(1) What are static packet filtering firewalls?

Static packet filtering firewalls are the firewalls that make filtering decisions (either a packet is forwarded or dropped) using the information in the packet headers based on the (manually) pre-defined filtering rules in a filtering-rule table.

(2) What are state-full packet inspection firewalls?

State-full packet inspection firewalls are the firewalls that make filtering decisions using not only the information in the packet headers but also “status” associated to each packet. For example, any TCP packet (except for those carrying TCP SYN, SYN-ACK, and ACK messages) should belong to an established TCP connection since TCP is a connection-oriented transport-layer protocol.

When a TCP connection is established by completing the process of the TCP three-way handshaking, a state-full firewall registers (remembers) the sender and the receiver of that TCP connection, until the TCP connection is explicitly dropped by “TCP FIN” message. Thus, any TCP packet should belong to an established TCP connection. Any TCP packet that does not belong to any established TCP connection is not innocent (a state-full packet inspection firewall drops such TCP packets).

(3) Explain the primary disadvantage of deep-packet inspection firewalls (over packet filtering firewalls)?

Deep packet inspection (DPI) firewalls perform many high-level investigations, especially by investigating the payload field in each packet. Therefore:

- Throughput is low (handling each packet takes much longer, compared to static packet filtering firewalls. This could cause a performance bottleneck especially to a busy network domain (or busy host computers).
- High delay also means that DPI firewalls can be a target of DoS attacks.
(4) Which of the following type (types) of firewall(s) is (are) effective for preventing OS-command injections?

(a) static packet filtering firewalls
(b) dynamic packet filtering firewalls
(c) state-full packet inspection firewalls
(d) deep-packet-inspection firewalls

**Answer key:** (d)

DPI firewalls should be used to detect and prevent preventing OS-command injections. Since malicious OS commands appear in the payload field of packets, DPI firewalls are the best match.

**Note:** OS commands are not “status”. They are one-shot activities (thus, state-full packet inspection firewalls are irrelevant).

(5) What are the primary advantages (give two examples) of gateway firewalls?

(a) Gateway firewalls are more “fail-safe” than packet-filtering firewalls. It is because, gateway firewalls are “closed” by default. The firewalls open its gate only if the safety is conformed (i.e., if filtering engines are not properly functioning by some reasons, any packet will not get through a firewall), while packet firewalls are “open” by default (i.e., if filtering engines are not properly functioning by some reasons, some packets that should not get through may get through a firewall).

(b) External host computers will never directly communicate with the host computers in side of a gateway firewalls. This prevents DoS attacks as well as many reconnaissance activities performed by attackers for their first step.