BIG-IP Application Security Manager

DATASHEET

What's Inside

Defend Against Web Attacks and Achieve Regulatory Compliance

With the continued growth of web application traffic, an increasing amount of sensitive data is exposed to potential theft, security vulnerabilities, and multi-layer attacks. Protect your organization and its reputation by maintaining the confidentiality, availability, and performance of the applications that are critical to your business.

F5® BIG-IP® Application Security Manager™ (ASM) is a web application firewall (WAF), deployed in more data centers than any enterprise WAF on the market. With advanced firewall capabilities, it secures applications against layer 7 distributed-denial-of-service (DDoS) attacks, malicious bot traffic, and application vulnerabilities where other WAFs fail. Built on F5's industry-leading Application Delivery Controller with the F5 TMOS® operating system, BIG-IP ASM delivers flexible and comprehensive protections wherever apps reside and without compromising performance—all on a platform that consolidates application protection and access management.

BIG-IP ASM is uniquely offered as an appliance, virtual edition, and as a managed service, providing automated WAF services that meet complex deployment and management requirements while protecting your apps with great precision. It is the most effective solution for guarding modern web applications and data from existing and emerging threats, and maintaining compliance with key regulatory mandates.

Key benefits

Ensure application security and compliance

Gain comprehensive security against sophisticated layer 7 attacks, blocking threats that evade traditional WAFs and enabling compliance with key regulatory mandates.

Turn on protection immediately

Simplify security with pre-built policies, thousands of out-of-the-box signatures, and a streamlined approach to policy management that decreases operational expenses.

Patch vulnerabilities fast

Identify and resolve app vulnerabilities in minutes with leading DAST integration and automatic virtual patching.

Deploy flexibly

Deploy as an appliance, in virtual or cloud environments, and as a managed service supporting multi-tenant services while incorporating external intelligence that secures against known IP threats.

Defend with proven advanced protections

Defend with highly programmable technology that dynamically adapts policies, proactively stops bots and DDoS, and demonstrates 99.89 percent overall security effectiveness.

Magnify threat knowledge

Easily understand your security status with detailed forensic analysis, full visibility into HTTP and WebSocket traffic, and rich insight into all events and user types.

Ensure Comprehensive Threat Protection

The volume and sophistication of attacks makes keeping up-to-date on security threat types and protection measures a challenge for application administrators and security teams. With industry-leading capabilities, predefined signatures, and superior flexibility, BIG-IP ASM delivers advanced, cost-effective security for the latest interactive Web 2.0 applications.

BIG-IP ASM secures any parameter from client-side manipulation and validates login parameters and application flow to prevent forceful browsing and logical flaws. It also allows organizations to effectively guard against existing and emerging Layer 7 application attacks—preventing costly data breaches, thwarting DDoS attacks, and maintaining compliance. BIG-IP ASM is the first leading WAF that supports the transition from AJAX/HTTP to WebSockets for greater efficiencies and less overhead with bi-directional streaming data. BIG-IP ASM uniquely provides visibility into WebSocket traffic—enabling companies to transition to protecting chat sessions and streaming information feeds (such as stock tickers) from data exposure, tampering, and theft. Users benefit from an extensive database of signatures, dynamic signature updates, DAST integration, and the flexibility of F5 IRules® scripting for customization and extensibility.

Organizations rely on BIG-IP ASM to protect the world's most visited web applications wherever they reside, with the highest level of security and without compromising performance. BIG-IP ASM enables organizations to detect and mitigate layer 7 threats including web scraping, web injection, brute force, CSRF, JSON web threats, DoS-heavy URLs, and zero-day attacks—providing early warnings, while mitigating threats per policy. It automatically defends against multiple, simultaneous, volumetric application-layer threats including stealthy, low-bandwidth DDoS attacks. BIG-IP ASM also prevents execution of fraudulent transactions, stops in-browser session hijacking, and reports regular and repeated attacks from IPs.

Using automatic learning capabilities, dynamic profiling, unique anomaly detection methods, and risk-based policies, BIG-IP ASM can impose needed protections to prevent even the most sophisticated attacks from ever reaching servers. When combined with BIG-IP® Application Acceleration Manager™ (AAM) and BIG-IP® Local Traffic Manager™ (LTM), BIG-IP ASM filters attacks and accelerates applications for an improved user experience.

Continuous expert security research

F5's security research team helps ensure continuous development of BIG-IP ASM signatures, policies, and capabilities. Researchers explore forums and third-party resources, investigate attacks, reverse engineer malware, and analyze vulnerabilities to determine effective detection and mitigation methods that guard against zero-day threats, DDoS attacks, and other evasive or evolving threats. BIG-IP ASM offers enhanced protection from advancements in technology, regular signature updates, threat intelligence, and tightening of existing capabilities.

Defend with proactive bot protections

An always-on defense is required to successfully identify and protect against automated layer DDoS attacks, web scraping, and brute force attacks before they occur. F5 delivers proactive bot defense capabilities that effectively provide controls to help prevent these attacks from ever taking place. Using advanced defense methods and reputation matching to identify non-human users (such as JS and CAPTCHA challenges, geolocation enforcement, and other techniques), BIG-IP ASM slows requests to distinguish bots and then drops those requests before they reach a server. BIG-IP ASM thoroughly inspects user interaction, analyzes the health of the server, and discerns transaction anomalies to help detect bots that may bypass client/application challenges, established rate limits, and other standard detection methods. It also automatically mitigates layer 7 attacks that show an unusual change in request patterns. Unique from other solutions, BIG-IP ASM provides security experts with greater control of bot defense enforcements, allowing them to force additional action (such as high-speed logging on block or challenge actions, JS challenges, URI overrides, customized HTML redirects, and more) before mitigations are applied. The BIG-IP ASM bot defense capabilities provide the most effective prevention methods, allowing you to identify suspicious automated activity, categorize bots detected, and mitigate attacks with the highest level of precision.

Track malicious user attempts

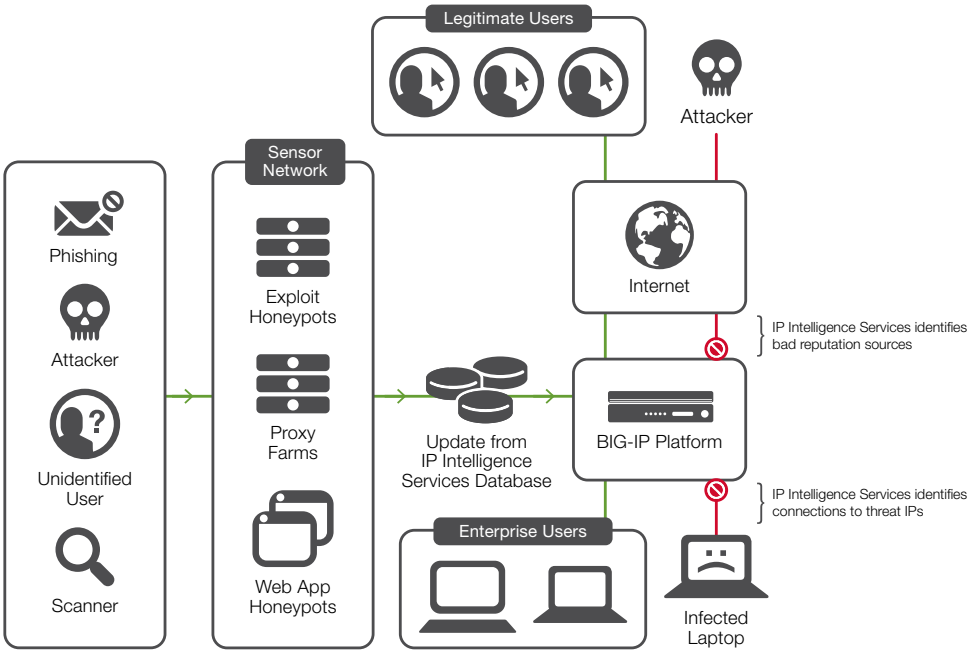
Distinguishing permitted users from bad actors whenever a website is visited helps minimize security risk and prevent malicious activity. With BIG-IP ASM, application security teams can employ device identification tracking techniques to identify specific end-users, application sessions, and attackers. This unique capability allows IT to easily distinguish human traffic from bot traffic, spot repeat visitors, prevent malicious attempts, and help WAFs more accurately mitigate brute force, session hijacking, web scraping, and DDoS attacks.

Device identification tracking enables BIG-IP ASM to identify the same browser, even when users switch sessions or source IPs. When activated, BIG-IP ASM captures and saves unique device characteristics and attributes, determines which clients are suspicious, and mitigates threats based on predefined settings. Whether an automated threat, denial-of-service attack, headless browser, or human user, BIG-IP ASM can distinguish between repeat attackers and customer visitors for every WAF use case.

Block malicious IP addresses

Delivering today's rich and complex Internet content to users can expose an organization to a variety of potentially malicious attacks from rapidly changing IP addresses. Inbound and outbound botnet traffic, such as DDoS and malware activity, can penetrate the organization's security layers. F5 IP Intelligence Services enhances automated security decisions with IP reputation intelligence. By identifying IP addresses and security categories associated with malicious activity, IP Intelligence Services can incorporate dynamic lists of threatening IP addresses from third parties into the BIG-IP® platform, adding context and automation to BIG-IP ASM blocking decisions. This adds granularity to BIG-IP ASM rules—allowing administrators to set an alarm, stop traffic, or fully block IPs based upon a specific IP reputation category while whitelisting approved IP addresses.

Additionally, BIG-IP ASM alleviates computational heavy mitigation of threats from known malicious IP addresses with a unique IP shun capability (accelerated blacklisting). Instead of wasting cycles on traffic from badly behaving IPs, BIG-IP ASM immediately blacklists IPs that repeatedly fail challenges or undergo high block ratios. This temporarily blocks malicious IPs in hardware at the network layer until IP intelligence feeds are up to date.



IP Intelligence Services gathers reputation data for use by F5 solutions.

Enabling secure SSL

As the increasing demand for data protection drives SSL growth, it is important to guard against SSL attacks that threaten the security of applications and information in transit. BIG-IP ASM protects against malicious attempts to overcome SSL and compromise private keys, user passwords, and other sensitive information. It provides full SSL termination, and decrypts and re-encrypts terminated traffic—allowing complete inspection and mitigation of concealed, malicious threats. When BIG-IP ASM is combined with BIG-IP LTM, organizations also gain comprehensive SSL DDoS mitigation and SSL offload protection to secure against SSL attacks including SSL floods, POODLE, Heartbleed, and various memory-cracking tools.

Identify anomalous behavior

With BIG-IP ASM, IT can easily detect traffic that does not conform with normal behavior and evades usual volumetric protections—such as an uncommon increase or decrease in latency or the transactions rate. BIG-IP ASM can identify and uniquely block excessive failures to authenticate IP addresses generating a high volume of login attempts, as well as other anomalies in the typical traffic pattern. These include sessions opened at high rates or requesting too much traffic.

Patch vulnerabilities immediately

BIG-IP ASM integrates with leading web application vulnerability scanners to allow you to easily manage assessments, discover vulnerabilities, and apply specific policies from a single location. These unique capabilities facilitate near-instantaneous mitigation of application assessment results, ensuring protection while developers correct vulnerable code—patching in minutes instead of weeks or months.

With BIG-IP ASM, administrators can import testing results from DAST scanners, including scanners from WhiteHat, IBM, and QualysGuard, and layer a vulnerability-driven policy (received from F5 scanner integrations) on top of a current rapid deployment or SharePoint policy. When combined with WhiteHat Sentinel, BIG-IP ASM also detects and reports recent website changes to the scanner. This ensures scanning of otherwise overlooked URLs and parameters, and the application of specific policies—enabling organizations to secure their applications immediately after updating.

BIG-IP ASM DAST support helps IT deliver next-generation website security using simple, accurate, automated services. These services protect assets in a dynamic threat environment with more comprehensive assessments, zero false positives, and more manual and automated virtual patches than any other WAF solution.

Enforce geolocation-based blocking

Attacks are increasing from a variety of global sources. BIG-IP ASM enables you to block these attacks based on geolocation: states, countries, or regions. Your administrators can easily select allowed or disallowed geolocations for strong policy enforcement and attack protection. Geolocation-based blocking also protects against anomalous traffic patterns from specific countries or regions, and enables traffic throttling based on location. BIG-IP ASM geolocation-based protection can be applied to a CAPTCHA challenge and to protect RAM cache and other resources from DDoS attacks.

Inspect SMTP and FTP

BIG-IP ASM enables SMTP and FTP security checks to protect against spam, viral attacks, directory harvesting, and fraud. Using default settings, administrators can easily configure security profiles to inspect FTP and SMTP traffic for network vulnerabilities and protocol compliance. Default settings can also be used to trigger alarms or block requests for violations.

SMTP security checks enable validation of incoming mail using several criteria, while disallowing or allowing common call methods used to attack mail servers. Additionally, administrators can set rate limits on the number of incoming messages, create gray and black lists, and validate DNS SPF records. FTP violations can be triggered for anonymous, passive, or active requests; specific FTP commands; command line length; and excessive login attempts. Administrators can use default SMTP/FTP settings for easy setup or customize profiles to address specific risks and more effectively ensure protocol compliance.

Protect commonly used APIs

As Web 2.0 applications expand from connected to collaborative via the extensive use of APIs, BIG-IP ASM ensures that API methods are enforced on URLs. It also secures applications against API attacks that commonly go undetected by traditional firewalls. With a unique defense mechanism that guards XML, JSON, and GTW APIs, BIG-IP ASM automatically detects application program interface threats, enforces strict policy rules for each use case, and blocks attacks and special content types—closing the back door on application threats.

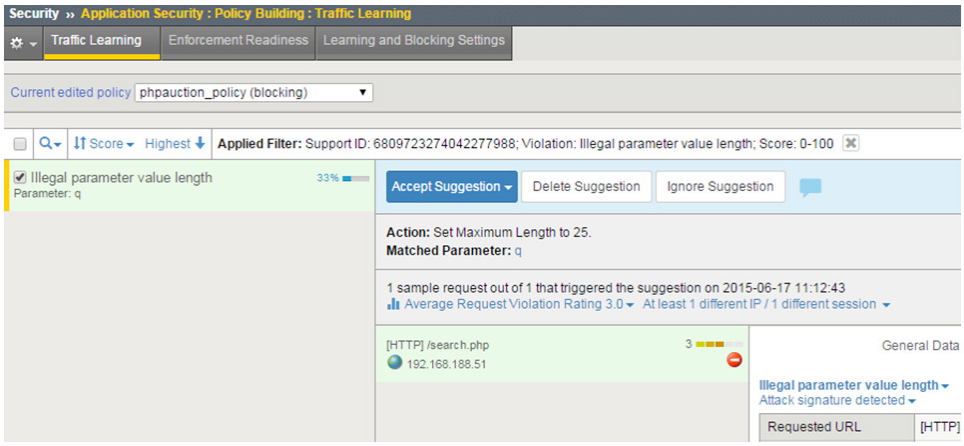
Streamline Learning, Deployment, and Management

Organizations want to turn on protections immediately without extensive security expertise. BIG-IP ASM simplifies and automates configuration and policy deployment with pre-built 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. The validated policies also serve as a starting point for more advanced policy creation. This allows even novice users to rapidly deploy policies and immediately secure applications with little-to-zero configuration time needed.

Unified learning and dynamic policy building

At the heart of BIG-IP ASM is the unified learning and dynamic policy builder engine, which automates policy creation and tuning for increased operational efficiency and scalability. The policy builder engine automatically builds security policies around security violations, advanced statistics, and heuristics over time. It also understands expected behavior to affect more accurate traffic filtering.

By examining hundreds or thousands of requests and responses, the policy builder engine populates the security policy with legitimate elements more precisely than most WAFs. Dynamically generated policies are initially put into staging and then automatically moved from staging and enforced as they meet the rule thresholds for stabilization. The policy builder engine supports automatic policy adaptation and learning following the occurrence of violations or as new parameters are observed. Policy maintenance is simplified by a GUI with a single-page view of all learning suggestions. One-click actions allow you to browse, search, accept, and ignore potential suggestions for policy adjustments, hardening policies with ease.



The enhanced learning GUI offers a single-page view of all learning suggestions.

Centralized management and monitoring

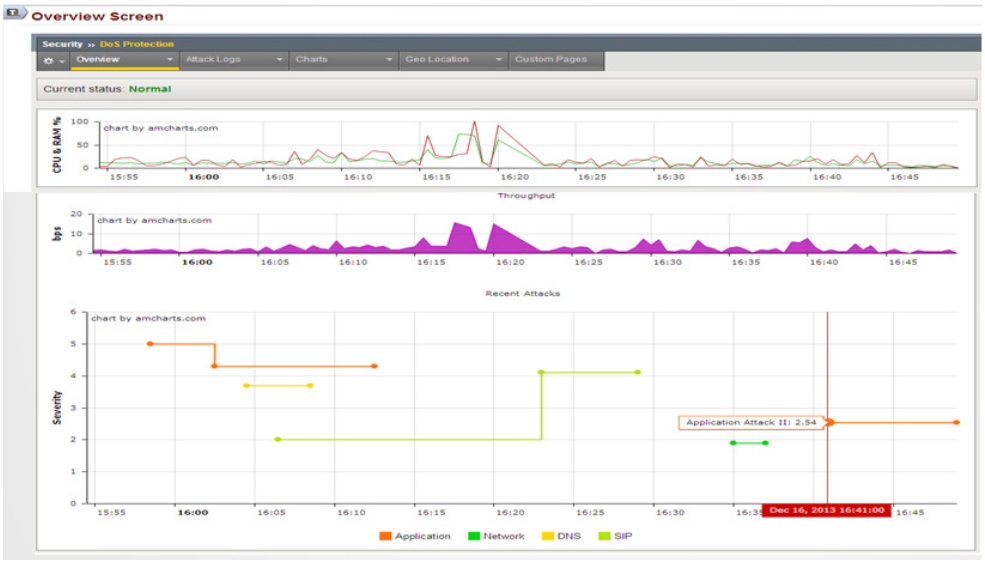
When you are deploying multiple BIG-IP ASM devices, F5 BIG-IQ® Centralized Management centralizes administration across your entire F5 infrastructure. Administrators get a consolidated view of all BIG-IP devices, which helps to manage better relationships between devices, reduce IT overhead, and minimize configuration errors.

BIG-IP ASM provides an open API that supports easy integration to cloud/aaS virtual platforms and third-party policy management solutions. Engineers can fully configure and manage BIG-IP ASM policies from a programmatic interface that supports all policy management tasks, including login configuration, learning, semi-automatic tuning, utilization queries, and health monitoring. The BIG-IP ASM REST API exposes the entire range of BIG-IP ASM policy entities to support open models of WAF as a service.

Leverage Rich, Actionable Reporting

BIG-IP ASM provides powerful reporting capabilities that allow you to easily analyze incoming requests, track trends in violations, generate security reports, evaluate possible attacks, and make informed security decisions. Whether you're a security expert or a generalist, BIG-IP ASM provides clear, discernable information with comprehensive visibility into attacks and changes in the threat landscape.

The BIG-IP ASM overview screen displays active security policies, security events and attacks, anomaly statistics, and networking and traffic statistics. You can save the information or send it as an email attachment. Monitoring capabilities show how the application is being accessed and how it is behaving. The unique REST API supports easy integrations with higher-level SIEM or management services. BIG-IP ASM also offers predefined and customizable dashboards, charts, reports, and stats—highlighting DDoS and brute force attacks, web scraping and IP enforcement, session tracking status, and more.



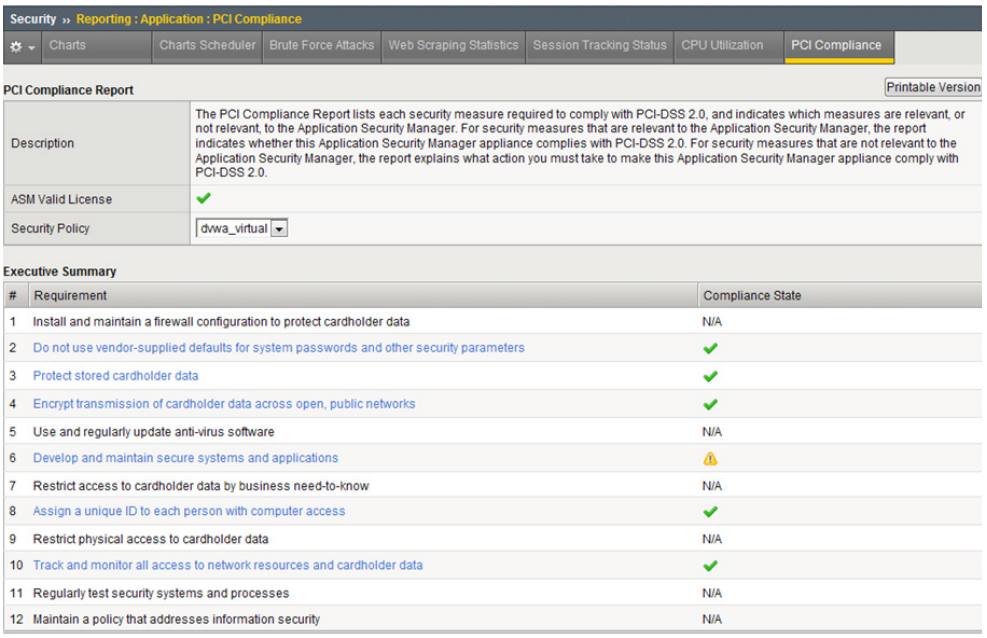
The security overview screen provides an easy view of what is happening on your system.

In-depth forensic analysis and database security

For deeper threat analysis, BIG-IP ASM integrates with high-speed indexing and search solutions like SPLUNK. These solutions offer deeper visibility into attack and traffic trends, long-term data aggregation, and identification of unanticipated threats before exposure occurs. BIG-IP ASM also supports database reporting for a real-time view into database activity and SQL statements generated by front-end users. Indexing and search solutions combine with BIG-IP ASM to provide richer forensic information for increased security effectiveness when mitigating threats.

Maintain compliance with industry and regulatory mandates

BIG-IP ASM makes it easy for organizations to understand and maintain regulatory compliance. Built-in security protection, logging and reporting, and remote auditing help organizations comply with industry security standards (including PCI DSS, HIPAA, BASEL II, FFIEC, SOX)—cost-effectively and without multiple appliances, application changes, or rewrites. With PCI reporting, BIG-IP ASM lists security measures required, determines if compliance is being met, and details necessary steps to becoming compliant.



Maintain compliance with industry and regulatory mandates.

Meet Complex Deployment Requirements

The explosion of the Internet of Things (IoT) has caused a tremendous impact on organizations. The number of web-facing applications that must be managed and secured has jumped dramatically from hundreds to thousands. In addition, the increasing focus toward hybrid application deployment means that business apps now reside in multiple settings—data center, private cloud, and public cloud. As a result of these changes, new requirements are necessary for securing apps and transitioning WAF services from the data center to the cloud.

Hybrid WAF deployment models

BIG-IP ASM offers flexible options that allow administrators to easily deploy firewall services close to the application. Administrators can also transition hardened security policies from data center appliances to BIG-IP ASM Virtual Edition (VE) in virtual and private cloud environments. BIG-IP ASM offers the same quality of protection and scalability with an appliance and software edition. Policies and iRules can seamlessly move between hardware devices and virtual appliances without manual updates.

F5's WAF technology supports application security in any environment, whether deployed on F5 hardware, as a virtual edition, or as a wholly managed cloud-based service.

The managed cloud-based service, F5 Silverline™ Web Application Firewall (WAF), is built on BIG-IP ASM, but provided via F5's Silverline cloud-based application services platform and wholly deployed, set up, and managed by the highly specialized experts in the F5 Security Operations Center (SOC). With 24x7x365 expert support to protect web applications and data (and enable compliance with industry security standards), the Silverline Web Application Firewall service provides application protection without the need for capital investment and security expertise.

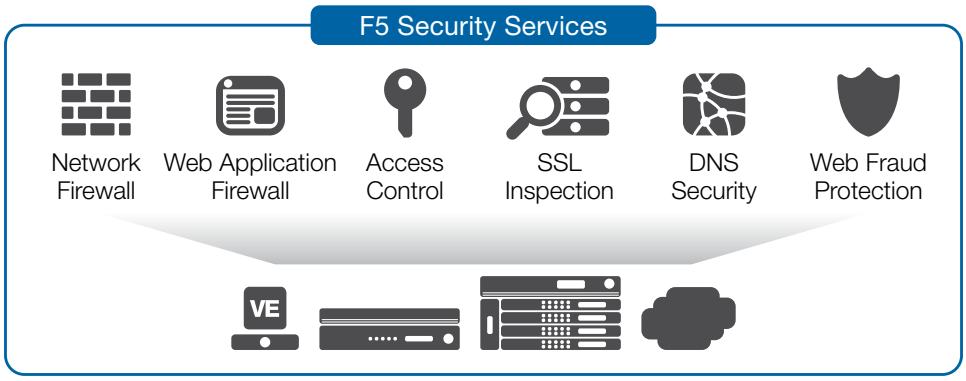
Running multiple instances of BIG-IP ASM

BIG-IP ASM uses F5 ScaleN® with Virtual Clustered Multiprocessing™ (vCMP) to provide the most cost-effective application security implementation for managing large-scale deployments—whether you are a managed service provider offering WAFs as a service or simply managing a large number of BIG-IP ASM devices.

With BIG-IP ASM and vCMP-enabled systems, administrators can easily consolidate multiple firewalls onto a single device and allocate BIG-IP ASM resources in a more flexible and isolated manner for different customers, groups, applications, and services. vCMP enables you to run multiple instances of BIG-IP ASM on a single BIG-IP platform with high-density firewall isolation through a combination of hardware and software. Guest firewalls can be clustered for easier administration and maintenance, and to ensure consistency throughout the firewall infrastructure. vCMP allows you to consolidate and better manage your security infrastructure, ensuring efficiencies and meeting service-level agreements (SLAs) with a dynamic, flexible WAF service infrastructure.

F5 Security Services

IT managers need a consolidated network and web application firewall solution to defend against multi-layered attacks, such as network and layer 7 events. BIG-IP ASM, together with F5 Web Fraud Protection, BIG-IP AFM, and BIG-IP® DNS, covers the threat spectrum—mitigating L3–L7 attacks, providing client-side fraud protection, and safeguarding the DNS infrastructure. When used with BIG-IP® Access Policy Manager® (APM), BIG-IP ASM provides context-aware, policy-based access with simplified authentication, authorization, and accounting (AAA) management for web applications. As a component of F5's comprehensive security services, BIG-IP ASM benefits from other BIG-IP modules to enable data center security, extensive application protection, and access management capabilities.



BIG-IP ASM, together with other BIG-IP modules, consolidates application protection and access management onto a single high-performing security platform.

BIG-IP ASM Features and Specifications

Web Application Firewall

Deployment

Rapid deployment wizard with self-help hints	Yes
Unified learning and policy builder	Yes—with manual and automated policy building
Policy staging	
Route domain support	Yes
VE, appliance, or managed service	Yes—managed services requires Silverline license

WAF Security

L7 DoS and DDoS detection including: HASH DoS, Slowloris, floods, Keep dead, XML bomb	Yes
Web scraping prevention	Yes
OWASP Top 10 prevention	Yes
Automated attack defense and bot detection	Yes
Advanced protections against threats including: Web injections, data leakage, session hijacking, HPP attacks, buffer overflows, shellshock	Yes
Geolocation blocking	Yes
IP intelligence reputation services	Yes—with F5 IP Intelligence Services
SSL termination with re-encryption	Yes
Security incident and violation correlation	Yes
Client-side certification support	Yes
Client authentication	LDAP, RADIUS
Database security	Yes—with Oracle Database firewall
Response checking	Yes
Violation risk scoring	Yes
Web service encryption and decryption	Yes—and with signature validation
Device-ID detection and finger printing	Yes
Live signature updates	Yes
WebSocket traffic filtering	Yes
IP shunning (layer 3 blacklisting in HW)	Requires BIG-IP AFM license

Reporting and Analytics

Customizable charts and reports	Yes
Security overview report	Yes—drill down capabilities to granular details
Combined network and application attack report	Yes—with combined BIG-IP AFM and BIG-IP ASM deployment
WAF health monitoring	Yes
Compliance support	PCI-DSS, HIPAA, SOX, Basel II
Central management and reporting with role-based access control	Yes—requires BIG-IQ Centralized Management
Automatic policy sync between WAF devices	Yes

Other

iRules and fast cache integration	Yes
SNMP reporting	Yes
REST API	Yes
ICAP support	Yes
DAST integration	Yes—WhiteHat, QualysGuard, and IBM
Fraud protection	Yes—Requires F5 WebSafe™ license
SSL acceleration	

BIG-IP Platform and TMOS support

Multi-tenancy	Yes—with vCMP
High availability	Yes—active-passive or active-active
64 bit OS support	Yes
Application acceleration	Yes—requires BIG-IP AAM
TCP optimization	Yes
Advanced rate shaping and QoS	Yes
F5 IPv6 Gateway™	Yes
IP port filtering	Yes
VLAN support	Yes
Secure SSL certificates from access	Yes
Integrates with BIG-IP AFM and BIG-IP APM for complete data center security with identity and access management.	Yes

BIG IP Application Security Manager

BIG-IP ASM is available as a standalone solution or as an add-on module for BIG-IP LTM on any BIG-IP platform, and on BIG-IP LTM Virtual Edition (VE). BIG-IP Access Policy Manager (APM) is available as an add-on module to the BIG-IP ASM standalone appliance. BIG-IP APM Lite (with 10 free user licenses) is included with any BIG-IP ASM standalone purchase. For detailed physical specifications, please refer to the BIG-IP System Hardware Datasheet.

BIG-IP Platforms

Only F5's next-generation, cloud-ready ADC platform provides DevOps-like agility with the scale, security depth, and investment protection needed for both established and emerging apps. The new BIG-IP® iSeries appliances deliver quick and easy programmability, ecosystem-friendly orchestration, and record-breaking, software-defined hardware performance. As a result, customers can accelerate private clouds and secure critical data at scale while lowering TCO and future-proofing their application infrastructures. F5 solutions can be rapidly deployed via integrations with open source configuration management tools and orchestration systems.

In addition to the iSeries, F5 offers VIPRION modular chassis and blade systems designed specifically for performance and for true on-demand linear scalability without business disruption. VIPRION systems leverage F5's ScaleN clustering technology so you can add blades without reconfiguring or rebooting.

Virtual editions of BIG-IP software run on commodity servers and support the range of hypervisors and performance requirements. These virtual editions provide agility, mobility, and fast deployment of app services in software-defined data centers and cloud environments.

See the BIG-IP System Hardware, VIPRION, and Virtual Edition datasheets for more details. For information about specific module support for each platform, see the latest release notes on AskF5. For the full list of supported hypervisors, refer to the VE Supported Hypervisors Matrix.

F5 platforms can be managed via a single pane of glass with BIG-IQ Centralized Management.

BIG-IP iSeries Appliance

VIPRION Chassis

BIG-IP Virtual Editions

Virtual Editions

BIG-IP LTM VE with the stand-alone BIG-IP ASM and BIG-IP ASM VE can help you meet the needs of your virtualized environment.

BIG-IP ASM VE

Hypervisors Supported:	VMware vSphere Hypervisor 4.0, 4.1, 5.0, and 5.1 and vCloud Director 1.5 Citrix XenServer 5.6 and 6.0 Microsoft Hyper-V for Windows Server 2008 R2 and 2012 KVM – Linux Kernel 2.6.32 (RHEL 6.2/6.3, CentOS 6.2/6.3)

BIG-IP ASM VE is also available as an Amazon Machine Image for use within Amazon Web Services.

amazon web services | Partner Network

F5 Global Services

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/support.

More Information

To learn more about BIG-IP ASM, visit f5.com to find these and other resources.

Datasheets

IP Intelligence

BIG-IP Application Acceleration Manager

Report

Gartner Web Application Firewall Magic Quadrant, 2014

White papers

Complying with PCI DSS

Protecting Against Application DDoS Attacks with BIG-IP ASM

Vulnerability Assessment with Application Security

Case study

Consolidating Security Solutions with F5

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

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan f5j-info@f5.com

Solutions for an application world.