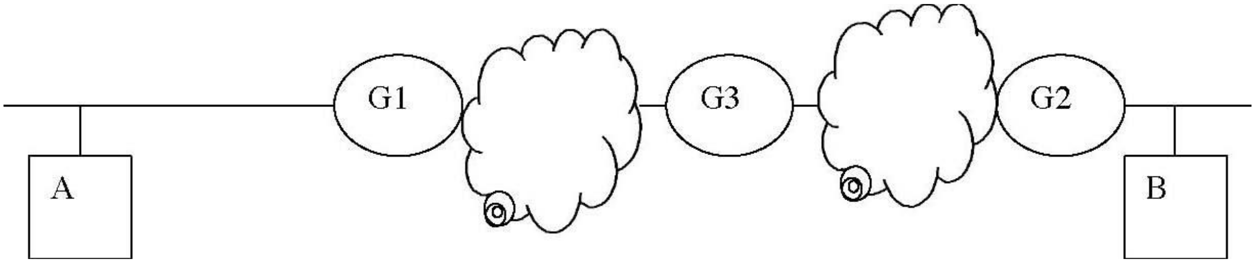
DALHOUSIE UNIVERSITY

Network Security (CSCI-6708)

Assignment - 9

Shivam Gupta
B00810723

Question 1.



a) ESP transport mode only from end to end

Original Diagram:

A,B	Payload

ESP Transport

A,B	ESP Header	Payload	ESP Trailer

<---------------Authenticated-->

<-----Encrypted----------->

b) AH transport from A to B, ESP tunnel from firewall G1 to firewall G3.

Original Diagram:

A,B	Payload

AH transport from A to B:

A,B	AH	Payload

<---------------Authenticated-->

ESP tunnel from G1 to G2:

G1,G2	ESP Header	A.B	AH	Payload	ESP Trailer

<----------------Authenticated--->

<----------------------Encrypted----------------------->

c) AH tunnel from A to B, ESP transport from firewall G1 to firewall G2.

Original Diagram:

A,B	Payload

AH tunnel from A to B:

A,B	AH	A,B	Payload

<---Authenticated-->

ESP transport from G1 to G2:

A,B	ESP Header	AH	Payload	ESP Trailer

<----------------Authenticated--->

<-----Encrypted--------------------------->

d) ESP tunnel from G3 to G2, and AH tunnel from G2 to B.

ESP tunnel from G3 to G2:

G3,G2	ESP Header	A.B	Payload	ESP Trailer

<----------------Authenticated--->

<-------------------Encrypted----------->

AH tunnel from G2 to B:

AH tunnel from G2 to B:

G2,B	AH	A,B	Payload

<---Authenticated-->

Question 2.

a) IKE can counter brute force attacks, as the keys are refreshed in phase 2, so searching for key space wont help to compromise the security.
b) Encrypted packets are protected by digital signatures, and they do another Diffie Hellman exchange, so replay attack won't make any sense and cant compromise the security.
c) Without knowing about the Diffie Hellman exchange and SKEYID, man in the middle cant do anything.
d) Even with having spoofed IP, the attacker will receive encrypted keys, SKEYID and DH secret with a random number. If tried more, it will reveal the true IP of attacker.
e) In TCP SYN Attacks, creation of local state must be avoided. In IKE, when the ACK message is received the value is validated and, in this attack, the ACK value of value+1 will not be validated and local state will not be built.