Chapter 9

Firewall and Intrusion Prevention System

Firewalls and Intrusion Prevention Systems

- Effective means of protecting LANs
- Can also secure workstations and servers
- Use firewall as perimeter defence
  - Single choke point to impose security
Firewall – Basic Idea

- Separate local network from the Internet
  - Restricts access from the outside
  - Restricts outbound connections too

Firewall Capabilities & Limits

- Capabilities:
  - Defines a single choke point
  - Provides a location for monitoring security events
  - Convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC VPNs
- Limitations:
  - Cannot protect against attacks bypassing firewall
  - May not protect fully against internal threats
  - Improperly secure wireless LAN
  - Laptop, PDA, portable storage device infected outside then used inside

Types of Firewall – Packet- or Session- Filtering Firewall
Packet Filtering Firewall

- Applies rules to each packet in/out of firewall to decide whether to allow packet to proceed
  - Decision must be made on a per-packet basis
  - Stateless: cannot examine packet’s context (such as TCP connection, application to which the packet belongs)
- Based on information in packet header
  - IP source and destination addresses, ports
  - Protocol identifier (TCP, UDP, ICMP etc)
  - TCP flags (SYN, ACK, RST, PSH, FIN)
  - ICMP message type

Packet Filtering Firewall

- Typically a list of rules of matches on fields
  - Rule says if forward or discard packet
- Two default policies:
  - Discard - prohibit unless expressly permitted
    - More conservative, controlled, visible to users
  - Forward - permit unless expressly prohibited
    - Easier to manage/use but less secure

Example Packet Filtering Firewall
Rule for FTP Traffic

- Illustration of FTP server and client interactions, including
  - TCP ports
  - Data transfer
  - Command exchange
FTP Packet Filter

The following filtering rules allow a user to FTP from any IP address to the FTP server at 172.168.10.12:

```
access-list 100 permit tcp any gt 1023 host 172.168.10.12 eq 21
access-list 100 permit tcp any gt 1023 host 172.168.10.12 eq 20
! Allows packets from any client to the FTP control and data ports
access-list 101 permit tcp host 172.168.10.12 eq 21 any gt 1023
access-list 101 permit tcp host 172.168.10.12 eq 20 any gt 1023
! Allows the FTP server to send packets back to any IP address with TCP ports > 1023
```

```
interface Ethernet 0
access-list 100 in  ! Apply the first rule to inbound traffic
access-list 101 out  ! Apply the second rule to outbound traffic
```

Packet Filter Weaknesses

- **Weaknesses**
  - Cannot prevent attack based on application bugs
    - For example, if there is a buffer overflow vulnerability in FTP server, firewall will not block an attack string
  - Limited logging functionality
  - Do not support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Packet Filter Attacks

- IP address spoofing
- Source route attacks
- Tiny fragment attacks
  - If fragment size is small it is possible to force some of a TCP packet’s TCP header fields into the second fragment
  - Filter rules that specify patterns for those fields will not match
Problem with Stateless Filtering

• In TCP connections, ports with numbers less than 1024 are permanently assigned to servers
  — 20, 21 for FTP, 23 for telnet, 25 for SMTP, 80 for HTTP...
• Clients use ports numbered from 1024 to 65535
• What should a firewall do if it sees, say, an outgoing request to some client’s port 8081?
  — It must allow it: this could be a server’s response to a previously established connection...
  — ...OR it could be malicious traffic
  — Can’t tell without keeping state for each connection

Stateful Inspection Firewall

• Reviews packet header information but also keeps info on TCP connections
  — Typically have low, “known” port no. for server
  — And high, dynamically assigned client port no.
  — Simple packet filter must allow all return high port numbered packets back in
  — Stateful inspection packet firewall tightens rules for TCP traffic using a directory of TCP connections
  — Only allow incoming traffic to high-numbered ports for packets matching an entry in this directory
  — May also track TCP seq numbers as well
Application-Level Gateway

- Acts as a relay of application-level traffic
  - User contacts gateway with remote host name
  - Authenticates themselves
  - Gateway contacts application on remote host and relays TCP segments between server and user

Application-level Gateway

- Must have proxy code for each application
  - May restrict application features supported
- More secure than packet filters
  - Can support user-to-gateway authentication
  - Can log and audit all activity
- But have higher overheads

Circuit-Level Gateway

- Splices and relays two TCP connections, to an inside host and to an outside host
- Relays TCP segments from one connection to the other without examining contents
Circuit Level Proxy

- Independent of application logic
  - Just determines whether relay is permitted
- Typically used when inside users trusted
  - May use application-level gateway inbound and circuit-level gateway outbound
  - Somewhat lower overheads
- SOCKS (most well known example)

Firewall Basing

- Several options for locating firewall:
  - Bastion host
  - Individual host-based firewall
  - Personal firewall
- Additionally, firewall can be located on router or LAN switch

Bastion Hosts

- Hardened system implementing application-level gateway behind packet filter
- Characteristics:
  - Runs secure O/S and only essential services
  - May require user authentication to access proxy and/or host application
  - Each proxy can restrict features (subset of commands), hosts accessed
  - Each proxy small, simple, checked for security
  - Each proxy is independent, non-privileged
  - Limited disk use, hence read-only code
Demilitarized Zone (DMZ)

Host-Based Firewalls
- Used to secure individual host
- Available in many OS or as an add-on
- Filter packet flows
- Often used on servers
- Advantages:
  - Tailored filter rules for specific host needs
  - Protection from both internal / external attacks
  - Additional layer of protection to org. firewall

Personal Firewall
- Controls traffic flow to/from PC/workstation
- For both home or corporate use
- May be software module on PC
- Or in home cable/DSL router/gateway
- Typically much less complex
- Primary role to deny unauthorized access
- May also monitor outgoing traffic to detect/block worm/malware activity
Virtual Private Networks

Firewall Limitations

- Interferes with networked applications
- Does not solve many real problems
  - Buggy software
  - Address spoofing
  - Bad protocol design
  - User malfeasance, indiscretions
- Not much of a solution for DoS attacks
- Does not prevent insider attack
- Increasing complexity and potential for misconfigurations

Intrusion Prevention Systems (IPS)

- Recent addition to security products where
  - Inline net/host-based IDS that can block traffic
  - Functional addition to firewall that adds IDS capabilities
- Can block traffic like a firewall
- Using IDS algorithms
- May be network or host based
Host-Based IPS

- Identifies attacks using both:
  - Signature techniques
    - malicious application packets
  - Anomaly detection techniques
    - behavior patterns that indicate malware
- Can be tailored to the specific platform
  - e.g. general purpose, web/database server specific
- Can also sandbox applets to monitor behavior
- May give desktop file, registry, I/O protection

Network-Based IPS

- Inline NIDS that can discard packets or Terminate TCP connections
- Uses signature and anomaly detection
- May provide flow data protection
  - Monitoring full application flow content
- Can identify malicious packets using:
  - Pattern matching, stateful matching, protocol anomaly, traffic anomaly, statistical anomaly
- cf. SNORT inline can drop/modify packets

Unified Threat Management Products