BIG-IP Application Security Manager

Delivering Next Generation Application Security

With the increase in application traffic moving to the web, more sensitive customer data is being exposed to new security vulnerabilities and attacks, such as targeted and untargeted attacks on web client/server applications and data. These attacks are also increasing at the application layer and can include sophisticated breach attempts within protocol and data access methods such as HTTP, XML, XSS, buffer overflow, and SQL injection.

F5 BIG-IP® Application Security Manager™ (ASM) is an advanced web application firewall providing comprehensive web application security that significantly reduces and mitigates the risk of loss or damage to data, intellectual property, and web applications. BIG-IP ASM protects an organization's brand equity and reputation, provides end-to-end data protection for business enterprises, and addresses key regulatory mandates such as PCI DSS, HIPPA, and SOX. BIG-IP ASM ensures the industry's most comprehensive protection of identity information (credit card numbers, bank accounts, etc.) by controlling access to this information as part of every HTTP request/response. With BIG-IP ASM, you get a complete solution that reduces the need for multiple appliances, lowers maintenance and management costs, and increases the confidentiality, availability, and integrity of your critical business applications and processes.

Key Benefits:

- **Comply with Industry Security Standards** – Built-in security protection helps companies achieve security standards compliance including PCI DSS, HIPAA, and SOX in a cost-effective way.
- **Reduce Risk with Fast Remediation** – An advanced automatic policy builder enables quick fixing of newly discovered vulnerabilities, eliminating the time, risk, and cost for application developers and third-party providers.
- **Get Out-of-the-Box Protection** – Pre-built rapid deployment policies provide out-of-the box protection with minimal configuration for any internal or third-party application.
- **Centralize Security Log Management** – Log entire HTTP messages—internally or externally—to a centralized log server where log messages can be collected, aggregated, and analyzed for quick troubleshooting and compliance with security standards.
- **Increase Business Agility** – Focus on fast business process application development and deployment with security policies that are automatically created and managed.
- **Secure Data While Improving Performance** – Improve overall user experience and application performance with the high performance and scale of the F5 TMOS™ architecture, including SSL offload, caching, compression, TCP optimization, and more.
- **Network, Application, and Protocol Protection** – Enable packet filtering, message inspection, and manipulation with a network firewall in a true proxy architecture.

Real-Time Traffic Policy Builder

At the heart of BIG-IP ASM is the dynamic policy builder engine, which is responsible for the automatic self-learning and creation of security policies. Once traffic flows through BIG-IP ASM, the policy builder starts to parse requests and responses, providing the unique ability to inspect the bi-directional flow of full client and application traffic—both data and protocol. By using the advanced statistics and heuristics engine, the policy builder can filter out attacks and abnormal traffic. The policy builder can also run in a mode in which it is made aware of site updates. By parsing responses and requests it can detect site changes and automatically update the policy accordingly, without any user intervention.

Out-of-the-Box Protection

BIG-IP ASM is equipped with a set of pre-built application security policies that provide out-of-the box protection for common applications such as Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials, and Microsoft Office SharePoint. In addition, BIG-IP ASM includes a rapid deployment policy, which secures any customer application. The validated policies require zero configuration time and serve as a starting point for more advanced policy creation, based on heuristic learning and specific customer application security needs.

Advanced Enforcement

BIG-IP ASM can secure any parameter from client-side manipulation and validate logon parameters and application flow to prevent forceful browsing and logical flaws. BIG-IP ASM also protects against OWASP top ten and zero-day web application attacks.

Integrated XML Firewall

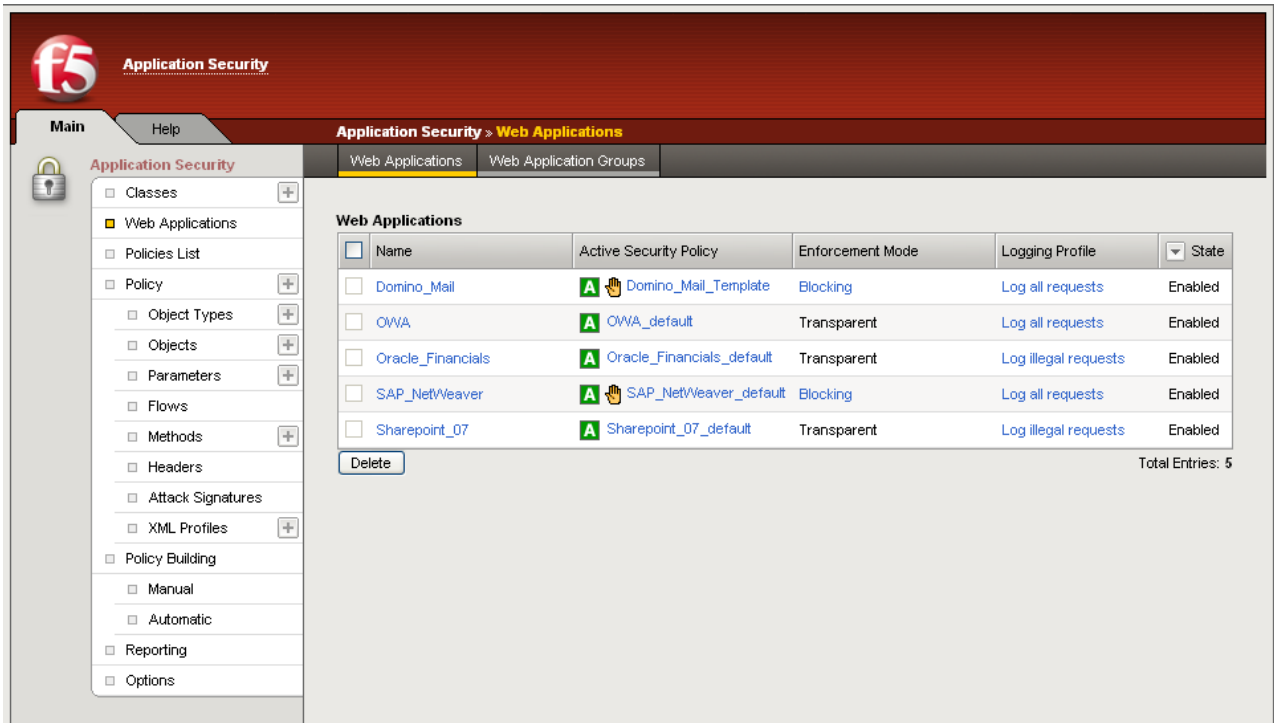
BIG-IP ASM provides application-specific XML filtering and validation functions that ensure that the XML input of web-based applications is properly structured. It provides schema validation, common attacks mitigation, and XML parser denial-of-service prevention.

Data Guard and Cloaking

BIG-IP ASM prevents the leakage of sensitive data (such as credit card numbers, social security numbers, and any sensitive customer data) by stripping it out. In addition BIG-IP ASM will hide error pages and application error information, preventing hackers from discovering the underlying architecture and launching a targeted attack.

WhiteHat Sentinel Integration

WhiteHat Security offers a unique vulnerability assessment service that combines automated tools with dedicated, highly skilled application security experts. Through integration with BIG-IP ASM, the industry-leading WhiteHat Sentinel service can create BIG-IP ASM rules that specifically address the vulnerabilities discovered in a web application. The result is a validated and actionable vulnerability assessment with a near-instantaneous mitigation response.

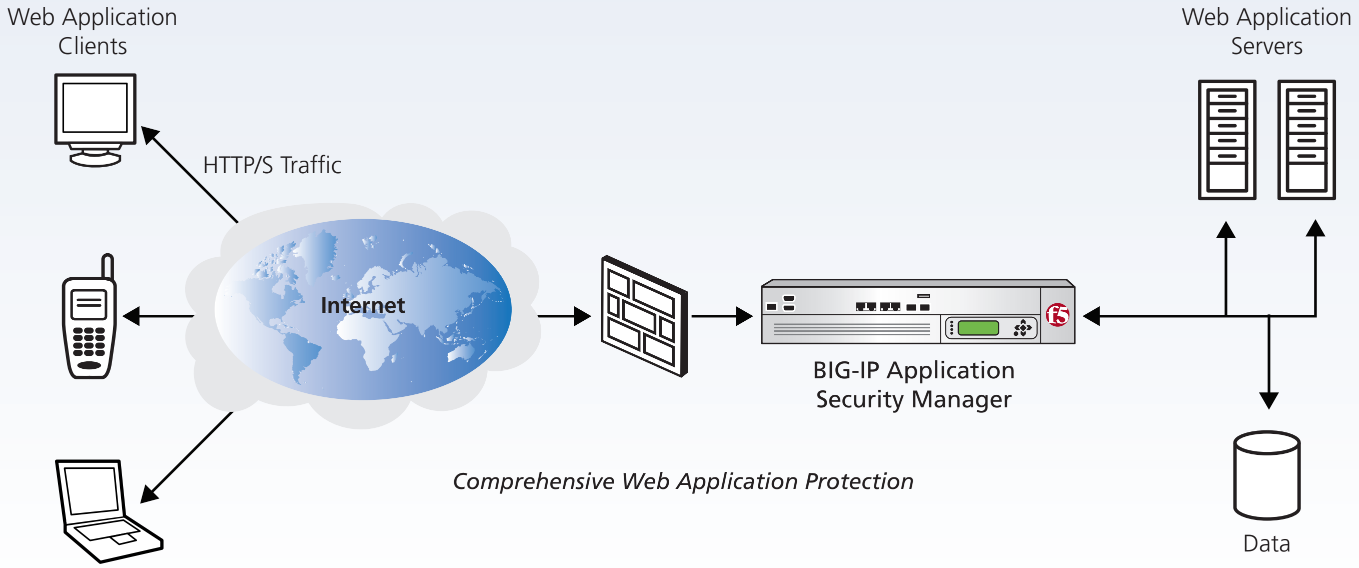


Web Applications

□	Name	Active Security Policy	Enforcement Mode	Logging Profile	State
□	Domino_Mail	A Domino_Mail_Template	Blocking	Log all requests	Enabled
□	OWA	A OWA_default	Transparent	Log all requests	Enabled
□	Oracle_Financials	A Oracle_Financials_default	Transparent	Log illegal requests	Enabled
□	SAP_NetWeaver	A SAP_NetWeaver_default	Blocking	Log all requests	Enabled
□	Sharepoint_07	A Sharepoint_07_default	Transparent	Log illegal requests	Enabled

Total Entries: 5

Pre-built, validated application security policies require no configuration to provide out-of-the-box protection for many mission-critical applications.



Comprehensive Web Application Protection

Live Update for Signatures

New signatures from new attacks are frequently required to ensure up-to-date protection. BIG-IP ASM queries the F5 signature service on a daily basis and automatically downloads and applies new signatures, providing up-to-date protection for new threats without the need for maintenance.

SMTP and FTP Security

BIG-IP ASM eases the manageability of FTP server farms. BIG-IP ASM validates the FTP protocol, mitigates brute force attacks, and can also whitelist the enabled FTP commands. In addition, it can enforce command length limits and passive/active connections. For SMTP, BIG-IP ASM provides additional security checks at the perimeter. It also supports graylisting to prevent SPAM, enforces the SMTP protocol, blacklists dangerous SMTP commands, and mitigates directory harvesting attacks. The rate-limiting capabilities of BIG-IP ASM help to fight DOS attacks.

Comprehensive Application Delivery Security

BIG-IP ASM runs on F5's unique purpose-built TMOS architecture. TMOS is an intelligent, modular, and high-performing platform that enhances every function of BIG-IP ASM. TMOS delivers insight, flexibility, and control, helping you intelligently protect your web applications.

TMOS delivers:

- SSL offload
- Caching
- Compression
- The ability to manipulate any application content on-the-fly, regardless of in- or outbound traffic
- TCP/IP optimization
- Advanced rate shaping and quality of service
- IPV6 support
- IP/port filtering
- VLAN support through a built-in switch

BIG-IP-ASM protects against various application attacks, including:

- Cross-site scripting
- SQL injection
- Parameter tampering
- Sensitive information leakage
- Session highjacking
- Buffer overflows
- Cookie manipulation
- Various encoding attacks
- Broken access control
- Forceful browsing
- Hidden fields manipulation
- Request smuggling
- XML bombs/DOS

Additional Network Security Services

BIG-IP ASM also includes:

- SSL accelerator
- Stateful layer 3–4 firewall
- Transparent and non-transparent reverse proxy
- Key management and failover handling
- SSL termination and re-encryption to web servers
- VLAN segmentation
- DOS protection
- Client-side certificates support
- Client authentication via LDAP/RADIUS
- Dedicated management port

Platform Specifications

BIG-IP ASM is available as a software module on the 3600, 6400, 6800, 8400, and 8800 BIG-IP® Local Traffic Manager™ series, or as a standalone BIG-IP ASM solution on the 3600 and 4100 platforms. The 3600 and 4100 standalone solutions include IPv6, advanced client authentication module, 5000 SSL TPS, rate shaping module, caching module, and 5 Mbits of compression.

Hardware Platforms

For detailed physical specifications, please refer to the BIG-IP Series Hardware Datasheet.

8800 Series and 8400 Series

6800 Series and 6400 Series

4100 Series

3600 Series

F5 Networks, Inc.
Corporate Headquarters

401 Elliott Avenue West
Seattle, WA 98119
+1-206-272-5555 Phone
(888) 88BIGIP Toll-free
+1-206-272-5556 Fax
www.f5.com
info@f5.com

F5 Networks
Asia-Pacific

+65-6533-6103 Phone
+65-6533-6106 Fax
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa

+44 (0) 1932-582-000 Phone
+44 (0) 1932-582-001 Fax
emeainfo@f5.com

F5 Networks
Japan K.K.

+81-3-5114-3200 Phone
+81-3-5114-3201 Fax
info@f5networks.co.jp