Firewalls

Network Security (NETSEC)

Yuhong Li

Stockholm University

Outline

Stockholm University

- Introduction
  - Design goals and limitations
  - Mechanisms
- Types
  - Packet filters
  - Stateful inspection
  - Proxy
- Firewall basing, location and configuration

Stockholm University

Introduction

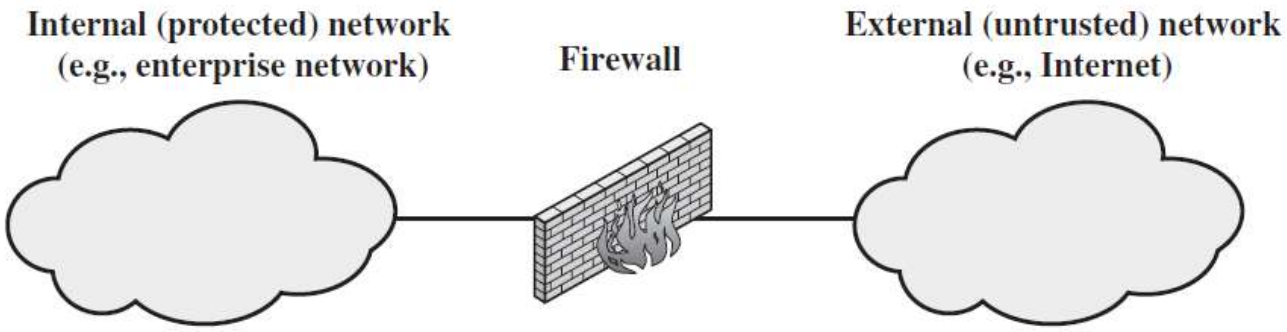
The Need for Firewalls

Stockholm University

- Internet connectivity no longer optional for organizations.
  - Interconnected PCs, servers, LANs create a threat to the organization, enable the outside world to reach and interact with local network assets
- Possible but not feasible or cost-effective to equip each workstation and server with strong security features
- When a security flaw is discovered, each affected system must be upgraded to fix that flaw
- A widely accepted alternative or complement to host-based security services is the firewall

Firewall -1

- Firewall is inserted between the organization network and the Internet to establish a controlled link and to set up an outer security wall or perimeter
- The aim is to protect the local network from Internet-based attacks and to provide a single control point where security and auditing can be enforced
- Firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function



Firewall -2

- Firewall may be a server
  - running a firewall software product
  - specialized hardware device
- Software firewalls
  - McAfee, Symantec, Microsoft
- Hardware firewalls
  - E.g., Cisco, Nokia, Watchguard
- Firewall is able to
  - Monitor packets coming into and out of the network it is protecting
  - Can discard, redirect, filter packets

Design Goals for a Firewall

Stockholm University

- All traffic from inside to outside, and vice versa, must pass 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

Mechanisms used by Firewall

Stockholm University

Mechanisms used to control access and enforce security policy:

1. Service control: determines the types of Internet services that can be accessed, inbound or outbound. Filtering can be done in different ways
2. Direction control: determines the direction in which particular service requests may be initiated and allowed to flow through the firewall
3. User control: controls access to a service according to which user is attempting to access it
4. Behavior control: controls how particular services are used. Example: the firewall may filter e-mail to eliminate spam.

Firewall - Expectations

Stockholm University

A single point that keeps unauthorized users out of the protected network
- Prohibits vulnerable services from entering or leaving the network
- Provides protection against IP spoofing and routing attacks

Provides a location for monitoring security related events.

Audits and alarms can be implemented on the firewall system

A convenient platform for several Internet functions that are not security related.
E.g., a network address translator (NAT); a network management function that audits or logs Internet usage

Serve as the platform for IPSec . Using the tunnel mode capability, the firewall can be used to implement virtual private networks

Firewall - Limitations

Stockholm University

- Cannot protect against attacks that bypass the firewall
- A laptop, or portable storage device may be used and infected outside the corporate network, and then attached and used internally
- May not protect fully against internal threats
- An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
- Cannot protect directly against malicious software – too much cost

Stockholm University

Types of Firewalls

- Packet filters
- Stateful Inspection
- Proxy Firewalls

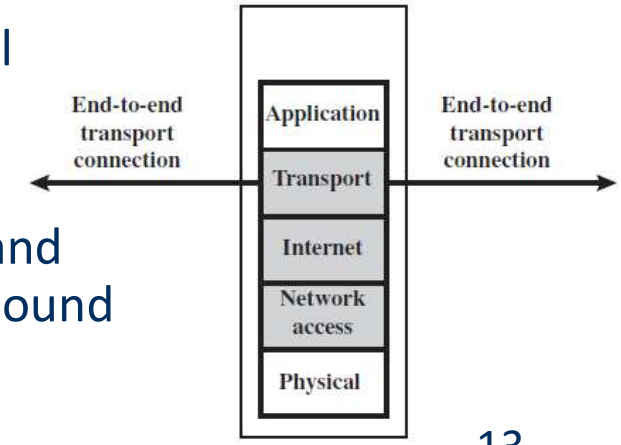
Packet Filters -1

Stockholm University

- First generation, most rudimentary type of firewall technologies
- Built into a majority of the firewall products
- Routers can be configured to perform packet filtering
- Configured with ACLs, which dictates rules (the type of traffic allowed into and out specific networks)

Packet Filters -2

- Capabilities
  - Review protocol header information at the network and transport levels
  - Carry out PERMIT and DENY actions on individual packets
- Makes access decisions based upon network-level protocol header values
- Decisions are based on:
  - Source and destination IP addresses, Source and destination port numbers, Protocol types, Inbound and outbound traffic direction, interface



Packet Filters -3

Stockholm University

- When packet arrives at a packet filtering device, ACLs filtering rules enforced in network interface of the device
- Device compare packet characteristics to each rule set in the ACL. If a successful match is found (permit or deny), then the remaining rules are not processed.
- If no matches are found when the device reaches the end of the list, the traffic should be denied.
- Each interface has own ACL values
  - indicate allowed type of traffic in (one interface) and out(another interface)

Pros and Cons

Stockholm University

- Weakness
  - Cannot protect from attacks at application level, does not understand ”full picture” of the communication
  - Can only focus on individual packet characteristics
  - Due to the limited information available to the firewall, the logging functionality present is limited
  - Most packet filter firewalls do not support advanced user authentication schemes
  - Generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack
  - Susceptible to security breaches caused by improper configurations
- Strength
  - Simple
  - Transparent to users and are very fast

Attacks and countermeasures

Stockholm University

IP address spoofing

The intruder transmits packets from the outside with a source IP address field containing an address of an internal host

Countermeasure is to discard packets with an inside source address if the packet arrives on an external interface

Source routing attacks

The source specifies the route that a packet should take as it crosses the internet, in the hopes that this will bypass security measures that do not analyze the source routing information

Countermeasure is to discard all packets that use this option

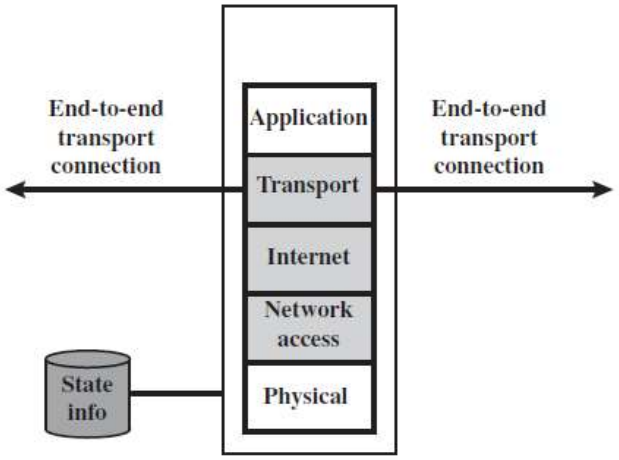
Tiny fragment attacks

The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. Small fragments may be used in denial of service attacks or in an attempt to bypass security measures or detection.

Countermeasure is to enforce a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header

Stateful Inspection -1

- Curious neighbor
- Packets are captured by the inspection engine operating at TCP layer
  - Some keep track of TCP sequence number -> prevent session hijacking
  - Some even inspect the higher layers of the packet (e.g., FTP, IM and SIPS commands) ->identify and track app level connections
- Store information of the specific connection in the state table (IP addresses, header flags, timestamps, etc.)
- Keep track on states (LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, etc.)



State Information (example)

Stockholm University

Example Stateful Firewall Connection State Table [WACK02]

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	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
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Stateful Inspection -2

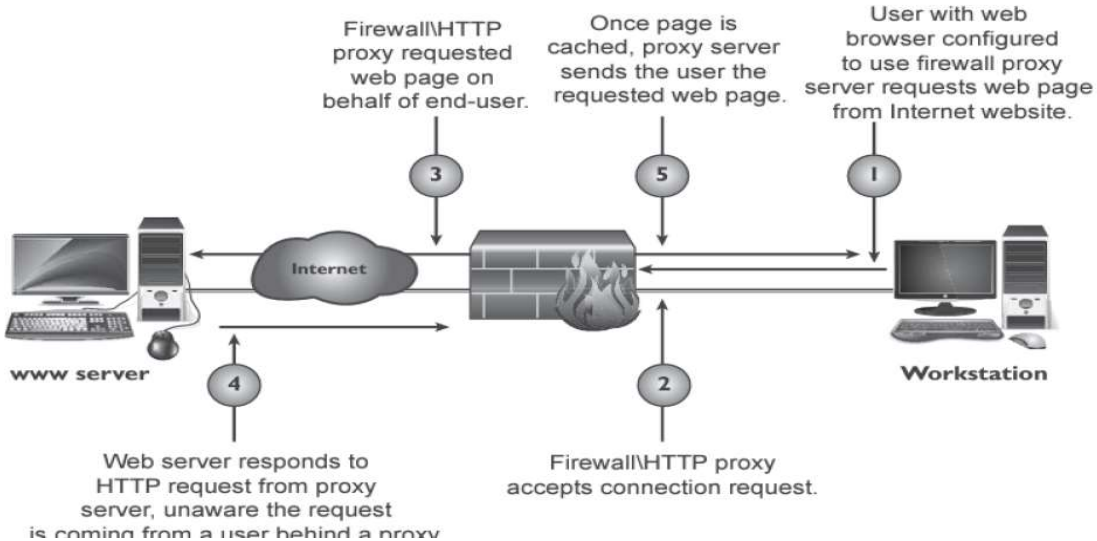
Stockholm University

- Knows how protocol are supposed to work
- Keep track on each step of communication (states, acknowledgement, sequence number)
  - SYN, SYN/ACK, ACK
- Cannot be fooled about ”already established connection”
  - SYN/ACK packet first
- Victim for flooding attacks (flooding the state table)
  - State table full ->device freeze or reboot->lose info about recent connections->deny legitimate packets

Proxy Firewalls -1

- Middleman, stands between trusted and untrusted network
- Breaks communication channel(no direct communication)
  - Stops the user connection at internal interface
  - Ends communication session and restarts it on behalf of the sending system at external interface

- Circuit-level proxy
- Application level proxy



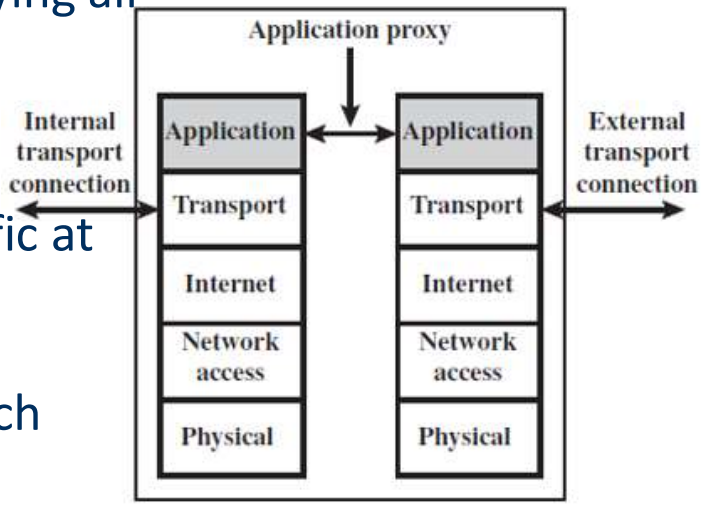
Application Level Gateway/Application Proxy

Stockholm University

- Acts as a relay of application-level traffic
- Understand the packet as a whole
- Make access decisions based on the packet content (e.g., can distinguish between FTP GET and FTP PUT command)
  - Understand services, protocols, and commands of the protocol it uses
    - E.g., an application level proxy/filter for email will understand RFC 822 headers, MIME-formatted attachments, and may identify virus-infected software, check email for dirty words
  - Has one proxy (a specialized program) per service and protocol (FTP, SMTP, HTTP, etc.)
  - The firewall must implement the proxy code for a specific application

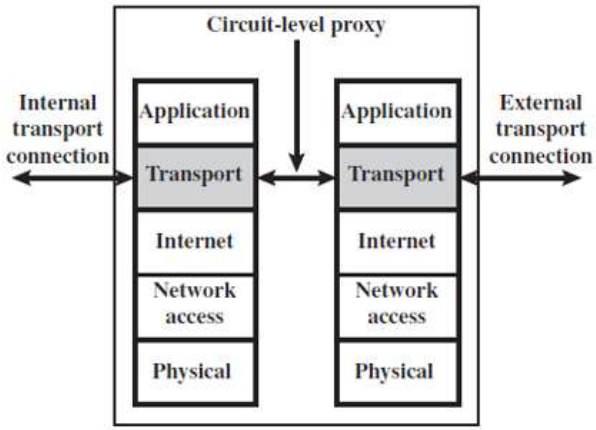
Application Level Gateway

- The gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features
- Tend to be more secure than packet filters
  - Check the whole packet
  - It is easy to log and audit all incoming traffic at the application level.
- Disadvantage:
  - The additional processing overhead on each connection



Circuit-Level Gateway/Circuit-level Proxy

- Work at transport level
- Does not permit an end-to-end transport connection
  - The gateway sets up two TCP connections
- Cannot look into contents of a packet
  - Application independent
- Decision based on
  - Protocol header
  - Session information
- Useful to hide info about internal computers (IP addresses, software programs, email addresses)
- Can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications



Circuit-Level Gateway

Stockholm University

- The security function consists of determining which connections will be allowed
- A typical use is a situation in which the system administrator trusts the internal users.
  - The gateway can be configured to support application-level service on inbound connections and circuit-level functions for outbound connections.
  - No overhead on outgoing data

Stockholm University

Firewall Basing

Bastion Host - Common Characteristics 1

Stockholm University

- A critical strong point in the network's security, typically serves as a platform for an application-level or circuit-level gateway
  - Can be used for collecting data, monitoring traffic for the purpose of alarm, auditing
- Highly exposed device, resides close to untrusted network or connected to it -> Special effort in designing and configuring bastion hosts to minimize the chances of penetration
  - Should be hardened(locked down)
  - Only the services that the network administrator considers essential are installed. These could include proxy applications for DNS, FTP, HTTP, and SMTP

Bastion Host - Common Characteristics 2

Stockholm University

- May require additional authentication before a user is allowed to access to the proxy services
  - Each proxy is configured to allow access only to specific host systems
- Each proxy is independent of other proxies on the bastion host.
  - If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications.
  - If the user requires support for a new service, the network administrator can easily install the required proxy on the bastion host
- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection

Host-Based Firewall

Stockholm University

- Is a software module used to secure an individual host
  - Is available in many operating systems or can be provided as an add-on package
- Filters and restricts the flow of packets
- Common location for host-based firewall is a server
- Advantages:
  - Filtering rules can be tailored to the host environment
  - Protection is provided independent of topology
  - Used in conjunction with stand-alone firewalls, provides an additional layer of protection

Personal Firewall

Stockholm University

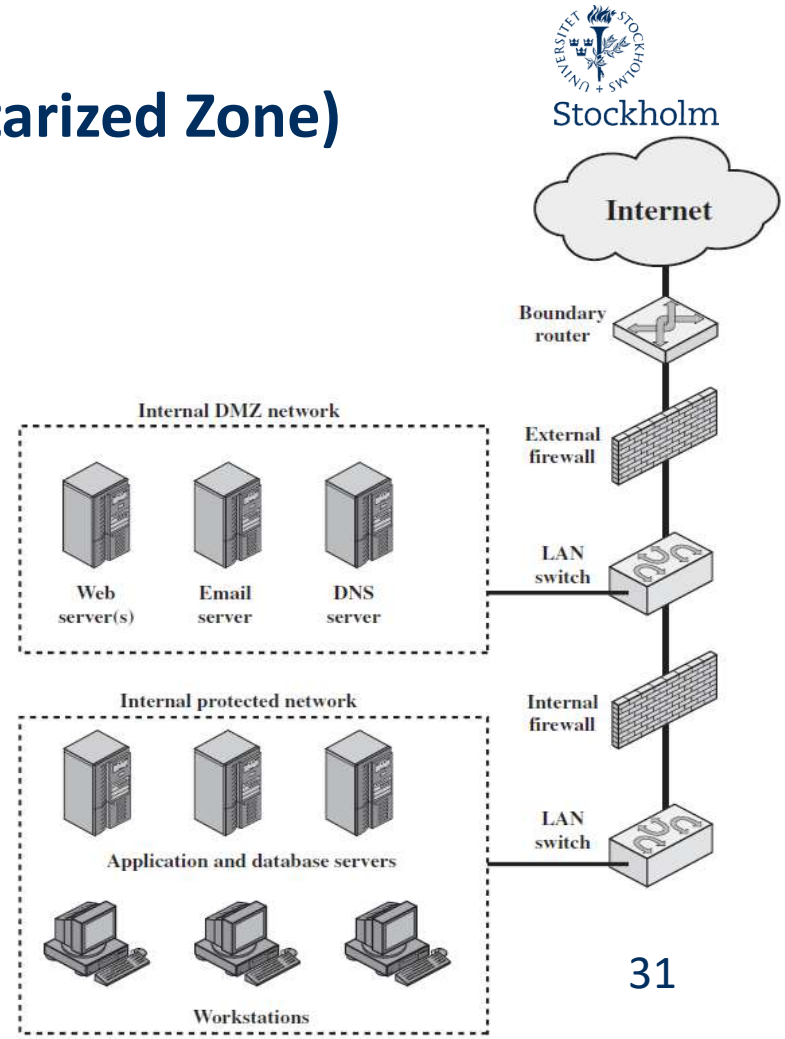
- Controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side
  - used in the home environment and on corporate intranets.
- The primary role is to deny unauthorized remote access to the computer.
- Can also monitor outgoing activity in an attempt to detect and block worms and other malware.

Stockholm University

Firewall Location and Configurations

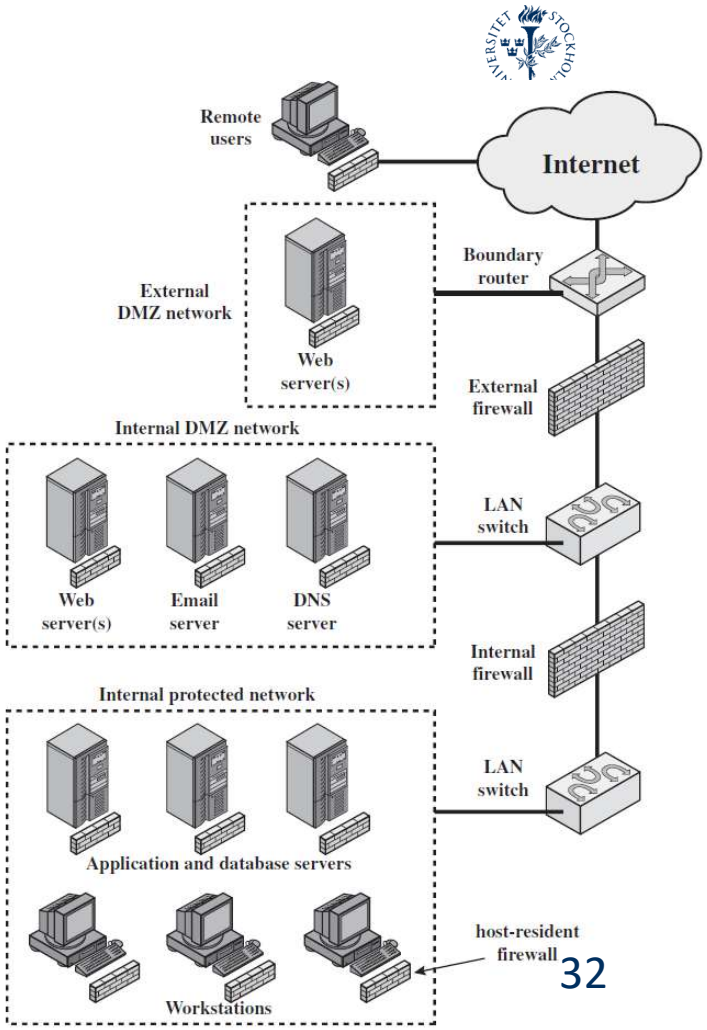
Firewall configuration – DMZ (Demilitarized Zone)

- External FW: at the edge of a local network.
- Internal FW
  1. Internal FW adds stricter filtering capability, compared to the external FW
  2. Internal FW provides two-way protection with respect to the DMZ.
     - protects the remainder of the network from attacks launched from DMZ systems.
     - can protect the DMZ systems from attack from the internal protected network.
  3. Multiple internal FWs can be used to protect portions of the internal network from each other.



Distributed Firewall Configuration

- Involves stand-alone FW devices and host-based FWs, working together
- Each individual host enforces the security policy, which is set by a central management node.
- Important aspect is security monitoring
  - Includes log aggregation and analysis, FW statistics
- Advantage: lack of central point of failure



VPN (Virtual Private Network)

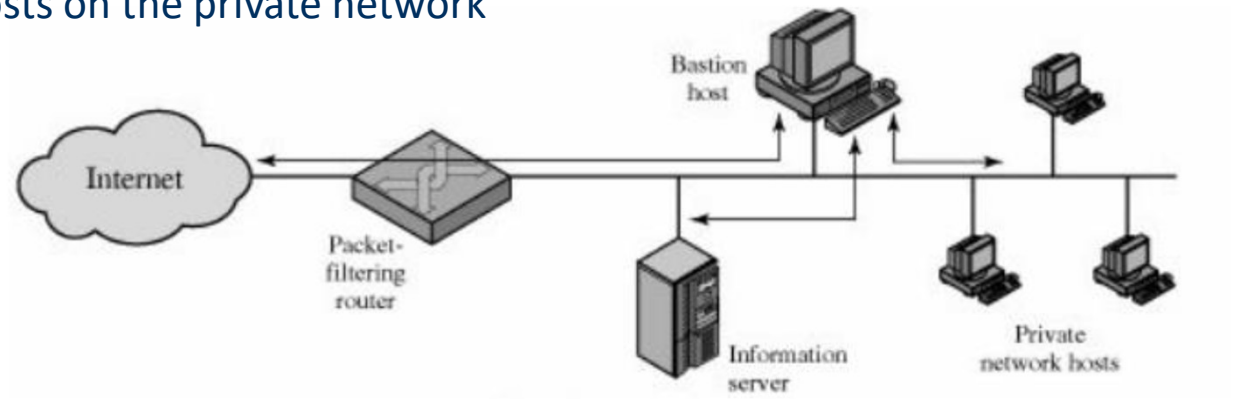
Stockholm University

- VPN: provide a secure connection through an insecure network (e.g., Internet) by using encryption and authentication in the lower protocol layers.
- Firewall: encryption

Screened Host Firewall System (single-homed bastion host)

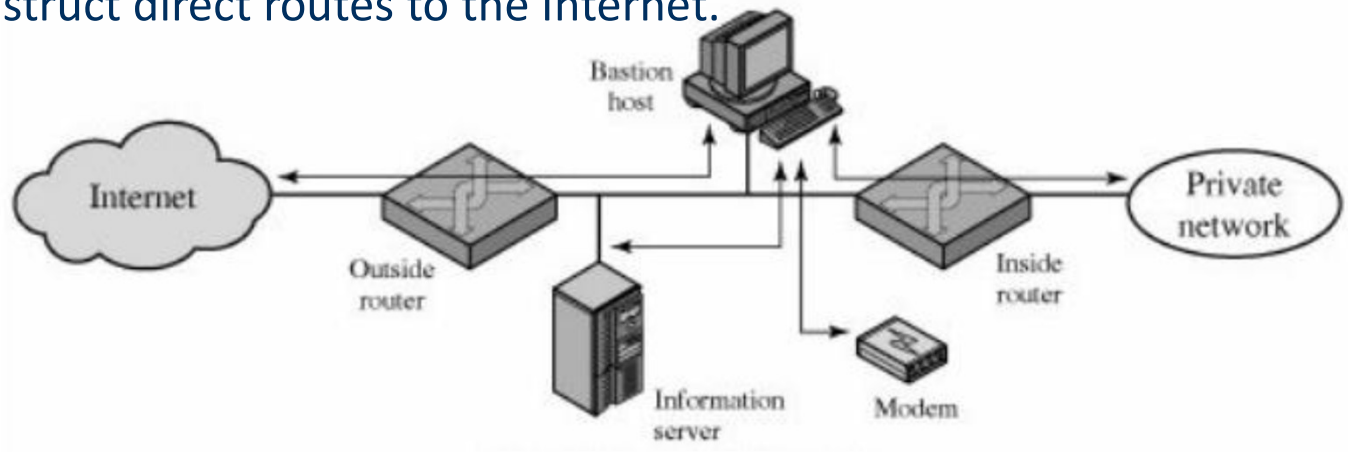
Stockholm University

- Consists of two systems: a packet-filtering router and a bastion host (application-level gateway)
- Typically, the router is configured so that
  - For traffic from the Internet, only IP packets destined for the bastion host are allowed in
  - For traffic from the internal network, only IP packets from the bastion host are allowed out
  - Physically prevents traffic flow directly through the router between the Internet and other hosts on the private network



Screened-subnet Firewall System

- Two packet-filtering routers are used, one between the bastion host and the Internet and one between the bastion host and the internal network
- The outside router advertises only the existence of the screened subnet to the Internet; therefore, the internal network is invisible to the Internet.
- The inside router advertises only the existence of the screened subnet to the internal network; therefore, the systems on the inside network cannot construct direct routes to the Internet.



Summary - Firewall Locations and Configurations

Stockholm University

- VPN: IPSec operates on router or firewall that connect enterprise LANs to the out side world
- DMZ networks
  - Systems that are externally accessible but need some protections are usually located on DMZ networks.
  - An external firewall is placed at the edge of an enterprise network
- Distributed FWs
  - Stand-alone FW + host-based FW working together under a central administrative control
- One or more internal firewalls protect the majority of the enterprise network.

Example of Rules -1

Stockholm University

- Inbound mail is allowed (port 25 is for SMTP incoming), but only to a gateway host. However, packets from a particular external host, SPIGOT, are blocked because that host has a “dark” history of sending massive files in e-mail

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

- This is an explicit statement of the default policy. All rulesets include this rule implicitly as the last rule.

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

Example of Rules -2

- This ruleset is intended to specify that any inside host can send mail to the outside. A TCP packet with a destination port of 25 is routed to the SMTP server on the destination machine.
- The problem with this rule is that the use of port 25 for SMTP receipt is only a default; an outside machine could be configured to have some other application linked to port 25.
- As this rule is written, an attacker could gain access to internal machines by sending packets with a TCP source port number of 25.

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

Summary - Firewalls should

Stockholm University

- Deny any packets not explicitly allowed
- Disallow access to firewall software from unauthorized systems
- Any packet entering network that has a source address of an internal host should be denied (masquerading, spoofing)
- No traffic should be allowed to leave a network that does not have an internal source address (spoofing, zombies for DDoS)
- Firewall should reassemble fragmented packets before sending them to their destination (malware, DoS)
- Check for source routing information within the packet and deny if it is present (no inspection done)
- Drop and log any traffic that does not meet above rules
- Tighten permission rights by specifying what system can be accessed and how

Expected Learning Outcomes

Stockholm University

- Understand and explain the principles of firewalls
- Understand and explain the principles of different types of firewalls (basic differences among them)
- Understand and explain the principles of rules of firewalls
- Design a basic firewall according to certain requirements

Stockholm University

Thank you!

References

1. Chapter 12 W. Stallings
2. Firewalls and Internet Security. 2ndEd., W.R.Cheswick, S.M. Bellovin, A.D. Rubin