INSTITUT UNIVERSITAIRE DES SCIENCES

Faculté des Sciences et Technologies (FST)

Td6 – réseau 2

Soumis au charge du Professeur : Ismaël St-Amour

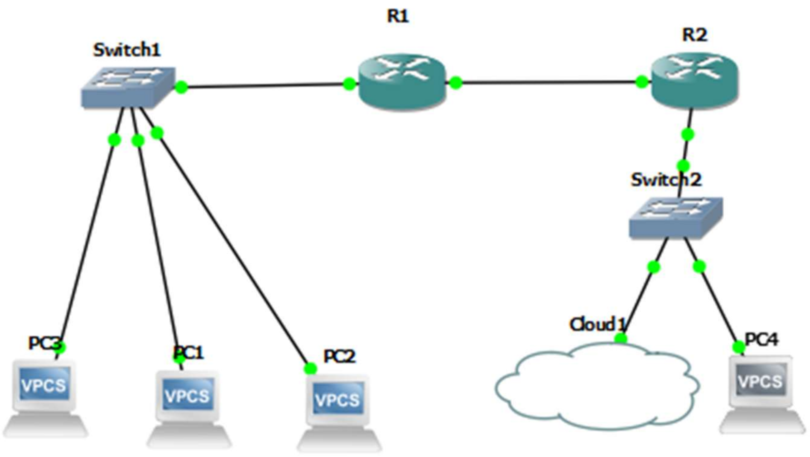
Nom : PIERRE

Prénom : Yann Lelay

Niveau : L3- Sciences Informatiques

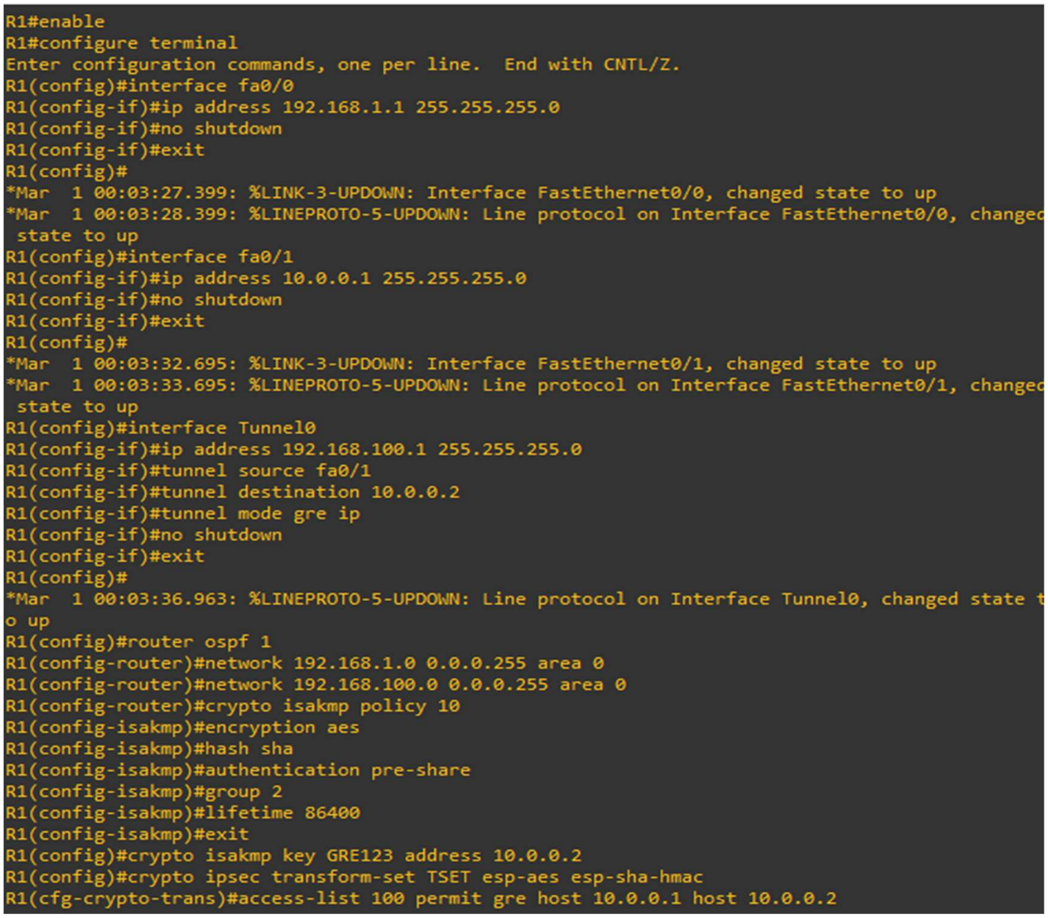
Date : 09 juin 2025

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



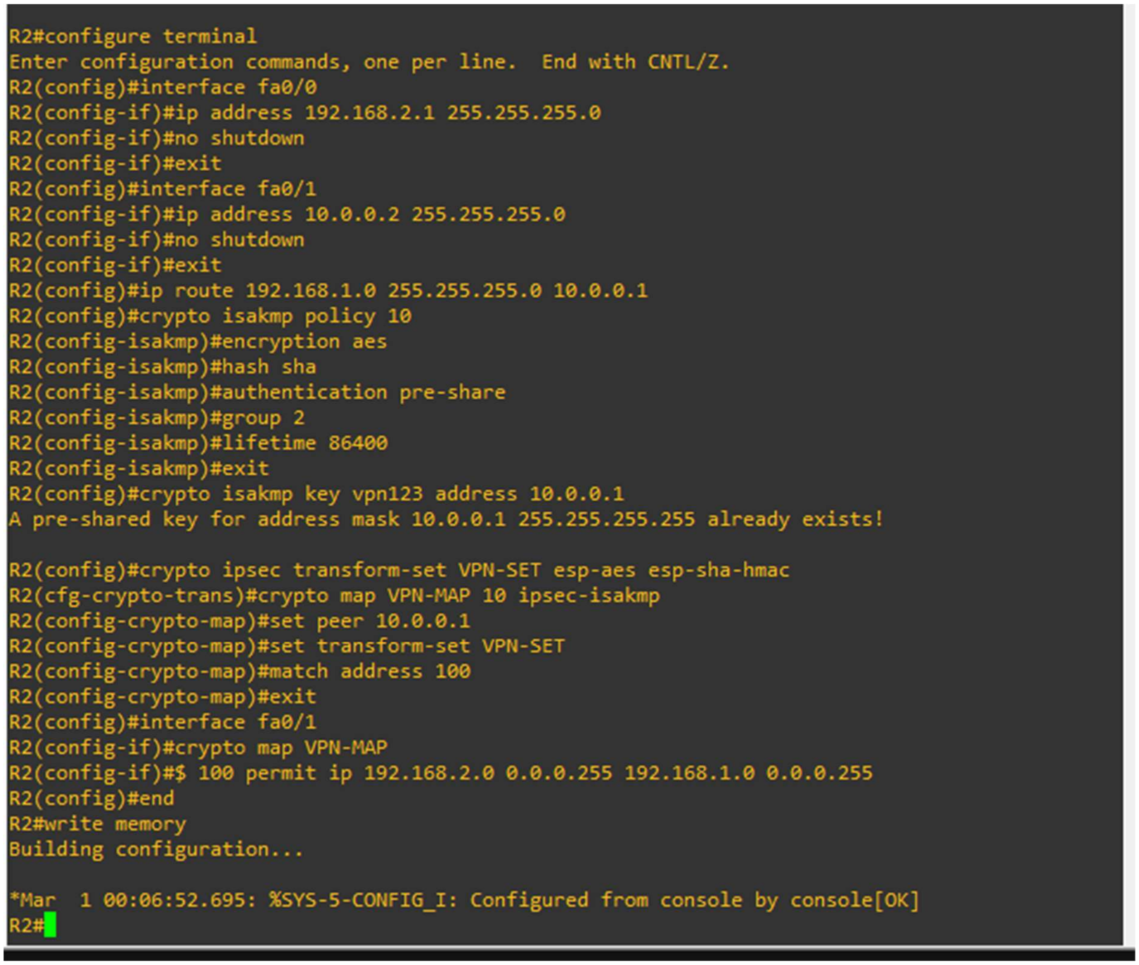
Configuration du VPN sur les Routeurs

Sur R1



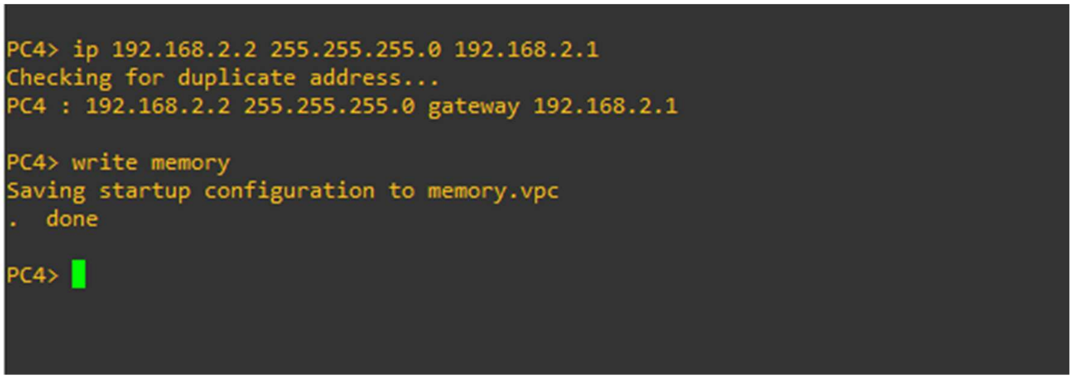
```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:03:27.399: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:03:28.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
 state to up
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)#
*Mar  1 00:03:32.695: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:03:33.695: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
 state to up
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 00:03:36.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state t
o 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
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
```

Sur R2

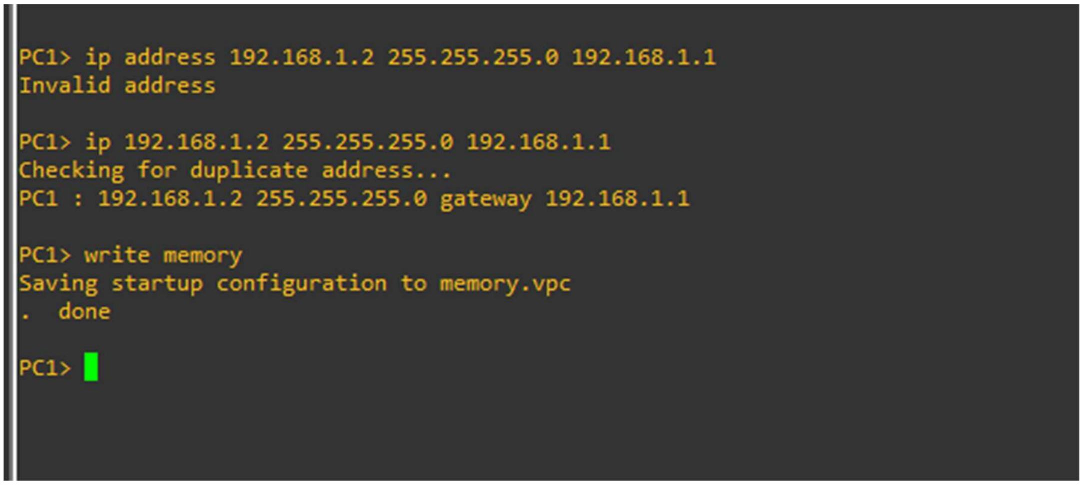


```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fa0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa0/1
R2(config-if)#ip address 10.0.0.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#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)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#crypto isakmp key vpn123 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 VPN-SET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#crypto map VPN-MAP 10 ipsec-isakmp
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)#$ 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...

*Mar  1 00:06:52.695: %SYS-5-CONFIG_I: Configured from console by console[OK]
R2#
```

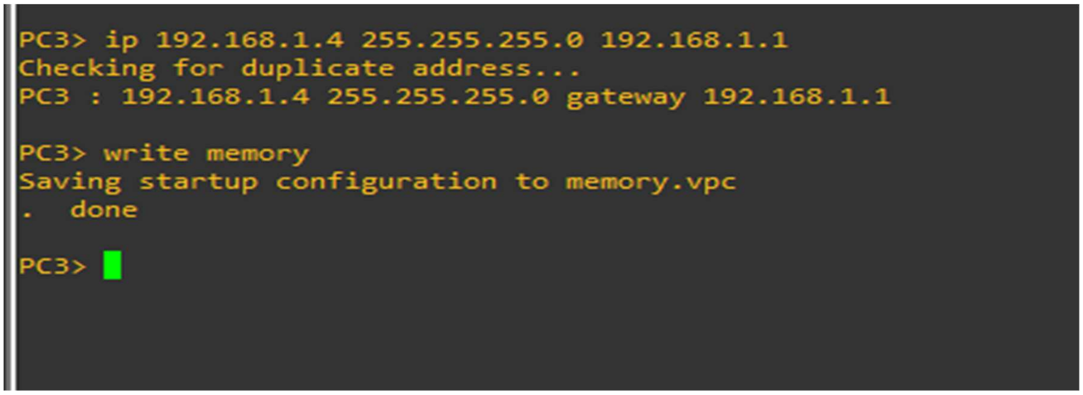
Adresse IP des Pcs



```
PC4> ip 192.168.2.2 255.255.255.0 192.168.2.1
Checking for duplicate address...
PC4 : 192.168.2.2 255.255.255.0 gateway 192.168.2.1

PC4> write memory
Saving startup configuration to memory.vpc
.  done

PC4>
```



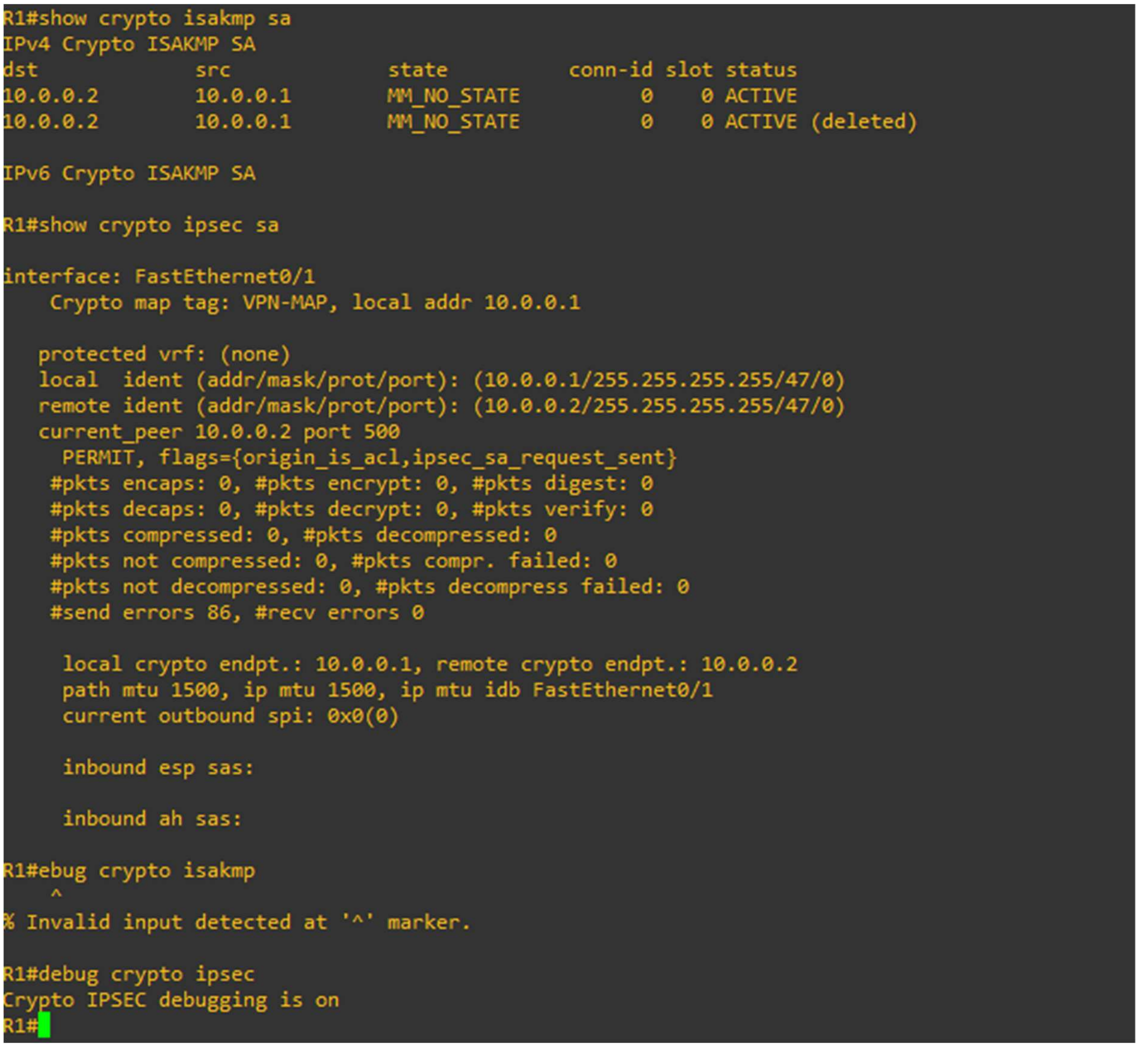
```
PC1> ip address 192.168.1.2 255.255.255.0 192.168.1.1
Invalid address

PC1> ip 192.168.1.2 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC1> write memory
Saving startup configuration to memory.vpc
.  done

PC1>
```



```
PC3> ip 192.168.1.4 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC3 : 192.168.1.4 255.255.255.0 gateway 192.168.1.1

PC3> write memory
Saving startup configuration to memory.vpc
.  done

PC3>
```

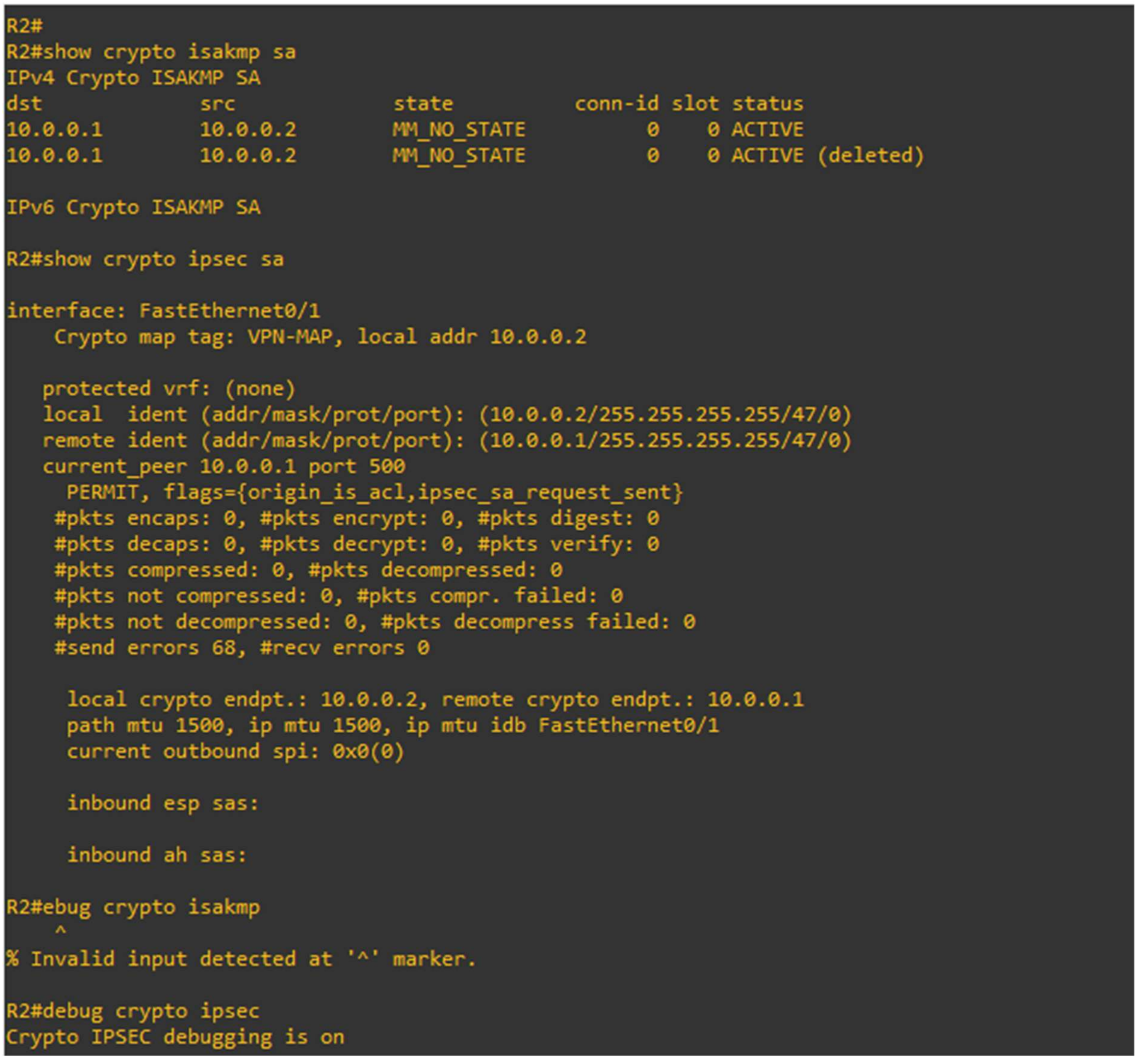
Vérifications

- **Vérifier les sessions VPN :**

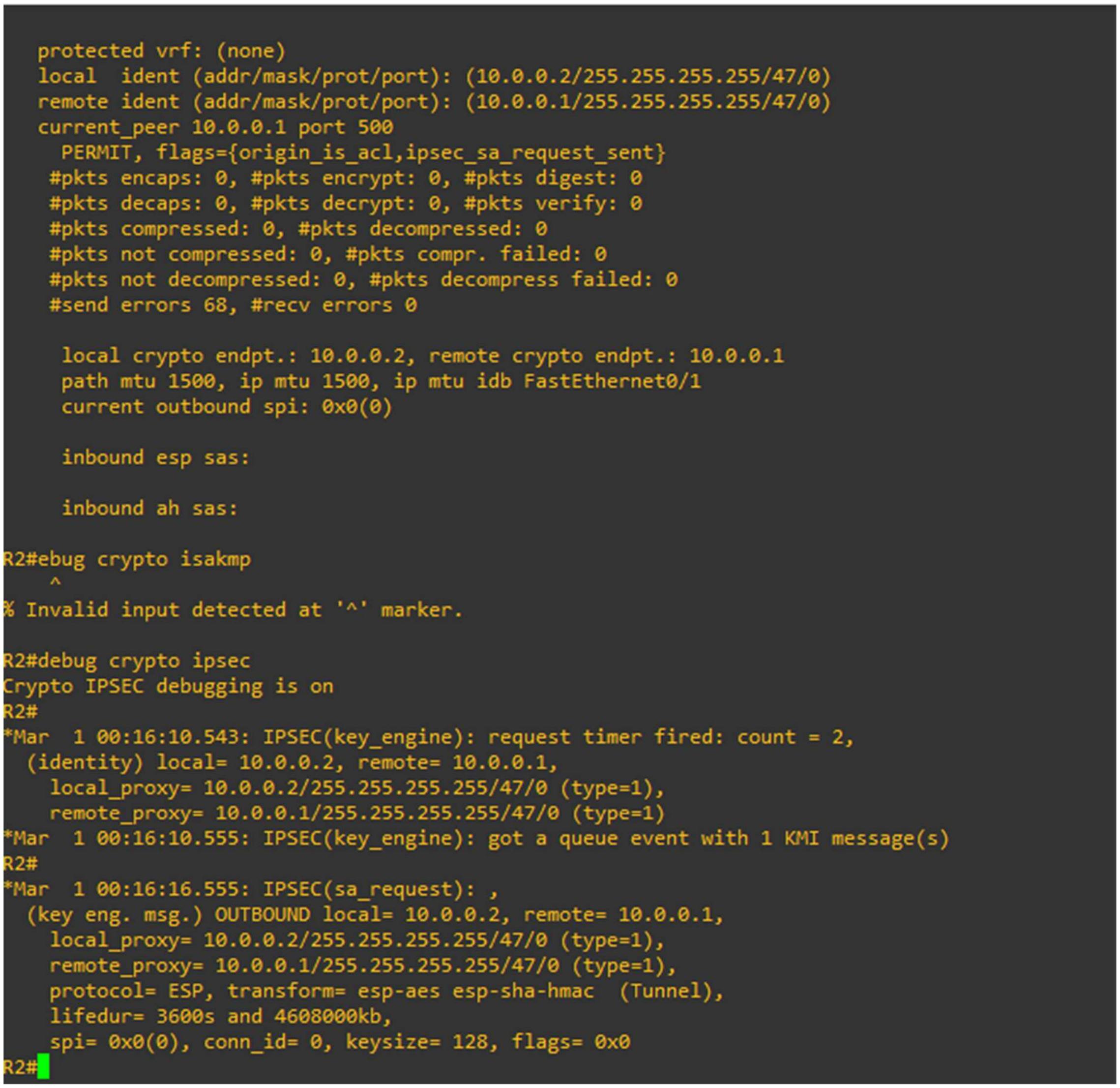


```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.2        10.0.0.1        MM_NO_STATE          0    0 ACTIVE
10.0.0.2        10.0.0.1        MM_NO_STATE          0    0 ACTIVE (deleted)

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): (10.0.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.0.0.2/255.255.255.255/47/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #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 86, #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#
```

R2

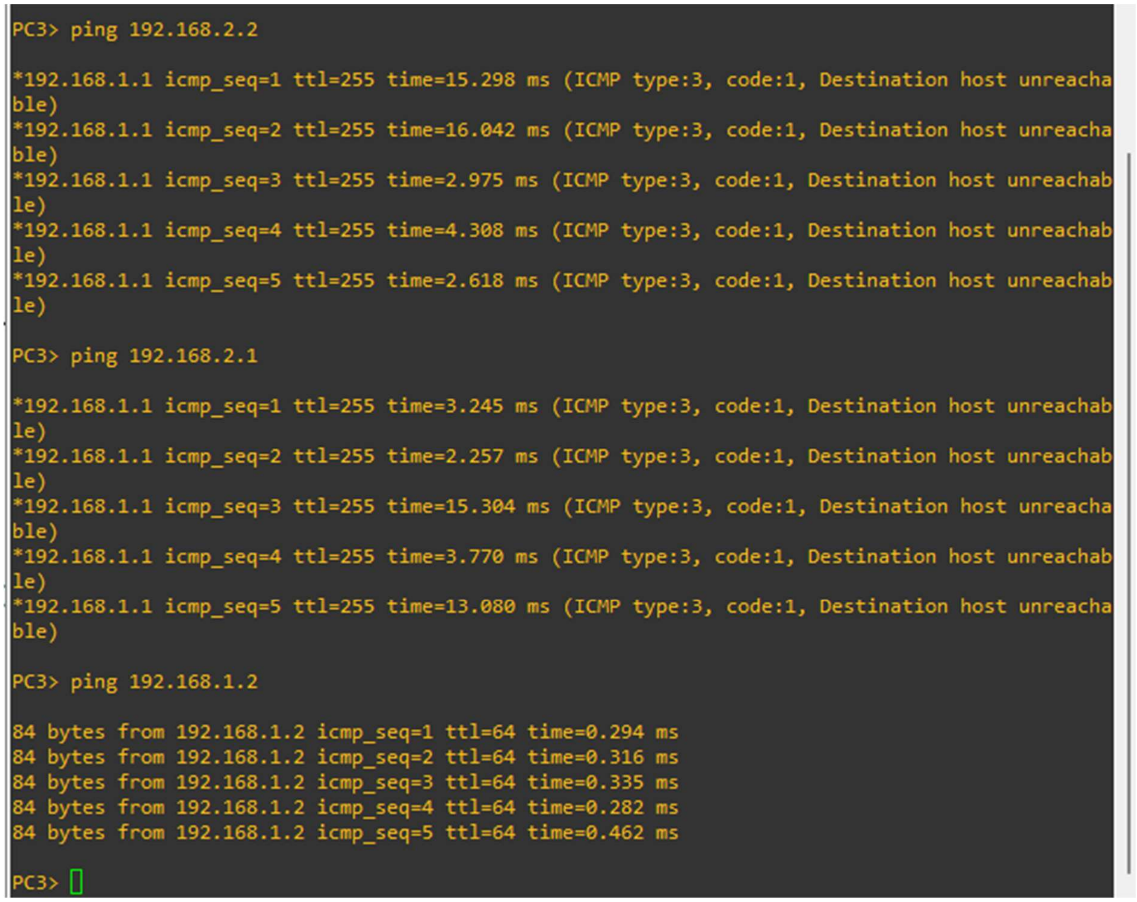


```
R2#
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.1        10.0.0.2        MM_NO_STATE          0    0 ACTIVE
10.0.0.1        10.0.0.2        MM_NO_STATE          0    0 ACTIVE (deleted)

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): (10.0.0.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/47/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #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 68, #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
```



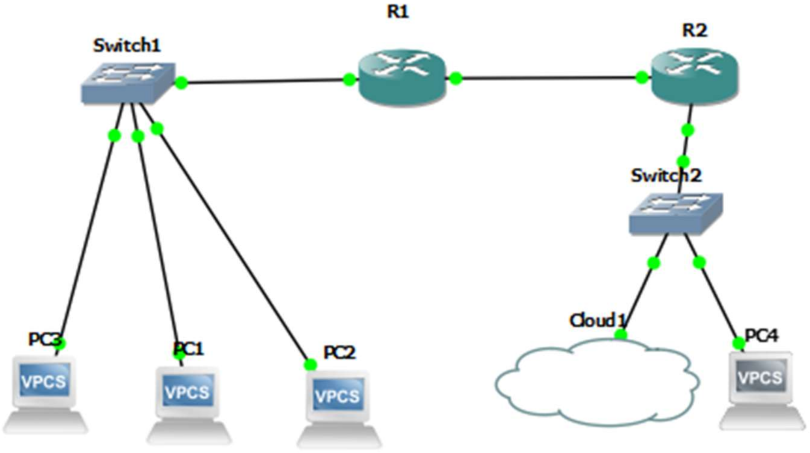
```
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/47/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #pkts encaps: 0, #pkts encrypt: 0, #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 68, #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#
*Mar  1 00:16:10.543: 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 00:16:10.555: IPSEC(key_engine): got a queue event with 1 KMI message(s)
R2#
*Mar  1 00:16:16.555: 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#
```

- Tester la communication : Depuis PC3 :



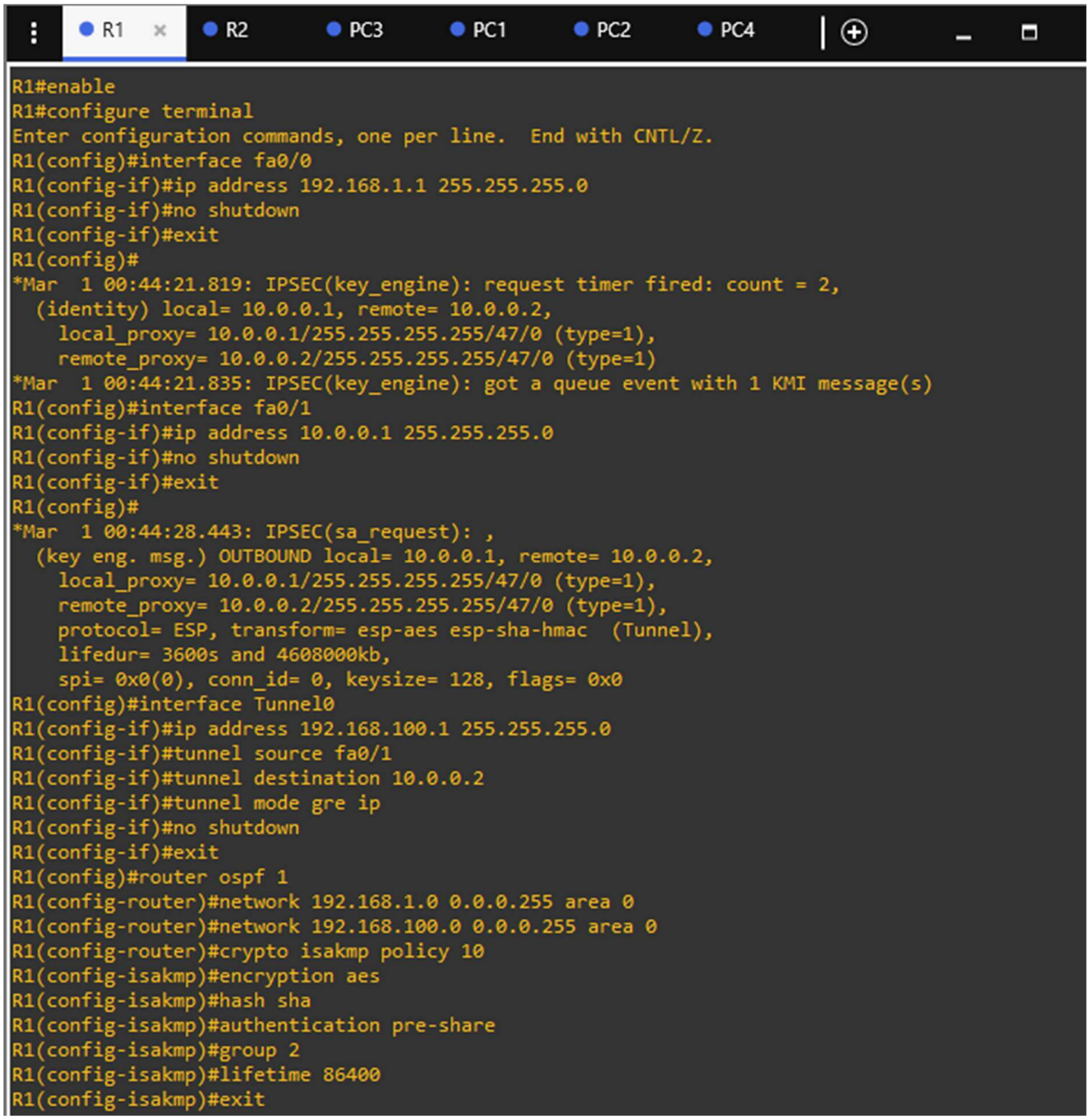
```
PC3> ping 192.168.2.2

*192.168.1.1 icmp_seq=1 ttl=255 time=15.298 ms (ICMP type:3, code:1, Destination host unreacha
ble)
*192.168.1.1 icmp_seq=2 ttl=255 time=16.042 ms (ICMP type:3, code:1, Destination host unreacha
ble)
*192.168.1.1 icmp_seq=3 ttl=255 time=2.975 ms (ICMP type:3, code:1, Destination host unreachab
le)
*192.168.1.1 icmp_seq=4 ttl=255 time=4.308 ms (ICMP type:3, code:1, Destination host unreachab
le)
*192.168.1.1 icmp_seq=5 ttl=255 time=2.618 ms (ICMP type:3, code:1, Destination host unreachab
le)

PC3> ping 192.168.2.1

*192.168.1.1 icmp_seq=1 ttl=255 time=3.245 ms (ICMP type:3, code:1, Destination host unreachab
le)
*192.168.1.1 icmp_seq=2 ttl=255 time=2.257 ms (ICMP type:3, code:1, Destination host unreachab
le)
*192.168.1.1 icmp_seq=3 ttl=255 time=15.304 ms (ICMP type:3, code:1, Destination host unreacha
ble)
*192.168.1.1 icmp_seq=4 ttl=255 time=3.770 ms (ICMP type:3, code:1, Destination host unreachab
le)
*192.168.1.1 icmp_seq=5 ttl=255 time=13.080 ms (ICMP type:3, code:1, Destination host unreacha
ble)

PC3> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.294 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.316 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.335 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.282 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=0.462 ms

PC3> 
```

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



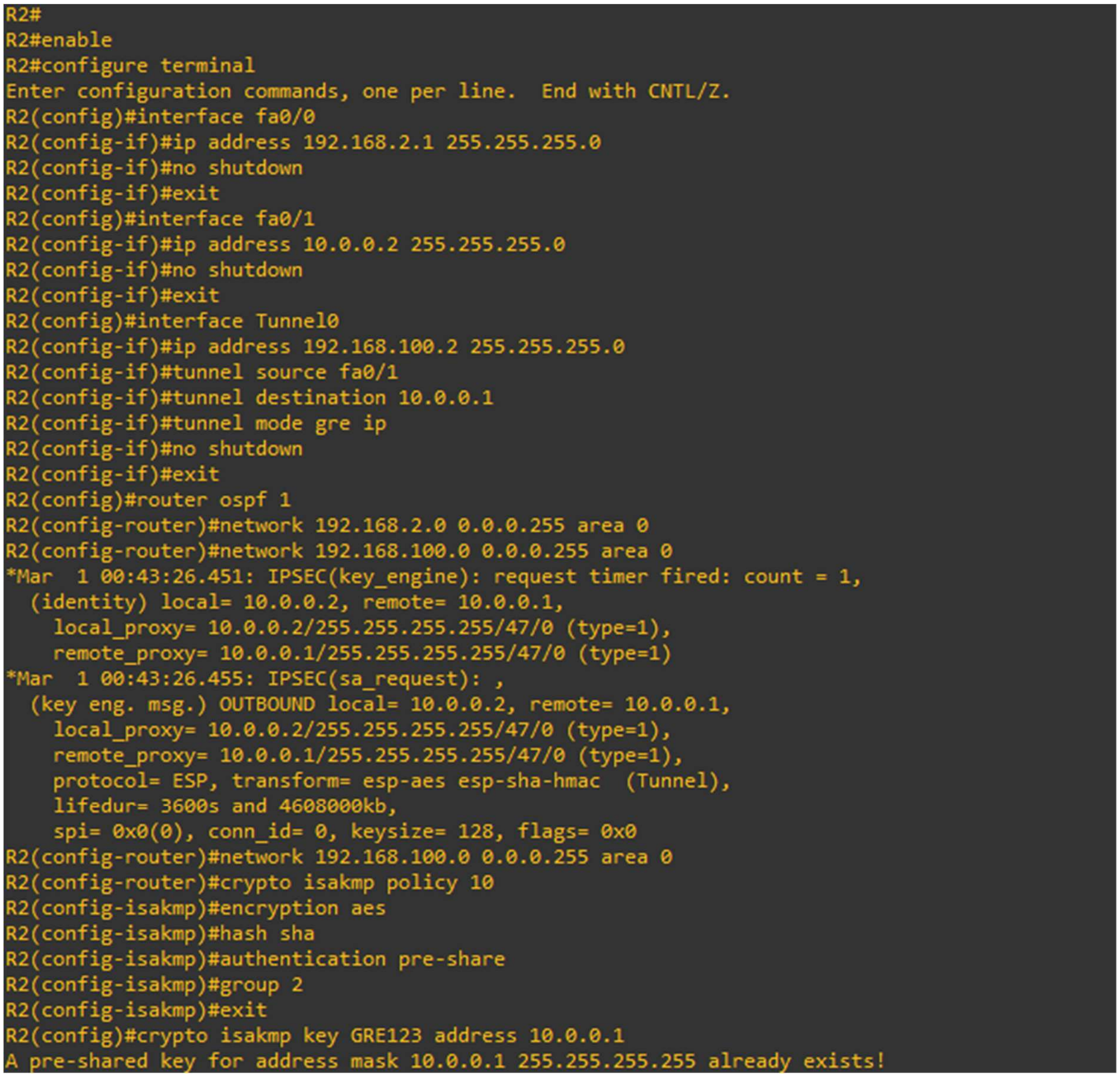
Configuration des Routeurs

R1 :



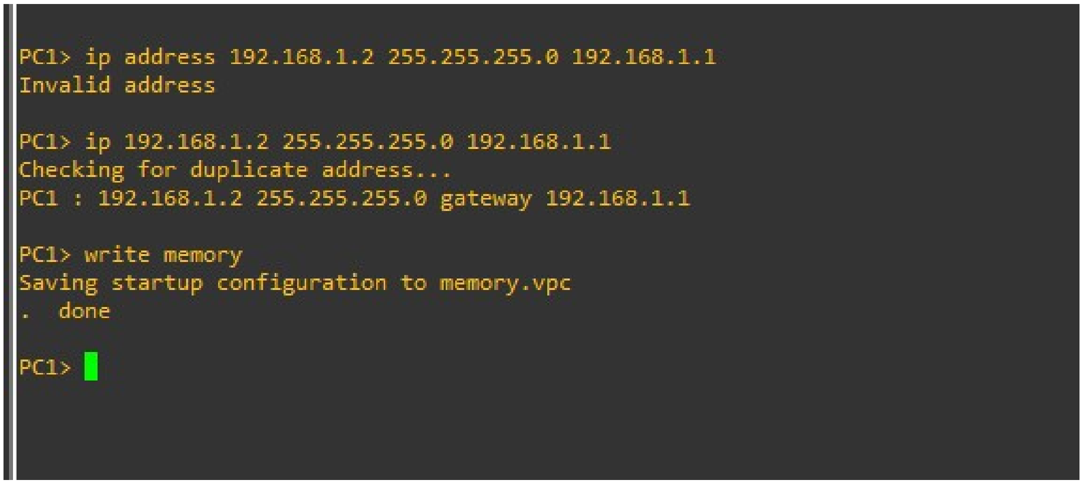
```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:44:21.819: IPSEC(key_engine): request timer fired: count = 2,
  (identity) local= 10.0.0.1, remote= 10.0.0.2,
    local_proxy= 10.0.0.1/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.0.0.2/255.255.255.255/47/0 (type=1)
*Mar  1 00:44:21.835: IPSEC(key_engine): got a queue event with 1 KMI message(s)
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)#
*Mar  1 00:44:28.443: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.0.0.1, remote= 10.0.0.2,
    local_proxy= 10.0.0.1/255.255.255.255/47/0 (type=1),
    remote_proxy= 10.0.0.2/255.255.255.255/47/0 (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
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)#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
```

R2

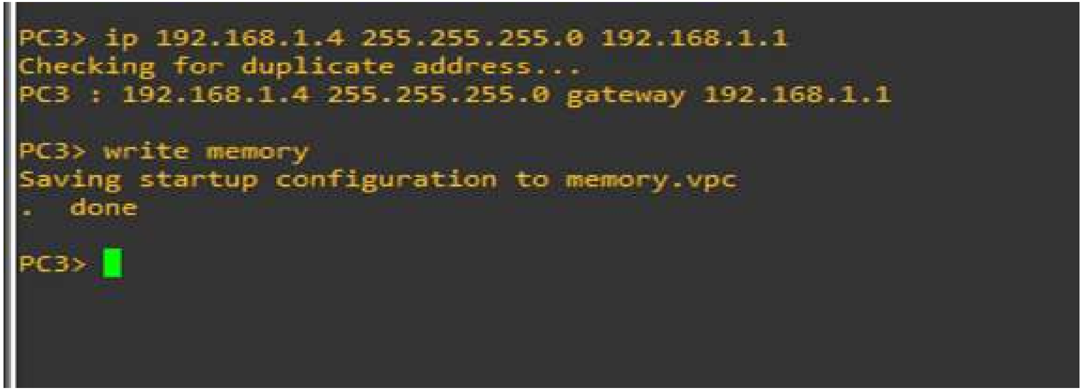


```
R2#
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface fa0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface fa0/1
R2(config-if)#ip address 10.0.0.2 255.255.255.0
R2(config-if)#no 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)#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
*Mar  1 00:43:26.451: 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 00:43:26.455: 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(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!
```

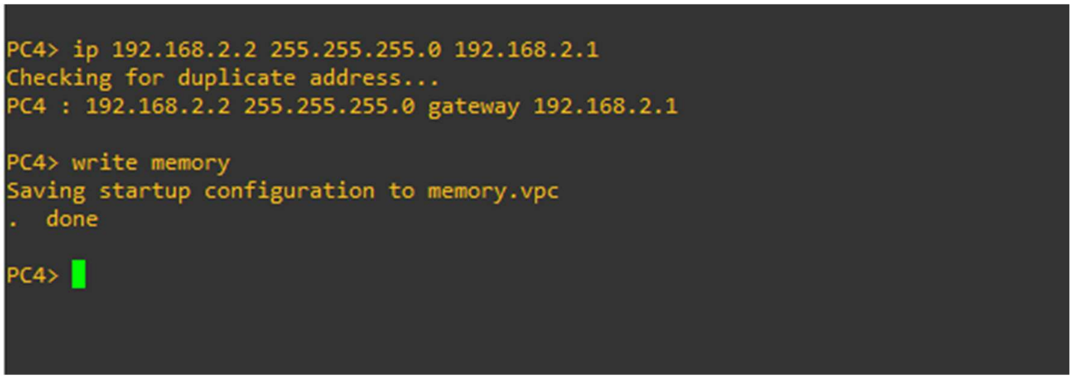
Adressage IP des Pcs



```
PC1> ip address 192.168.1.2 255.255.255.0 192.168.1.1
Invalid address

PC1> ip 192.168.1.2 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC1> write memory
Saving startup configuration to memory.vpc
.  done

PC1>
```

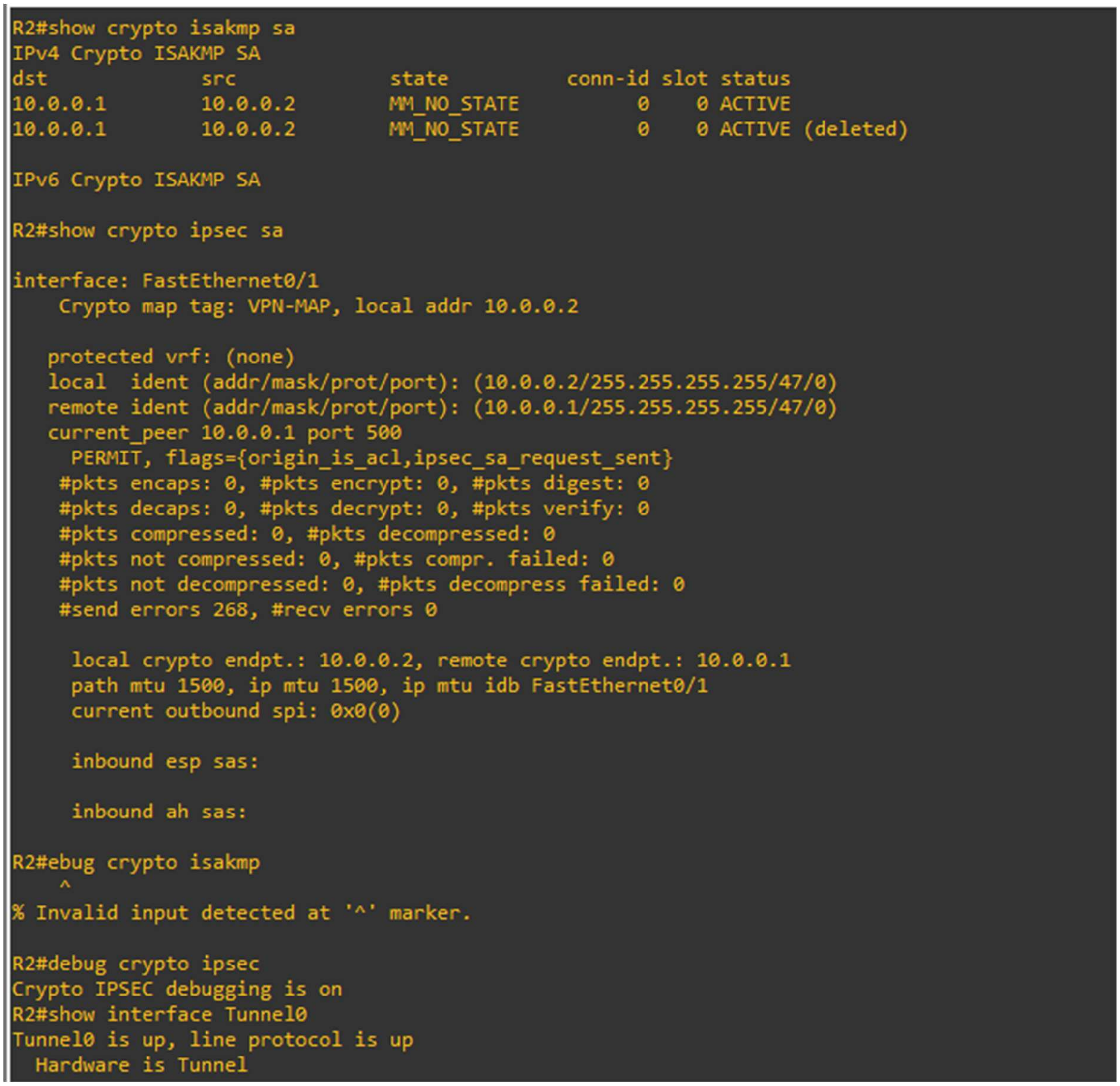


```
PC3> ip 192.168.1.4 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC3 : 192.168.1.4 255.255.255.0 gateway 192.168.1.1

PC3> write memory
Saving startup configuration to memory.vpc
.  done

PC3>
```



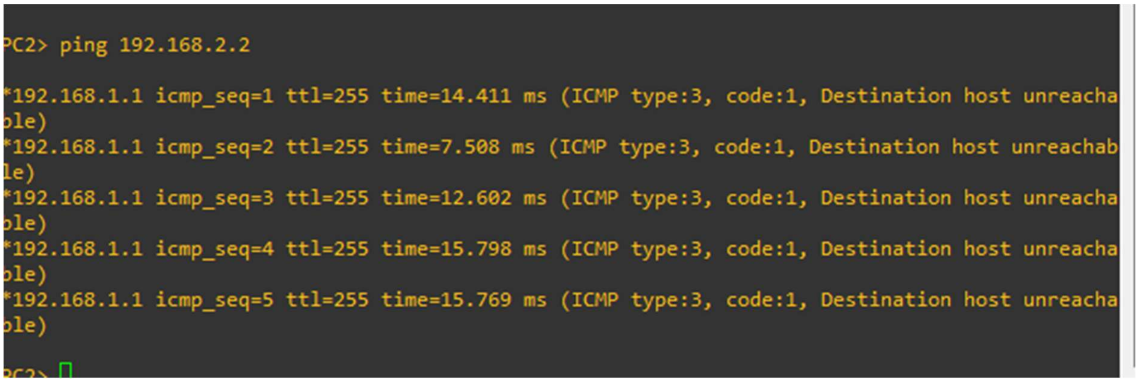
```
PC4> ip 192.168.2.2 255.255.255.0 192.168.2.1
Checking for duplicate address...
PC4 : 192.168.2.2 255.255.255.0 gateway 192.168.2.1

PC4> write memory
Saving startup configuration to memory.vpc
.  done

PC4>
```

Verifier des sessions VPN :



```
R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.0.0.1        10.0.0.2        MM_NO_STATE          0    0 ACTIVE
10.0.0.1        10.0.0.2        MM_NO_STATE          0    0 ACTIVE (deleted)

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): (10.0.0.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/47/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,ipsec_sa_request_sent}
    #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 268, #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#show interface Tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
```

Tezte de communication depuis PC2 :



```
PC2> ping 192.168.2.2

*192.168.1.1 icmp_seq=1 ttl=255 time=14.411 ms (ICMP type:3, code:1, Destination host unreacha
ble)
*192.168.1.1 icmp_seq=2 ttl=255 time=7.508 ms (ICMP type:3, code:1, Destination host unreachab
le)
*192.168.1.1 icmp_seq=3 ttl=255 time=12.602 ms (ICMP type:3, code:1, Destination host unreacha
ble)
*192.168.1.1 icmp_seq=4 ttl=255 time=15.798 ms (ICMP type:3, code:1, Destination host unreacha
ble)
*192.168.1.1 icmp_seq=5 ttl=255 time=15.769 ms (ICMP type:3, code:1, Destination host unreacha
ble)

PC2>
```

Conclusion :

Grace à ce Td j’arrive par configurer VPN site à site et VPN GRE over IPSec avec Routage Dynamique tout en approfondissant mes compétences en OSPF.