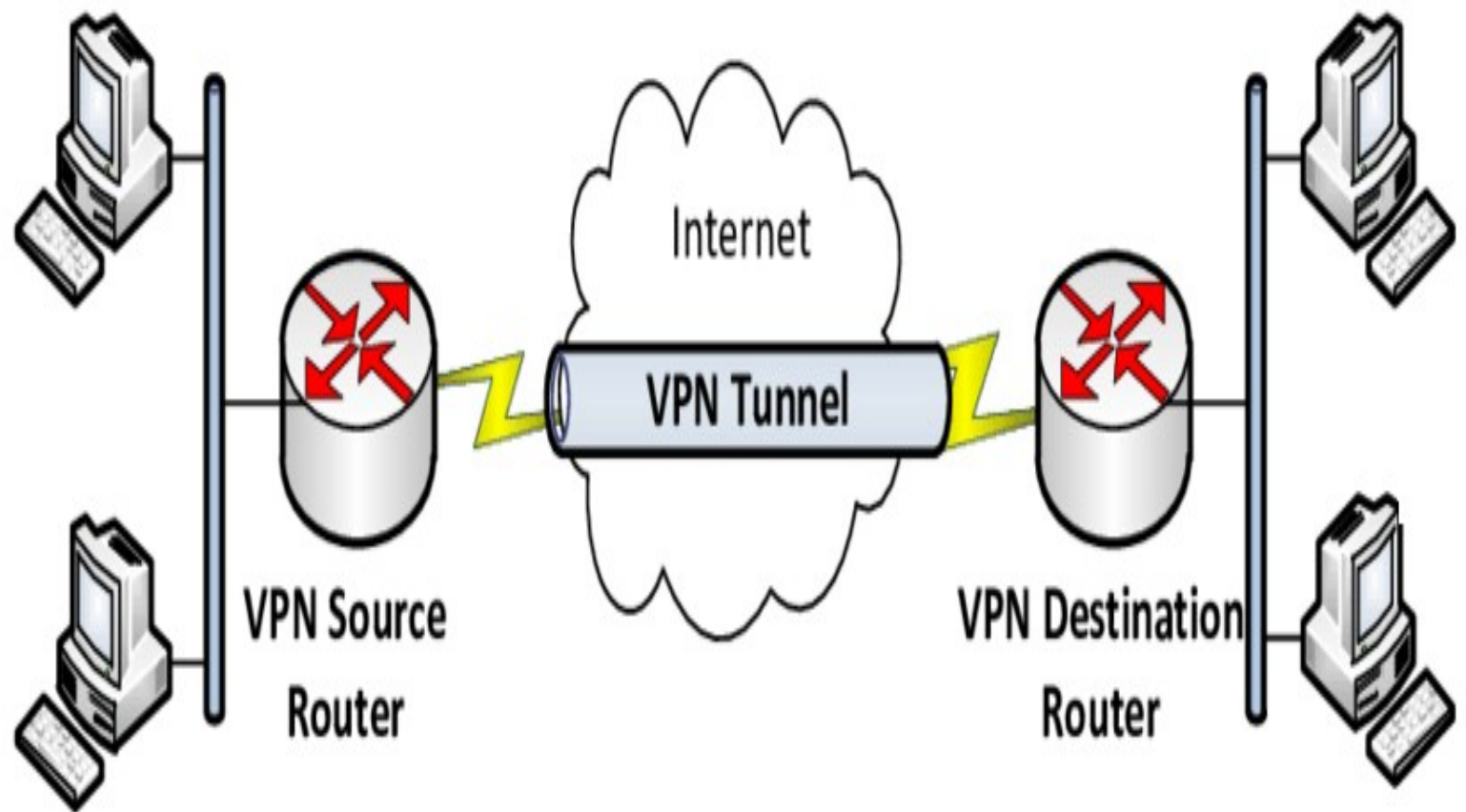


Tunneling : VPN (Virtual Private Network)



Sommaire

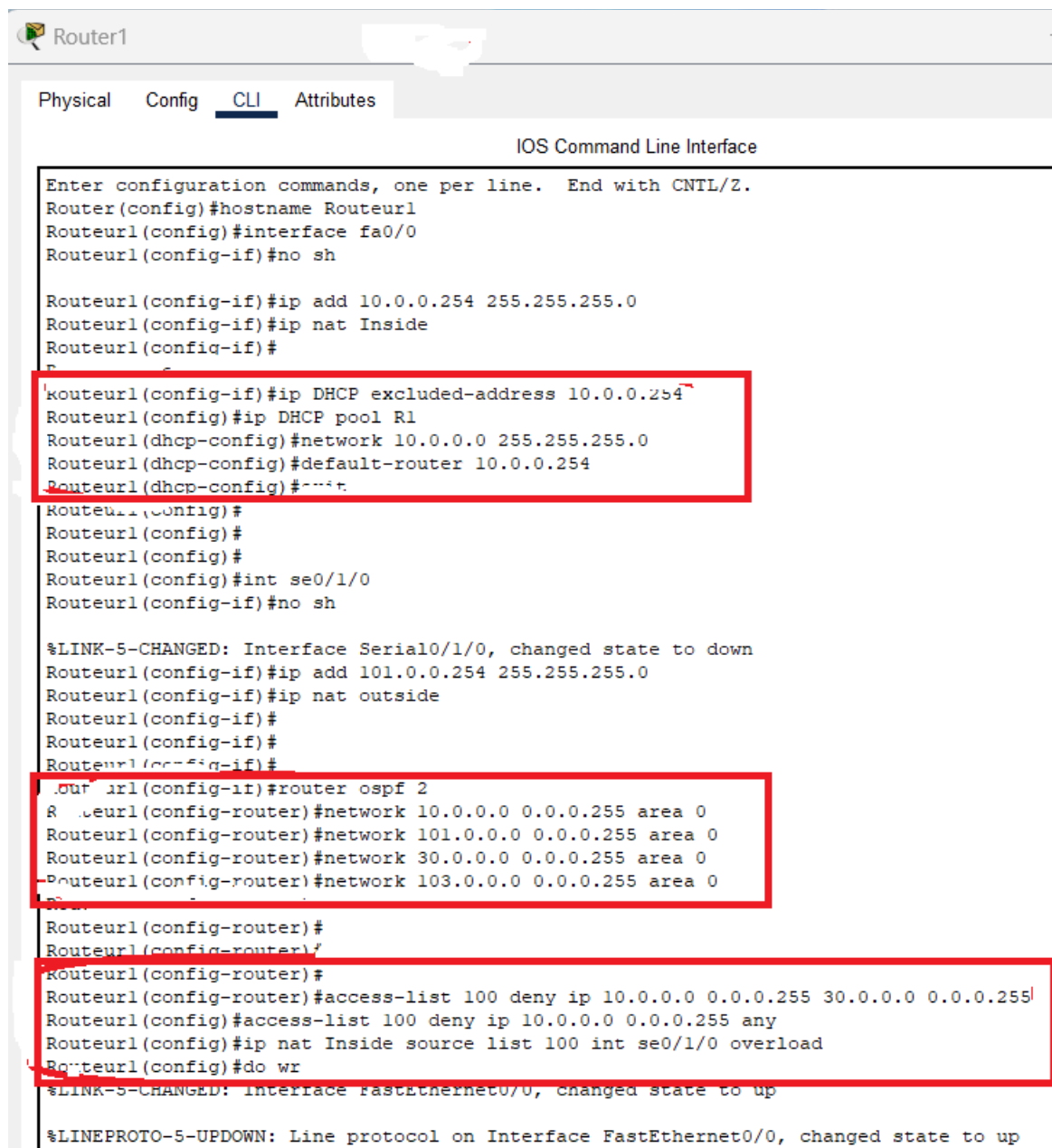
1.C'est quoi un VPN ?.....	4
2.Configuration de base.....	4
3.Configuration du routeur 3.....	5
4.mise en place du tunnel Ipsec.....	6
Étape 1 : configuration de la négociation des clés.....	6
Étape 2 : Configuration de chiffrement.....	6
5.Vérification.....	8
6.Plan.....	9

1.C'est quoi un VPN ?

Un **VPN (Virtual Private Network)** est une technologie qui crée une connexion sécurisée entre un utilisateur et un réseau distant via Internet. Il protège les données grâce au chiffrement et masque l'adresse IP, offrant confidentialité, sécurité et accès aux ressources distantes ou restreintes.

2.Configuration de base

Pour assurer le routage inter réseau. Même configuration pour le routeur 2



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Routeurl
Routeurl(config)#interface fa0/0
Routeurl(config-if)#no sh

Routeurl(config-if)#ip add 10.0.0.254 255.255.255.0
Routeurl(config-if)#ip nat Inside
Routeurl(config-if)#
Routeurl(config-if)#ip DHCP excluded-address 10.0.0.254
Routeurl(config)#ip DHCP pool R1
Routeurl(dhcp-config)#network 10.0.0.0 255.255.255.0
Routeurl(dhcp-config)#default-router 10.0.0.254
Routeurl(dhcp-config)#exit
Routeurl(config)#
Routeurl(config)#
Routeurl(config)#
Routeurl(config)#int se0/1/0
Routeurl(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Routeurl(config-if)#ip add 101.0.0.254 255.255.255.0
Routeurl(config-if)#ip nat outside
Routeurl(config-if)#
Routeurl(config-if)#
Routeurl(config-if)#
Routeurl(config-if)#
Routeurl(config-if)#router ospf 2
Routeurl(config-router)#network 10.0.0.0 0.0.0.255 area 0
Routeurl(config-router)#network 101.0.0.0 0.0.0.255 area 0
Routeurl(config-router)#network 30.0.0.0 0.0.0.255 area 0
Routeurl(config-router)#network 103.0.0.0 0.0.0.255 area 0
Routeurl(config-router)#
Routeurl(config-router)#
Routeurl(config-router)#
Routeurl(config-router)#access-list 100 deny ip 10.0.0.0 0.0.0.255 30.0.0.0 0.0.0.255
Routeurl(config)#access-list 100 deny ip 10.0.0.0 0.0.0.255 any
Routeurl(config)#ip nat Inside source list 100 int se0/1/0 overload
Routeurl(config)#do wr

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

3. Configuration du routeur 3

clock rate 2000000 configure la vitesse de l'horloge de les interfaces série 0/1/0 et /0/1/1 du router permettant la synchronisation de la communication



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started.

Router>!Configuration de base du routeur
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Routeur3
Routeur3(config-if)#clock rate 2000000
This command applies only to DCE interfaces
Routeur3(config-if)#no sh
Routeur3(config-if)#ip add 101.0.0.253 255.255.255.0
Routeur3(config-if)#exit
Routeur3(config)#
Routeur3(config)#int se0/1/1
Routeur3(config-if)#clock rate 2000000
Routeur3(config-if)#no sh
Routeur3(config-if)#ip add 103.0.0.253 255.255.255.0
Routeur3(config-if)#
Routeur3(config-if)#
Routeur3(config-if)#router ospf 4
Routeur3(config-router)#network 10.0.0.0 0.0.0.255 area 0
Routeur3(config-router)#network 101.0.0.0 0.0.0.255 area 0
Routeur3(config-router)#network 30.0.0.0 0.0.0.255 area 0
Routeur3(config-router)#network 103.0.0.0 0.0.0.255 area 0
Routeur3(config-router)#do wr
```

4.mise en place du tunnel Ipsec

Étape 1 : configuration de la négociation des clés

```
Routeurl>
Routeurl>
Routeurl>
Routeurl>!Mise en place du tunnel VPN IPsec
Routeurl>en
Routeurl#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Routeurl(config)#crypto isakmp enable
Routeurl(config)#crypto isakmp Policy 10
Routeurl(config-isakmp)#encryption aes
Routeurl(config-isakmp)#authentication pre-share
Routeurl(config-isakmp)#hash sha
Routeurl(config-isakmp)#group 2
Routeurl(config-isakmp)#lifetime 86400
Routeurl(config-isakmp)#exit
Routeurl(config)#crypto isakmp key CLESCRETE address 103.0.0.254
Routeurl(config)#
```

Étape 2 : Configuration de chiffrement

Routeur 1

```
Routeurl>en
Routeurl#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Routeurl(config)#crypto IPsec transform-set VPNLABO esp-aes esp-sha-hmac
Routeurl(config)#crypto IPsec security-association lifetime seconds 86400
Routeurl(config)#ip access-list extended VPN
Routeurl(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 30.0.0.0 0.0.0.255
Routeurl(config-ext-nacl)#exit
Routeurl(config)#
Routeurl(config)#crypto map CARTEVPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Routeurl(config-crypto-map)#match address VPN
Routeurl(config-crypto-map)#set peer 103.0.0.254
Routeurl(config-crypto-map)#set transform-set VPNLABO
Routeurl(config-crypto-map)#exit
Routeurl(config)#
Routeurl(config)#|
Routeurl(config)#interface se0/1/0
Routeurl(config-if)#crypto map CARTEVPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Routeurl(config-if)#do wr
```

Routeur 2

```
Router2
Physical Config CLI Attributes
IOS Command Line Interface

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

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

Routeur2>
Routeur2>en
Routeur2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Routeur2(config)#!R2
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)#
Routeur2(config)#crypto isakmp key CLESECRETE address 101.0.0.254
Routeur2(config)#
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 0.0.0.255 10.0.0.0 0.0.0.255
Routeur2(config-ext-nacl)#exit
Routeur2(config)#
Routeur2(config)#crypto map CARTEVPN 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Routeur2(config-crypto-map)#match address VPN
Routeur2(config-crypto-map)#set peer 101.0.0.254
Routeur2(config-crypto-map)#set transform-set VPNLABO
Routeur2(config-crypto-map)#exit
Routeur2(config)#interface serial 0/1/0
Routeur2(config-if)#crypto map CARTEVPN
*Jan 3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
Routeur2(config-if)#do wr
```

5.Vérification

```
Routeur1>
Routeur1>en
Routeur1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
  encryption algorithm:  AES - Advanced Encryption Standard (128 bit keys).
  hash algorithm:        Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group:  #2 (1024 bit)
  lifetime:              86400 seconds, no volume limit
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:        Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group:  #1 (768 bit)
  lifetime:              86400 seconds, no volume limit
Routeur1#
```

```
Routeur1#show crypto isakmp sa
```

IPv4 Crypto ISAKMP SA				
dst	src	state	conn-id	slot status
IPv6 Crypto ISAKMP SA				

```
Routeur1#show crypto ipsec sa
```

```
interface: Serial0/1/0
  Crypto map tag: CARTEVPN, local addr 101.0.0.254

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (30.0.0.0/255.255.255.0/0/0)
  current_peer 103.0.0.254 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.: 101.0.0.254, remote crypto endpt.:103.0.0.254
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
    current outbound spi: 0x0(0)

  inbound esp sas:
```

```
--More--
```

Ping depuis le PC 2 au PC 1

```
Ping statistics for 30.0.0.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>tracert 30.0.0.2

Tracing route to 30.0.0.2 over a maximum of 30 hops:

  1  0 ms      0 ms      0 ms      10.0.0.254
  2  1 ms      1 ms      2 ms      103.0.0.254
  3  2 ms      2 ms      2 ms      30.0.0.2

Trace complete.

C:\>
```

6. Plan

