Unit – 2

**Q.1. What are the various uses of IDPS technologies?**

**Ans:**

* IDPSs are primarily focused on identifying possible incidents. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting a vulnerability in the system.
* The IDPS could then report the incident to security administrators, who could quickly initiate incident response actions to minimize the damage caused by the incident.
* The IDPS could also log information that could be used by the incident handlers. Many IDPSs can also be configured to recognize violations of security policies.
* For example, some IDPSs can be configured with firewall rule set-like settings, allowing them to identify network traffic that violates the organization’s security or acceptable use policies.
* Also, some IDPSs can monitor file transfers and identify ones that might be suspicious, such as copying a large database onto a user’s laptop.
* Many IDPSs can also identify reconnaissance activity, which may indicate that an attack is imminent.
* For example, some attack tools and forms of malware, particularly worms, perform reconnaissance activities such as host and port scans to identify targets for subsequent attacks.
* An IDPS might be able to block reconnaissance and notify security administrators, who can take actions if needed to alter other security controls to prevent related incidents.
* Because reconnaissance activity is so frequent on the Internet, reconnaissance detection is often performed primarily on protected internal networks.

Other uses for IDPSs includes the following:

**Identifying security policy problems:**

* An IDPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rule sets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.

**Documenting the existing threat to an organization:**

* IDPSs log information about the threats that they detect. Understanding the frequency and characteristics of attacks against an organization’s computing resources is helpful in identifying the appropriate security measures for protecting the resources. The information can also be used to educate management about the threats that the organization faces.

**Deterring individuals from violating security policies:**

* If individuals are aware that their actions are being monitored by IDPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection

|  |
| --- |
| **Q.2. What are the various functions of IDPS technologies?**  **Ans:**   * There are many types of IDPS technologies, which are differentiated primarily by the types of events that they can recognize and the methodologies that they use to identify incidents. * In addition to monitoring and analyzing events to identify undesirable activity, all types of IDPS technologies typically perform the following functions:   **Recording information related to observed events:**   * Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.   **Notifying security administrators of important observed events:**   * This notification, known as an *alert*, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. * A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.   **Producing reports:**   * Reports summarize the monitored events or provide details on particular events of interest. |

* IPS technologies are differentiated from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding.
* They use several response techniques, which can be divided into the following groups:

**The IPS stops the attack itself:**

Examples of how this could be done are as follows:

* Terminate the network connection or user session that is being used for the attack
* Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute
* Block all access to the targeted host, service, application, or other resource.

**The IPS changes the security environment:**

* The IPS could change the configuration of other security controls to disrupt an attack.
* Common examples are reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks.
* Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.

**The IPS changes the attack’s content:**

* Some IPS technologies can remove or replace malicious portions of an attack to make it benign.
* A simple example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.
* A more complex example is an IPS that acts as a proxy and *normalizes* incoming requests, which means that the proxy repackages the payloads of the requests, discarding header information.
* This might cause certain attacks to be discarded as part of the normalization process.

**Q.3. What are the common detection methodologies of IDPS?**

**Ans:**

IDPS technologies use many methodologies to detect incidents. Most IDPS technologies use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection.

**1.Signature-Based Detection:**

A *signature* is a pattern that corresponds to a known threat. *Signature-based detection* is the process of comparing signatures against observed events to identify possible incidents.

Examples of signatures are as follows:

* A telnet attempt with a username of “root”, which is a violation of an organization’s security policy
* An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware
* An operating system log entry with a status code value of 645, which indicates that the host’s auditing has been disabled.

Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats.

**2.Anomaly-Based Detection:**

* *Anomaly-based detection* is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
* An IDPS using anomaly-based detection has *profiles* that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time.
* For example, a profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours.
* The IDPS then uses statistical methods to compare the characteristics of current activity to thresholds related to the profile, such as detecting when Web activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly.
* Profiles can be developed for many behavioral attributes, such as the number of e-mails sent by a user, the number of failed login attempts for a host, and the level of processor usage for a host in a given period of time.

**3.Stateful Protocol Analysis:**

* *Stateful protocol analysis* is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.
* Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.
* The “stateful” in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state.
* For example, when a user starts a File Transfer Protocol (FTP) session, the session is initially in the unauthenticated state.
* Unauthenticated users should only perform a few commands in this state, such as viewing help information or providing usernames and passwords.
* An important part of understanding state is pairing requests with responses, so when an FTP authentication attempt occurs, the IDPS can determine if it was successful by finding the status code in the corresponding response.
* Once the user has authenticated successfully, the session is in the authenticated state, and users are expected to perform any of several dozen commands.
* Performing most of these commands while in the unauthenticated state would be considered suspicious, but in the authenticated state performing most of them is considered benign.

**Q.4. What are the various types of IDPS technologies?**

**Ans:**

There are many types of IDPS technologies. they are divided into the following four groups based on the type of events that they monitor and the ways in which they are deployed:

**1.Network-Based:**

* **Network-Based**, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
* It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

**2.Wireless:**

* **Wireless**, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves.
* It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring.
* It is most commonly deployed within range of an organization’s wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring.

**3.Network Behavior Analysis (NBA):**

* **Network Behavior Analysis (NBA)**, which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems).
* NBA systems are most often deployed to monitor flows on an organization’s internal networks, and are also sometimes deployed where they can monitor flows between an organization’s networks and external networks (e.g., the Internet, business partners’ networks).

**4.Host-Based:**

* **Host-Based,** which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.
* Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes.
* Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

**Q.5. What are the typical components of IDPS System?**

**Ans:**

**Typical Components:**

The typical components in an IDPS solution are as follows:

**1.Sensor or Agent:**

* Sensors and agents monitor and analyze activity. The term *sensor* is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term *agent* is typically used for host-based IDPS technologies.

**2.Management Server:**

* A *management server* is a centralized device that receives information from the sensors or agents and manages them.
* Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot.
* Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as *correlation*. Management servers are available as both appliance and software-only products.
* Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

**3.Database Server:**

* A *database server* is a repository for event information recorded by sensors,

agents, and/or management servers. Many IDPSs provide support for database servers.

**4.Console:**

* A *console* is a program that provides an interface for the IDPS’s users and administrators.
* Console software is typically installed onto standard desktop or laptop computers.
* Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

**Q.6. What are the typical components of network based IDPS System?**

**Ans:**

* A typical network-based IDPS is composed of sensors, one or more management servers, multiple consoles, and optionally one or more database servers (if the network-based IDPS supports their use).
* All of these components are similar to other types of IDPS technologies, except for the sensors.
* A network-based IDPS sensor monitors and analyzes network activity on one or more network segments. The network interface cards that will be performing monitoring are placed into *promiscuous mode*, which means that they will accept all incoming packets that they see, regardless of their intended destinations.
* Most IDPS deployments use multiple sensors, with large deployments having hundreds of sensors. Sensors are available in two formats:

**1.Appliance:**

* An appliance-based sensor is comprised of specialized hardware and sensor software.
* The hardware is typically optimized for sensor use, including specialized NICs and NIC drivers for efficient capture of packets, and specialized processors or other hardware components that assist in analysis.
* Parts or all of the IDPS software might reside in firmware for increased efficiency. Appliances often use a customized, hardened operating system (OS) that administrators are not intended to access directly.

**2.Software Only:**

* Some vendors sell sensor software without an appliance. Administrators can install the software onto hosts that meet certain specifications.
* The sensor software might include a customized OS, or it might be installed onto a standard OS just as any other application would.

Sensors can be deployed in one of two modes:

**1.Inline:**

* An *inline sensor* is deployed so that the network traffic it is monitoring must pass through it, much like the traffic flow associated with a firewall. In fact, some inline sensors are hybrid firewall/IDPS devices, while others are simply IDPSs.
* The primary motivation for deploying IDPS sensors inline is to enable them to stop attacks by blocking network traffic.
* Inline sensors are typically placed where network firewalls and other network security devices would be placed—at the divisions between networks, such as connections with external networks and borders between different internal networks that should be segregated.

**2.Passive:**

* A *passive sensor* is deployed so that it monitors a copy of the actual network traffic; no traffic actually passes through the sensor.
* Passive sensors are typically deployed so that they can monitor key network locations, such as the divisions between networks, and key network segments, such as activity on a demilitarized zone (DMZ) subnet.

**Q.7. List and explain various security capabilities of IDPS technologies.**

**Ans:**

**Various security capabilities of IDPS technologies are as follows:**

1.Information Gathering Capabilities

2.Logging Capabilities

3.Detection Capabilities

4.Prevention Capabilities

**1.Information Gathering Capabilities:**

* Some network-based IDPSs offer limited information gathering capabilities, which means that they can collect information on hosts and the network activity involving those hosts. Examples of information gathering capabilities are as follows:

􀀟 **Identifying Hosts:**

* An IDPS sensor might be able to create a list of hosts on the organization’s

network arranged by IP address or MAC address. The list can be used as a profile to identify new hosts on the network.

􀀟 **Identifying Operating Systems:**

* An IDPS sensor might be able to identify the OSs and OS versions used by the organization’s hosts through various techniques.

􀀟 **Identifying Applications:**

* For some applications, an IDPS sensor can identify the application versions in use by keeping track of which ports are used and monitoring certain characteristics of application communications.

􀀟 **Identifying Network Characteristics:**

* Some IDPS sensors collect general information about network traffic related to the configuration of network devices and hosts, such as the number of hops between two devices. This information can be used to detect changes to the network configuration.

**2.Logging Capabilities:**

* Network-based IDPSs typically perform extensive logging of data related to detected events.
* This data can be used to confirm the validity of alerts, to investigate incidents, and to correlate events between the IDPS and other logging sources.
* Data fields commonly logged by network-based IDPSs include the following:

􀀟 Timestamp (usually date and time)

􀀟 Connection or session ID (typically a consecutive or unique number assigned to

each TCP connection or to like groups of packets for connectionless protocols)

􀀟 Event or alert type 21

􀀟 Rating (e.g., priority, severity, impact, confidence)

􀀟 Network, transport, and application layer protocols

􀀟 Source and destination IP addresses

􀀟 Source and destination TCP or UDP ports, or ICMP types and codes

􀀟 Number of bytes transmitted over the connection

􀀟 Decoded payload data, such as application requests and responses

􀀟 State-related information (e.g., authenticated username)

􀀟 Prevention action performed (if any).

**3.Detection Capabilities:**

* The detection methods are usually tightly interwoven; for example, a stateful protocol analysis engine might parse activity into requests and responses, each of which is examined for anomalies and compared to signatures of known bad activity.

The following are the aspects of detection capabilities:

􀀟 Types of events detected

􀀟 Detection accuracy

􀀟 Tuning and customization

􀀟 Technology limitations.

Network-based IDPS sensors offer various prevention capabilities, including the following (grouped by sensor type):

1. **Passive Only:**

– **Ending the Current TCP Session:**

* A passive sensor can attempt to end an existing TCP session by sending TCP reset packets to both endpoints; this is sometimes called *session sniping*.
* The sensor does this to make it appear to each endpoint that the other endpoint is trying to end the connection.
* The goal is for one of the endpoints to terminate the connection before an attack can succeed.

1. **Inline Only:**

– **Performing Inline Firewalling:**

* Most inline IDPS sensors offer firewall capabilities that can be used to drop or reject suspicious network activity.

– **Throttling Bandwidth Usage:**

* If a particular protocol is being used inappropriately, such as for a DoS attack, malware distribution, or peer-to-peer file sharing, some inline IDPS sensors can limit the percentage of network bandwidth that the protocol can use.
* This prevents the activity from negatively impacting bandwidth usage for other resources.

– **Altering Malicious Content:**

* Some inline IDPS sensors can sanitize part of a packet, which means that malicious content is replaced with benign content and the sanitized packet sent to its destination.
* A sensor that acts as a proxy might perform automatic normalization of all traffic, such as repackaging application payloads in new packets.
* This has the effect of sanitizing some attacks involving packet headers and some application headers, whether or not the IDPS has detected an attack.

3. **Both Passive and Inline:**

– **Reconfiguring Other Network Security Devices:**

* Many IDPS sensors can instruct network security devices such as firewalls, routers, and switches to reconfigure themselves to block certain types of activity or route it elsewhere.
* This can be helpful in several situations, such as keeping an external attacker out of a network and quarantining an internal host that has been compromised (e.g., moving it to a quarantine VLAN).

– **Running a Third-Party Program or Script:**

* Some IDPS sensors can run an administrator specified script or program when certain malicious activity is detected.
* This could trigger any prevention action desired by the administrator, such as reconfiguring other security devices to block the malicious activity.
* Third-party programs or scripts are most commonly used when the IDPS does not support the prevention actions that administrators want to have performed.

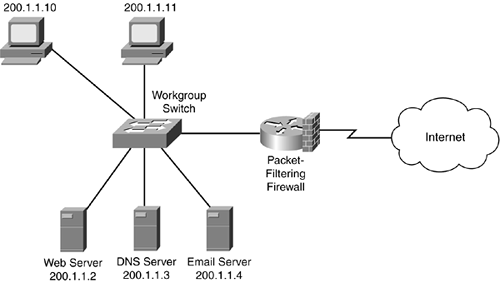
**Q.8. What are the various types of sensors used in network based IDPS System?**

**Ans:**

**Refer Q.6.**

**Q.9. Explain packet filtering firewall technology.**

**Ans:**



* The most basic feature of a firewall is the *packet filter*. Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering.
* Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a *ruleset*.
* Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.
* In their most basic form, firewalls with packet filters operate at the network layer. This provides network access control based on several pieces of information contained in a packet, including:
* The packet’s source IP address—the address of the host from which the packet originated (such as 192.168.1.1)
* The packet’s destination address—the address of the host the packet is trying to reach (e.g., 192.168.2.1)
* The network or transport protocol being used to communicate between source and destination hosts, such as TCP, UDP, or ICMP
* Possibly some characteristics of the transport layer communications sessions, such as session source and destination ports (e.g., TCP 80 for the destination port belonging to a web server, TCP 1320 for the source port belonging to a personal computer accessing the server)
* The interface being traversed by the packet, and its direction (inbound or outbound).
* Filtering inbound traffic is known as *ingress filtering*. Outgoing traffic can also be filtered, a process referred to as *egress filtering*.
* Here, organizations can implement restrictions on their internal traffic, such as blocking the use of external file transfer protocol (FTP) servers or preventing denial of service (DoS) attacks from being launched from within the organization against outside entities.
* Organizations should only permit outbound traffic that uses the source IP addresses in use by the organization—a process that helps block traffic with spoofed addresses from leaking onto other networks.
* Spoofed addresses can be caused by malicious events such as malware infections or compromised hosts being used to launch attacks, or by inadvertent misconfigurations.
* Stateless packet filters are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack.
* For example, many packet filters are unable to detect when a packet’s network layer addressing information has been spoofed or otherwise altered, or uses options that are permitted by standards but generally used for malicious purposes, such as IP source routing.
* Spoofing attacks, such as using incorrect addresses in the packet headers, are generally employed by intruders to bypass the security controls implemented in a firewall platform.
* Firewalls that operate at higher layers can thwart some spoofing attacks by verifying that a session is established, or by authenticating users before allowing traffic to pass.
* Because of this, most firewalls that use packet filters also maintain some state information for the packets that traverse the firewall.
* Some packet filters can specifically filter packets that are fragmented. Packet fragmentation is allowed by the TCP/IP specifications and is encouraged in situations where it is needed.
* However, packet fragmentation has been used to make some attacks harder to detect (by placing them within fragmented packets), and unusual fragmentation has also been used as a form of attack.

**Q.10. Explain the dedicated proxy server, application proxy server firewall technology.**

**Ans:**

**Q.11. Explain how firewall act as network address translators.**

**Ans:**

* Most firewalls can perform NAT, which is sometimes called port address translation (PAT) or network address and port translation (NAPT). Despite the popular misconception, NAT is not part of the security functionality of a firewall.
* The security benefit of NAT—preventing a host outside the firewall from initiating contact with a host behind NAT—can just as easily be achieved by a stateful firewall with less disruption to protocols that do not work as well behind NAT.
* However, turning on a firewall’s NAT feature is usually easier than properly configuring the firewall policy to have the same protections, so many people think of NATs as primarily a security feature.
* Typically, a NAT acts as a router that has a network with private addresses on the inside and a single public address on the outside.
* The way a NAT performs this many-to-one mapping varies between implementations, but almost always involves the following:

􀀟 Hosts on the inside network initiating connections to the outside network cause the NAT to map the source port of the connection to a different source port that is controlled by the NAT. The NAT uses this source port number to map connections from the outside back to the host on the inside.

􀀟 Hosts on the outside of the network cannot initiate contact with hosts on the inside network. In some firewalls, the NAT can be configured to map a particular destination port on the NAT to a particular host on the inside of the NAT; for example, all HTTP requests that go to the NAT could be directed to a single host on the protected side of the firewall. This feature is sometimes called *pinholing*.

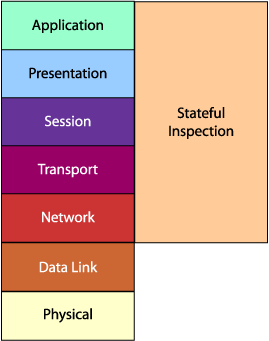
* Although NATs are not in and of themselves security features of a firewall, they interact with the firewall’s security policy.
* For example, any policy that requires that all HTTP servers accessible to the

outside be on the DMZ must prevent the NAT from pinholing TCP port 80. Another example of where NATs interact with security policy is the ability to identify the source of traffic in a firewall’s logs.

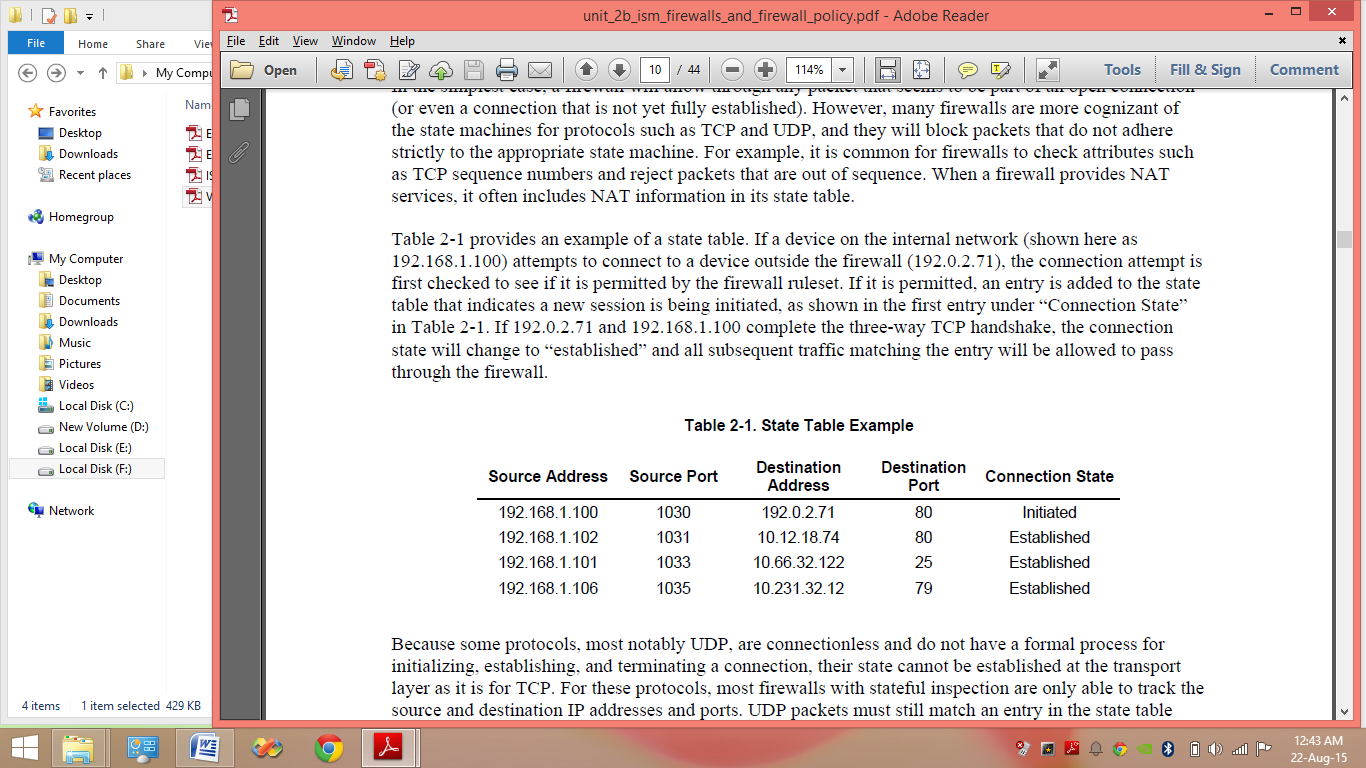
* If a NAT is used, it must report the private address in the logs instead of the translated public address, otherwise the logs will incorrectly identify many hosts by the single public address.

**Q.12. Explain stateful inspection.**

**Ans:**



* *Stateful inspection* improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer.
* As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table.
* While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.
* Three major states exist for TCP traffic—connection establishment, usage, and termination (which refers to both an endpoint requesting that a connection be closed and a connection with a long period of inactivity.)
* Stateful inspection in a firewall examines certain values in the TCP headers to monitor the state of each connection. Each new packet is compared by the firewall to the firewall’s state table to determine if the packet’s state contradicts its expected state.
* For example, an attacker could generate a packet with a header indicating it is part of an established connection, in hopes it will pass through a firewall. If the firewall uses stateful inspection, it will first verify that the packet is part of an established connection listed in the state table.
* In the simplest case, a firewall will allow through any packet that seems to be part of an open connection (or even a connection that is not yet fully established).
* However, many firewalls are more cognizant of the state machines for protocols such as TCP and UDP, and they will block packets that do not adhere strictly to the appropriate state machine.
* For example, it is common for firewalls to check attributes such as TCP sequence numbers and reject packets that are out of sequence. When a firewall provides NAT services, it often includes NAT information in its state table.
* Table 2-1 provides an example of a state table. If a device on the internal network (shown here as 192.168.1.100) attempts to connect to a device outside the firewall (192.0.2.71), the connection attempt is first checked to see if it is permitted by the firewall ruleset.
* If it is permitted, an entry is added to the state table that indicates a new session is being initiated, as shown in the first entry under “Connection State” in Table 2-1. If 192.0.2.71 and 192.168.1.100 complete the three-way TCP handshake, the connection state will change to “established” and all subsequent traffic matching the entry will be allowed to pass through the firewall.



* Because some protocols, most notably UDP, are connectionless and do not have a formal process for initializing, establishing, and terminating a connection, their state cannot be established at the transport layer as it is for TCP.
* For these protocols, most firewalls with stateful inspection are only able to track the

source and destination IP addresses and ports.

* UDP packets must still match an entry in the state table based on source and destination IP address and port information to be permitted to pass—a DNS response from an external source would be permitted to pass only if the firewall had previously seen a corresponding DNS query from an internal source.
* Since the firewall is unable to determine when a session has ended, the entry is removed from the state table after a preconfigured timeout value is reached.
* Application-level firewalls that are able to recognize DNS over UDP will terminate a session after a DNS response is received, and may act similarly with the Network Time Protocol (NTP).

**Q.13. Write short note on application firewalls.**

**Ans:**

* A newer trend in stateful inspection is the addition of a *stateful protocol analysis* capability, referred to by some vendors as *deep packet inspection*.
* Stateful protocol analysis improves upon standard stateful inspection by adding basic intrusion detection technology—an inspection engine that analyzes protocols at the application layer to compare vendor-developed profiles of benign protocol activity against observed events to identify deviations.
* This allows a firewall to allow or deny access based on how an application is running over the network. For instance, an application firewall can determine if an email message contains a type of attachment that the organization does not permit (such as an executable file), or if instant messaging (IM) is being used over port 80 (typically used for HTTP).
* Another feature is that it can block connections over which specific actions are being performed (e.g., users could be prevented from using the FTP “put” command, which allows users to write files to the FTP server).
* This feature can also be used to allow or deny web pages that contain particular types of active content, such as Java or ActiveX, or that have SSL certificates signed by a particular certificate authority (CA), such as a compromised or revoked CA.
* Application firewalls can enable the identification of unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command that was not preceded by another command on which it is dependent.
* These suspicious commands often originate from buffer overflow attacks, DoS

attacks, malware, and other forms of attack carried out within application protocols such as HTTP.

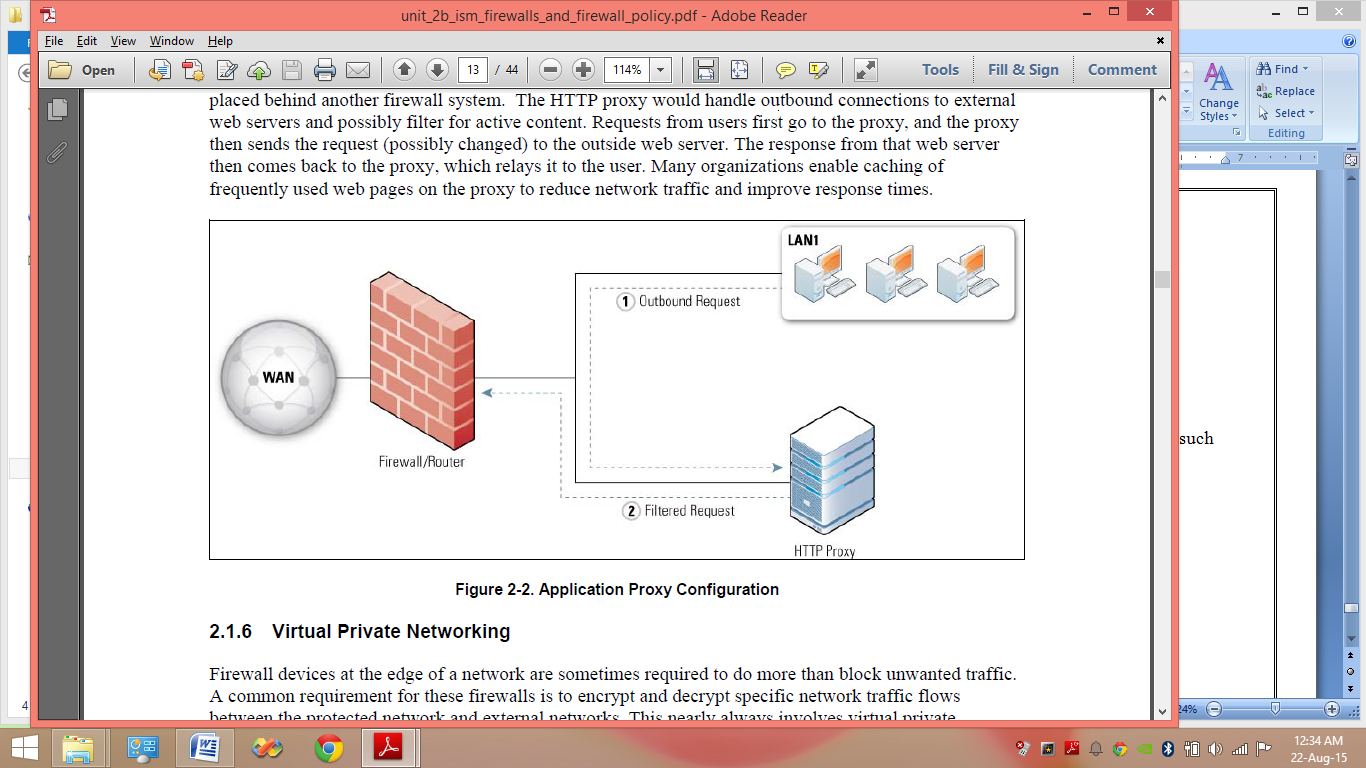
* Another common feature is input validation for individual commands, such as minimum and maximum lengths for arguments.
* For example, a username argument with a length of 1000 characters is suspicious—even more so if it contains binary data. Application firewalls are available for many common protocols including HTTP, database (such as SQL), email (SMTP, Post Office Protocol [POP], and Internet Message Access Protocol [IMAP])3, voice over IP (VoIP), and Extensible Markup Language (XML).
* Another feature found in some application firewalls involves enforcing application state machines, which are essentially checks on the traffic’s compliance to the standard for the protocol in question.
* This compliance checking, sometimes call “RFC compliance” because most protocols are defined in RFCs issued by the Internet Engineering Task Force (IETF), can be a mixed blessing.
* Many products implement protocols in ways that almost, but not completely, match the specification, so it is usually necessary to let such implementations communicate across the firewall.
* Compliance checking is only useful when it detects and blocks communication that can be harmful to protected systems.
* Firewalls with both stateful inspection and stateful protocol analysis capabilities are not full-fledged intrusion detection and prevention systems (IDPS), which usually offer much more extensive attack detection and prevention capabilities.
* For example, IDPSs also use signature-based and/or anomaly-based analysis to detect additional problems within network traffic.

**Q.14. Write short note on Application-Proxy Gateways & Dedicated Proxy Servers.**

**Ans:**

**1.Dedicated Proxy Servers:**

* *Dedicated proxy servers* differ from application-proxy gateways in that while dedicated proxy servers retain proxy control of traffic, they usually have much more limited firewalling capabilities.
* Many dedicated proxy servers are application-specific, and some actually perform analysis and validation of common application protocols such as HTTP.
* Because these servers have limited firewalling capabilities, such as simply blocking traffic based on its source or destination, they are typically deployed behind traditional firewall platforms.
* Typically, a main firewall could accept inbound traffic, determine which application is being targeted, and hand off traffic to the appropriate proxy server (e.g., email proxy). This server would perform filtering or logging operations on the traffic, then forward it to internal systems.
* A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and pass it to the firewall for outbound delivery.
* An example of this is an HTTP proxy deployed behind the firewall—users would need to connect to this proxy en route to connecting to external web servers.
* Dedicated proxy servers are generally used to decrease firewall workload and conduct specialized filtering and logging that might be difficult to perform on the firewall itself.
* Figure 2-2 shows a sample diagram of a network employing a dedicated HTTP proxy server that has been placed behind another firewall system.
* The HTTP proxy would handle outbound connections to external web servers and possibly filter for active content.
* Requests from users first go to the proxy, and the proxy then sends the request (possibly changed) to the outside web server. The response from that web server then comes back to the proxy, which relays it to the user.
* Many organizations enable caching of frequently used web pages on the proxy to reduce network traffic and improve response times.

****

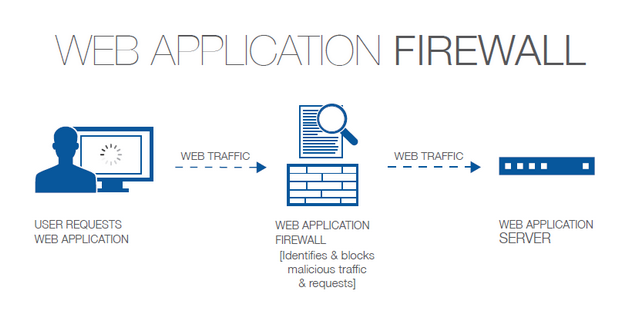
**2.Application-Proxy Gateways:**

* An *application-proxy gateway* is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality.
* These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them.
* Each successful connection attempt actually results in the creation of two separate connections—one between the client and the proxy server, and another between the proxy server and the true destination.
* The proxy is meant to be transparent to the two hosts—from their perspectives there is a direct connection. Because external hosts only communicate with the proxy agent, internal IP addresses are not visible to the outside world.
* The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall. Application-proxy gateways are quite different than application firewalls.
* First, an application-proxy gateway can offer a higher level of security for some applications because it prevents direct connections between two hosts and it inspects traffic content to identify policy violations.
* Another potential advantage is that some application-proxy gateways have the ability to decrypt packets (e.g., SSL-protected payloads), examine them, and re-encrypt them before sending them on to the destination host.
* Data that the gateway cannot decrypt is passed directly through to the application. When choosing the type of firewall to deploy, it is important to decide whether the firewall actually needs to act as an application proxy so that it can match the specific policies needed by the organization.

**Q.15. Write short note on Web Application Firewalls & Firewalls for Virtual Infrastructures.**

**Ans:**

**Web Application Firewalls:**



* The HTTP protocol used in web servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise.
* Many of these exploits can be detected by specialized application firewalls called *web application firewalls* that reside in front of the web server.
* Web application firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently.
* Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.

**Firewalls for Virtual Infrastructures:**

* Many virtualization solutions allow more than one operating system to run on a single computer simultaneously, each appearing as if it were a real computer.
* This has become popular recently because it allows organizations to make more efficient use of computer hardware.
* Most of these types of virtualization systems include *virtualized networking*, which allows the multiple operating systems to communicate as if they were on a standard Ethernet, even though there is no actual networking hardware.
* Network activity that passes directly between virtualized operating systems within a host cannot be monitored by an external firewall.
* However, some virtualization systems offer built-in firewalls or allow third-party software firewalls to be added as plug-ins.
* Using firewalls to monitor virtualized networking is a relatively new area of firewall technology, and it is likely to change significantly as virtualization usage continues to increase.

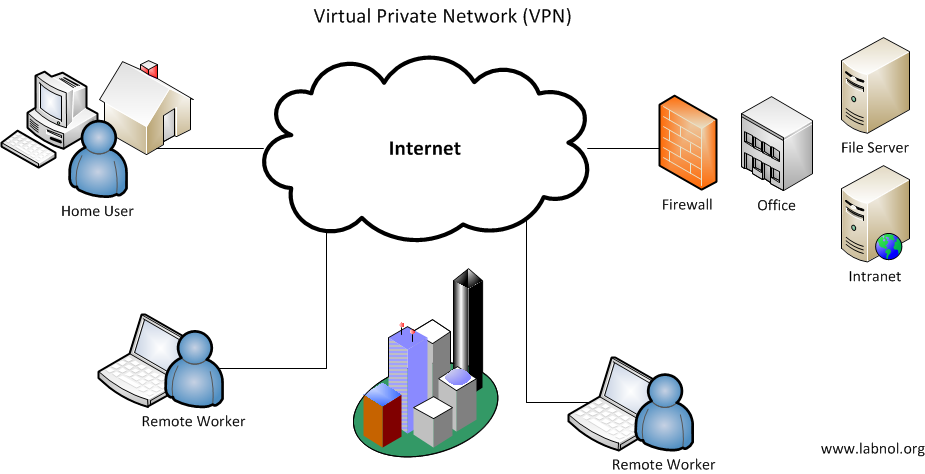
**Q.16. State the Limitations of Firewall Inspection.**

**Ans:**

* Firewalls can only work effectively on traffic that they can inspect. Regardless of the firewall technology chosen, a firewall that cannot understand the traffic flowing through it will not handle that traffic properly—for example, allowing traffic that should be blocked.
* Many network protocols use cryptography to hide the contents of the traffic. Other encrypting protocols include Secure Shell (SSH) and Secure Real-time Transport Protocol (SRTP).
* Firewalls also cannot read application data that is encrypted, such as email that is encrypted using the S/MIME or OpenPGP protocols, or files that are manually encrypted.
* Another limitation faced by some firewalls is understanding traffic that is tunneled, even if it is not encrypted.
* For example, IPv6 traffic can be tunneled in IPv4 in many different ways. The content may still be unencrypted, but if the firewall does not understand the particular tunneling mechanism used, the traffic cannot be interpreted.
* In all these cases, the firewall’s rules will determine what to do with traffic it does not (or, in the case of encrypted traffic, cannot) understand.
* An organization should have policies about how to handle traffic in such cases, such as either permitting or blocking encrypted traffic that is not authorized to be encrypted.

**Q.17. Write short note on VPN.**

**Ans:**



* Firewall devices at the edge of a network are sometimes required to do more than block unwanted traffic. A common requirement for these firewalls is to encrypt and decrypt specific network traffic flows between the protected network and external networks.
* This nearly always involves virtual private networks (VPN), which use additional protocols to encrypt traffic and provide user authentication and integrity checking. VPNs are most often used to provide secure network communications across untrusted networks.
* For example, VPN technology is widely used to extend the protected network of a multi-site organization across the Internet, and sometimes to provide secure remote user access to internal organizational networks via the Internet.
* Two common choices for secure VPNs are IPsec6 and Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
* The two most common VPN architectures are gateway-to-gateway and host-to-gateway.
* Gateway-to-gateway architectures connect multiple fixed sites over public lines through the use of VPN gateways— for example, to connect branch offices to an organization’s headquarters.
* A VPN gateway is usually part of another network device such as a firewall or router. When a VPN connection is established between the two gateways, users at branch locations are unaware of the connection and do not require any special

settings on their computers.

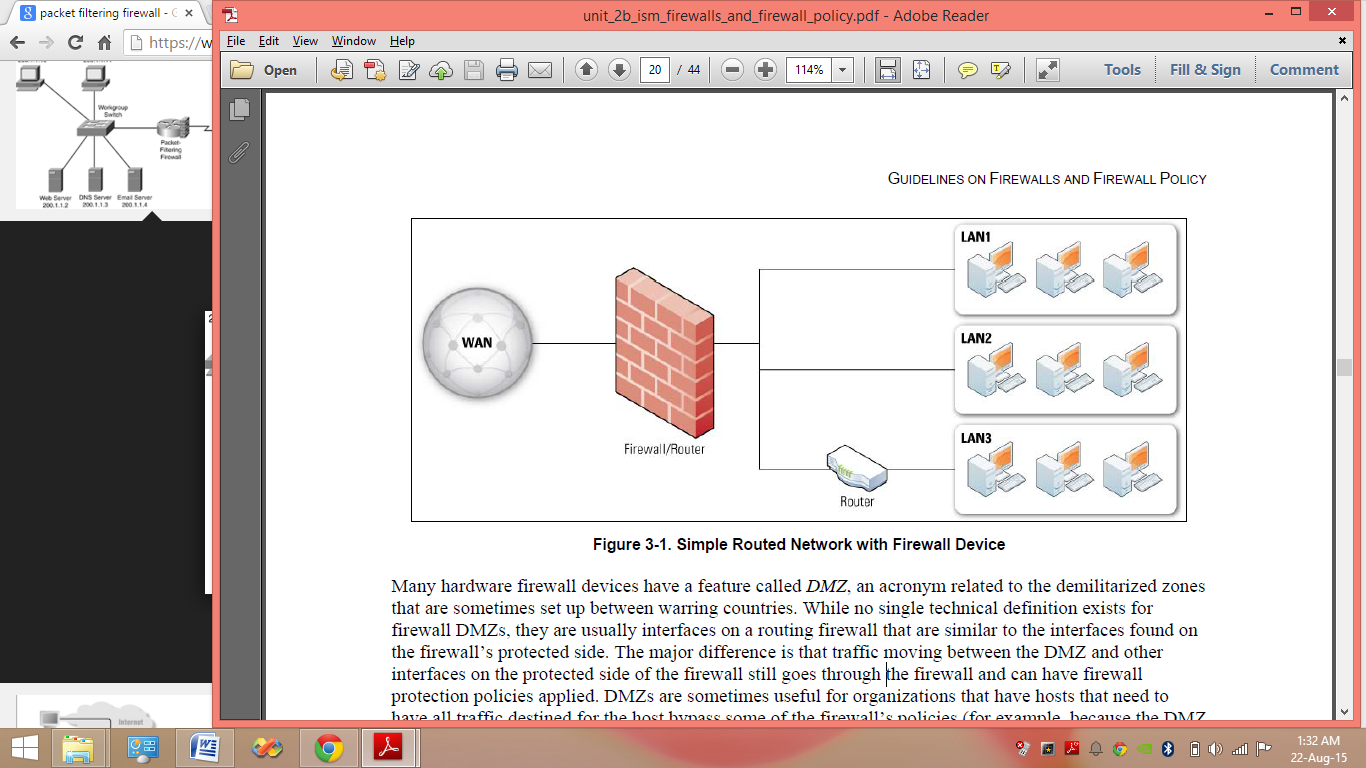
* The second type of architecture, host-to-gateway, provides a secure connection to the network for individual users, usually called *remote users*, who are located outside of the organization (at home, in a hotel, etc.)
* Here, a client on the user machine negotiates the secure connection with the organization’s VPN gateway.
* For gateway-to-gateway and host-to-gateway VPNs, the VPN functionality is often part of the firewall itself. Placing it behind the firewall would require VPN traffic to be passed through the firewall while encrypted, preventing the firewall from inspecting the traffic.
* All remote access (host-to-gateway) VPNs allow the firewall administrator to decide which users have access to which network resources. This access control is normally available on a per-user and per-group basis; that is, the VPN policy can specify which users and groups are authorized to access which resources, should an organization need that level of granularity.
* VPNs generally rely on authentication protocols such as Remote Authentication Dial In User Service (RADIUS). RADIUS uses several different types of authentication credentials, with the most common examples being username and password, digital signatures, and hardware tokens.
* Another authentication protocol often used by VPNs is the Lightweight Directory Access Protocol (LDAP); it is particularly useful for making access decisions for individual users and groups.
* To run VPN functionality on a firewall requires additional resources that depend on the amount of traffic flowing across the VPN and the type of encryption being used. For some environments, the added traffic associated with VPNs might require additional capacity planning and resources.
* Planning is also needed to determine the type of VPN (gateway-to-gateway and/or host-to-gateway) that should be included in the firewall.
* Many firewalls include hardware acceleration for encryption to minimize the impact of VPN services.

**Q.18. Explain various network layouts with firewall implementation.**

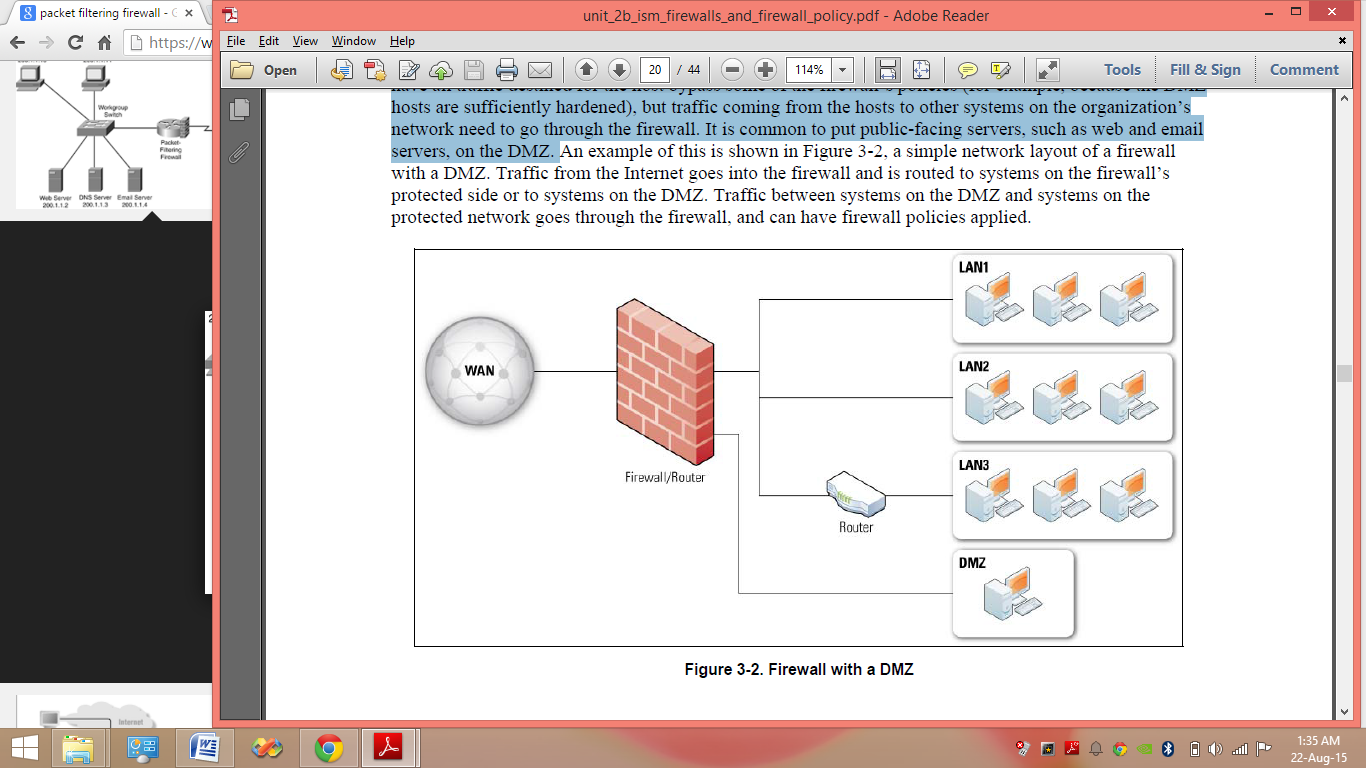
**Ans:**

* Figure 3-1 shows a typical network layout with a hardware firewall device acting as a router. The unprotected side of the firewall connects to the single path labeled “WAN,” and the protected side connects to three paths labeled “LAN1,” “LAN2,” and “LAN3.” The firewall acts as a router for traffic between the wide area network (WAN) path and the LAN paths.
* In the figure, one of the LAN paths also has a router; some organizations prefer to use multiple layers of routers due to legacy routing policies

within the network.

****

* Many hardware firewall devices have a feature called *DMZ*, an acronym related to the demilitarized zones that are sometimes set up between warring countries.
* While no single technical definition exists for firewall DMZs, they are usually interfaces on a routing firewall that are similar to the interfaces found on the firewall’s protected side.
* The major difference is that traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.
* DMZs are sometimes useful for organizations that have hosts that need to have all traffic destined for the host bypass some of the firewall’s policies (for example, because the DMZ hosts are sufficiently hardened), but traffic coming from the hosts to other systems on the organization’s network need to go through the firewall.
* It is common to put public-facing servers, such as web and email servers, on the DMZ.



* An example of this is shown in Figure 3-2, a simple network layout of a firewall

with a DMZ. Traffic from the Internet goes into the firewall and is routed to systems on the firewall’s protected side or to systems on the DMZ.

* Traffic between systems on the DMZ and systems on the protected network goes through the firewall, and can have firewall policies applied.

**Q.19. What are the various policies based on ip addresses.**

**Ans:**

* Firewall policies should only allow necessary IP protocols through. Examples of commonly used IP protocols, with their IP protocol numbers,17 are ICMP (1), TCP (6), and UDP (17).
* Other IP protocols, such as IPsec components Encapsulating Security Payload (ESP) (50) and Authentication Header (AH) (51) and routing protocols, may also need to pass through firewalls.

**IP Addresses and Other IP Characteristics:**

Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendations for IP addresses include:

* Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location. Examples of relatively common invalid IPv4 addresses are 127.0.0.0 127.255.255.255 (also known as the *localhost* addresses) and 0.0.0.0 (interpreted by some operating systems as a localhost or a broadcast address). These have no legitimate use on a network. Also, traffic using link-local addresses (169.254.0.0 to 169.254.255.255) should be blocked.
* Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid “external” address) should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks, or misconfigured equipment. The most common type of invalid external addresses is an IPv4 address within the ranges in RFC 1918, *Address Allocation for Private Internets*, that are reserved for private networks. These ranges are 10.0.0.0 to 10.255.255.255 (10.0.0.0/8 in Classless Inter-Domain Routing [CIDR] notation), 172.16.0.0 to 172.31.255.255 (172.16.0.0/12), and 192.168.0.0 to 192.168.255.255 (192.168.0.0/16).
* Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an “internal” address) should be blocked at the network perimeter. Perimeter devices can perform address translation services to permit internal hosts with private addresses to communicate through the perimeter, but private addresses should not be passed through the network perimeter.
* Outbound traffic with invalid source addresses should be blocked (this is often called *egress filtering*). Systems that have been compromised by attackers can be used to attack other systems on the Internet; using invalid source addresses makes these kinds of attacks more difficult to stop. Blocking this type of traffic at an organization’s firewall helps reduce the effectiveness of these attacks.
* Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.

**Q.20. What are the various policies based on protocols.**

**Ans:**

**Q.21. What are the various policies based on applications, user identity & Network Activity.**

**Ans:**

**Policies Based on Applications:**

* Inbound application firewalls or application proxies take a different approach—they let traffic destined for a particular server into the network, but capture that traffic in a server that processes it like a port-based firewall.
* The application-based approach provides an additional layer of security for incoming
* traffic by validating some of the traffic before it reaches the desired server.
* The inbound application firewall’s or proxy’s additional security layer can protect the server better than the server can protect itself—and can also remove malicious traffic before it reaches the server to help reduce server load.
* In some cases, an application firewall or proxy can remove traffic that the server might not be able to remove on its own because it has greater filtering capabilities. An application firewall or proxy also prevents the server from having direct access to the outside network.
* If possible, inbound application firewalls and proxies should be used in front of any server that does not have sufficient security features to protect it from application-specific attacks.

The main considerations when deciding whether or not to use an inbound application firewall or proxy are:

* Is a suitable application firewall available? Or, if appropriate, is a suitable application proxy available?
* Is the server already sufficiently protected by existing firewalls?
* Can the main server remove malicious content as effectively as the application firewall or proxy?
* Is the latency caused by an application proxy acceptable for the application?
* How easy it is to update the filtering rules on the main server and the application firewall or proxy to handle newly developed threats?

**Policies Based on User Identity:**

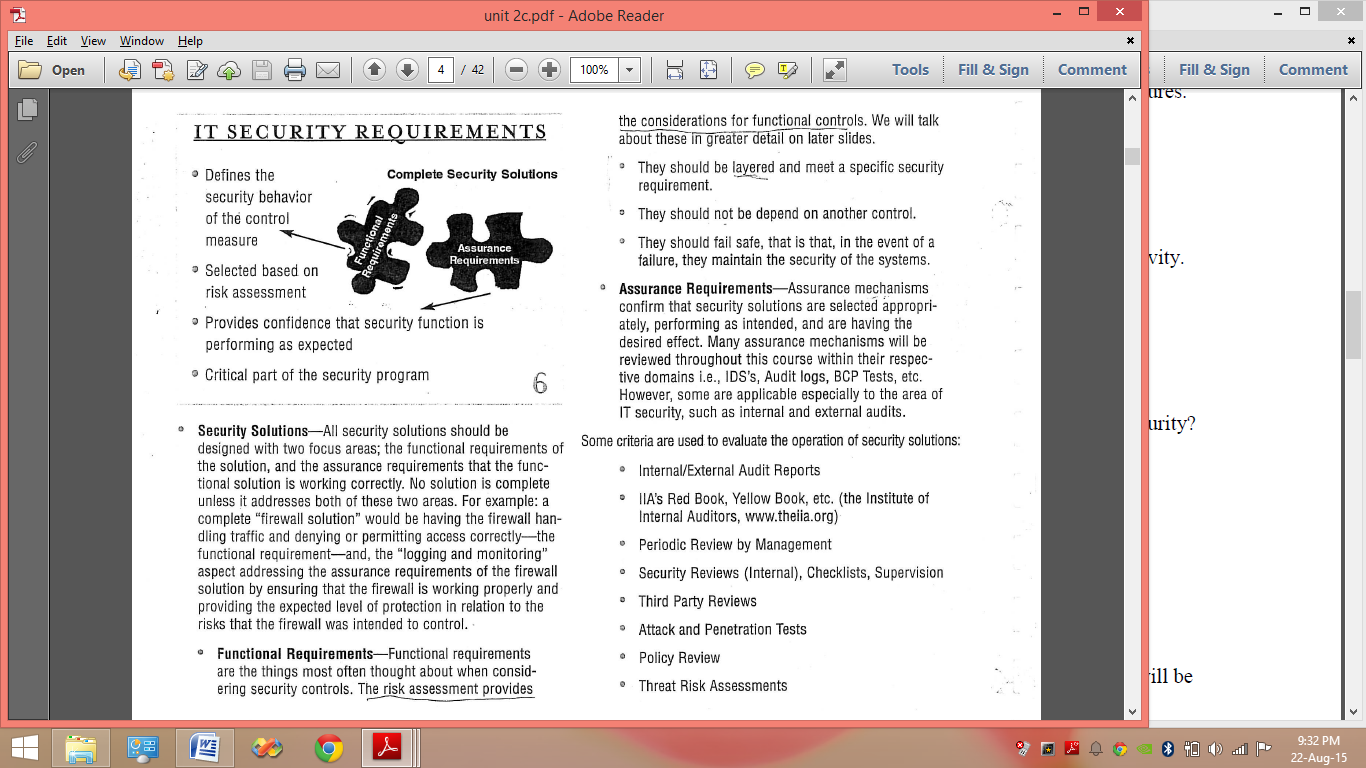
* Traditional packet filtering does not see the identities of the users who are communicating in the traffic traversing the firewall, so firewall technologies without more advanced capabilities cannot have policies that allow or deny access based on those identities.
* However, many other firewall technologies can see these identities and therefore enact policies based on user authentication. One of the most common ways to enforce user identity policy at a firewall is by using a VPN.
* Both IPsec VPNs and SSL VPNs have many ways to authenticate users, such as with secrets that are provisioned on a user-by-user basis, with multi-factor authentication (e.g., time-based cryptographic tokens protected with PINs), or with digital certificates controlled by each user.
* NAC has also become a popular method for firewalls to allow or deny users access to particular network resources. In addition, application firewalls and proxies can allow or deny access to users based on the user authentication within the applications themselves.
* Firewalls that enforce policies based on user identity should be able to reflect these policies in their logs.
* That is, it is probably not useful to only log the IP address from which a particular user connected if the user was allowed in by a user-specific policy; it is also important to log the user’s identity as well.

**Policies Based on Network Activity:**

* Many firewalls allow the administrator to block established connections after a certain period of inactivity.
* For example, if a user on the outside of a firewall has logged into a file server but has not made any requests during the past 15 minutes, the policy might be to block any further traffic on that connection.
* Time-based policies are useful in thwarting attacks caused by a logged-in user walking away from a computer and someone else sitting down and using the established connections (and therefore the logged-in user’s credentials).
* However, these policies can also be bothersome for users who make connections but do not use them frequently. For instance, a user might connect to a file server to read a
* file and then spend a long time editing the file.
* If the user does not save the file back to the file server before the firewall-mandated timeout, the timeout could cause the changes to the file to be lost.
* Some organizations have mandates about when firewalls should block connections that are considered to be inactive, when applications should disconnect sessions if there is no activity, etc.
* A firewall used by such an organization should be able to set policies that match the mandates while being specific enough to match the security objective of the mandates.
* A different type of firewall policy based on network activity is one that throttles or redirects traffic if the rate of traffic matching the policy rule is too high.
* For example, a firewall might redirect the connections made to a particular inside address to a slower route if the rate of connections is above a certain threshold.
* Another policy might be to drop incoming ICMP packets if the rate is too high. Crafting such policies is quite difficult because throttling and redirecting can cause desired traffic to be lost or have difficult-to diagnose transient failures.

**Q.22. Explain with diagram IT security requirements.**

**Ans:**

****

**Q.23. What should be considered in the planning stages of a Web server?**

**Ans:**

In the planning stages of a Web server, the following items should be considered [Alle00]:

* Identify the purpose(s) of the Web server.

􀂃 What information categories will be stored on the Web server?

􀂃 What information categories will be processed on or transmitted through the Web

server?

􀂃 What are the security requirements for this information?

􀂃 Will any information be retrieved from or stored on another host (e.g., back-end

database, mail server)?

􀂃 What are the security requirements for any other hosts involved (e.g., back-end

database, directory server, mail server, proxy server)?

􀂃 What other service(s) will be provided by the Web server (in general, dedicating

the host to being only a Web server is the most secure option)?

􀂃 What are the security requirements for these additional services?

􀂃 What are the requirements for continuity of services provided by Web servers,

such as those specified in continuity of operations plans and disaster recovery

plans?

􀂃 Where on the network will the Web server be located (see Section 8)?

* Identify the network services that will be provided on the Web server, such as those supplied through the following protocols:

􀂃 HTTP

􀂃 HTTPS

􀂃 Internet Caching Protocol (ICP)

􀂃 Hyper Text Caching Protocol (HTCP)

􀂃 Web Cache Coordination Protocol (WCCP)

􀂃 SOCKS

􀂃 Database services (e.g., Open Database Connectivity [ODBC]).

* Identify any network service software, both client and server, to be installed on the Web server and any other support servers.
* Identify the users or categories of users of the Web server and any support hosts.
* Determine the privileges that each category of user will have on the Web server and support hosts.
* Determine how the Web server will be managed (e.g., locally, remotely from the internal network, remotely from external networks).
* Decide if and how users will be authenticated and how authentication data will be protected.
* Determine how appropriate access to information resources will be enforced.
* Determine which Web server applications meet the organization’s requirements. Consider servers that may offer greater security, albeit with less functionality in some instances. Some issues to consider include—

􀂃 Cost

􀂃 Compatibility with existing infrastructure

􀂃 Knowledge of existing employees

􀂃 Existing manufacturer relationship

􀂃 Past vulnerability history

􀂃 Functionality.

* Work closely with manufacturer(s) in the planning stage.

The choice of Web server application may determine the choice of OS. However, to the degree possible, Web server administrators should choose an OS that provides the following [Alle00]:

* Ability to restrict administrative or root level activities to authorized users only
* Ability to control access to data on the server
* Ability to disable unnecessary network services that may be built into the OS or server software
* Ability to control access to various forms of executable programs, such as Common Gateway Interface (CGI) scripts and server plug-ins in the case of Web servers
* Ability to log appropriate server activities to detect intrusions and attempted intrusions
* Provision of a host-based firewall capability.

**Q.24. What are the steps for securely installing web server?**

**Ans:**

* The secure installation and configuration of the Web server application mirrors the OS process.
* The overarching principle, as before, is to install only the services required for the Web server and to eliminate any known vulnerabilities through patches or upgrades.
* Any unnecessary applications, services, or scripts that are installed should be removed immediately once the installation process is complete.
* During the installation of the Web server, the following steps should be performed:

􀀟 Install the Web server software either on a dedicated host or on a dedicated guest

OS if virtualization is being employed.

􀀟 Apply any patches or upgrades to correct for known vulnerabilities.

􀀟 Create a dedicated physical disk or logical partition (separate from OS and Web

server application) for Web content.

􀀟 Remove or disable all services installed by the Web server application but not

required (e.g., gopher, FTP, remote administration).

􀀟 Remove or disable all unneeded default login accounts created by the Web server

installation.

􀀟 Remove all manufacturers’ documentation from the server.

􀀟 Remove all example or test files from the server, including scripts and executable

code.

􀀟 Apply appropriate security template or hardening script to server.

􀀟 Reconfigure HTTP service banner (and others as required) not to report Web

server and OS type and version (this may not be possible with all Web servers).

* Organizations should consider installing the Web server with non-standard directory names, directory locations, and filenames.
* Many Web server attack tools and worms targeting Web servers only look for files and directories in their default locations.
* While this will not stop determined attackers, it will force them to work harder to compromise the server, and it also increases the likelihood of attack detection because of the failed attempts to access the default filenames and directories and the additional time needed to perform an attack.

**Q.25. Sate and explain any 4 Wireless Standards.**

**Ans:**

**1.Wireless personal area networks (WPAN):**

* small-scale wireless networks that require little or no infrastructure. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables.
* For example, WPANs can provide print services or enable a wireless keyboard or mouse to communicate with a computer. Examples of WPAN standards include the following:

- **IEEE 802.15.1 (Bluetooth)**:

* This WPAN standard is designed for wireless networking between small portable devices. The original Bluetooth operated at 2.4 GHz and has a maximum data rate of approximately 720 kilobits per second (Kbps); Bluetooth 2.0 can reach 3 Mbps.

- **IEEE 802.15.3 (High-Rate Ultrawideband; WiMedia, Wireless USB)**:

* This is a low-cost, low power consumption WPAN standard that uses a wide range of GHz frequencies to avoid interference with other wireless transmissions.
* It can achieve data rates of up to 480 Mbps over short ranges and can support the full range of WPAN applications.
* One expected use of this technology is the ability to detect shapes through physical barriers such as walls and boxes, which could be useful for applications ranging from law enforcement to search and rescue operations.

- **IEEE 802.15.4 (Low-Rate Ultrawideband; ZigBee)**:

* This is a simple protocol for lightweight WPANs. It is most commonly used for monitoring and control products, such as climate control systems and building lighting.

**2.Wireless local area networks (WLAN):**

* IEEE 802.11 is the dominant WLAN standard, but others have also been defined.
* For example, the European Telecommunications Standards Institute (ETSI) has published the **High Performance Radio Local Area Network (HIPERLAN)** WLAN standard that transmits data in the 5 GHz band and operates at data rates of approximately 23.5 Mbps.
* However, HIPERLAN appears to have been supplanted by IEEE 802.11 in the commercial arena.

**3.Wireless metropolitan area networks (WMAN):**

* networks that can provide connectivity to users located in multiple facilities that are generally within a few miles of each other.
* Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.
* For example, IEEE 802.16e (better known as WiMAX) is a WMAN standard that transmits in the 10 to 66 GHz band range. An IEEE 802.16a addendum allows for large data transmissions with minimal interference.
* WiMAX provides throughput of up to 75 Mbps, with a range of up to 30 miles for fixed line-of-site communication.
* However, there is generally a tradeoff; 75 Mbps throughput is possible at half a mile, but at 30 miles the throughput is much lower.

**4.Wireless wide area networks (WWAN):**

* networks that connect individuals and devices over large geographic areas, often globally. WWANs are typically used for cellular voice and data communications, as well as satellite communications.

**Q.26. State IEEE 802.11 Network Components and explain its Architectural Models.**

**Ans:**

**IEEE 802.11 Network Components and Architectural Models:**

IEEE 802.11 has two fundamental architectural components, as follows:

**i.Station (STA):**

* A *STA* is a wireless endpoint device. Typical examples of STAs are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with IEEE 802.11 capabilities.

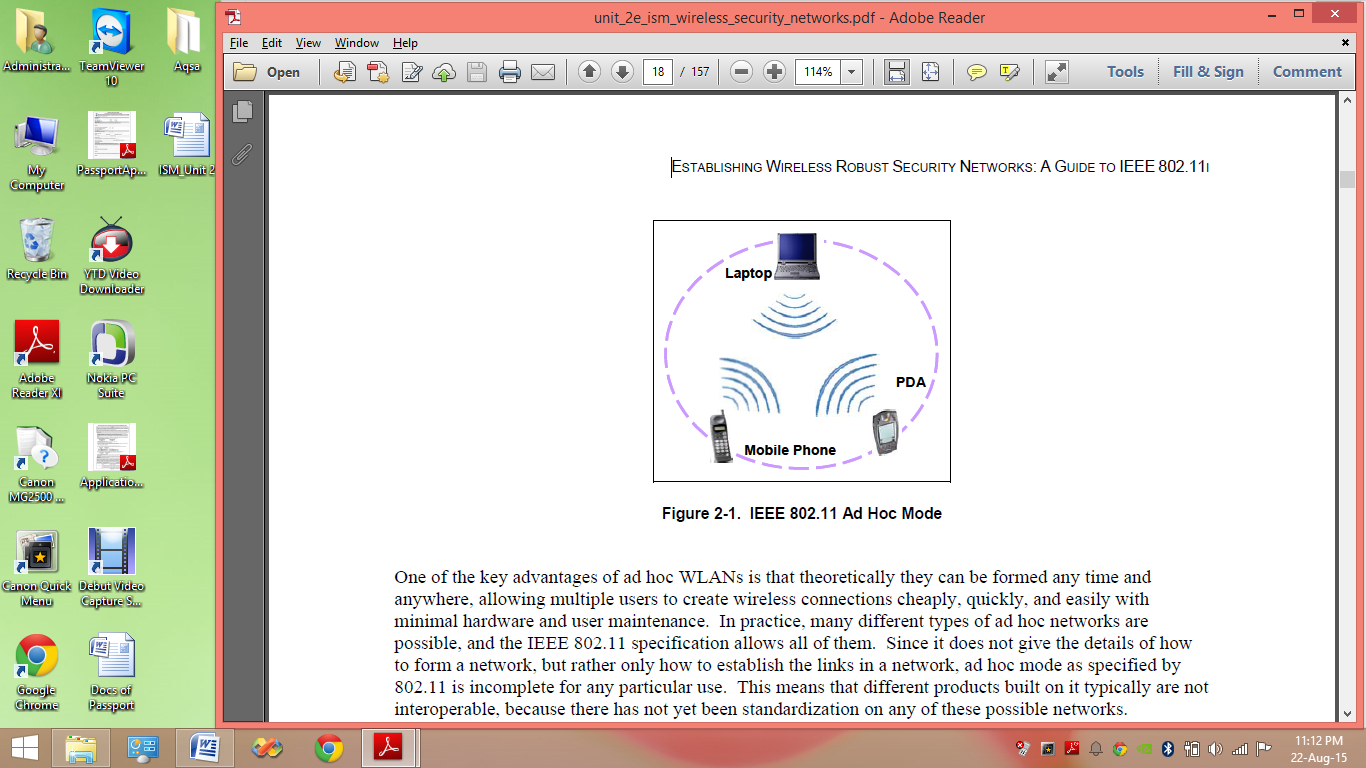
**ii.Access Point (AP):**

* 12 An *AP* logically connects STAs with a distribution system (DS), which is typically an organization’s wired infrastructure. APs can also logically connect wireless STAs with each other without accessing a distribution system.

The IEEE 802.11 standard also defines the following two WLAN design structures or configurations:

**i.Ad hoc Mode:**

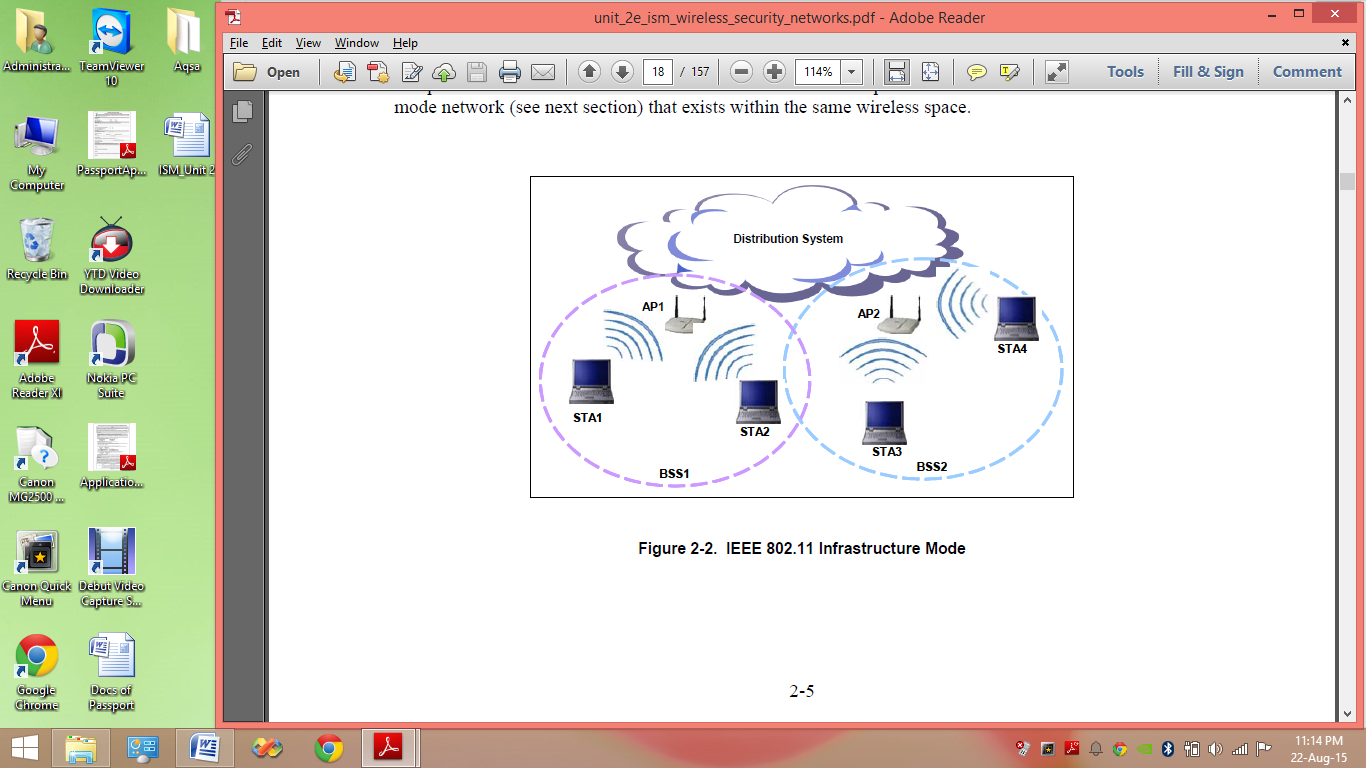
* The ad hoc mode (or topology) is depicted conceptually in Figure 2-1. This mode of operation, also known as *peer-to-peer mode*, is possible when two or more STAs are able to communicate directly to one another. Figure 2-1 shows three devices communicating with each other in a peer-to-peer fashion without any infrastructure. A set of STAs configured in this ad hoc manner is known as an *independent basic service set* (IBSS).



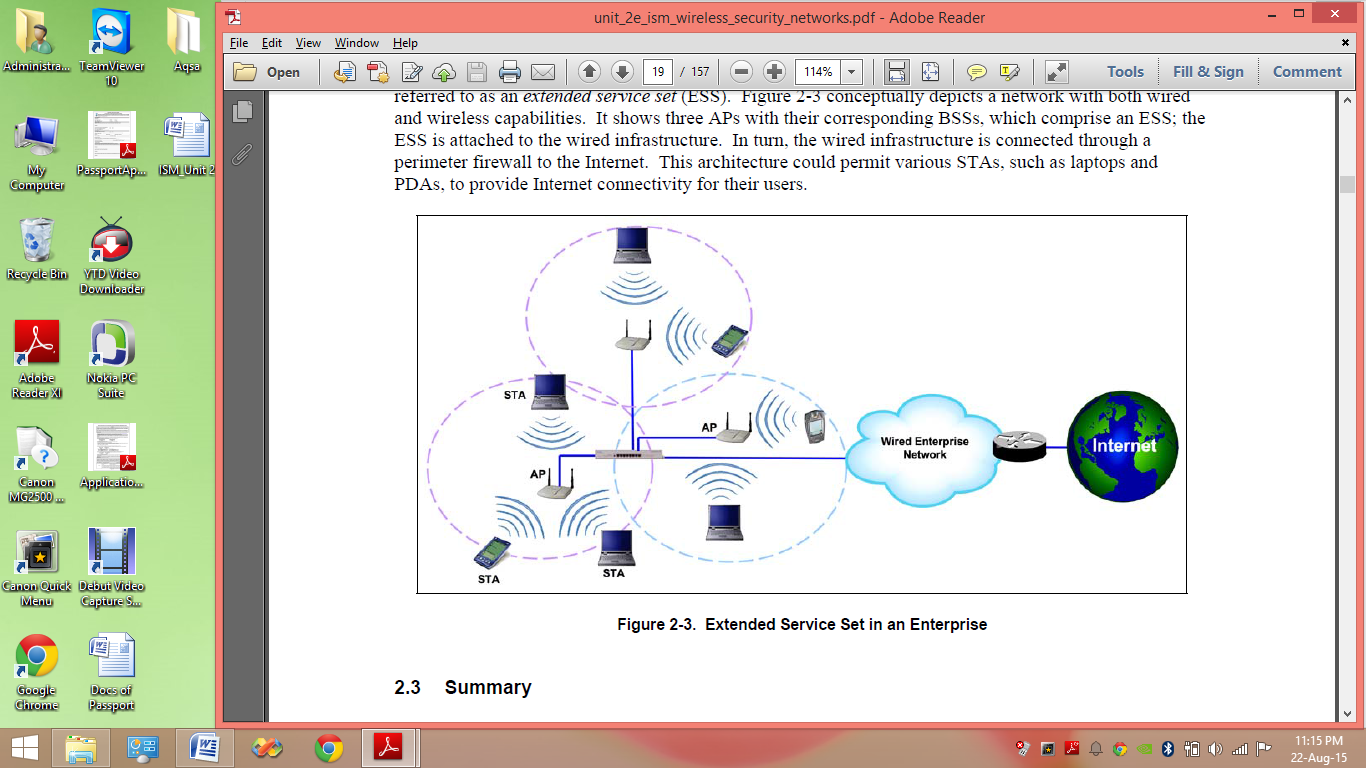
* In Figure 2-1, the STAs in the IBSS are a mobile phone, a laptop, and a PDA. IEEE 802.11 and its variants continue to increase in popularity; scanners, printers, digital cameras and other portable devices can also be STAs.
* The circular shape in Figure 2-1 depicts the IBSS. It is helpful to consider this as the radio frequency coverage area within which the stations can remain in communication.

**ii.Infrastructure Mode:**

* In infrastructure mode, an IEEE 802.11 WLAN comprises one or more Basic Service Sets (BSS), the basic building blocks of a WLAN. A *BSS* includes an AP and one or more STAs.
* The AP in a BSS connects the STAs to the DS. The DS is the means by which STAs can communicate with the organization’s wired LANs and external networks such as the Internet.
* The IEEE 802.11 infrastructure mode is depicted in Figure 2-2.



* The DS and use of multiple BSSs and their associated APs allow for the creation of wireless networks of arbitrary size and complexity. In the IEEE 802.11 specification, this type of multi-BSS network is referred to as an *extended service set* (ESS).
* Figure 2-3 conceptually depicts a network with both wired and wireless capabilities.
* It shows three APs with their corresponding BSSs, which comprise an ESS; the ESS is attached to the wired infrastructure.
* In turn, the wired infrastructure is connected through a perimeter firewall to the Internet.
* This architecture could permit various STAs, such as laptops and PDAs, to provide Internet connectivity for their users.



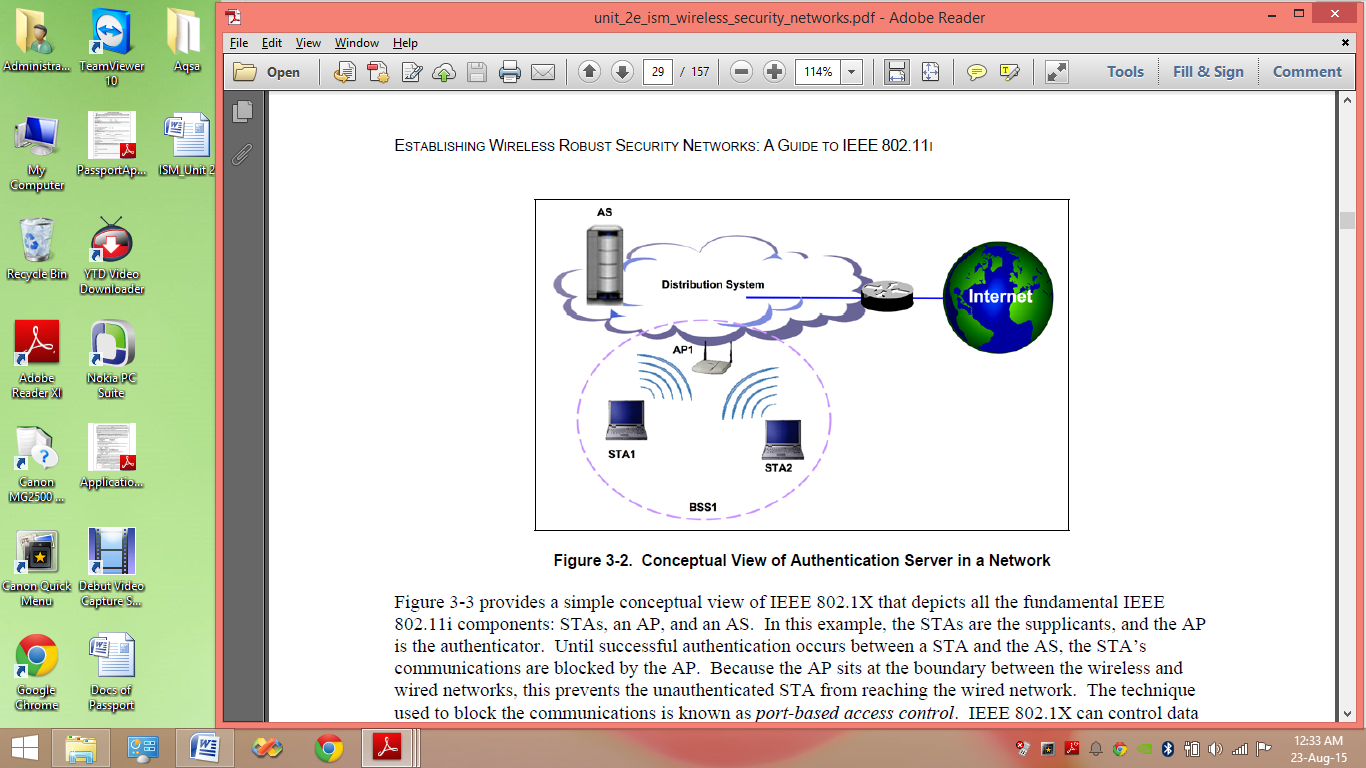
**Q.27. What are the various types of authentic methods implemented in IEEE 802.11 security?**

**Ans:**

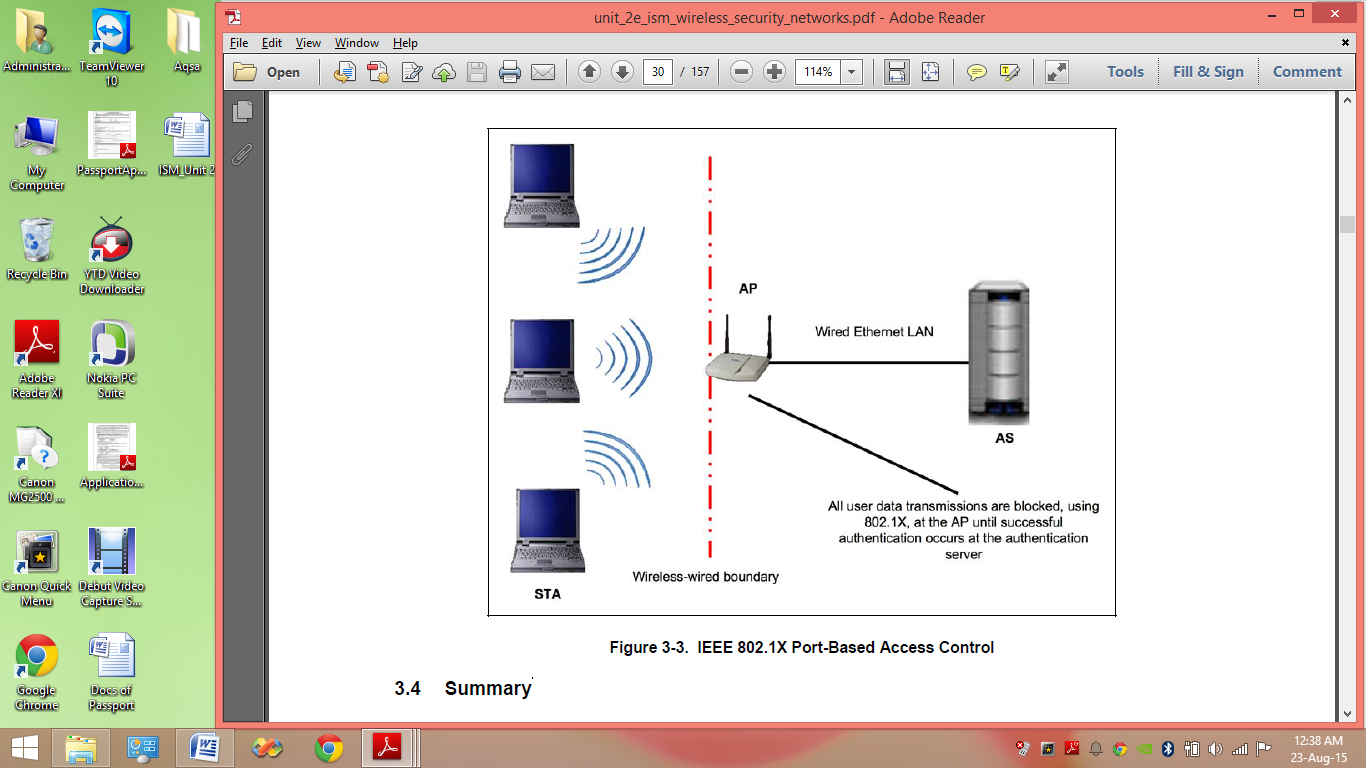
**Q.28. Write short note on IEEE 802.11i security.**

**Ans:**

* The IEEE 802.11i standard is the sixth amendment to the baseline IEEE 802.11 standards. It includes many security enhancements that leverage mature and proven security technologies.
* For example, IEEE 802.11i references the Extensible Authentication Protocol (EAP) standard, which is a means for providing mutual authentication between STAs and the WLAN infrastructure, as well as performing automatic cryptographic key distribution.
* EAP is a standard developed by the Internet Engineering Task Force (IETF).20. IEEE 802.11i employs accepted cryptographic practices, such as generating cryptographic checksums through hash message authentication codes (HMAC).
* The IEEE 802.11i specification introduces the concept of a Robust Security Network (RSN).
* An RSN is defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA). An RSNA is a logical connection between communicating IEEE 802.11 entities established through the IEEE 802.11i key management scheme, called the 4-Way Handshake, which is a protocol that validates that both entities share a pairwise master key (PMK), synchronizes the installation of temporal keys, and confirms the selection and configuration of data confidentiality and integrity protocols.
* The entities obtain the PMK in one of two ways—either the PMK is already configured on each device, in which case it is called a pre-shared key (PSK), or it is distributed as a side effect of a successful EAP authentication instance, which is a component of IEEE 802.1X port-based access control.
* The PMK serves as the basis for the IEEE 802.11i data confidentiality and integrity protocols that provide enhanced security over the flawed WEP. Most large enterprise deployments of RSN technology will use IEEE 802.1X and EAP rather than PSKs because of the difficulty of managing PSKs on numerous devices.
* WLAN connections employing ad hoc mode, which typically involve only a few STAs, are more likely to use PSKs.
* The IEEE 802.1X standard defines several terms related to authentication. The ***authenticator***is an entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.
* For example, the AP in Figure 3-2 serves as an authenticator.

****

* The ***supplicant*** is the entity being authenticated. The STA may be viewed as a supplicant.
* The ***authentication serve****r* (AS) is an entity that provides an authentication service to an authenticator.
* Figure 3-3 provides a simple conceptual view of IEEE 802.1X that depicts all the fundamental IEEE 802.11i components: STAs, an AP, and an AS.

****

* In this example, the STAs are the supplicants, and the AP is the authenticator. Until successful authentication occurs between a STA and the AS, the STA’s communications are blocked by the AP.
* Because the AP sits at the boundary between the wireless and wired networks, this prevents the unauthenticated STA from reaching the wired network. The technique used to block the communications is known as *port-based access control*.
* IEEE 802.1X can control data flows by distinguishing between EAP and non-EAP frames, then passing EAP frames through an uncontrolled port and non-EAP frames through a controlled port, which can block access.
* IEEE 802.11i extends this to block the AP’s communication until keys are in place as well. Thus, the IEEE 802.11i extensions prevent a rogue access point from exchanging anything but EAP traffic with the STA’s host.

**Q.29. Write short note on the following:**

**1.Server Backup Procedures**

**2.Recovering From a Security Compromise**

**3.Security Testing Servers**

**Ans:**

1. **Server Backup Procedures:**

* One of the most important functions of a Web server administrator is to maintain the integrity of the data on the Web server. This is important because Web servers are often some of the most exposed and vital servers on an organization’s network.
* There are two principal components to backing up data on a Web server: regular backup of the data and OS on the Web server, and maintenance of a separate protected authoritative copy of the organization’s Web content.

**i.Web Server Backup Policies and Strategies:**

* The Web server administrator needs to perform backups of the Web server on a regular basis for several reasons.
* A Web server could fail as a result of a malicious or unintentional act or a hardware or software failure.
* In addition, Federal agencies and many other organizations are governed by regulations on the backup and archiving of Web server data.
* Web server data should also be backed up regularly for legal and financial reasons. All organizations need to create a Web server data backup policy.
* Three main factors influence the contents of this policy:

􀀟 Legal requirements

􀂃 Applicable laws and regulations (Federal, state, and international)

􀂃 Litigation requirements

􀀟 Mission requirements

􀂃 Contractual

􀂃 Accepted practices

􀂃 Criticality of data to organization

􀀟 Organizational guidelines and policies.

**ii.Maintain a Test Web Server:**

* Most organizations will probably wish to maintain a test or development Web server.
* Ideally, this server should have hardware and software identical to the production or live Web server and be located on an internal network segment (intranet) where it can be fully protected by the organization’s perimeter network defenses.
* Although the cost of maintaining an additional Web server is not inconsequential, having a test Web server offers numerous advantages:
* It provides a platform to test new patches and service packs prior to application on the production Web server.
* It provides a development platform for the Webmaster and Web server administrator to develop and test new content and applications.
* It provides a platform to test configuration settings before applying them to production Web servers.

**iii.Maintain an Authoritative Copy of Organizational Web Content:**

* All organizations should maintain an authoritative (i.e., verified and trusted) copy of their public Web sites on a host that is inaccessible to the Internet. This is a supplement to, but not replacement for, an appropriate backup policy.
* For simple, relatively static Web sites, this could be as simple as a copy of the Web site on a read-only medium (e.g., Compact Disc-Recordable [CD-R]).
* However, for most organizations, the authoritative copy of the Web site is maintained on a secure host.
* This host is usually located behind the organization’s firewall on the internal network and not on the DMZ.
* The purpose of the authoritative copy is to provide a means of restoring information on the public Web server if it is compromised as a result of an accident or malicious action.
* This authoritative copy of the Web site allows an organization to rapidly recover from Web site integrity breaches (e.g., defacement).

**2.Recovering From a Security Compromise:**

* Most organizations eventually face a successful compromise of one or more hosts on their network. The first step in recovering from a compromise is to create and document the required policies and procedures for responding to successful intrusions *before* an intrusion.
* The response procedures should outline the actions that are required to respond to a successful compromise of the Web server and the appropriate sequence of these actions (sequence can be critical).
* Most organizations already have a dedicated incident response team in place, which should be contacted immediately when there is suspicion or confirmation of a compromise.
* In addition, the organization may wish to ensure that some of its staff are knowledgeable in the fields of computer and network forensics.
* A Web server administrator should follow the organization’s policies and procedures for incident handling, and the incident response team should be contacted for guidance before the organization takes any action after a suspected or confirmed security compromise.
* Examples of steps commonly performed after discovering a successful compromise are as follows:

􀀟 Report the incident to the organization’s computer incident response capability.

􀀟 Isolate the compromised systems or take other steps to contain the attack so that

additional information can be collected.

􀀟 Consult expeditiously, as appropriate, with management, legal counsel, and law

enforcement.

􀀟 Investigate similar80 hosts to determine if the attacker also has compromised other

systems.

􀀟 Analyze the intrusion, including—

* The current state of the server, starting with the most ephemeral data (e.g., current network connections, memory dump, files time stamps, logged in users)
* Modifications made to the system’s software and configuration
* Modifications made to the data
* Tools or data left behind by the attacker
* System, intrusion detection, and firewall log files.

􀀟 Restore the system.

* Either install a clean version of the OS, applications, necessary patches, and Web content; or restore the system from backups (this option can be more risky because the backups may have been made after the compromise, and restoring from a compromised backup may still allow the attacker access to the system).
* Disable unnecessary services.
* Apply all patches.
* Change all passwords (including on uncompromised hosts, if their passwords are believed to have been seen by the compromised host, or if the same passwords are used on other hosts).
* Reconfigure network security elements (e.g., firewall, router, IDPS) to provide additional protection and notification.

􀀟 Test system to ensure security.

􀀟 Reconnect system to network.

􀀟 Monitor system and network for signs that the attacker is attempting to access the

system or network again.

􀀟 Document lessons learned.

* Based on the organization’s policy and procedures, system administrators should decide whether to reinstall the OS of a compromised system or restore it from a backup. Factors that are often considered include the following:

􀀟 Level of access that the attacker gained (e.g., root, user, guest, system)

􀀟 Type of attacker (internal or external)

􀀟 Purpose of compromise (e.g., Web page defacement, illegal software repository,

platform for other attacks)

􀀟 Method used for the system compromise

􀀟 Actions of the attacker during and after the compromise (e.g., log files, intrusion

detection reports)

􀀟 Duration of the compromise

􀀟 Extent of the compromise on the network (e.g., the number of hosts compromised)

􀀟 Results of consultation with management and legal counsel.

* The lower the level of access gained by the intruder and the more the Web server administrator understands about the attacker’s actions, the less risk there is in restoring from a backup and patching the vulnerability.
* For incidents in which there is less known about the attacker’s actions and/or in which the attacker gains high-level access, it is recommended that the OS and applications be reinstalled from the manufacturer’s original distribution media and that the Web server data be restored from a known good backup.
* If legal action is pursued, system administrators need to be aware of the guidelines for handling a host after a compromise. Consult legal counsel and relevant law enforcement authorities as appropriate.

**3.Security Testing Servers :**

* Periodic security testing of public Web servers is critical. Without periodic testing, there is no assurance that current protective measures are working or that the security patch applied by the Web server administrator is functioning as advertised.
* Although a variety of security testing techniques exists, vulnerability scanning is the most common. Vulnerability scanning assists a Web server administrator in identifying vulnerabilities and verifying whether the existing security measures are effective.
* Penetration testing is also used, but it is used less frequently and usually only as part of an overall penetration test of the organization’s network.

**i.Vulnerability Scanning:**

* Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfigurations of hosts. Many vulnerability scanners also provide information about mitigating discovered vulnerabilities.
* Vulnerability scanners attempt to identify vulnerabilities in the hosts scanned. Vulnerability scanners can help identify out-of-date software versions, missing patches, or system upgrades, and they can validate compliance with or deviations from the organization’s security policy.
* To accomplish this, vulnerability scanners identify OSs and major software applications running on hosts and match them with known vulnerabilities in their vulnerability databases.
* However, vulnerability scanners have some significant weaknesses. Generally, they identify only surface vulnerabilities and are unable to address the overall risk level of a scanned Web server.
* Although the scan process itself is highly automated, vulnerability scanners can have a high false positive error rate (reporting vulnerabilities when none exist). This means an individual with expertise in Web server security and administration must interpret the results.
* Furthermore, vulnerability scanners cannot generally identify vulnerabilities in custom code or applications.
* Vulnerability scanners rely on periodic updating of the vulnerability database to recognize the latest vulnerabilities. Before running any scanner, Web server administrators should install the latest updates to its vulnerability database.
* Some databases are updated more regularly than others (the frequency of updates should be a major consideration when choosing a vulnerability scanner).
* Vulnerability scanners are often better at detecting well-known vulnerabilities than more esoteric ones because it is impossible for any one scanning product to incorporate all known vulnerabilities in a timely manner.
* In addition, manufacturers want to keep the speed of their scanners high (the more vulnerabilities detected, the more tests required, which slows the overall scanning process).
* Therefore, vulnerability scanners may be less useful to Web server administrators operating less popular Web servers, OSs, or custom-coded applications.
* Vulnerability scanners provide the following capabilities:

􀀟 Identifying active hosts on a network

􀀟 Identifying active services (ports) on hosts and which of these are vulnerable

􀀟 Identifying applications and banner grabbing

􀀟 Identifying OSs

􀀟 Identifying vulnerabilities associated with discovered OSs and applications

􀀟 Testing compliance with host application usage/security policies.

**Q.30. What is penetration testing?**

**Ans:**

* “Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation” [NISS99].
* The purpose of penetration testing is to exercise system protections (particularly human response to attack indications) by using common tools and techniques developed by attackers.
* This testing is highly recommended for complex or critical systems. Penetration testing can be an invaluable technique to any organization's information security program.
* However, it is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems. At a minimum, it may slow the organization's network response time because of network mapping and vulnerability scanning.
* Furthermore, the possibility exists that systems may be damaged or rendered inoperable in the course of penetration testing. Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated.

Penetration testing does offer the following benefits [NIST02b]:

􀀟 Tests the network using the same methodologies and tools employed by attackers

􀀟 Verifies whether vulnerabilities exist

􀀟 Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can

be exploited iteratively to gain greater access

􀀟 Demonstrates that vulnerabilities are not purely theoretical

􀀟 Provides the “realism” necessary to address security issues

􀀟 Allows for testing of procedures and susceptibility of the human element to social

engineering.

The goals of penetration tests are:

1. Determine feasibility of a particular set of attack [vectors](https://en.wikipedia.org/wiki/Vector_(malware))
2. Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
3. Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
4. Assess the magnitude of potential business and operational impacts of successful attacks
5. Test the ability of network defenders to detect and respond to attacks
6. Provide evidence to support increased investments in security personnel and technology

**Q.31. Write a note on Identification & Authentication Technologies.**

**Ans:**

Identification is the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim.

1.**I&A Based on Something the User Knows:**

* The most common form of I&A is a user ID coupled with a password. This technique is based solely on something the user knows. There are other techniques besides conventional passwords that are based on knowledge, such as knowledge of a cryptographic key.

**Passwords:**

Password systems work by requiring the user to enter a user ID and password (or passphrase or personal identification number). The system compares the password to a previously stored password for that user ID. If there is a match, the user is authenticated and granted access.

**Cryptographic Keys:**

Although the authentication derived from the knowledge of a cryptographic key may be based entirely on something the user knows, it is necessary for the user to also possess (or have access to) something that can perform the cryptographic computations, such as a PC or a smart card. However, it is possible to implement these types of protocols without using a smart token.

**2.I&A Based on Something the User Possesses:**

* Although some techniques are based solely on something the user possesses, most of the techniques are combined with something the user knows. This combination can provide significantly stronger security than either something the user knows or possesses alone.
* Objects that a user possesses for the purpose of I&A are called tokens. This technique divides tokens into two categories: memory tokens and smart tokens.

**i.Memory Tokens:**

Memory tokens store, but do not process, information. Special reader/writer devices control the writing and reading of data to and from the tokens. The most common type of memory token is a magnetic striped card, in which a thin stripe of magnetic material is affixed to the surface of a card (e.g., as on the back of credit cards). A common application of memory tokens for authentication to computer systems is the automatic teller machine (ATM) card. This uses a combination of something the user possesses (the card) with something the user knows (the PIN).

**ii.Smart Tokens:**

A smart token expands the functionality of a memory token by incorporating one or more integrated circuits into the token itself. When used for authentication, a smart token is another example of authentication based on something a user possesses (i.e., the token itself). A smart token typically requires a user also to provide something the user knows (i.e., a PIN or password) in order to "unlock" the smart token for use.

**3. I&A Based on Something the User Is:**

* Biometric authentication technologies use the unique characteristics (or attributes) of an individual to authenticate that person's identity. These include physiological attributes (such as fingerprints, hand geometry, or retina patterns) or behavioral attributes (such as voice patterns and hand-written signatures).
* Biometric authentication technologies based upon these attributes have been developed for computer log-in applications. Biometric authentication is technically complex and expensive, and user acceptance can be difficult.
* However, advances continue to be made to make the technology more reliable, less costly, and more user-friendly.
* Biometric systems can provide an increased level of security for computer systems, but the technology is still less mature than that of memory tokens or smart tokens.
* Imperfections in biometric authentication devices arise from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes.
* These may change, depending on various conditions. For example, a person's speech pattern may change under stressful conditions or when suffering from a sore throat or cold.

**Q.32. List and explain the important implementation issues for I&A systems.**

**Ans:**

Some of the important implementation issues for I&A systems include administration, maintaining authentication, and single log-in.

**1.Administration:**

* Administration of authentication data is a critical element for all types of authentication systems. The administrative overhead associated with I&A can be significant. I&A systems need to create, distribute, and store authentication data.
* For passwords, this includes creating passwords, issuing them to users, and maintaining a password file. Token systems involve the creation and distribution of tokens/PINs and data that tell the computer how to recognize valid tokens/PINs. For biometric systems, this includes creating and storing profiles.
* The administrative tasks of creating and distributing authentication data and tokens can be a substantial. Identification data has to be kept current by adding new users and deleting former users.
* If the distribution of passwords or tokens is not controlled, system administrators will not know if they have been given to someone other than the legitimate user.

**2.Maintaining Authentication:**

* It is also possible for someone to use a legitimate user's account after log-in." 2 Many computer systems handle this problem by logging a user out or locking their display or session after a certain period of inactivity.
* However, these methods can affect productivity and can make the computer less user-friendly.

**3.Single Log-in:**

* From an efficiency viewpoint, it is desirable for users to authenticate themselves only once and then to be able to access a wide variety of applications and data available on local and remote systems, even if those systems require users to authenticate themselves. This is known as single log-in.
* If the access is within the same host computer, then the use of a modern access control system (such as an access control list) should allow for a single log-in.
* If the access is across multiple platforms, then the issue is more complicated.
* There are three main techniques that can provide single log-in across multiple computers:
* host-to-host authentication,
* authentication servers, and
* user-to-host authentication.

**Q.33. What are various criteria used by the system to determine if a request for access will be granted?**

**Ans:**

**Access Criteria:**

* In deciding whether to permit someone to use a system resource logical access controls examine whether the user is authorized for the type of access requested.
* The system uses various criteria to determine if a request for access will be granted. They are typically used in some combination. Many of the advantages and complexities involved in implementing and managing access control are related to the different kinds of user accesses supported.

**1.Identity:**

* It is probably fair to say that the majority of access controls are based upon the identity of the user (either human or process), which is usually obtained through identification and authentication (I&A).
* The identity is usually unique, to support individual accountability, but can be a group identification or can even be anonymous.

**2.Roles:**

* Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access.
* Examples of roles include data entry clerk, purchase officer, project leader, programmer, and technical editor.
* Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role.
* An individual may be authorized for more than one role, but may be required to act in only a single role at a time.
* Changing roles may require logging out and then in again, or entering a role-changing command.

**3.Location:**

* Access to particular system resources may also be based upon physical or logical location.
* For example, in a prison, all users in areas to which prisoners are physically permitted may be limited to read-only access. Changing or deleting is limited to areas to which prisoners are denied physical access.
* The same authorized users (e.g., prison guards) would operate under significantly different logical access controls, depending upon their physical location.
* Similarly, users can be restricted based upon network addresses (e.g., users from sites within a given organization may be permitted greater access than those from outside).

**4.Time:**

* Time-of-day or day-of-week restrictions are common limitations on access.
* For example, use of confidential personnel files may be allowed only during normal working hours - and may be denied before 8:00 a.m. and after 6:00 p.m. and all day during weekends and holidays.

**5.Transaction:**

* Another approach to access control can be used by organizations handling transactions (e.g., account inquiries). Phone calls may first be answered by a computer that requests that callers key in their account number and perhaps a PIN.
* Some routine transactions can then be made directly, but more complex ones may require human intervention.
* In such cases, the computer, which already knows the account number, can grant a clerk, for example, access to a particular account for the duration of the transaction. When completed, the access authorization is terminated.
* This means that users have no choice in which accounts they have access to, and can reduce the potential for mischief.
* It also eliminates employee browsing of accounts (e.g., those of celebrities or their neighbors) and can thereby heighten privacy.

**6.Service Constraints:**

* Service constraints refer to those restrictions that depend upon the parameters that may arise during use of the application or that are preestablished by the resource owner/manager.
* For example, a particular software package may only be licensed by the organization for five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorized to use the application.
* Another type of service constraint is based upon application content or numerical thresholds.
* For example, an ATM machine may restrict transfers of money between accounts to certain dollar limits or may limit maximum ATM withdrawals to $500 per day. Access may also be selectively permitted based on the type of service requested.
* For example, users of computers on a network may be permitted to exchange electronic mail but may not be allowed to log in to each others' computers.

**7.Common Access Modes:**

* In addition to considering criteria for when access should occur, it is also necessary to consider the types of access, or access modes. The concept of access modes is fundamental to access control.
* Common access modes, which can be used in both operating or application systems, include the following:

**Read access** provides users with the capability to view information in a system resource (such as a file, certain records, certain fields, or some combination thereof), but not to alter it, such as delete from, add to, or modify in any way.

**Write access** allows users to add to, modify, or delete information in system resources (e.g., files, records, programs). Normally user have read access to anything they have write access to.

**Execute** privilege allows users to run programs.

**Delete access** allows users to erase system resources (e.g., files, records, fields, programs).