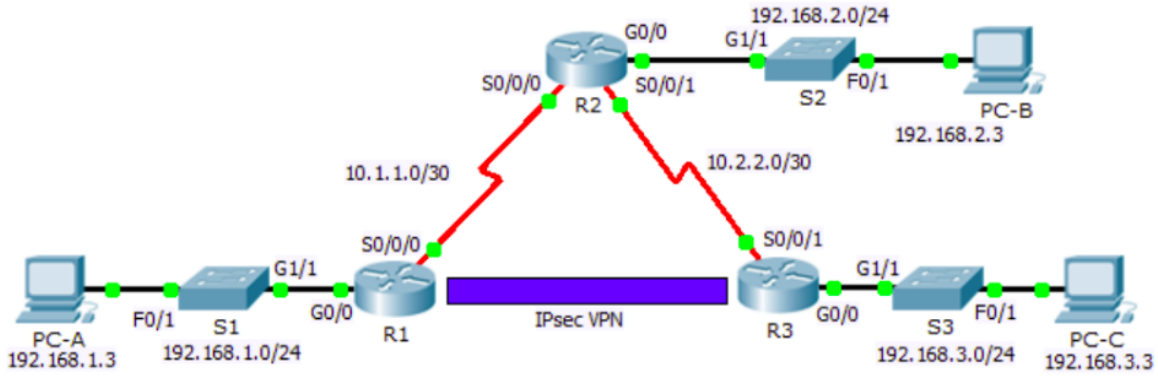
# TP 03: Configuration d'un VPN LAN to LAN

**<u>Scénario</u> : La topologie du réseau montre trois routeurs et la tâche consiste à configurer *R1* et *R3* pour prendre en charge un *VPN IPsec* <u>site à site</u> lorsque le trafic circule entre leurs réseaux locaux respectifs. Le tunnel VPN IPsec va de R1 à R3 via R2. R2 agit comme un intermédiaire et n'a aucune connaissance du VPN. IPsec assure la transmission sécurisée d'informations sensibles sur des réseaux non protégés, tels qu'Internet. IPsec fonctionne au niveau de la couche réseau et protège et authentifie les paquets IP entre les périphériques IPsec participants, tels que Cisco routeurs.**




**Addressing Table**

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| R1 | G0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| R2 | G0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| R3 | G0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |

## Partie 00 : Création de la topologie, adressage et Routage

1. Créer la topologie ci-dessus et Affecter les adresses ***ip*** aux interfaces.
2. Configurer le routage dynamique **Rip** dans les **3** routeurs, par exemple dans **R1** :
   - Router(config) # **router rip**
   - Router(config-router) # **version 2**
   - Router(config-router) #no **auto-summary**
   - Router(config-router) **#network 10.1.1.0**
   - Router(config-router) **#network 192.168.1.0**
3. Tester la connectivité entre les réseaux en utilisant la commande Ping.

### ISAKMP Phase 1 Policy Parameters

| Parameters | | R1 | R3 |
|---|---|---|---|
| Key distribution method | Manual or **ISAKMP** | ISAKMP | ISAKMP |
| Encryption algorithm | **DES**, 3DES, or AES | AES | AES |
| Hash algorithm | MD5 or **SHA-1** | SHA-1 | SHA-1 |
| Authentication method | Pre-shared keys or **RSA** | pre-share | pre-share |
| Key exchange | DH Group **1**, 2, or 5 | DH 2 | DH 2 |
| IKE SA Lifetime | 86400 seconds or less | 86400 | 86400 |
| ISAKMP Key | | cisco | cisco |

**Bolded** parameters are defaults. Other parameters need to be explicitly configured.

### IPsec Phase 2 Policy Parameters

| Parameters | R1 | R3 |
|---|---|---|
| Transform Set | VPN-SET | VPN-SET |
| Peer Hostname | R3 | R1 |
| Peer IP Address | 10.2.2.2 | 10.1.1.2 |
| Network to be encrypted | 192.168.1.0/24 | 192.168.3.0/24 |
| Crypto Map name | VPN-MAP | VPN-MAP |
| SA Establishment | ipsec-isakmp | ipsec-isakmp |

## Partie 01: Activation de la fonctionnalité du sécurité dans les routeurs R1 &R3

a. Issue the **show version** command in the user EXEC or privileged EXEC mode to verify that the Security Technology Package license is activated.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

b. If not, activate the **securityk9** module for the next boot of the router, accept the license, save the configuration, and reboot.

```
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. After the reloading is completed, issue the **show version** again to verify the Security Technology Package license activation.

```
Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Repeat Steps 1a to 1c with **R3**.

## Partie 02 : Configuration du protocole IPsec dans le routeur R1

## 1 Identifiez le trafic intéressant sur R1 :

Configurez l'**ACL 110** pour identifier le trafic du LAN sur **R1** vers le LAN sur **R3** comme **intéressant**. Ce trafic intéressant déclenchera la mise en œuvre du **VPN IPsec** lorsqu'il y a du trafic entre les LAN **R1** à **R3**. Tout autre trafic provenant des réseaux locaux ne sera pas chiffré.

Router(config) # **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

## 2 Configurez la stratégie IKE Phase 1 ISAKMP sur R1.

Configurez les propriétés de la stratégie **crypto ISAKMP 10** sur R1 avec la clé de chiffrement partagée vpnpa55. Reportez-vous au tableau **ISAKMP** Phase 1 pour les paramètres spécifiques à configurer. Les valeurs par défaut ne doivent pas être configurées. Donc, seule la méthode de chiffrement, la méthode d'échange de clés et la méthode DH doivent être configurées.

*Router(config) # crypto isakmp policy 10*

*Router(config-isakmp) # encryption aes*

*Router(config-isakmp) # authentication pre-share*

*Router(config-isakmp) # group 2*

*Router(config-isakmp) # exit*

*Router(config) # crypto isakmp key cisco address **10.2.2.2***

## 3 Configurez la stratégie IPsec IKE Phase 2 sur R1.

a. Créez le jeu de transformation VPN-SET pour utiliser **esp-aes** et **esp-sha-hmac**.

b. Créez la carte de chiffrement **VPN-MAP** qui lie tous les paramètres Phase2 ensemble. Utilisez le numéro de séquence 10 et identifiez-le comme une carte ipsec-isakmp.

*Router(config) # crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac*

*Router(config) # crypto map VPN-MAP 10 ipsec-isakmp*

*Router(config-crypto-map) # description VPN connection to R3*

*Router(config-crypto-map) # set peer 10.2.2.2*

*Router(config-crypto-map) # set transform-set VPN-SET*

*Router(config-crypto-map) # match address 110* *Router(config-crypto-map) # exit*

## 4 Configurer la crypto map sur l'interface sortante

Liez la carte de chiffrement **VPN-MAP** à l'interface **s 0/0/0** sortante

*Router(config) # interface s0/0/0*

*Router(config-if) # crypto map VPN-MAP*

## Partie 03 : Configuration du protocole IPsec dans le routeur R3 (Mêmes étapes R1)

## Partie 04 : Vérification du VPN IPsec

### 1- Vérifiez le tunnel avant tout trafic intéressant.

Issue the **show crypto ipsec sa** command on **R1**. Notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #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.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
<output omitted>
```

**2- Créer un trafic intéressant.** Envoyez une requête ping à **PC-C** depuis **PC-A**.

**3- Vérifiez le tunnel après un trafic intéressant.** Sur R1, relancez ***show* crypto ipsec sa**.

On **R1**, re-issue the **show crypto ipsec sa** command. Now notice that the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   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 10.2.2.2 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.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0A496941(172583233)
<output omitted>
```

**4- Créer un trafic sans intérêt.** Envoyez une requête ping à **PC-B** à partir de **PC-A**.

L'émission d'un ping du routeur **R1** vers PC-B ou **R2** vers PC-A n'est pas un trafic intéressant.

**5- Vérifiez le tunnel.** Sur R1, relancez la commande **show crypto ipsec sa.** On note que le nombre de paquets n'est pas changé ce qui prouve que le trafic sans intérêt n'est pas crypté.