

Firewalls

Chapter 11

The function of a strong position is to make the forces holding it practically unassailable.

- On War, Carl Von Clausewitz

Contents

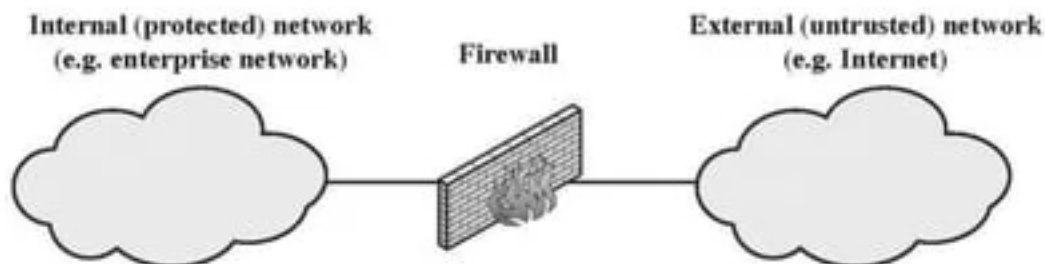
- Firewall
 - Characteristics
 - Types
- Firewall Basing
 - Bastion Host
 - Host Based
 - Personal Firewall
- Firewall Location and Configurations

Firewalls : Need

- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN's or the Internet
- The firewall is inserted between the premises network and the Internet
- Aims:
 - Establish a controlled link
 - Protect the premises network from Internet-based attacks
 - Provide a single choke point

Design goals

- All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
- Only authorized traffic (defined by the local security policy) will be allowed to pass
- The firewall itself is immune to penetration (use of trusted system with a secure operating system)



(a) General model

Characteristics: Access Control

- 4 general techniques:

III. Service control

- Determines the types of Internet services that can be accessed, inbound or outbound

IV. Direction control

- Determines the direction in which particular service requests are allowed to flow

V. User control

- Controls access to a service according to which user is attempting to access it

VI. Behavior control

- Controls how particular services are used (e.g. filter e-mail)

Characteristics: Capabilities & Limitations

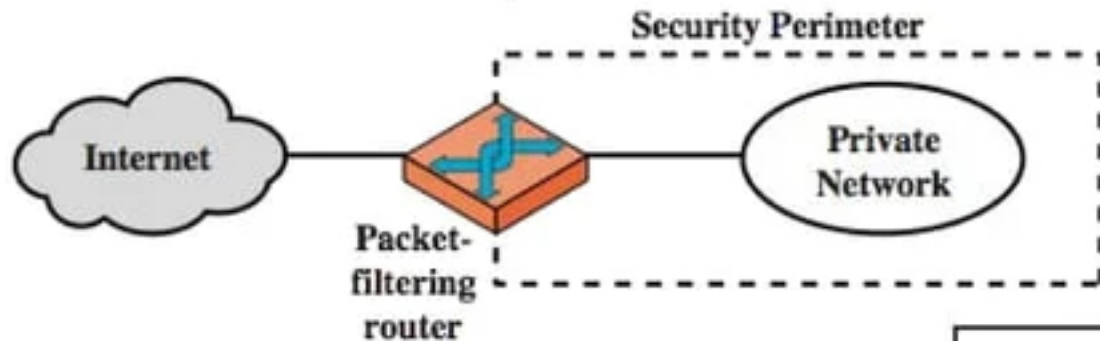
- Capabilities
 - Single Choke
 - Prohibit potentially vulnerable services from entering or leaving the network
 - Provides protection from attacks (different kinds)
 - Provide a location for monitoring security-related events
- Limitations
 - Can not protect against attacks that bypass firewall
 - May not protect fully against internal threats
 - Can not secure improperly secured wireless LAN
 - Can not secure adhoc systems which are already infected

Types of Firewalls

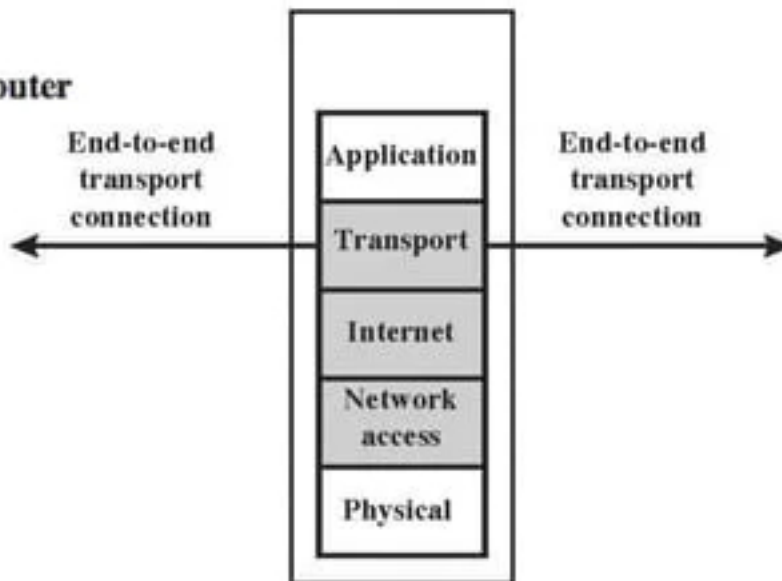
- 4 common types of Firewalls:
 - Packet-filtering routers
 - Stateful Inspection Firewalls
 - Application-level gateways
 - Circuit-level gateways

Types of Firewalls

- Packet-filtering



(a) Packet-filtering router



Packet filtering firewall

Packet-filtering

- 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)

Packet-filtering

▷ 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
- Tiny fragment attacks

Packet-filtering

Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

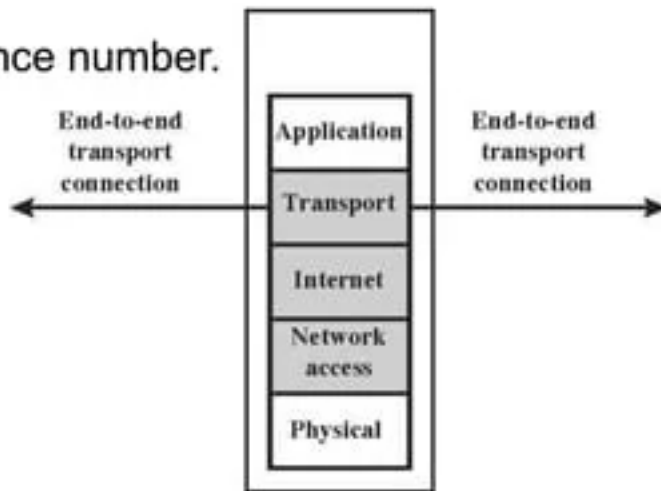
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Types of Firewalls

- Stateful Inspection Firewall
 - Most standard applications that run on top of TCP follow client server model
 - Creates a directory of outbound TCP connections.
 - An entry for each currently established connection.
 - Reviews same packet information as packet filtering firewall but also records information about TCP connections
 - Can keep track TCP sequence number.



Packet filtering firewall

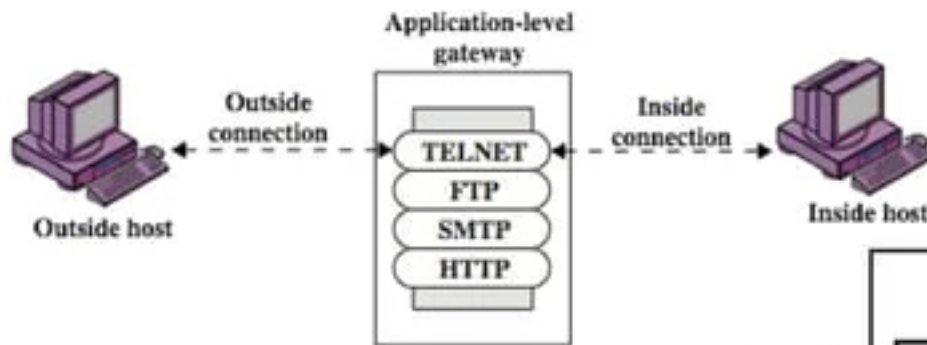
Stateful Inspection Firewall

Example Stateful Firewall Connection State Table

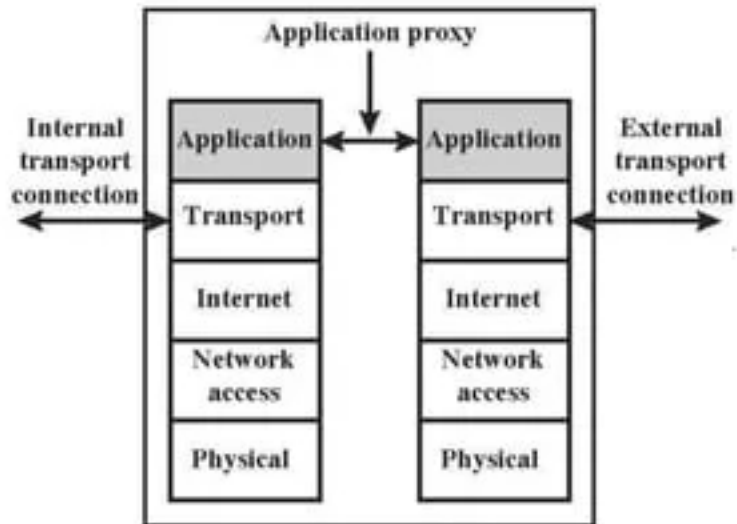
Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

Types of Firewalls II

- Application-level Gateway



(b) Application-level gateway



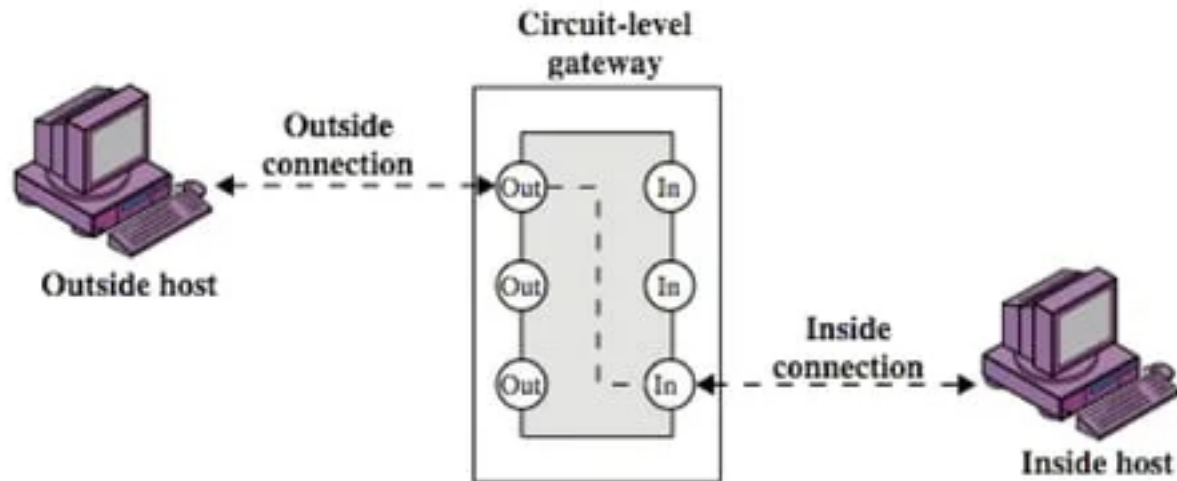
Application proxy firewall

Application-level Gateway

- Application-level Gateway
 - Also called proxy server
 - Acts as a relay of application-level traffic
- Advantages:
 - Higher security than packet filters
 - Only need to scrutinise a few allowable applications
 - Easy to log and audit all incoming traffic
- Disadvantages:
 - Additional processing overhead on each connection (gateway as splice point)

Types of Firewalls III

- Circuit-level Gateway

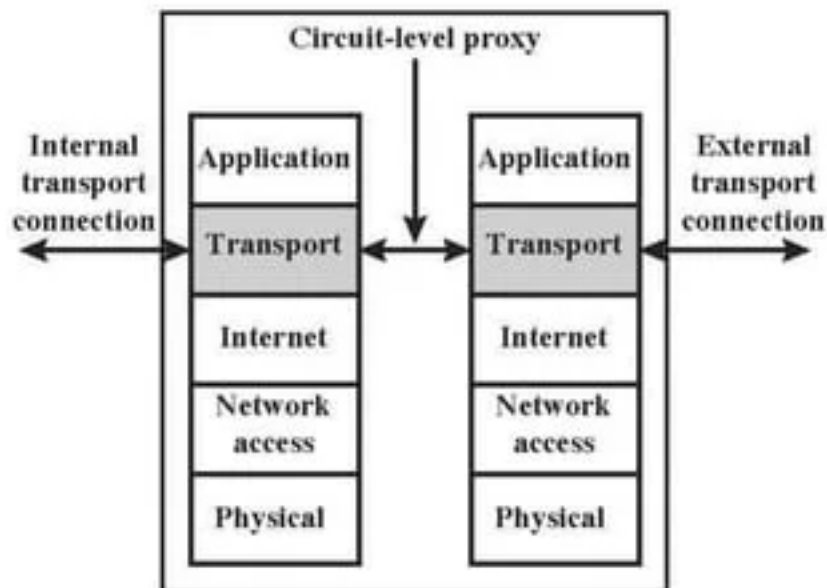


(c) Circuit-level gateway

Circuit-level Gateway

- Circuit-level Gateway
 - Stand-alone system or
 - Specialised function performed by an Application-level Gateway
 - Sets up two TCP connections
 - The gateway typically relays TCP segments from one connection to the other without examining the contents
 - The security function consists of determining which connections will be allowed
 - Typically use is a situation in which the system administrator trusts the internal users
 - An example is the SOCKS package

Circuit-level Gateway



Circuit-level proxy firewall

Firewall Basing

Bastion Host

- Bastion Host
 - A system identified by the firewall administrator as a critical strong point in the network's security
 - Hardware with its own secured version of OS
 - Only allowable services are installed
 - May require additional authentication from users for accessing services.
 - The bastion host serves as a platform for an application-level or circuit-level gateway

Host-Based Firewalls

- Software Module used to secure an individual host.
 - Commonly available in OS
 - Filter and restrict flow of packets
 - Common location : Server
- Advantages
 - Rules can be tailored
 - Independent of topology
 - As independent firewall, may provide extra layer of protection without changing the existing network

Personal Firewall

- Controls traffic between a personal computer or workstation
- May be used in home and in enterprise both
- Less complex as primary goal is to deny unauthorized remote access
- Can also monitor outgoing activity

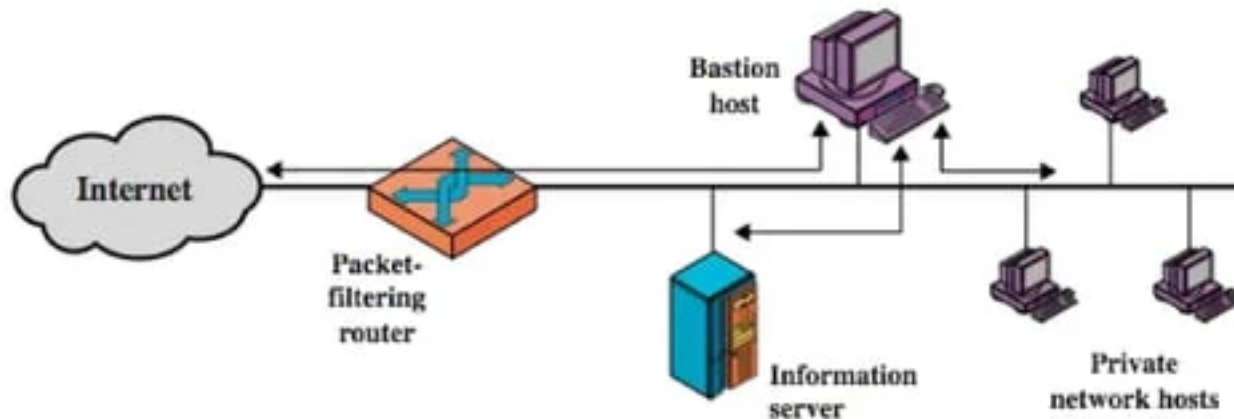
Locations and Configurations

Firewall Configurations

- ▷ Greater security than single configurations because of two reasons:
 - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
 - An intruder must generally penetrate two separate systems
- ▷ This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)

Screened host firewall

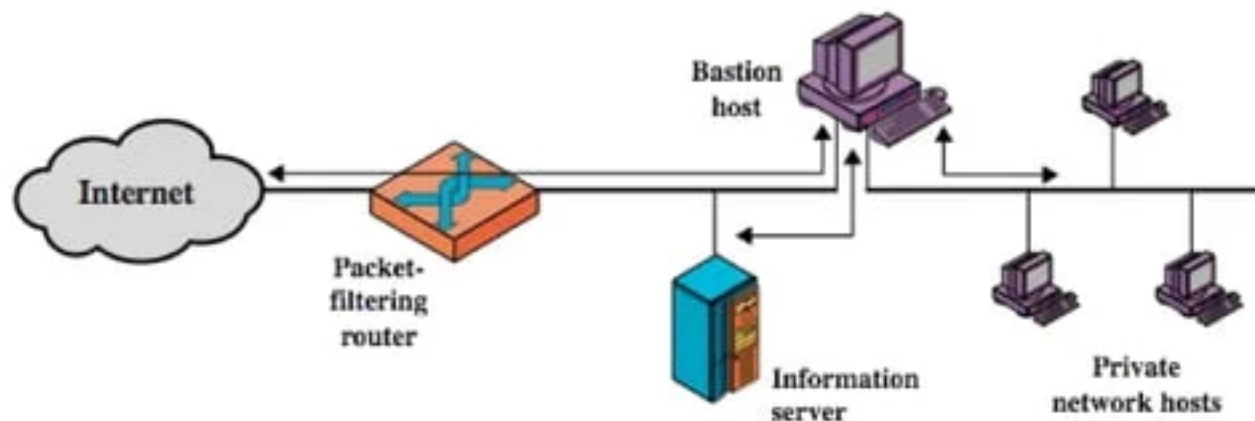
- Screened host firewall system (single-homed bastion host)
- Screened host firewall, single-homed bastion configuration
- Firewall consists of two systems:
 - A packet-filtering router
 - A bastion host



(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations

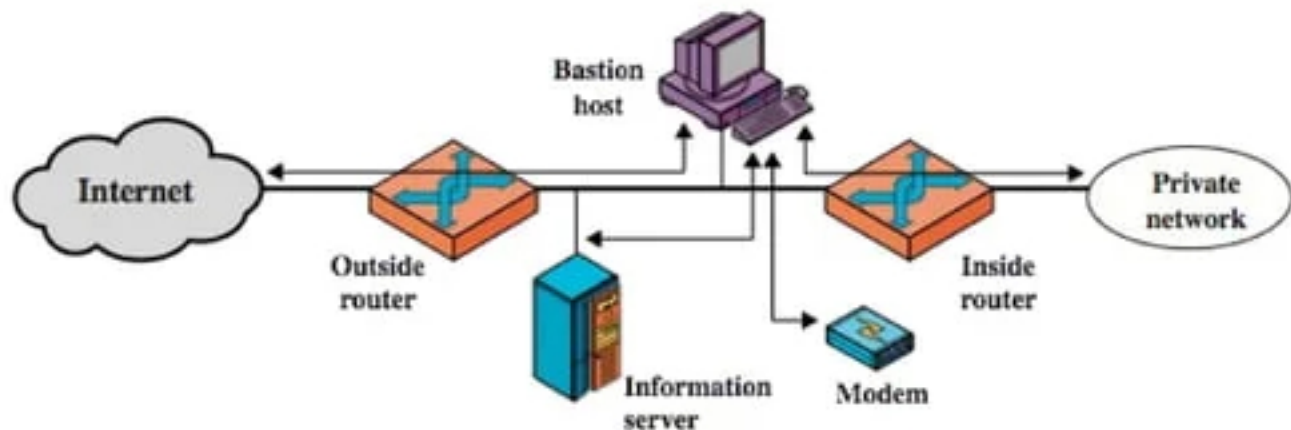
- ▷ Screened host firewall system (dual-homed bastion host)
- ▷ Screened host firewall, dual-homed bastion configuration
 - The packet-filtering router is not completely compromised
 - Traffic between the Internet and other hosts on the private network has to flow through the bastion host



(b) Screened host firewall system (dual-homed bastion host)

Firewall Configurations

- ▷ Screened-subnet firewall system
- ▷ Screened subnet firewall configuration
 - Most secure configuration of the three
 - Two packet-filtering routers are used
 - Creation of an isolated sub-network



(c) Screened-subnet firewall system

Firewall Configurations

▷ Advantages:

- Three levels of defense to thwart intruders
- The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)
- The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)

Firewall Configuration

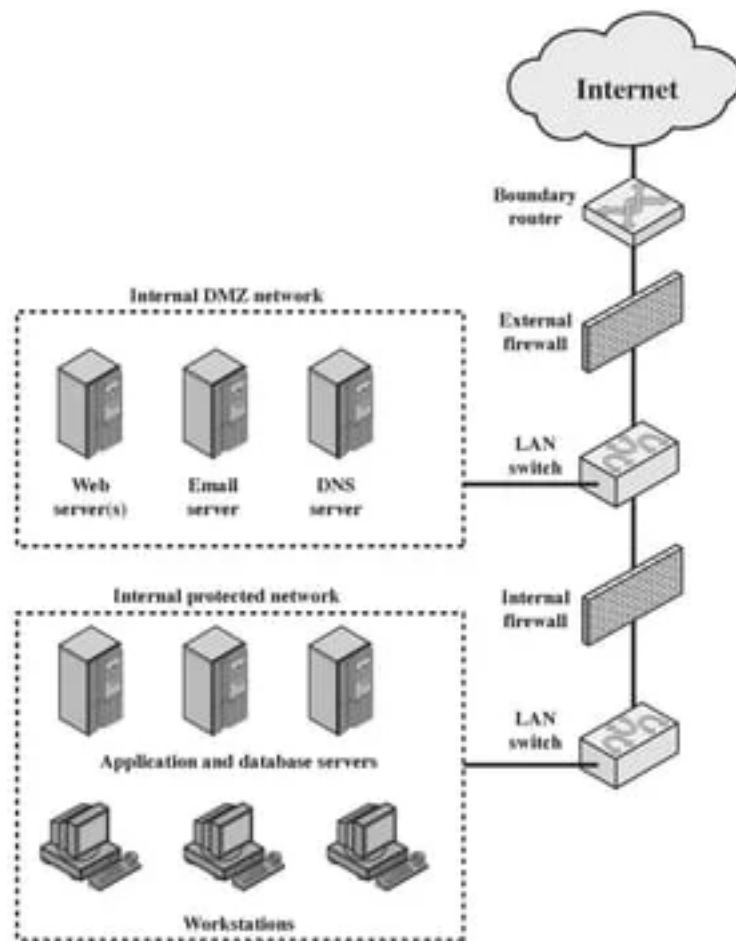
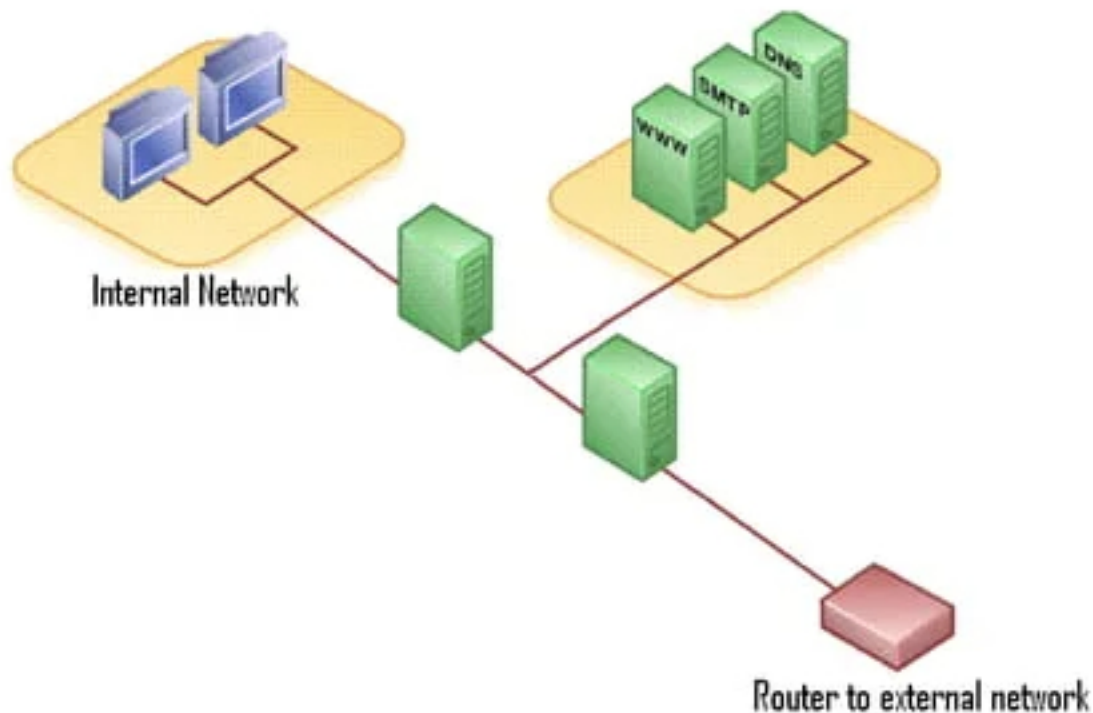


Figure 11.3 Example Firewall Configuration

Demilitarized zone (DMZ)

- Usage of firewalls to create a “no mans land” for services that should be accessible from the external network



Virtual Private Networks

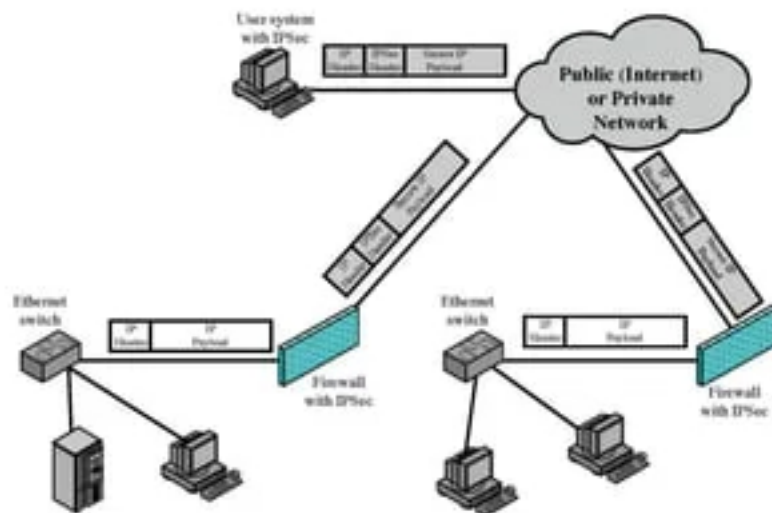


Figure 11.4 A VPN Security Scenario

Ditributed Firewalls

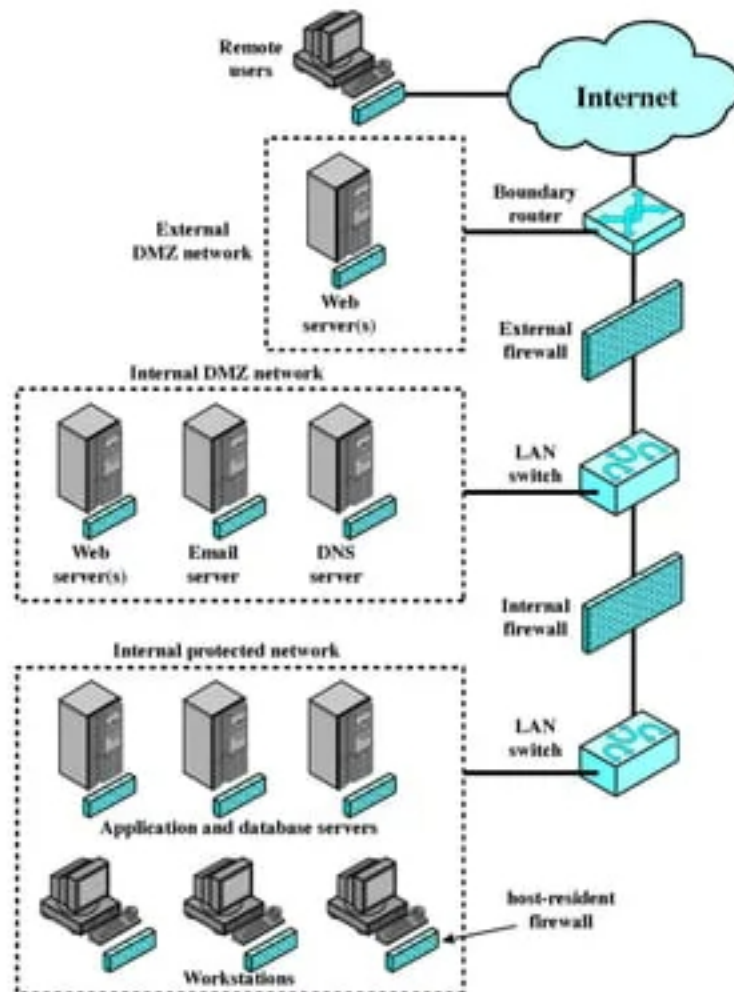


Figure 11.5 Example Distributed Firewall Configuration

Trusted Systems & Data Access Control

- ▷ One way to enhance the ability of a system to defend against intruders and malicious programs is to implement trusted system technology

- ▷ Data Access control
 - Through the user access control procedure (log on), a user can be identified to the system
 - Associated with each user, there can be a profile that specifies permissible operations and file accesses
 - The operation system can enforce rules based on the user profile

- ▷ General models of access control:
 - Access matrix
 - Access control list
 - Capability list

Data Access Control

- ▷ Access Matrix: Basic elements of the model
 - Subject: An entity capable of accessing objects, the concept of subject equates with that of process
 - Object: Anything to which access is controlled (e.g. files, programs)
 - Access right: The way in which an object is accessed by a subject (e.g. read, write, execute)

- ▷ Access Control List
 - An access control list lists users and their permitted access right
 - The list may contain a default or public entry

- ▷ Capability list
 - A capability ticket specifies authorised objects and operations for a user
 - Each user have a number of tickets

The Concept of Trusted Systems

- ▷ Trusted Systems
 - Protection of data and resources on the basis of levels of security (e.g. military)
 - Users can be granted clearances to access certain categories of data
- ▷ Multilevel security
 - Definition of multiple categories or levels of data
- ▷ A multilevel secure system must enforce:
 - No read up: A subject can only read an object of less or equal security level (Simple Security Property)
 - No write down: A subject can only write into an object of greater or equal security level (*-Property)
- (Please read the concepts of Bell—LaPadula Confidentiality Model and Biba Integrity Model **(Important Reading Assignment)**)

(http://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models)

The Concept of Trusted Systems II

▷ Reference Monitor

- Controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on basis of security parameters
- The monitor has access to a file (security kernel database)
- The monitor enforces the security rules (no read up, no write down)

▷ Properties of the Reference Monitor

- Complete mediation: Security rules are enforced on every access
- Isolation: The reference monitor and database are protected from unauthorised modification
- Verifiability: The reference monitor's correctness must be provable (mathematically)

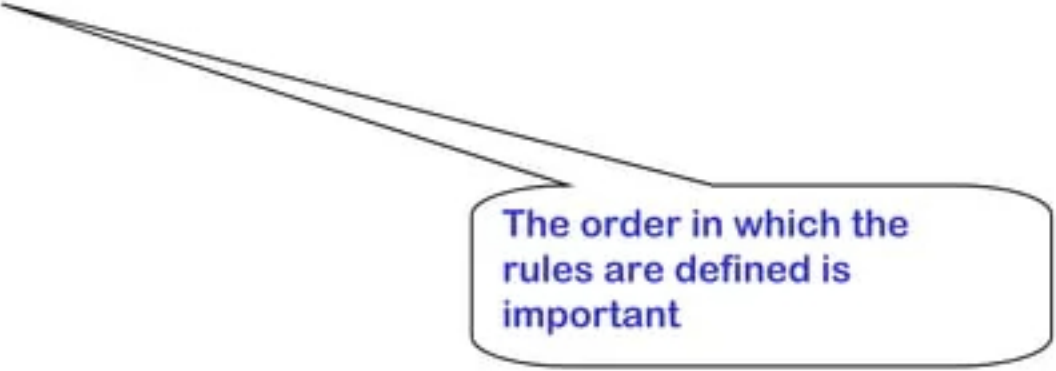
Linux Firewall

iptables

- Firewall administration program
- Implemented within the operating system
- Works at the IP network and Transport Protocol Layers
- Protects the system by making routing decisions after filtering packets based on information in the IP packet header
- Consists of a list of acceptance and denial rules
- The rules are stored in kernel tables, in an input output or forward chain

Packet-Filtering Concepts

- Rules based on:
 - Specific NIC
 - Host IP address
 - Network layer's source and destination IP addresses
 - The transport layer's TCP and UDP service ports
 - TCP connection flags
 - The network layer's ICMP message types
 - Whether the packet is incoming or outgoing



The order in which the rules are defined is important

Tables

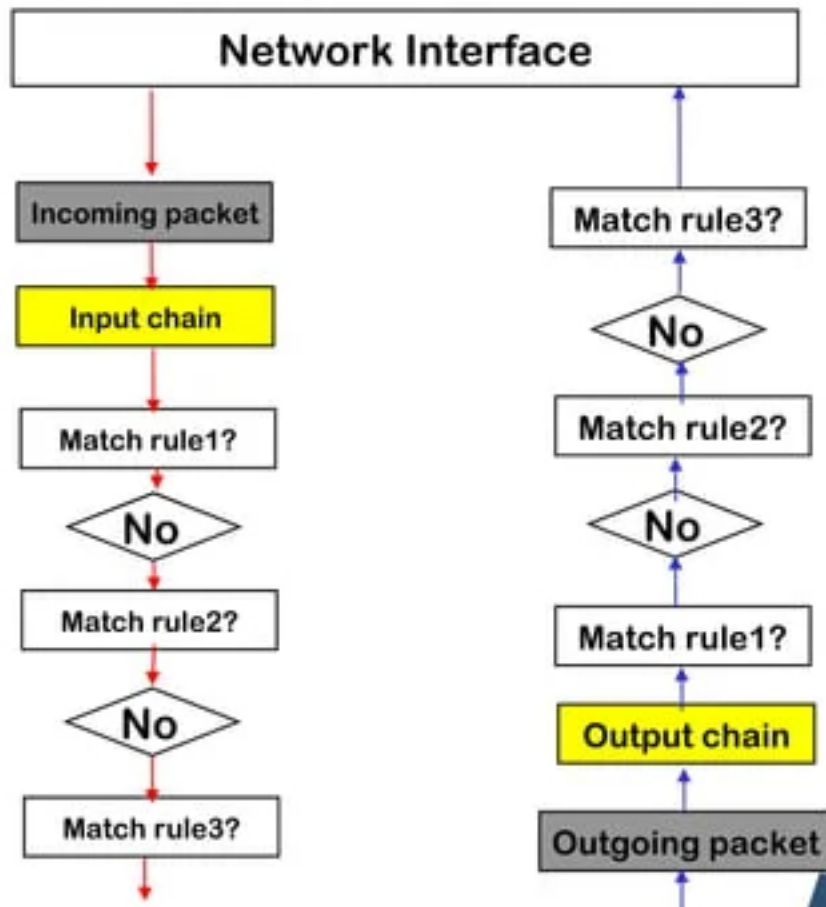
1. filter table - responsible for filtering - default table
 - INPUT chain - All packets arriving into the system go through this chain.
 - OUTPUT chain - All packets leaving the system go through this chain.
 - FORWARD chain - All packets passing through the system (being routed) go through this chain.
2. nat table - responsible for rewriting packet addresses or ports.
 - consulted when a packet that creates a new connection is encountered
 - PREROUTING chain - Incoming packets pass through this chain before the local routing table is consulted, primarily for DNAT (destination-NAT).
 - POSTROUTING chain - Outgoing packets pass through this chain after the routing decision has been made, primarily for SNAT (source-NAT).
- mangle table - responsible for adjusting packet options, such as quality of service. (Reading Assignment)
 - PREROUTING chain.
 - INPUT chain.
 - FORWARD chain.
 - OUTPUT chain.
 - POSTROUTING chain.

Firewall Characteristics

- ▷ The list of rules defining what can come in and what can go out are called chains

- ▷ 2 chains:

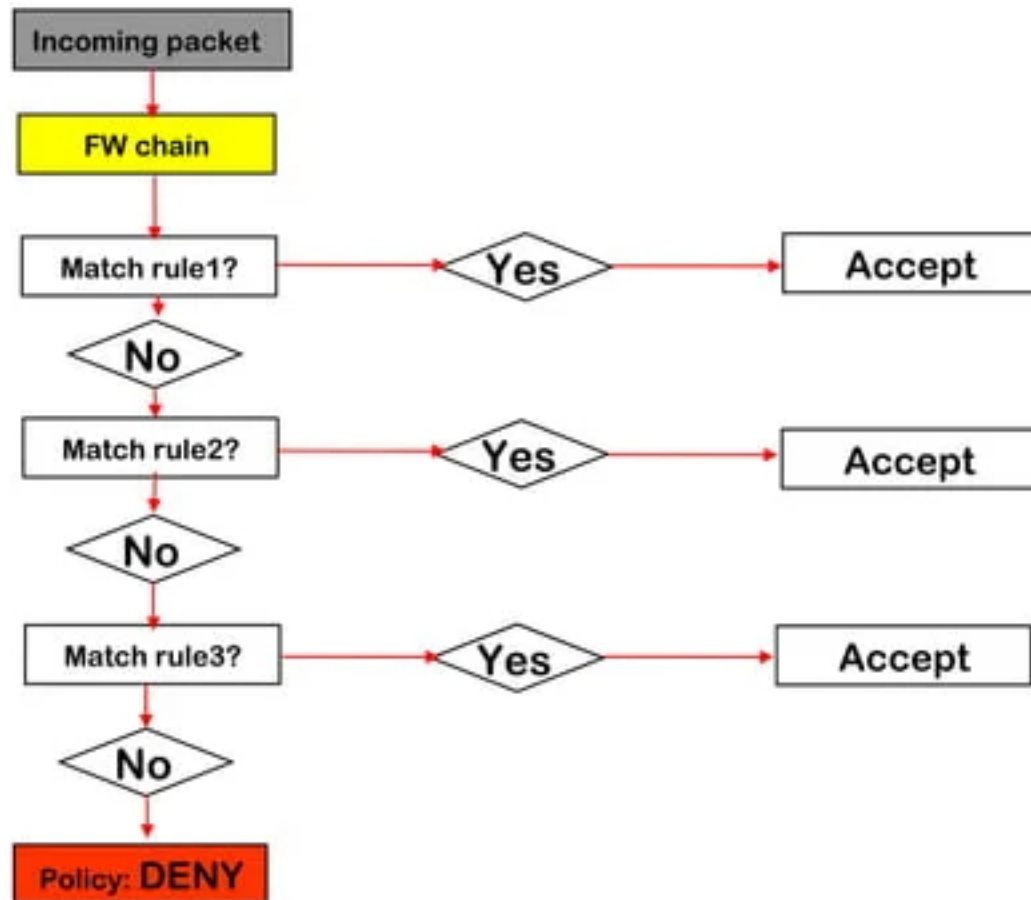
- Input chain
- Output chain
- (Forward chain)



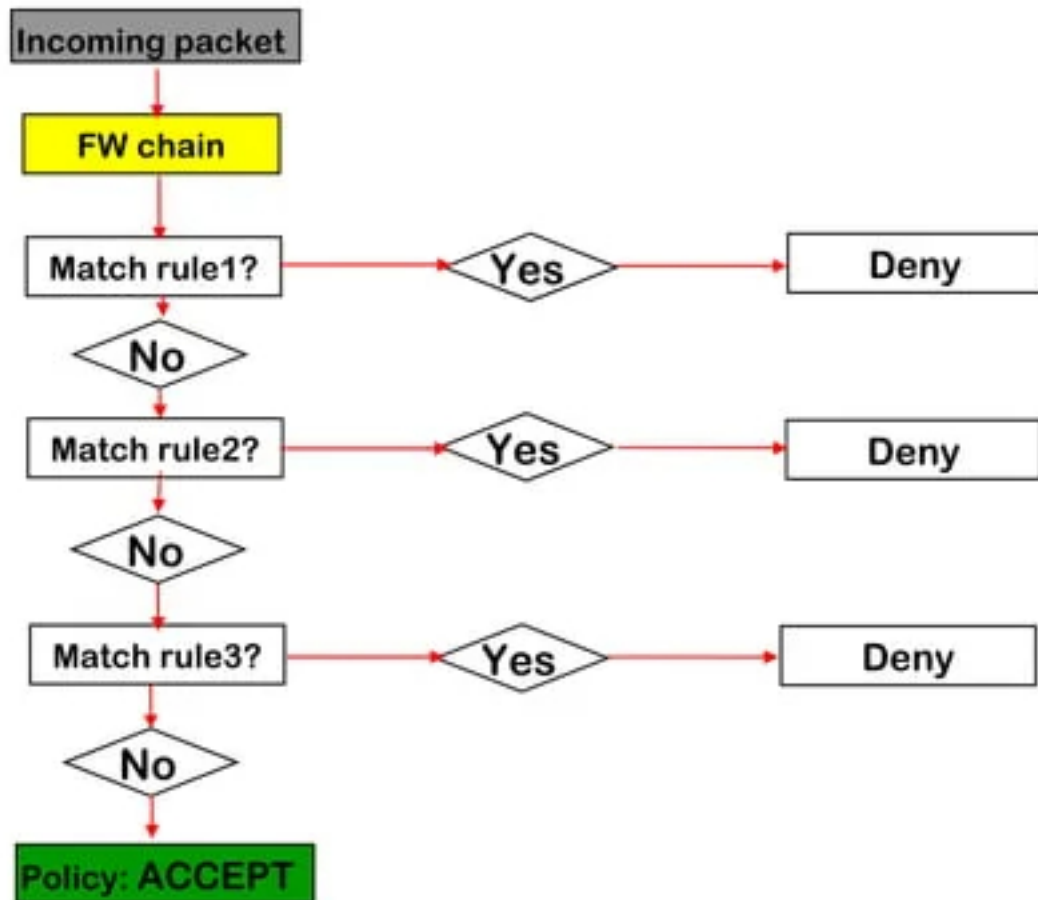
Default Packet-filtering policy

- ▷ Each chain has a default policy
- ▷ If the packet doesn't match any rule the default policy is applied
- ▷ 2 basic approaches to a firewall:
 1. Deny everything by default and explicitly allow selected packets through
 2. Accept everything by default and explicitly deny selected packets through

Deny-everything-by-default policy

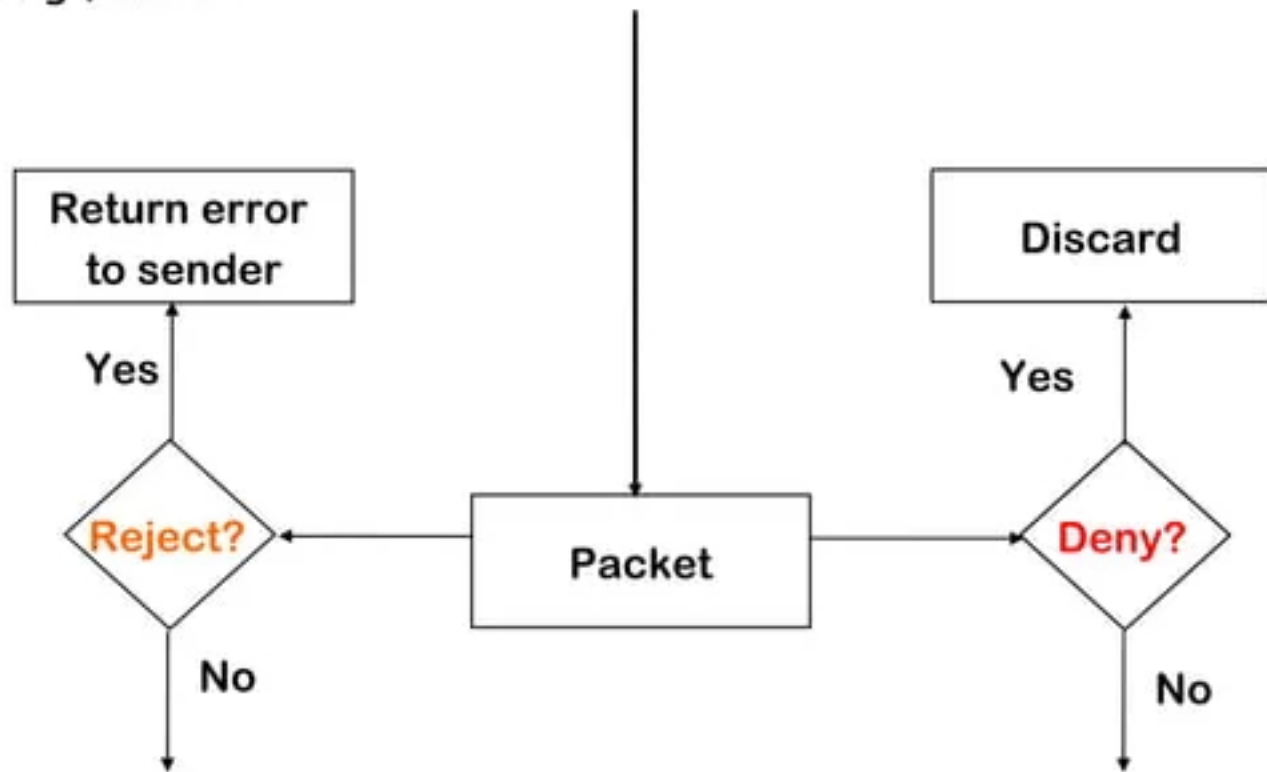


Accept-everything-by-default policy



Reject vs Deny

Firewall mechanism gives you the option of either rejecting or denying packets



iptables command-line arguments

- `iptables -A|I|D [chain] [-i interface] [-p protocol] [[!] --syn`
- `[-s address [port [:port]]]`
- `[-d address [port [:port]]]`
- `-j policy [-l]`

A | I | S : Append | Insert | Delete

- #Set the default policy to deny
- `iptables -P input DENY`
- `iptables -P output REJECT`
- `iptables -P forward REJECT`
-P (Chain Target)

iptables command-line arguments

- # Unlimited traffic on the loopback interface.
- `iptables -A input -i $LOOPBACK_INTERFACE -j ACCEPT`
- `iptables -A output -o $LOOPBACK_INTERFACE -j ACCEPT`
- `iptables -A output -o $EXTERNAL_INTERFACE -p icmp \`
- `-s $IPADDR -- icmp-type echo-request -j ACCEPT`
- `iptables -A input -i $EXTERNAL_INTERFACE -p icmp \`
- `--icmp-type echo-reply -d $IPADDR -j ACCEPT`

iptables command-line arguments

- # HTTP Web client
- iptables -A output -o \$EXTERNAL_INTERFACE -p tcp \
- -s \$IPADDR --sport \$UNPRIVPORTS \
- --dport 80 -j ACCEPT
- iptables -A input -i \$EXTERNAL_INTERFACE -p tcp ! --syn \
- -sport 80 \
- -d \$IPADDR --dport \$UNPRIVPORTS -j ACCEPT

iptables command-line arguments

- `iptables -A output -o $EXTERNAL_INTERFACE -p tcp \`
- `-s $IPADDR --sport $UNPRIVPORTS \`
- `--dport 443 -j ACCEPT`

- `iptables -A input -i $EXTERNAL_INTERFACE -p tcp ! --syn \`
- `-sport 443 \`
- `-d $IPADDR --dport $UNPRIVPORTS -j ACCEPT`

iptables command-line arguments

- # DNS client (53)
- iptables -A output -o \$EXTERNAL_INTERFACE -p udp \
 - -s \$IPADDR --sport \$UNPRIVPORTS \
 - -d \$NAMESERVER_1 --dport 53 -j ACCEPT
- iptables -A input -i \$EXTERNAL_INTERFACE -p udp \
 - -s \$NAMESERVER_1 --sport 53 \
 - -d \$IPADDR --dport \$UNPRIVPORTS -j ACCEPT