

Packet Tracer : configuration de GRE sur IPsec (facultatif) (version de l'instructeur)

Remarque à l'intention de l'instructeur : le texte en rouge ou surligné en gris apparaît uniquement dans la version de l'instructeur.

Topologie

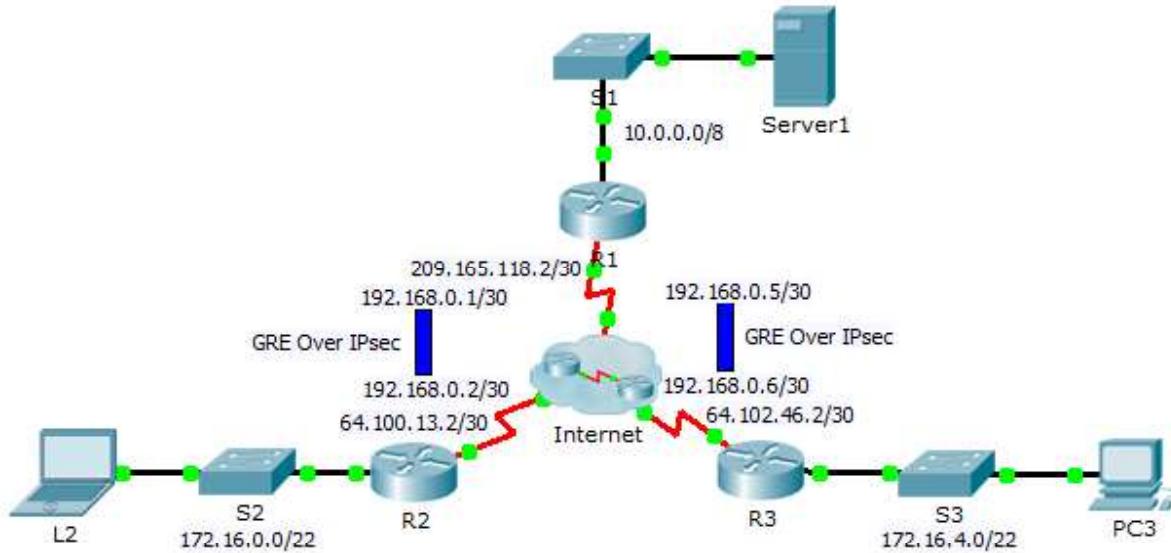


Table d'adressage

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.

- À partir de **R1**, envoyez une requête ping à l'adresse IP de S0/0/0 sur **R2**.
- 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 ? Les requêtes ping ont échoué, car il n'existe aucune route vers la destination.

Packet Tracer : configuration de GRE sur IPsec (facultatif)

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 ? Les requêtes ping ont échoué, car il n'existe aucune route vers la destination.

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.

- 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

- 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
```

- 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

- Répétez les Étapes 1a à 1c avec **R2** et **R3**.

Partie 3 : Configuration des paramètres IPsec

Étape 1 : Identifiez le trafic intéressant sur R1.

- 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
```

- 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.

```
R1(config)# access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0  
0.0.3.255
```

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

- 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
```

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

```
R1(config)# crypto isakmp policy 103  
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 64.102.46.2
```

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

- 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
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

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

```
R1(config)# crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
R1(config)# crypto map R1_R3_Map 103 ipsec-isakmp
R1(config-crypto-map)# set peer 64.102.46.2
R1(config-crypto-map)# set transform-set R1_R3_Set
R1(config-crypto-map)# match address 103
R1(config-crypto-map)# exit
```

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**.

```
R2(config)# access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0
0.255.255.255
R2(config)# crypto isakmp policy 102
R2(config-isakmp)# encryption aes
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 5
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco address 209.165.118.2
R2(config)# crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
R2(config)# crypto map R1_R2_Map 102 ipsec-isakmp
R2(config-crypto-map)# set peer 209.165.118.2
R2(config-crypto-map)# set transform-set R1_R2_Set
R2(config-crypto-map)# match address 102
R2(config-crypto-map)# exit
R2(config-if)# interface s0/0/0
R2(config-if)# crypto map R1_R2_Map

R3(config)# access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0
0.255.255.255
R3(config)# crypto isakmp policy 103
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 209.165.118.2
R3(config)# crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
R3(config)# crypto map R1_R3_Map 103 ipsec-isakmp
R3(config-crypto-map)# set peer 209.165.118.2
R3(config-crypto-map)# set transform-set R1_R3_Set
R3(config-crypto-map)# match address 103
R3(config-crypto-map)# exit
R3(config)# interface s0/0/0
R3(config-if)# crypto map R1_R3_Map
```

Partie 4 : Configuration de tunnels GRE sur IPsec

Étape 1 : Configurez les interfaces de tunnel de R1.

- Accédez au mode de configuration du tunnel 0 de R1.

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

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

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

- 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
```

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

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

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

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

```
R1(config)# interface tunnel 1
```

```
R1(config-if)# ip address 192.168.0.5 255.255.255.252
```

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

```
R1(config-if)# tunnel destination 64.102.46.2
```

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

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

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

```
R2(config)# interface tunnel 0
```

```
R2(config-if)# ip address 192.168.0.2 255.255.255.252
```

```
R2(config-if)# tunnel source s0/0/0
```

```
R2(config-if)# tunnel destination 209.165.118.2
```

```
R2(config-if)# tunnel mode gre ip
```

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

```
R3(config)# interface tunnel 0
```

```
R3(config-if)# ip address 192.168.0.6 255.255.255.252
```

```
R3(config-if)# tunnel source s0/0/0
```

```
R3(config-if)# tunnel destination 209.165.118.2
```

```
R3(config-if)# tunnel mode gre ip
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

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

- 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.

```
R1(config)# ip route 172.16.0.0 255.255.252.0 192.168.0.2  
R1(config)# ip route 172.16.4.0 255.255.252.0 192.168.0.6
```

- 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.

```
R2(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.1  
R3(config)# ip route 10.0.0.0 255.0.0.0 192.168.0.5
```

Partie 5 : Vérification de la connectivité

Étape 1 : 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** et **PC3**. La requête ping devrait aboutir.
- 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.

Scripts de configuration

Routeur R1

```
license boot module c2900 technology-package securityk9  
access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255  
crypto isakmp policy 102  
    encryption aes  
    authentication pre-share  
    group 5  
exit  
crypto isakmp key cisco address 64.100.13.2  
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac  
crypto map R1_R2_Map 102 ipsec-isakmp  
    set peer 64.100.13.2  
    set transform-set R1_R2_Set  
    match address 102  
interface S0/0/0  
    crypto map R1_R2_Map  
access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255  
crypto isakmp policy 103  
    encryption aes  
    authentication pre-share  
    group 5  
exit  
crypto isakmp key cisco address 64.102.46.2  
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac  
crypto map R1_R3_Map 103 ipsec-isakmp  
    set peer 64.102.46.2  
    set transform-set R1_R3_Set
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
match address 103
interface S0/0/0
crypto map R1_R3_Map
interface Tunnel 0
  ip address 192.168.0.1 255.255.255.252
  tunnel source serial 0/0/0
  tunnel destination 64.100.13.2
  tunnel mode gre ip
ip route 172.16.0.0 255.255.252.0 192.168.0.2
interface Tunnel 1
  ip address 192.168.0.5 255.255.255.252
  tunnel source serial 0/0/0
  tunnel destination 64.102.46.2
  tunnel mode gre ip
ip route 172.16.4.0 255.255.252.0 192.168.0.6
```

Routeur R2

```
license boot module c2900 technology-package securityk9
access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255
crypto isakmp policy 102
  encryption aes
  authentication pre-share
  group 5
exit
crypto isakmp key cisco address 209.165.118.2
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
  set peer 209.165.118.2
  set transform-set R1_R2_Set
  match address 102
interface Serial0/0/0
  crypto map R1_R2_Map
interface Tunnel0
  ip address 192.168.0.2 255.255.255.252
  tunnel source Serial0/0/0
  tunnel destination 209.165.118.2
  tunnel mode gre ip
ip route 10.0.0.0 255.0.0.0 192.168.0.1
```

Routeur R3

```
license boot module c2900 technology-package securityk9
access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255
crypto isakmp policy 103
  encryption aes
  authentication pre-share
  group 5
exit
crypto isakmp key cisco address 209.165.118.2
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
crypto map R1_R3_Map 103 ipsec-isakmp
  set peer 209.165.118.2
  set transform-set R1_R3_Set
  match address 103
interface S0/0/0
  crypto map R1_R3_Map
interface Tunnel 0
  ip address 192.168.0.6 255.255.255.252
  tunnel source serial 0/0/0
  tunnel destination 209.165.118.2
  tunnel mode gre ip
ip route 10.0.0.0 255.0.0.0 192.168.0.5
```

Configurations des périphériques

Routeur R1

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
crypto isakmp policy 102
  encr aes
  authentication pre-share
  group 5
crypto isakmp policy 103
  encr aes
  authentication pre-share
  group 5
crypto isakmp key cisco address 64.100.13.2
crypto isakmp key cisco address 64.102.46.2
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
  set peer 64.100.13.2
  set transform-set R1_R2_Set
  match address 102
crypto map R1_R3_Map 103 ipsec-isakmp
  set peer 64.102.46.2
  set transform-set R1_R3_Set
  match address 103
license udi pid CISCO2911/K9 sn FTX15241LLM
license boot module c2900 technology-package securityk9
spanning-tree mode pvst
interface Tunnel0
  ip address 192.168.0.1 255.255.255.252
  tunnel source Serial0/0/0
  tunnel destination 64.100.13.2
  tunnel mode gre ip
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
interface Tunnel1
    ip address 192.168.0.5 255.255.255.252
    tunnel source Serial0/0/0
    tunnel destination 64.102.46.2
    tunnel mode gre ip
interface GigabitEthernet0/0
    ip address 10.0.0.1 255.0.0.0
    duplex auto
    speed auto
interface GigabitEthernet0/1
    no ip address
    duplex auto
    speed auto
    shutdown
interface GigabitEthernet0/2
    no ip address
    duplex auto
    speed auto
    shutdown
interface Serial0/0/0
    ip address 209.165.118.2 255.255.255.252
    crypto map R1_R3_Map
interface Serial0/0/1
    no ip address
    shutdown
interface Vlan1
    no ip address
    shutdown
    ip classless
    ip route 0.0.0.0 0.0.0.0 Serial0/0/0
    ip route 172.16.0.0 255.255.252.0 192.168.0.2
    ip route 172.16.4.0 255.255.252.0 192.168.0.6
    access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255
    access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255
line con 0
line aux 0
line vty 0 4
    login
end
```

Routeur R2

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
crypto isakmp policy 102
    encr aes
    authentication pre-share
    group 5
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
crypto isakmp key cisco address 209.165.118.2
crypto ipsec transform-set R1_R2_Set esp-aes esp-sha-hmac
crypto map R1_R2_Map 102 ipsec-isakmp
    set peer 209.165.118.2
    set transform-set R1_R2_Set
    match address 102
license udi pid CISCO2911/K9 sn FTX15249J0B
license boot module c2900 technology-package securityk9
spanning-tree mode pvst
interface Tunnel0
    ip address 192.168.0.2 255.255.255.252
    tunnel source Serial0/0/0
    tunnel destination 209.165.118.2
    tunnel mode gre ip
interface GigabitEthernet0/0
    ip address 172.16.0.1 255.255.252.0
    duplex auto
    speed auto
interface GigabitEthernet0/1
    no ip address
    duplex auto
    speed auto
    shutdown
interface GigabitEthernet0/2
    no ip address
    duplex auto
    speed auto
    shutdown
interface Serial0/0/0
    ip address 64.100.13.2 255.255.255.252
    crypto map R1_R2_Map
interface Serial0/0/1
    no ip address
    shutdown
interface Vlan1
    no ip address
    shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 10.0.0.0 255.0.0.0 192.168.0.1
access-list 102 permit ip 172.16.0.0 0.0.3.255 10.0.0.0 0.255.255.255
line con 0
line aux 0
line vty 0 4
    login
end
```

Routeur R3

```
no service timestamps log datetime msec
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
no service timestamps debug datetime msec
no service password-encryption
hostname R3
crypto isakmp policy 103
  encr aes
  authentication pre-share
  group 5
crypto isakmp key cisco address 209.165.118.2
crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
crypto map R1_R3_Map 103 ipsec-isakmp
  set peer 209.165.118.2
  set transform-set R1_R3_Set
  match address 103
license udi pid CISCO2911/K9 sn FTX1524446J
license boot module c2900 technology-package securityk9
spanning-tree mode pvst
interface Tunnel0
  ip address 192.168.0.6 255.255.255.252
  tunnel source Serial0/0/0
  tunnel destination 209.165.118.2
  tunnel mode gre ip
interface GigabitEthernet0/0
  ip address 172.16.4.1 255.255.255.252
  duplex auto
  speed auto
interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
interface GigabitEthernet0/2
  no ip address
  duplex auto
  speed auto
  shutdown
interface Serial0/0/0
  ip address 64.102.46.2 255.255.255.252
  crypto map R1_R3_Map
interface Serial0/0/1
  no ip address
  shutdown
interface Vlan1
  no ip address
  shutdown
  ip classless
  ip route 0.0.0.0 0.0.0.0 Serial0/0/0
  ip route 10.0.0.0 255.0.0.0 192.168.0.5
access-list 103 permit ip 172.16.4.0 0.0.3.255 10.0.0.0 0.255.255.255
line con 0
```

Packet Tracer : configuration de GRE sur IPsec (facultatif)

```
line aux 0
line vty 0 4
 login
end
```