Question 17.5:

When sending encrypted traffic from firewall to firewall, IPsec is utilized in tunnel mode (Original IP datagrams are encapsulated inside new IP packets and prefixed with IPsec header). Since packets are encrypted, the data has to be forwarded to a node that can do the decryption. Furthermore that server has to have some information about where that package comes from so that it can use the corresponding key for the decryption. These nodes are the F1 and F2. We cannot just change the already existing header, cause we would lose the actual destination of the packet.

If we just encrypted the packets without changing the source-destination addresses, packets would not be able to be decrypted properly. Each packet would be transferred to its final destination that would be incapable of decrypting the packet -since it does not share a common key with F1. In addition, in such a scenario there would be less protection against traffic analysis (at least now an eavesdropper sees F1 talking to F2 and not A talking to B). Having a packet with only encrypted payload traversing the Internet we won't be able to provide protection against all active types of attacks such as IP address spoofing, data reading and data injection could also benefit from that.

Question 17.6:

Advantages:
- less computing power(less encryption=>faster packet processing at the firewalls)
- smaller size(smaller overhead)=>less traffic volume.

Disadvantages:
- no protection against traffic analysis - identities of communicating parties revealed
- F2 can no longer to filtering based on trust of the firewall F1 because there is no longer encryption that only F1 can do.

Question 17.7

1. given to A's IPsec layer:
IP header | data

The IPheader contains: src = A, dst = B, protocol = TCP

2. transmitted by A:

IP header1 | data

The IPheader1 contains: src = A, dst = B, protocol = ESP/AH

3. transmitted by F1 :
IP header2 | IP header1 | data

The IPheader2 contains: src = F1, dst = F2 , proto = ESP/AH
The IPheader1 contains: src = A, dst = B, protocol = ESP/AH

4. received by B
IP header | data

The IPheader contains: src = A, dst = B, protocol = ESP