Université Abdelmalek Essaâdi

Faculté des Sciences et Techniques-Tanger

Département Génie Informatique

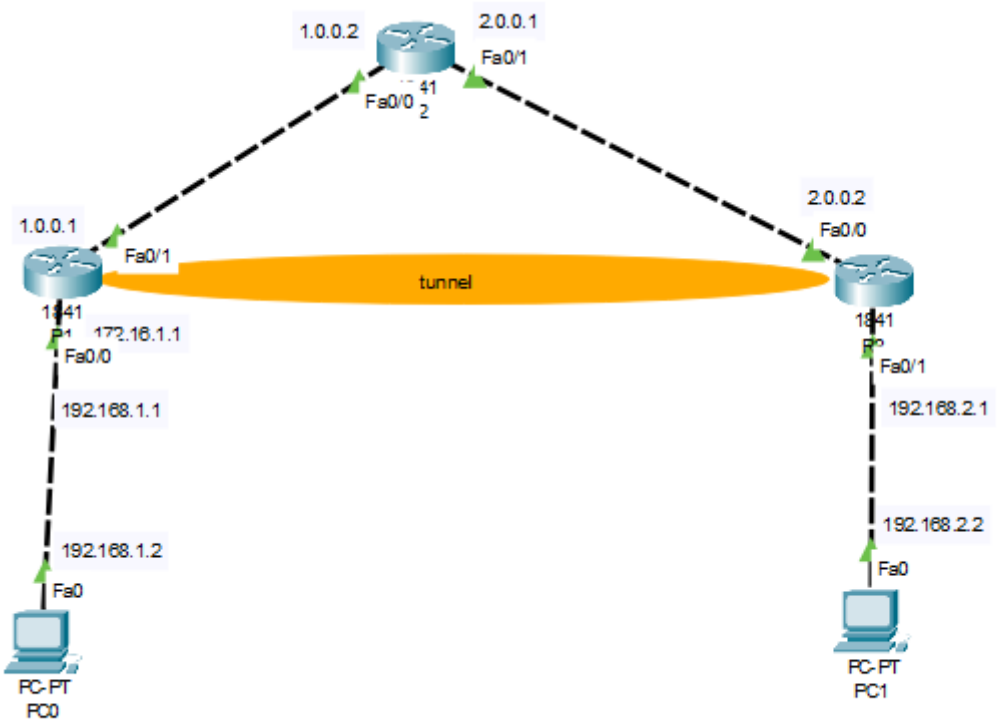
Cryptographie-Sécurité Services

VPN

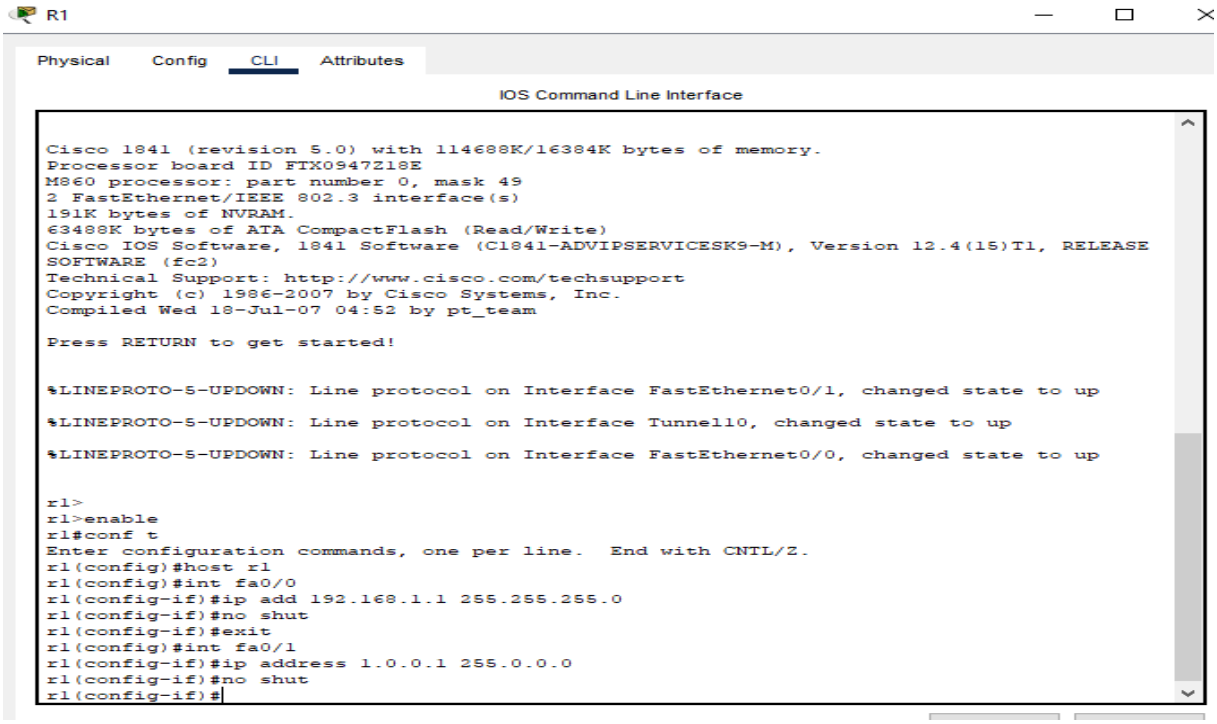
Réalisé Par :

Yossra safi chetouan

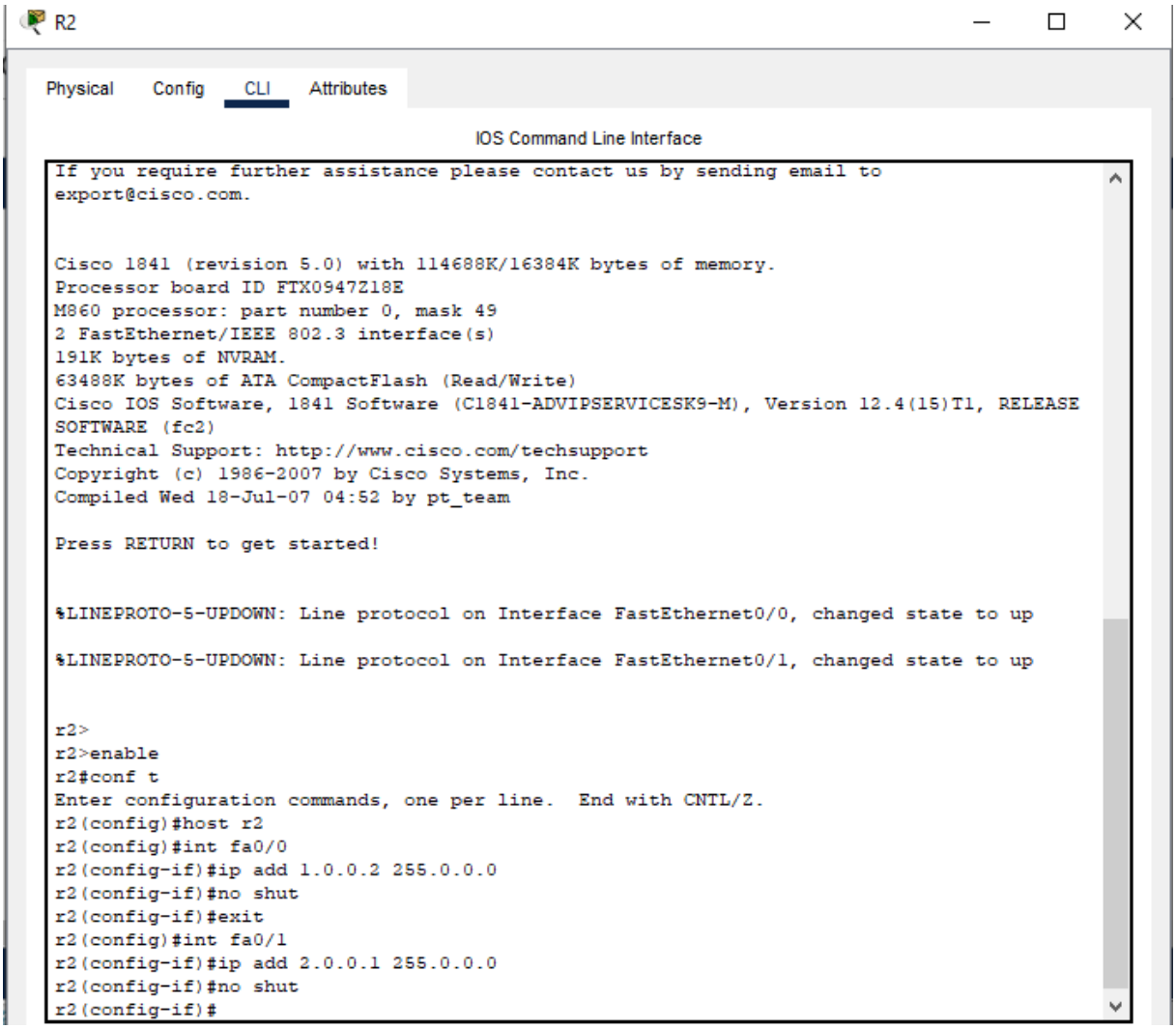
TP-1 vpn configuration lab using routers in cisco packet tracer



CONFIGURATION ON ROUTER R1



CONFIGURATION ON ROUTER R2



CONFIGURATION ON ROUTER R3:

R3

Physical Config CLI Attributes

IOS Command Line Interface

```
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!


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

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed state to up


r3>
r3>enbale
Translating "enbale"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

r3>enable
r3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r3(config)#host r3
r3(config)#int fa0/0
r3(config-if)#ip add 2.0.0.2 255.0.0.0
r3(config-if)#no shut
r3(config-if)#exit
r3(config)#int fa0/1
r3(config-if)#ip add 192.168.2.1 255.255.255.0
r3(config-if)#no shut
r3(config-if)#
```

Now its time to do routing.here i am going to configure default routing.

```
r1(config-if)#exit
r1(config)#ip route 0.0.0.0 0.0.0.0 1.0.0.2
r1(config)#
```

```
r3(config-if)#exit
r3(config)#ip route 0.0.0.0 0.0.0.0 2.0.0.1
r3(config)#
```

First we go to router r1 and ping with router r3: r1#ping 2.0.0.2
Now we go to router r3 and ping with router r1: r3#ping 1.0.0.1

```
r1#
%SYS-5-CONFIG_I: Configured from console by console

r1#ping 1.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/32 ms

r1#
```

```
r3#
%SYS-5-CONFIG_I: Configured from console by console

r3#ping 2.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/10 ms

r3#
```

NOW CREATE VPN TUNNEL between R1 and R3:

```
r3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r3(config)#interface tunnel 100
r3(config-if)#ip address 172.16.1.2 255.255.0.0
r3(config-if)#tunnel source fa0/0
r3(config-if)#tunnel destination 1.0.0.1
r3(config-if)#no shut
r3(config-if)#
```

```
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#interface tunnel 10
r1(config-if)#ip address 172.16.1.1 255.255.0.0
r1(config-if)#tunnel source fa0/1
r1(config-if)#tunnel destination 2.0.0.2
r1(config-if)#no shut
r1(config-if)#
```

Now test communication between these two routers again by pinging eah other:

```
r3#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/12 ms

r3#
```

```
r1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 7/16/27 ms

r1#
```

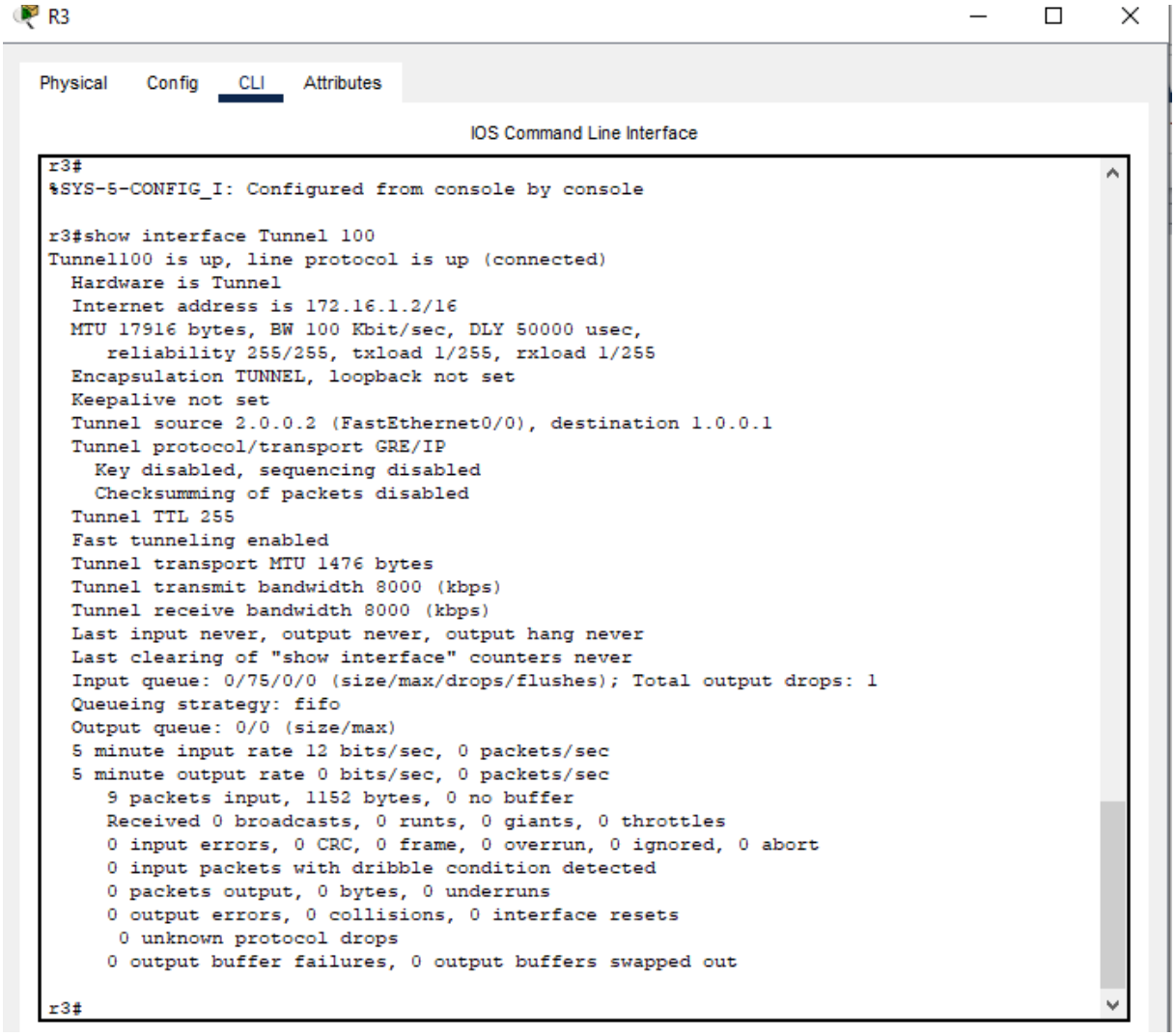
Now Do routing for created VPN Tunnel on Both Router R1 and R3:
r1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2
r3(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1

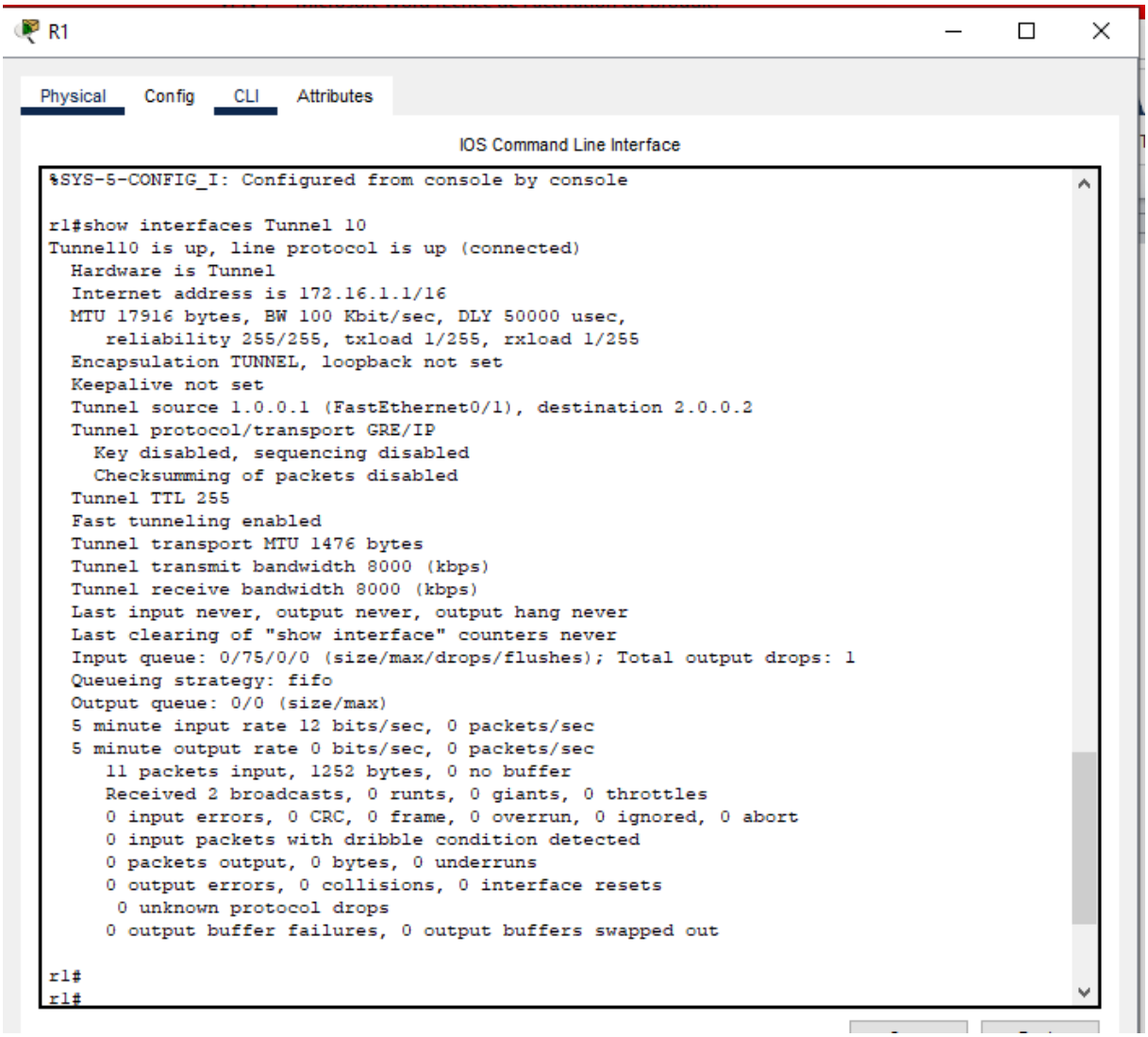
```
r3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r3(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1
r3(config)#
```

n

```
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2
r1(config)#
```

TEST VPN TUNNEL CONFIGURATION:
r1#show interfaces Tunnel 10 and r3#show interface Tunnel 100





HOW TO TRACE THE VPN TUNNEL PATH?

Now if you want to check what path vpn tunnel is using just go to any of the computer i.e pc and then ping

anothr pc located in different network. And then trace the path using tracert. Its result will show the path followed by VPN Tunnel created by you.

PC1

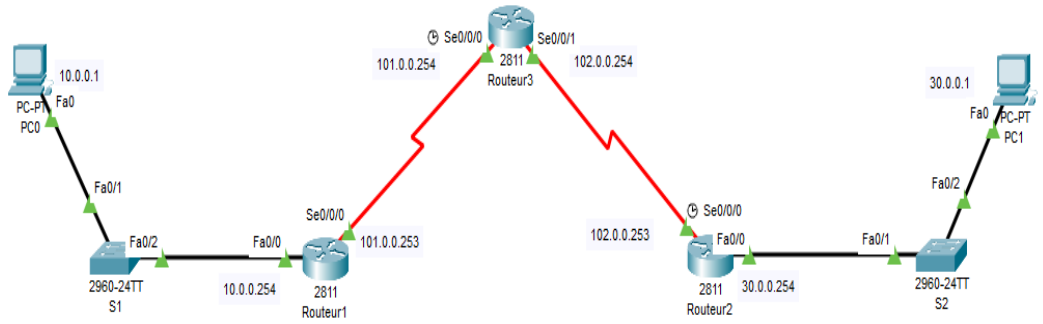
Physical Config Desktop Programming Attributes

Command Prompt

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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::202:4AFF:FE8E:6431
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.2.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.2.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=27ms TTL=126
Reply from 192.168.1.2: bytes=32 time=10ms TTL=126
Reply from 192.168.1.2: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 27ms, Average = 16ms
```

```
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.2.1
  2    17 ms     18 ms     22 ms     172.16.1.1
  3    28 ms     23 ms     0 ms      192.168.1.2

Trace complete.

C:\>
```

TP-2 : VPN IPsec CISCO de site à site



Les routeurs utilisés sont des Cisco 2811.

Configuration de base de routeur1

Routeur1

Physical Config CLI Attributes

IOS Command Line Interface

```
62720K bytes of  ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

Press RETURN to get started!


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

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Routeur1>
Routeur1>enable
Routeur1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur1(config)#hostname Routeur1
Routeur1(config)#interface FastEthernet 0/0
Routeur1(config-if)#no shutdown
Routeur1(config-if)#ip address 10.0.0.254 255.0.0.0
Routeur1(config-if)#ip nat inside
Routeur1(config-if)#exit
Routeur1(config)#interface Serial 0/0/0
Routeur1(config-if)#no shutdown
Routeur1(config-if)#ip address 101.0.0.253 255.0.0.0
Routeur1(config-if)#ip nat outside
Routeur1(config-if)#exit
Routeur1(config)#ip route 0.0.0.0 0.0.0.0 101.0.0.254
Routeur1(config)#do wr
Building configuration...
[OK]
Routeur1(config)#
```

Copy Paste

Mise en place de la fonction NAT sur Routeur1

```
Routeur1(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255
Routeur1(config)#access-list 100 permit ip 10.0.0.0 0.255.255.255 any
Routeur1(config)#ip nat inside source list 100 interface Serial 0/0/0 overload
Routeur1(config)#do wr
Building configuration...
[OK]
Routeur1(config)#
```

Copy Paste

Configuration de base de routeur2

Mise en place de la fonction NAT sur Routeur2

```
% Unknown command or computer name, or unable to find computer address

Routeur2>enable
Routeur2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur2(config)#hostname Routeur2
Routeur2(config)#interface FastEthernet 0/0
Routeur2(config-if)#no shutdown
Routeur2(config-if)#ip address 30.0.0.254 255.0.0.0
Routeur2(config-if)#ip nat inside
Routeur2(config-if)#exit
Routeur2(config)#interface Serial 0/0/0
Routeur2(config-if)#no shutdown
Routeur2(config-if)#ip address 102.0.0.253 255.0.0.0
Routeur2(config-if)#ip nat outside
Routeur2(config-if)#exit
Routeur2(config)#ip route 0.0.0.0 0.0.0.0 102.0.0.254
Routeur2(config)#do wr
Building configuration...
[OK]
Routeur2(config)#access-list 100 deny ip 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
Routeur2(config)#access-list 100 permit ip 30.0.0.0 0.255.255.255 any
Routeur2(config)#ip nat inside source list 100 interface Serial 0/0/0 overload
Routeur2(config)#do wr
Building configuration...
[OK]
Routeur2(config)#
```

Configuration de base de routeur3 (le routeur central)

Routeur3

Physical Config CLI Attributes

IOS Command Line Interface

```
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up


Routeur3>
Routeur3>enable
Routeur3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Routeur3(config)#hostname Routeur3
Routeur3(config)#interface Serial 0/0/0
Routeur3(config-if)#clock rate 2000000
Routeur3(config-if)#no shutdown
Routeur3(config-if)#ip address 101.0.0.254 255.0.0.0
Routeur3(config-if)#exit
Routeur3(config)#interface Serial 0/0/1
Routeur3(config-if)#clock rate 2000000
This command applies only to DCE interfaces
Routeur3(config-if)#no shutdown
Routeur3(config-if)#ip address 102.0.0.254 255.0.0.0
Routeur3(config-if)#exit
Routeur3(config)#ip route 10.0.0.0 255.0.0.0 101.0.0.253
Routeur3(config)#ip route 30.0.0.0 255.0.0.0 102.0.0.253
Routeur3(config)#do wr
Building configuration...
[OK]
Routeur3(config)#
```

Mise en place du tunnel VPN IPsec

Configuration de la négociation des clés (phase 1)

Routeur1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router1 con0 is now available




Press RETURN to get started.









Router1>enable
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto isakmp enable
Router1(config)#crypto isakmp policy 10
Router1(config-isakmp)#encryption aes
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#hash sha
Router1(config-isakmp)#group 2
Router1(config-isakmp)#lifetime 86400
Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key CLESECRETE address 102.0.0.253
A pre-shared key for address mask 102.0.0.253 255.255.255.255 already exists!
Router1(config)#
```

Configuration de la méthode de chiffrage des données (phase 2)

```
Routeur1(config)#crypto isakmp key CLESECRETE address 102.0.0.253
A pre-shared key for address mask 102.0.0.253 255.255.255.255 already exists!
Routeur1(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeur1(config)#crypto ipsec security-association lifetime seconds 86400
Routeur1(config)#ip access-list extended VPN
Routeur1(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255
Routeur1(config-ext-nacl)#exit
Routeur1(config)#crypto map CARTEVPN 10 ipsec-isakmp
Routeur1(config-crypto-map)#match address VPN
Routeur1(config-crypto-map)#set peer 102.0.0.253
Routeur1(config-crypto-map)#set transform-set VPNLABO
Routeur1(config-crypto-map)#exit
Routeur1(config)#interface serial 0/0/0
Routeur1(config-if)#crypto map CARTEVPN
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Routeur1(config-if)#do wr
Building configuration...
[OK]
Routeur1(config-if)#
```

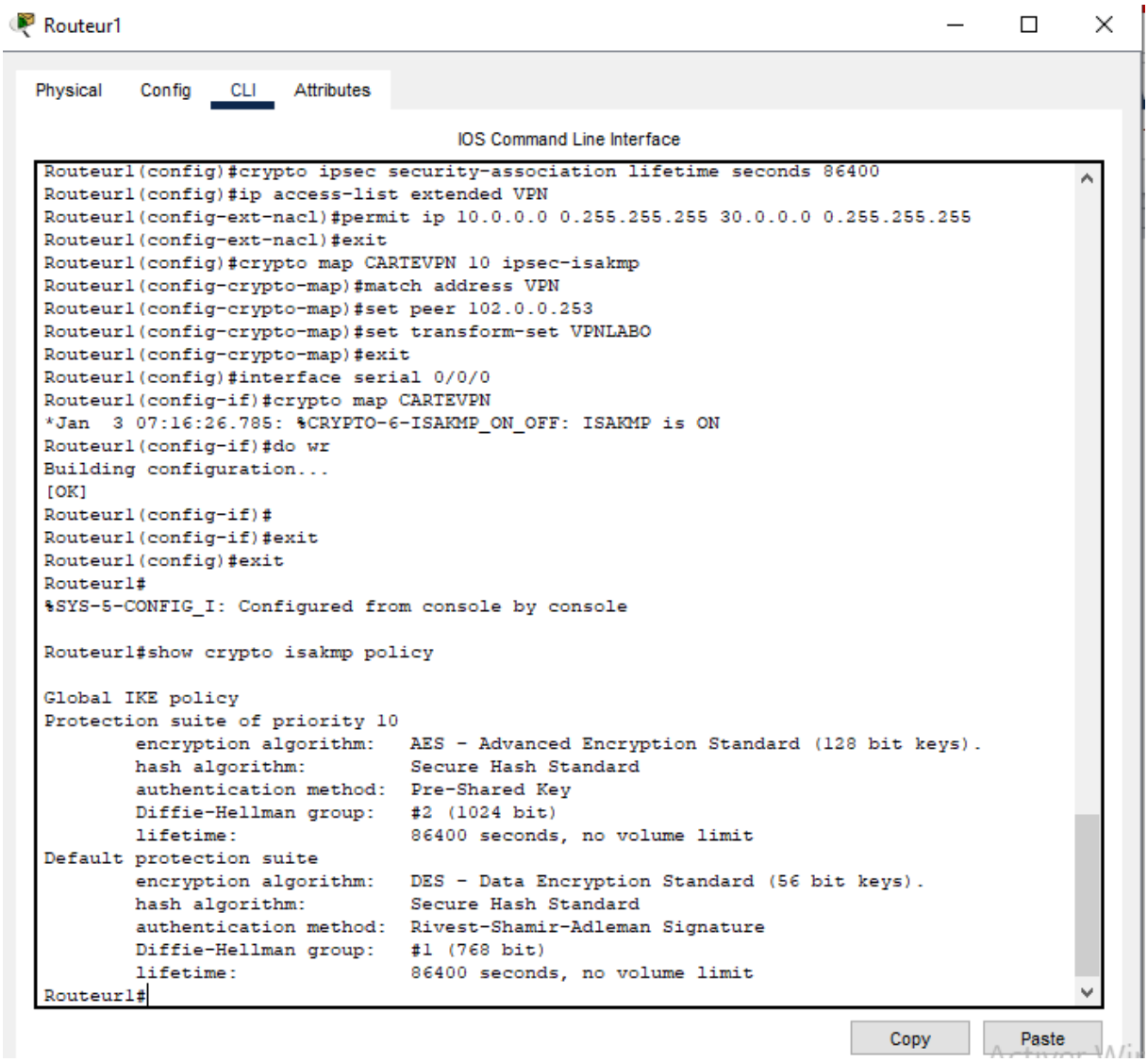
Le Routeur1 est prêt, il reste à faire l'équivalent sur Routeur2.

Voici le détail de la configuration sur Routeur2

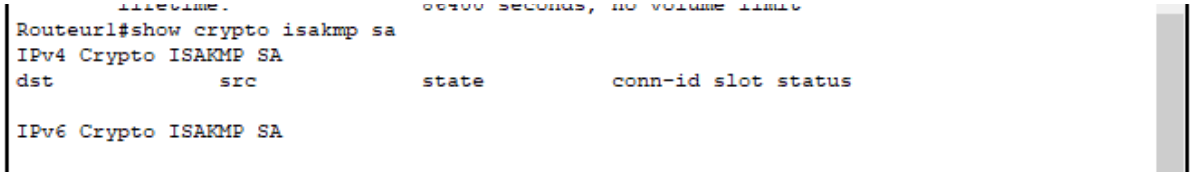
```
Routeur2(config)#crypto isakmp enable
Routeur2(config)#crypto isakmp policy 10
Routeur2(config-isakmp)#encryption aes
Routeur2(config-isakmp)#authentication pre-share
Routeur2(config-isakmp)#hash sha
Routeur2(config-isakmp)#group 2
Routeur2(config-isakmp)#lifetime 86400
Routeur2(config-isakmp)#exit
Routeur2(config)#crypto isakmp key CLESECRETE address 101.0.0.253
A pre-shared key for address mask 101.0.0.253 255.255.255.255 already exists!
Routeur2(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeur2(config)#crypto ipsec security-association lifetime seconds 86400
Routeur2(config)#ip access-list extended VPN
Routeur2(config-ext-nacl)#permit ip 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
Routeur2(config-ext-nacl)#exit
Routeur2(config)#crypto map CARTEVPN 10 ipsec-isakmp
Routeur2(config-crypto-map)# match address VPN
Routeur2(config-crypto-map)#set peer 101.0.0.253
Routeur2(config-crypto-map)#set transform-set VPNLABO
Routeur2(config-crypto-map)#exit
Routeur2(config)#interface serial 0/0/0
Routeur2(config-if)#crypto map CARTEVPN
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Routeur2(config-if)#do wr
Building configuration...
[OK]
Routeur2(config-if)#
```

Vérification du fonctionnement tunnel VPN

- Routeur1#show crypto isakmp policy



- Routeur1#show crypto isakmp sa



- Routeur1#show crypto ipsec sa

```
Routeur1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: CARTEVPN, local addr 101.0.0.253

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   remote  ident (addr/mask/prot/port): (30.0.0.0/255.0.0.0/0/0)
   current_peer 102.0.0.253 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.: 101.0.0.253, remote crypto endpt.:102.0.0.253
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

Routeur1#
```