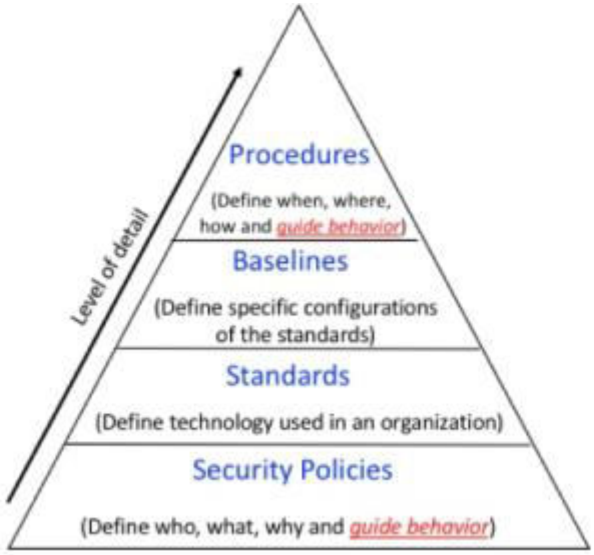
#132, AECS Layout, IT Park Road, Kundalahalli, Bangalore 560 037
T: +91 80 28524466/77

CMR
INSTITUTE
OF TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

INFORMATION AND NETWORK SECURITY
IAT – 1 SOLUTION

1 (a) With a block schematic diagram explain how policies, standards, practices, procedures and guidelines are related? [6]


Level of detail
Procedures
(Define when, where, how and guide behavior)
Baselines
(Define specific configurations of the standards)
Standards
(Define technology used in an organization)
Security Policies
(Define who, what, why and guide behavior)

Policies are put in place to support the mission, vision, and strategic planning of an organization. The **mission** of an organization is a written statement of an organization's purpose. The **vision** of an organization is a written statement about the organization's goals—where will The organization be in five years? In ten? Strategic planning is the process of moving the organization toward its vision.The meaning of the term **security policy** depends on the context in which it is used. Governmental agencies view security policy in terms of national security and national policies to deal with foreign states. A security policy can also communicate a credit card agency's method for processing credit card numbers. In general, a security policy is a set of rules that protect an organization's assets. An **information security policy** provides rules for the protection of the information assets of the organization.

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

For a policy to be effective and thus legally enforceable, it must meet the following criteria:
Dissemination (distribution)—The organization must be able to demonstrate that the policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution
Review (reading)—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recording the policy in English and other languages.
Comprehension (understanding)—The organization must be able to demonstrate the employee understood the requirements and content of the policy. Common techniques

include quizzes and other assessments.
Compliance (agreement)—The organization must be able to demonstrate that the
employee agrees to comply with the policy, through act or affirmation. Common techniques include logon banners which require a specific action (mouse click or keystroke)to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
Uniform enforcement—The organization must be able to demonstrate that the policy
has been uniformly enforced, regardless of employee status or assignment.

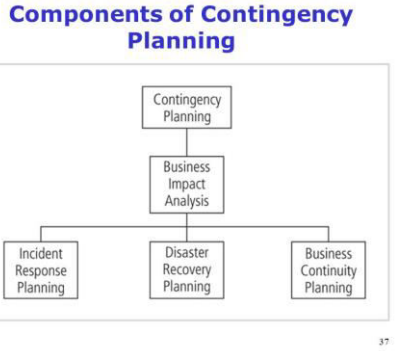
(b) What are the three components of the CIA triangle? What are they used for? [4]

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.
Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades.

2 What are the components of contingency planning? Describe briefly with diagram the important steps involved in the recovery process after the extent of damage caused by an incident has been assessed? [10]


Components of Contingency Planning

Contingency Planning
Business Impact Analysis
Incident Response Planning
Disaster Recovery Planning
Business Continuity Planning

37

An **incident** is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability. An **incident response (IR) plan** addresses the identification, classification, response, and recovery from an incident. A **disaster recovery (DR) plan** addresses the preparation for and recovery from a disaster, whether natural or man-made. A **business continuity (BC) plan** ensures that critical business functions continue if a catastrophic incident or disaster occurs. The primary functions of these three types of planning are as follows:
The IR plan focuses on immediate response, but if the attack escalates or is disastrous
(e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery
and the BC plan.

The DR plan typically focuses on restoring systems at the original site after disasters
occur, and as such is closely associated with the BC plan.

The BC plan occurs concurrently with the DR plan when the damage is major or
ongoing, requiring more than simple restoration of information and information
resources. The BC plan establishes critical business functions at an alternate site.

RECOVERY

Full recovery from an incident requires that you perform the following:

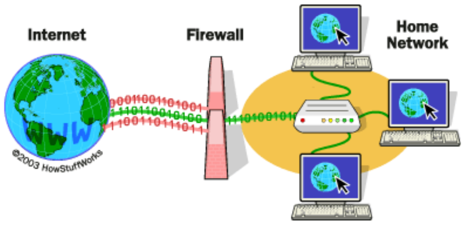
1. Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
2. Address the safeguards that failed to stop or limit the incident, or were missing from the system in the first place. Install, replace, or upgrade them.
3. Evaluate monitoring capabilities (if present). Improve their detection and reporting methods, or simply install new monitoring capabilities.
4. Restore the data from backups. See the Technical Details boxes on the following topics for more information:
(1) data storage and management,
(2) system backups and recovery,
(3) redundant array of independent disks (RAID).
Restoration requires the IR team
to understand the backup strategy used by the organization, restore the data contained in backups, and then recreate the data that were created or modified since the last backup.

5. Restore the services and processes in use. Compromised services and processes must be examined, cleaned, and then restored. If services or processes were interrupted during the process of regaining control of the systems, they need to be brought back online.

6. Continuously monitor the system. If an incident happened once, it can easily happen again. Just because the incident is over doesn't mean the organization is in the clear. Hackers frequently boast of their abilities in chat rooms and dare their peers to match their efforts. If word gets out, others may be tempted to try their hands at the same or different attacks. It is therefore important to maintain vigilance during the entire IR process.
7. Restore the confidence of the organization's communities of interest. It may be advisable to issue a short memorandum that outlines the incident and assures everyone that it was handled and the damage controlled. If the incident was minor, say so. If the incident was major or severely damaged the systems or data, reassure the users that they can expect operations to return to normal shortly. The objective is not to placate or lie, but to prevent panic or confusion from causing additional disruptions to the operations of
the organization.

3 (a) What is a firewall? Show the working of a screened host and dual homed firewall with diagram [7]

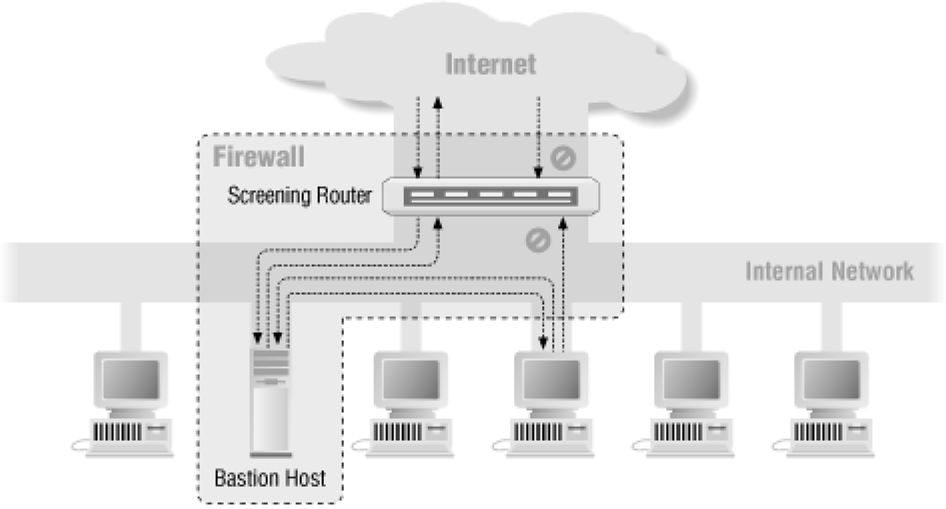
A **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.



SCREENED HOST

Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy. The application proxy examines an application layer protocol, such as HTTP,
and performs the proxy services. This separate host is often referred to as a **bastion host**; it can be a rich target for external attacks and should be very thoroughly secured. Even
though the bastion host/application proxy actually contains only cached copies of the internal Web documents, it can still present a promising target, because compromise of the bastion host can disclose the configuration of internal networks and possibly provide attackers with internal

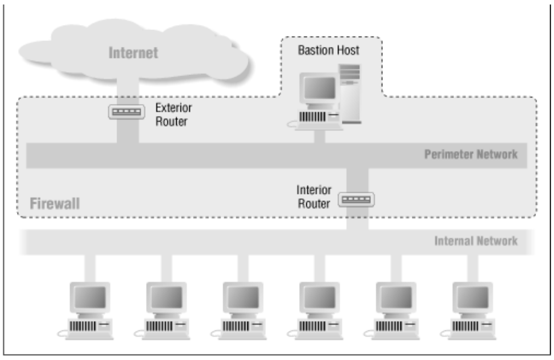
information. Since the bastion host stands as a sole defender on the network perimeter, it is commonly referred to as the **sacrificial host**.



DUAL HOMED HOST

When this architectural approach is used, the bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration.

One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With two NICs, all traffic *must* physically go through the firewall to move between the internal and external networks. Implementation of this architecture often makes use of NAT. As described earlier in this chapter, NAT is a method of mapping real, valid, external IP addresses to special ranges of no routable internal IP addresses.



(b) What are virtual private networks and its characteristics? Name the two modes of VPN[3]

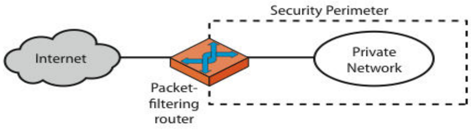
A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location.

Encapsulation
Encryption
Authentication

2 modes:
Transport mode
Tunnel mode

4 (a) Explain the categories of firewall based on the processing modes and depict it using OSI layer? [8]

PACKET FILTERING



(a) Packet-filtering router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)
- Address Restrictions

◉ Static packet filtering firewall

Static filtering requires that the filtering rules be developed and installed within the firewall.

◉ Dynamic packet filtering

Dynamic packet filtering filters packets based on:

◉ Administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model.

◉ Advantages:

- Simplicity
- Transparency to users
- High speed

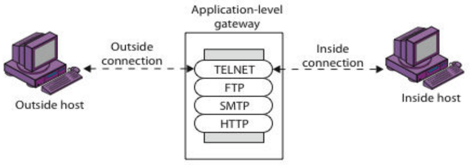
◉ Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication

◉ Possible attacks and appropriate countermeasures

- IP address spoofing
- Source routing attacks

APPLICATION LEVEL



(b) Application-level gateway

Has full access to protocol user requests service from proxy ,proxy validates request as legal then actions request and returns result to user .
Need separate proxies for each service
E.g., SMTP (E-Mail)
NNTP (Net news)
DNS (Domain Name System)
NTP (Network Time Protocol)
custom services generally not supported

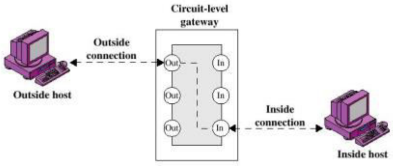
Advantages:

- Higher security than packet filters
- Only need to scrutinize a few allowable applications

Disadvantages:

- Additional processing overhead on each connection (gateway as splice point)

CIRCUIT GATEWAY



- Circuit-level Gateway

  It does not control the traffic flow between one network and the other rather

  It prevents direct connection between one network and the other .
- Tunnels
- Allows only authorized traffic
  - An example is the SOCKS package

MAC LAYER FIREWALL

operates on OSI Layer 2 and bases its filtering decision on devices' MAC/NIC addresses MAC addresses of specific hosts are included in ACL,allowing only specific packets to be sent to/from these hosts and blocking others not as widely used as other types of firewalls **only used within a single-authority LAN - MAC addresses get stripped off on each 'hop'.**

HYBRID

Hybrid Firewall – combines elements of other
types of firewalls

- Typically implies the use of two or more separate firewall devices.
- Allows an organization to make security improvements without completely replacing its existing firewalls

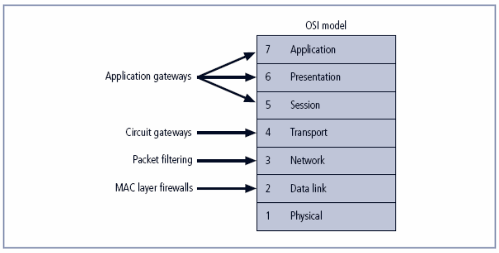


FIGURE 6-5 Firewall Types and the OSI Model

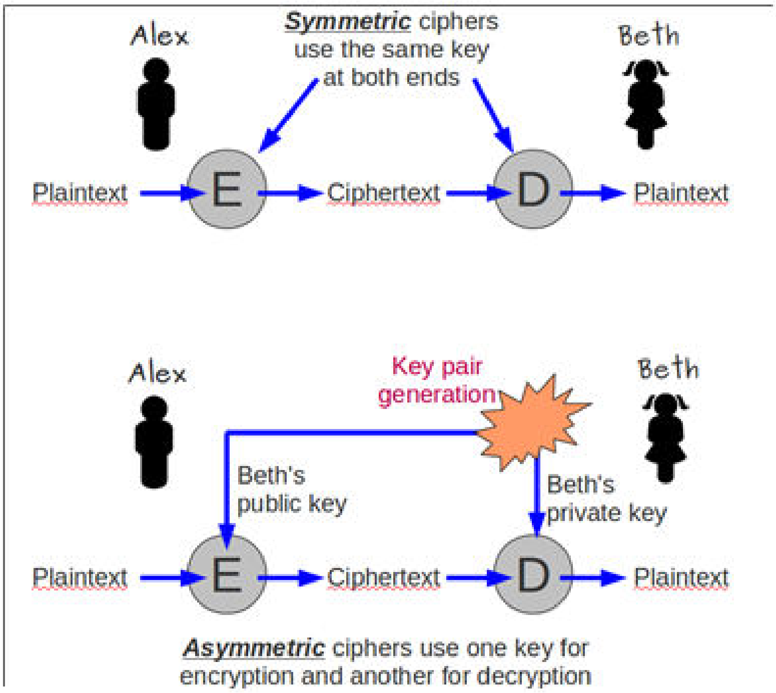
(b) How is static filtering different from dynamic filtering of packets? [2]

In a static filter, each packet is independently evaluated, with no reference to any preceding packets that may have passed in either direction. A static filter may also be referred to as a *static NAT* or *passive screening firewall*..

In a dynamic filter, the decision on whether to pass a packet depends on what packets have already been through the firewall.

5 (a) What is an encryption? Discuss the symmetric and asymmetric encryption methods with neat diagram ?[5]

Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties.



\

Symmetric-key algorithms are algorithms for **cryptography** that use the same **cryptographic** keys for both **encryption** of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys.

Public key **cryptography**, or **asymmetric cryptography**, is any **cryptographic** system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

(b) List out the elements of cryptosystems and explain ceaser and transposition cipher technique.[5]

Cryptology is a broader subject, consisting of two branches: cryptography, the science of creating secure *cryptosystems* for converting data into a form that is unintelligible to unauthorized persons, and cryptanalysis, the science of 'attacking' cryptosystems in order to 'crack' them or at least discover their weaknesses. The aim of cryptography is to convert any data in its original form, called the *plaintext*, into an incomprehensible form, known as the *cipher text*. This process is called *encryption*. The reverse process of recovering the plaintext from the cipher text is called *decryption*. In popular writing, one often finds the (incorrect) terms 'encoding' and 'decoding', but technically these have quite different meanings and should not be used in the present context.

CEASER CIPHER

a letter in the alphabet with the letter three values to the right. Or you can substitute one bit for another bit that is four places to its left. A three-character substitution to the right results in the following transformation of the standard English alphabet:

Initial alphabet yields ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption alphabet DEFGHIJKLMNOPQRSTUVWXYZABC

TRANSPOSITION CIPHER
Key pattern: 1 4, 2 8, 3 1, 4 5, 5 7, 6 2, 7 6, 8 3
In this key, the bit or byte (character) in position 1 (with position 1 being at the far right) moves to position 4 (counting from the right), and the bit or byte in position 2 moves to position 8, and so on. This is similar to another newspaper puzzle favorite: the Word Jumble, as illustrated in Figure 8-3.
The following rows show the numbering of bit locations for this key; the plaintext message 00100101011010111001010101010100, which is broken into 8-bit blocks for clarity; and

the ciphertext that is produced when the transposition key depicted above is applied to the plaintext:
Bit locations: 87654321 87654321 87654321 87654321
Plaintext 8-bit blocks: 00100101|01101011|10010101|01010100
Ciphertext: 00001011|10111010|01001101|01100001

6 (a) Describe the terms: authentication, integrity, privacy, authorization, plaintext, steganography and non repudiation? [7]

Privacy: *Privacy* is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively

Authentication and authorization

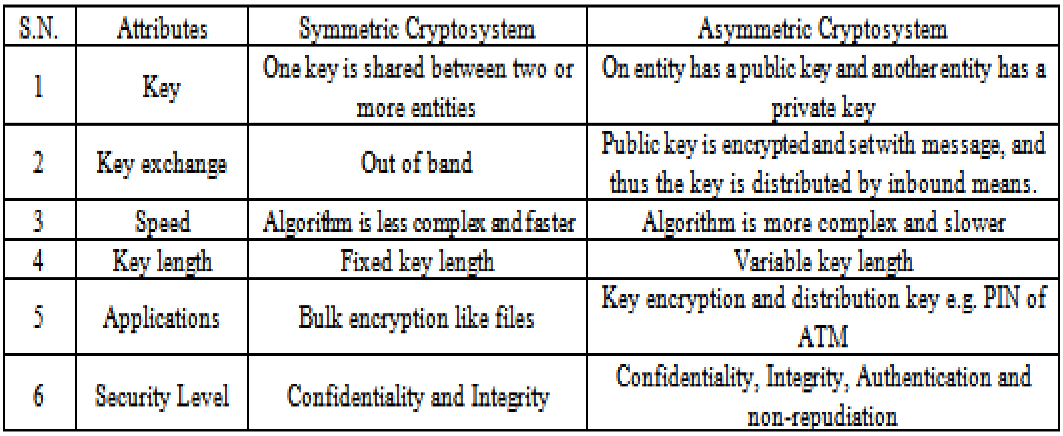
When you log on to a PC with a user name and password you are **authenticating**. **Authorization** is the process of verifying that you have access to something. Gaining access to a resource (e.g. directory on a hard disk) because the permissions configured on it allow you access is **authorization**

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

Nonrepudiation is the assurance that someone cannot deny something. Typically, **nonrepudiation** refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video

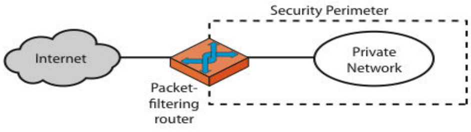
(b) Distinguish between symmetric and asymmetric encryption ?[3]



S.N.	Attributes	Symmetric Cryptosystem	Asymmetric Cryptosystem
1	Key	One key is shared between two or more entities	On entity has a public key and another entity has a private key
2	Key exchange	Out of band	Public key is encrypted and set with message, and thus the key is distributed by inbound means.
3	Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
4	Key length	Fixed key length	Variable key length
5	Applications	Bulk encryption like files	Key encryption and distribution key e.g. PIN of ATM
6	Security Level	Confidentiality and Integrity	Confidentiality, Integrity, Authentication and non-repudiation

7 Draw a schematic diagram of a packet filtering router used as a firewall and explain its function using a sample firewall rule? [10]

PACKET FILTERING



(a) Packet-filtering router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)
- Address Restrictions

- Static packet filtering firewall

  Static filtering requires that the filtering rules be developed and installed within the firewall.
- Dynamic packet filtering

  Dynamic packet filtering filters packets based on:
- Administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model.
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication
- Possible attacks and appropriate countermeasures
  - IP address spoofing
  - Source routing attacks

8 RULES

Rule Set 1: Responses to internal requests are allowed.
Rule Set 2:The firewall device is never accessible directly from the public network
Rule Set 3: All traffic from the trusted network is allowed out.
Rule Set 4: The rule set for the Simple Mail Transport Protocol (SMTP) data
the packets governed by this rule are allowed to pass through the firewall,but are all routed to a well-configured SMTP gateway.
Rule Set 5: All Internet Control Message Protocol (ICMP) data should be denied. Pings, formally known as ICMP Echo requests, are used by internal systems administrators to ensure that clients and servers can communicate.
Rule Set 6: Telnet (terminal emulation) access to all internal servers from the public networks should be blocked. Though not used much in Windows environments,
Rule Set 7: When Web services are offered outside the firewall, HTTP traffic (and HTTPS traffic) should be blocked from the internal networks via the use of some form of proxy access or DMZ architecture.
Rule Set 8: The cleanup rule. As a general practice in firewall rule construction, if a request for a service is not explicitly allowed by policy, that request should be denied by a rule.