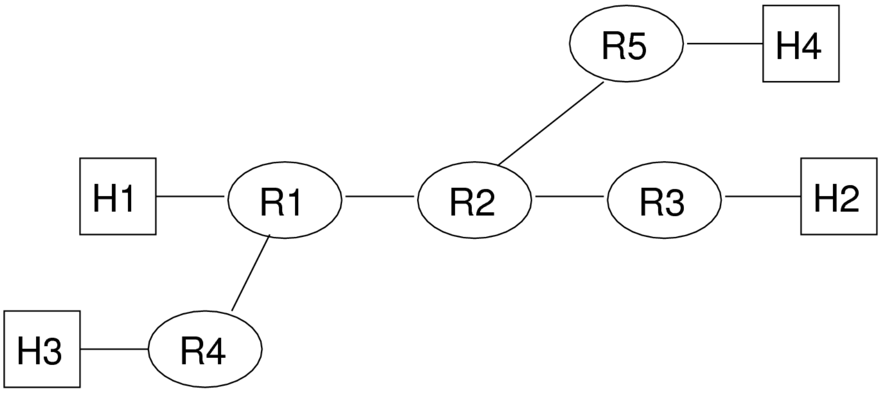
CSS322 – Quiz 7 Answers

Name: ____

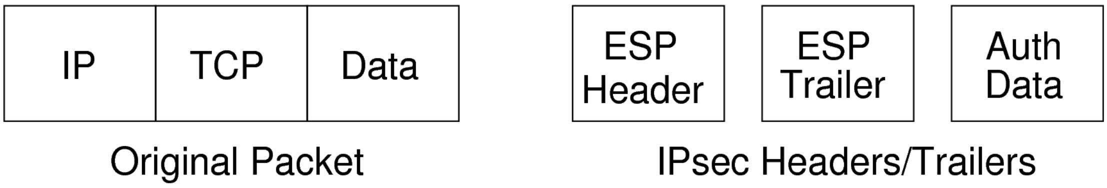
ID: ______________________________ Mark: __________ (out of 6)

Question 1 [6 marks]

Consider the IP network shown below.



A source host has an original IP packet, shown below, to send to a destination host. The figure below also shows the set of IPsec headers/trailers that are available when using Encapsularing Security Payload (ESP) with both confidentiality and authentication.

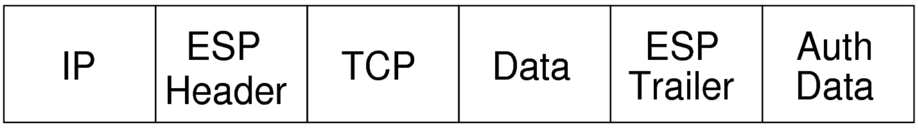


In your answers you can use the host and router names as the IP addresses. For example, the IP addres of host H1 is: H1.

Host H1/H3 has the original IP packet to send to H2/H4.

a) If ESP transport mode is used, draw the IP packet sent by R2. [2 marks]

Answer



b) List the parts of the above packet that are:

i. Encrypted [1 mark]

Answer

TCP, Data and ESP trailer

ii. Authenticated [1 mark]

Answer

ESP header, TCP, Data, ESP trailer

c) If, instead of transport mode, ESP tunnelling mode was used from R1 to R3/R5, for the packet sent by R2/R5 what would the source IP address be in the outer IP header? [1 mark]

Answer

Tunnel R1 to R3 and packet sent by R2: source IP address is R1

Tunnel R1 to R5 and packet sent by R5: source IP address is H1

d) Host H1/H3 has the original IP packet to send to H2/H4. If ESP tunnelling mode is used from R1 to R3/R5, draw the IP packet sent by R2. [3 marks]

Answer

IP	ESP Header	IP	TCP	Data	ESP Trailer	Auth Data

e) List the parts of the above packet that are encrypted. [1 mark]

Answer

IP (inner), TCP, Data, ESP Trailer

f) What is the source/destination IP address in the inner/outer header of the above packet? [1 mark]

Answer

Inner source IP address from R1 to R3: H1

Outer destination IP address from R1 to R5: R5

g) What is an advantage of tunnelling mode (instead of transport mode) in ESP? [1 mark]

Answer

Installation, configuration and management of IPsec can be performed on routers and be applied for all hosts in a network.

The original source and final destination IP addresses are encrypted; not viewable by intermediate nodes.