Firewall

Copyright © 2005 Jun Li.
All rights reserved.

Outline

• Intro
• Packet filters
• Circuit gateways
• Application-level filtering
• A case study
• A brief overview of VPN

Firewall Introduction

• A firewall is any device, software, or arrangement or equipment that limits network access between nodes inside your network and “outsiders”
• Three main categories
  – Packet filtering
  – Circuit gateways
  – Application gateways

Packet Filters

• Cheap and useful
  – You need a router to connect to outside anyway
• Drop packets based on source or destination addresses or port numbers
  – Often has an access control list
• Filtering can be done at the incoming interface, the outgoing interface, or both

Stateless vs. Stateful Packet Filter

• Stateless packet filter: decisions are solely based on the contents of the current packet
• Stateful packet filter: remembers what has happened in the recent past in order to change its filtering rules dynamically
  – E.g. Only if there is an outgoing connection from \( s \) to \( d \) will the firewall allow an connection from \( d \) to \( s \)

Configuring a Packet Filter

• Step 1: one must have a security policy
  – Know what is allowed, and what’s not
• Step 2: specify the policy formally
  – E.g. in terms of logical expressions on packet fields
• Step 3: implement the policy
  – E.g. the expressions must be rewritten in whatever syntax your vendor supports
A Packet Filtering Example

<table>
<thead>
<tr>
<th>Action</th>
<th>Our host</th>
<th>Port</th>
<th>Their host</th>
<th>Port</th>
<th>comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>*</td>
<td>*</td>
<td>evil.com</td>
<td>*</td>
<td>We don’t trust them</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>

Packet Filtering Performance

- Packet filtering takes time and can defeat optimization efforts
- Fortunately, often the bottleneck is not CPU, but the bandwidth
  - E.g., if a router is connected to the Internet via a T1 line (1.544 Mbps)
- Not true any more if the filtering operations are very complex

Circuit-level Gateways

- Work at the TCP level
- TCP connections are relayed through a computer
  - The relay computer copies bytes between two connections
- Can handle UDP traffic as well
- Often replace addresses of internal nodes

Application-Level Filtering

- Deals with the details of a particular service
- Usually more complex than packet filters
  - Special-purpose code used for each application
- Question is: can one provide application-level filtering for ALL applications?
- Other drawbacks:
  - More intrusive
  - Slow
  - Hard to be comprehensive
  - More options as moving up the network layer stack

An Example: Email Filter

- It understands RFC 822 headers
- It understands MIME-formatted attachments
- May be able to scan viruses
- Or look for information leaks
- Users can keep the same email address, no matter which machines they use

Case Study: The Dribble Inc.

- The Dribble Corporation wants to provide certain services:
  - Web access (ads, online sale, etc.)
  - Email
  - And connection to the Internet from inside
- While still having a solid security
Security Policy

<table>
<thead>
<tr>
<th></th>
<th>Outsiders</th>
<th>Developers</th>
<th>Executives</th>
<th>Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Data</td>
<td>read</td>
<td>read</td>
<td>read</td>
<td>read</td>
</tr>
<tr>
<td>Data for existing</td>
<td>read</td>
<td></td>
<td>read</td>
<td></td>
</tr>
<tr>
<td>products</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data for future</td>
<td>read, write</td>
<td>read</td>
<td></td>
<td></td>
</tr>
<tr>
<td>products</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate data</td>
<td>read, write</td>
<td>read</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer data</td>
<td>write</td>
<td>read</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

DMZ

- **DMZ** (demilitarized zone): a portion of a network that separates a purely internal network from an external network.

The Drib’s Firewalls

- The public cannot communicate directly with internal network.
- Nor the internal network can communicate directly with the public.
- DMZ is the “bottleneck” for both.
- Firewalls help conceal the addresses of the internal network.

Outer Firewall

- **Properties:**
  - Restrict public access to the Drib’s network.
  - Restrict the Drib’s access to the Internet.
  - While allowing certain sanitized info exchanges.
    - Based on source or destination address, port number, etc.

The Drib’s Network Infrastructure

- **Outbound:**
  - Public Data Subnet
Inner Firewall

- Goal: protect the internal network where sensitive data resides
- Implementation: block all traffic except for that specifically authorized to enter
  - DMZ web server to the internal web server
  - DMZ email server to the internal mail server

So, What Can’t Firewalls Do?

- Often useless against attacks from inside
  - Imagine a legitimate user who has just turned to the dark side
  - Or a newly compromised machine from inside
  - Hard and crunchy on the outside; soft and chewy on the inside
- Traffic often transformed
  - Compressed, encrypted, etc.
- Performance issue
  - Line-speed processing is not always guaranteed
- Recommendation: do not rely on firewalls as your sole protection mechanism

VPNs

- If a single site can be protected using firewall technique, what if multiple sites that all belong to a private company?
- Virtual Private Networks extend the boundary of a protected domain through use of cryptography

VPN Types

- Type 1: enable remote branch offices to share a security parameter
  - And even an address space
- Type 2: enable remote users to connect to their work location from home, hotel, or coffeeshop
- Type 3: implement a DMZ among companies that wish to share data and services
  - But do not wish to open their entire networks to each other