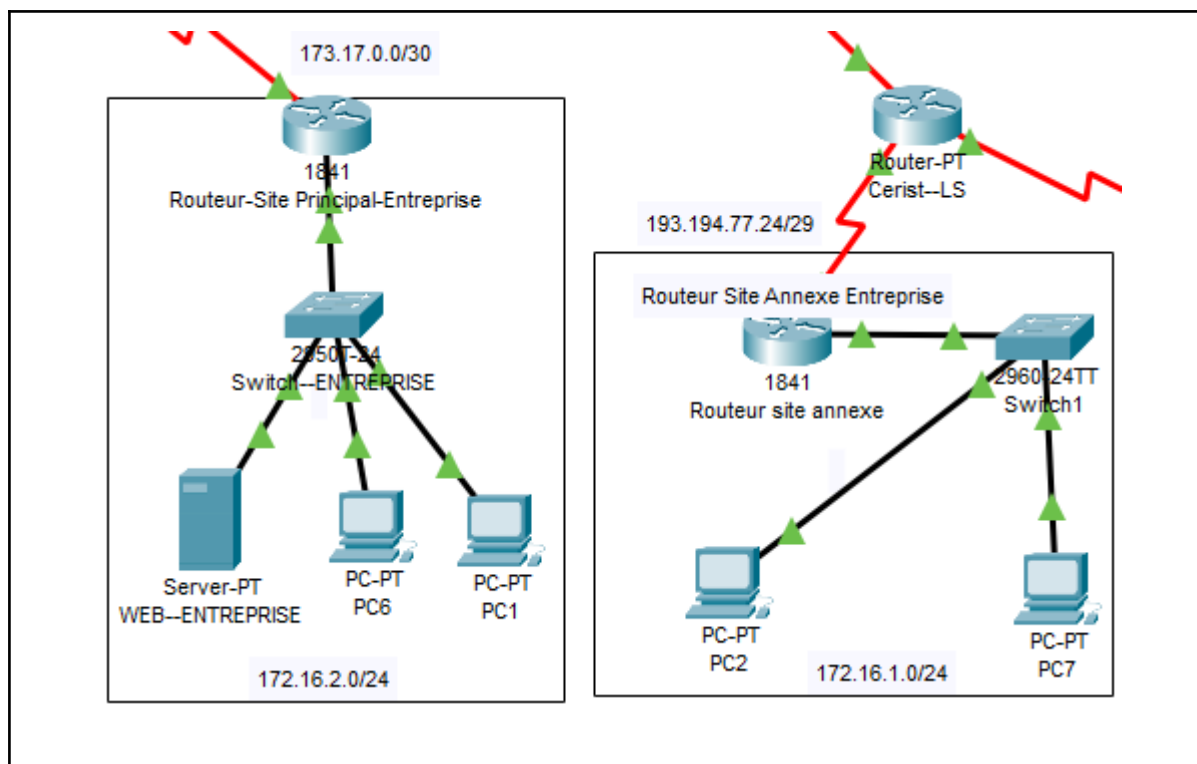


Activité :**1. Complétude de la configuration des deux routeurs d'extrémité. (Commandes)**

Protocole d'encapsulation	AH
Algorithme de hachage	md5

Au niveau Routeur du site Principal:

*/*pour annuler la transform-set qui est crier dans la partie applicative du TP (set qui a le nom 50) au niveau de cette routeur*/*

vpnPrincipale(config)#no crypto ipsec transform-set 50 esp-3des esp-md5-hmac

*/*on définit une autre transform-set qui va utiliser seulement la fonction de hachage et il n'utilise pas l'algorithme de cryptage car le mode AH implique que il ya pas un cryptage de données*/*

vpnPrincipale(config)#crypto ipsec transform-set 51 ah-md5-hmac

vpnPrincipale(config)#crypto map test 10 ipsec-isakmp

vpnPrincipale(config-crypto-map)#set peer 193.194.77.26

vpnPrincipale(config-crypto-map)#set security-association lifetime seconds 900

vpnPrincipale(config-crypto-map)#set transform-set 51

vpnPrincipale(config-crypto-map)#match address 101

vpnPrincipale(config-crypto-map)#exit

```

vpnPrincipale(config)#interface serial0/0/0
vpnPrincipale(config-if)#crypto map test
vpnPrincipale(config-if)#exit
vpnPrincipale(config)#exit
vpnPrincipale#

```

Au niveau Routeur du site Annexe:

*/*pour annuler la transform-set qui est crier dans la partie applicative du TP (set qui a le nom 50) au niveau de cette routeur*/*

```
vpnAnnexe(config)#no crypto ipsec transform-set 50 esp-3des esp-md5-hmac
```

*/*on définit une autre transform-set qui va utiliser seulement la fonction de hachage et il n'utilise pas l'algorithme de cryptage car le mode AH implique que il ya pas un cryptage de données*/*

```
vpnAnnexe(config)#crypto ipsec transform-set 51 ah-md5-hmac
```

```
vpnAnnexe(config)#crypto map test 10 ipsec-isakmp
```

```
vpnAnnexe(config)#set peer 173.17.0.2
```

```
vpnAnnexe(config)#set security-association lifetime seconds 900
```

```
vpnAnnexe(config)#set transform-set 51
```

```
vpnAnnexe(config)#match address 101
```

```
vpnAnnexe(config-crypto-map)#exit
```

```
vpnAnnexe(config)#interface serial0/0/0
```

```
vpnAnnexe(config-if)#crypto map test
```

```
vpnPrincipale(config-if)#exit
```

```
vpnPrincipale(config)#exit
```

2. Vérification de la création du tunnel et son fonctionnement.

Commande												
show crypto isakmp sa												
Résultat												
<pre>vpnPrincipale# show crypto isakmp sa IPv4 Crypto ISAKMP SA</pre> <table><tr><th>dst</th><th>src</th><th>state</th><th>conn-id</th><th>slot</th><th>status</th></tr><tr><td>193.194.77.26</td><td>173.17.0.2</td><td>QM_IDLE</td><td>1072</td><td>0</td><td>ACTIVE</td></tr></table> <pre>IPv6 Crypto ISAKMP SA</pre>	dst	src	state	conn-id	slot	status	193.194.77.26	173.17.0.2	QM_IDLE	1072	0	ACTIVE
dst	src	state	conn-id	slot	status							
193.194.77.26	173.17.0.2	QM_IDLE	1072	0	ACTIVE							
Explication												
<ul style="list-style-type: none">On voit bien les deux extrémités du tunnel, ça veut dire les interfaces du deux routeurs qui permettent de se connecter site to site.												

Commande (Routeur vpnPrincipale)

show crypto ipsec sa

Résultat

```
vpnPrincipale#show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: test, local addr 173.17.0.2

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer 193.194.77.26 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 173.17.0.2, remote crypto endpt.:193.194.77.26
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0xB77B4C8C(3078311052)

inbound esp sas:
  spi: 0x981E523A(2552123962)
    transform: ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: FPGA:1, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4525504/797)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:
  spi: 0xA34B17B7(2739607479)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: FPGA:1, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4525504/797)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

inbound pcp sas:

outbound esp sas:
  spi: 0xB77B4C8C(3078311052)
    transform: ,
    in use settings ={Tunnel, }
    conn id: 2003, flow_id: FPGA:1, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4525504/797)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:
  spi: 0x526B0F03(1382747907)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2003, flow_id: FPGA:1, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4525504/797)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE

outbound pcp sas:
```

Explication
<ul style="list-style-type: none"> • A partir de cette commande on peut vérifier l'intervalle des adresses IP qui est validé à travers ce tunnel, il permet aussi de vérifier notre algorithme de hachage et la méthode d'authentification (bien évidemment d'autres informations importantes).

Commande
show crypto ipsec transform-set
Résultat
<pre>vpnAnnexe#show crypto ipsec transform-set Transform set 51: { ah-md5-hmac } will negotiate = { Tunnel, },</pre>
Explication
<ul style="list-style-type: none"> • Il permet aussi de vérifier notre algorithme de hachage (ah-sha-hmac) et la méthode d'authentification et le mode du protocole d'encapsulation AH (Tunnel).

Commande
show crypto map
Résultat
<pre>vpnPrincipale#show crypto map Crypto Map test 10 ipsec-isakmp Peer = 193.194.77.26 Extended IP access list 101 access-list 101 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 Current peer: 193.194.77.26 Security association lifetime: 4608000 kilobytes/900 seconds PFS (Y/N): N Transform sets={ 51, } Interfaces using crypto map test: Serial0/0/0</pre>
Explication
<ul style="list-style-type: none"> • Il permet aussi de vérifier d'autres informations importantes dont on a paramétrer et configurer dans le début.

Machine qui émettre paquet vers serveur
PC2
Commande
ping 172.16.2.254 tracert 172.16.2.254
Résultat

The screenshot shows a virtual PC2 desktop with a taskbar and a window titled 'Command Prompt'. The window displays the output of the following commands:

```

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 172.16.2.254

Pinging 172.16.2.254 with 32 bytes of data:

Reply from 172.16.2.254: bytes=32 time=58ms TTL=126
Reply from 172.16.2.254: bytes=32 time=13ms TTL=126
Reply from 172.16.2.254: bytes=32 time=15ms TTL=126
Reply from 172.16.2.254: bytes=32 time=56ms TTL=126

Ping statistics for 172.16.2.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 58ms, Average = 35ms

C:\>tracert 172.16.2.254

Tracing route to 172.16.2.254 over a maximum of 30 hops:

  0  3 ms    0 ms    0 ms    172.16.1.1
  1  *        *        *        Request timed out.
  2  12 ms   12 ms   46 ms   172.16.2.254

Trace complete.

C:\>

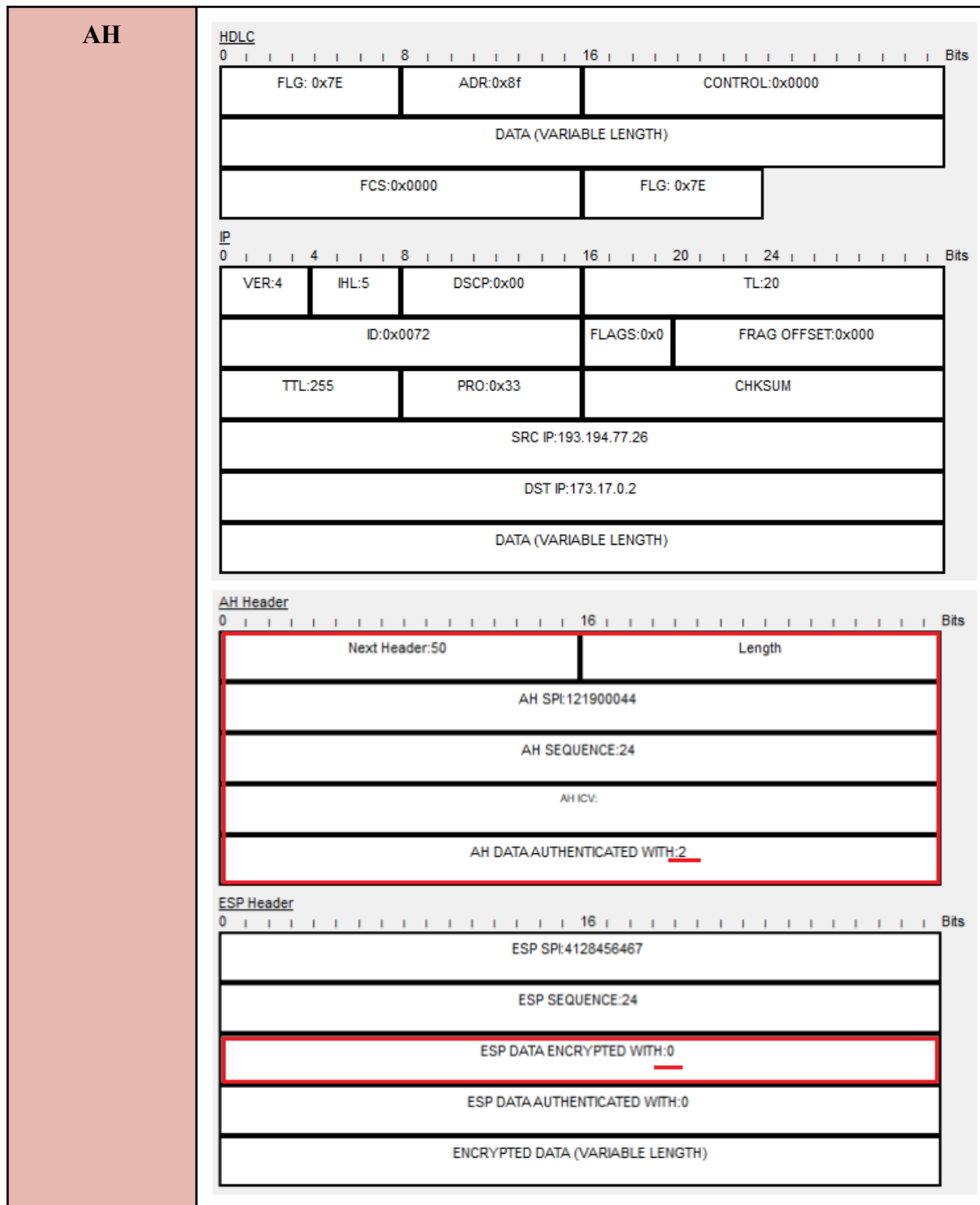
```

Explication
<ul style="list-style-type: none"> Le test de connectivité passé avec succès car c'est une connexion VPN site to site sans passer à l'application VPN pour s'inscrire. La commande ping valide que les paquets de test sont envoyés avec succès. La commande tracert permet de nous donner les deux adresses IP de l'émetteur et récepteur, il ya pas d'autres adress des routeurs en milieu car c'est ca le principe de VPN et tunnelisation (sécurité de suivre la trace).

3. La différence avec IPsec en utilisant ESP.

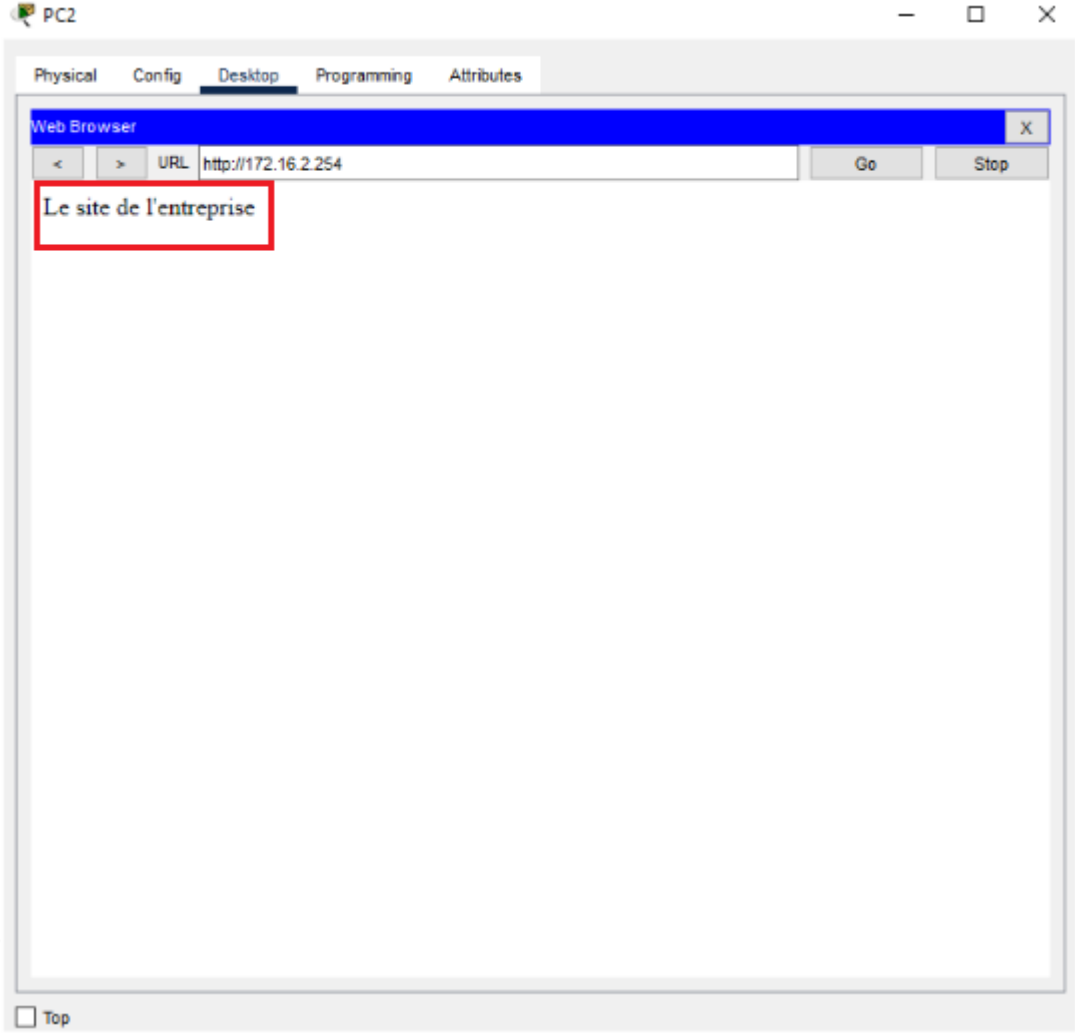
Encapsulation	Champs du Paquet
ESP	HDLC-IP-ESP HEADER
AH	HDLC-IP-AH HEADER-ESP HEADER

Encapsulation	Capture de simulation
ESP	<div><div>HDLC</div><div><div>0816</div><div>Bits</div></div><div><div>FLG: 0x7E</div><div>ADR: 0x8f</div><div>CONTROL: 0x0000</div></div><div>DATA (VARIABLE LENGTH)</div><div><div>FCS: 0x0000</div><div>FLG: 0x7E</div></div></div>
	<div><div>IP</div><div><div>048162024</div><div>Bits</div></div><div><div>VER: 4</div><div>IHL: 5</div><div>DSCP: 0x00</div><div>TL: 20</div></div><div><div>ID: 0x001c</div><div>FLAGS: 0x0</div><div>FRAG OFFSET: 0x000</div></div><div><div>TTL: 255</div><div>PRO: 0x32</div><div>CHKSUM</div></div><div>SRC IP: 193.194.77.26</div><div>DST IP: 173.17.0.2</div><div>DATA (VARIABLE LENGTH)</div></div>
	<div><div>ESP Header</div><div><div>016</div><div>Bits</div></div><div><div>ESP SPI: 1810965513</div></div><div><div>ESP SEQUENCE: 4</div></div><div><div>ESP DATA ENCRYPTED WITH: 6</div></div><div><div>ESP DATA AUTHENTICATED WITH: 1</div></div><div>ENCRYPTED DATA (VARIABLE LENGTH)</div></div>



Encapsulation	Explication
ESP	<ul style="list-style-type: none"> La taille de ESP header différent de 0, tout la partie données est crypté, et aussi il ya pas le champ AH header.
AH	<ul style="list-style-type: none"> La taille de ESP header est 0, rien n'a crypté (les données encryptées sont 0). Une entête AH header est ajoutée afin de remplacer les adresses IP dans ce mode tunnel.

4. Test de connexion entre un PC du site annexe au serveur Web de l'entreprise dans le site principal (utiliser l'URL : <http://172.16.2.254>).

Résultat

Explication
<p>La connexion au site de l'entreprise qui est hébergée dans le serveur du site principal (http://172.16.2.254) à partir d'une station du site annexe (PC2) est établie avec succès à travers le VPN site to site qui est configuré durant tout cette partie du TP.</p>