Exercice: VPN

Soit la capture wireshark suivante :

```
2A8F14E40D648E28
*Apr 29 16:57:40.944: IKEv2:(SESSION ID = 27621,SA ID = 1):Sending Packet [To 198.19.252.1:500/From 10.11.6.2:500/VRF 10:f0]
Initiator SPI : 2A8F14E40D648E28 - Responder SPI : 000000000000000 Message id: 0
IKEv2 IKE SA INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID NOTIFY(NAT DETECTION SOURCE IP) NOTIFY(NAT DETECTION DESTINATION IP) NOTIFY(IKEV2 FRAGMENTATION SUPPORTED) VID
*Apr 29 16:57:42.200: IPSEC:(SESSION ID = 27621) (key engine) request timer fired: count = 1,
 (identity) local= 10.11.6.2:0, remote= 198.19.252.1:0,
   local proxy= 0.0.0.0/0.0.0.0/256/0,
   remote_proxy= 0.0.0.0/0.0.0.0/256/0
*Apr 29 16:57:42.200: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.11.6.2:500, remote= 198.19.252.1:500,
    local_proxy= 0.0.0.0/0.0.0.0/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0,
    protocol= ESP, transform= esp-aes 256 esp-sha-hmac (Tunnel),
    lifedur= 28800s and 4294967295kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
omr2-site1#
                5638222923EA3C5A
*Apr 29 16:57:53.763: IKEv2:Received Packet [From 198.19.252.1:500/To 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 5638222923EA3C5A - Responder SPI : 000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N NOTIFY(NAT DETECTION SOURCE IP) NOTIFY(NAT DETECTION DESTINATION IP) NOTIFY(IKEV2 FRAGMENTATION SUPPORTED) NOTIFY(Unknown - 16431) NOTIFY(REDIRECT SUPPORTED)
```

- 1- Donner les protocoles VPN utilisés pour protéger la communication dans cette communication. (A identifier sur la figure)
- 2- Donner sur cette figure l'identifiant de la SA
- 3- Est-ce qu'il s'agit de la phase 1 ou la phase 2 ? Expliquer
- 4- Est-ce qu'il s'agit d'une création, modification ou suppression de SA? Expliquer.
- 5- Donner sur un tableau 3 différences entre SA (IKE) et SA (IPSec)

QCM (10 pts): Une ou plusieurs réponses peuvent être correctes

- 1- Le protocole AH est un protocole
 - a. De transfert de données
 - b. De sécurisation de données
 - c. De négociation de SA
 - d. De cryptage
- 2- La SA dans un tunnel VPN est
 - a. Un accord entre deux routeurs
 - b. Un accord entre les deux bouts du tunnel
 - c. Bidirectionnelle
 - d. Unidirectionnelle
- 3- Le protocole ESP garantie
 - a. La confidentialité
 - b. L'intégrité
 - c. La non répudiation

- d. L'authentification
- 4- La SA négociée entre deux routeurs est identifiée par a. le AD

 - b. le SPI
 - c. 1'adresse IP
 - d. 1'adresse MAC