RealSentry™ SSL overview

Advanced Protection for Web Services

- SSL Accelerator
- Intrusion Detection System
- Reverse Proxy
- Application-Firewall
Web services deployment

The principal reasons which delay the deployment of web technologies

- Technology with a poor level of security: 43%
- Insufficient XML knowledge: 37.8%
- Immaturity of standards: 31.9%
- Not in adequation with company’s needs: 31.1%
- No vendor leader clearly identified: 30.4%
- Not enough tools: 24.4%
- Young and unstable technology: 22.2%

This survey was carried out in November 2001 with 135 French companies
(Source: 01 Informatique)
How to protect Web Servers today?

Today, the best solution uses three components:

- Firewall: To forward only HTTP(S) packets to Web servers
- Network-based Intrusion Detection System (NIDS): To prevent from malicious packets
- Vulnerability scanner: To detect known vulnerabilities on systems
Vulnerabilities: A worrying progression

Vulnerabilities reported
Source: CERT Coordination Center

1998: 262
1999: 417 (+59%)
2000: 1090 (+161%)
2001: 2437 (+123%)

Code Red: 2.6 billion US dollars of damage
Nimda: 590 million US dollars of damage
Why are Firewalls insufficient?

- Security Policy based only on type of protocols (not on content)
- Unable to analyse encrypted network traffic like HTTPS
- Unable to process a finer-grained analysis of the application activities
- Usually protects only from external network
- Network device managed by a security administrator (in opposition with a Web server managed by a webmaster)
Why are NIDS insufficient?

- Protect only against known vulnerabilities (pattern matching)
- Cannot scan content if network traffic is encrypted
- Difficult to deploy on switched networks
- Cannot handle high-speed networks
- Critical setup: Bad configuration generates many false alarms
- Unable to process a finer-grained analysis of the application activities
A new approach against HTTP attacks

**Real-time virus detection**

The Antivirus detects and blocks viruses

**Real-time HTTP traffic control**

RealSentry detects and protects against known or unknown vulnerabilities
(1) HTTP request send by a user
(2) Hardware (RealSentry SSL) or software (RealSentry) decryption
(3) Check HTTP packet with Full HTTP Inspection™ Technology
(4) If validated by security policy, safe HTTP packet is forwarded to Web Server
(5) Check HTTP packet with Full HTTP Inspection™ Technology
(6) Hardware (RealSentry SSL) or software (RealSentry) encryption
(7) HTTP answer is sent back to the user
RealSentry provides the ultimate protection

More than 200 new vulnerabilities each month

More than 20 new vulnerabilities each month

No vulnerability can reach your Web Server

Full connectivity

Restricted connectivity

High Secure connectivity

Hacker

Firewall

RealSentry SSL

Web Servers

FTP
DNS
HTTP
HTTPS
SMTP
ICMP

HTTP
HTTPS
Four technologies in a single box

**Reverse Proxy**

Like reverse Proxy:
- RealSentry breaks direct connection between browser and Web server.

But unlike Reverse Proxy:
- RealSentry includes filter capability to exclude malicious HTTP packets.
- RealSentry keeps original IP address when operates in stealth mode.

**NIDS**

Like IDS Probe:
- RealSentry is a network-based protection and runs in stealth mode.

But unlike IDS Probe:
- RealSentry protects against unknown vulnerabilities.
- RealSentry protection is effective even on encrypted packets (HTTPS).

**Application Firewall**

Like Application Firewall:
- RealSentry allows to implement a security Policy to accept or deny packets.

But unlike Application Firewall:
- RealSentry performs a detailed protocol analysis to prevent against malicious HTTP requests.

**SSL Accelerator**

Like SSL Accelerator:
- RealSentry handles decryption and encryption tasks for SSL transactions.

But unlike SSL Accelerator:
- RealSentry incorporates built-in security mechanism to protect your website from fraudulent activities.
RealSentry Technology

Black List Detection (IDS technology)

- **Concept**
  - Signature-based method
  - Requires regular updates
  - Protects only against known vulnerabilities

- **RealSentry Implementation**
  - Automatic updates
  - Multiple rules to prevent IDS evasion
  - Very easy to setup: Protect your Web server in a few minutes

- **RealSentry Benefits**
  - Detects more than 600 HTTP vulnerabilities
  - Effective protection including on encrypted traffic (HTTPS)
  - No need to monitor vulnerabilities or patch your Web server
  - Plug and Protect solution
White List Filtering (Exclusive Axiliance technology)

- **Concept**
  - All HTTP requests that are not expressly authorized are prohibited
  - Non signature-based method
  - Protection against known or unknown vulnerabilities

- **RealSentry Implementation**
  - Security Policy define by URL groups, directories or single URL
  - Security Policy includes syntax, URL length, Variables, cookies, ...
  - Setup assistants with learning, tracking and protecting modes

- **RealSentry Benefits**
  - Identify and prevent both known and unknown vulnerabilities
  - Effective protection including on encrypted traffic (HTTPS)
  - Represents the most secure solution for Web services currently available in the world
Normal Life Cycle of a vulnerability ...

- Vulnerability discovered
- Exploit publication
- Hotfix provided by vendor
- Hotfix applied

Minimum delay generally observed: 10 - 15 days
RealSentry with only Black List Protection

Security Level vs Time

- Vulnerability discovered
- Exploit publication
- Hotfix provided by vendor
- Hotfix applied

Vendor reactivity → Customer reactivity

Update attack signature

Maximum delay generally observed: 24 hours
RealSentry with White List Protection

- Insensitive to new vulnerabilities
- Update attack signature
- Vulnerability discovered
- Exploit publication
- Hotfix provided by vendor
- Hotfix applied
The 4 solutions to prevent vulnerabilities

- **Manual Vulnerability Assessment**
  - (Vulnerability scanner used manually)

- **Automated Vulnerability Assessment**
  - (Vulnerability scanner used automatically)

- **RealSentry (minimum secure configuration)**
  - (RealSentry in non-stealth mode with only Black List Protection)

- **RealSentry (full secure configuration)**
  - (RealSentry in stealth mode with integral White List Protection)
**Black List Mode**

- **RFC conformity check**
  - (HTTP Header Fields)
  - **OK**
  - **KO**

- **HTTP IDS**
  - (Black List Protection)
  - **OK**
  - **KO**

- **Reject**
  - **Logs**
  - **SNMP**
  - **SMTP**
  - **SMS**

---

RealSentry & RealSentry SSL Overview – v1.1 – © Copyright 2002 - AXILIANCE
Counter measures with HTTP IDS

- Buffer overflow
- Cross Site Scripting
- Remote Command
- SQL injection
- Path Transversal
- Meta Characters
- Null Bytes
- Predefined Pattern

Requête HTTP contenant un pattern réputé vulnérable

Toute requête (pour compatibilité ancienne version)
Counter measures with IDS et FW HTTP

Black List

- Toute requête
  (pour compatibilité ancienne version)

White List

- Requête dynamique avec politique de sécurité

Application vulnerabilities
- Brute Force
- Buffer overflow
- Cross Site Scripting
- Remote Command
- SQL injection
- Path Transversal
- Meta Caracters
- Null Bytes
- Predefined Pattern

Requête HTTP contenant un pattern réputé vulnérable
RealSentry Security Level

High

RealSentry with a maximum security policy

White List Filtering
(URL syntax, variables and cookies supervised by security policies)

RealSentry with a strong security policy

Default Security Policy
(RFC conformity, URL Length, Authorized char, …)

RealSentry with a minimum security policy

Black List Protection
(pattern matching)

Low

Setup and management

Easy

Protection against unknown attacks or vulnerabilities

Difficult

Protection against known attacks or vulnerabilities
High Availability: Normal operation

NORMAL OPERATION

Out-of-band monitoring with RS-MONITOR & RS-FAILOVER

unsafe HTTP(S) → safe HTTP

Master: Active – Monitoring HTTP(S) Traffic
Slave: Passive - Monitoring Master activities

Master: Electronic bypass
Slave: Electronic bypass
High Availability: Fault operation

**DEFAULT OPERATION**

**Master**
- Fail – Ethernet IN/OUT in Bypass mode
- Electronic bypass

**Slave**
- Active – Monitoring HTTP(S) Traffic
- Electronic bypass

**Unsafe HTTP – Unsafe HTTPS**

- Master: Fail – Ethernet IN/OUT in Bypass mode
- Slave: Active – Monitoring HTTP(S) Traffic
RealSentry SSL v1.0 Features

- - - - APPLIANCE
  Integrated solution (hard and soft)

- - - - SSL ACCELERATION
  Boosted and secure encrypted traffic

- - - - INTRUSION DETECTION
  Exclusive technology from Axiliance

- - - - STEALTH MODE
  « Plug and Protect » solution

- - - - FAULT TOLERANCE
  High availability - 24/7
## Competitive Comparisons

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Native Fault Tolerance</th>
<th>Stealth Mode</th>
<th>SSL Acceleration</th>
<th>Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kavado</td>
<td>Interdo</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sanctum Inc</td>
<td>AppShield</td>
<td>No</td>
<td>Yes</td>
<td>compliant with 3rd party</td>
<td>Option</td>
</tr>
<tr>
<td>Deny-All</td>
<td>Rweb</td>
<td>No</td>
<td>No</td>
<td>compliant with 3rd party</td>
<td>No</td>
</tr>
<tr>
<td>Ubizen</td>
<td>dmz/shield</td>
<td>No</td>
<td>No</td>
<td>compliant with 3rd party</td>
<td>Option</td>
</tr>
<tr>
<td>Stratum 8</td>
<td>APS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Axiliance</td>
<td>RealSentry</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Axiliance</td>
<td>RealSentry SSL</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
RealSentry: Setup and management

Full out-of-band management by serial or ethernet interface

- SSH Ethernet
- TELNET Serial
- HTTP Packets Inspection modules
- APACHE Reverse Proxy
- Stealth Modules
- LINUX Kernel
- Database
  - Configuration
  - Security policies
  - Logs
- Administration Web

- HTTPS Ethernet
Network Installation
- First setup by serial console
- Access restricted to a special account (ADMIN)

Management of services and security policies
- Network Interface card dedicated to management operations
- Intuitive and secure Web-based administration (HTTPS)
- Command line based administration via restricted and secure shell
- Service creation is only allowed to an administrator account (ADMIN)
- Each service is associated to one or several Webmaster
- Services Management is only allowed to the Webmaster
Black List Mode

- - - - Initial Setup
- - - - RS232 Console

- - - - Create Services
- - - - HTTPS via dedicated interface

- - - - Connect to network
- - - - Web servers protected
White List Mode

- - - - Initial Setup
- - - - Create Services
- - - - Bypass Mode
- - - - Learning Mode
- - - - Tracking Mode
- - - - Protected Mode
- - - - RS232 Console
- - - - HTTPS via dedicated interface
- - - - Open network traffic
- - - - Generate White List
- - - - Check White List
- - - - Web servers are protected

Protected Mode

Web servers are protected
Case Studies

- Case Study 1: RealSentry SSL protects Intranet Web Servers
- Case Study 2: RealSentry dedicated for hosting in ISP architecture
- Case Study 3: RealSentry mutualized for hosting in ISP architecture
- Case Study 4: DMZ Protection with non transparent mode
- Case Study 5: DMZ Protection with stealth mode
- Case Study 6: Multiple DMZ Protection with non transparent mode
- Case Study 7: Multiple DMZ Protection with stealth mode
CS1 : Intranet Web Servers Protection

Before

Critical web-based intranet applications

Private Network

After

Critical web-based intranet applications

Stealth mode
Firewall mode
Full White List
SSL acceleration

Private Network

Customer benefits :

- Forward only HTTP(S) packets to Web Server (Firewall mode)
- Protect Web server against known or unknown HTTP Attacks
- Non restrictive SSL usage without need to upgrade server hardware
- Installation without any network modification
- Native simple fault tolerance by electronic bypass
CS3 : RealSentry mutualized for ISP

Internet

Secure Web Servers

RealSentry

Web Servers

DMZ
CS4 : Non Transparent Mode
CS5 : Stealth Mode

Diagram:
- Internet
- DMZ
- RealSentry
- Secure Web Servers

Network Configuration:
1. Internet
2. DMZ
3. RealSentry
4. Secure Web Servers
CS6 : Multiple DMZs – Non Transparent
CS7: Multiple DMZs – Stealth Mode

Internet

RealSentry

DMZ 1

Secure Web Servers

DMZ 2

Secure Web Servers
Thank you for your attention

Boris MOTYLEWSKI
e-mail : bm@axiliance.com

AXILIANCE S.A.
Société Anonyme au capital de 120 000 Euros
Siège social : Montpellier - FRANCE

TEL : +33 (0)4 67 79 79 31
FAX : +33 (0)4 67 79 79 32

WEB : http://www.axiliance.com
MAIL : info@axiliance.com