Perimeter security

- Intruders ⇒ An intruder is someone who tries to gain unauthorized access to computer system, network or data.
  * significant issue for networked systems is hostile or unwanted access
  * either via network or local
  * Each access type requires different security measures for effective protection

Classes of Intruders (Types of intruders)
There are three type

① Masquerader ② misfeasor ③ clandestine user
* varying level of competence.

- Types of intruders

1) Masqueraders : An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

2) Misfeasor : A legitimate user who accesses data programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges

3) clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to ~~suppress~~ suppress audit actions

*What is an intrusion ?

Any set of actions that attempts to compromise the confidentiality, integrity or availability of a computer resource

Intrusion are a big problem because they can lead to stolen information, damaged system, or even loss of control over the network.

To prevent intrusions, systems use security tools like firewalls and alarms to detect and stop unauthorized access

* Consequences of Intrusion.

Intruder attacks rang from benign (mild) to the serious. At the benign (mild) end of the scale there are many people who simply wish to explore internet and what is out there.

At the serious end, intruder may attemp following

* Read privileged data
* perform unauthorized modification to data
* disrupt the system settings

Why IDS ?

→ to protect data and system integrity

fact : can not be done with ordinary password and file security.

Intrusion Detection Systems (IDS)

* Intrusion detection is the process of identifying and responding to malicious activity targeted at resources
* IDS is a system designed to test / analyze network system traffic / events against a given set of parameters and alert / capture data when these thresholds are met
* IDS uses collected information and predefined knowledge-based system to reason about the possibility of an intrusion
* IDS also provides services to cop with intrusion such as giving alarms, activating programs to try to deal with intrusion, etc.

Functions of IDS

* An IDS detects attacks as soon as possibles and takes appropriate action
* An IDS does not usually take preventive measures when an attack is detected
* It is a reactive rather than a pro-active agent
* It plays a role of informant rather than a police officer

mathematical IDS remaining

Principles of Intrusion Detection systems

* An IDS must run unattended for extended periods of time
* The IDS must stay active and secure
* The IDS must be able to recognize unusual activity
* The IDS must operate without unduly affecting the system's activity
* The IDS must be configurable

Typical intrusion scenario

Information gathering -: find as much as info. as possible
- who is lookup and DNS zone transfers
- Normal browsing

↓

further information Gathering -:
- Ping sweeps, port scanning
- web server vulnerabilities
- version of application / services

↓

Attack -:
- start trying out different attacks
- try to find misconfigured running services
- passive Attack / Active attack

↓

Successful intrusion -: install own backdoors & delete log files
- replace existing services with own Trojan horses that have backdoor passwords or create own user accounts

↓

Fun and profit :- · Steal confidential information
- change the web-site for fun

Intrusion Techniques

- aim to gain access and/or increase privileges on a system
- basic attack methodology
  - target acquisition and information gathering
  - initial access
  - privilege escalation
- key goal often is to acquire passwords
- so then exercise access rights of owner

Password Guessing

* one of the most common attacks
* attacker knows a login (from email/web page)
* then attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info
  - exhaustively searching all possible passwords
* check by login or against stolen password file
* success depends on password chosen by user
* surveys show many users choose poorly

Password capture

* another attack involves password capture
  - watching over shoulder as password is entered
  - using a trojan horse program to collect
  - monitoring an insecure network login
    e.g telnet, FTP, web, email

. extracting recorded info after successful login (web history, last number dialed etc)
* using valid login / password can impersonate user
* users need to be educated to use suitable precautions / countermeasures

criteria	variable monitored	Event of interest	possible attack
definition	A specific data or condition being observed or tracked	A significant event that indicates potential threat or abnormal behavior	An action or behavior that indicate a threat or compromise
purpose	To track and gather data for analysis	To identify something unusal that needs attention	To spot possible threats or security issues
Example	Number of failed logins. network usage	A sudden jump in traffic, a strange login pattern	Hacking attempt, malware activity
Scope	A specific item or condition	A broader event that seems out of the ordinary	Something harmful or suspicious that might compromise security
Detection	Through tracking tools or logs	By noticing unusual patterns or actions	By recognizing harmful activities or attacks

Intrusion Detection

* Inevitably will have security failures
* so need also to detect instrusions so can
  - block if detected quickly
  - act as deterrent
  - collect info to improve security
* assume intruder will behave differently to an legitimate user
  - but will have imperfect distinction between

Or

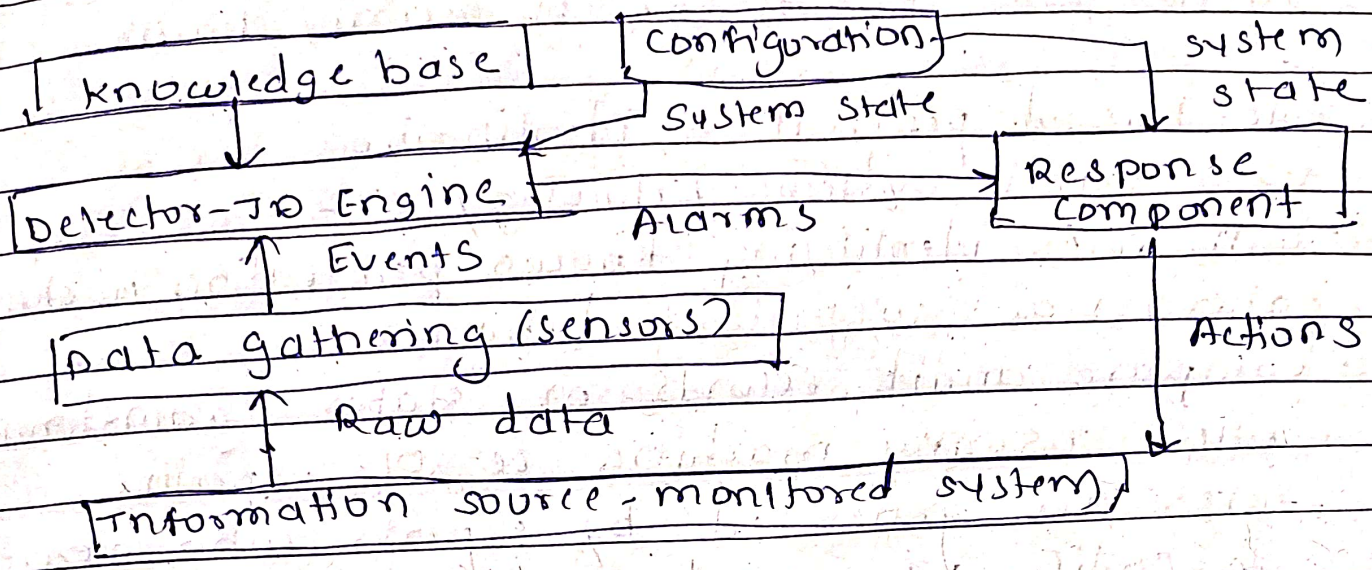
An Intrusion Detection systems helps protect a system by detecting harmful activities like unauthorized access

1. Security failures: No system is perfect, so IDS is there to catch any intrusions
2. Detect Quickly: If an attack happens, the IDS tries to find it fast so it can stop
3. Deterrent for attackers: knowing an IDS is watching can scare attackers away.
4. Improve security: It gathers data from attacks to make the system together.

Approaches to Intrusion Detection

- Statistical anomaly detection
- rule-based detection
- Audit Records

Architecture of IDS



Statistical Anomaly Detection

1) threshold detection
- count occurences of specific event over time
- if exceed reasonable value asume intrusion
- alone is a crude & ineffective detector

2) profile based
- characterize past behavior of user
- detect significant deviations from this
- profile usually multi-parameter

Rule-Based Detection

observe events on system & apply rules to decide if activity is suspicious or not

* rule-based anomaly detection
- analyze historical audit records to identify usage patterns & auto-generate rules for them
- then observe current behavior & match against rules to see if conforms

- like statistical anomaly detection does not require prior knowledge of security flaws

* rule-based penetration identification
  - uses expert systems technology
  - with rules identifying known penetration, weakness patterns, or suspicious behavior
  - compare audit records or states against rules
  - rules usually machine & OS specific
  - rules are generated by experts who interview & codify knowledge of security admins
  - quality depends on how well this done

Audit Record

- fundamental tool for intrusion detection
- native audit records
  - part of all common multi-user OS
  - already present for use
  - may not have info wanted in desired form
- detection-specific audit records
  - created specifically to collect wanted info
  - at cost of additional overhead on system

Audit Record Analysis

- foundation of statistical approaches
- analyze records to get metrics over time
  - use various tests on these to determine if current behavior is acceptable
    - mean & standard deviation, time series
  - key advantage is no prior knowledge used

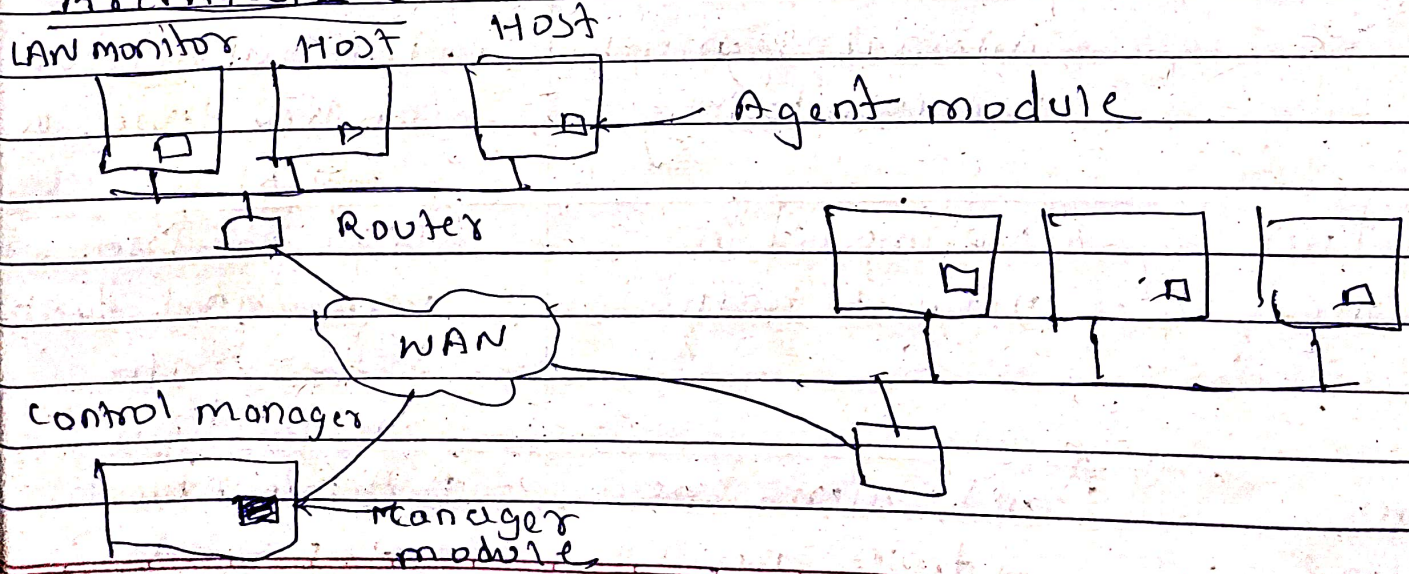
Base - Rate Fallacy

- practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
  - i) if too few intrusions detected → false security
  - 2) if too many false alarms → ignore / waste time
- this is very hard to do
- existing systems seem not to have a good record

Distributed Intrusion Detection

- traditional focus is on single systems
- but typically have networked systems
- more effective defense has these working together to detect intrusions
- Issues
  - dealing with varying audit record formats
  - integrity and confidentiality of networked data
  - centralized or decentralized architecture

Architecture



*malwares
* Trusted systems - done
* firewall configuration - done

Network-Based Intrusion Detection Systems (NIDS)

* A network-Based ID system monitors the traffic on its network segment as a data source.
* This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment
* network traffic no other segment, and traffic on other means of communication can't be monitored by sing NIDS

IDS and IPS Placement

Features	IDS	IPS
Main function	1) Detects and alert on threats	1) Detect and block threats in real time
Location	2) Typically placed in monitoring position	2) placed in an active path to block attacks inline
Network placement	3) placed at the network perimeter or internal segments for monitoring	3) placed inline behind the firewall be internal network or key devices for blocking
Impact on Traffic	4) No impact on network traffic	4) can affect network performance due to active traffic inspection
Action Taken	5) only alerts the admin no automatic action	5) Actively blocks or prevents attacks based on set rules

** (chatgpt)

IDPS : Technology Types

An Intrusion detection and prevention system is designed to monitor network or system activities, and detect or prevent any malicious activities or policy violations

Main IDPS technology types

1. Network-Based IDPS

Function : Monitors network traffic to detect suspicious activities

Detection : Look at packets traveling through the network to identify potential threats based on signatures or abnormal behavior

Deployment : Typically placed at key points in the network like perimeter or between internal segments

Example : Detecting an unauthorized attempt to access a sensitive server through abnormal traffic patterns

2. Host-Based IDPS

Function : Monitors and analyze the internal activities of a single host or system

Detection : Observes system files, logs, running processes, and file integrity to detect suspicious or malicious actions

Deployment : Installed on individual machines such as servers or workstations

Examples : Detecting unauthorized changes to system files or abnormal file access patterns on a critical server

3. Signature - Based IDPS

1) Function: Detect known attacks by comparing incoming traffic or system behaviors to a database of known attack signature

2) Detection: Relies on predefined patterns of known threats or attack signatures to identify and flag suspicious activity

3) Deployment: Can be used in both network and host-based systems

4) Example: Identifying a specific attack like a virus or worm based on its unique signature pattern in network traffic or system logs

4. Anomaly - Based IDPS

1) Function: Detect attacks by comparing current activity against a baseline of normal behavior

2) Detection: Flags activities that deviate significantly from normal patterns as potential threats

3) Deployment: used in both network and host systems require initial baseline behavior profiling

4) Example: flagging unusual outbound traffic form an internal network that might indicate data exfiltration or malware activity

5. Behavior - Based IDPS

1) Function: Similar to anomaly-based but focuses more on behavioral analysis and identifying abnormal user or system actions

2) Detection: Detects deviations in typical patterns of behavior, such as abnormal system resources usage or unauthorized access attempts

6. Hybrid IDPS
7. Inline vs passive IDPS

Honeypots (Intrusion prevention)
* decoy systems to lure attackers
  - away from accessing critical systems
  - to collect information of their activities
  - to encourage attacker to stay on system so administrator can respond
* are filled with fabricated information
* instrumented to collect detailed information on attackers activities
* Single or multiple networked systems

Honeypots Purpose
1) Attract Attackers: By setting up a vulnerable-looking system, the honeypot attracts attackers, who believe they are accessing a real target
2) Monitor Attacker Behavior: Security teams can observe how attackers behave, which tools and technique they use, and understand the methods they deploy
3) Gather Intelligence: This data helps in enhancing overall security by knowing the latest threats and preparing defenses accordingly
4) Divert Attention: Attackers may spend time on the honeypot instead of real assets, thus protecting critical systems

chatgpt

Honeypot Deployment

1) preparation : set up the honeypot to look like a genuine system, including configuring operating system, software and services

2) Location : Deploy the honeypot strategically within a network so it appears assible to attackers while being isolated from critical assets

3) monitoring and logging : configure monitoring tools to record any interaction with the honeypot.

4) containment : Ensure that the honeypot does not connect to sensitive systems!, as a compromised honeypot could be used as a gateway for further attacks

Chatgpt

Honeypots Advantages

1) Enhanced Threat Detection : Honeypots can identify and log threats in realtime

2) understanding Attack patterns : provides insights into the tactics, techniques and procedures used by attackers

3) Minimal False positives : Since no legitimate users are expected to access the honeypot, any interaction can be considered suspicious, reducing false positives

Disadvantages

1) Limited View : Honeypots only capture attacks targeted at them. They don't reveal attacks aimed at other parts of the network

2) Risk of compromise : If attackers recognize the honeypot, they could exploit it to infiltrate the rest of the network

3) Maintenance : Honeypots require continuous monitoring, updates and maintenance to stay effective and secure

Q

Types of Honeypots

1) low Interaction Honeypots
- description : Emulates only a few services or parts of a system, providing minimal interaction with attackers
- Advantages : safer and easier to maintain as attackers can only interact with limited parts of the system
- disadvantages : limited data collection since attackers don't engage with a full System

2) High Interaction Honeypots
- description : Emulates an entire operating system allowing extensive interaction with attackers
- Advantages : Provides detailed insights into attackers methods and intension
- disadvantages : Higher risk and require more resources to manage, since attackers have more interaction possibilities

Honeypot System
- Architecture : Plan the honeypot's structure within the network, deciding its placement and connection with other monitoring systems
- Integration with security tools : connect the honeypots to security information and event management System for better data analysis
- Maintenance : Regular updates are needed to ensure the honeypots remains attractive to attackers and doesn't compromise security

- usage in Threat intelligence : The honeypots acts as a valuable tool for gathering data on new threats, which can inform the development of stronger security protocols across the organization

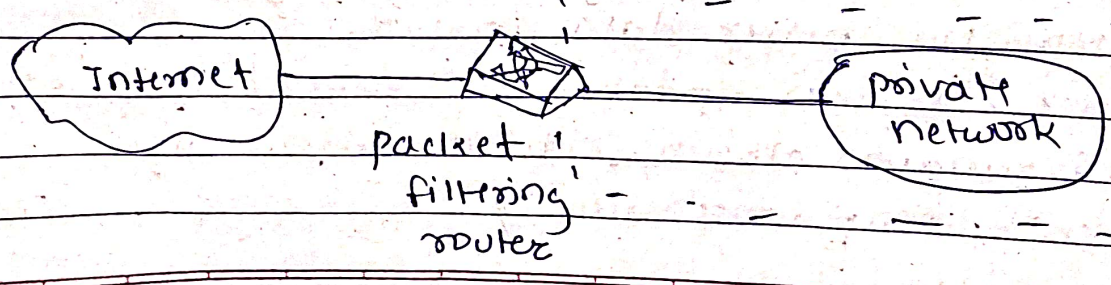
Firewalls

- a choke point of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
  - only authorized traffic is allowed
- auditing and controlling access
  - can implement alarms for abnormal behavior
- is itself immune to penetration
- provide perimeter defence

Firewall Limitation

- cannot protect from attacks bypassing it
  e.g sneaker net, trusted services, utility modems
- cannot protect against internal threats
  e.g disgruntled employee
- cannot protect against transfer of all virus infected programs or files
  - because of huge range of OIs & file type

Firewalls - Packet filters



(a) packet-filtering router

- simplest of components
- foundation of any firewall system
- examine each IP packet (no context) and permit or deny according to rules
- hence restrict access to services (ports)
- possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

① Attacks on packet filters

1 IP address spoofing
- fake source address to be trusted
- add filters on router to block

2 Source routing attacks
- attacker sets a router other than default
- block source routed packets

3 tiny fragment attacks
- split header info over several tiny packets
- either discard or reassemble before check

or

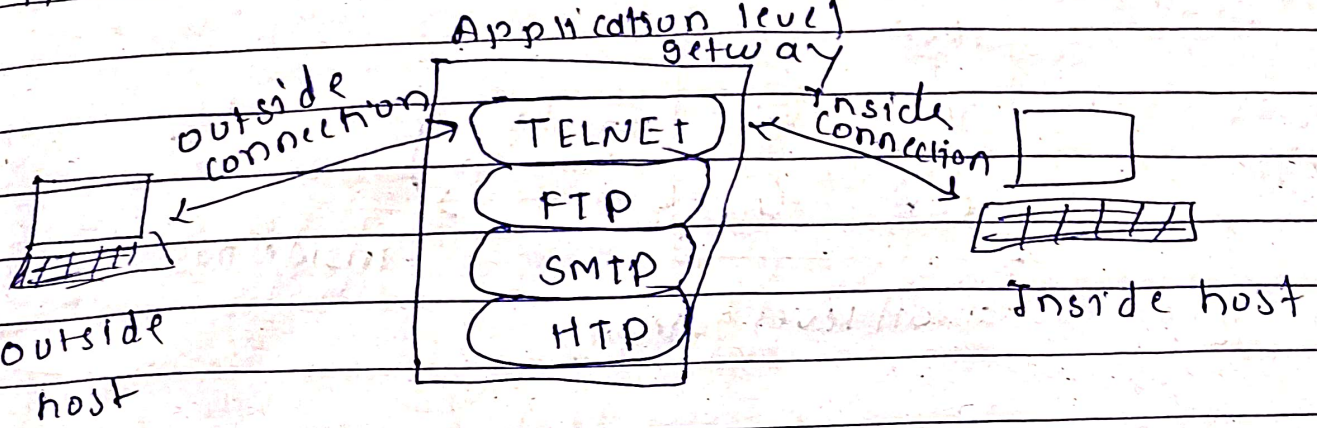
1. IP address spoofing
- The attacker forges the source IP address in a packet to mimic a trusted host
- The firewall may allow these packets if it relies ~~stor~~ solely on sourie if addresses for access control

2. Source Routing Attacks
- This attacker specifies the route that packets take through the network instead of allowing routers to determine the path
- This can bypass security controls and expose sensitive network segments

3. Tiny fragmentation
- Similar to fragmentation attacks, this involves splitting the header information across tiny packets to bypass firewalls
- The firewall may not analyze or enforce rules properly on such fragmented headers

(2) Firewalls - stateful packet filters
- stateful packet filters are a type of firewall technology that examines the state and context of packet in a network
- examine each IP packet in context
  - keeps tracks of client-server sessions
  - checks each packet validity belongs to one
- better able to detect bogus packets out of context

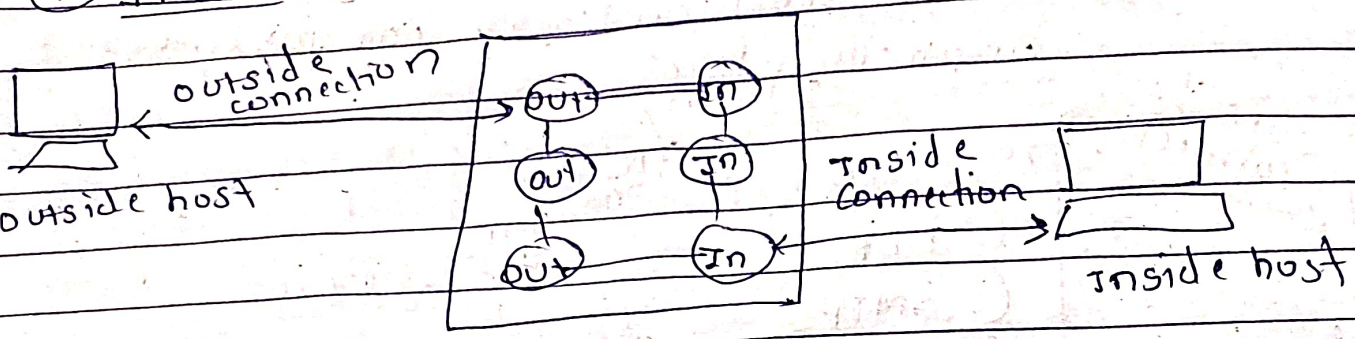
2) Firewalls - Application level gateway (or proxy)



Application-level gateway

- ALGs also knowns as proxy firewalls, are a type of firewall that operate at the application layer of the OSI model
- They serve as intermediaries betwn the user and the destination server, analyzing and filtering traffic based on the application protocol
- use an application specific gateway / proxy
- has full access to protocol
  - user requests services from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- need separate proxies for each services
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported

(4) Firewall - circuit level gateway



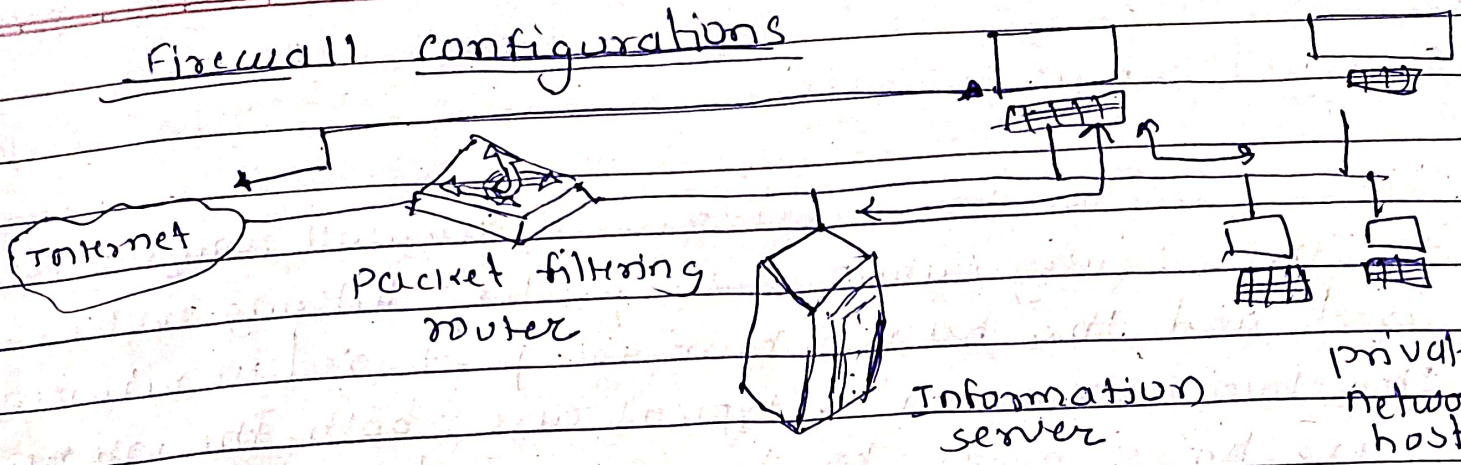
circuit level gateway

- relay two TCP connections.
- Imposes security by limiting which such connections are allowed
- one created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- socks commonly used for this

Bastion Host

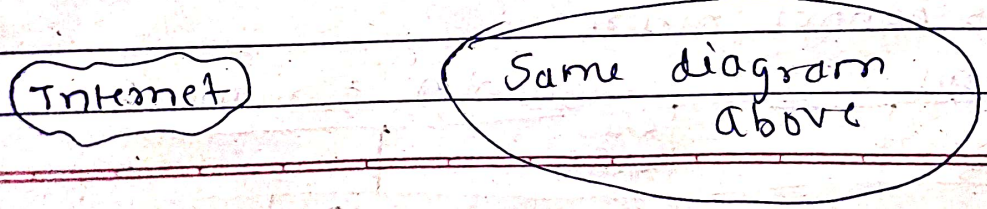
- highly secure host system
- potentially exposed to "hostile" elements
- hence is secured to withstand this
- may support 2 or more net connections
- may be trusted to enforce trusted separation between network connections
- run circuit / application level getways
- or provide extremely accessible services

Firewall configurations



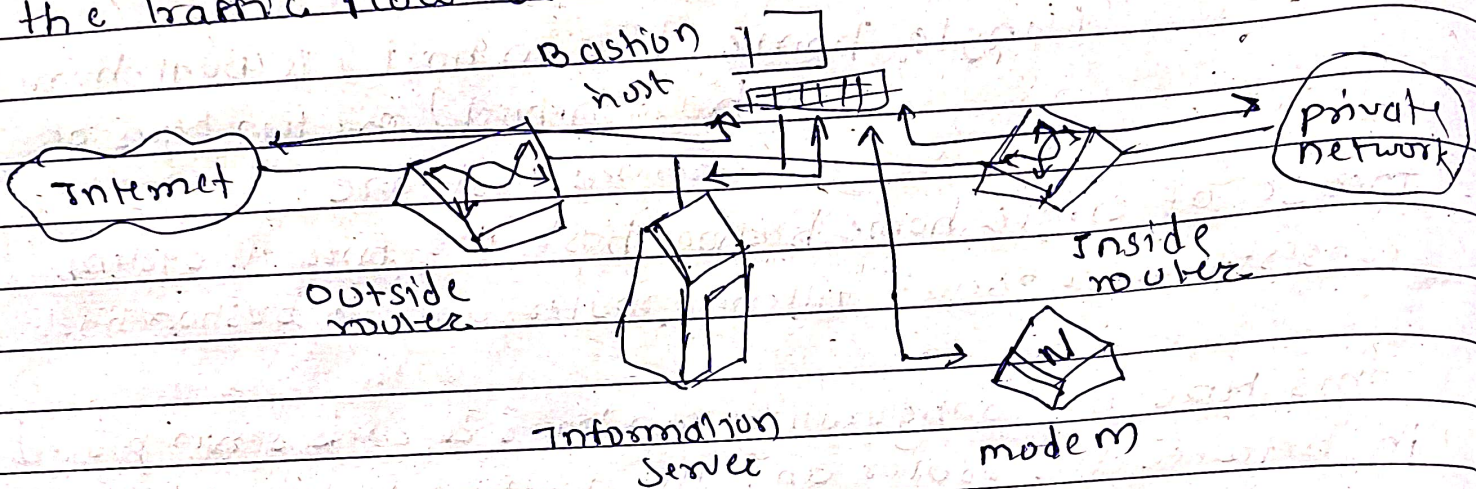
(5) Screened host firewall system (single-home bastion host) & (dual-homed bastion host) are two types of screened host-one

- Incase of single home bastion host the firewall system consists of a packet filtering router and a bastion host
- This type of configuration can have a web server placed in between the router and the bastion host in order to allow the public to access the server from the Internet
- The main problem with the single home bastion host is that if the packet filter router get compromised then the entire network will be compromised
- To eliminate this drawback, we can use the dual homed bastion host firewall system, where a bastion host has two network card-one is used for internal connection and the second one is used for connection with the router. In case, even if the router got compromised, the internal network will remain unaffected since it is in the separate network zone



① Screened subnet firewalls

- This is one of the most secured firewall configurations. In this configuration, two packet filtering routers are used and the bastion host is positioned in between the two routers. In a typical case, both the internet users have access to the screened subnet, but the traffic flow between the two subnets is blocked



Access control

- given system has identified a user
- determine what resources they can access
- general model is that of access matrix with
  - subject - active entity (user, process)
  - object - passive entity (file or resource)
  - access right - way object can be accessed
- can decompose by
  - columns as access control lists
  - rows as capability tickets

Access control matrix

	programs	segment A	segment B
process 1	Read Execute	Read write	
process 2			Read

Trusted computer systems

1. information security is increasingly important
2. have varying degrees of sensitivity of information
   - cf military info classifications : confidential, secret etc
3. subjects (people or programs) have varying rights of access to objects
4. want to consider ways of increasing confidence in systems to enforce these rights
5. known as multilevel security
   - subjects have maximum & current security level
   - objects have a fixed security level classification