Network Admin

Firewall	A firewall is used to provide security to the private networks connected to the internet. They can be implemented as hardware or software, or a combination of both. All incoming and outgoing network traffic are examined and accepted/rejected by the firewall as per defined rules. Firewall is available either in software or in hardware form. For a single PC you may need a software firewall while a large corporate implements hardware firewall to protect all of their systems from such attacks.
Difference between network gateway and a firewall	A network gateway joins two networks together and a network firewall protects a computer network against unauthorized incoming or outgoing access. Network firewalls may be hardware devices or software programs.
Difference between IPS and a firewall	The primary function of a firewall is to prevent/control traffic flow from an untrusted network (outside). A firewall is not able to detect an attack in which the data is deviating from its regular pattern, whereas an IPS can detect and reset that connection as it has inbuilt anomaly detection.
Transparent firewall	A transparent firewall is considered as Layer 2. Deploying a new firewall into a network can be a complicated process due to various issues (e.g. IP address reconfiguration, network topology changes, current firewall etc.) because the firewall is not a routed hop and you can easily introduce a transparent firewall into an existing network.
Stateful failover	Every time a session is created for a flow of traffic on the primary node, it is synced to the secondary node. When the primary node fails, sessions continue to pass traffic through the secondary node without having to re-establish.
Firewalls work at what layer? Define firewall generations and their roles.	Firewalls work at layer 3, 4 & 7. First generation firewalls provide packet filtering and they generally operate at layer 3 (Network Layer). Second generation firewalls operate up to the Transport layer (layer 4) and records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. Second generation firewall is mainly used for Stateful Inspection. Third generation firewalls operate at layer 7. The key benefit of application layer filtering is that it can “understand” certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)).
Packet filtering	Packet filtering is the process of permitting or blocking ip packets based on source and destination addresses, ports, or protocols. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing or allow. Packet filtering is also part of a firewall program for protecting a local network from unwanted access.

Hub Vs Switch	***Hub: -*** Layer 1 device Half duplex (Transmission Mode) Collision occurs commonly ***Switch: -*** Layer 2 device Half/Full duplex (Transmission Mode) No collision occurs in full duplex switch
What is VLAN?	VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate. ***VLAN provides following advantages: -*** Solve broadcast problem Reduce the size of broadcast domains Allow us to add additional layer of security **VLAN Connections** Switch supports two types of VLAN connection 1. ***Access link*** Access link connection is the connection where switch port is connected with a device that has a standardized Ethernet NIC. 2. ***Trunk link*** Trunk link connection is the connection where switch port is connected with a device that is capable to understand multiple VLANs.
IP Spoofing	An IP spoofing attack enables an attacker to replace its identity as trusted for attacking host. For example, if an attacker convinces a host that he is a trusted client, he might gain privileged access to a host.
What are the security-levels in cisco ASA?	ASA uses security levels to determine the parameters of trust given to a network attached to the respective interface. The security level can be configured between 0 to 100 where higher number are more trusted than lower. By default, the ASA allows packets from a higher (trusted) security interface to a lower (untrusted) security interface without the need for an ACL explicitly allowing the packets.

What is AAA?	AAA stands for authentication, authorization and accounting, used to control user's rights to access network resources and to keep track of the activity of users over a network. The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS).
What is IPS? How does it work?	An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. An Intrusion Prevention System can play a good role to protect against various network security attacks such as brute force attacks, Denial of Service (DoS) attacks, and vulnerability detection. Moreover, an IPS also ensures prevention against protocol exploits. Intrusion Prevention System uses four types of approaches to secure the network from intrusions which include: • Signature-Based • Anomaly-Based • Policy-Based • Protocol-Analysis-Based

OSI (OSI is a standard reference model for how messages should be transmitted between any two points in a network.)

Layer	Description	Examples
7. Application	Provides interface for users to communicate with applications.Responsible for initiating or services the request.	SMTP, DNS, HTTP, and Telnet etc
6. Presentation	The Presentation layer controls theformatting and syntax of user data for the application layer. This ensures that data from the sending application can be understood by the receiving application.	JPEG,MP3,MPEG etc
5. Session	Responsible for establishing, managing, and terminating the session. If a session is broken, this layer can attempt to recover the session.	NetBIOS
4. Transport	Breaks information into segments and is responsible for connection and connectionless communication.	TCP and UDP
3. Network	Responsible for logical addressing and routing.Packets are formed in network layer	IP, ICMP, and routers
2. Data Link	Responsible for physical addressing, error correction, and preparing the information for the media.Frames present here.Consist of two sublayers LLC and MAC	MAC address, CSMA/CD, switches, and bridges
1. Physical	Deals with the electrical signal.	Cables, connectors, hubs, and repeaters

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium.

The following 3 layers of OSI are referred to as network support layers:
a. Physical Layer
b. Data link Layer
c. Network Layers

Which layers of OSI are referred to as user support layers?
The block of user support layers consists of:
a. Session Layer
b. Presentation Layer and
c. Application Layer