

FIT1047
SUPPLEMENTARY WORKSHEET -02
WEEK 11

1. Why HTTP is termed as a stateless protocol.

The server does not know that if the same person requests from the server again
It is an independent transaction.

2. Explain SSL/TLS protocol.

TLS establishes a shared key to exchange messages that provide confidentiality and integrity or authenticity.
It consists of three protocols:

1. TLS Handshake: to authenticate server and client, which will then result in a shared key and a session ID.
2. TLS Record: after the exchange of ChangeCipherSpec messages, all data is encrypted.
3. TLS Alert: immediately closes a session when it is done

3. What is a VPN?

An encrypted channel which logically connects a client to a network.
It secures the channel at the tunnel endpoints only (client and gateway).

4. What is the difference between interior and exterior routing protocols?

Interior routing routes packets between devices within an autonomous system. Exterior routing routes packets from one autonomous system to another via the Border Gateway Protocol (BGP).

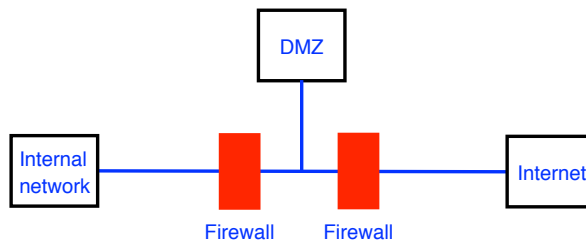
5. Certificates are used to identify servers when using TLS. Give one reason, why certificates can be problematic.

Some certificates have been revoked.

FIT1047
SUPPLEMENTARY WORKSHEET -02
WEEK 11

6. Explain the term “demilitarised zone” and provide two examples of firewall placements for such a zone.

Demilitarised zone is a zone placed between an internal network and the internet, which is considered to be less secured than the internal network but still protected from direct access. One of the firewalls can be placed at the internal network and another firewall could be placed at the internet. In other words, we could see that the DMZ is “in between” the two firewall placements.



7. Compare public Message Authentication Codes and Hash Functions showing their similarity and differences.

8. What is a currently recommended hash function for use in digital signatures and which hash function is still used, but no longer recommended.

SHA-1