F5 Advanced WAF

DATA SHEET

What's Inside

Proactive Application Protection

Applications are critical to your business. Without the right protection, however, they can become an attack vector that may ultimately lead to a data breach. Consider this alarming statistic: Organizations have an average of 765 web applications and these applications are the initial target of data breaches 53% of the time.[1]

Protect your organization and its reputation by maintaining the confidentiality, availability, and performance of the applications that are critical to your business with F5® Web Application Firewall (WAF) solutions.

F5 WAF solutions are deployed in more data centers than any enterprise WAF on the market. The comprehensive suite of F5 WAF solutions includes managed rulesets for Amazon Web Services (AWS); cloud-based, self-service, and managed service in the F5 Silverline® cloud-based service delivery platform; application delivery controller (ADC) integration with F5 BIG-IP® Application Security Manager™ (ASM)[2]; and F5 Advanced Web Application Firewall™ (Advanced WAF).

Advanced WAF redefines application security to address the most prevalent threats organizations face today:

- Automated attacks and bots that overwhelm existing security solutions.
- Web attacks that steal credentials and gain unauthorized access across user accounts.
- Application layer attacks that evade static security based on reputation and manual signatures.
- New attack surfaces and threats due to the rapid adoption of APIs.

Advanced WAF is built on proven F5 technology and goes beyond reactive security such as static signatures and reputation to proactively detect and mitigate bots, secure credentials and sensitive data, and defend against application denial-of-service (DoS).

Advanced WAF delivers flexible and comprehensive protections wherever apps reside and without compromising performance. Advanced WAF is 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 applications and data from existing and emerging threats while maintaining compliance with key regulatory mandates.

[1] 2018 Application Protection Report

[2] BIG-IP ASM continues to be offered through F5 Good/Better/Best licensing.

Key benefits

Protect web and mobile applications from malicious bots

F5 secures an organization's most valued assets, applications, and sensitive data from bots, automated attacks, web scrapers, and exploits. Advanced WAF extends bot protection to mobile applications through the F5 Anti-Bot Mobile SDK, providing rapid deployment of mobile bot protection through an easy-to-use web portal without requiring any changes to the application or mobile device. Applications fused with mobile bot protection are supported in vendor and third-party application stores.

Safeguard credentials and sensitive data from theft and abuse

Advanced WAF secures credentials and sensitive data from theft and abuse, preventing data breaches and mitigating automated attacks that leverage previously stolen credentials. F5 BIG-IP DataSafe™ application layer encryption in Advanced WAF masks sensitive fields directly within the user's web browser, rendering data stolen by bad actors through client-side attacks useless. Using BIG-IP DataSafe, customers can encrypt data at the field level transparently, without requiring any changes on clients or Web servers. Comprehensive brute force mitigation including credential stuffing protection defends against automated attacks that leverage previously stolen credentials.

Defend against sophisticated application denial-of-service (DoS)

Advanced WAF discovers and fingerprints new and unusual traffic patterns without human intervention, distinguishing and isolating potential malicious traffic from legitimate traffic. This automated mitigation capability is based on a continuous feedback loop of client behavior and server stress. If anomalous behavior is detected, Advanced WAF automatically builds a dynamic signature and begins mitigating the attack. The effectiveness of the mitigation is then monitored through the continuous feedback loop. False positives are reduced while accuracy and performance are improved through continuous mitigation tuning as the attack starts, evolves, or stops.

Mitigate sophisticated threat campaigns

Threat Campaigns provide targeted signatures to protect organizations from pervasive attacks that are often coordinated by organized crime and nation states. Based on F5 Labs research, Threat Campaigns provide critical intelligence to fingerprint and mitigate sophisticated attacks with nearly real-time updates. Metadata is used to determine both malicious requests and malicious intent, and the high accuracy of Threat Campaign signatures immediately blocks active threats with low false positives and no learning cycle.

Protect APIs

As web applications expand from connected to collaborative via the extensive use of Application Programming Interfaces (APIs), Advanced WAF 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 through rate limiting, behavioral analysis, and anti-automation, Advanced WAF 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. With F5 Access Manager™, API protection is improved through comprehensive authentication and token enforcement.

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 dynamic application security testing (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 DoS attacks, and demonstrates 99.89% 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 and superior flexibility, F5 Advanced WAF delivers advanced, cost-effective security for the latest web and mobile applications.

Advanced WAF protects credentials from theft and abuse, and secures any parameter from client-side manipulation by validating 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 DoS attacks, and maintaining compliance. Advanced WAF 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. Advanced WAF also 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 Advanced WAF to protect the world's most visited web applications wherever they reside, with the highest level of security and without compromising performance. Advanced WAF 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 application-layer threats including stealthy, low-bandwidth DoS attacks. Advanced WAF also 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, Advanced WAF can impose needed protections to prevent even the most sophisticated attacks from ever reaching servers. When combined with F5 BIG-IP Local Traffic Manager™ (LTM), Advanced WAF filters attacks and accelerates applications for an improved user experience.

Continuous expert security research

F5's security research team helps ensure continuous development of Advanced WAF 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, DoS attacks, and other evasive or evolving threats. Advanced WAF 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 DoS 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 JavaScript and CAPTCHA challenges, geolocation enforcement, and other techniques), Advanced WAF slows requests to distinguish bots and then drops those requests before they reach a server. Advanced WAF 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, Advanced WAF 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, JavaScript challenges, URI overrides, customized HTML redirects, and more) before mitigations are applied. The Advanced WAF 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. The F5 Anti-Bot Mobile SDK, in conjunction with Advanced WAF, extends F5's comprehensive bot protection to mobile applications without any changes to application code.

Track malicious user attempts

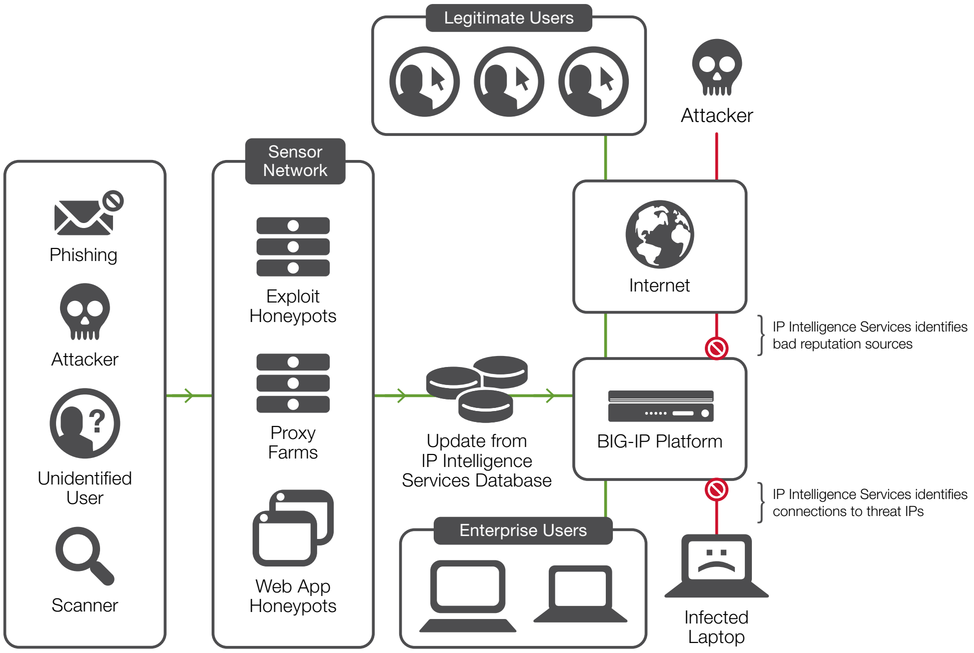
Distinguishing permitted users from bad actors whenever a website is visited helps minimize security risk and prevent malicious activity. With Advanced WAF, application security teams can employ device identification tracking techniques to identify specific end-users, application sessions, and attackers. 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 DoS attacks.

Device identification tracking enables Advanced WAF to identify the same browser, even when users switch sessions or source IPs. When activated, Advanced WAF captures and saves unique device characteristics and attributes determines which clients are suspicious, and mitigates threats based on predefined settings. Whether an automated threat, DoS attack, headless browser, or human user, Advanced WAF 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 DoS 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 F5 platform, adding context and automation to Advanced WAF blocking decisions. This adds granularity to Advanced WAF rules—allowing administrators to set an alarm, stop traffic, or fully block IPs based upon a specific IP reputation category while allowlisting approved IP addresses.

Additionally, Advanced WAF alleviates computational heavy mitigation of threats from known malicious IP addresses with a unique IP shun capability (accelerated denylisting). Instead of wasting cycles on traffic from badly behaving IPs, Advanced WAF immediately denylists 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 encryption

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

Identify anomalous behavior

With Advanced WAF, IT can easily detect traffic that does not conform to normal behavior and evades usual volumetric protections—such as an uncommon increase or decrease in latency or the transactions rate. Advanced WAF 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. Behavioral analytics and machine learning in Advanced WAF automatically monitor client and server traffic for anomalies in a continuous feedback loop.

Patch vulnerabilities immediately

Advanced WAF 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 Advanced WAF, 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, Advanced WAF 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.

Advanced WAF 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. Advanced WAF enables you to block these attacks based on geolocation: states, countries, or regions. 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. Advanced WAF 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

Advanced WAF 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 allowlists and denylists, 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.

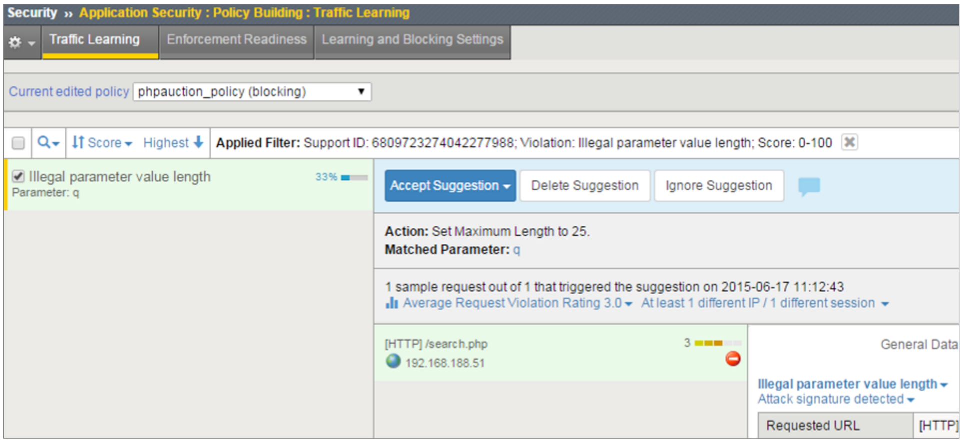
Streamline Learning, Deployment, and Management

Organizations want to turn on protections immediately without extensive security expertise. F5 Advanced WAF 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 Advanced WAF 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 other WAFs. Dynamically generated policies are initially put into staging, 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.



Current edited policy: phpauction_policy (blocking)

Applied Filter: Support ID: 6809723274042277988; Violation: Illegal parameter value length; Score: 0-100

☑ Illegal parameter value length 33%
Parameter: q

Action: Set Maximum Length to 25.
Matched Parameter: q

1 sample request out of 1 that triggered the suggestion on 2015-06-17 11:12:43
Average Request Violation Rating 3.0 At least 1 different IP / 1 different session

[HTTP] /search.php 3
192.168.188.51

Illegal parameter value length
Attack signature detected

Requested URL	[HTTP]

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

Centralized management and monitoring

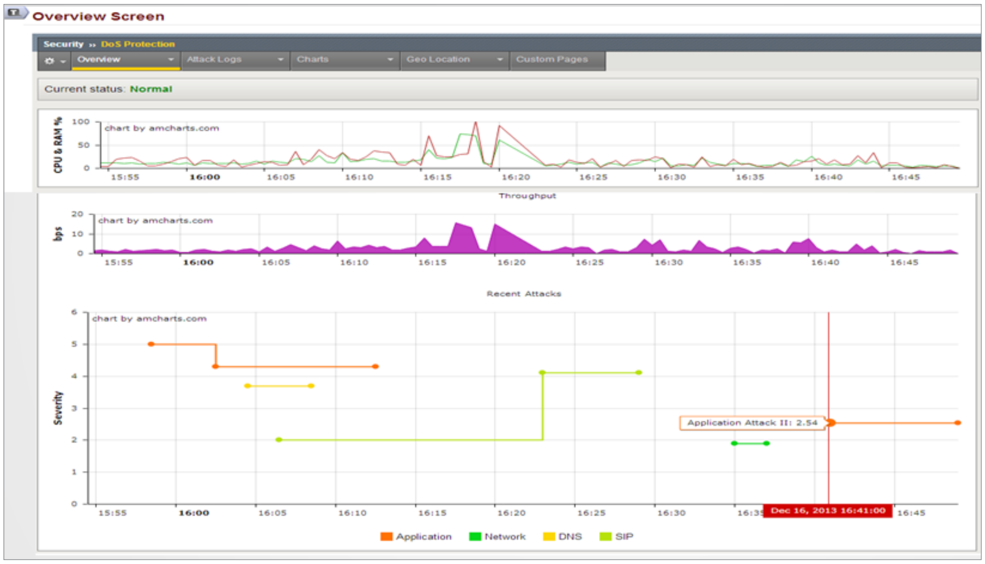
When you are deploying multiple Advanced WAF devices, F5 BIG-IQ® Centralized Management centralizes administration across your entire F5 infrastructure. Administrators get a consolidated view of all F5 devices, which helps to manage better relationships between devices, reduce IT overhead, and minimize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

Advanced WAF 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 Advanced WAF policies from a programmatic interface that supports all policy management tasks, including login configuration, learning, semi-automatic tuning, utilization queries, and health monitoring. The Advanced WAF REST API exposes the entire range of Advanced WAF policy entities to support open models of WAF as a Service.

Leverage Rich, Actionable Reporting

F5 Advanced WAF provides powerful reporting capabilities that allow you to easily analyze incoming requests, track trends in violations through event correlation, generate security reports, evaluate possible attacks, and make informed security decisions. For security experts or generalists, Advanced WAF provides clear, discernable information with comprehensive visibility into attacks and changes in the threat landscape.

The Advanced WAF overview screen displays active security policies, security events and attacks, anomaly statistics, and networking and traffic statistics. Information can be saved or sent 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. Advanced WAF also offers predefined and customizable dashboards, charts, reports, and stats—highlighting DoS and brute force attacks, web scraping and IP enforcement, session tracking status, and more.



Current status: Normal

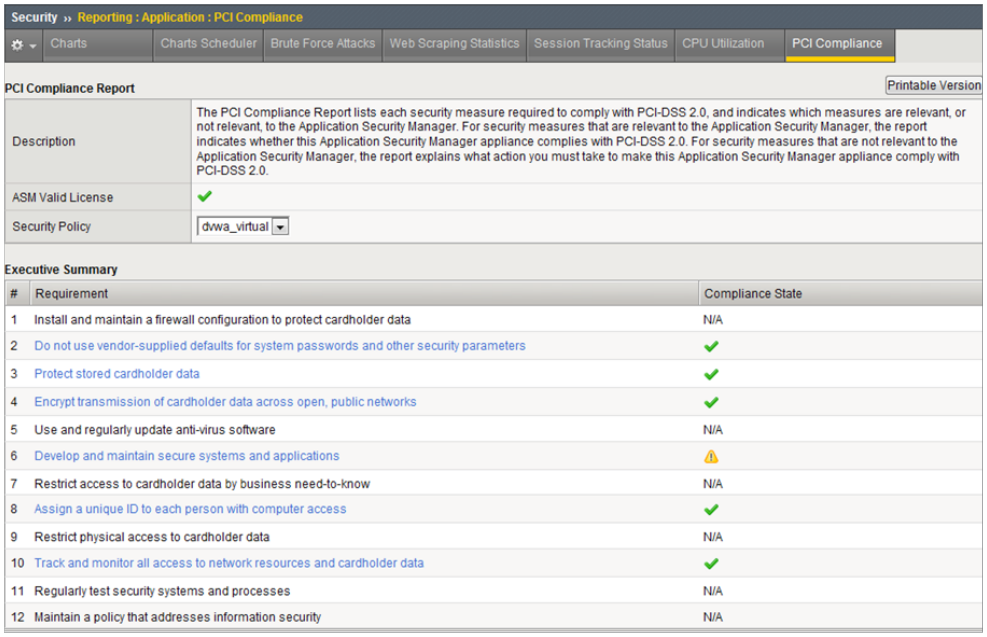
The security overview screen provides an easy view of what is happening on your system.

In-depth forensic analysis and database security

For deeper threat analysis, Advanced WAF 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. Advanced WAF 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 Advanced WAF to provide richer forensic information for increased security effectiveness when mitigating threats.

Maintain compliance with industry and regulatory mandates

Advanced WAF 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, Advanced WAF lists required security measures, determines if compliance is being met, and details necessary steps to becoming compliant.



PCI Compliance Report

Description	The PCI Compliance Report lists each security measure required to comply with PCI-DSS 2.0, and indicates which measures are relevant, or not relevant, to the Application Security Manager. For security measures that are relevant to the Application Security Manager, the report indicates whether this Application Security Manager appliance complies with PCI-DSS 2.0. For security measures that are not relevant to the Application Security Manager, the report explains what action you must take to make this Application Security Manager appliance comply with PCI-DSS 2.0.
ASM Valid License	✓
Security Policy	dvwa_virtual

Executive Summary

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

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. 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

F5 Advanced WAF 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 Advanced WAF Virtual Edition (VE) in virtual and private cloud environments. Advanced WAF 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.

F5 Silverline Web Application Firewall is built on F5 Advanced WAF, but is provided via the 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.

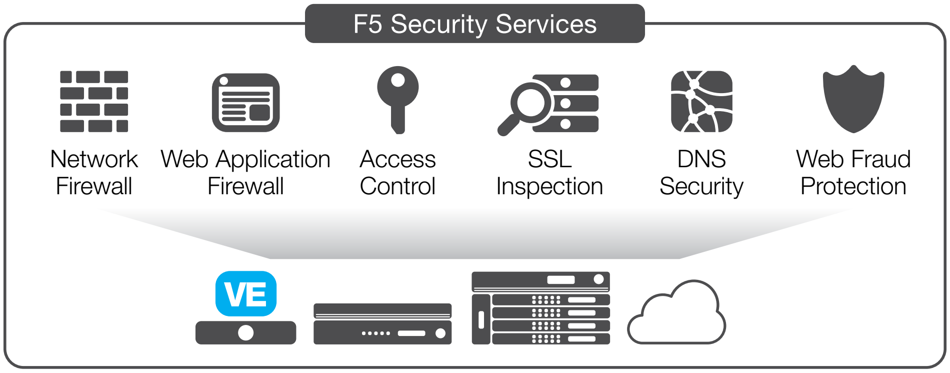
Running multiple instances of Advanced WAF

Advanced WAF uses F5 ScaleN® with F5 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 Advanced WAF devices.

With Advanced WAF and vCMP-enabled systems, administrators can easily consolidate multiple firewalls onto a single device and allocate Advanced WAF resources in a more flexible and isolated manner for different customers, groups, applications, and services. vCMP enables you to run multiple instances of Advanced WAF on a single F5 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. F5 Advanced WAF, together with F5 Web Fraud Protection, F5 BIG-IP Advanced Firewall Manager™ (AFM), and F5 BIG-IP DNS, covers the threat spectrum—mitigating L3–L7 attacks, providing client-side fraud protection, and safeguarding the DNS infrastructure. When used with F5 Access Manager® (AM), Advanced WAF 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, Advanced WAF benefits from other F5 modules to enable data center security, extensive application protection, and access management capabilities.



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

F5 Advanced WAF 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	Yes
Route domain support	Yes
VE, appliance, or managed service	Yes—managed services require Silverline License

WAF Security

Application layer encryption	Yes
Brute Force mitigation	Yes
Credential Stuffing protection	Yes
Behavioral denial-of-service (DoS) protection	Yes—protection for all applications
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
Mobile bot protection	Yes—with the F5 Anti-Bot Mobile SDK
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; more methods available with F5 Access Manager
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 denylisting in HW)	Requires F5 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 F5 BIG-IP AFM and F5 WAF deployment
WAF health monitoring	Yes
Compliance support PCI-DSS, HIPAA, SOX, Basel II	PCI-DSS, HIPAA, SOX, Basel II
Central management and reporting with role-based access control	Yes—requires F5 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 Fraud Protection Service license
SSL acceleration	Yes—core to the BIG-IP platform

BIG-IP Platform and TMOS support

Multi-tenancy	Yes—with F5 vCMP
High availability	Yes—active-passive or active-active
64-bit OS support	Yes
Application acceleration	Yes—requires F5 BIG-IP LTM
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 F5 AM for complete data center security with identity and access management	Yes

F5 Advanced WAF

F5 Advanced WAF is available as a standalone solution or as an add-on module for BIG-IP Local Traffic Manager (LTM) on any F5 platform, and on BIG-IP LTM Virtual Edition (VE). F5 Access Manager (AM) is available as an add-on module to the Advanced WAF standalone appliance. F5 AM Lite (with 10 free user licenses) is included with any Advanced WAF standalone purchase. For detailed physical specifications, please refer to the BIG-IP System Hardware Data Sheet.

BIG-IP Platforms

Only F5's next-generation, cloud-ready application delivery controller (ADC) platform provides DevOps-like agility with the scale, security depth, and investment protection needed for both established and emerging apps. The new F5 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 iSeries, F5 offers the 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 F5 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 F5 System Hardware, VIPRION, and Virtual Edition data sheets 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

F5 Advanced WAF Virtual Edition (VE) can help you meet the needs of your virtualized environment by scaling to 20 cores/vCPUs.

F5 Advanced WAF 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)

Advanced WAF VE is also available as an Amazon Machine Image for use within Amazon Web Services.

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 F5 Advanced WAF, visit f5.com to find these and other resources.

Additional Resources

F5 Advanced WAF Overview

Advanced Application Threats Require an Advanced WAF

F5 Labs 2018 Application Protection Report

eBooks

Bots Mean Business

Credential Stuffing | A Security Epidemic

OWASP Top 10 and Beyond

Report

Gartner Web Application Firewall Magic Quadrant, 2018

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