement d'une association (basée sur ISAKMP) de se mettre d'accord durant les échanges afin de fixer la méthode de sécurisation des*

données. Les paramètres du transform set devrons être les mêmes des deux côtés. Le transform set va permettre de sécuriser les flux déterminés à partir d'une access-list associée à une crypto map.

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

5.Configuration de la crypto map : La carte de cryptage (ou crypto map) permet de lier les SA négociées et la politique de sécurité (SP : Security Policy). En d'autres termes, elle permet de renseigner :

- L'autre extrémité du tunnel vers lequel le trafic IPSec devrait être envoyé ;
- L'adresse locale à employer pour le trafic d'IPSec ;
- Quelle sécurité d'IPSec devrait être appliquée à ce trafic (transform-sets)
- Durée de vie de du tunnel IPSec

R1(config)#crypto map nom_de_map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900

6.Configuration d'une liste de contrôle d'accès : Il faut configurer une liste d'accès qui définit le trafic à sécuriser.

R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

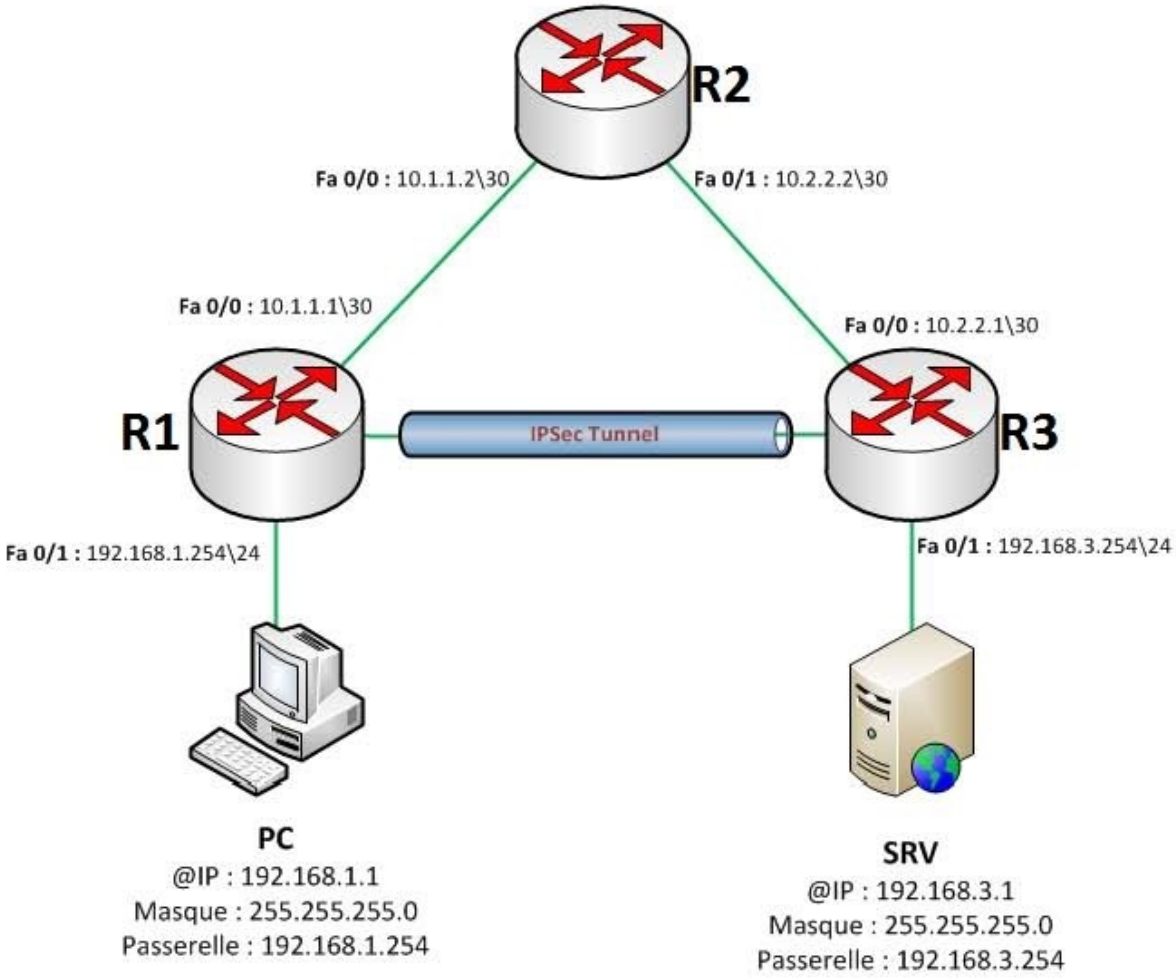
7.Activer ISAKMP sur l'interface concernée : Il faut lier la crypto map ainsi définie à une interface du routeur par laquelle le trafic d'IPSec passera. Tout trafic arrivant ou sortant de cette interface est comparé avec le trafic à sécuriser défini dans une liste d'accès: s'il y a correspondance ce dernier est chiffré.

R1(config)#interface FastEthernet 0/0
R1(config-if)#crypto map m1ssice2

R1(config-if)#exit

On procède de la même manière à la configuration de routeur R3

8.Vérifications : On vérifie la map m1ssice2 : R1#show cypto map



I) Configurations de base

Nous commencerons par configurer notre PC et notre serveur en leur attribuant la bonne configuration réseau. Nous attaquerons ensuite la configuration du routeur R1 :

1) Routeur R1

On commence par le Hostname :

```
Router#configure terminal
Router(config)#hostname R1
```

Nous configurons ensuite les adresses IP des deux interfaces :

```
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage. J'ai choisi de faire du routage RIP, c'est un choix qui n'engage que moi et qui ne vous empêche pas de faire un routage OSPF ou routage statique si

vous préférez.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#exit
```

La configuration de base de notre routeur R1 est terminée.

2) Routeur R2

Même procédure pour notre routeur R2 :

On commence par le Hostname :

```
Router#configure terminal
Router(config)#hostname R2
```

Nous configurons ensuite les adresses IP des deux interfaces :

```
R2(config)#interface FastEthernet 0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 10.2.2.0
R2(config-router)#network 10.1.1.0
R2(config-router)#exit
```

La configuration de base de notre routeur R2 est terminée.

3) Routeur R3

Même procédure pour notre routeur R3 :

On commence par le Hostname :

```
Router#configure terminal
Router(config)#hostname R3
```

Nous configurons ensuite les adresses IP des deux interfaces :

```
R3(config)#interface FastEthernet 0/1
R3(config-if)#ip address 192.168.3.254 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface FastEthernet 0/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
```

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#exit
```

La configuration de base de notre routeur R3 est terminée.

4) Test de fonctionnement

Nous essayons de pinger le serveur depuis le PC :

```
PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=27ms TTL=125
Reply from 192.168.3.1: bytes=32 time=23ms TTL=125
Reply from 192.168.3.1: bytes=32 time=26ms TTL=125
Reply from 192.168.3.1: bytes=32 time=19ms TTL=125

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 27ms, Average = 23ms
```

Voici le fichier Packet tracert représentant la configuration de base de notre réseau :

IV) Configuration du VPN

Il faut savoir que le VPN se configure juste sur les Routeurs d'extrémités dans notre cas R1 et R3 on n'aura aucune modification à faire sur R2.

1) Configuration VPN sur R1

Première étape :

Commençons par notre routeur R1, vous devez vérifier que l'IOS de vos routeurs supporte le VPN. On active ensuite les fonctions crypto du routeur :

```
R1(config)#crypto isakmp enable
```

Cette fonction est activée par défaut sur les IOS avec les options cryptographiques.

Deuxième étape :

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

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
```

group 5 : Spécifie l'identifiant Diffie-Hellman
lifetime : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

Troisième étape :

Ensuite nous devons configurer la clef :

```
R1(config)#crypto isakmp key mot_de_passe address 10.2.2.1
```

Sur certains routeur avec certains IOS la commande ne fonctionne pas car le routeur demande si le mot de passe doit être chiffré ou pas, tapez cette commande :

```
R1(config)#crypto isakmp key 6 mot_de_passe address 10.2.2.1
```

Quatrième étape :

Configurons les options de transformations des données :

```
R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
```

esp : Signifie **Encapsulation Security Protocol**

N'oubliez pas d'utiliser les mêmes protocoles d'encryptions et de Hash utilisés dans la première étape.

Dans notre cas :

Encryption : 3des
hash : md5

On fixe ensuite une valeur de Lifetime :

```
R1(config)#crypto ipsec security-association lifetime seconds 1800
```

Cinquième étape :

La 5éme étape consiste à créer une ACL qui va déterminer le trafic autorisé.

```
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Dernière étape de la configuration :

Dans cette dernière étape nous configurons la crypto map qui va associé l'access-list, le traffic, et la destination :

```
R1(config)#crypto map nom_de_map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
```

La configuration de R1 est presque terminée nous devons appliquer la crypto map sur l'interface de sortie :

Dans notre cas FastEthernet 0/0.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#crypto map nom_de_map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Un message vous indique que la crypto map fonctionne.

2) Configuration VPN sur R3

On refait la même configuration que sur R1 :

Première étape :

```
R3(config)#crypto isakmp enable
```

Deuxième étape :

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#hash md5
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit
```

Troisième étape :

```
R3(config)#crypto isakmp key mot_de_passe address 10.1.1.1
```

ou

```
R3(config)#crypto isakmp key 6 mot_de_passe address 10.1.1.1
```

Quatrième étape :

```
R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(config)#crypto ipsec security-association lifetime seconds 1800
```

Cinquième étape :

```
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Dernière étape de la configuration :

```
R3(config)#crypto map nom_de_map 10 ipsec-isakmp
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#exit
R3(config)#interface FastEthernet 0/0
R3(config-if)#crypto map nom_de_map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Voici le fichier Packet tracert représentant la configuration avec le VPN IPsec :

3) Vérifications

On réalise un ping pour voir si la communication n'est pas coupée :

```
PC>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.1: bytes=32 time=22ms TTL=126
Reply from 192.168.3.1: bytes=32 time=20ms TTL=126
Reply from 192.168.3.1: bytes=32 time=18ms TTL=126

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 22ms, Average = 20ms
```

Nous vérifions les informations retournées par le VPN sur R1 et R3 :

```
R1#show crypto ipsec transform-set
Transform set 50: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

```
R3#show crypto ipsec transform-set
Transform set 50: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Nous vérifions la map vpn :

Pour information j'ai nommé ma map "vpn".

```
R1#show crypto map
Crypto Map vpn 10 ipsec-isakmp
        Peer = 10.2.2.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.25
5
        Current peer: 10.2.2.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): Y
        Transform sets={
                50,
        }
        Interfaces using crypto map vpn:
                FastEthernet0/0
```

```
R3#show crypto map
Crypto Map vpn 10 ipsec-isakmp
        Peer = 10.1.1.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.25
5
        Current peer: 10.1.1.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): Y
        Transform sets={
                50,
        }
        Interfaces using crypto map vpn:
                FastEthernet0/0
```

On vérifie les opérations d'IPsec :

```
R1#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: vpn, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.:10.2.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x1E396F8C(507080588)

     inbound esp sas:
      spi: 0x1A85342C(444937260)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4525504/517)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1E396F8C(507080588)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4525504/517)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

```
R3#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: vpn, local addr 10.2.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #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.: 10.2.2.1, remote crypto endpt.:10.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x1A85342C(444937260)

     inbound esp sas:
      spi: 0x1E396F8C(507080588)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4525504/457)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A85342C(444937260)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4525504/457)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Pour finir on vérifie les opérations d'Isakmp :

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.2.1        10.1.1.1        QM_IDLE           1073    0 ACTIVE


R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.1.1.1        10.2.2.1        QM_IDLE           1063    0 ACTIVE
```