Tutorial Week 6

Question 1

1. What are the three types of VPN and in what situations would each be used?
2. What protocol is used in association with IPSec for key management?
3. Why is automatic key management desirable?
4. What are the main components in tunnelling?
5. What is the difference between a compulsory and a voluntary tunnel?
6. In what situations is a voluntary tunnel likely to be used and in what situations is a compulsory tunnel likely to be used?
7. What is the purpose of the SPI field in an IPSec SA?
8. What is the difference between AH and ESP?

Question 2

The following questions are based on the following output:

```
R0#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.0.2     192.168.0.1     QM_IDLE           1032    0 ACTIVE

IPv6 Crypto ISAKMP SA


R0#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: vpnmap, local addr 192.168.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
   current_peer 192.168.0.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #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.: 192.168.0.1, remote crypto endpt.:192.168.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x43D3076E(1137903470)

     inbound esp sas:
      spi: 0x31F917AA(838408106)
        transform: esp-aes 128 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2000, flow_id: FPGA:1, crypto map: vpnmap
        sa timing: remaining key lifetime (k/sec): (4525504/3546)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x43D3076E(1137903470)
        transform: esp-aes 128 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: FPGA:1, crypto map: vpnmap
        sa timing: remaining key lifetime (k/sec): (4525504/3546)
```

```
            IV size: 16 bytes
            replay detection support: N
            Status: ACTIVE

         outbound ah sas:

         outbound pcp sas:

      R0#
```

1. What VPN protocols are being used?
2. Is this an intranet or remote access VPN?
3. At what IP address are the two endpoints of the VPN?
4. At what interfaces are the two endpoints of the VPN?
5. What IPSec transform sets are being used?
6. Is traffic that passes through the VPN encrypted or passed as plaintext?
7. Is IPSec operating in tunnel or transport mode?
8. What symmetric key algorithm is used? What is the key length?
9. How many packets have been sent? How many received?
10. Why are there ISAKMP and IPSec SAs?
11. How many IPSec SAs?

Question 3

1. VoIP traffic is transmitted as a number of voice samples with an RTP, UDP and IP header. If the payload consists of 160 samples, each one byte in length, what is the protocol efficiency?

   (Useful additional information is that the RTP header is 12 bytes in length, UDP header is 8 bytes and the IP header is 20 bytes.)
2. What is the protocol efficiency in the following situations where the same VoIP stream is transmitted over a VPN. (Use AH header length of 256 bits. Use ESP header length of 32 bits, ESP trailer of 32 bits long and ESP authentication of 160 bits)
   a. IPSec AH transport mode
   b. IPSec AH tunnel mode
   c. IPSec ESP transport mode with authentication
   d. IPSec ESP tunnel mode with authentication
3. If 8000 samples per second are generated by the voice codec, what bit rate is needed per voice stream in each of the above examples?