Firewalls

NIST Special Publication: 800-41

Douglas Couch
IT Security Analyst
Purdue University
Why we need firewalls  
-Historically

ROBERT TAPPAN MORRIS  
ADRIAN LAMO  
JONATHAN JAMES
Why we need firewalls
-Today

- Storm Worm
- IRC Bots
- Identity Theft
- $$$
- At Purdue: HIPPA, FERPA, GLBA, VISA
History of firewalls

- First firewalls = router ACL’s
- 1988 DEC created packet filter firewalls
- 1990 AT&T Bell Labs created circuit level firewalls
- Gene Spafford, Bill Cheswick, and Marcus Ranum publish descriptions of an application layer firewall
- June 1991: Emergence of the first commercial firewall: DEC SEAL
Types of firewalls

- Packet Filtering
  - Layer 3 (Network) of the OSI model
  - Filters on Source, Destination, and Type
  - Fast and flexible
- Stateful Inspection
  - Adds layer 4 (Transport) awareness
- Application-Proxy Gateways
  - Layer 7 (Application) functionality
  - Authentication
Architecture topologies
-Dual Homed
Architecture topologies
-Multi-Homed (DMZ)
Architecture topologies
-Screened Subnet
Basic Guidelines

- KISS
- Use devices as they were intended
- Defense in Depth
- Pay attention to internal threats
## Cisco Firewall

### Configuration > Security Policy > Access Rules

<table>
<thead>
<tr>
<th>#</th>
<th>Rule Enabled</th>
<th>Action</th>
<th>Source Host/Network</th>
<th>Destination Host/Network</th>
<th>Rule Applied To Traffic</th>
<th>Interface</th>
<th>Service</th>
<th>Syslog Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>any</td>
<td>any</td>
<td>incoming</td>
<td>inside</td>
<td>TCP</td>
<td>ip</td>
</tr>
<tr>
<td>2</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:Network-Support</td>
<td>Group:NOC:Hosts</td>
<td>incoming</td>
<td>inside</td>
<td>ICMP</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:DNS-Servers</td>
<td>Group:NOC:Hosts</td>
<td>incoming</td>
<td>inside</td>
<td>TCP</td>
<td>echo-reply/icmp</td>
</tr>
<tr>
<td>4</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:DNS-Servers</td>
<td>Group:NOC:Hosts</td>
<td>incoming</td>
<td>inside</td>
<td>TCP</td>
<td>domain/tcp</td>
</tr>
<tr>
<td>5</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>any</td>
<td>Group:DNS-Servers</td>
<td>incoming</td>
<td>inside</td>
<td>TCP</td>
<td>domain/udp</td>
</tr>
<tr>
<td>6</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>224.0.0.0/4</td>
<td>Group:Network-Support</td>
<td>incoming</td>
<td>outside</td>
<td>TCP</td>
<td>ip</td>
</tr>
<tr>
<td>7</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:EMC_ECC_Hosts</td>
<td>Group:All_Servers</td>
<td>incoming</td>
<td>outside</td>
<td>TCP</td>
<td>Group:EMC_ECC_TCP</td>
</tr>
<tr>
<td>8</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>ariba.qa.qs01.itap/128.210.23.24</td>
<td>Group:All_Servers</td>
<td>incoming</td>
<td>outside</td>
<td>TCP</td>
<td>Group:Ariba_T0</td>
</tr>
<tr>
<td>9</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:PowerCenter_Hosts</td>
<td>Group:All_Servers</td>
<td>incoming</td>
<td>outside</td>
<td>TCP</td>
<td>Group:Powercenter_TCP</td>
</tr>
<tr>
<td>10</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:SSH_Hosts</td>
<td>Group:All_Servers</td>
<td>incoming</td>
<td>outside</td>
<td>TCP</td>
<td>Group:ssh</td>
</tr>
<tr>
<td>11</td>
<td>✔️</td>
<td>✔️ ✔️</td>
<td>Group:Purdue_Nets</td>
<td>Group:All_Servers</td>
<td>incoming</td>
<td>outside</td>
<td>TCP</td>
<td>Group:UC4_Range</td>
</tr>
</tbody>
</table>
Always Deny

- Inbound traffic to the firewall itself
- Inbound traffic with a source IP from behind the firewall
- Inbound ICMP
- Inbound traffic with a “private” address
- Inbound SNMP
- Using an address of 127.0.0.1
- Using an address of 0.0.0.0
Best Practices

- Deny all traffic by default
- Identify and allow only necessary services
- Perform vulnerability assessments
- Perform ongoing audits
- Use change-management
- Enable logging and alerting
- Monitor logs
- Use Host Based Firewalls
Caveats

- Firewalls can’t read packets with bad intent
- Firewalls can’t protect from inside threats
- Modems and Wifi hubs can circumvent Firewalls
Conclusion

- Firewalls are necessary in today’s environment
- Decide on a topology
- Determine what access is needed
- Keep it simple
- Monitor your environment

- Questions?