Institut Universitaire des Sciences (IUS)

Faculté des Sciences et Technologies

(FST)

RAPPORT

SUR LE TRAVAIL DE LABORATOIRE № 8

Cours : Cisco Packet Tracer (Reseau 1)

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

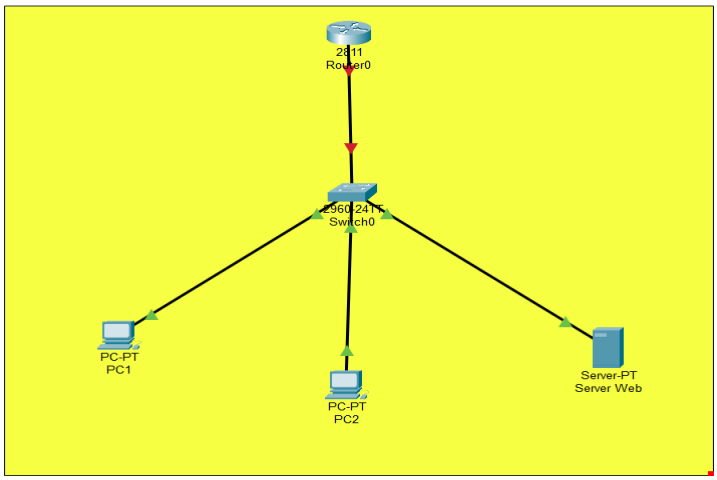
Niveau L3

Préparé par : **Robaldo BADIO**

Date : Le 26 / 02 / 2025

Exécution du TD

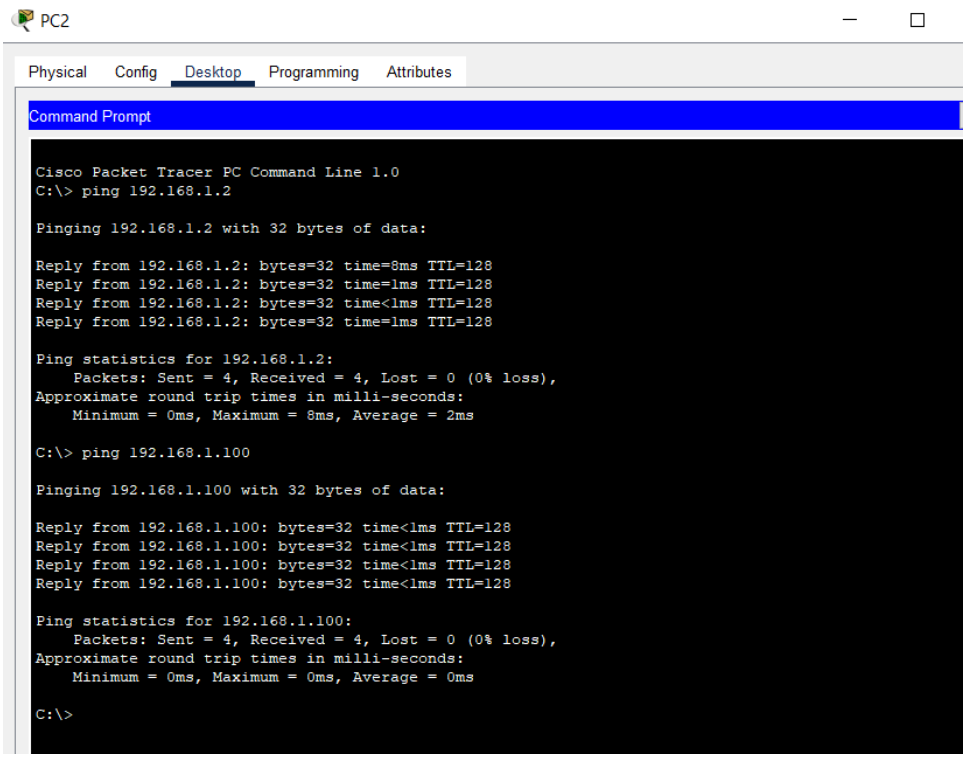
1. Configurez un pare-feu et un VPN site-à-site.




```
Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#exit
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config)#
```

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

MonCommutateur(config-if)#vlan 10
MonCommutateur(config-vlan)#name Utilisateurs
MonCommutateur(config-vlan)#
MonCommutateur(config-vlan)## Configuration d'un VLAN pour les voix
                            ^
% Invalid input detected at '^' marker.

MonCommutateur(config-vlan)#vlan 20
MonCommutateur(config-vlan)#name Voix
MonCommutateur(config-vlan)#
MonCommutateur(config-vlan)## Configuration des interfaces pour les VLANs
                            ^
% Invalid input detected at '^' marker.

MonCommutateur(config-vlan)#interface range FastEthernet0/1 - 24
MonCommutateur(config-if-range)#switchport mode access
MonCommutateur(config-if-range)#switchport access vlan 10
MonCommutateur(config-if-range)#
MonCommutateur(config-if-range)#interface range GigabitEthernet0/1 - 2
MonCommutateur(config-if-range)#switchport mode trunk
MonCommutateur(config-if-range)#switchport trunk allowed vlan 10,20
MonCommutateur(config-if-range)#
MonCommutateur(config-if-range)## Configuration des mots de passe de scurit
                               ^
% Invalid input detected at '^' marker.

MonCommutateur(config-if-range)#line console 0
MonCommutateur(config-line)#password cisco
MonCommutateur(config-line)#login
MonCommutateur(config-line)#line vty 0 4
MonCommutateur(config-line)#password cisco
MonCommutateur(config-line)#login
MonCommutateur(config-line)#
MonCommutateur(config-line)## Enregistrement de la configuration
                            ^
% Invalid input detected at '^' marker.

MonCommutateur(config-line)#end
MonCommutateur#write memory
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
MonCommutateur#
```

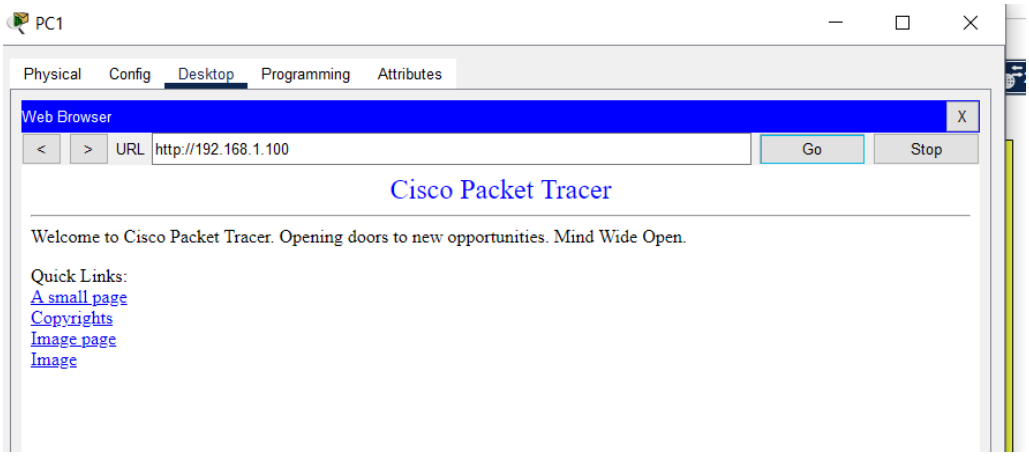
```
Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```




```
User Access Verification

Password:
Password:

MonCommutateur> enable
MonCommutateur#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MonCommutateur(config)#access-list 100 deny tcp host 192.168.1.3 host 192.168.1.100 eq 80
MonCommutateur(config)#access-list 100 permit ip any any
MonCommutateur(config)#
```

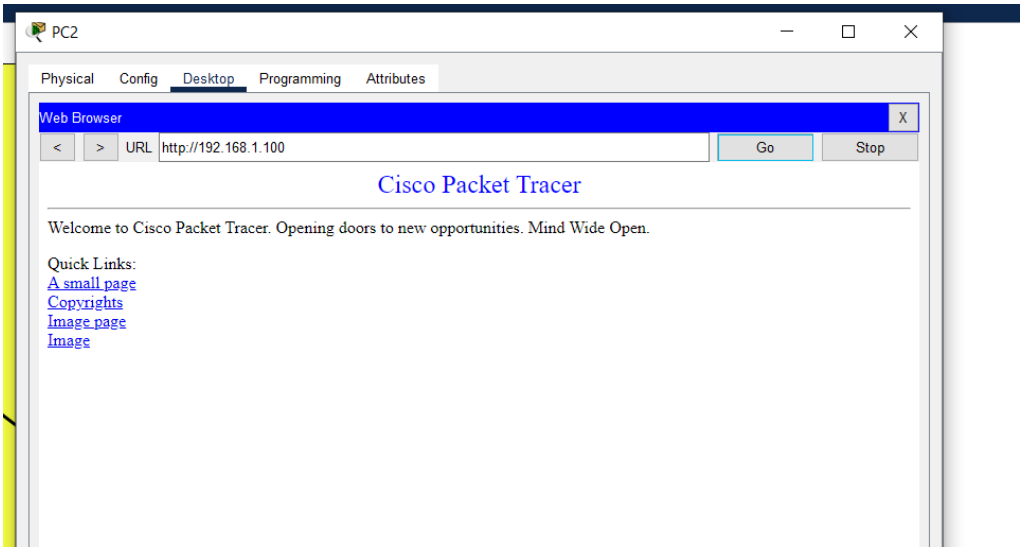
Copy Paste

```
R1>enbale
Translating "enbale"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip access-group 100 in
R1(config-if)#exit
R1(config)#
```

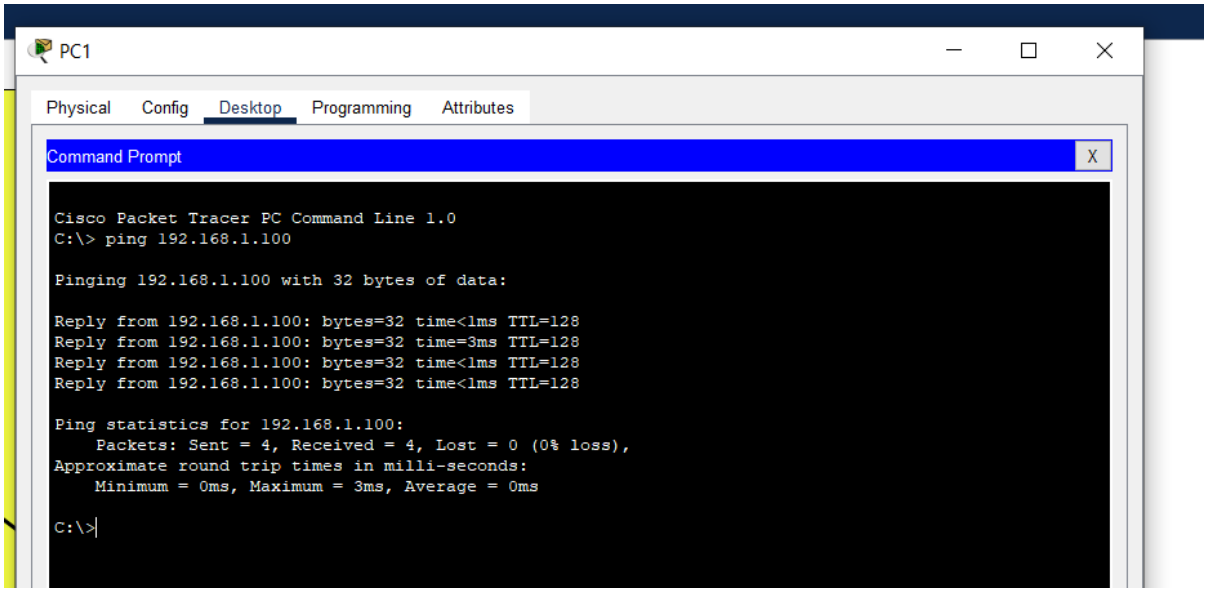


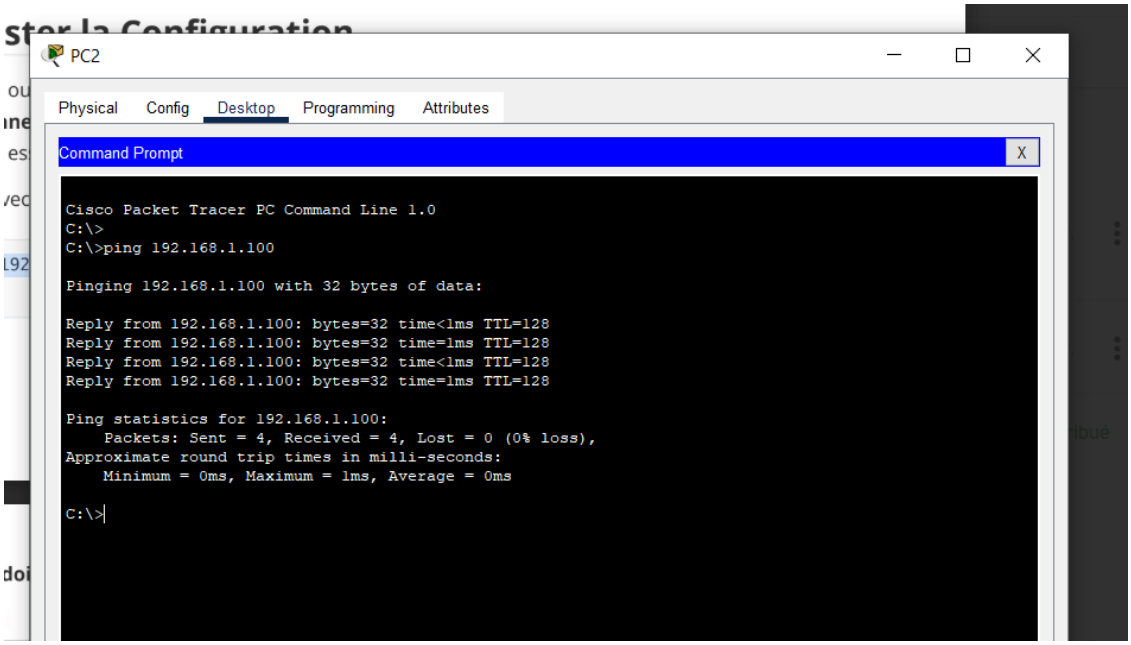
Pour Bloqué l'accès à l'internet pour le PC 2, j'ai fait la commande qu'on a demandé mais, ça ne passe pas.

Je fais des recherches pour savoir comment pour bloquer l'accès mais ça n'a pas pus passer.

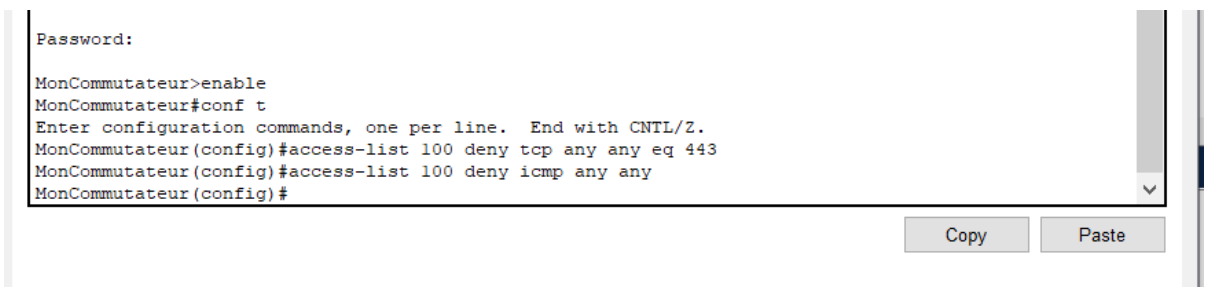


Testez avec la commande ping





Bloquer le Trafic HTTPS et ICMP



```
MonCommutateur(config)#access-list 100 deny icmp any any
MonCommutateur(config)#
MonCommutateur(config)#interface FastEthernet0/0
MonCommutateur(config-if)#ip access-group 100 in
MonCommutateur(config-if)#exit
MonCommutateur(config)#
```

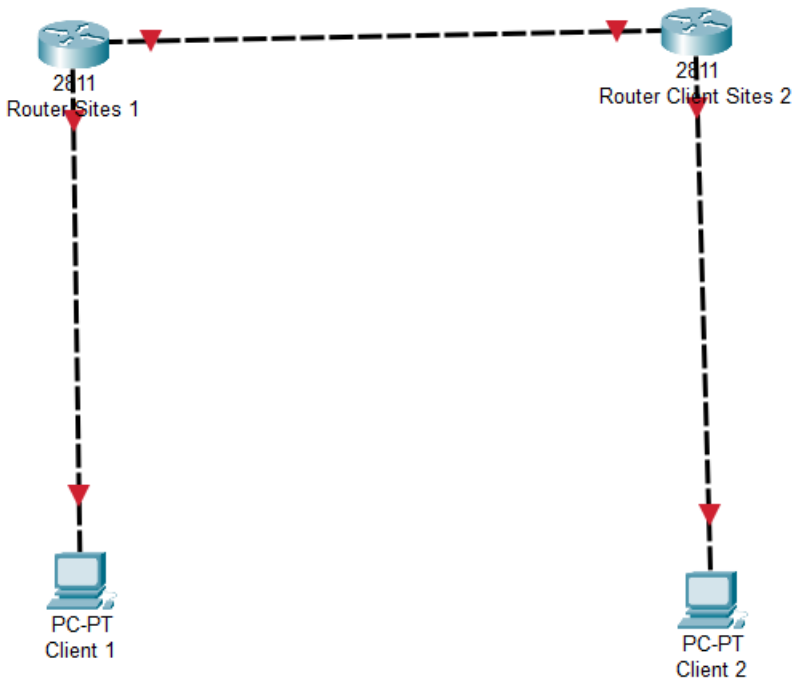
Copy Paste

Sauvegarde de la Configuration

```
%SYS-5-CONFIG_I: Configured from console by console

MonCommutateur#write memory
Building configuration...
[OK]
MonCommutateur#
```

Configuration d'un VPN Site-à-Site

Architecture du Réseau



Configuration des Adresses IP

Sur R1 (Site 1)

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)## Interface LAN
              ^
% Invalid input detected at '^' marker.

Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)## Interface WAN (vers Internet)
              ^
% Invalid input detected at '^' marker.

Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)## Route statique vers le rseau de Site 2 via VPN
              ^
% Invalid input detected at '^' marker.

Router(config)#ip route 192.168.2.0 255.255.255.0 10.0.0.2
Router(config)#exit
Router#write memory
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Sur R2 (Site 2)

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)## Interface LAN
              ^
% Invalid input detected at '^' marker.

Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)## Interface WAN (vers Internet)
              ^
% Invalid input detected at '^' marker.

Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 10.0.0.2 255.255.255.252
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)## Route statique vers le rseau de Site 1 via VPN
              ^
% Invalid input detected at '^' marker.

Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.0.1
Router(config)#exit
Router#write memory
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Configuration du VPN IPsec

Sur R1 (Site 1)

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key VPN_SECRET address 10.0.0.2
Router(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
Router(config)#mode tunnel
               ^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#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.
Router(config-crypto-map)#set peer 10.0.0.2
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#interface GigabitEthernet0/1
%Invalid interface type and number
Router(config)#crypto map VPN-MAP
% Incomplete command.
Router(config)#exit
Router#write memory
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Copy Paste

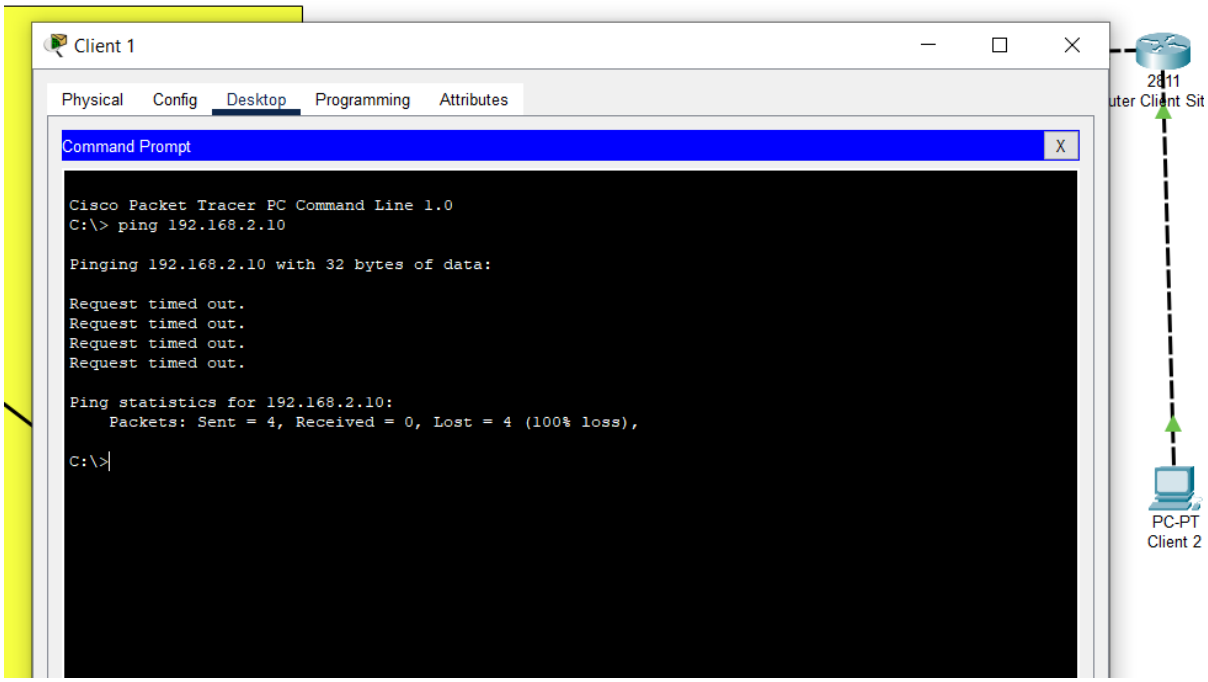
Sur R2 (Site 2)

```
Router#
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
Router(config)#crypto isakmp key VPN_SECRET address 10.0.0.1
Router(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
Router(config)#mode tunnel
                ^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
Router(config-crypto-map)#set peer 10.0.0.1
Router(config-crypto-map)#set transform-set VPN-SET
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#interface GigabitEthernet0/1
%Invalid interface type and number
Router(config)#crypto map VPN-MAP
% Incomplete command.
Router(config)#exit
Router#write memory
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Copy Paste

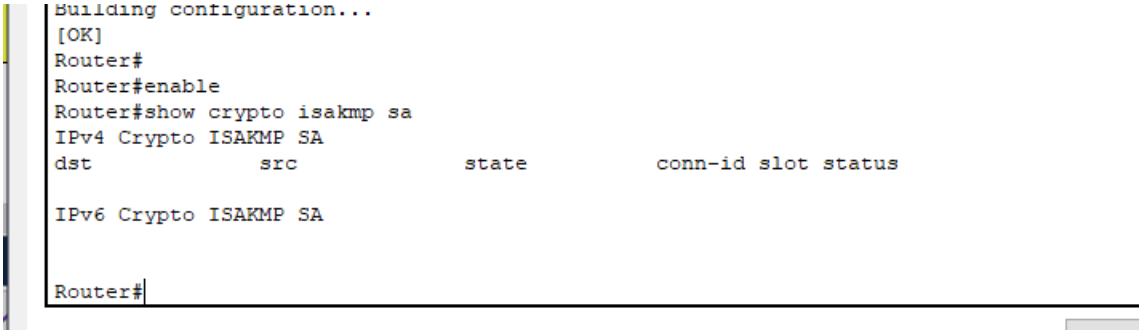
Vérification du VPN

Tester la connectivité



La commande pour le mode tunnel n'avait pas passer, je pense que c'est la raison pour laquelle qu'on n'as pas pu trouver les bons résultats.

Vérifier l'établissement du VPN



En Conclusion, Ce TD propose une approche pratique et didactique pour configurer des pare-feu et des VPN site-à-site dans Cisco Packet Tracer. En commençant par la configuration de pare-feu à l'aide de listes de contrôle d'accès (ACL), ce TD enseigne les fondamentaux pour bloquer et autoriser différents types de trafic réseau, garantissant ainsi un niveau de sécurité renforcé. Les tests de connectivité et de sécurité permettent de valider l'efficacité des configurations mises en place.

Ensuite, la configuration d'un VPN site-à-site entre deux routeurs Cisco offre une solution robuste pour sécuriser les communications entre deux réseaux distants en utilisant IPsec. Cette étape est cruciale pour protéger les données sensibles lors de leur transit sur des réseaux publics. En testant la connectivité et en vérifiant le bon fonctionnement du VPN, les participants peuvent s'assurer que les communications sont non seulement sécurisées, mais aussi stables et fiables.

En conclusion, ce TD offre une formation complète sur les bases de la configuration des pare-feu et des VPN dans un environnement Cisco Packet Tracer, permettant ainsi aux apprenants de renforcer leurs compétences en sécurité réseau et de mieux protéger les infrastructures informatiques.

Le mode tunnel ne m'a pas permis de faire tous les travail et aboutir au bon résultat dans le dernier partis du TD mais, je comprends tous les concepts.