Firewall Architectures of E-Commerce

EE657 Midterm Project Presentation – Professor Hwang

Andy Yan

Four State-of-the-art Firewall Architectures

• Description of 4 solutions
  – IBM – eNetwork
  – Compaq – AXENT’s Raptor Firewall
  – Sun Microsystems – SunScreen Firewall
  – Milkyway – SecurIT Firewall

• Functionality and System Requirement Comparison

• Improved firewall solutions
IBM FIREWALL SOLUTION - eNetwork

Main Features
- VPN support based on IPSec Standard
- It supports TDP and UDP applications by SOCKS Version 5
- It periodically scans hosts and firewalls for potential security exposures
- It is capable to use the Internet as the VPN media instead of using privately leased line

IBM FIREWALL SOLUTION - eNetwork

- It provides a centralized, easy, and secure management of multiple firewalls
- It can disable suspicious applications to ensure a secure platform for the firewall
- It provides real-time log and performance statistics monitoring
- It provides a Secure Mail Proxy for anti-spamming and anti-mail-spoofing capabilities
IBM FIREWALL SOLUTION - eNetwork

Application-Level Proxy
- It enables Telnet and FTP and also Transparent Telnet, FTP, and HTTP
- When a user contacts the proxy server using one of the TCP/IP applications, the proxy server does all the connections with the remote system on behalf of the user
- It authenticates users with several techniques, such as SecurID cards, S/Key, SecurNet Key cards and also password verification

IBM FIREWALL SOLUTION - eNetwork

Circuit-Level Proxy – The circuit-level proxy is implemented in 2 ways
- As a SOCKS server
  - It authenticates the user and redirect all the related traffic through the firewall.
- Network Address Translation (NAT)
IBM FIREWALL SOLUTION - eNetwork

High Level of Protection

- It uses 56-bit data encryption standard (DES), which is the strongest encryption techniques on the market approved by federal government.
- It provides a program, Network Security Audition, which is the tool that is used to scan servers, firewalls, and network to look for potential security holes. It also lets administrator to manage the all the firewalls in a centralized manner.

Milkyway – SecurIT Firewall

Dual SecurIT Firewall Configuration
Compaq’s Solution – AXENT’s Raptor Firewall

• Compaq is a major vendor in building high performance severs, works with AXENT to provide an enterprise solution to e-commerce. AXENT's Raptor Firewall is one of the most well-developed security systems available to the market. Compaq’s high performance Proliant 800 with dual 500MHz processors and AXENT Raptor Firewall for NT provides a safe VPN network environment, efficient data integrity on individual servers, and secure system for electronic business.

Compaq’s Solution – AXENT’s Raptor Firewall

Address Redirection -- The address redirection is a function to provide a way to alias between a virtual or external server and a host with the network.

– Load balancing, it provides the ability to service to multiple clients using a single interface while redirecting traffic accesses to multiple server. For example, DNS.
– The internal IP are still encapsulated and hidden from outside system.
– An illusion of accessing hosts from public view.
Authentication Mechanism

- Secure Dynamics SecureID (ACE)
  - A 6-digit password generated by ACE/Server software
- AXENT’s Defender
  - A hardware password generation device
- CRYPTOCard
  - Challenge and response using CRYPTOCard hardware device
- Bellcore S/Key
  - Software-based authentication method based on a seed value

Virtual Private Networking operates in a Finance Network
**Compaq’s Solution – AXENT’s Raptor Firewall**

*Monitoring and Administration*

<table>
<thead>
<tr>
<th>Message Severity</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>Raptor Firewall (gwcontrol) has failed, and network traffic through the gateway has been shut down.</td>
</tr>
<tr>
<td>Critical</td>
<td>A Raptor Firewall ancillary service has failed</td>
</tr>
<tr>
<td>Alert</td>
<td>A suspicious activity threshold has been met or exceeded.</td>
</tr>
<tr>
<td>Error</td>
<td>Normal gateway activities cannot complete successfully.</td>
</tr>
<tr>
<td>Warning</td>
<td>Recoverable errors exist.</td>
</tr>
<tr>
<td>Notice</td>
<td>Attempted connection denied by the Raptor Firewall.</td>
</tr>
<tr>
<td>Informational</td>
<td>Connection attempt allowed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action Type</th>
<th>System Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>Plays as audio file on the gateway</td>
</tr>
<tr>
<td>Mail</td>
<td>Emails the text of the message to a designated recipient</td>
</tr>
<tr>
<td>Page</td>
<td>Transmits the text of the message to a designated alphanumeric paging device</td>
</tr>
<tr>
<td>Client</td>
<td>Launches a client program</td>
</tr>
<tr>
<td>SNMPv1</td>
<td>Sends an SNMPv1 trap to a designated system</td>
</tr>
<tr>
<td>SNMPv2</td>
<td>Sends an SNMPv2 trap to a designated system</td>
</tr>
</tbody>
</table>

**Sun Microsystems – SunScreen Firewall**

- This product emphasizes on a Secure Virtual Private Networks for enterprise corporations. SunScreen’s secures electronic business solution composed of three server products, SunScreen SPF, SunScreen EFS, and SunScreen SKIP, to secure the network completely.
Sun Microsystems – SunScreen Firewall

SunScreen SPF -- perimeter defense system
- Stealth Design
  - It avoid exposures of internal identities from the outside
- It protects both UDP and TCP services
- Data Encryption
  - Sun’s SKIP protects data by encryption, and a high level of authentication to ensure data integrity
- Network Address Translation

SunScreen EFS -- is used to protect sites and multiple subnetworks within an organization.

Traditional Firewall Configuration

SunScreen Firewall Configuration
Milkyway – SecurIT Firewall

- SecurIT Firewall is an application and circuit-level gateway without using any form of packet filtering mechanism that is a common technique used by many firewall vendors.
- Using a patented Bi-Directional Transparency implemented inside the firewall. The parties involved are unaware that they are connecting through a security check while providing a bullet proof system.

Milkyway – SecurIT Firewall

Dual SecurIT Firewall Configuration – provides an ultimate defense against man-in-the-middle attacks in the subnetwork as well as providing transparent access to the Internet. It enhances the security of the corporate network by dividing the network into private network and secure subnetwork.
Milkyway – SecurIT Firewall

**Dual SecurIT Firewall Configuration**

SecurIT firewall is designed to especially protect from these attacks:

- **Buffer Overflow**
  - It anticipates buffer overflow and terminates all connections for fast recovery rather than crash the network system.

- **Trojan Horses**
  - Unauthorized applications are not allowed to run on the firewall.

- **Spoofing**
  - The firewall listens to all ports and all IP packets in both directions. Any spoofing activities will be detected and terminated.

- **Sniffing and Hijacking**
  - It protects the traffic from sniffing and hijacking by keeping the traffic invisible to outside the secure network.
## Functionalities and System Requirement Comparison

### General Information

<table>
<thead>
<tr>
<th>Price Range</th>
<th>IBM-eNetwork 4.2</th>
<th>Sun-SunScreen 3.0</th>
<th>AXENT-Raptor 6.0</th>
<th>Milkyway-SecurIT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$1976 - $19500</td>
<td>$1500 - $29995</td>
<td>$6500 (25)- $24999</td>
<td>$2900-$20500</td>
</tr>
<tr>
<td>NCSA Certified</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Type</td>
<td>Packet Filtering, proxy, circuit-level gateway</td>
<td>Packet-filtering, stateful inspection</td>
<td>Application-Level</td>
<td>Application-level &amp; circuit-level gateway</td>
</tr>
<tr>
<td>Processor Requirement</td>
<td>RISC 6000</td>
<td>SPARC or Pentium</td>
<td>Pentium 90</td>
<td>Pentium 133</td>
</tr>
<tr>
<td>Operating System</td>
<td>AIX 4.1.5 ( Win NT 4.0 and AS/400)</td>
<td>SunOS or Windows NT</td>
<td>Windows NT 4.0</td>
<td>Windows NT 4.0</td>
</tr>
<tr>
<td>Memory Requirement</td>
<td>64MB</td>
<td>64MB</td>
<td>64MB</td>
<td>64MB</td>
</tr>
<tr>
<td>Diskspace Requirement</td>
<td>800MB</td>
<td>1GB</td>
<td>500MB</td>
<td>1GB</td>
</tr>
</tbody>
</table>

### Product Features

<table>
<thead>
<tr>
<th>Access Prohibition</th>
<th>IBM-eNetwork 4.2</th>
<th>Sun-SunScreen 3.0</th>
<th>AXENT-Raptor 6.0</th>
<th>Milkyway-SecurIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCKS Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NAT</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IP Forwarding</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP Address Filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrity Check</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrity Monitoring and Notification</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>SecurID cards, S/Key, SecurNet Key Cards</td>
<td>Sun’s SKIP</td>
<td>SecurID cards, NXENT’s Defender, CRYPTOCard, S/Key</td>
<td>SecurIT Access</td>
</tr>
<tr>
<td>Full Encryption</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevent IP Spoofing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevent SYNC Flooding</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Functionalities and System Requirement Comparison

Firewall Product Management

<table>
<thead>
<tr>
<th></th>
<th>GUI</th>
<th>Remote Management</th>
<th>Centralized Administration</th>
<th>Activities Logging</th>
<th>Statistics Auditing</th>
<th>User-Definable Logging</th>
<th>Remote log Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM-eNetwork 4.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sun-SunScreen 3.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AXENT-Raptor 6.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Milkyway-SecurIT</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Elements in Improved Firewall Architecture

- Effective firewall capable to protect from several kinds of attacks include passive eavesdropping, packet sniffing, IP address spoofing, port scans, denial-of-service attacks, application-layer attack, as well as virus immune system.
- Automatic virus upgrade from major anti-virus vendors.
- Intrusion prevention and intrusion detection.
- Secure network perimeter control.
- Secure Virtual Private networks with network address translation, data encryption, packet filtering, and strong authentication.
- Advanced monitoring of all connections with smart detection of suspicious connections from monitoring data. Efficient logging system to record all the activities across and inside of the system.
- High speed and high performance firewall with load balancing for all connections.
- Distributed or collaborative processing power from multiple firewalls.
Elements in Improved Firewall Architecture

- Encapsulation of internal network structure and identity of the network from outside system.
- Increase availability of the VPN when using the Internet as a connection media. The VPN connections should not depend on the reliability of the Internet.
- Easy-to-use interface to control and maintain the network system in a centralized manner with secure remote administration capability independent of system, for example, a web-based interface is a good feature.
- With perimeter control of the network, internal subnetworks or departments should also be individually secured.
- Capable to fast recover and learn from past system attacks or system failure. The system should able to detect and avoid from the same attacks.
- Open system architecture capable for future development of new technology.
- The firewall architecture must be scalable when the network size increases