INTRODUCTION TO FIREWALL SECURITY
SESSION SEC-1N20

Agenda

• Introduction to Firewalls
• Types of Firewalls
• Modes and Deployments
• Key Features in a Firewall
• Emerging Trends
What Is a Firewall

- A firewall is an access control device that looks at the IP packet, compares with policy rules and decides whether to allow, deny or take some other action on the packet.

A Simple Analogy
The Firewall as the Premise Guard
Guard Responsibility

You Are Mr. John and You Want to Meet Mr. Fred—**Should I Allow? Let Me Check My Rules Book**

I Will Allow You to Come in, Provided You Prove Your Identity—**Authenticate Yourself**

I Am Supposed to Log All the Information—**Name, Address, Time, etc.**

---

Key Access Control Parameters

- **Application**
  - HTTP Data—Kaaza, FTP—abc
- **Presentation**
- **Session**
- **Transport**
  - TCP and UDP Port Numbers
- **Network**
  - IP Addresses, Protocol, Flags
- **Data Link**
  - MAC Addresses
- **Physical**

- **Policy database**—collection of access control rules based on the above parameters
- **Other names**—rules table, access control lists, firewall policies
Examples

• **DATA LINK LAYER**
  - Deny all packets from MAC address 00-1b-ef-01-01-01
  - Do not prompt for authentication if MAC address is 00-1b-15-01-02-03 (IP phone)

• **NETWORK LAYER**
  - Deny everything except outbound packets from 10.10.0.0/24 subnet
  - Permit only GRE traffic
  - Deny everything except IP traffic from network 192.168.1.0 to network 171.69.231.0

• **TRANSPORT LAYER**
  - Allow web traffic from anybody (Internet) provided the destination address is my web server (10.10.10.1)
  - Allow FTP traffic from anybody (Internet) to my FTP server (10.10.10.2) but only after successful authentication
  - Deny all UDP traffic

• **APPLICATION LAYER**
  - Deny all peer-to-peer networks
  - Do not allow HTTP headers with POST subcommand
  - Do not allow DEBUG option in SMTP (MAIL) commands
Agenda

- Introduction to Firewalls
- Types of Firewalls
- Modes and Deployments
- Key Features in a Firewall
- Emerging Trends

Firewall Technologies

- Packet filtering gateways
  - Cisco routers with simple ACLs
- Stateful inspection firewalls
  - Cisco PIX, Cisco routers with firewall feature set, Checkpoint
- Proxy firewalls
  - Gauntlet, Sidewinder
- Personal firewalls
  - Cisco CSA, Check Point Zone, Sygate
- NAT firewalls
  - Cisco Linksys, Netgear
Packet Filtering Gateways

- Drop/allow packets based on source or destination addresses or ports (some exceptions)
- No state information is maintained; decisions are made only from the content of the current packet
- Integrated feature in routers and switches
- High performance
- Fragmentation may cause a problem

Packet Filtering Gateways

Stateless—Two Separate ACLs Are Required

1. Permit HTTP traffic from 10.0.0.0 to www.yahoo.com
2. Permit HTTP traffic from www.yahoo.com to 10.0.0.0
Stateful Inspection Firewalls

- Packet filtering gateways plus...
- Maintaining state

Stateful firewalls inspect and maintain a record (a state table) of the state of each connection that passes through the firewall.

To adequately maintain the state of a connection the firewall needs to inspect every packet.

But short cuts can be made once a packet is identified as being part of an established connection.

Different vendors record slightly different information about the state of a connection.

- High performance and most popular

Example: Stateful Inspection of a TCP Connection
(A Connection-Oriented Reliable Protocol)

<table>
<thead>
<tr>
<th>Private Network</th>
<th>Public Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Addr</td>
<td>192.168.0.10</td>
</tr>
<tr>
<td>Destination Addr</td>
<td>198.133.219.25</td>
</tr>
<tr>
<td>Source Port</td>
<td>1026</td>
</tr>
<tr>
<td>Destination Port</td>
<td>23</td>
</tr>
<tr>
<td>Initial Sequence #</td>
<td>49091</td>
</tr>
<tr>
<td>Ack</td>
<td>Syn</td>
</tr>
<tr>
<td>Flag</td>
<td></td>
</tr>
<tr>
<td>192.168.0.10</td>
<td></td>
</tr>
</tbody>
</table>

Checks for a Translation Slot—Is It Part of an Existing Connection
1. Check for: (Src IP, Src Port, Dest IP, Dest Port)
2. Check Sequence Number
3. Check Flags

If the Code Bit Is Not syn-ack, Drop the Packet

<table>
<thead>
<tr>
<th>IP Header</th>
<th>TCP Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.133.219.25</td>
<td>Syn-Ack</td>
</tr>
<tr>
<td>192.168.0.10</td>
<td>Syn-Ack</td>
</tr>
</tbody>
</table>

1. # 1 Source Port: 1026 (Syn)
2. # 2 Destination Port: 23
3. # 3 Initial Sequence #: 49091
4. # 4 No Data
Example: Stateful Inspection of a TCP Connection (Cont.)

- Private Network:
  - IP Header: 192.168.0.10, 198.133.219.25
  - TCP Header: 1026, 23, 49092, 92514
  - #5 Data Flows: 10.0.0.3 -> 198.133.219.25

- Public Network:
  - IP Header: 192.168.0.10, 198.133.219.25
  - TCP Header: 1026, 23, 49770, 92514

- Checks for a Translation Slot:
  - If not, it creates one after verifying NAT, Global, Access Control, and Authentication or Authorization, if any; if OK, a connection is created.

Example: Stateful Inspection of a UDP Connection (A Connectionless Unreliable Protocol)

- Private Network:
  - Source Addr: 192.168.0.10
  - Destination Addr: 172.30.0.50
  - Source Port: 1028
  - Destination Port: 53

- Public Network:
  - Source Addr: 192.168.0.10
  - Destination Addr: 172.30.0.50
  - Source Port: 1028
  - Destination Port: 53

- The Firewall Checks for a Translation Slot; if not, it creates one after verifying NAT, Global, Access Control, and Authentication or Authorization, if any; if OK, a connection is created.

- SIF Firewall:
  - All UDP Responses Arrive from Outside and within UDP User-Configurable Timeout
  - (Src IP, Src Port, Dest IP, Dest Port) Check
  - Translation check
Stateful Inspection Firewalls

Stateful—Only One ACL Is Required
1. Permit HTTP traffic from 10.0.0.0 to www.yahoo.com

Proxy Firewalls

- All requests and replies pass though a proxy server; no direct connection between a client and the server; everything is proxied—thus the name
## Proxy Firewalls

Two Separate TCP Connections
- Client to proxy firewall
- Proxy firewall to www.yahoo.com

## How a Proxy Service Works

User Request to Gateway Server
ftp gw.foobar.com

Authentication by Gateway Server
gw.foobar.com
DNS Lookup
Internal.foobar.com
Re-Routing to Application Server
internal.foobar.com
Proxy Firewalls

- Proxy firewalls permit no traffic to pass directly between networks
- Provide “intermediary” style connections between the client on one network and the server on the other
- Addition of new applications require proxy development on server and client
- For HTTP (application specific) proxies all web browsers must be configured to point at proxy server

Personal Firewalls

- LITE version of network firewalls for laptops and desktops
- Disallow inbound connections unless explicitly allowed
- Watches inbound/outbound traffic
- Protect laptops and desktops from attacks
- Host Intrusion Prevention Systems (HIPS) integrated with a distributed firewall is a much better solution—provides zero day protection against worms and viruses
NAT/PAT Firewalls: Concept

NAT

Global pool
192.168.0.17-30
10.2.0.0 /24

192.168.0.0

Global pool
192.168.0.3-14
10.0.0.0/24

PAT

192.168.0.20
Port 2000

192.168.0.20
Port 2001

NAT Firewalls

• NAT Firewalls hide all internal addresses—thus protect small networks from external attacks as internal addresses are not exposed

• May offer minimal stateful inspection and basic VPN

• A full fledged stateful firewall is much powerful then basic NAT firewalls
Agenda

- Introduction to Firewalls
- Types of Firewalls
  - Modes and Deployments
- Key Features in a Firewall
- Emerging Trends

Form Factors

Dedicated Appliances
- Specialized and secure OS
- Ease of management
- Many price/performance levels

Software (Network and Personal)
- Runs on general purpose OS
- Multi-purpose server
- Light version—personal FW

Firewall Switch Module
- Very high performance
- Leverages existing infrastructure—saves rack space

Integrated in Router Software
- Investment protection
- WAN connections
- Performance considerations
Firewall Deployment

- Small Business/Branch Office
- Telecommuter
- Regional Office
- Internet
- Service Provider
- Corp HQ
- Perimeter
- Data Center and Internal Firewalls
- ASP
- Regional Office

Firewall Modes

- Virtual firewall mode
- Transparent firewall mode
Virtual Firewalls

- Logical partitioning of a single firewall into multiple logical firewalls, each with its own unique policies and administration
- Each virtual firewall provides the same firewall features provided by a standalone firewall
- Provides method to consolidate multiple firewalls into a single appliance, thus reducing overall management and operational overhead

Transparent Firewall

- Provides ability to easily "drop in" a firewall into existing networks without requiring any addressing changes
- Simplifies deployment, providing an ideal solution for small and medium businesses with limited IT resources
Agenda

• Introduction to Firewalls
• Types of Firewalls
• Modes and Deployments
  • **Key Features in a Firewall**
• Emerging Trends

**Key Features to Look for in a Firewall**

• **Performance**
  • Throughput (real world vs. best case)
  • Scalability—investment protection
  • ASIC vs. NP vs. general purpose CPU

• **Resiliency**
  • Active passive
  • Active active
  • Asymmetric routing
Key Features to Look for in a Firewall

• ACL management
  Performance
  Debugging
  Insertion/enabling
  Integration with AAA

• Dynamic protocols
  Multimedia applications
  FTP

Key Features to Look for in a Firewall

• Content filtering
  ActiveX/JAVA
  URL filtering
  Virus scanning

• VPN
  Site-to-site VPN
  Remote access VPN
  SSL VPN
Key Features to Look for in a Firewall

• Integration with the existing infrastructure
  - Integration with AAA servers
  - Integration with PKI servers
  - Centralized ACLs
  - Integration with VoIP protocols

• Management
  - Device managers
  - Multi-device managers
  - Logging and reporting
  - SOHO devices with dynamic IP addresses

Agenda

• Introduction to Firewalls
• Types of Firewalls
• Modes and Deployments
• Key Features in a Firewall
  • Emerging Trends
Emerging Trends

- Application inspection and WEB ACLs
  - Application firewalls
  - Instant messenger firewalls
  - Email firewalls
  - Web firewalls
- Integration with In-line IDS
- Integration with antivirus

Application Firewall: Many Definitions

- Application layer ACLs
  - Filtering based on normal application traffic (port 80 misuse and others)
- Protection against known vulnerabilities—signatures
- Protocol anomalies
- User defined filters (Layer 7 filtering)
  - Patterns (streams and context-based)
- Old proxy firewalls with enhanced speeds
Integration with Inline IDS

- Mixed opinion—supporters in both camps
- Direction—firewall vendors adding IDS and IDS vendors adding firewall features

**Key Issues**
- False positives—good traffic may be dropped
- Performance—Regex, a taxing operation
- Failover

- **No complete solution today by anybody**

Integration with Antivirus

- Integrated vs. stand-alone
- Some firewall vendors are integrating anti-virus software in low end boxes—all in one solution

**Key issue**
- Performance
THANK YOU