



What's Inside:

- 2 Built-in Compliance Capabilities
- 3 Comprehensive Attack Protection
- 5 Policy Control
- 6 Integration for Agility and Adaptability
- 8 The BIG-IP ASM Architecture
- 9 F5 Services
- 9 More Information



Achieve Regulatory Compliance and Defend Against Attacks

As more application traffic moves over the web, sensitive data is exposed to theft, security vulnerabilities, and attacks, especially at the application layer. F5 BIG-IP® Application Security Manager™ (ASM) is an advanced web application firewall that significantly reduces and mitigates the risk of loss or damage to data, intellectual property, and web applications. BIG-IP ASM provides unmatched application and website protection, a complete attack expert system, and compliance for key regulatory mandates—all on a platform that consolidates application delivery with network and application acceleration and optimization.

The result is the industry's most comprehensive web application security and application integrity solution. The award-winning BIG-IP ASM solution protects your organization and its reputation by maintaining the confidentiality, availability, and performance of the applications that are critical to your business.

Key benefits

Reduce costs and enable compliance

Achieve security standards compliance with built-in application security protection.

Ensure app security and availability

Get comprehensive attack protection from DDoS, layer 7 DoS, brute force, XSS, SQL injection, OWASP Top Ten, and more.

Get out-of-the-box app security policies

Provide protection with pre-built rapid deployment policies and minimal configuration.

Improve app security and performance

Enable advanced application security while accelerating performance and improving cost effectiveness.

Handle threats with greater agility

Focus on fast application development and deployment with automatic security policies.

PCI reporting specifies which requirements are being met as well as steps required to become compliant.

According to the Web Application Security Consortium [96.85%](#) of websites have vulnerabilities providing immediate risk of attack while [69.37%](#) of the vulnerabilities are client-side. As more applications move to the web, data breach from web applications is a real concern. Once a breach occurs, the Ponemon Institute estimates the total average costs of a data breach is \$202 per record compromised and \$225 for malicious insiders or former workers.¹

Built-in Compliance Capabilities

Advanced, built-in security protection and remote auditing help your organization comply with industry security standards, including Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Basel II, and SOX, in a cost-effective way—without requiring multiple appliances, application changes, or rewrites. BIG-IP ASM reports previously unknown threats, such as layer 7 denial-of-service (DoS) and SQL injection attacks, and it mitigates web application threats to shield the organization from data breaches. All reports are GUI-driven and provide drill-down options with a click.

[Printable Version...](#)

PCI Compliance Report	
Description	The PCI Compliance Report lists each security measure required for PCI-DSS 1.2 compliance. It indicates which measures are relevant and which are not relevant to the ASM appliance. For relevant security measures, it indicates whether this ASM appliance is in compliance, and if it is not, explains what you must do to bring it into compliance.
ASM Valid License	✓
Web Application	asas <input type="text" value=""/>
Active Policy (Version)	asas_default [v9]
Active Web Application	✓

Executive Summary			
#	Requirement	Compliance State	Details
1	Install and maintain a firewall configuration to protect cardholder data	N/A	N/A
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✓	View Details
3	Protect stored cardholder data	✓	View Details
4	Encrypt transmission of cardholder data across open, public networks	✓	View Details
5	Use and regularly update anti-virus software	N/A	N/A
6	Develop and maintain secure systems and applications	✓	View Details
7	Restrict access to cardholder data by business need-to-know	N/A	N/A
8	Assign a unique ID to each person with computer access	✓	View Details
9	Restrict physical access to cardholder data	N/A	N/A
10	Track and monitor all access to network resources and cardholder data	✓	View Details
11	Regularly test security systems and processes	N/A	N/A
12	Maintain a policy that addresses information security	N/A	N/A

PCI reporting

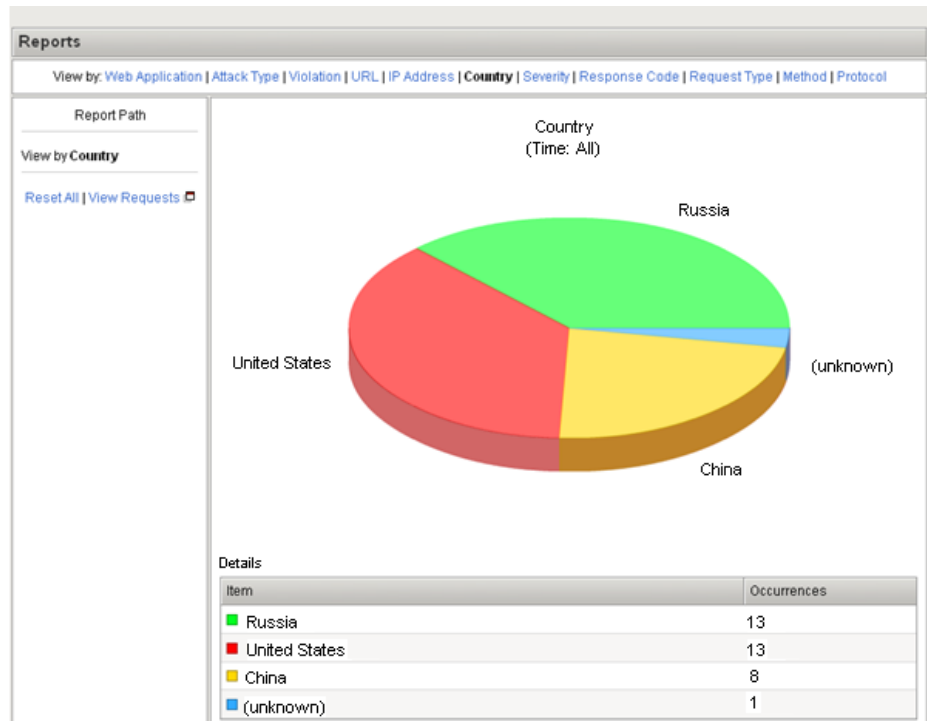
With PCI reporting, BIG-IP ASM lists security measures required by PCI DSS 1.2, determines if compliance is being met, and details steps required to become compliant if not.

Geolocation reporting

Geolocation reporting informs you of the country where threats originate in addition to attack type, violation, URL, IP address, severity, and more. You can also schedule reports to be sent to a designated email address automatically for up-to-date reporting.

¹ [“Data breach costs rise as firms brace for next loss,” Robert Westervelt, SearchSecurity.com.](#)

With attacks coming from around the world, geolocation reporting helps you identify where threats originate.



Easy-to-read format for remote auditing

BIG-IP ASM makes security compliance easier and saves valuable IT time by exporting policies in human readable format. The flat, readable XML file format enables auditors to view the policies off site. Auditors working remotely can view, select, review, and test policies without requiring time and support from the web application security administrator.

Comprehensive Attack Protection

Keeping up to date on the large amount of security attacks and protection measures can be a challenge for administrators and security teams. Information overload and increasingly sophisticated attacks add to the difficulty. BIG-IP ASM delivers comprehensive and cost-effective protection for web applications while improving manageability for administrators.

Advanced enforcement

BIG-IP ASM can secure any parameter from client-side manipulation and validate log-on parameters and application flow to prevent forceful browsing and logical flaws.

HTTP parameter pollution (HPP) attacks are illegal requests with the URL separated with illegal parameters to bypass application security. BIG-IP ASM recognizes these attacks and blocks these requests, providing granular attack protection.

BIG-IP ASM also protects against layer 7 DoS, SQL injection, cross-site scripting (XSS), brute force, and zero-day web application attacks. In addition, BIG-IP ASM protects against OWASP Top Ten² application security risks. For example, Cross Site Request Forgery, an

2 To read the OWASP Top Ten for BIG-IP ASM, contact your F5 representative.

According to the [September 2009 SANS Report](#), 60 percent of all attacks occur on web applications and more than 80 percent of vulnerabilities are in web applications—mostly SQL injection and XSS.

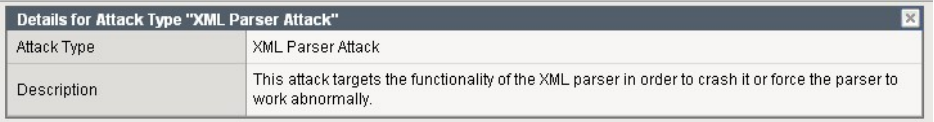
The attack expert system provides detailed descriptions of detected attacks.

OWASP Top Five attack, forces a victim's browser to send a stealth valid request to a trusted website in which the victim has a valid session. Attackers execute fraudulent transactions, such as fund transfers, and it is hard for victims to prove they did not execute the request. BIG-IP ASM mitigates those attacks and protects applications with easy checkbox enablement.

Attack expert system

As threats grow in number and complexity, the integrated and comprehensive attack expert system provides an immediate, detailed description of the attack, as well as enhanced visibility into the mitigation techniques used by BIG-IP ASM to detect and prevent the attack.

The attack expert system bridges the gap between the network and the application team, educating the administrator on application security.



Details for Attack Type "XML Parser Attack"	
Attack Type	XML Parser Attack
Description	This attack targets the functionality of the XML parser in order to crash it or force the parser to work abnormally.

Web scraping prevention

BIG-IP ASM helps you protect your brand by shielding your websites from web scraping attacks that copy and reuse valuable intellectual property and information. By differentiating between a human and a bot behind a browser, BIG-IP ASM protects against automated requests to obtain data. Policies for web applications can recognize an increase in request volumes and alert BIG-IP ASM to review whether requests are desired. Known IP addresses previously found to web scrape can be blacklisted for detection and blocking.

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.

DataGuard and cloaking

BIG-IP ASM prevents the leakage of sensitive data (such as credit card numbers, Social Security numbers, and more) by stripping out the data and masking the information. In addition, BIG-IP ASM hides error pages and application error information, preventing hackers from discovering the underlying architecture and launching a targeted attack.

Live update for attack 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.

Antivirus security protocol support

The most widely used security protocol for sending and receiving uploaded files for antivirus scanning is Internet Content Adaptation Protocol (ICAP). BIG-IP ASM strips an uploaded file from the HTTP request and forwards it to an antivirus server over ICAP. If the file is clean, the antivirus server responds to accept the request. If the file is not clean, BIG-IP ASM blocks the request to protect the network from virus intrusion.

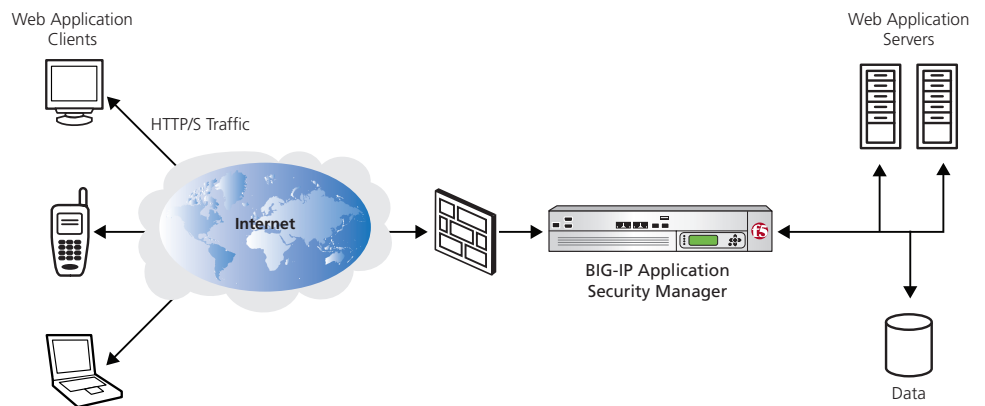
SMTP and FTP security

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 greylisting 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.

Easy web services security

BIG-IP ASM offloads web services encryption and decryption as well as digital signature signing and validation. You can easily manage and configure these functions from one location directly on the BIG-IP system, including the ability to encrypt or decrypt SOAP messages and verify signatures without the need to change application coding.

BIG-IP ASM provides comprehensive web application protection.



Policy Control

Websites are diverse, complex, and constantly changing, requiring policies with hundreds if not thousands of clear and precise rules. BIG-IP ASM helps security teams manage these changes while maintaining the delicate balance between ensuring the strictest security controls possible and allowing legitimate user access.

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 Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials, and Microsoft SharePoint. In addition,

BIG-IP ASM provides pre-built, validated application security policies requiring no configuration and giving out-of-the-box protection for mission-critical applications.

BIG-IP ASM includes a rapid deployment policy that immediately 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.

<input type="checkbox"/>	Name	Active Security Policy	Enforcement Mode	Logging Profile	State
<input type="checkbox"/>	OWA	OWA_default	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	Oracle_111	Oracle_111	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	PeopleSoft_Portal	PeopleSoft_Portal_default	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	SharePoint	SharePoint_Template	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	www.mycompany.com	www.mycompany.com_default	Blocking	Log all requests	VS1 Enabled

Staging

Staging functionality enables updated policies to be transparent for testing in a live environment without reducing current protection levels. BIG-IP ASM makes it easy to stage policies using attack signatures, file types, URLs, and other parameters, and to test whether changes are needed before a policy is enforced. The policy can be redesigned and retested until you are satisfied and the policy is ready for live implementation.

iRules integration

You can design custom iRules® to be triggered to respond to BIG-IP ASM events. For example, a policy for a blocking page can be used to protect multiple websites using an iRule that displays a customized blocking page for a specific web domain when a web scraping bot is detected. Many BIG-IP ASM events can be customized to your unique environment.

Real-time traffic policy builder

At the heart of BIG-IP ASM is the dynamic policy builder engine, which is responsible for automatic self-learning and creation of security policies. It automatically builds and manages security policies around newly discovered vulnerabilities, deploying fast, agile business processes without manual intervention.

When traffic flows through BIG-IP ASM, the policy builder parses 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.

Integration for Agility and Adaptability

The ability to respond to frequent changes in attack methods and your IT environment is a key component of web application security. By integrating with third-party products, BIG-IP ASM provides a dynamic and adaptable security solution. BIG-IP ASM integrates with WhiteHat, Splunk, and Oracle products for vulnerability assessment, auditing, and real-time database reporting to provide security breach reviews, attack prevention, and compliance.

In addition to integrating with third-party products, BIG-IP ASM works together with other F5 products to provide even greater benefits, such as web application acceleration and access control.

Vulnerability assessment with WhiteHat Sentinel

Integration with WhiteHat Sentinel 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 scan a web application and create BIG-IP ASM rules that specifically address the vulnerabilities discovered in the application. The result is a validated and actionable vulnerability assessment with a near-instantaneous mitigation response, protecting the application while development corrects the vulnerable code.

Centralized reporting with Splunk

Splunk, a large-scale, high-speed indexing and search solution, provides 15 different BIG-IP ASM-specific reports. These reports provide visibility into attack and traffic trends, long-term data aggregation for forensics, acceleration of incident response, and identification of unanticipated threats before exposure occurs.

Database reporting and security with Oracle

The integration between Oracle Database Firewall and BIG-IP ASM is the leading solution for web application and database security. This unique solution shares common reporting for web-based attempts to gain access to sensitive data, subvert the database, or execute DoS attacks against the database. Malicious users can be isolated while reports and alerts provide immediate detection and information on the type and threat of such attacks.

Acceleration and application security

With BIG-IP ASM and BIG-IP® WebAccelerator™ running together on BIG-IP® Local Traffic Manager™ you can secure applications while also accelerating performance. This efficient, multi-solution platform adds security without sacrificing performance. Attacks are filtered immediately and web applications are accelerated for improved user experience. Since there is no need to introduce a new appliance to the network, you get an all-in-one solution for maximum cost effectiveness.

Granular access control and application security

BIG-IP® Access Policy Manager™ (APM) and BIG-IP ASM bring access control and application security services layered together on your BIG-IP system. With BIG-IP APM, you can provide context-aware, policy-based access to users while simplifying authentication, authorization, and accounting (AAA) management for web applications.

The BIG-IP ASM Architecture

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 to help 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 Gateway™
- IP/port filtering
- VLAN support through a built-in switch
- Resource provisioning
- Route domains (virtualization)
- Remote authentication
- Security
 - Display customized legal notices and security login banners
 - Enforce admin session timeouts
 - Securely log out of the BIG-IP system
 - Comply with enhanced auditing and logging requirements
 - Completely isolate and secure SSL certificates from being read or modified

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

- Layer 7 DoS and DDoS
- Brute force
- Cross-site scripting (XSS)
- Cross Site Request Forgery
- SQL injection
- Parameter and HPP tampering
- Sensitive information leakage
- Session hijacking
- Buffer overflows
- Cookie manipulation
- Various encoding attacks
- Broken access control
- Forceful browsing
- Hidden fields manipulation
- Request smuggling
- XML bombs/DoS

Additional network and application security services include:

- PCI compliance reports
- Human readable policies (remote audit)
- Attack expert system
- Staging
- Reporting
- Web scraping prevention
- IP penalty enforcement
- iRules and Fast Cache™ integrations
- Report scheduling
- 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
- Web services encryption/decryption and digital signature verification
- VLAN segmentation
- DoS protection
- Client-side certificates support
- Client authentication via LDAP/RADIUS
- BIG-IP modules layering access control and web acceleration
- Dedicated management port
- Monitoring of URIs
- ICAP support
- Centralized advanced reporting with Splunk
- Database security with Oracle Database Firewall

Pre-built application security policies include:

- Lotus Domino 6.5
- OWA Exchange 2003
- OWA Exchange 2007 Oracle 10g Portal
- Oracle Application 11i
- PeopleSoft Portal 9
- Rapid Deployment security policy
- SAP NetWeaver 7
- SharePoint 2003
- SharePoint 2007
- ActiveSync v1.0, v2.0
- WhiteHat Sentinel Baseline

BIG-IP ASM Platforms

BIG-IP ASM is available as a standalone solution or as an add-on module for BIG-IP Local Traffic Manager on the 11050, 8950, 8900, 6900, 3900, and 3600 platforms, and as an add-on module for VIPRION®. For detailed physical specifications, please refer to the BIG-IP® System Hardware Datasheet.



11050 Series



8900 Series



6900 Series



3900 Series



3600 Series

F5 Services

F5 is dedicated to helping you get the most from your F5 products. To find out how F5 Services can help you improve your ROI, reduce administrative time and expense, and optimize the performance and reliability of your IT infrastructure, contact consulting@f5.com.

More Information

To learn more about BIG-IP ASM, use the search function on F5.com to find these and other resources.

Product overview

[BIG-IP Application Security Manager](#)

White paper

[Manageable Application Security](#)

Case study

[Human Kinetics Boosts Website Performance, Security, and Innovation](#)

Article

[SC Magazine, 2010 Reader Trust Award for Best Web Application Security](#)

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

