6
Packet Filtering
Learning Objectives

- Describe packets and packet filtering
- Explain the approaches to packet filtering
- Recommend specific filtering rules
Introduction

♦ Packets: discrete blocks of data; basic unit of data handled by a network
♦ Packet filter: hardware or software designed to block or allow transmission of packets based on criteria such as port, IP address, protocol
♦ To control movement of traffic through the network perimeter, know how packets are structured and what goes into packet headers
Understanding Packets and Packet Filtering

♦ Packet filter inspects packet headers before sending packets on to specific locations within the network

♦ A variety of hardware devices and software programs perform packet filtering:
  – Routers: probably most common packet filters
  – Operating systems: some have built-in utilities to filter packets on TCP/IP stack of the server software
  – Software firewalls: most enterprise-level programs and personal firewalls filter packets
Anatomy of a Packet

♦ Header
  – Contains IP source and destination addresses
  – Not visible to end users

♦ Data
  – Contains the information that it is intending to send (e.g., body of an e-mail message)
  – Visible to the recipient
Anatomy of a Packet (continued)
Anatomy of a Packet (continued)
Packet-Filtering Rules

- Packet filtering: procedure by which packet headers are inspected by a router or firewall to make a decision on whether to let the packet pass.
- Header information is evaluated and compared to rules that have been set up (Allow or Deny).
- Packet filters examine only the header of the packet (application proxies examine data in the packet).
Packet-Filtering Rules (continued)

- Drop all inbound connections; allow only outbound connections on Ports 80 (HTTP), 25 (SMTP), and 21 (FTP)
- Eliminate packets bound for ports that should not be available to the Internet (e.g., NetBIOS)
- Filter out ICMP redirect or echo (ping) messages (may indicate hackers are attempting to locate open ports or host IP addresses)
- Drop packets that use IP header source routing feature
Packet-Filtering Rules (continued)

♦ Set up an access list that includes all computers in the local network by name or IP address so communications can flow between them
  – Allow all traffic between “trusted” hosts
  – Set up rules yourself
Packet-Filtering Rules (continued)

[Image of Norton Internet Security interface showing settings for trusted and restricted network addresses.]

Identify trusted and restricted computers. Trusted computers have unlimited access to your computer; restricted computers have none.

- Trusted
  - IP: 207.177.178.140
  - Mask: 255.255.255.0

- Restricted
  - IP: 208.177.178.142
  - Mask: 255.255.255.0
Packet-Filtering Rules (continued)

![Advanced Rule Settings](image)
Packet-Filtering Methods

- Stateless packet filtering
- Stateful packet filtering
Stateless Packet Filtering

- Determines whether to block or allow packets—based on several criteria—without regard to whether a connection has been established.
- Also called static packet filtering.
- Useful for completely blocking traffic from a subnet or other network.
Criteria That a Stateless Filter Can Be Configured to Use

♦ IP header information
♦ TCP or UDP port number being used
♦ Internet Control Message Protocol (ICMP) message type
♦ Fragmentation flags (e.g., ACK and SYN)
Filtering on IP Header Criteria

- Packet’s source IP address
- Destination or target IP address
- Specify a protocol for the hosts to which you want to grant access
- IP protocol ID field in the header

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.0.1</td>
<td>80</td>
<td>Allow</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.0.1</td>
<td>443</td>
<td>Allow</td>
</tr>
<tr>
<td>Telnet</td>
<td>TCP</td>
<td>10.0.0.1/24</td>
<td>Any</td>
<td>192.168.0.5</td>
<td>223</td>
<td>Allow</td>
</tr>
</tbody>
</table>
TCP Flags in a Packet Header
Filtering by TCP or UDP Port Number

- Helps filter wide variety of information
  - SMTP and POP e-mail messages
  - NetBIOS sessions
  - DNS requests
  - Network News Transfer Protocol (NNTP) newsgroup sessions
- Commonly called port filtering or protocol filtering
Filtering by ICMP Message Type

- ICMP helps networks cope with communication problems
- No authentication method; can be used by hackers to crash computers on the network
- Firewall/packet filter must be able to determine, based on its message type, whether an ICMP packet should be allowed to pass
## Common ICMP Message Types

<table>
<thead>
<tr>
<th>ICMP Type</th>
<th>Name</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Echo reply</td>
<td>Normal response to a ping</td>
</tr>
<tr>
<td>3</td>
<td>Destination unreachable</td>
<td>Destination unreachable</td>
</tr>
<tr>
<td>3 code 6</td>
<td>Destination network unknown</td>
<td>Destination network unknown</td>
</tr>
<tr>
<td>3 code 7</td>
<td>Destination host unknown</td>
<td>Destination host unknown</td>
</tr>
<tr>
<td>4</td>
<td>Source quench</td>
<td>Router receiving too much traffic</td>
</tr>
<tr>
<td>5</td>
<td>Redirect</td>
<td>Faster route located</td>
</tr>
<tr>
<td>8</td>
<td>Echo request</td>
<td>Normal ping request</td>
</tr>
<tr>
<td>11</td>
<td>Time exceeded</td>
<td>Too many hops to destination</td>
</tr>
<tr>
<td>12</td>
<td>Parameter problem</td>
<td>There is a problem with a parameter</td>
</tr>
</tbody>
</table>
Filtering by Fragmentation Flags

♦ Security considerations
  – TCP or UDP port number is provided only at the beginning of a packet; appears only in fragments numbered 0
  – Fragments numbered 1 or higher will be passed through the filter
  – If a hacker modifies an IP header to start all fragment numbers of a packet at 1 or higher, all fragments will go through the filter
Filtering by Fragmentation Flags (continued)

- Configuration considerations
  - Configure firewall/packet filter to drop all fragmented packets
  - Have firewall reassemble fragmented packets and allow only complete packets to pass through
Filtering by ACK Flag

- ACK flag
  - Indicates whether a packet is requesting a connection or whether the connection has already been established
  - A hacker can insert a false ACK bit of 1 into a packet
- Configure firewall to allow packets with the ACK bit set to 1 to access only the ports you specify and only in the direction you want
Filtering Suspicious Inbound Packets

- Firewall sends alert message if a packet arrives from external network but contains an IP address from inside network
- Most firewalls let users decide whether to permit or deny the packet
  - Case-by-case basis
  - Automatically, by setting up rules
Filtering Suspicious Inbound Packets (continued)
Filtering Suspicious Inbound Packets (continued)
Stateful Packet Filtering

- Performs packet filtering based on contents of the data part of a packet and the header
- Filter maintains a record of the state of a connection; allows only packets that result from connections that have already been established
- More sophisticated and secure
- Has a rule base and a state table
Stateful Packet Filtering (continued)

1. Host attempts to connect to www.course.com

2. Router checks state table and sees that no connection exists; state entry created and request passed to rule base.

3. Rule that internal hosts can access TCP/80 exists; packet allowed to pass through.

4. Packet received by course.com Web server; SYN/ACK reply sent to firewall

5. Packet received state table entry referenced

6. Packet allowed to pass

State Table
Source IP: www.course.com
Source port: 80
Destination IP: 10.0.0.5
Destination port: 1037
Transport: TCP
Filtering Based on Packet Content

- Stateful inspection
- Proxy gateway
- Specialty firewall
Setting Specific Packet-Filter Rules

- Rules to filter potentially harmful packets
- Rules to pass packets that you want to be passed through
Best Practices for Firewall Rules

♦ All traffic from trusted network is allowed out
♦ Firewall device is never accessible directly from public network
♦ SMTP data allowed to pass through firewall but all is routed to well-configured SMTP gateway
♦ All ICMP data is denied
♦ Telnet access to all internal servers from public networks is blocked
♦ When Web services are offered outside firewall, implement proxy access or DMZ architecture
Rules That Cover Multiple Variations

♦ Must account for all possible ports that a type of communication might use or for all variations within a protocol
Sample Network to Be Protected by a Firewall
Rules for ICMP Packets

♦ ICMP lets you test network connectivity and makes you aware of communications problems
♦ Rules are especially important because ICMP packets can be easily forged and used to redirect other communications
# ICMP Packet-Filter Rules

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>Source Quench</td>
<td>Allow</td>
</tr>
<tr>
<td>2</td>
<td>ICMP Outbound</td>
<td>ICMP</td>
<td>192.168.2.1/24</td>
<td>Any</td>
<td>Echo Request</td>
<td>Allow</td>
</tr>
<tr>
<td>3</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>Echo Reply</td>
<td>Allow</td>
</tr>
<tr>
<td>4</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>Destination Unreachable</td>
<td>Allow</td>
</tr>
<tr>
<td>5</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>Service Unavailable</td>
<td>Allow</td>
</tr>
<tr>
<td>6</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>Time to Live (TTL)</td>
<td>Allow</td>
</tr>
<tr>
<td>7</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>Echo Request</td>
<td>Drop</td>
</tr>
<tr>
<td>8</td>
<td>ICMP Inbound</td>
<td>ICMP</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>Redirect</td>
<td>Drop</td>
</tr>
<tr>
<td>9</td>
<td>ICMP Outbound</td>
<td>ICMP</td>
<td>192.168.2.1/24</td>
<td>Any</td>
<td>Echo Reply</td>
<td>Drop</td>
</tr>
<tr>
<td>10</td>
<td>ICMP Outbound</td>
<td>ICMP</td>
<td>192.168.2.1/24</td>
<td>Any</td>
<td>TTL Exceeded</td>
<td>Drop</td>
</tr>
<tr>
<td>11</td>
<td>ICMP Block</td>
<td>ICMP</td>
<td>Any</td>
<td>Any</td>
<td>All</td>
<td>Drop</td>
</tr>
</tbody>
</table>
Rules That Enable Web Access

- Rules need to cover both standard HTTP traffic on TCP Port 80 as well as Secure HTTP (HTTPS) traffic on TCP Port 443

<table>
<thead>
<tr>
<th>Rule</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>HTTP Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.32</td>
<td>80</td>
<td>Allow</td>
</tr>
<tr>
<td>13</td>
<td>HTTPS Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.32</td>
<td>443</td>
<td>Allow</td>
</tr>
<tr>
<td>14</td>
<td>HTTP Outbound</td>
<td>TCP</td>
<td>192.168.1.2/24</td>
<td>Any</td>
<td>Any</td>
<td>80</td>
<td>Allow</td>
</tr>
<tr>
<td>15</td>
<td>HTTPS Outbound</td>
<td>TCP</td>
<td>192.168.2.32</td>
<td>Any</td>
<td>Any</td>
<td>443</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Rules That Enable DNS

- Set up rules that enable external clients to access computers in your network using the same TCP and UDP ports

<table>
<thead>
<tr>
<th>Rule</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>DNS Outbound</td>
<td>TCP</td>
<td>192.168.2.31</td>
<td>Any</td>
<td>Any</td>
<td>53</td>
<td>Allow</td>
</tr>
<tr>
<td>17</td>
<td>DNS Outbound</td>
<td>UDP</td>
<td>192.168.2.31</td>
<td>Any</td>
<td>Any</td>
<td>53</td>
<td>Allow</td>
</tr>
<tr>
<td>18</td>
<td>DNS Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.31</td>
<td>53</td>
<td>Allow</td>
</tr>
<tr>
<td>19</td>
<td>DNS Inbound</td>
<td>UDP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.31</td>
<td>53</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Rules That Enable FTP

- Rules need to support two separate connections
  - TCP Port 21 (FTP Control port)
  - TCP 20 (FTP Data port)
Rules That Enable FTP (continued)

<table>
<thead>
<tr>
<th>Rule</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>FTP Control Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.1.25</td>
<td>21</td>
<td>Allow</td>
</tr>
<tr>
<td>21</td>
<td>FTP Data Inbound</td>
<td>TCP</td>
<td>192.168.1.25</td>
<td>20</td>
<td>Any</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>22</td>
<td>FTP PASV</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.1.25</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>23</td>
<td>FTP Control Outbound</td>
<td>TCP</td>
<td>192.168.1.25</td>
<td>Any</td>
<td>Any</td>
<td>21</td>
<td>Allow</td>
</tr>
<tr>
<td>24</td>
<td>FTP Data Outbound</td>
<td>TCP</td>
<td>Any</td>
<td>20</td>
<td>192.168.1.25</td>
<td>Any</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Rules That Enable E-Mail

♦ Complicated; a variety of protocols might be used
  – For inbound mail transport
    • Post Office Protocol version 3 (POP3)
    • Internet E-mail Access Protocol version 4 (IMAP4)
  – For outbound mail transport
    • Simple Mail Transfer Protocol (SMTP)
  – For looking up e-mail addresses
    • Lightweight Directory Access Protocol (LDAP)
  – For Web-based mail service
    • HyperText Transport Protocol (HTTP)
## POP3 and SMTP E-Mail Rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Protocol</th>
<th>Transport Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Outbound POP3</td>
<td>TCP</td>
<td>192.168.2.1/24</td>
<td>Any</td>
<td>Any</td>
<td>110</td>
<td>Allow</td>
</tr>
<tr>
<td>26</td>
<td>Outbound POP3/S</td>
<td>TCP</td>
<td>192.168.2.1/24</td>
<td>Any</td>
<td>Any</td>
<td>995</td>
<td>Allow</td>
</tr>
<tr>
<td>27</td>
<td>Inbound POP3</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>110</td>
<td>Allow</td>
</tr>
<tr>
<td>28</td>
<td>Inbound POP3/S</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.1/24</td>
<td>995</td>
<td>Allow</td>
</tr>
<tr>
<td>29</td>
<td>SMTP Outbound</td>
<td>TCP</td>
<td>192.168.2.29</td>
<td>Any</td>
<td>Any</td>
<td>25</td>
<td>Allow</td>
</tr>
<tr>
<td>30</td>
<td>SMTP/S Outbound</td>
<td>TCP</td>
<td>192.168.2.29</td>
<td>Any</td>
<td>Any</td>
<td>465</td>
<td>Allow</td>
</tr>
<tr>
<td>31</td>
<td>SMTP Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.29</td>
<td>25</td>
<td>Allow</td>
</tr>
<tr>
<td>32</td>
<td>SMTP/S Inbound</td>
<td>TCP</td>
<td>Any</td>
<td>Any</td>
<td>192.168.2.29</td>
<td>465</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Chapter Summary

- Packet header criteria that can be used to filter traffic
- Approaches to packet filtering
- Specific packet-filter rules