Internet Security

Firewalls

Ozalp Babaoglu

Overview

- Cryptographic technologies
  - Secure Sockets Layer
  - IPSec
- Exo-structures
  - Firewalls
  - Virtual Private Networks

Firewall

- “Firewall” of a car that separates the passenger compartment from the engine
- More like a moat around a medieval castle
  - restricts entry to carefully controlled points
  - prevents attackers from getting close to defenses
  - restricts exits to carefully controlled points

- Combination of hardware and software to regulate traffic between an internal network and an external network (Internet)
- Benefits of being “connected” while minimizing the risks of threats

![Diagram of firewall with internal and external network connections]
What a firewall can do?
- Focus security decisions
- Enforce security policies
- Provide location for monitoring and logging Internet activity

What a firewall can’t do?
- Protect against internal threats
- Protect against connections that bypass it
- Protect against completely new threats
- Protect against viruses and worms
- Set itself up correctly

Problems with firewalls
- Interfere with the Internet end-to-end communication model
- Create false sense of perfect security
- Increase inconvenience for users

Firewall Technologies
- Packet filtering
- Stateful packet inspection
- Application proxy
- Network address translation
- Virtual Private Networks
Packet Filtering

- Implemented through a screening router
  - Router: can the packet be routed to its destination?
  - Screening router: should the packet be routed to its destination?
- Applies a set of filtering rules to each inbound/outbound packet and then forwards or discards it

Filtering rules based on information in the IP packet header
- IP source address
- IP destination address
- Protocol (TCP, UDP, ICMP)
- Source transport-level address (port number)
- Destination transport-level address (port number)
- Packet size

Additional information
- Interface the packet arrives on
- Interface the packet will go out on

Stateful Packet Inspection

- Screening router that can base forwarding decisions on state information that is collected and stored during operation
- Examples of state-based forwarding decisions:
  - Is the packet a response to an earlier packet?
  - Do the number of packets seen from some host exceed a threshold?
  - Is the packet identical to a recently seen packet?
  - Is the packet a fragment?
(Stateful and Stateless) Packet Filtering

Advantages
- One screening router can protect the entire network
- Extremely efficient
- Widely available

Disadvantages
- Hard to configure
- Reduces router performance
- Because they cannot examine upper-layer data, they are limited in the range of policies that they can implement (e.g., no application-specific rules)
- They are vulnerable to attacks that take advantage of problems within the TCP/IP protocol stack, such as network layer address spoofing

Application Proxy Firewall

Also called an application-level gateway

Specialized application programs for Internet services (HTTP, FTP, telnet, etc.)
- Proxy server
- Proxy client

Need a mechanism to restrict direct communication between the internal and external networks
- Typically combined with caching for performance
- Effective only when used in conjunction with mechanisms that restrict direct communications between the internal and external hosts (dual-homed host)

Advantages
- Can perform user-level authentication
- Can do intelligent (application specific) filtering
- Can be combined with caching
- Can do good logging

Disadvantages
- Require different servers for each service
- Require modifications to clients
Network Address Translation

- Allows a network to use a set of addresses internally and a different set of addresses externally
- Invented not for security but for conserving IP addresses
- Typically implemented within a router

Advantages
- Enforces firewall control over outbound traffic
- Restricts incoming traffic (no spontaneous connections)
- Hides structure and details of internal network

Disadvantages
- Interferes with some encryption-based techniques
- Dynamic allocation of addresses interferes with logging
- Internal network cannot host externally-visible services (requires port mapping)
Firewall Architectures

- Host-based and "personal"
- Screening Router
- Dual-Homed Host
- Screened Host
- Screened Subnet

Host-based Firewalls

- Secures an individual host
  - Available in many operating systems
  - Commonly used to protect servers
- Advantages
  - Highly customizable
  - Topology independent — all (internal and external) attacks must go through the firewall
  - Extensible — new servers can be added to the network, with their own firewall, without the need of altering the network configuration

Personal Firewalls (Incoming connections)

- Controls the traffic between a personal computer or workstation and a network (or Internet)

Personal Firewalls (Outgoing connections)
- **Screening Router**: Routes or blocks packets, as determined by the site’s security policy.

- **Dual-Homed Host**: Application proxy example

- **Screened Host**: A computer on a network specifically designed and configured to resist attacks.

- **Bastion Host**: Great exposure to attacks.

- **Bastion Host**: All traffic crosses the bastion host, that can control and block/forward it.

- **Bastion Host**: Generally runs only a few applications, mainly proxies.
**Bastion Host**

- Basic rules to set up a bastion host:
  - No other hosts can be reached from outside
  - Trusted operating system
  - No unnecessary software (no compilers)
  - Read-only file system (apart from strictly required write operations)
  - Only strictly required services
  - No user accounts
  - Additional authentication mechanisms
  - Extensive logging

**Screened Subnet**

- Exterior router (access router)
  - protects DMZ (De-Militarized Zone) and internal network from Internet
  - allows incoming traffic only for bastion hosts/services.
- Interior router (or choke router)
  - protects internal network from Internet and DMZ
  - does most of packet filtering for firewall
  - allows selected outbound services from internal network
  - limits services between bastion host and internal network