Packet Tracer : configuration de GRE sur IPsec (facultatif)

Topologie

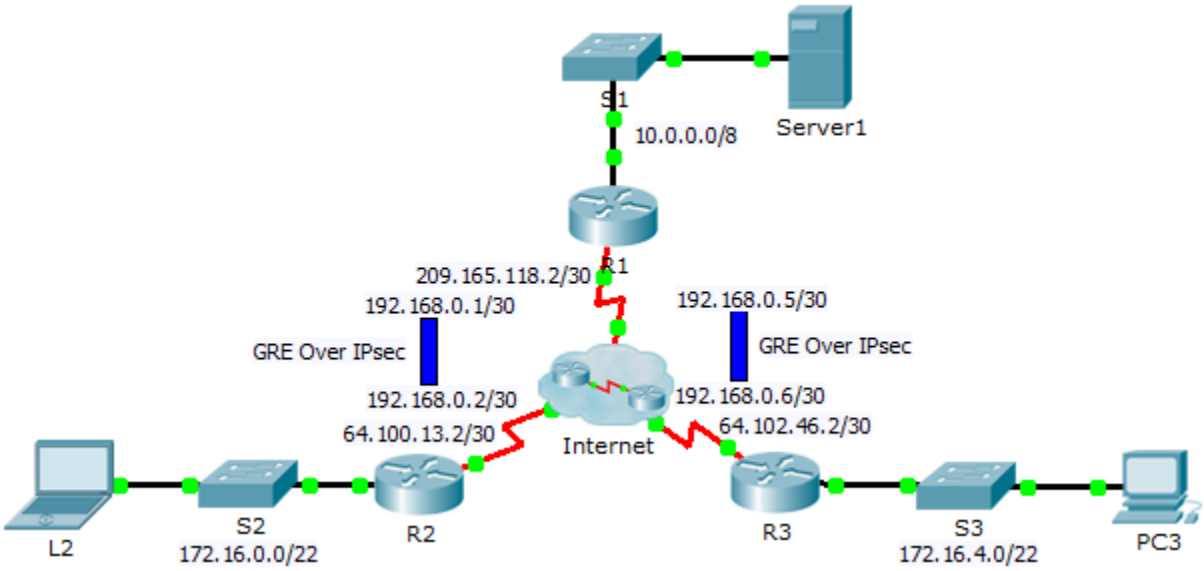

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	S0/0/0	209.165.118.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.1	255.255.255.252	N/A
	Tunnel 1	192.168.0.5	255.255.255.252	N/A
R2	G0/0	172.16.0.1	255.255.252.0	N/A
	S0/0/0	64.100.13.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.2	255.255.255.252	N/A
R3	G0/0	172.16.4.1	255.255.252.0	N/A
	S0/0/0	64.102.46.2	255.255.255.252	N/A
	Tunnel 0	192.168.0.6	255.255.255.252	N/A
Server1	NIC	10.0.0.2	255.0.0.0	10.0.0.1
L2	NIC	172.16.0.2	255.255.252.0	172.16.0.1
PC3	NIC	172.16.4.2	255.255.252.0	172.16.4.1

Objectifs

Partie 1 : vérification de la connectivité du routeur

Partie 2 : activation des fonctions de sécurité

Partie 3 : configuration des paramètres IPsec

Partie 4 : configuration de tunnels GRE sur IPsec

Partie 5 : vérification de la connectivité

Scénario

Vous êtes l'administrateur réseau d'une entreprise qui souhaite configurer un tunnel GRE sur IPsec vers des bureaux distants. Tous les réseaux sont configurés localement et ils n'ont besoin que du tunnel et du chiffrement qui ont été configurés.

Partie 1 : Vérifier la connectivité du routeur

Étape 1 : Envoyez une requête ping à R2 et R3 à partir de R1.

a. À partir de **R1**, envoyez une requête ping à l'adresse IP de S0/0/0 sur **R2.**

b. À partir de **R1**, envoyez une requête ping à l'adresse IP de S0/0/0 sur **R3.**

Étape 2 : Envoyez une requête ping à Server1 à partir de L2 et de PC3.

Essayez d'envoyer une requête ping à l'adresse IP de **Server1** à partir de **L2**. Nous recommencerons ce test après avoir configuré le tunnel GRE sur IPsec. Quels étaient les résultats des requêtes ping ? Pourquoi ?

Étape 3 : Envoyez une requête ping à PC3 à partir de L2.

Essayez d'envoyer une requête ping à l'adresse IP de **PC3** à partir de **L2**. Nous recommencerons ce test après avoir configuré le tunnel GRE sur IPsec. Quels étaient les résultats des requêtes ping ? Pourquoi ?

Partie 2 : 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.

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
<Accept the License>
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 **R2** et **R3**.

Partie 3 : Configuration des paramètres IPsec

Étape 1 : Identifiez le trafic intéressant sur R1.

a. Configurez la liste de contrôle d'accès 102 afin d'identifier le trafic issu du LAN sur **R1** vers le LAN sur **R2** 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 **R2**. 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 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0
0.0.3.255
```

b. Répétez l'étape 1a pour configurer la liste de contrôle d'accès 103 en vue d'identifier le trafic sur le LAN de R3 comme étant le trafic intéressant.

Étape 2 : Configurez les propriétés ISAKMP de phase 1 sur R1.

a. Configurez les propriétés **102** de la stratégie de chiffrement ISAKMP sur **R1** avec la clé de chiffrement partagée **cisco**. 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 102
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 64.100.13.2
```

b. Répétez l'Étape 2a afin de configurer la stratégie 103. Modifiez l'adressage IP, le cas échéant.

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

a. Créez le transform-set **VPN-SET** de manière à utiliser **esp-aes** 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 R1_R2_Set esp-aes esp-sha-hmac
R1(config)# crypto map R1_R2_Map 102 ipsec-isakmp
R1(config-crypto-map)# set peer 64.100.13.2
R1(config-crypto-map)# set transform-set R1_R2_Set
R1(config-crypto-map)# match address 102
R1(config-crypto-map)# exit
```

b. Répétez l'Étape 3a afin de configurer R1_R3_Set et R1_R3_Map. Modifiez l'adressage, le cas échéant.

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

Enfin, liez les cartes de chiffrement **R1_R2_Map** et **R1_R3_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 R1_R2_Map
R1(config-if)# crypto map R1_R3_Map
```

Étape 5 : Configuration des paramètres IPsec sur R2 et R3

Répétez les Étapes 1 à 5 sur **R2** et **R3**. Utilisez les mêmes listes de contrôle d'accès, paramètres et noms de cartes que pour **R1**. Remarquez que chaque routeur ne nécessite qu'une seule connexion chiffrée à **R1**. Il n'y a aucune connexion chiffrée entre **R2** et **R3**.

Partie 4 : Configuration de tunnels GRE sur IPsec

Étape 1 : Configurez les interfaces de tunnel de R1.

a. Accédez au mode de configuration du tunnel 0 de **R1**.

```
R1(config)# interface tunnel 0
```

b. Configurez l'adresse IP comme indiqué dans la table d'adressage.

```
R1(config-if)# ip address 192.168.0.1 255.255.255.252
```

c. Définissez la source et la destination des points d'extrémité du tunnel 0.

```
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 64.100.13.2
```

d. Configurez le tunnel 0 de manière à transmettre le trafic IP sur GRE.

```
R1(config-if)# tunnel mode gre ip
```

e. L'interface du tunnel 0 devrait déjà être active. Si ce n'est pas le cas, traitez cette interface comme n'importe quelle autre.

f. Répétez les Étapes 1a - f pour créer l'interface Tunnel 1 sur R3. Modifiez l'adressage, le cas échéant.

Étape 2 : Configurez l'interface du tunnel 0 de R2 et R3.

a. Répétez les Étapes 1a - e avec **R2**. Veillez à modifier l'adressage IP, selon le cas.

b. Répétez les Étapes 1a - e avec **R3**. Veillez à modifier l'adressage IP, selon le cas.

Étape 3 : Configurez une route pour le trafic IP privé.

a. Définissez une route à partir de **R1** vers les réseaux 172.16.0.0 et 172.16.4.0 en utilisant l'adresse de tronçon suivant de l'interface de tunnel.

b. Définissez une route à partir de **R2** et **R3** vers le réseau 10.0.0.0 en utilisant l'adresse de tronçon suivant de l'interface de tunnel.

Partie 5 : Vérification de la connectivité

Étape 1 : Envoyez une requête ping à Server1 à partir de L2 et de PC3.

a. Essayez d'envoyer une requête ping à l'adresse IP de **Server1** à partir de **L2** et **PC3**. La requête ping devrait aboutir.

b. Essayez d'envoyer une requête ping à l'adresse IP de **L2** à partir de **PC3**. La requête ping devrait échouer, car il n'y a pas de tunnel entre les deux réseaux.