#1: Transport gateway firewalls

(a) Firewalls that investigate payload for each specific network applications, such as HTTP, FTP, SMTP, POP, and etc.

(b) Firewalls that work as proxy. Instead of investigating packets “on the fly”, these firewalls establish new connections to destination hosts only after the firewalls confirm the safety of the packets using the contents in network applications.

(c) Firewalls that work as proxy. Instead of investigating packets “on the fly”, these firewalls establish new connections to destination hosts only after the firewalls confirm the safety of the packets using the contents mainly in TCP/UDP headers.

(d) Firewalls that mainly investigate the contents in IP header of both incoming and outgoing packets.

Solution: (c)

#2: OP25B

(a) OP25B is a technique (or configuration or firewall) that prohibits any outgoing network traffic originated from TCP port #25 of a mail server in a local network domain (“local network domain” means the network domain your host computer belongs to).

(b) OP25B is a technique (or configuration or firewall) that prohibits any incoming network traffic from TCP port #25 of host computers in remote network domains (“remote network domains” means any network domain your host computer does NOT belong to).

(c) OP25B is a technique (or configuration or firewall) that prohibits a mail server to receive (accept) any incoming network traffic to its TCP port #25 from any host computers within the same network domain (i.e., “local network domain”).

(d) OP25B is a technique (or configuration or firewall) that prohibits any outgoing network traffic to TCP port #25 of host computers in remote network domains (“remote network domains” means any network domain your host computer does NOT belong to).
Solution: (d)

#3: WAF

(a) Firewall that investigate contents (payload) specific to web applications.
(b) Firewalls that perform TLS encryption/decryption using specially designed hardware to reduce the processor workload of web servers.
(c) Special firewalls that are designed to protect server hosts placed in DMZ.
(d) Firewall that allows only web-related network traffic.

Solution: (a)

#4: DMZ

(a) DMZ is a specific place in a network domain where network servers that do not require high-volume network traffic should be placed.
(b) DMZ is a specific place in a network domain that (“the specific place”) can be reached without going through firewalls that take high workload to investigate each network traffic.
(c) DMZ is a specific place in a network domain that (“the specific place”) is not under the control of any network security administrators in each network domain.
(d) DMZ is a specific place in a network domain where prototypes of new security solutions, such as honeynets should be tested.

Solution: (b)
#5: NAPT (Network Address Port Translations)

(a) NAPT lets security administrators (in each network domain) prevent attackers (from the public internet domain) from reaching vulnerabilities in web servers open to public accesses.

(b) NAPT lets security administrators (in each network domain) detect intrusions by attackers from the public internet domain.

(c) NAPT lets security administrators (in each network domain) protect web servers in their domain detect TCP connections for specific web applications.

(d) NAPT lets security administrators (in each network domain) protect local host computers (host computers in the network domain security administrators need to protect) from attacking network traffic from outside of the domain.

**Solution:** (d)