Institut Universitaire des Sciences (IUS)

Faculté des Sciences et Technologies

(FST)

RAPPORT

SUR LE TRAVAIL DE LABORATOIRE № 6

Cours : Reseau 2

Soumis au Chargé de cours : **Ismael SAINT AMOUR**

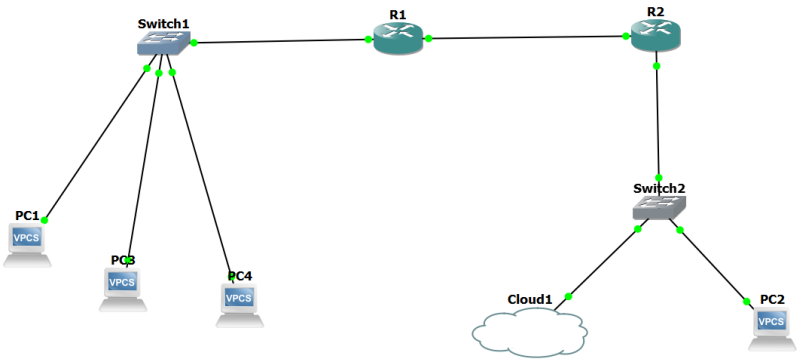
Niveau L3

Préparé par : **Robaldo BADIO**

Date : Le 10 / 06 / 2025

Exécution du TD

1. Reproduisez cette topologie en Configurant d'un VPN Site-à-Site



R1

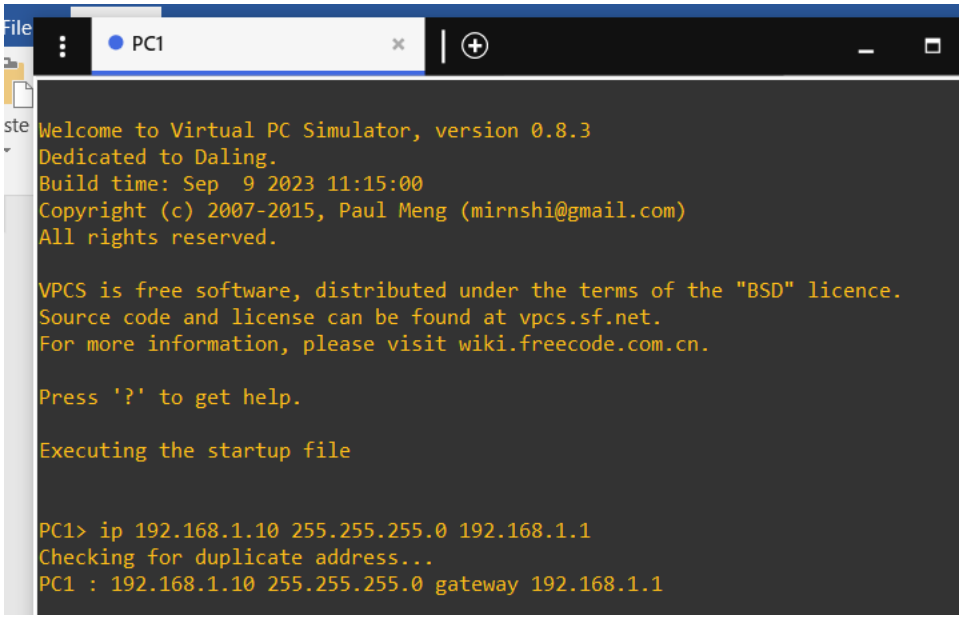
```
R1
*Mar  1 00:07:50.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R1(config-if)#exit
R1(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vpn123 address 10.0.0.2
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.0.0.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exitinterface fa0/1
                     ^
% Invalid input detected at '^' marker.

R1(config-crypto-map)#crypto map VPN-MAP
                      ^
% Invalid input detected at '^' marker.

R1(config-crypto-map)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.0.0.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface fa0/1
R1(config-if)#crypto map VPN-MAP
R1(config-if)#
*Mar  1 00:09:26.443: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#$ 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#end
R1#
*Mar  1 00:09:55.707: %SYS-5-CONFIG_I: Configured from console by console
R1#write memory
Building configuration...
[OK]
R1#
```

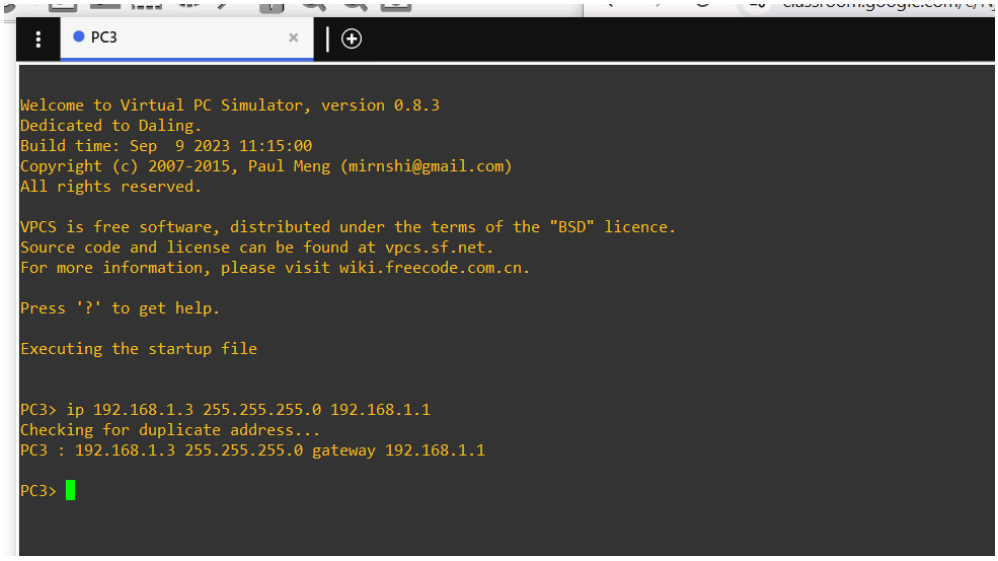
R2

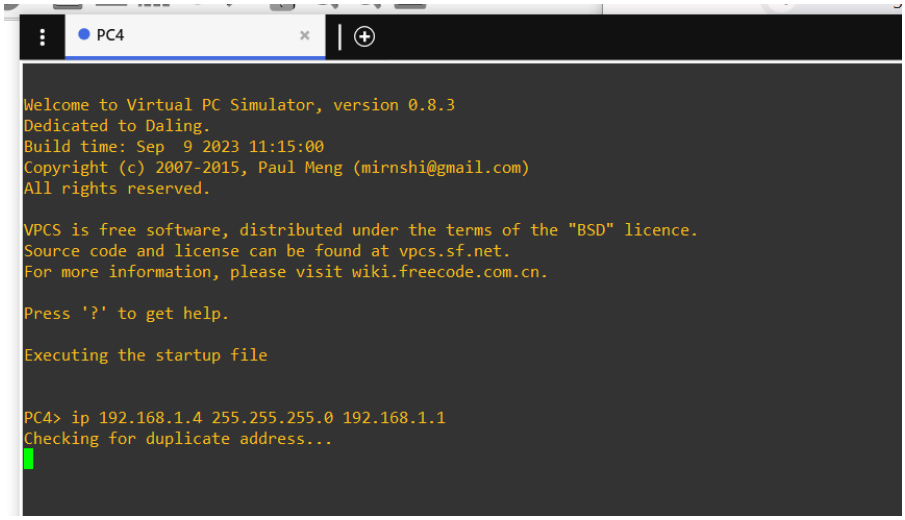
```
to administratively down
*Mar  1 00:00:10.835: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T14
, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 17-Aug-10 12:08 by prod_rel_team
*Mar  1 00:00:10.855: %SNMP-5-COLDSTART: SNMP agent on host R2 is undergoing a c
old start
*Mar  1 00:00:10.931: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Mar  1 00:00:10.931: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Mar  1 00:00:11.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Mar  1 00:00:11.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
R2#en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fa0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:12:44.383: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:12:45.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R2(config)#interface fa0/1
R2(config-if)#ip address 10.0.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:12:51.383: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:12:52.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R2(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes
R2(config-isakmp)#hash sha
R2(config-isakmp)#authentication pre-share
```

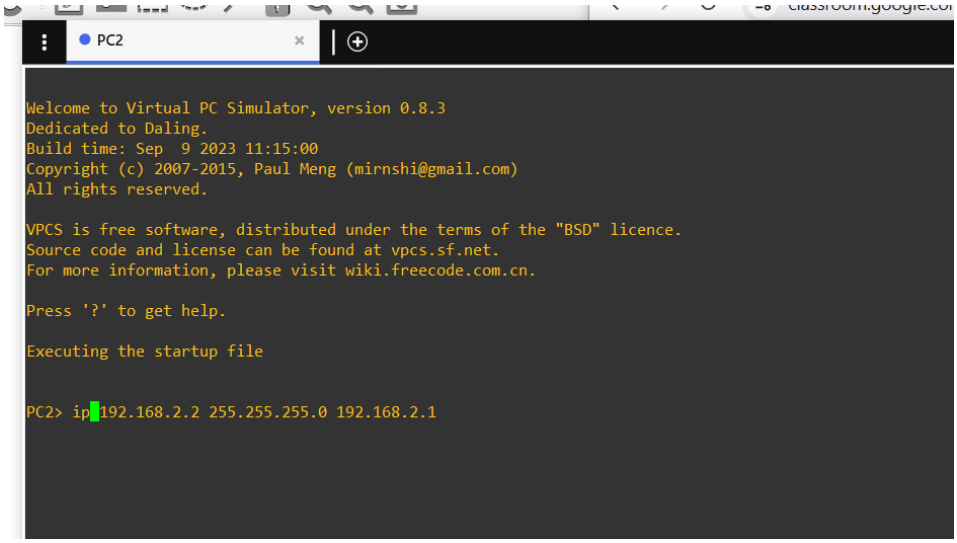
```
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#crypto isakmp key vpn123 address 10.0.0.1
R2(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)#set peer 10.0.0.1
R2(config-crypto-map)#set transform-set VPN-SET
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
R2(config)#interface fa0/1
R2(config-if)#crypto map VPN-MAP
R2(config-if)#
*Mar  1 00:13:47.227: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R2(config-if)#$ 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#end
R2#write memory
Building configuration...
[OK]
R2#
*Mar  1 00:14:00.915: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

Adressage IP des Pcs









Vérifier les sessions VPN

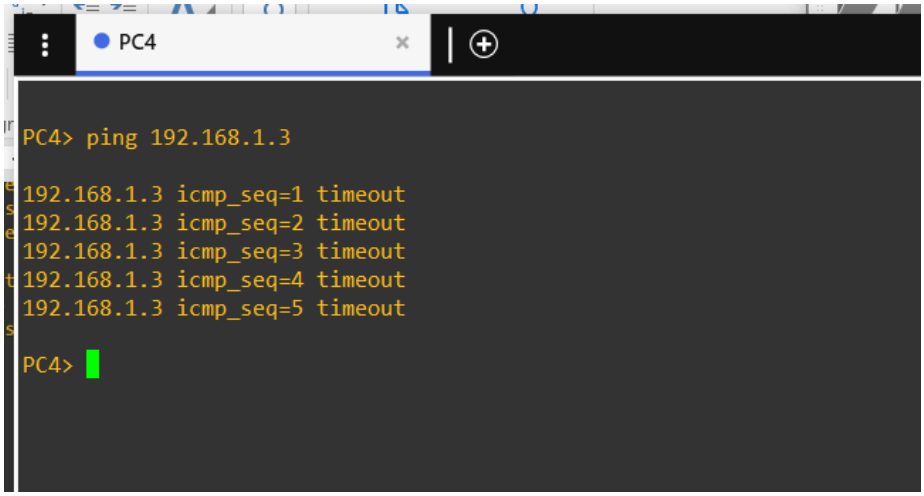
Sur R1

```
R1(config-if)#$ 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#end
R1#
*Mar  1 00:09:55.707: %SYS-5-CONFIG_I: Configured from console by console
R1#write memory
Building configuration...
[OK]
R1#
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA

R1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: VPN-MAP, local addr 10.0.0.1

   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): (192.168.2.0/255.255.255.0/0/0)
   current_peer 10.0.0.2 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.: 10.0.0.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

R1#ebug crypto isakmp
    ^
% Invalid input detected at '^' marker.

R1#debug crypto ipsec
Crypto IPSEC debugging is on
R1#
```

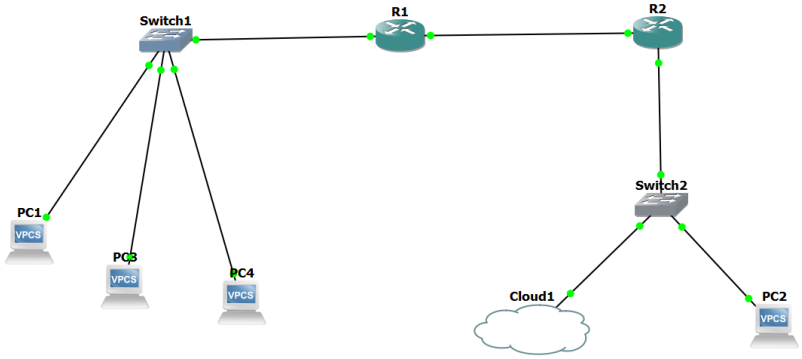
Sur R2

```
R2
R2(config-if)#$ 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#end
R2#write memory
Building configuration...
[OK]
R2#
*Mar  1 00:14:00.915: %SYS-5-CONFIG_I: Configured from console by console
R2#
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA

R2#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: VPN-MAP, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.0.0.1 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.: 10.0.0.2, remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

R2#ebug crypto isakmp
    ^
% Invalid input detected at '^' marker.

R2#debug crypto ipsec
Crypto IPSEC debugging is on
R2#
```

Tester la communication : Depuis PC4 **:**



2. **Reproduisez cette topologie en Configurant VPN GRE over IPSec avec Routage Dynamique (OSPF)**



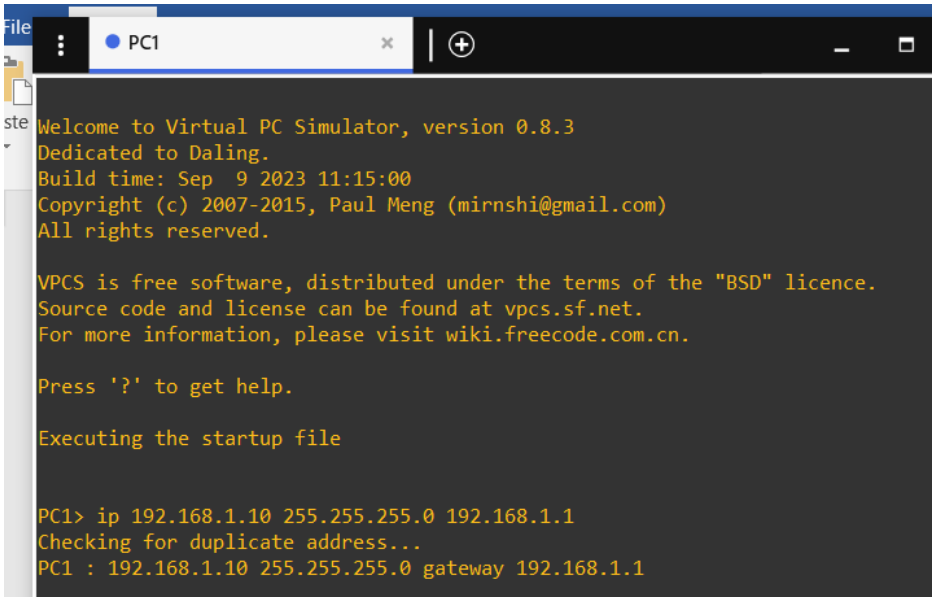
R1

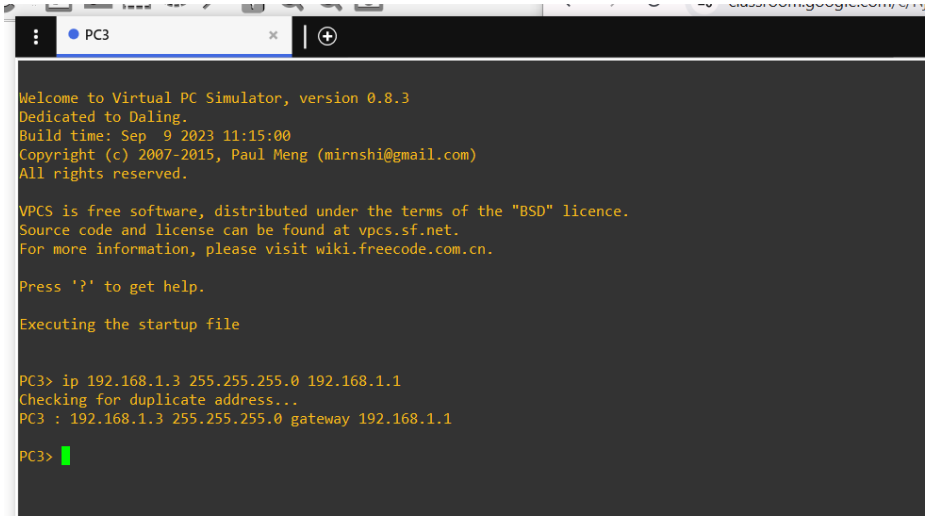
```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fa0/1
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Tunnel0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#tunnel source fa0/1
R1(config-if)#tunnel destination 10.0.0.2
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:18:19.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, c
hanged state to up
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.100.0 0.0.0.255 area 0
R1(config-router)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#crypto isakmp key GRE123 address 10.0.0.2
A pre-shared key for address mask 10.0.0.2 255.255.255.255 already exists!

R1(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R1(cfg-crypto-trans)#access-list 100 permit gre host 10.0.0.1 host 10.0.0.2
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.0.0.2
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface fa0/1
R1(config-if)#crypto map VPN-MAP
R1(config-if)#end
R1#write memory
Building configuration...
[OK]
```

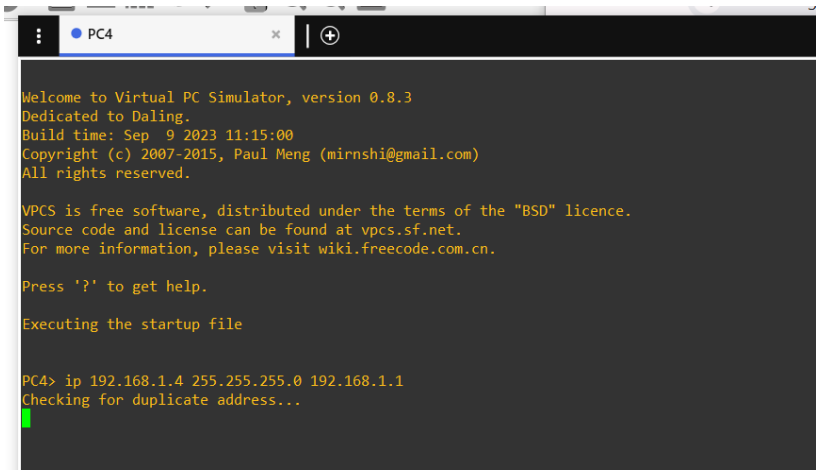
R2

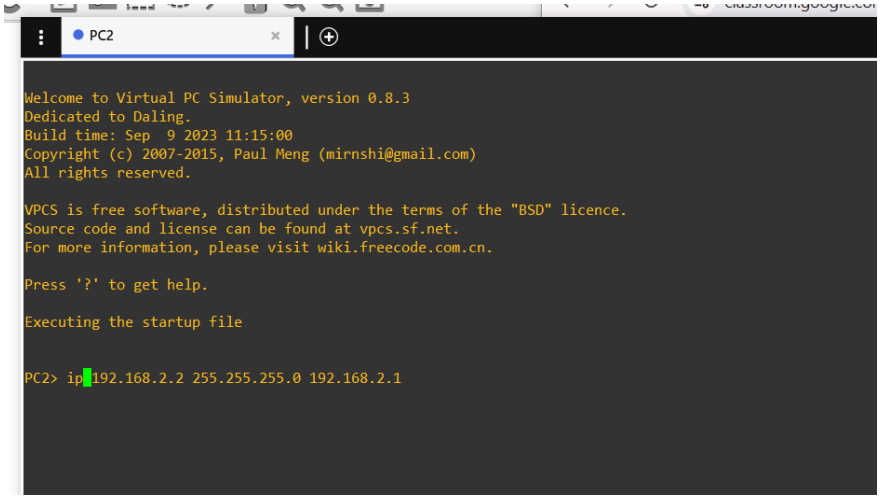
```
R2(config)#interface fa0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa0/1
R2(config-if)#ip address 10.0.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Tunnel0
R2(config-if)#ip address 192.168.100.2 255.255.255.0
R2(config-if)#tunnel source fa0/1
R2(config-if)#tunnel destination 10.0.0.1
R2(config-if)#tunnel mode gre ip
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:21:46.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, chan
ged state to up
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.100.0 0.0.0.255 area 0
R2(config-router)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes
R2(config-isakmp)#hash sha
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#exit
R2(config)#crypto isakmp key GRE123 address 10.0.0.1
A pre-shared key for address mask 10.0.0.1 255.255.255.255 already exists!

R2(config)#crypto ipsec transform-set TSET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#access-list 100 permit gre host 10.0.0.2 host 10.0.0.1
R2(config)#crypto map VPN-MAP 10 ipsec-isakmp
R2(config-crypto-map)#set peer 10.0.0.1
R2(config-crypto-map)#set transform-set TSET
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
R2(config)#interface fa0/1
R2(config-if)#crypto map VPN-MAP
R2(config-if)#end
R2#write memory
Building configuration...
[OK]
R2#
*Mar  1 00:22:52.247: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

Adressage IP des Pcs









Vérifier les sessions VPN :

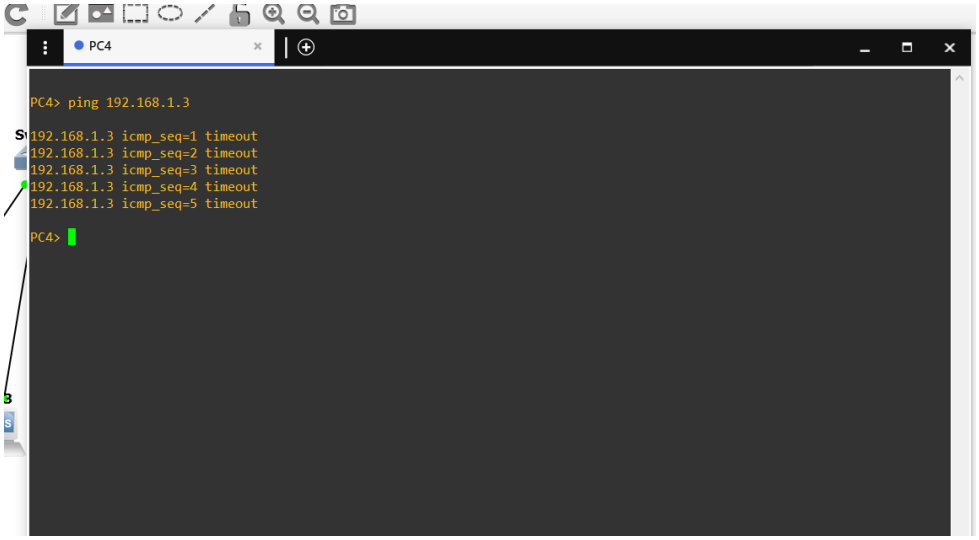
R1

```
% Invalid input detected at '^' marker.

R1#debug crypto ipsec
Crypto IPSEC debugging is on
R1#show interface Tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.100.1/24
  MTU 1514 bytes, BW 9 Kbit/sec, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (FastEthernet0/1), destination 10.0.0.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 64
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
R1#
R1#
R1#
```

R2

```
R2#debug crypto ipsec
Crypto IPSEC debugging is on
R2#show interface Tunnel0
*Mar  1 00:26:24.367: IPSEC(key_engine): request timer fired: count = 1,
  (identity) local= 10.0.0.2, remote= 10.0.0.1,
    local_proxy= 10.0.0.2/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/47/0 (type=1)
*Mar  1 00:26:24.367: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.0.0.2, remote= 10.0.0.1,
    local_proxy= 10.0.0.2/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
R2#show interface Tunnel0
*Mar  1 00:26:54.367: IPSEC(key_engine): request timer fired: count = 2,
  (identity) local= 10.0.0.2, remote= 10.0.0.1,
    local_proxy= 10.0.0.2/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/47/0 (type=1)
*Mar  1 00:26:54.371: IPSEC(key_engine): got a queue event with 1 KMI message(s)
R2#show interface Tunnel0
*Mar  1 00:26:59.767: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.0.0.2, remote= 10.0.0.1,
    local_proxy= 10.0.0.2/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.0.0.1/255.255.255.255/47/0 (type=1),
    protocol= ESP, transform= esp-aes esp-sha-hmac  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
R2#show interface Tunnel0
```

Tester la communication



En conclusion, La configuration du VPN Site-à-Site et du VPN GRE over IPSec avec routage dynamique (OSPF) sur GNS3 me fait bien comprendre que la communication sécurisée et évolutive entre sites distants. L'intégration d'OSPF optimise la gestion du routage, garantissant une connectivité fluide et adaptative. Ces configurations renforcent la sécurité et la performance du réseau en simulant un environnement proche des déploiements réels.