Firewalls and VPNs
Firewalls

- Prevent specific types of information from moving between the outside world (untrusted network) and the inside world (trusted network)
- May be separate computer system; a software service running on existing router or server; or a separate network containing supporting devices
- A Roadmap
  - Firewall categorization
  - Firewall configuration and management
Firewall Categorization

1. Processing mode
2. Development era
3. Intended deployment structure
4. Architectural implementation
Firewall Categorization (1): Processing Modes

• Packet filtering
• Application gateways
• Circuit gateways
• MAC layer firewalls
• Hybrids
## Firewall Proc. Modes: Network Layers

<table>
<thead>
<tr>
<th>Processing Mode</th>
<th>Network Layer (OSI)</th>
<th>Network Layer (TCP/IP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application gateways</td>
<td>7: Application</td>
<td>5: Application</td>
</tr>
<tr>
<td></td>
<td>6: Presentation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5: Session</td>
<td></td>
</tr>
<tr>
<td>Circuit gateways</td>
<td>4: Transport</td>
<td>4: Transport</td>
</tr>
<tr>
<td>Packet filtering</td>
<td>3: Network</td>
<td>3: Network</td>
</tr>
<tr>
<td>MAC address filtering</td>
<td>2: Data Link</td>
<td>2: Data Link</td>
</tr>
<tr>
<td>—</td>
<td>1: Physical</td>
<td>1: Physical</td>
</tr>
</tbody>
</table>

*Source*: Adapted from Fig. 6-5 in the textbook
Packet Filtering (1)

- Packet filtering firewalls examine header info. for data pkts
- Most often based on combination of:
  - Internet Protocol (IP) source and destination address
  - Direction (inbound or outbound)
  - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), destination port requests
- Simple firewall models enforce rules that prohibit packets with certain IP address ranges
Packet Filtering (2)

• Three subsets of packet filtering firewalls:
  – *Static filtering*: requires manual configuration of firewall rules that determine which packets are allowed, denied
  – *Dynamic filtering*: firewall can react to emergent event, update/create rules to deal with it
  – *Stateful inspection*: firewalls track each network connection between internal and external systems using a state table
IPv4 Packet Structure (Fig. 6-1)

<table>
<thead>
<tr>
<th>0 bits</th>
<th>32 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header version (4 bits)</td>
<td>Type of service (16 bits)</td>
</tr>
<tr>
<td>Header length (4 bits)</td>
<td></td>
</tr>
<tr>
<td>Type of service (8 bits)</td>
<td>Flags (3 bits)</td>
</tr>
<tr>
<td>Identification (16 bits)</td>
<td>Fragment offset (13 bits)</td>
</tr>
<tr>
<td>Time to live (8 bits)</td>
<td>Protocol (8 bits)</td>
</tr>
<tr>
<td>Source IP address (32 bits)</td>
<td>Header checksum (16 bits)</td>
</tr>
<tr>
<td>Destination IP address (32 bits)</td>
<td></td>
</tr>
</tbody>
</table>

Options

Data
## TCP, UDP Segment Structures

### TCP Segment

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source port #</td>
<td>32 bits</td>
</tr>
<tr>
<td>Dest port #</td>
<td>32 bits</td>
</tr>
<tr>
<td>Sequence number</td>
<td></td>
</tr>
<tr>
<td>Acknowledgement number</td>
<td></td>
</tr>
<tr>
<td>Rcvr window size</td>
<td></td>
</tr>
<tr>
<td>Head Len</td>
<td></td>
</tr>
<tr>
<td>Not Used</td>
<td></td>
</tr>
<tr>
<td>U</td>
<td>A</td>
</tr>
<tr>
<td>Checksum</td>
<td>Ptr urgent data</td>
</tr>
<tr>
<td>Options (variable length)</td>
<td></td>
</tr>
<tr>
<td>Application data</td>
<td>(variable length)</td>
</tr>
</tbody>
</table>

### UDP Segment

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port #</td>
<td>32 Bits</td>
</tr>
<tr>
<td>Dest Port #</td>
<td>32 Bits</td>
</tr>
<tr>
<td>Length</td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
</tr>
<tr>
<td>Application data</td>
<td>(message)</td>
</tr>
</tbody>
</table>

Packet Filtering Router (Fig. 6-4)
Sample Firewall Rules (Table 6-1)

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>Service (HTTP, SMTP, FTP, Telnet)</th>
<th>Action (Allow or Deny)</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.x.x</td>
<td>10.10.x.x</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>192.168.x.x</td>
<td>10.10.10.25</td>
<td>HTTP</td>
<td>Allow</td>
</tr>
<tr>
<td>192.168.0.1</td>
<td>10.10.10.10</td>
<td>FTP</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Application Gateways

• Frequently installed on a dedicated computer; also called *proxy server*

• Proxy server is often placed in unsecured area of network (e.g., DMZ) ⇒ it faces higher levels of risk from attackers

• We can place extra filtering routers behind the proxy server to protect internal systems
Circuit Gateways

• Circuit gateway firewall: transport layer
• Does not usually look at data traffic flowing between two networks; prevents direct connections between one network and another
• Mechanism: create tunnels connecting specific processes/systems on each side of firewall; only allow authorized traffic in tunnels
MAC Layer Firewalls

• Operates at data-link layer
• Considers specific host computer’s identity in filtering decision
• Only outbound traffic originating from MAC addresses of specific computers allowed
  – Mechanism: link (MAC address, Ethernet port #), administered via switches
Hybrid Firewalls

• Combine elements of multiple types of firewalls (e.g., packet filtering and proxy servers; packet filtering and circuit gateways)

• Alternately, may consist of two separate firewall devices; separate firewall systems connected to work together
Firewall Categorization (2): Development Era

• First generation: static packet filtering firewalls
• Second generation: application-level firewalls or proxy servers
• Third generation: stateful inspection firewalls
• Fourth generation: dynamic packet filtering firewalls; allow only packets with particular source, destination and port addresses to enter
• Fifth generation: kernel proxies; specialized form working under operating system kernel
Firewall Categorization (3): Deployment Structure

• Most firewalls are appliances: stand-alone, self-contained systems

• Commercial firewall systems: consists of firewall software running on general-purpose computer

• Small office/home office (SOHO) or residential firewalls connect users’ LANs or specific computers to network devices
  – Often, firewall software placed on user system
Sample Firewall Devices (Fig. 6-6)
Firewalls Categorization (4): Architectural Implementation

• Firewall devices can be configured in a number of network connection architectures

• Four common architectural implementations of firewalls:
  – Packet filtering routers
  – Screened host firewalls
  – Dual-homed firewalls
  – Screened subnet firewalls
Packet Filtering Routers

• Most organizations with Internet connection have a router connecting to Internet

• Routers can be configured to reject packets that org. forbids entering its network

• Drawbacks: limited auditing, weak authentication
Packet Filtering Router (Fig. 6-4)

FIGURE 6-4 Packet Filtering Router
Screened Host Firewalls

- Combines packet filtering router with stand-alone firewall (e.g., application proxy server)
- Allows router to pre-screen packets to minimize load on internal proxy
- Separate host is often referred to as *bastion host*; can be rich target for external attacks, needs to be secured carefully
Screened Host Firewall (Fig. 6-11)
Dual-Homed Host Firewalls

• Bastion host contains two network interface cards (NICs): one connected to external network, other connected to internal network

• Architecture typically uses network address translation (NAT)
  – Another barrier to intrusion from attackers
## Non-Routable IP Address Ranges

<table>
<thead>
<tr>
<th>Type</th>
<th>IP Address Range</th>
<th>CIDR Mask</th>
<th>IP Subnet Mask</th>
<th># Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td>10.0.0.0 – 10.255.255.255</td>
<td>/8</td>
<td>255.0.0.0</td>
<td>(2^{24} (&gt; 16 \text{ M}))</td>
</tr>
<tr>
<td>Class B</td>
<td>172.16.0.0 – 172.31.255.255</td>
<td>/12 or /16</td>
<td>255.240.0.0 or 255.255.0.0</td>
<td>(2^{12} (4,096) or 2^{16} (&gt; 65K))</td>
</tr>
<tr>
<td>Class C</td>
<td>192.168.0.0 – 192.168.255.255</td>
<td>/16 or /24</td>
<td>255.255.0.0 or 255.255.255.0</td>
<td>(2^{16} (&gt; 65K) or 2^{8} (256))</td>
</tr>
</tbody>
</table>

*Source: Adapted from Table 6-4 in textbook, RFC 1918*
Dual-Homed Firewall (Fig. 6.12)
Screened Subnet Firewalls (DMZ) (1)

- Dominant architecture used today
- Typically has $\geq 2$ internal bastion hosts behind packet filtering router, each host protects trusted network:
  - Connections from outside (untrusted network) routed through external filtering router
  - Connections from outside (untrusted network) are routed into, out of routing firewall to separate network segment: demilitarized zone (DMZ)
  - Connections into trusted internal network allowed only from DMZ bastion host servers
Screened Subnet Firewalls (DMZ) (2)

• Screened subnet performs two functions:
  – Protects DMZ systems and information from outside threats
  – Protects the internal networks by limiting how external connections can gain access to internal systems

• Another facet of DMZs: extranets
Screened Subnet Firewall (Fig. 6-13)
Selecting the Right Firewall

• When selecting firewall, consider a number of factors:
  – Which is the best trade-off between protection, cost for needs of organization?
  – What’s included (and what’s not) in base price?
  – How easy is configuration? Are staff technicians available for this purpose?
  – How well firewall adapt to org.’s growing network?

• Second most important issue: cost
Configuring and Managing Firewalls

• Each firewall device must have own set of configuration rules regulating its actions

• Firewall policy configuration is usually complex and difficult ("black art")

• When security rules conflict with business performance, security often loses!

• Linux firewall
Best Practices for Firewalls

• All traffic from trusted network is allowed out
• Use MAC address filtering for Ethernet ports, authentication for wireless LANs
• Firewall device never directly accessed from public network
• Allow Simple Mail Transport Protocol (SMTP)
• Deny Internet Control Message Protocol (ICMP)
• Telnet access to internal servers should be blocked
• If Web services offered outside firewall, block HTTP traffic from reaching internal networks
Firewall Rules

• Operate by examining data packets and performing comparison with predetermined logical rules

• Logic based on set of guidelines most commonly referred to as firewall rules, rule base, or firewall logic

• Most firewalls use packet header information to determine whether specific packet should be allowed or denied
Example Network Config. (Fig. 6-14)
Firewall Rules (1) (Table 6-16)

<table>
<thead>
<tr>
<th>Rule #</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.0</td>
<td>&gt;1023</td>
<td>Allow</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.1</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.2</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>4</td>
<td>10.10.10.1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>5</td>
<td>10.10.10.2</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>6</td>
<td>10.10.10.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>7</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.6</td>
<td>25</td>
<td>Allow</td>
</tr>
<tr>
<td>8</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.0</td>
<td>7</td>
<td>Deny</td>
</tr>
<tr>
<td>9</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.0</td>
<td>23</td>
<td>Deny</td>
</tr>
<tr>
<td>10</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.4</td>
<td>80</td>
<td>Allow</td>
</tr>
<tr>
<td>11</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>
### Firewall Rules (2) (Table 6-17)

<table>
<thead>
<tr>
<th>Rule #</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.0</td>
<td>&gt;1023</td>
<td>Allow</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>10.10.10.3</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.1</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>4</td>
<td>10.10.10.3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>5</td>
<td>192.168.2.1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>6</td>
<td>192.168.2.0</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>7</td>
<td>10.10.10.5</td>
<td>Any</td>
<td>192.168.2.0</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>8</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>
Virtual Private Networks (VPNs) (1)

• Private, secure network connection between systems over insecure, public Internet
• Securely extends org.’s internal network connections to remote locations beyond its perimeter
Virtual Private Networks (VPNs) (2)

• VPN must achieve three goals:

  – Encapsulate incoming, outgoing data

  – Encrypt incoming, outgoing data

  – Authenticate remote computer, user (?)
Transport Mode

• IP packet data is encrypted, header info. is not
• Lets user establish secure link directly with remote host easily
• Two popular uses:
  – End-to-end transport of encrypted data
  – Remote worker connects to office network over Internet by connecting to VPN server at perimeter
Transport Mode VPN (Fig. 6-18)

Teleworker client machine encrypts data and sends to destination system with unencrypted header OR
Teleworker client machine requests intranet connection using transport mode VPN then the client machine acts as if locally connected

Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client
Destination client machine receives encrypted data and decrypts

**FIGURE 6-18** Transport Mode VPN
Tunnel Mode

- Org. sets up two perimeter tunnel servers as *encryption points*: all net traffic encrypted in transit
- Main benefit to tunnel mode: intercepted packets reveal nothing about true destination
- Examples of tunnel mode VPNs:
  - Pulse Secure appliance
  - Microsoft Internet Application Gateway
Tunnel Mode VPN (Fig. 6-19)
Example VPN: Pulse Secure

Source: Pulse Secure, LLC; https://www.pulsesecure.net/products/psa-series/ (PSA 5000)

Summary

• Firewall technology
  – Four methods for categorization
  – Firewall configuration and management

• Virtual Private Networks
  – Two modes