Tutorial Solution Week 6

Question 1

1. What are the three types of VPN and in what situations would each be used?

   Remote access: Single user located at diverse locations.

   Intranet: Remote office.

   Extranet: External business entities in partnership. Many possibilities as to how used

2. What protocol is used in association with IPSec for key management?

   Internet Key Exchange

3. Why is automatic key management desirable?

   Many keys needed in VPNs. Keys need frequent change. Manual installation only feasible in small networks

4. What are the main components in tunnelling?

   Target network, Initiator node, Home Agent, Foreign Agent

5. What is the difference between a compulsory and a voluntary tunnel?

   Voluntary tunnels: end to end, created at the request of one of the end-points and used exclusively by a single communication

   Compulsory tunnels: created and configured by an intermediate node (eg a router) usually shared by multiple communications.

6. In what situations is a voluntary tunnel likely to be used and in what situations is a compulsory tunnel likely to be used?

   Voluntary tunnels will be used when communicating end-to-end. Most likely used in a remote access VPN.

   Compulsory tunnels will be used when the VPN is terminated at intermediate devices such as firewalls or routers. Most likely used in an Intranet VPN.

7. What is the purpose of the SPI field in an IPSec SA?

   It provides an index into the Security Association Database (SAD)

8. What is the difference between AH and ESP?

   AH is authentication only.

   ESP is both authentication and encryption.

   AH protects the complete encapsulated packet, while ESP protects only the payload.

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?

   IPSec, ISAKMP, ESP

2. Is this an intranet or remote access VPN?

   intranet

3. At what IP address are the two endpoints of the VPN?

   192.168.0.1 and 192.168.0.2

4. At what interfaces are the two endpoints of the VPN?

   S0/0/0 on both routers

5. What IPSec transform sets are being used?

   esp-aes, esp-sha-hmac

6. Is traffic that passes through the VPN encrypted or passed as plaintext?

   Encrypted using AES

7. Is IPSec operating in tunnel or transport mode?

   tunnel

8. What symmetric key algorithm is used? What is the key length?

AES with 128 bit key

9. How many packets have been sent? How many received?

   3 and 2

10. Why are there ISAKMP and IPSec SAs?

    ISAKMP is used to set up the IPSec tunnels.

11. How many IPSec SAs?

    2

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.)

   IP header / UDP / RTP / Payload

   20 bytes 20 160

   Efficiency is 160 / (20 +20 + 160) = 80%

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

      IP / AH / UDP / RTP / Payload

      20 32 20 160

      Efficiency is 160 / (20 +32 + 20 + 160) = 69 %

   b. IPSec AH tunnel mode

      IP / AH / IP / UDP / RTP / Payload

      20 32 20 20 160

      Efficiency is 160 / (20 +32 + 20 + 20 + 160) = 63 %

   c. IPSec ESP transport mode with authentication

      IP / ESPHead / UDP / RTP / Payload / ESPTrail / ESPAuthent

      20 4 20 160 4 20

      Efficiency is 70%

   d. IPSec ESP tunnel mode with authentication

      IP / ESPHead / IP / UDP / RTP / Payload / ESPTrail / ESPAuthent

      20 4 20 20 160 4 20

      Efficiency 65%

Tutorial Solution Week 6

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?

   Simplest approach is to calculate how many packets needed per second. 8000 samples per second so need 8000 / 160 = 50 packets per second. So

   No VPN 50 * (20 + 20 + 160) * 8 = 80,000 bps

   a. 50 * (20 +32 + 20 + 160) * 8 = 92,800 bps

   b. 50 * (20 +32 + 20 + 20 + 160) * 8 = 100,800 bps

   c. 50 * (20 + 4 + 20 + 160 + 4 + 20) * 8 = 91,200 bps

   d. 50 * (20 + 4 + 20 + 20 + 160 + 4 + 20) * 8 = 99,200 bps

   Alternative approach is to divide by efficiency. (Will be slight difference because of rounding of efficiency.) 8000 samples per second is 64000 bps. Divide by efficiency and multiply by 8 to convert from bytes to bits.

   No VPN 64000 / 0.8 = 80 kbps

   a. 64000 / 0.69 = 92, 754 bps

   b. 64000 / 0.63 = 101,508 bps

   c. 64000 / 0.70 = 91,429 bps

   d. 64000 / 0.65 = 98,462 bps