Packet filtering firewall –

Circuit-level proxy –

Application level gateway-

Unified threat management device-

Content filter- prevents access based on websites rating and classification

Proxy server- when the number of clients exceeds the amount it can handle

Reverse Proxy Server- handles the client request

SSH- protocol TCP/IP port **22**

**161**- SNMP

**UDP 67**- BOOTP/DHCP

**443**- SSL on port 433 needs to be enabled

Port **80 and 443**- easy to hack a web page through these ports

**53-** DNS service

**21**- FTP

Downloading a file- NETSTAT command using TCP/IP **21**

Open port **25** to allow SMTP service- Unable to send email after blocking a port

HTTP port should be changed to **80**- unable to access a web page

Network traffic- The workstations is using NETBIOS to access shared resource on the server

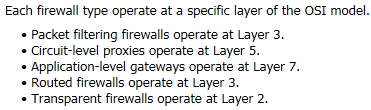
Someone is using voice over IP to make a telephone call

Host-based firewall- to protect your laptop from internet-based attack

Just installed a packet filtering firewall- port number, source address of a packet, destination address of a packet.

Application-level – the firewall

The UTM represents a signal point of failure- the weakest exist in this implementation



FTP- files transfer protocol

ACL- acting as a firewall use to control which packets are forwarded or dropped

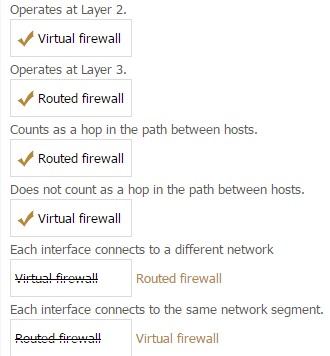
Use firewalls to create a DMZ, place the webserver inside the DMZ. The private network behind the DMZ.

Packet filtering firewall on your network- destination address of a packet, source address of a packet, and port number.

To improve network security- access list filters traffic based on the IP header information such as source or destination IP address.

Best way to protect the server- put the web server inside the DMZ, put the database server on the private network.

Designing a firewall- close all ports; open only ports required by applications inside the DMZ



No traffic is allowed through the WAN interface- add a permit statement to the bottom of the access list.

DMZ- firewall implementation creates a buffer network that can be used to host email or web servers.

Firewalls- count as a router hop, and support multiple interfaces.

