The Multilayer Firewall

Dan Nessett
Technology Development Center
3Com Corporation
Polar Humenn
BlackWatch Technology
Usual Disclaimer

This talk describes a prototype

• No commitment by 3Com to turn it into product.

• No commitment by 3Com to do anything with technology described in this talk.
Partnering arrangements are a problem

- Survey of 35 fortune 1000 companies shows 46% give business partners corporate intranet access (Forrester Report - Partners on the Internet).

- Ineffective controls for containing partner accesses.
Hypothetical Example

- Transmissions
- Ford
- Mufflers
- Mazda
- Arvin

Improper Access
Motivation

Another problem is insider threat

• Estimate 50-70% of security incidents are by insiders (FBI/CSI report; ASIS Intellectual Property Report).

• Insiders may violate security for various reasons:
  – Disgruntled employee
  – Criminal activity
  – The “thrill of hacking”
What to do?

Need a set of tools:

- Application level - GSSAPI mechanisms, CORBAsec, PKI (credentials management), ...

- Session level - TLS (protection of legacy apps/systems)

- Network level - IPSEC, Firewalls, Routing security (traffic containment/protection)
Part of the solution

Extend notion of Firewall into network

- Control traffic in network with network device (router, switch) filtering.

- Create filter information on central management system.

- Distribute to network (enforcement) devices.
Multilayer Firewall (MLF)
System Architecture

Enforcement devices:

- Filters must have sufficient reach (e.g., at least to TCP/UDP port information).

- Should support “fast” filtering (e.g., tens to hundreds of thousands of packets/sec).

- Need not support same filtering “language”.
System Architecture

Enforcement devices:

- Routers (NB2)
  > 85K pps (no filtering);
  > 47K pps (filtering)

- Switch (CB 2500 - 1/3 cost of NB2)
  > 148K pps (no filtering);
  > 75K pps (filtering)

- Switch (CB 3500 L3 switch - 1/2 cost)
  > 4 Mpps (no filtering);
  > not yet released (filtering)
System Architecture

MLF Management Station:

- Groups hosts according to administrative view, not physical connectivity.
- Define firewall rules between host groups (e.g., src/dst/protocol/allow:disallow).
- For each rule, compute which enforcement devices get filters.
- Compile high-level rule into low-level filtering commands based on device type.
Filter Rule Generation

Key idea in MLF:

• Use the physical topology of the network to drive filter rule computation.

• Each end system is “behind” one or more enforcement devices.

• For each firewall rule, compute a cut-vertex set (of enforcement devices) that isolates the src hosts from the dst hosts.
Filter Rule Generation

A Cut-set of
HG 1 and
HG 3

Host Group 1
Host Group 2
Host Group 3

Another One
Filter Rule Generation

Some details

• Cut-set need not be minimum.

• There may be different device types in cut-set, each with own filtering language.

• Translate firewall rule into filters expressed in each filtering language.

• Download filters to enforcement devices in cut-set. Iterate over all firewall rules.
Prototype Implementation

Architecture

- Host groups defined by ‘traffix’ - RMON2 monitor app.

- Once src & dst host groups are selected, policy editor called.

- Policy editor works on rule table (similar to traditional FW table).
Traffix Console
## Policy Editor

### Tartan Multi-Layer Firewall Policy Tool

#### Policy Specification Editor

<table>
<thead>
<tr>
<th>Grouped by:</th>
<th>Security Policy Grouping: Security View</th>
<th>Company, Department, Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>3Com. Engineering. *</td>
<td>3Com. Sales. *</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>Rule Description</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Policy</th>
<th>Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3Com. Engineering. East</td>
<td>3Com. Sales. *</td>
<td>172.15.168.82</td>
<td>HTTP</td>
<td>Allow</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td>3Com. Sales. unassigned</td>
<td>3Com. Sales West</td>
<td>172.15.168.80</td>
<td>FTP</td>
<td>Allow</td>
<td>Both</td>
</tr>
</tbody>
</table>

#### Filter Policy

- Protocol:
  - ARCHIE
  - ALL
  - COURIER
  - DNS\Svr\Svr

#### Enforcement

- Source
- Destination
- Both
Backup Slides
Traditional Firewall

- Firewall Management
- Border Firewall
Internal Threats

Traffic should be heavily controlled

- Marketing
- Sales
- Engineering
Multilayer Firewall Architecture

1. Update Policy
2. Signal Device
3. Request New Policy
4. Policy Returned

Persistent Store

Web Based Network Management Station

Managed Device
Special Case