CS 465 Computer Security

Kent Seamons

Sources:

Schneier, Secrets and Lies
Stallings, Network Security Essentials

Last update: Nov 14, 2005

Network Security and Defenses

- Goals:
  - Understand basic terminology
  - Understand basic threats
  - Understand defenses
    - limitations

Network Security

- IP security
  - IP spoofing
- DNS security
- Denial-of-service attacks
  - SYN flooding
  - Mail bombing
- Distributed denial-of-service attacks
  - Pizza delivery attack

Network Defenses

- Firewalls
- Demilitarized zones
- Virtual private networks
- Intrusion detection systems
- Honeypots
- Vulnerability scanners

Firewalls

- A machine that protects a company’s internal network from attackers
- Ways to defeat a firewall
  - Go around it
  - Sneak something through it
  - Take it over
- Types
  - Packet filters
  - Application gateways (proxies)

Demilitarized Zone

- Employ two logical firewalls
- One firewall protects DMZ from the outside world
- Another firewall protects the internal network from the DMZ
- Place web servers in the DMZ

Virtual Private Networks

- A secure connection over a public network
- Two main uses
  - Connect disjoint pieces of the same network
  - Connect mobile users
- Common protocol – IPSec (growing use of TLS)

Intrusion Detection Systems (IDS)

- Network monitors
- Two basic approaches
  - Misuse detection
  - Anomaly detection
- Example: Snort
  - www.snort.org
  - www.sans.org/resources/idfaq/
- Example: Tripwire (file system intrusions)
  - www.tripwire.org
  - sourceforge.net/projects/tripwire

Honeypots

- Entire dummy computers and subnetworks designed to look inviting to attackers
- Early example (if not the first)
  - Cliff Stoll, “The Cuckoos Egg”

Vulnerability Scanners

- Automated program to scan the network looking for weaknesses
  - Identify information about a host
    - What O/S is running
    - What ports accept connections
- A useful tool for attackers and defenders
- Example: nmap (“Network Mapper”)
  - www.insecure.org

Firewalls (more details)

- Effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet
- It is not practical to equip each server and workstation on a network with strong security features

Firewall Design

- The firewall is inserted between the local area network and the Internet
- Aims:
  - Establish a controlled link and erect an outer security wall or perimeter
  - Protect the local network from Internet-based attacks
  - Provide a single choke point where security and audit can be imposed

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

Firewall Limitations

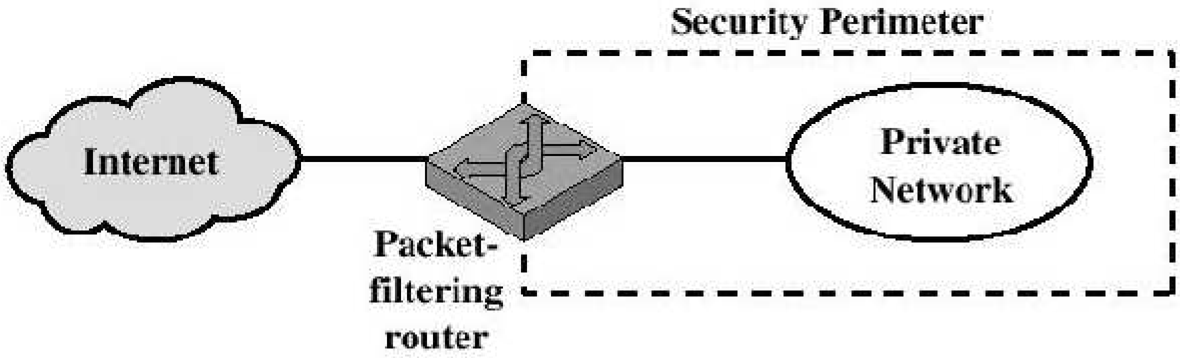
- Cannot protect against attacks that bypass the firewall, such as dial-in and dial-out capabilities
- The firewall does not protect against internal threats
- The firewall cannot protect against the transfer of virus-infected programs or files

Types of Firewalls

- Three common types of firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways

Types of Firewalls

- Packet-filtering Router



Types of Firewalls

- 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)

Types of Firewalls

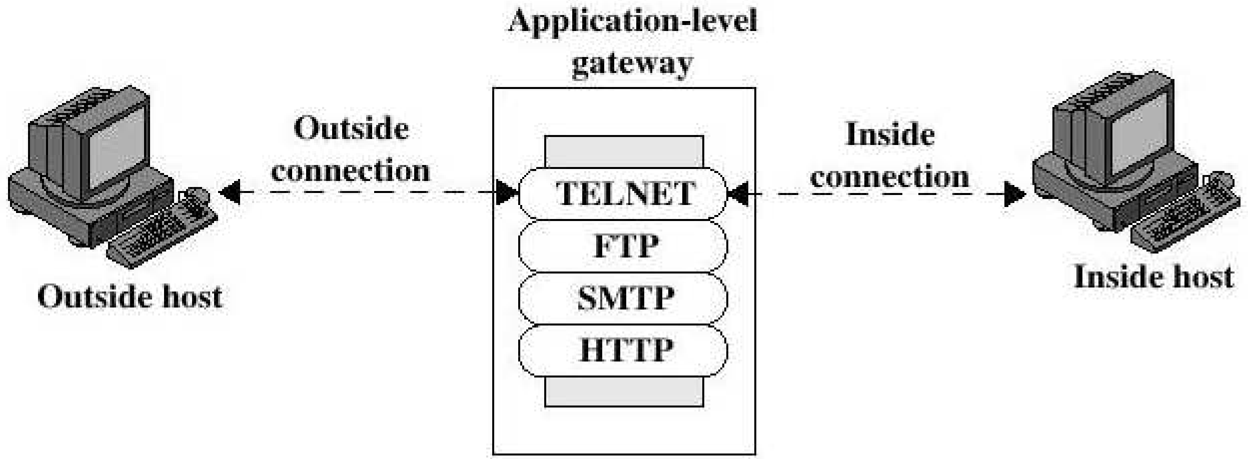
- Advantages:
  - – Simplicity
  - – Transparency to users
  - – High speed
- Disadvantages:
  - – Difficulty of setting up packet filter rules
  - – Lack of authentication

Types of Firewalls

- Possible attacks
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

Types of Firewalls

- Application-level Gateway



Types of Firewalls

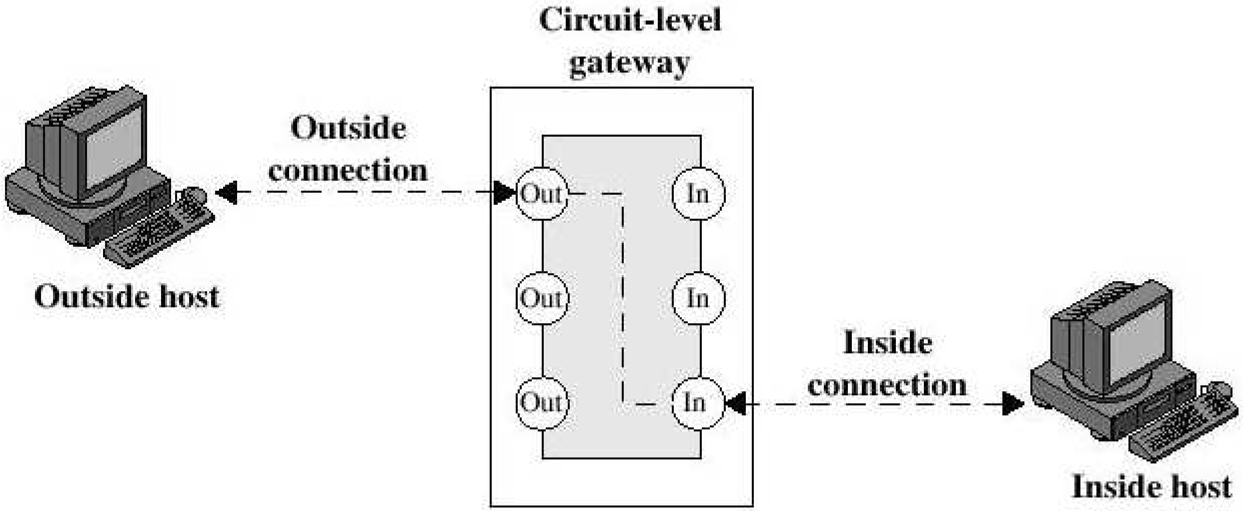
- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic

Types of Firewalls

- Advantages:
  - Tend to be more secure than packet filters
  - Only need to scrutinize 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

- Circuit-level Gateway



Types of Firewalls

- Circuit-level Gateway
  - Stand-alone system or
  - Specialized 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

Types of Firewalls

- Circuit-level Gateway
  - The security function consists of determining which connections will be allowed
  - Typically used is a situation in which the system administrator trusts the internal users
  - An example is the SOCKS package

Types of Firewalls

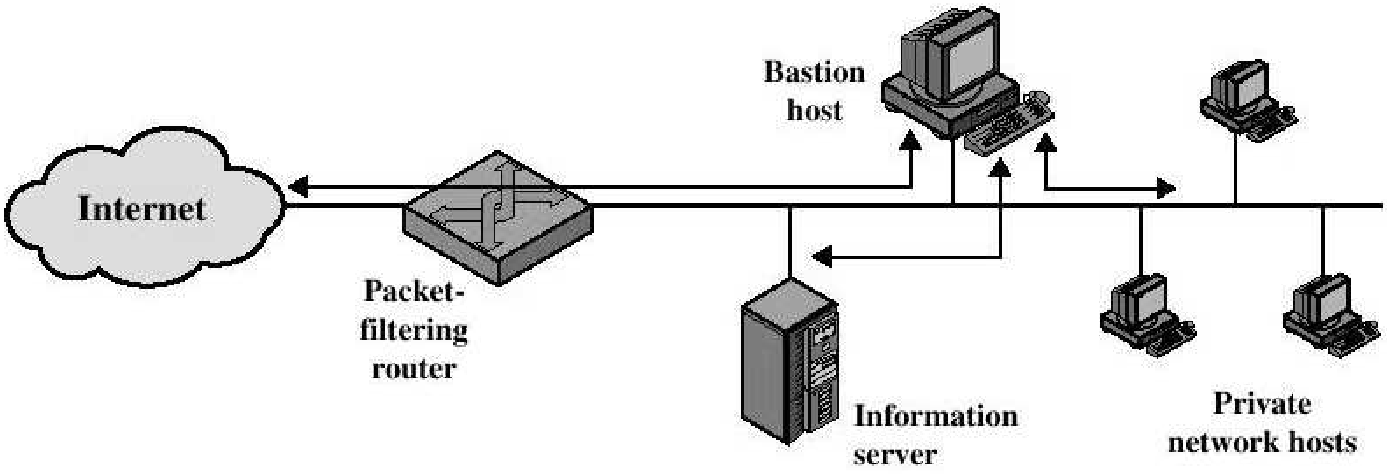
- Bastion Host
  - A system identified by the firewall administrator as a critical strong point in the network´s security
  - The bastion host serves as a platform for an application-level or circuit-level gateway

Firewall Configurations

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- Three common configurations

Firewall Configurations

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



Firewall Configurations

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

Firewall Configurations

- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions

Firewall Configurations

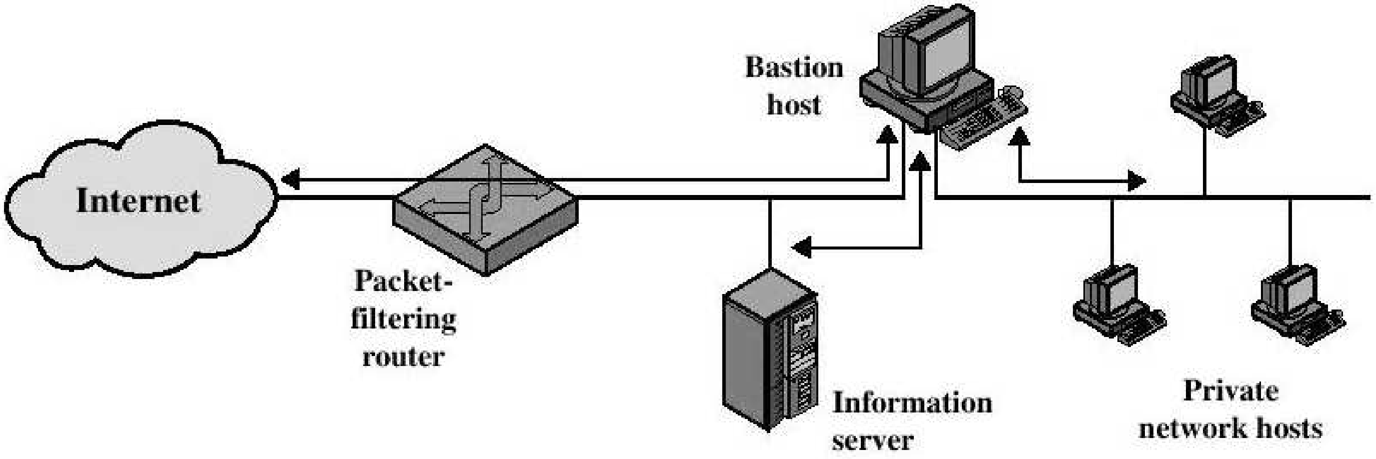
- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems

Firewall Configurations

- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)
  - The packet filtering router may allow direct traffic between the information server and the Internet

Firewall Configurations

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

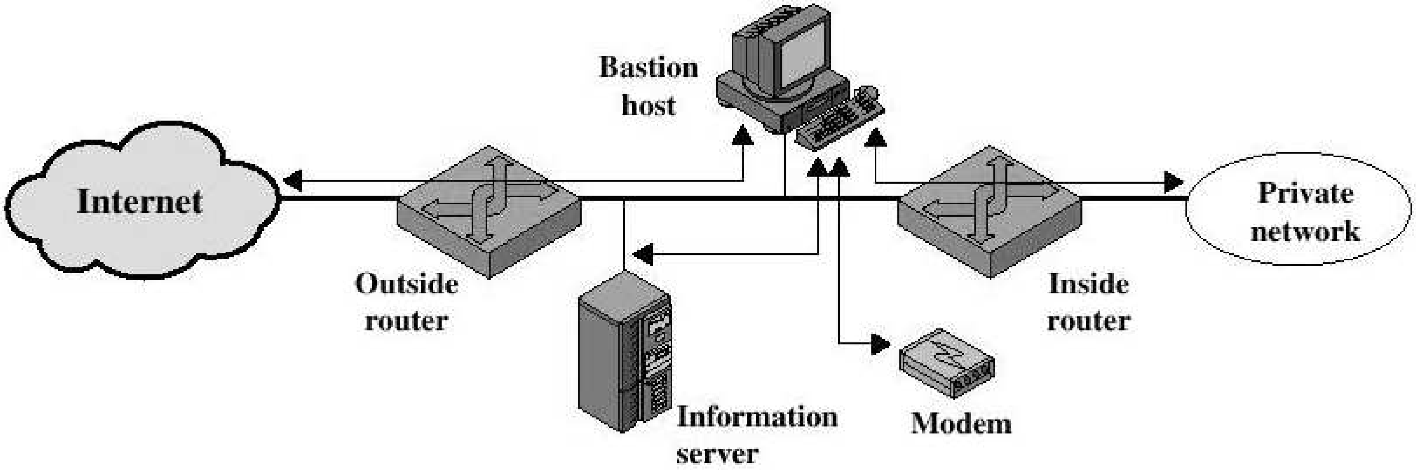


Firewall Configurations

- Screened host firewall, dual-homed bastion configuration
  - If the packet-filtering router is completely compromised, traffic must still flow through the bastion host
  - Traffic between the Internet and other hosts on the private network must flow through the bastion host

Firewall Configurations

- Screened-subnet firewall system



Firewall Configurations

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

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

- Examples
  - Packet filtering – Unix iptables (ipchains)
  - Personal firewall – run on your PC to protect your home network
    - BlackICE
    - Zone Alarm Pro
    - Symantec Norton Personal Firewall
    - Many others