Firewalls

Special Thanks to our friends at The Blekinge Institute of Technology, Sweden for providing the basis for these slides.

Outline

• Firewall Design Principles
  - Firewall Characteristics
  - Types of Firewalls

Firewalls

• Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WANs or the Internet
• Information systems undergo a steady evolution (from small LAN’s to Internet connectivity)
• Strong security features for all workstations and servers not established

Why?

• Systems provide many services by default
  - Many workstations provide remote access to files and configuration databases (for ease of management and file sharing)
  - Even if configured only for specific users, they can sometimes be tricked into providing services they shouldn’t
    - E.g. missing bounds check in input parsers
  - Also, users sometimes forget to close temporary holes
    - E.g. leaving file system remote mountable for file sharing

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

Why?

• Firewalls enforce policies that centrally manage access to services in ways that workstations should, but don’t
• Which services?
  - Finger
  - telnet: requires authentication, but password sent in clear
  - rlogin: similar to telnet, but uses IP address based authentication (Bad!)
  - ftp: Tricky because two connections, control channel from sender, and data connection from receiver. (passive ftp has both sender originated)
  - X Windows
  - ICMP
**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)

- **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

- **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)

**Firewall Limitations**

- Cannot protect against attacks that bypass the firewall
  - E.g. an internal modem pool
- Firewall does not protect against internal threats
- Firewall cannot protect against transfer of virus infected programs
  - Too many different apps and operating systems supported to make it practical to scan all incoming files for viruses

**Types of Firewalls**

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways
  - (Bastion host)

**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)

Advantages:
- Simplicity
- Transparency to users
- High speed

Disadvantages:
- Difficulty of setting up packet filter rules
- Lack of Authentication
- Who really sent the packet?

Advantages:
- Can be clever:
  - Allow connections initiated from inside network to outside, but not initiated from outside.
  - Traffic flows both way, but if firewall only allows incoming packets with ACK set in TCP header, this manages the issue.
  - Problem: some apps require outside node to initiate connection with inside node (e.g. ftp, Xwindows), even if original request initiated by inside node.
  - Solution (sort of): allow packets from outside if they are connecting to high port number.

Stateful Packet Filter

- Changes filtering rules dynamically (by remembering what has happened in recent past)
- Example: Connection initiated from inside node S to outside IP address D. For short time allow incoming connections from D to appropriate ports (i.e. ftp port).
- In practice, much more caution
  - Stateful filter notices the incoming port requested by S and only allows connections from D to that port. Requires parsing ftp control packets

Possible attacks and appropriate countermeasures
- IP address spoofing
  - Discard packet with inside source address if it arrives on external interface
- Source routing attacks
  - Discard all source routed packets
Possible attacks and appropriate countermeasures

- **Tiny fragment attacks**
  - Intruder uses IP fragment option to create extremely small IP packets that force TCP header information into separate packet fragments
  - Discard all packets where protocol type is TCP and IP fragment offset is small

---

**Application-level Gateway**

- Also called proxy server
- Acts as a relay of application-level traffic
- Can act as router, but typically placed between two packet filtering firewalls (for total of three boxes)
  - Two firewalls are routers that refuse to forward anything from the global net that is not to gateway, and anything to global net that is not from gateway.
  - Sometimes called a bastion host (we use the term differently)

---

** Benefits:**

- Higher security 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)

---

**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 use is a situation in which the system administrator trusts the internal users

- 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
- We won’t go into these

Why Firewalls Don’t Work

- Assume all bad guys are on outside, and everyone inside can be trusted.
- Firewalls can be defeated if malicious code can be injected into corporate network
  - E.g. trick someone into launching an executable from an email message or into downloading something from the net.
- Often make it difficult for legitimate users to get their work done.
  - Misconfiguration, failure to recognize new app

Why Firewalls Don’t Work

- If firewall allows anything through, people figure out how to do what they need by disguising their traffic as allowed traffic
  - E.g. file transfer by sending it through email. If size of emails limited, then user breaks them into chunks, etc.
  - Firewall friendly traffic (e.g. using http for other purposes)
    - Defeats effort of sysadmin to control traffic
    - Less efficient than not using http

Recommended Reading

- Chapman, D., and Zwicky, E. Building Internet Firewalls. O’Reilly, 1995
- Cheswick, W., and Bellovin, S. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2000