Chapter 9

Firewalls
The Need For Firewalls

- Internet connectivity is essential
  - however it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
  - can be a single computer or a set of two or more systems working together
- Used as a perimeter defense
  - single choke point to impose security and auditing
  - insulates internal systems from external networks
Firewall Characteristics

Design goals

- 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
Firewall Access Policy

- A critical component in the planning & implementation of a firewall is specifying a suitable access policy
  - this lists the types of traffic authorized to pass through the firewall
  - includes address ranges, protocols, applications and content types
- Policy should be developed from the organization’s information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
  - then refined to detail the filter elements which can then be implemented within an appropriate firewall topology
Firewall Filter Characteristics

Characteristics that a firewall access policy could use to filter traffic include:

- IP address and protocol values
- Application protocol
- User identity
- Network activity
Firewall Capabilities And Limits

- **Capabilities:**
  - defines a single choke point
  - provides a location for monitoring security events
  - convenient platform for several Internet functions that are not security related
  - can serve as the platform for IPSec

- **Limitations:**
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - improperly secured wireless LAN can be accessed from outside the organization
  - laptop, PDA, or portable storage device may be infected outside the corporate network then used internally
Types of Firewalls
Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
  - list of rules based on matches in the TCP/IP header
  - forwards or discards the packet based on rules match
- Filtering rules are based on information contained in a network packet
  - Source IP address
  - Destination IP address
  - Source and destination transport-level address
  - IP protocol field
  - Interface

Two default policies:

- discard - prohibit unless expressly permitted
  - more conservative, controlled, visible to users
- forward - permit unless expressly prohibited
  - easier to manage and use but less secure
### Packet Filter Rules

#### Rule Set A

<table>
<thead>
<tr>
<th>action</th>
<th>ourhost</th>
<th>port</th>
<th>theirhost</th>
<th>port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td>*</td>
<td>*</td>
<td>SPIGOT</td>
<td>*</td>
<td>we don't trust these people</td>
</tr>
<tr>
<td>allow</td>
<td>OUR-GW</td>
<td>25</td>
<td>*</td>
<td>*</td>
<td>connection to our SMTP port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action</th>
<th>ourhost</th>
<th>port</th>
<th>theirhost</th>
<th>port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>default</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action</th>
<th>ourhost</th>
<th>port</th>
<th>theirhost</th>
<th>port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td>connection to their SMTP port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action</th>
<th>src</th>
<th>port</th>
<th>dest</th>
<th>port</th>
<th>flags</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>{our hosts}</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td></td>
<td>our packets to their SMTP port</td>
</tr>
<tr>
<td>allow</td>
<td>*</td>
<td>25</td>
<td>*</td>
<td>*</td>
<td>ACK</td>
<td>their replies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Direction</th>
<th>Src address</th>
<th>Dest address</th>
<th>Protocol</th>
<th>Dest port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In</td>
<td>External</td>
<td>Internal</td>
<td>TCP</td>
<td>25</td>
<td>Permit</td>
</tr>
<tr>
<td>2</td>
<td>Out</td>
<td>Internal</td>
<td>External</td>
<td>TCP</td>
<td>&gt;1023</td>
<td>Permit</td>
</tr>
<tr>
<td>3</td>
<td>Out</td>
<td>Internal</td>
<td>External</td>
<td>TCP</td>
<td>25</td>
<td>Permit</td>
</tr>
<tr>
<td>4</td>
<td>In</td>
<td>External</td>
<td>Internal</td>
<td>TCP</td>
<td>&gt;1023</td>
<td>Permit</td>
</tr>
<tr>
<td>5</td>
<td>Either</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>
Packet Filter: Advantages And Weaknesses

- **Advantages**
  - simplicity
  - typically transparent to users and are very fast

- **Weaknesses**
  - cannot prevent attacks that employ application specific vulnerabilities or functions
  - limited logging functionality
  - do not support advanced user authentication
  - vulnerable to attacks on TCP/IP protocol bugs
  - improper configuration can lead to breaches
Stateful Inspection Firewall

● Tightens rules for TCP traffic by creating a directory of outbound TCP connections
  ○ there is an entry for each currently established connection
  ○ packet filter allows incoming traffic to high numbered ports
    ■ only for those packets that fit the profile of one of the entries

● Reviews packet information but also records information about TCP connections
  ○ keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
  ○ inspects data for protocols like FTP, IM and SIPS commands
Stateful Firewall Connection State

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Connection State</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.100</td>
<td>1030</td>
<td>210.9.88.29</td>
<td>80</td>
<td>Established</td>
</tr>
<tr>
<td>192.168.1.102</td>
<td>1031</td>
<td>216.32.42.123</td>
<td>80</td>
<td>Established</td>
</tr>
<tr>
<td>192.168.1.101</td>
<td>1033</td>
<td>173.66.32.122</td>
<td>25</td>
<td>Established</td>
</tr>
<tr>
<td>192.168.1.106</td>
<td>1035</td>
<td>177.231.32.12</td>
<td>79</td>
<td>Established</td>
</tr>
<tr>
<td>223.43.21.231</td>
<td>1990</td>
<td>192.168.1.6</td>
<td>80</td>
<td>Established</td>
</tr>
<tr>
<td>219.22.123.32</td>
<td>2112</td>
<td>192.168.1.6</td>
<td>80</td>
<td>Established</td>
</tr>
<tr>
<td>210.99.212.18</td>
<td>3321</td>
<td>192.168.1.6</td>
<td>80</td>
<td>Established</td>
</tr>
<tr>
<td>24.102.32.23</td>
<td>1025</td>
<td>192.168.1.6</td>
<td>80</td>
<td>Established</td>
</tr>
<tr>
<td>223.21.22.12</td>
<td>1046</td>
<td>192.168.1.6</td>
<td>80</td>
<td>Established</td>
</tr>
</tbody>
</table>
Application-Level Gateway

- Also called an **application proxy**
- Acts as a relay of application-level traffic
  - user contacts gateway using a TCP/IP appl.
  - user is authenticated
  - gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
  - may restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection
Circuit-Level Gateway

● Circuit level proxy
  ○ sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
  ○ relays TCP segments from one connection to the other without examining contents
  ○ security function consists of determining which connections will be allowed

● Typically used when inside users are trusted
  ○ may use application-level gateway inbound and circuit-level gateway outbound
  ○ lower overheads
SOCKS Circuit-Level Gateway

- SOCKS v5 defined in RFC1928

- Provide a framework for client-server applications to conveniently and securely use the services of a network firewall

- Client application contacts SOCKS server, authenticates, sends relay request
  - server evaluates and either establishes or denies the connection
Bastion Hosts

- System identified as a critical strong point in the network’s security
- Serves as a platform for an application-level or circuit-level gateway
- Common characteristics:
  - runs secure O/S, only essential services
  - may require user authentication to access proxy or host
  - each proxy can restrict features, hosts accessed
  - each proxy is small, simple, checked for security
  - each proxy is independent, non-privileged
  - limited disk use, hence read-only code
Firewall Topologies

- **Host-resident firewall**
  - includes personal firewall software and firewall software on servers

- **Screening router**
  - single router between internal and external networks with stateless or full packet filtering

- **Single bastion inline**
  - single firewall device between an internal and external router

- **Single bastion T**
  - has a third network interface on bastion to a DMZ where externally visible servers are placed

- **Double bastion inline**
  - DMZ is sandwiched between bastion firewalls

- **Double bastion T**
  - DMZ is on a separate network interface on the bastion firewall

- **Distributed firewall configuration**
  - used by large businesses and government organizations
Host-Based Firewalls

- Used to secure an individual host
- Available in operating systems
  - can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server
- Advantages:
  - filtering rules can be tailored to the host environment
  - protection is provided independent of topology
  - provides an additional layer of protection
Personal Firewall

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- Typically is a software module
- Can be housed in a router that connects all of the home computers to Internet such as a DSL or cable modem
- Typically much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity
Personal Firewall Interface

Firewall On
Click Stop to allow incoming network communication to all services and ports.

Allow:
<table>
<thead>
<tr>
<th>On</th>
<th>Description (Ports)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Personal File Sharing (548, 427)</td>
</tr>
<tr>
<td></td>
<td>Windows Sharing (139)</td>
</tr>
<tr>
<td></td>
<td>Personal Web Sharing (80, 427)</td>
</tr>
<tr>
<td></td>
<td>Remote Login – SSH (22)</td>
</tr>
<tr>
<td></td>
<td>FTP Access (20–21, 1024–65535 from 20–21)</td>
</tr>
<tr>
<td></td>
<td>Remote Apple Events (3031)</td>
</tr>
<tr>
<td></td>
<td>Printer Sharing (631, 515)</td>
</tr>
</tbody>
</table>

To use FTP to retrieve files while the firewall is on, enable passive FTP mode using the Proxies tab in Network Preferences.
Double bastion inline
Distributed firewall configuration
Virtual Private Networks (VPNs)
Intrusion Prevention Systems (IPS)

- a.k.a. Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
  - anomaly detection to identify behavior that is not that of legitimate users, or
  - signature/heuristic detection to identify known malicious behavior
- Can block traffic as a firewall does
  - uses algorithms developed for IDSs to determine when to do so
Host-Based IPS (HIPS)

- Identifies attacks using both signature and anomaly detection techniques
  - **signature**: focus is on the specific content of application payloads in packets, looking for patterns that have been identified as malicious
  - **anomaly**: IPS is looking for behavior patterns that indicate malware

- Can be tailored to the specific platform
- Can also use a sandbox approach to monitor behavior
Host-Based IPS (HIPS)

- **Examples of addressed malicious behavior**
  - modification of system resources
  - Privilege-escalation
  - Buffer-overflow
  - access to e-mail contact list
  - directory traversal

- **Advantages**
  - the various tools work closely together
  - threat prevention is more comprehensive
  - management is easier
HIPS

- A set of general purpose tools may be used for a desktop or server system
- Some packages are designed to protect specific types of servers, such as Web servers and database servers
  - In this case the HIPS looks for particular application attacks
- Can use a sandbox approach
  - Sandboxes are especially suited to mobile code such as Java applets and scripting languages

→HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior

- Areas for which a HIPS typically offers desktop protection:
  - System calls
  - File system access
  - System registry settings
  - Host input/output
The Role of HIPS

● Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals
  ○ thus security vendors are focusing more on developing endpoint security products
  ○ traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, antispam, and personal firewalls

● Approach is an effort to provide an integrated, single-product suite of functions
  ○ advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier

● A prudent approach is to use HIPS as one element in a defense-in-depth strategy that involves network-level devices, such as either firewalls or network-based IPSs
Network-Based IPS (NIPS)

- Inline NIDS with the authority to discard packets and tear down 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
Digital Immune System

- Comprehensive defense against malicious behavior caused by malware
- Developed by IBM and refined by Symantec
- Motivation for this development includes the rising threat of Internet-based malware, the increasing speed of its propagation provided by the Internet, and the need to acquire a global view of the situation
- Success depends on the ability of the malware analysis system to detect new and innovative malware strains
Worm Monitors

Figure 9.5 Placement of Worm Monitors
Snort Inline

- Enables Snort to function as an intrusion prevention capability
- Includes a replace option which allows the Snort user to modify packets rather than drop them
  - useful for a honeypot implementation
  - attackers see the failure but can’t figure out why it occurred
- **Drop**: Snort rejects a packet based on the options defined in the rule and logs the result
- **Reject**: packet is rejected and result is logged and an error message is returned
- **Sdrop**: packet is rejected but not logged
Unified Threat Management Products

Figure 9.6 Unified Threat Management Appliance (based on [JAME06])
Summary

- Firewalls
- Types of firewalls
  - packet filtering firewall
  - stateful inspection firewalls
  - application proxy firewall
  - circuit level proxy firewall
- Firewall basing
  - bastion host
  - host-based firewall
  - personal firewall
- Firewall location and configurations
  - DMZ networks
  - virtual private networks
  - distributed firewalls
- Intrusion prevention systems (IPS)
  - host-based IPS (HIPS)
  - network-based IPS (NIPS)
  - Distributed or hybrid IPS
  - Snort Inline
- UTM products