Firewalls

Firewalls

Firewalls

- A piece of software or hardware used to screen out malicious programs or users that try to reach computer systems over a network
- Facilitate filtering incoming and outgoing traffic that flows through a system
- Use sets of rules to inspect network packets as they come in and go out of network connections
- Either blocks or allows the traffic
- The rules can inspect one or more packet characteristics (Source, Destination, Protocol type, ports etc)

Firewalls

- Provides perimeter defense :
  - Protect and insulate applications, services and machines of an internal network from unwanted, untrusted Internet traffic.
- Support Network Address Translation (NAT)
  - Internal computers to use private IP addresses
  - Internal computers share a single connection to the Internet
- Examples: Cisco PIX, Check point Firewall-1, NetScreen

General Firewall Features

- Port Control
- Network Address Translation
- Application Monitoring (Program Control)
- Packet Filtering

Additional Firewall Features

- Data encryption
- Hiding presence
- Reporting/logging
- e-mail virus protection
- Pop-up ad blocking
- Cookie digestion
- Spy ware protection etc.

Firewall Design Principles

- 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

Firewall Characteristics

- 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

Firewall Characteristics

- Design goals:
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Firewall Characteristics

- Four general techniques:
- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
- Direction control
  - Determines the direction in which particular service requests are allowed to flow

Firewall Characteristics

- User control
  - Controls access to a service according to which user is attempting to access it
- Behavior control
  - Controls how particular services are used (e.g. filter e-mail)

Network Address Translation (NAT)

- Basic definition:
  - Process of converting one IP address to another by modifying the IP address information in the IP headers while a packet is on transit
  - Usually implemented in a firewall separate from the policy or rule set.

Network Address Translation (NAT)

- Static NAT
  - The host is defined with a local address and a corresponding global address
  - Simple to implement
  - Used to provide access to trusted hosts inside a firewall perimeter

Network Address Translation (NAT)

- Dynamic NAT
  - Maps a group of internal local addresses to one or more global addresses
  - Secure than static NAT
  - Limits the number of concurrent users on the inside who can access external resources simultaneously

Firewalls

- Desired attributes
  - All communication must pass through the firewall
  - Permits only authorized traffic
  - Immune to penetration
    - Can withstand attacks directed on it

Firewall Layer of Operation

- Network Layer
- Application Layer

Network Layer

- Makes decision based on the source, destination addresses, and ports in individual IP packets.
- Based on routers
- Has the ability to perform static and dynamic packet filtering and stateful inspection.

Firewalls and TCP/IP

- Data transmission achieved in blocks of data called packets
- Each layer of the OSI model adds a header to the packet; a process called encapsulation
- Firewall uses information contained in the packet headers to make access control decisions

Encapsulation

- Email message: Hello word.
- Application data:
- APP Protocol :SMTP + App Data
- Transport header{TCP/UDP}
- TCP hdr+ App hdr+ App data {Port number}
- IP hdr+ TCP hdr+ App hdr+ App data {IP Addr SA;DA}
- Ethernt hdr + IP hdr+ TCP hdr+ App hdr+ App data + Ethernet Trailer {MAC Address}

Firewalls and TCP/IP

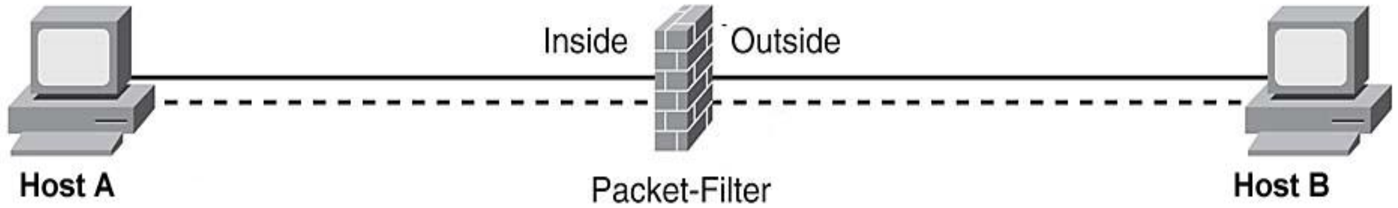
- TCP connection
  - Server ports: Integer less than 1024
  - Client ports: Integer between 1024 and 16383
- TCP/IP ports:
  - Most well known services listen on universally known ports (httpd:80, FTP:21, SSH:22, DNS: 53 etc)

Firewalls

- Classification
  - Packet filters
  - Application Gateways
  - Circuit-Level gateways
  - Stateful packet inspection engines

Packet Filtering Firewalls

- Simplest form of firewalls to implement



- Offer security by filtering network communications based on information contained in packet headers

Packet Filtering Firewalls

- Decision making based on the following packet header information:
  - The source and destination IP addresses
  - Protocol in use (TCP, UDP or ICMP) or Next header
  - TCP or UDP source and destination ports
  - TCP flags (SYN, ACK, FIN etc)
  - For ICMP: ICMP message type

Packet Filtering Firewalls

- Filtering by Interfaces
  - Based on incoming or outgoing interfaces
    - Ingress filtering (e.g. of spoofed IP addresses) and egress filtering
- Filtering by services
  - Relies on information about ports

Packet Filtering Firewalls

- Configuration approaches
  - Guided by corporate security policy
  - Use logical expressions to specify allowable packets based on packet fields
  - Expression writing will be vendor specific
  - Rule of thumb:
    - All that is not expressly allowed is prohibited
    - Build rules from most to least specific
    - Place the most active rules near the top of the rule set

PF Firewalls – Security and Performance

- Performance:
  - Degradation depends on the number of rules
  - Order rules to deal with most common traffic first
  - Correctness vs speed trade-off
- Security:
  - IP spoofing
  - Tiny fragments attack:
    - Splits TCP header info into tiny fragments
    - Soln: Discard or reassemble before check

Packet Filtering Firewalls

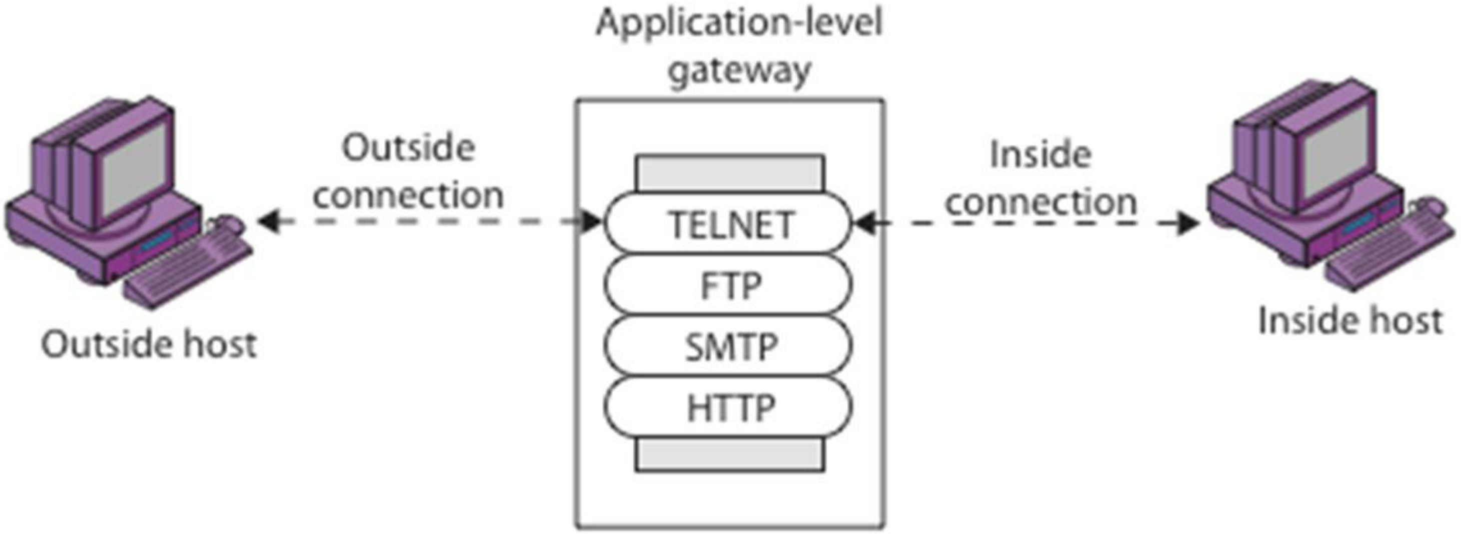
- Advantages
  - Good performance
  - Cost-effective
  - Transparency
  - Good for traffic management

Packet Filtering Firewalls

- Disadvantages
  - Direct connections permitted
  - Poor scalability
  - Large port ranges may be opened
  - Vulnerability to spoofing attacks

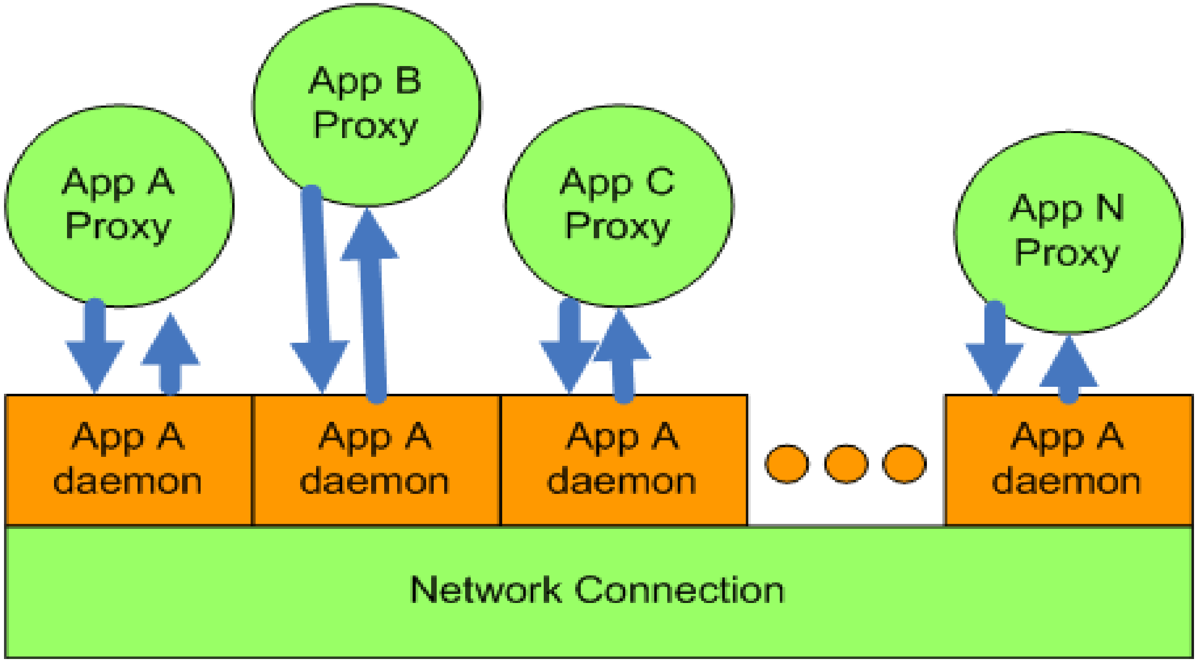
Application Gateways

- Has full access to protocol
  - User requests services from proxy
  - Proxy validates then forwards user requests
  - Returns results to the user



Application Gateways

- Architecture



  - Apps: Telnet, FTP, SMTP
  - Daemons spawn proxies

Application Gateways

- Access decision making
  - Packet information at all seven layers of the OSI model
  - Thought of as being application aware
  - Often act as intermediary of other applications e.g. email, FTP or HTTP etc
  - Act as server to the client and as client to the true server.
  - Complete requests on behalf of the users it is protecting
- Has been used variously to mean:
  - Bastion host
  - Proxy gateway
  - Proxy server

Application Gateways

- Provide security at the expense of:
  - Performance: Higher latency. i.e. Each user request is in reality two separate connections
  - Transparency
    - Require modification of the client behaviour to recognize proxies
    - Gateways must differentiate between safe and dangerous actions of an application
  - Reliance on proxy for all applications
    - Proxy servers for popular services are widely available

Circuit Level Gateways

- Similar to application gateways but are not application aware
- Work at TCP level. i.e. by relaying TCP connections from trusted network to untrusted networks
- Connection information supplied by clients i.e. application gateways use modified procedures while circuit level gateways use modified clients

Circuit Level Gateways

- Advantages
  - Provide services to many different protocols
  - Can support a wider variety of communications
- Disadvantages
  - Clients must be able to use them
  - Cannot inspect application layer

Stateful Packet Inspection (SPI) Firewalls

- Based on a set of rules similar to Packet filters
- State-awareness:
  - Decision made not only based on IP address and ports but also on other packet header information such as SYN, FIN, sequence number etc
  - Examine higher layer packets i.e. match returning packets with outgoing flows
  - Keep track of client-server connections
  - Checks that each packet validly belongs to a connection

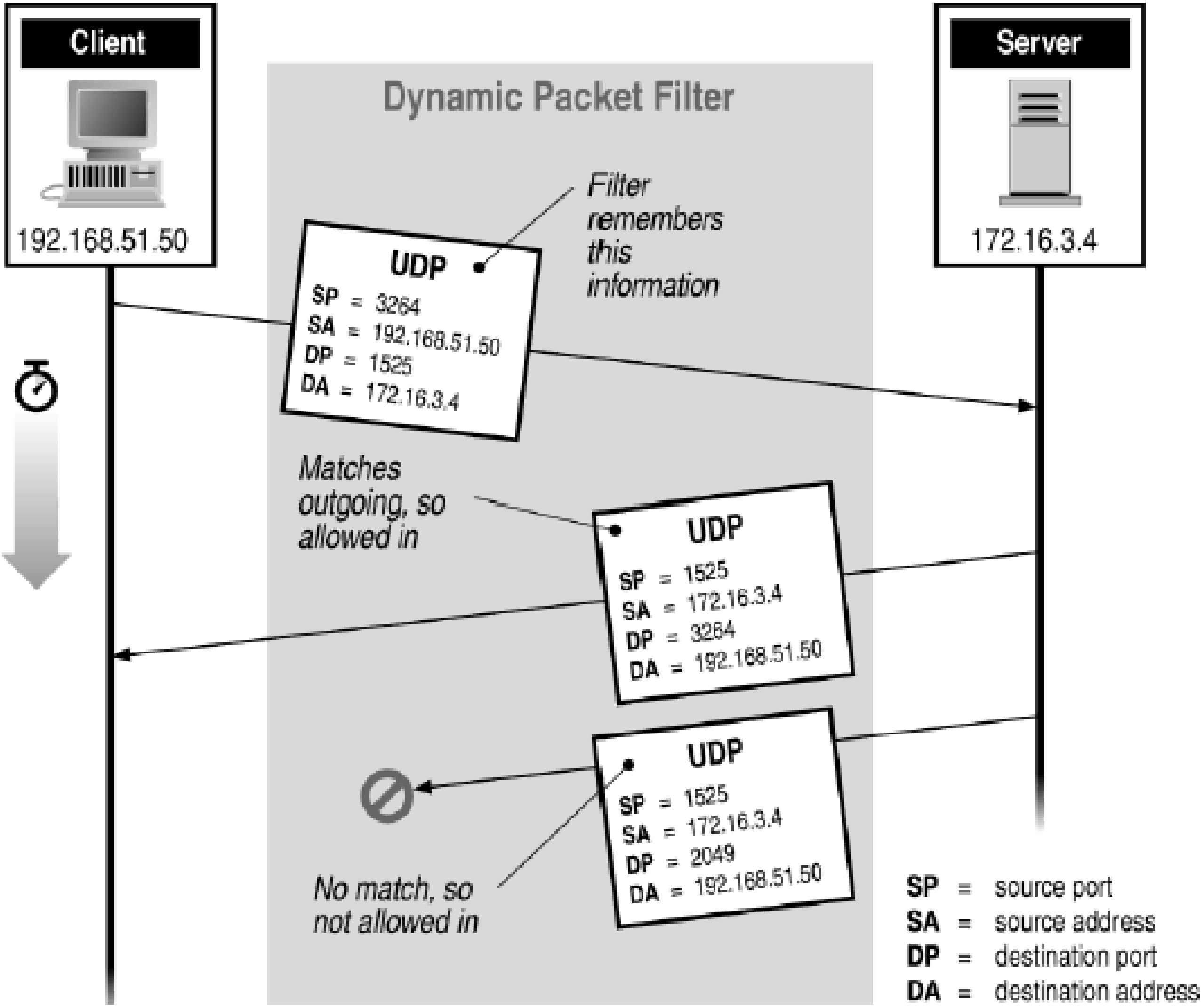
SPI Firewalls

- When packet arrives on an interface
  - Headers are inspected to determine whether the packet is part of an existing, established flow. This information is retrieved from the “connections table”.
  - Can further inspect the application layer details of the packet to make decisions
  - If no corresponding entry in the connections table, SPIF inspects the packet against configured rule set

SPI Firewalls

– SPIF use timers and other details e.g. TCP packets with FIN bit set as away to determine when to delete entries from the connection table

SPI Firewalls



SPI Firewalls

- Advantages
  - Protect against spoofing
  - Ability to look into the data of certain packet types

Firewalls

- Strengths:
  - Effective at enforcing corporate policy
  - Can be used to provide selective access to specific services
  - Excellent auditing tools
  - Good at incidence reporting (alert features)

Firewalls

- Weaknesses
  - Cannot protect against attacks embedded in authorized traffic
  - Are only as effective as the rules they are configured to enforce
  - Are not immune to social engineering attacks
  - Cannot fix poor security policies or poor administrative practices
  - Cannot stop attacks if the traffic does not pass through them

Viruses and Firewalls

- In general, firewalls cannot protect against viruses
  - An anti-virus software is needed for that purpose
- However, many security suites such as those offered by MacAfee and Norton offer the complete protection
- Some software firewalls such as Zone Alarm Pro may contain limited virus protection features