**DV300\_28\_SAS on video related to Security Protocols**

**Q1. IPsec is a set of protocols for security at the network layer of\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

A1. OSI Model

**Q1.1 IPsec \_\_\_\_\_\_\_\_\_\_\_\_ the data when communication is happening between two computers**

A1.1. Encrypts

**Q2. In order to use IPsec both sender and receiver must share a public key. (True/False)**

A2. True

**Q3. In addition to encryption IPsec also\_\_\_\_\_\_\_\_\_\_\_\_\_ the data will ensure the data is received exactly that which was sent.**

A3. Verifies

**Q4. What are IPsec modes?**

A4. a. Transport Mode

b. Tunnel Mode

**Q5. Transport mode only the \_\_\_\_\_\_\_\_\_\_\_\_of the data packet is encrypted.**

A5. Message Portion

**Q6. In Tunnel mode the entire data packet is encrypted. (True/False)**

A6. True

**Q7. Layer 2 tunnelling protocol is a combination of Cisco’s layer 2 \_\_\_\_\_\_\_\_\_\_\_\_\_and point to point tunnelling protocol.**

A7. Forwarding

**Q8. L2TP protocol authenticates in few ways using digital certificates, it authenticates both the computer and user (True/False)**

A8. True

**Q9. SSL stands for \_\_\_\_\_\_\_\_\_**

A9. Secure Socket Layer

**Q10. If you were to go to E-commerce websites you would notice that \_\_\_\_\_\_\_\_\_\_\_\_ is added to the HTTP which indicates that you were now using a SSL in your web browser.**

A10. s

**Q11. Which ways protection does SSL provides?**

A11. a. It authenticates the server.

b. Authenticates the client

c. Encrypts the data

**Q12. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is the latest industry standard SSL protocol, it’s the successor to SSL. And it’s based on the same specifications.**

A12. TLS

**Q13. SSL also authenticates the server, client, and \_\_\_\_\_\_\_\_\_\_\_\_the data.**

A13. Encrypts

**Q14. TLS is made up of two layers: the first layer is \_\_\_\_\_\_\_\_\_\_\_\_\_protocol which provides connection security by making sure that the connection is private and reliable.**

A14. TLS Record

**Q15. A4 second layer is a TLS Handshake Protocol which allows a server and client to authenticate each other and negotiable an encryption algorithm and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_key before data is sent**

A15. Cryptographic Key

**Q16. What is the goal of TLS?**

A16. The goal for TLS is to make SSL safer and more secure.

**Q17. \_\_\_\_\_\_\_\_\_\_standard protocol is used for both wired and wireless networks.**

A17. 802.1x

**Q18. 802.1x controls access by ports. It authentication passes the port based opened. And if the authentications fail the port is closed. (True/False)**

A18. True