SecureSphere® Web Application Firewall

The Industry's Only Automated Web Application Firewall

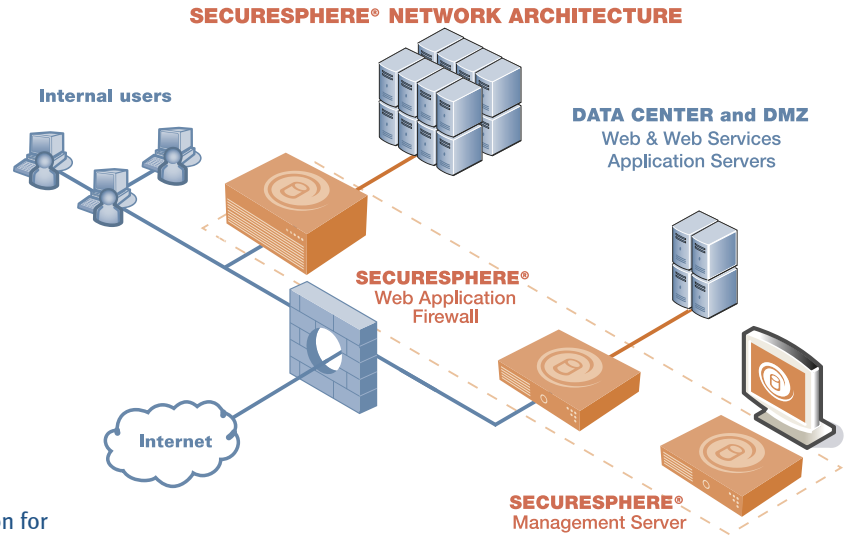
Web applications have lowered costs and increased revenue by extending the enterprise's strategic business systems to customers and partners. However, Web applications also expose these critical systems to continuous threats from both internal and external sources.

Defending Web applications is one of the most challenging aspects of information security. Because Web applications constantly change to meet business requirements, the security model must adapt as changes are made to the applications. In addition, because data centers are highly optimized, deploying an application security solution must require minimal changes to the existing infrastructure. Unfortunately, first generation Web Application Firewalls are too inflexible for most customer environments, too intrusive to deploy and too costly to maintain.

What is needed is a new type of Web Application Firewall that can automatically adapt as applications change, can be deployed without disrupting the existing infrastructure and can meet stringent enterprise requirements for security, performance, deployment, operations and regulatory compliance.

Automated Web Application Security

The SecureSphere® Web Application Firewall is the only solution to provide automated attack protection for Web and Web Services applications. Imperva's Dynamic Profiling technology builds a model of legitimate application behavior and adapts to application changes over time, keeping SecureSphere's application protection up to date and accurate. Deployed in minutes with no changes to the data center infrastructure, SecureSphere enables precise attack protection without manual configuration or tuning.



Dynamic Profiling is the foundation of a multi-layer security architecture that provides complete protection for all layers of the application infrastructure, including the network, server and application. Imperva's Transparent Inspection technology delivers multi-gigabit performance, sub-millisecond latency and options for high availability that meet the most demanding data center requirements. For large scale deployments, the SecureSphere MX Management Server centralizes and streamlines configuration, administration, monitoring and reporting. And because SecureSphere supports a broad range of network deployment options, it can be deployed into any environment without requiring any network changes.

Complete Attack Protection

Web Application Firewall
SecureSphere protects custom Web application code against attacks such as SQL injection, cookie poisoning, parameter tampering, directory traversal and more (see list below). Dynamic Profiling automatically creates a dynamic positive security model of Web application usage and structure, including URLs, http methods, parameters, hidden fields, cookies, session IDs and response codes. As users interact with the application, SecureSphere closely monitors their activities and compares them to the profile. Any attempted attack is detected and blocked.

Automated and Accurate Protection Against:

- Web, HTTPS and XML application attacks
- SQL Injection
- Session Hijacking
- Cross Site Scripting (XSS)
- Form Field Tampering
- Known Worms
- Zero Day Web Worms
- Buffer Overflow
- Cookie Poisoning
- Denial of Service
- Malicious Robots
- Parameter Tampering
- Brute Force Login
- Malicious Encoding
- Directory Traversal
- Web Server and Operating System Attacks
- Scanning
- Command Injection
- Illegal Encoding
- Identity Theft
- Data Theft
- Patient and Financial Data Disclosure
- Corporate Espionage
- Phishing
- Data Destruction

Web Services Firewall
SecureSphere's Web services firewall protects against attacks targeting XML, SOAP and WSDL applications. Like SecureSphere's Web application firewall the Web services firewall leverages Imperva's Dynamic Profiling technology to create a dynamic positive security model of allowed application usage and structure, including XML URLs, SOAP actions, XML elements and XML attributes. Any attempts to tamper with Web services application schemas or variables are identified and blocked.

Intrusion Prevention System (IPS)
SecureSphere IPS provides broad protection against known infrastructure attacks and zero day worms. These attacks typically target vulnerabilities in commercial web server, application server and operating system software (e.g. IIS, Apache, and Windows 2000). SecureSphere's zero day worm profiling technology identifies attacks for which there are no signatures by detecting the specific combinations of attributes that uniquely characterize such attacks. SecureSphere also provides full Snort®-compatible signature support across all protocols, HTTP protocol compliance and advanced application protection signatures from the Application Defense Center – Imperva's own international security research organization. The SecureSphere Security Update Service provides regular updates to ensure the most up to date protection is continuously enforced.

Network Firewall
SecureSphere's integrated stateful network firewall protects against unauthorized users, dangerous protocols, common network layer attacks and worm infections. Access control policies support both black and white listing of protocol/IP address combinations to eliminate data center exposure to non-essential or dangerous protocols such as Telnet, pcAnywhere, or even SQL.

Extending SecureSphere to Databases
The SecureSphere Web Application Firewall can be extended to include database protection for Oracle, MS-SQL Server, DB2 (including mainframe) and Sybase databases. SecureSphere database security protects against external attacks and insider abuse, providing end-to-end defense for the data center.

Unparalleled Accuracy
SecureSphere incorporates both dynamic positive (white list) and dynamic negative (black list) security models. Instant Attack Validation (IAV) immediately validates and blocks any clear violations according to either model. For complex attacks that are neither clearly good nor clearly bad, Imperva's unique Correlated Attack Validation (CAV) technology correlates violations across multiple layers and over time to separate actual attacks from legitimate user traffic. CAV effectively correlates information from all of SecureSphere security layers to achieve overall accuracy that cannot be matched by several standalone security products.

Deployment

No Changes to Existing Network
SecureSphere can be flexibly deployed in the network as a transparent inline bridge, an inline router, an inline proxy or non-inline network monitor. Because of this flexibility, deployment requires no changes to the existing network architecture, including network routers, load balancers and servers.

No Changes to Application
Powered by a unique Transparent Inspection technology, SecureSphere examines Web traffic for attacks and malicious activity without altering or rewriting Web content. This enables SecureSphere to provide complete and accurate application security without forcing organizations to redesign their Web applications, change authentication schemes or install new SSL certificates.

Gigabit Performance
SecureSphere delivers multi-gigabit throughput and over 36,000 transactions per second while maintaining sub-millisecond packet latency. This level of performance is an order of magnitude better than competing approaches. A single SecureSphere gateway is sufficient for many customers and SecureSphere can scale to meet the requirements of the largest enterprise by deploying multiple gateways managed from a single unified management server. With SecureSphere, security will never impact your data center service level agreements (SLAs).

High Availability
SecureSphere supports a broad range of options to ensure maximum uptime and application availability.

- Imperva High Availability (IMPVHA) protocol provides sub-second failover for two or more SecureSphere gateways deployed in bridging mode.
- Virtual Router Redundancy Protocol (VRRP) provides for failover when SecureSphere is configured as a router or proxy.
- Redundant gateways can be deployed in environments with redundant system infrastructures. SecureSphere's transparent deployment modes support both active-active and active-passive fail-over configurations when using external HA mechanisms.
- Inline fail-open network interfaces ensure availability in the event of software, hardware, or power failures
- Non-inline monitoring configuration offers transparent deployment with no single point of failure.

Operations

Automated Application Security
Ongoing policy maintenance is the most significant component of a security solution's total cost of ownership (TCO).

It is not practical to expect multiple organizations (e.g. operations, security, and software development) to jointly tune a security product every time the application changes. Dynamic Profiling eliminates manual tuning by automatically adapting to application changes as they are deployed. However, administrators have full access to view and modify profiled information as well as create custom policy rules as desired. The result is comprehensive protection of data center assets without new burdensome operational processes.

Centralized Management
SecureSphere G4 and G8 appliances can be deployed in standalone configurations and include all of the administration and reporting capabilities needed to manage a deployment. For larger environments, including mixed Web and database gateway deployments, the SecureSphere MX Management Server provides centralized management capability; including profile management, status monitoring, alerting, logging and reporting activity.

Regulatory Compliance Reporting
SecureSphere delivers rich graphical reporting capabilities, enabling customers to easily understand security status and meet regulatory compliance requirements. SecureSphere provides both pre-defined and fully-customizable Web-based reports. Reports can be viewed on demand or emailed on a daily, weekly or monthly basis. In addition, a real-time dashboard offers a high-level view of system status and security events. SecureSphere's flexible reporting and monitoring tools provide instant visibility into security, compliance, and content delivery concerns.

SecureSphere's Web-based reports and real-time dashboard

Automated and Configurable Security Policy Definition

Dynamic Profiling™ - Automated Application Modeling
At the heart of SecureSphere's automated approach to security is Dynamic Profiling. Dynamic Profiling automatically examines live traffic to create a comprehensive model (profile) of an application's structure and dynamics. Valid application changes are automatically recognized and incorporated into the profile over time.

SecureSphere employs Dynamic Profiling to create positive security models of legitimate user behaviors for Web and Web Services applications. By comparing profiled elements to actual traffic, SecureSphere is able to detect malicious activity of any kind.

Dynamic Profiling overcomes the biggest drawback of other application firewall solutions – manual rule creation and maintenance. Unlike network firewall solutions where policy may be limited to a few dozen static rules, application firewall policy requires hundreds or thousands of rules governing thousands of constantly changing variables including URLs, parameters, cookies, XML elements and form fields. Dynamic Profiling delivers completely automated security with no need for manual configuration or tuning. If desired, administrators can always manually modify the profiles to bridge any differences between actual usage and corporate security policies.

Custom Policy Definition
In addition to the automated policy definition provided by Dynamic Profiling, SecureSphere allows security administrators to define policies regarding specific attributes of Web traffic. Custom policy rules are manually configured and provide the power to perform operations that are not available or convenient to implement via profile and protocol violation rules.

SecureSphere Appliance Specifications

Specification	G4	G8	G16
Throughput	500 Mbps	1000 Mbps	2000 Mbps
Transactions per Second	16,000	24,000	36,000
Latency	Sub-millisecond	Sub-millisecond	Sub-millisecond
Form Factor	1U	1U	4U
Interfaces	6 x 10/100/1000 Mbps (max 4 fiber interfaces)	6 x 10/100/1000 Mbps (max 4 fiber interfaces)	6 x 10/100/1000 Mbps (max 4 fiber interfaces)
Interface Types	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX	Copper/Fiber SX/Fiber LX
Max Bridging/Routing Segments	2/5	2/5	2/5
Inline Fail Open (Bridging Only)	Yes	Yes	Yes
Hard Drive	250GB SATA; FT Model: hot-swap 250GB SATA	250GB SATA; FT Model: hot-swap 250GB SATA	Hot-Swappable 300GB SCSI
External Drive	CD-ROM	CD-ROM	DVD-ROM
Enclosure	19 inch rack	19 inch rack	19 inch rack
Weight	40 lbs (18Kg)	40 lbs (18Kg)	90lbs (41Kg)
Power Supply	500W; FT Model: Dual, hot-swap 520W	500W; FT Model: Dual, hot-swap 520W	Dual, hot-swap 1470W
AC Power Requirements	100-240V, 50-60 Hz	100-240V, 50-60 Hz	220-240V, 50-60 Hz
Dimensions	W 16.93" (430mm) D 26.46" (672mm) H 1.7" (43mm)	W 16.93" (430mm) D 26.46" (672mm) H 1.7" (43mm)	W 17.6" (447mm) D 27.8" (706mm) H 6.8" (173mm)
Operating Environment	5°C (41°F) to 35°C (95°F)	5°C (41°F) to 35°C (95°F)	5°C (41°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)
Electromagnetic Capability	FCC Part 15, ICES-003, CE, VCCI	FCC Part 15, ICES-003, CE, VCCI	FCC Part 15, ICES-003, CE, VCCI

Specification	MX Management Server
Form Factor	1U
Interfaces	2 x 10/100/1000 Mbps Copper
Hard Drive	250GB SATA; FT Model: Hot-swap 250GB SATA
External Drive	CD-ROM
Enclosure	19 inch rack
Weight	40 lbs (18Kg)
Power Supply	500W; FT Model: Dual, hot-swap 520W
AC Power Requirements	100-240V, 50-60 HZ
Dimensions	W 16.93" (430mm), D 26.46" (672mm), H 1.7" (43mm)
Operating Environment	5°C (41°F) to 35°C (95°F)
Non-Operating Environment	-40°C (-40°F) to 70°C (158°F) relative humidity 95%, non-condensing at 35°C (95°F)
Electromagnetic Capability	FCC Part 15, ICES-003, CE, VCCI

Imperva Inc.
U.S. Headquarters
950 Tower Lane
Suite 1550
Foster City, CA 94404
Tel: (650) 345-9000
Fax: (650) 345-9004

International Headquarters
12 Hachilazon Street
Ramat-Gan 52522
Israel
Tel: +972-3-6120133
Fax: +972-3-7511133

Toll Free (U.S. only): 866-592-1289
www.imperva.com

eWEEK Excellence Award
Network Data-Stream Protection
June 19, 2006
SecureSphere 4.2

IBM Business Partner

ORACLE PARTNER

SYBASE BUSINESS SOLUTIONS ALLIANCE