Réponses :

1. **Vérification de la création du tunnel et son fonctionnement.**

Commande
show crypto isakmp sa
Résultat
vpnAnnexe#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id slot status 173.17.0.2 193.194.77.26 QM_IDLE 1097 0 ACTIVE IPv6 Crypto ISAKMP SA
Explication
• **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
show crypto ipsec sa
Résultat
vpnAnnexe#show crypto ipsec sa interface: Serial0/0/0 Crypto map tag: TEST, local addr 193.194.77.26 protected vrf: (none) local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0) current_peer 173.17.0.2 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 0 #pkts decaps: 29, #pkts decrypt: 29, #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 1, #recv errors 0 local crypto endpt.: 193.194.77.26, remote crypto endpt.:173.17.0.2 path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0 current outbound spi: 0x0(0) inbound esp sas: vpnAnnexe#show crypto ipsec transform-set Transform set 50: { { esp-3des esp-sha-hmac } } will negotiate = { Tunnel, },
Explication
• **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 cryptage et l'algorithme de hachage et la méthode d'authentification (bien évidemment d'autres informations importantes).

Commande
show crypto ipsec transform-set
Résultat

```
vpnAnnexe#show crypto ipsec transform-set
Transform set 50: {    { esp-3des esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Explication

- **Il permet aussi de vérifier notre algorithme de cryptage et l'algorithme de hachage et la méthode d'authentification.**

Commande
show crypto map
Résultat

```
vpnAnnexe#show crypto map
Crypto Map test 10 ipsec-isakmp
        Peer = 173.17.0.2
        Extended IP access list 101
            access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
        Current peer: 173.17.0.2
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): N
        Transform sets={
                50,
        }
        Interfaces using crypto map test:

Crypto Map TEST 10 ipsec-isakmp
        Peer = 173.17.0.2
        Extended IP access list 101
            access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
        Current peer: 173.17.0.2
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): N
        Transform sets={
                50,
        }
        Interfaces using crypto map TEST:
                Serial0/0/0
```

Explication

- **Il permet aussi de vérifier d'autres informations importantes.**

Commande
ping 172.17.2.254 **tracert 172.17.2.254**

Résultat

```
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=10ms TTL=126
Reply from 172.16.2.254: bytes=32 time=12ms TTL=126
Reply from 172.16.2.254: bytes=32 time=13ms TTL=126
Reply from 172.16.2.254: bytes=32 time=12ms 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 = 10ms, Maximum = 13ms, Average = 11ms

C:\>tracert 172.16.2.254

Tracing route to 172.16.2.254 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.16.1.1
  2    *         *         *         Request timed out.
  3    12 ms     12 ms     11 ms     172.16.2.254

Trace complete.
```

Explication

- **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.**

2. **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).**