Packet Tracer : configuration de VPN (facultatif)

Topologie

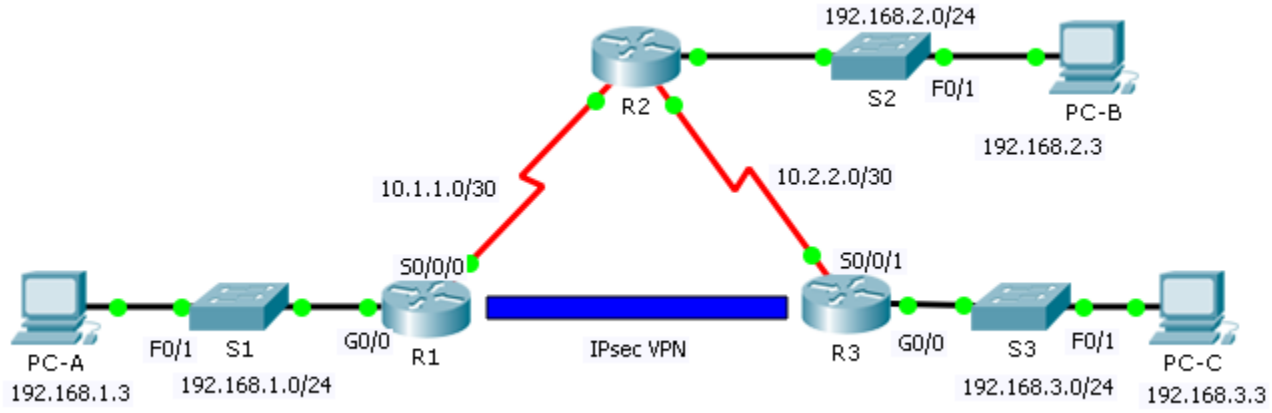

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
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

Paramètres de stratégie ISAKMP de phase 1

Paramètres		R1	R3
Méthode de distribution de clé	Mode manuel ou **ISAKMP**	ISAKMP	ISAKMP
Algorithme de chiffrement	**DES**, 3DES ou AES	AES	AES
Algorithme de hachage	MD5 ou **SHA-1**	SHA-1	SHA-1
Méthode d'authentification	Clés prépartagées ou **RSA**	prépartage	prépartage
Échange de clés	Groupe DH **1**, 2 ou 5	DH 2	DH 2
Durée de vie des associations de sécurité IKE	86400 secondes ou moins	86400	86400
Clé ISAKMP		cisco	cisco

Les paramètres en gras sont les valeurs par défaut. D'autres paramètres doivent être explicitement configurés.

Paramètres de stratégie IPsec de phase 2

Paramètres	R1	R3
Transform Set	VPN-SET	VPN-SET
Nom d'hôte d'homologue	R3	R1
Adresse IP d'homologue	10.2.2.2	10.1.1.2
Réseau à chiffrer	192.168.1.0/24	192.168.3.0/24
Nom de carte de chiffrement	VPN-MAP	VPN-MAP
Établissement d'association de sécurité	ipsec-isakmp	ipsec-isakmp

Objectifs

Partie 1 : activation des fonctions de sécurité

Partie 2 : configuration des paramètres IPsec sur R1

Partie 3 : configuration des paramètres IPsec sur R3

Partie 4 : vérification du VPN IPsec

Scénario

Au cours de cet exercice, vous allez configurer deux routeurs de telle sorte qu'ils prennent en charge un VPN IPsec de site à site pour le trafic issu de leurs LAN respectifs. Le trafic VPN IPsec passera par un autre routeur qui n'a pas connaissance du VPN. IPsec permet la transmission sécurisée d'informations sensibles sur des réseaux non protégés tels qu'Internet. IPsec agit en tant que couche réseau, qui protège et authentifie les paquets IP entre les périphériques IPsec participants (homologues), comme les routeurs Cisco.

Partie 1 : Activation des fonctions de sécurité

Étape 1 : Activez le module securityk9.

La licence du pack technologique de sécurité doit être activée pour pouvoir effectuer cet exercice.

Remarque : le mot de passe du mode d'exécution utilisateur et celui du mode d'exécution privilégié sont tous les deux **cisco**.

a. Exécutez la commande **show version** en mode d'exécution utilisateur ou en mode d'exécution privilégié pour vérifier que la licence du pack technologique de sécurité est activée.

```
-----------------------------------------------------------------
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. Si ce n'est pas le cas, activez le module **securityk9** pour le prochain démarrage du routeur, acceptez la licence, enregistrez la configuration et redémarrez.

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

c. Après le redémarrage, exécutez à nouveau la commande **show version** afin de vérifier l'activation de la licence du pack technologique de sécurité.

```
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. Répétez les étapes 1a à 1c avec **R3**.

Partie 2 : Configuration des paramètres IPsec sur R1

Étape 1 : Tester la connectivité

Envoyez une requête ping à partir de **PC-A** vers **PC-C**.

Étape 2 : Identifiez le trafic intéressant sur R1.

Configurez la liste de contrôle d'accès 110 afin d'identifier le trafic issu du LAN sur **R1** vers le LAN sur **R3** comme étant le trafic intéressant. Ce trafic intéressant déclenchera le réseau privé virtuel IPsec à implémenter, pour autant qu'il y ait du trafic entre les LAN de **R1** et de **R3**. Tout autre trafic provenant des LAN ne sera pas chiffré. Rappelez-vous qu'en raison de l'instruction deny any implicite, il n'est pas nécessaire d'ajouter l'instruction à la liste.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
```

Étape 3 : Configurez les propriétés ISAKMP de phase 1 sur R1.

Configurez les propriétés **10** de la stratégie de chiffrement ISAKMP sur **R1** avec la clé de chiffrement partagée **cisco**. Référez-vous au tableau ISAKMP de phase 1 pour connaître les paramètres spécifiques à configurer. Les valeurs par défaut ne doivent pas être configurées et par conséquent seules les méthodes de chiffrement, d'échange de clés et DH doivent être configurées.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

Étape 4 : Configurez les propriétés ISAKMP de phase 2 sur R1.

Créez le transform-set **VPN-SET** de manière à utiliser **esp-3des** et **esp-sha-hmac**. Créez ensuite la carte de chiffrement **VPN-MAP** qui lie ensemble tous les paramètres de phase 2. Utilisez le numéro d'ordre **10** et identifiez-le comme étant une carte **ipsec-isakmp**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Étape 5 : Configurez la carte de chiffrement sur l'interface de sortie.

Enfin, liez la carte de chiffrement **VPN-MAP** à l'interface Serial 0/0/0 de sortie. **Remarque** : cet exercice n'est pas noté.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Partie 3 : Configuration des paramètres IPsec sur R3

Étape 1 : Configurez le routeur R3 de manière à prendre en charge un VPN de site à site avec R1.

Configurez maintenant les paramètres réciproques sur **R3**. Configurez la liste de contrôle d'accès **110** en identifiant le trafic issu du LAN sur **R3** vers le LAN sur **R1** comme étant le trafic intéressant.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Étape 2 : Configurez les propriétés ISAKMP de phase 1 sur R3.

Configurez les propriétés **10** de la stratégie de chiffrement ISAKMP sur **R3** avec la clé de chiffrement partagée **cisco**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

Étape 3 : Configurez les propriétés ISAKMP de phase 2 sur R1.

Comme vous l'avez fait sur **R1**, créez le transform-set **VPN-SET** de manière à utiliser **esp-3des** et **esp-sha-hmac**. Créez ensuite la carte de chiffrement **VPN-MAP** qui lie ensemble tous les paramètres de phase 2. Utilisez le numéro d'ordre **10** et identifiez-le comme étant une carte **ipsec-isakmp**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Étape 4 : Configurez la carte de chiffrement sur l'interface de sortie.

Enfin, liez la carte de chiffrement **VPN-MAP** à l'interface Serial 0/0/1 de sortie. **Remarque** : cet exercice n'est pas noté.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Partie 4 : Vérification du VPN IPsec

Étape 1 : Vérifiez le tunnel avant le trafic intéressant.

Exécutez la commande **show crypto ipsec sa** sur **R1**. Notez que le nombre de paquets encapsulés, chiffrés, décapsulés et déchiffrés est défini à 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)
<Résultat omis>
```

Étape 2 : Créez du trafic intéressant.

Envoyez une requête ping de **PC-C** à **PC-A**.

Étape 3 : Vérifiez le tunnel après le trafic intéressant.

Sur **R1**, réexécutez la commande **show crypto ipsec sa**. Notez maintenant que le nombre de paquets est supérieur à 0, ce qui indique que le tunnel VPN IPsec fonctionne.

```
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)
<Résultat omis>
```

Étape 4 : Créez du trafic non intéressant.

Envoyez une requête ping de **PC-B** vers **PC-A**.

Étape 5 : Vérifiez le tunnel.

Sur **R1**, réexécutez la commande **show crypto ipsec sa**. Remarquez pour terminer que le nombre de paquets n'a pas changé, ce qui prouve que le trafic qui n'est pas intéressant n'est pas chiffré.