Module 2: Application Layer (Lecture – 5)

Dr. Nirnay Ghosh

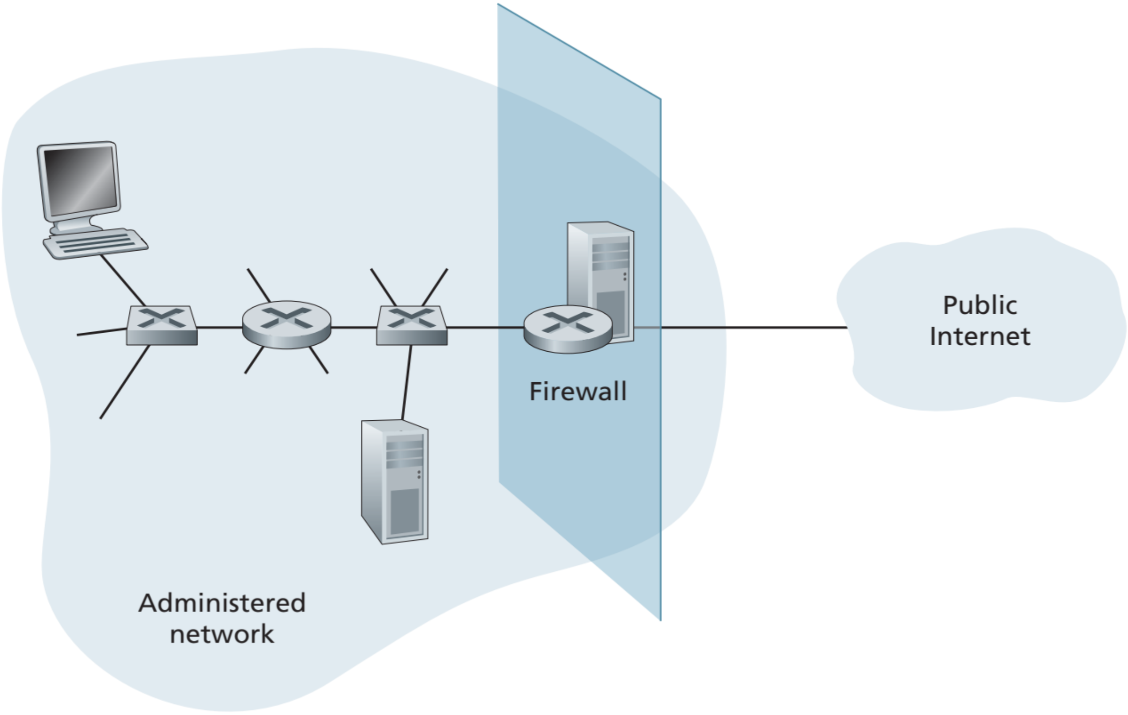
Assistant Professor

Department of Computer Science & Technology

IIEST, Shibpur

Firewalls

- Combination of hardware and software
- Placed on the edge of an organization's network – as a part of the gateway router
- Isolates an organization's traffic from the Internet at large
- Manages traffic flow by allowing some packets to pass and block others
- Allows network administrators to control access between the outside world and the resources within the administered network
- Three goals of firewall are:
  - All traffic from outside to inside, and vice-versa, passes through the firewall
  - Only authorized traffic (as defined by the local security policy) will be allowed to pass
  - The firewall itself is immune to penetration

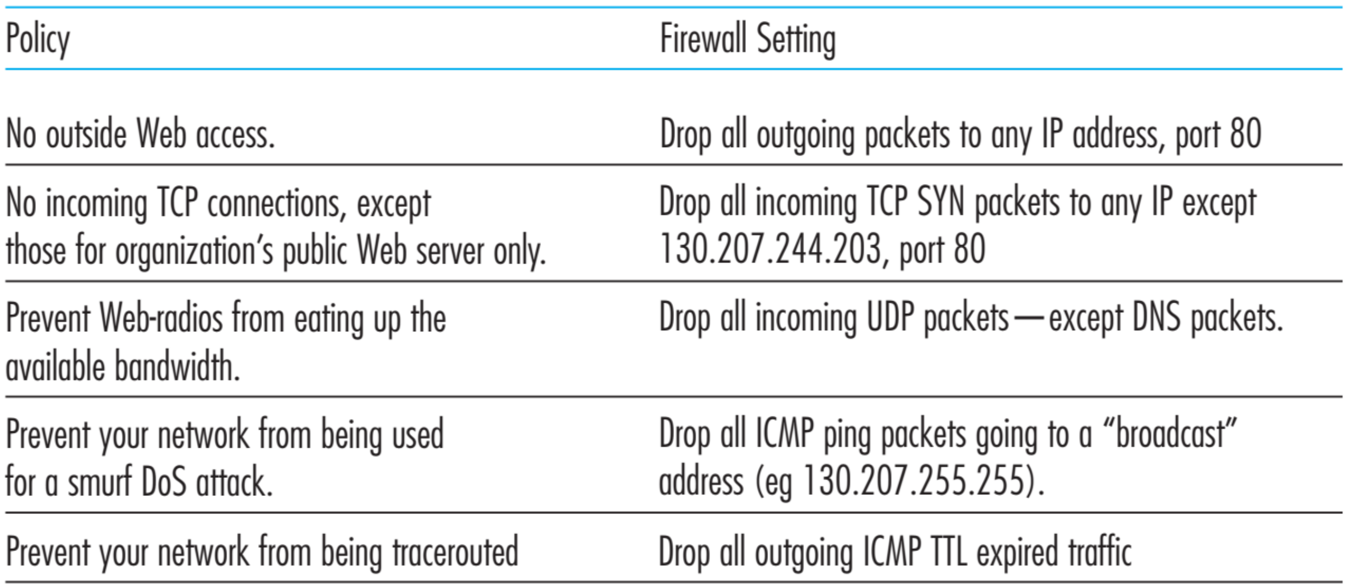


Firewall – Placed between Administered Network and Public Network

- Cisco & CheckPoint: leading firewall vendors today
- Firewall can be created from a Linux box using iptables (public domain software usually shipped with Linux)
- Three categories of firewalls:
  - Traditional packet filters
  - Stateful filters
  - Application gateways

Traditional Packet Filter Firewall

- Gateway router: connects internal network to its ISP (and hence to the larger public Internet)
- All traffic entering and leaving the internal network passes through this router
- Packet filtering: done at the gateway router
- Examines each datagram in isolation and determines if it should be allowed to pass or drop based on administrator-specific rule
- Filtering decisions are based on the following:
  - IP source or destination address
  - Protocol type: TCP, UDP, ICMP, OSPF, and so on
  - TCP or UDP source and destination port



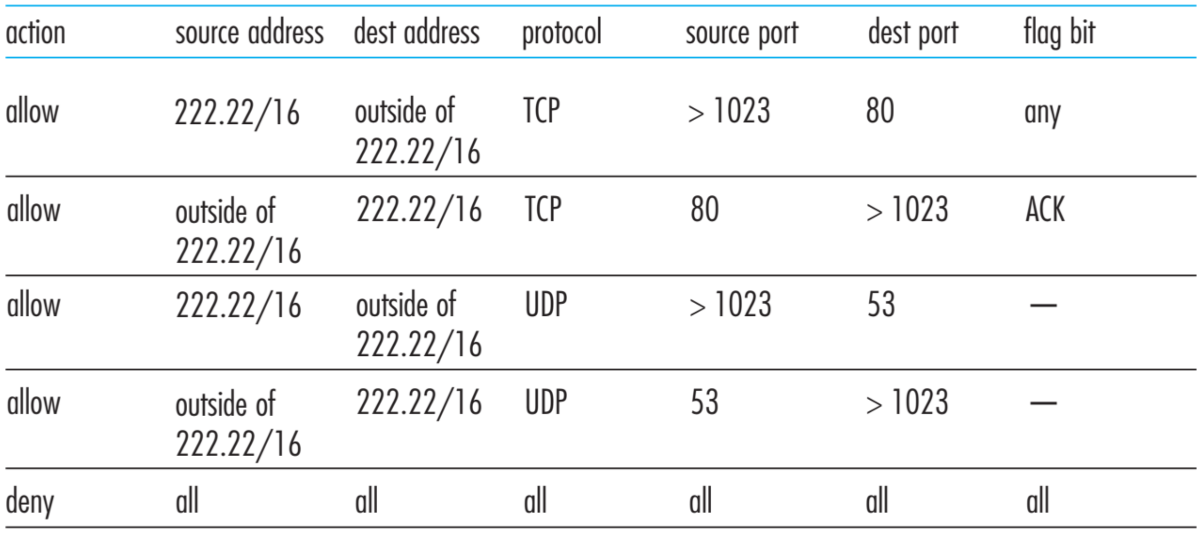
Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Policies and Corresponding Filtering Rules for an Organization's network 130.27/16 with Web server at 130.207.244.203

- TCP flags: SYN, ACK, and so on
- ICMP message type
- Different rules for datagrams leaving and entering the network
- Different rules for the different router interfaces

Traditional Packet Filter Firewall

- Network administrator- configures the firewall based on the policies of the organization
  - Policies are based on user productivity (rules 1, 2 in the policy table), bandwidth usage (rule 3 in the policy table), security (rules 4, 5 in the policy table), etc.
- Policies are manifested as rules – implemented in routers (having multiple interfaces)
- Each router interface is associated with an access control list (See table)
- All the rules are applied to each datagram that passes through the interface



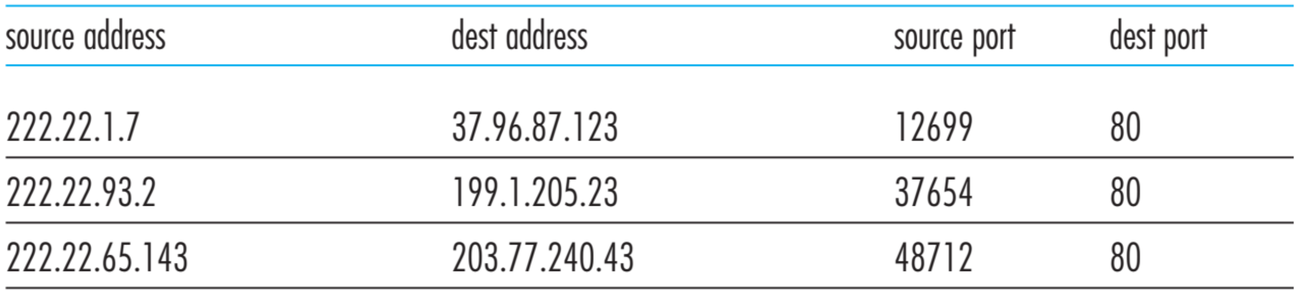
action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	—
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	—
deny	all	all	all	all	all	all

An Access Control List for a Router Interface

- Filtering is done based on a combination of address and port numbers
  - Example: forward all Telnet datagram (those with port number 23) except those going to or coming from a list of specific IP addresses
- Packet filters use the value of TCP ACK bit (0 or 1) to allow or deny requests from external clients to establish connection with internal servers
- Limitation of packet-filtering: provides no protection against datagrams that have their source addresses spoofed

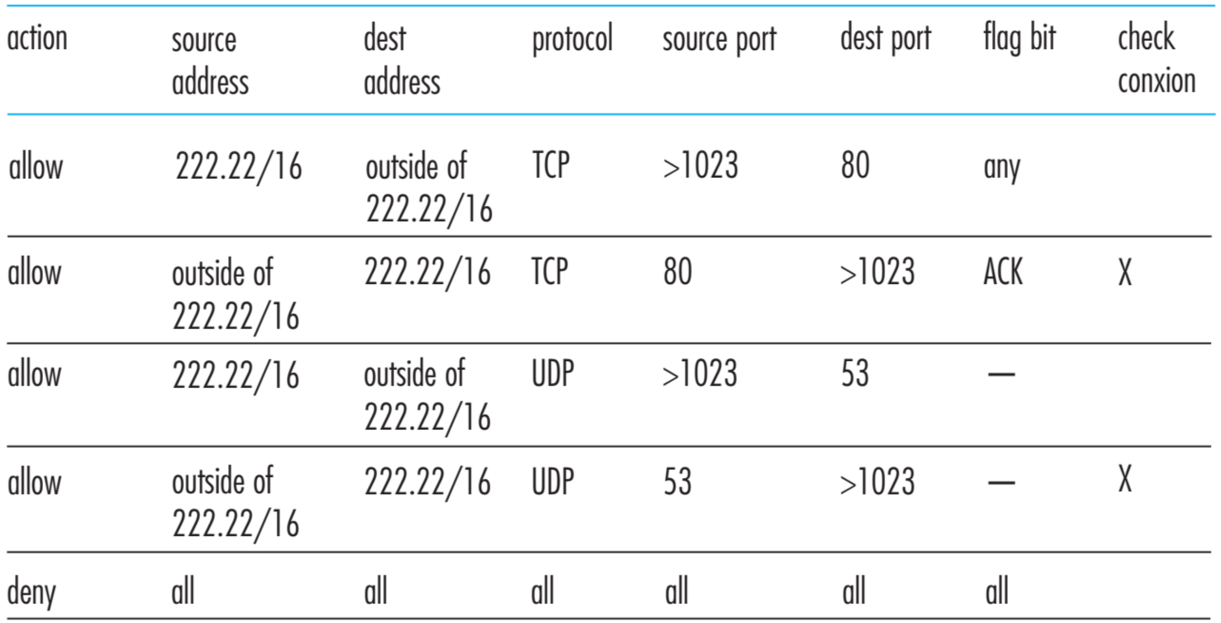
Stateful Packet Filter Firewall

- Tracks TCP connections in a connection table and use this knowledge to make filtering decisions
- Stateful firewall can observe the beginning of a new connection by observing a three-way handshake mechanism (SYN, SYN-ACK, and ACK)
- It can also observe the end of a connection when it sees a packet with TCP FIN bit set to 1
- The firewall can also (conservatively) assume that the connection is over when it hasn’t seen any activity over the connection for a preconfigured duration of time
- Along with the connection table, an extended access control list is also maintained which a new column “check connection” for the incoming traffic



source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Connection Table for Stateful Filter

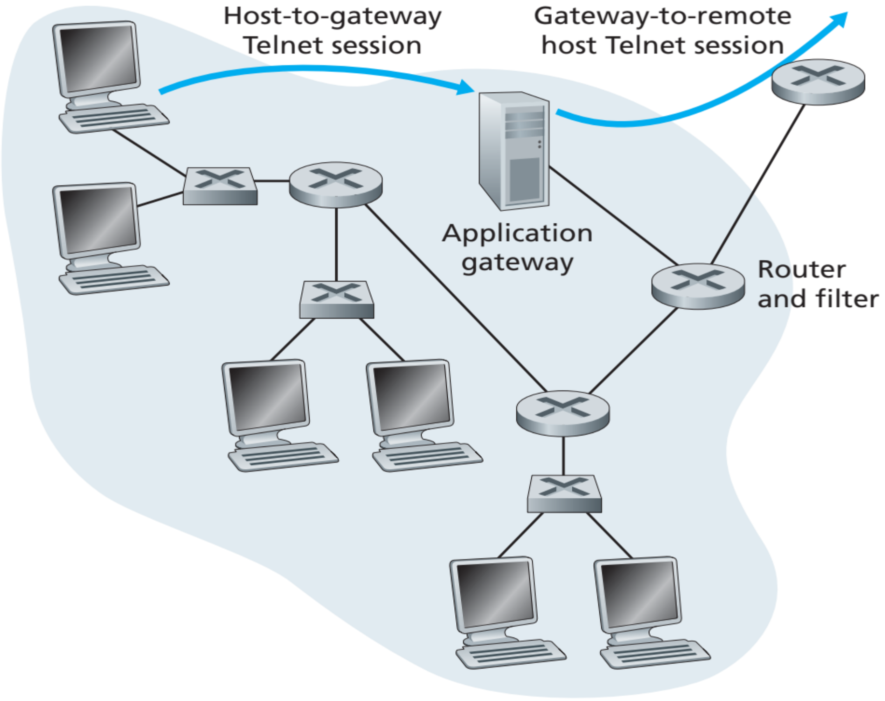


action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	>1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	>1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	>1023	53	—	
allow	outside of 222.22/16	222.22/16	UDP	53	>1023	—	X
deny	all	all	all	all	all	all	

Access Control List for Stateful Filter

Application Gateway

- Limitation of packet-filter firewall
  - Performs coarse grain filtering on the basis of the contents of IP and TCP/UDP headers, including IP addresses, port numbers, and acknowledgement bits
- Finer-level security requirements may frequently arise in any organization
  - Example: providing a Telnet service to a restricted set of internal users such that they authenticate themselves first
  - Not possible with only packet filtering capabilities
  - Need to combine packet filters with application gateways
- Application gateway
  - It is an application-specific server through which all application data (inbound and outbound) must pass
  - Looks beyond the IP/TCP/UDP headers and makes policy decisions based on application data

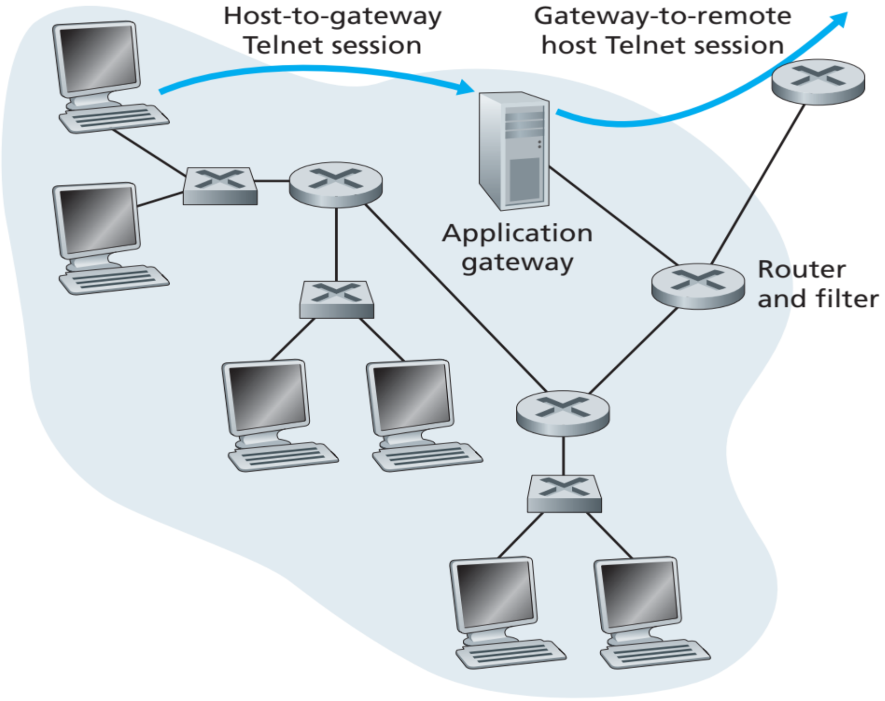


Firewall consist of an Application Gateway and a Filter

- Performs the following functions:
  - User authorization
  - Acts as an application client by setting up connection with an external host
  - Acts as an application server by relaying information from the external server to the user

Application Gateway

- Multiple application gateways can run on single host
  - Each gateway is a separate server with its own set of processes
- Internal networks often have multiple application gateways – HTTP, FTP, and e-mail
- Organization's mail server and Web cache are application gateways
- Disadvantages:
  - A different application gateway is needed for each application
  - There is a performance penalty to be paid, since all data will be relayed via the gateway
    - Overhead increases when multiple users or applications use the same gateway machine
  - Client software must know how to contact the gateway when a user makes a request, and must know how to tell the application gateway what external server to connect


Host-to-gateway Telnet session
Gateway-to-remote host Telnet session
Application gateway
Router and filter

Firewall consist of an Application Gateway and a Filter