

QUIZ

Lecture 1

Question 1.1

- Which are the applications for both modes of IPSec: the transport mode and the tunnel mode?

Question 1.2

- Can the contents of protected packets be read when the Authentication Header (AH) protocol is used in transport mode?
- What if the Encapsulating Security Payload (ESP) protocol is used?

Question 1.3

- IPSec provides *limited traffic flow confidentiality*. How can this be achieved?
Bonus: Why is it limited?

Question 1.4

- Security controls are safeguards/ countermeasures for avoiding, counteract, or minimize security threats.
- Which are the three security controls provided by IPSec? (**Hint:** security controls can be *preventive, detective, and/or corrective*)

Question 2.1

- In IPSec tunnels denote security associations between two nodes. A pair of nodes can have several security associations at once. It is even possible to construct tunnels within tunnels - this is called “*iterated tunneling*”.
- Can you give an example of a configuration that requires this *iterated tunneling* setup?

Question 3.1

- What is the difference between SSL Connections and SSL Sessions?

Question 3.2

- What is the purpose of the SSL record protocol and what are the steps involved into this protocol?