



What's Inside

- 2 Full-Proxy Application-Centric Security
- 4 Intelligent Control
- 4 Centralized Firewall Policy Management
- 5 Deep Visibility and Reporting
- 5 Increased Scalability, Performance, and Reliability
- 5 Consolidated Application Protection
- 6 Protection for Service Provider Environments
- 7 BIG-IP AFM Features and Specifications
- 9 BIG-IP AFM Availability
- 10 BIG-IP Advanced Firewall Manager
- 10 VIPRION Platforms
- 10 BIG-IP Platforms
- 11 Simplified Licensing
- 11 F5 Global Services
- 11 More Information



Secure the Data Center, Defend the Network, and Protect Applications

Businesses rely on applications for internal productivity and for external customer access. At the same time, applications and the data centers that host them are increasingly under threat from sophisticated, targeted attacks.

F5® BIG-IP® Advanced Firewall Manager™ (AFM) is a high-performance, stateful, full-proxy network firewall designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols. Built on F5's industry-leading Application Delivery Controller (ADC), BIG-IP AFM gives enterprises and service providers the scalability, flexibility, performance, and control needed to mitigate the most aggressive, volumetric distributed denial-of-service (DDoS) attacks before they reach the data center.

BIG-IP AFM's unique application-centric design enables greater effectiveness in guarding against targeted network-level attacks. It tracks the state of network sessions, maintains deep application awareness, and uniquely mitigates attacks based on more granular details than traditional firewalls. With BIG-IP AFM, organizations receive protection from over 100 attack signatures—more hardware-based signatures than any other vendor—and unsurpassed programmability, interoperability, and visibility into threat conditions.

Key benefits

Scale to meet network demand

Meet demands for higher bandwidth usage and concurrency rates with F5's proven TMOS® architecture, hardware systems, and virtual editions to ensure performance while under attack.

Ensure application availability

Secure networks from DDoS threats across a variety of protocols, with in-depth rules customization and increased performance and scalability.

Protect with an app-centric full-proxy firewall

Inspect all incoming client connections and server-to-client responses, and mitigate threats based on security and application parameters before forwarding them on to the server.

Inspect SSL sessions

Fully terminate and decrypt SSL traffic to identify potentially hidden attacks—at high rates and with high throughput.

Streamline firewall deployment

Simplify security configuration with firewall policies oriented around applications and an efficient rules and policy GUI.

Customize reporting for visibility

Easily understand your security status with rich customizable reports, logging, and charts that provide insight to all event types and enable effective forensic analysis.

Full-Proxy Application-Centric Security

Full-proxy stateful security

Unlike traditional firewalls, BIG-IP AFM is built on the full-proxy architecture of the F5 TMOS operating system. Incoming client connections are fully terminated, inspected for possible security threats, and only then forwarded to the server—assuming no threats are present.

With the full-proxy capabilities of TMOS, BIG-IP AFM has in-depth understanding of the most commonly used inbound protocols such as HTTP/S, DNS, ICMP, and TCP, and supports a rich set of services that expand traditional stateful firewall capabilities. Additionally, this security enables deeper visibility into connections, allowing data to be manipulated and modified before it's sent to servers or otherwise.

In the reverse direction, server-to-client communication is also proxied. BIG-IP AFM can scrub return data for sensitive information—for instance, protocol response codes that could divulge network information for reconnaissance attacks—and private data, such as credit card or Social Security numbers.

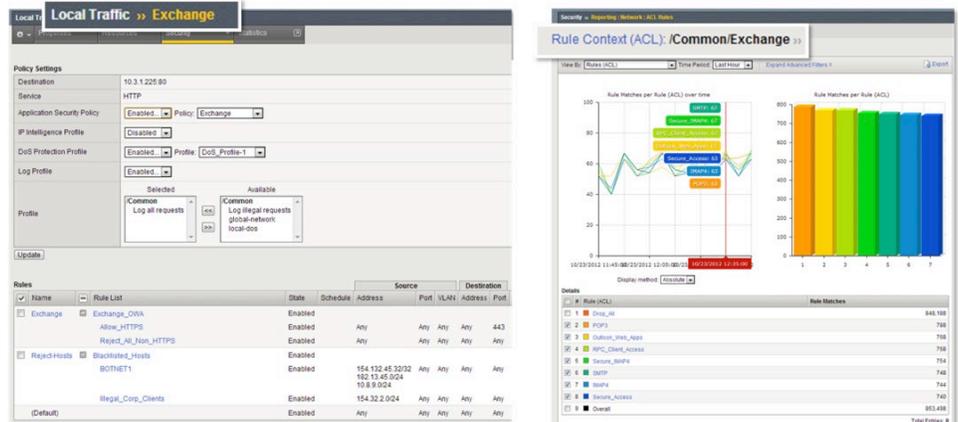
The full-proxy design enables termination of SSL, enforcement of security policies, and other performance-related services—helping organizations address challenges in volatility inside and outside of the data center.

Application-centric firewall policies

Gone are the days of mapping applications to zones, or scouring through spreadsheets of firewall policies to distinguish attacks on specific applications or to identify the IP address for a particular application server.

Unlike most network firewall solutions, BIG-IP AFM firewall policies are logically aligned with the applications in specific traffic flows—streamlining security operations and heightening security effectiveness. But similar to web application firewall solutions, BIG-IP AFM attaches the network firewall policy to application objects. Details about the application parameters, including server addressing, SSL offload, and access policies, can be grouped together with security parameters, including firewall policies, SSL inspection, and logging. This approach provides increased efficiency in addressing app concerns and more accuracy in threat detection and policy effectiveness.

Further, since the configuration for an application is unified with its associated firewall policy, deprovisioning of applications is also streamlined. When an application is deprovisioned, the obsolete firewall rules are simultaneously deprovisioned. BIG-IP AFM helps ensure the effectiveness of application deployment and simplifies firewall policy assurance above rigid zone-based or segment-based constructs.



BIG-IP AFM orients firewall policies around the application itself—streamlining security operations.

Network DDoS protection

The full-proxy architecture of BIG-IP AFM helps to ensure the application infrastructure is protected using advanced capabilities to mitigate denial-of-service (DoS) and DDoS attacks. The out-of-the-box functionality includes a comprehensive set of signatures that enable organizations to defend against, track, and report a breadth of well-known network DDoS attacks and methodologies. Furthermore, it allows you to configure packet limits, percentage increases thresholds, and set absolute rate limits of packets used in attack vectors. Using DoS profiles, BIG-IP AFM performs a variety of checks and mitigates a multitude of attacks, including flood, sweep, teardrop, and smurf attacks, while protecting protocols like SIP and DNS.

BIG-IP AFM offers more granularity and visibility into traffic and DDoS attacks than most solutions, with detailed logging and reporting of attack detection and mitigation. It also delivers increased SYN cookie protections, per-server granular DDoS policies, IP reputation intelligence, and custom whitelist and blacklist support. BIG-IP AFM uses hardware-based DDoS mitigation that scales to prevent high-volume, targeted, network flood attacks—while allowing legitimate traffic to flow without compromising performance.

Unsurpassed flexibility and extensibility

Rapid response is vital in minimizing risk imposed by uncommon attacks. Many firewalls fail to secure the perimeter when faced with less common attacks like Heartbleed. As a component of the F5 BIG-IP® platform, BIG-IP AFM benefits from the extensibility of F5 iRules®, allowing administrators to expand functionality and deploy custom rules that protect against complex and multi-level attacks.

F5 iRules is a scripting language with open APIs that can operate directly on payloads in the data plane. With iRules, administrators can create custom rules to mitigate uncommon, highly-sophisticated DDoS attacks that may not be covered by the BIG-IP AFM packaged solution. The scope of iRules commands provides deep visibility into packets, especially IP/TCP header fields, enabling effective L2–L4 DDoS signatures and flow control via iRule signatures. iRules benefits from BIG-IP AFM anti-DDoS support, which distinguishes between good and bad traffic based on signature(s) and takes action to block, drop, log, redirect, or stop traffic for inspection based on signature matching.

With iRules customization, capabilities including IP intelligence, geolocation features, and statistical sub-sampling can also be applied. iRules has been leveraged by the F5 DevCentral™ community of over 195,000 users, collaborating and creating custom rules that mitigate less common threats. These rules are shared to enable other administrators to flexibly expand the functionality of BIG-IP AFM deployments.

Intelligent Control

IP intelligence

Organizations today are exposed to a variety of potentially malicious attacks from rapidly changing IP addresses. A major advantage in your network protection scheme is the ability to detect and block bad actors before they hit the data center. BIG-IP AFM integrates with [F5 IP Intelligence Services™](#), which provides a real-time glimpse into suspicious sources and guards against known bad actors at the earliest point in the traffic flow.

IP Intelligence Services incorporates external intelligent services to enhance dynamic security with better IP intelligence and stronger, context-based security. By identifying IP addresses and security categories associated with malicious activity, IP Intelligence Services can incorporate dynamic lists of threatening IP addresses into the BIG-IP platform, adding context to BIG-IP AFM policy decisions. Administrators are then able to configure policies that automatically query feed lists and specify blacklist and (whitelist) IP address entries. They can also assign default classes and behaviors to those feed lists. This allows more control for each IP intelligence category by specifying response actions in a policy, and default logging for each policy. IP Intelligence Services reduces risk and increases data center efficiency by eliminating the effort to process bad traffic.

IP shunning

BIG-IP AFM also provides IP shunning capabilities, which help organizations to minimize enforcement time of dynamic security controls that guard against known malicious IPs. IP shunning complements existing IP Intelligence Services. It facilitates more immediate filtering of malicious traffic until intelligence feeds containing blacklisted IP addresses are updated. Up to 100,000 entries can be blacklisted almost instantaneously to enable temporary, immediate blocking (or whitelisting) of malicious IPs. IP shunning reduces time-to-enforcement and increases speed of mitigation based on real-time intelligence from BIG-IP AFM, other BIG-IP modules, and third-party monitoring systems.

Centralized Firewall Policy Management

Large organizations face a growing challenge in managing a consistent and effective security posture across an ever-expanding number of firewall devices. Too often, security administrators must independently manage each device, reducing operational scalability and increasing overhead costs.

F5 BIG-IQ® is an intelligent platform for managing and orchestrating F5 devices and the services they deliver. [The BIG-IQ security component](#) provides central firewall management when deploying and managing multiple BIG-IP AFM devices. Whether deployed in the data center as an appliance, as a virtual edition, or in an SDDC environment, the BIG-IQ security component provides integrated monitoring of BIG-IP AFM rules. This allows administrators to easily manage security policies across multiple devices and quickly respond to today's changing threats and ever-evolving attack profiles.

The BIG-IQ security component simplifies firewall policy lifecycle management for all F5 Application Protection Solutions, providing a single point of control and consolidated view of security policies across BIG-IP AFM and BIG-IP® Application Security Manager™ (ASM) devices. With the BIG-IQ security component, organizations are equipped with a highly scalable and extensible approach to managing firewall rules and configuration elements throughout the entire BIG-IP security infrastructure—making it easier to create, modify, deploy, and manage policies.

Deep Visibility and Reporting

IT and security teams struggle with collecting sufficient threat intelligence and analyzing data that allows them to accurately implement security measures. BIG-IP AFM gives organizations deep insight into attacks and mitigation techniques, enabling them to make more informed decisions that increase overall security effectiveness.

With advanced logging and intelligent threat reporting capabilities, BIG-IP AFM logs millions of records in real time, providing granular visibility into DDoS attacks for in-depth analysis of security events. BIG-IP AFM reports provide clear, concise, and actionable information highlighting attacks and trends with drill-down and page-view capabilities. These offer comprehensive details into attacks, threat progression, and firewall health.

With BIG-IP AFM, organizations can also benefit from F5 Analytics, a module of the BIG-IP platform, which combines DDoS reports from BIG-IP ASM and BIG-IP AFM for a single comprehensive view of the entire threat field. F5 Analytics, previously known as the Application Visibility and Reporting module, allows administrators to view and analyze metrics gathered about the network and servers as well as the applications themselves. Additionally, BIG-IP AFM uses SNMP and JSON reporting to easily communicate DDoS attack details and other key events to higher-level monitoring and forensics systems. These systems offer greater analysis that strengthens the organization's overall security posture.

Increased Scalability, Performance, and Reliability

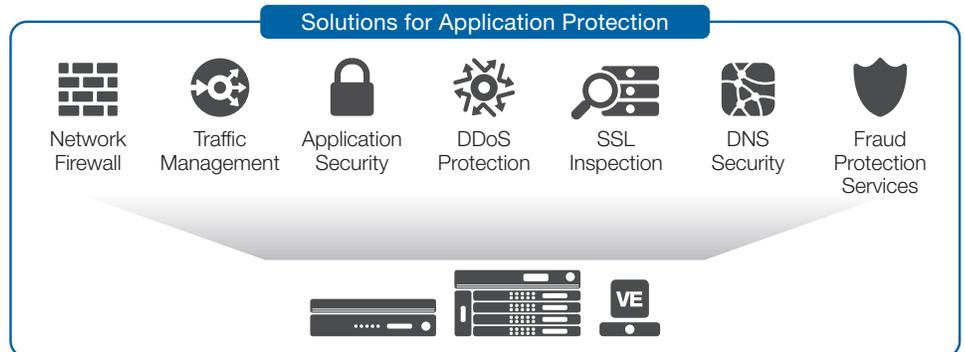
BIG-IP AFM delivers the scalability and performance to tackle the most demanding firewall requirements with outstanding speed and throughput. A single F5 platform scales to handle up to 576 million concurrent connections, 640 Gbps of throughput, and 8 million connections per second to mitigate even the largest volumetric attacks. And when combined with hardware redundancy, synchronization, health monitoring, and automatic failover/failback capabilities, this provides greater assurance in availability and reliability.

BIG-IP AFM uses F5 ScaleN™ with Virtual Clustered Multiprocessing™ (vCMP) enabled systems to give cloud and communications service providers, as well as enterprises, the most cost-effective approach for managing their large-scale firewall deployments. With vCMP, administrators can easily consolidate multiple firewalls onto a single device and allocate BIG-IP AFM resources in a more flexible and isolated manner for different customers, groups, applications, and services. vCMP supports high-density firewall isolation and guest firewall clustering for easier administration and maintenance and to ensure consistency throughout the firewall infrastructure.

Consolidated Application Protection

BIG-IP AFM is a core component of F5's solutions for application protection, which combine the network firewall with traffic management, application security, anti-fraud protections,

and DNS security. These solutions can be consolidated onto a single BIG-IP platform, reducing management complexity and overhead, while offering superior performance and scalability. Building upon BIG-IP® Local Traffic Manager™ (LTM), the consolidated protection delivers deep application fluency for the most widely deployed enterprise applications. This makes it ideal for protecting Internet-facing data center applications, wherever they reside.



F5's solutions for application protection bring together key network and security functions on a single platform.

F5's solutions for application protection are made up of the following BIG-IP modules:

- BIG-IP Advanced Firewall Manager (AFM)—This advanced network firewall forms the core of the F5 application delivery firewall solution. It provides full SSL visibility at scale, as well as network-layer and session-layer DDoS mitigation.
- BIG-IP Local Traffic Manager (LTM)—Provides advanced traffic management, load balancing, and application delivery.
- BIG-IP Application Security Manager (ASM)—Delivers application security, web scraping and bot prevention, and HTTP DDoS mitigation.
- F5 WebSafe™ and MobileSafe™—Protect against threats targeting online and mobile banking application users.
- BIG-IP® DNS (formerly BIG-IP® Global Traffic Manager™ [GTM])—Hyperscales and secures the DNS infrastructure during DDoS attacks and keeps global applications online.
- IP Intelligence and Geolocation—These additional services provide IP reputation and geolocation information for added context-aware security.

Protection for Service Provider Environments

BIG-IP AFM—with its unmatched scale and performance—is also ideal for cloud and communications service provider deployments. In service provider environments, BIG-IP AFM helps to ensure performance as it protects not only the network itself, but also subscribers, from attacks.

In mobile networks, BIG-IP AFM forms the basis of the F5 S/Gi firewall solution. Deployed at the Gi interface of 3G networks and the SGi interface of 4G/LTE networks, the S/Gi firewall solution enforces network perimeters, protects the mobility infrastructure and mobile subscribers, and gives service providers the scalability and flexibility for advanced service enforcement. The S/Gi firewall solution takes advantage of F5's intelligent services framework, meaning CSPs can consolidate additional network and security functions such as carrier-grade NAT and subscriber traffic visibility—all on a single platform.

BIG-IP AFM Features and Specifications

BIG-IP Advanced Firewall Manager is a stateful, full-proxy firewall that provides advanced network protection.

Firewall

Protocol anomaly detection	Yes—SYN/ICMP/ACK/UDP/TCP/IP**/DNS/ARP
L4 DoS and DDoS protection	Yes
SSL DoS and DDoS protection	Yes
DNS and DDoS protection	Yes
HTTP DoS and DDoS protection	Yes
SSL reverse proxy	Yes
IP reputation* and geolocation	Yes—including identifying Tor proxies, malware, and command-and-control (C&C) servers
Central management with role-based access control	Yes—with BIG-IQ Security
SNMP reporting	Yes
DDoS traffic sampling	Yes

*Licensed separately

**IPv4 and IPv6 supported

IPsec

Site-to-site	Yes
Keying methods	Manual, Internet Key Exchange (IKEv1 and IKEv2)
Authentication methods	Preshared key, RSA signature
Diffie-Hellman groups	1, 2, 5, 14, 15, 16, 17, 18
Encryption algorithms	3DES, AES-128, AES-192, AES-256, AES-GCM-128, AES-GCM-256
Hash/HMAC algorithms	SHA-1, AES-GMAC-128, AES-GMAC-192, AES-GMAC-256

Platform Features

Multi-tenancy	Yes—with vCMP
High availability	Yes—active-passive or active-active

SSL VPN

Remote access	Yes—with BIG-IP APM
---------------	---------------------

Scale and Performance	VIPRION 4800 (8 x B4300/ B4340)	VIPRION 4480 (4 x B4300/ B4340)	VIPRION 2400 (4 x B2150/ B2250)	VIPRION 2200 (2 x B2150/ B2250)
Maximum firewall throughput	640 Gbps	320 Gbps	160/160/320 Gbps	80/80/160 Gbps
Connections per second	7.5 million	4.8 million	1.5 million/ 3.8 million	750,000/ 1.9 million
Maximum concurrent connections	576 million	144 million	88 million/ 176 million	44 million/ 88 million

Scale and Performance	BIG-IP 10050s/10250v	BIG-IP 7050s/7250v	BIG-IP 5050s/5250v
Maximum firewall throughput	80 Gbps	40 Gbps	30 Gbps
Connections per second	850,000	370,000/ 750,000	670,000/ 330,000
Maximum concurrent connections	36 million	22 million	22 million

Scale and Performance	BIG-IP 4000s/4200v	BIG-IP 2200s/2000s
Maximum firewall throughput	10 Gbps	5 Gbps
Connections per second	130,000/ 250,000	135,000/ 67,000
Maximum concurrent connections	9 million/ 10 million	5 million/ 4.5 Million

BIG-IP AFM Availability

BIG-IP Advanced Firewall Manager is available bundled with other modules to enable specific application delivery firewall use cases, as follows.

Bundle Name	BIG-IP AFM	BIG-IP LTM	BIG-IP ASM	BIG-IP APM	BIG-IP APM Lite (10 users)
Application Delivery Firewall	✓	✓			✓
Application Delivery Firewall with Application Security	✓	✓	✓		✓
Application Delivery Firewall with Access Management	✓	✓		✓	✓
Application Delivery Firewall with Application Security and Access Management	✓	✓	✓	✓	✓
Advanced Firewall Manager Add-On (for systems that already have BIG-IP LTM)	✓				

Note: All BIG-IP AFM licenses include protocol security, routing, and maximum SSL. IP Intelligence and Geolocation are available add-ons for all bundles.

BIG-IP Advanced Firewall Manager

BIG-IP Advanced Firewall Manager is available as an add-on module for integration with BIG-IP Local Traffic Manager on any BIG-IP platform. For detailed physical specifications, please refer to the [BIG-IP System Hardware Datasheet](#).

BIG-IP LTM Virtual Edition

BIG-IP LTM Virtual Edition (VE) is a version of the BIG-IP system that runs as a virtual machine. BIG-IP Advanced Firewall Manager can be deployed on a virtual edition. BIG-IP VEs include all features of BIG-IP devices running on the standard F5 TMOS, except as noted in release notes and product documentation.

VIPRION Platforms

BIG-IP Advanced Firewall Manager is also available as an add-on module to BIG-IP Local Traffic Manager on the modular F5 VIPRION® platform. This chassis and blade architecture enables simple scalability as your Application Delivery Network grows. See the [VIPRION Datasheet](#) for details.

BIG-IP Platforms

F5 Software-Defined Application Services™ are delivered via both hardware and software to flexibly support your specific environments—physical, virtualized, or cloud.

Hardware includes BIG-IP appliances or the VIPRION modular chassis and blade system designed specifically for application delivery, security, and high performance. VIPRION uses [ScaleN](#) technologies to provide on-demand linear scalability by enabling you to add blades without re-configuration. BIG-IP® virtual edition (VE) software runs on commodity servers and provides agility and fast deployment of services in cloud environments. See the [BIG-IP System Hardware](#), [VIPRION](#), and [Virtual Edition](#) datasheets for 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 solutions can be centrally managed through [F5 BIG-IQ](#), an intelligent platform for managing and orchestrating F5 devices and the services they deliver.



BIG-IP Appliance



VIPRION Chassis



BIG-IP Virtual Edition

Simplified Licensing

Meeting your applications' needs in a dynamic environment has never been easier. F5's **Good, Better, Best** provides you with the flexibility to provision advanced modules on demand, at the best value.

- Decide what solutions are right for your applications' environment with F5's reference architectures.
- Provision the modules needed to run your applications with F5's Good, Better, Best offerings.
- Implement complete application flexibility with the ability to deploy your modules on a virtual or physical platform.

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 Advanced Firewall Manager and complimentary solutions, visit f5.com to find these and other resources:

Datasheets

[BIG-IP Application Security Manager](#)

[IP Intelligence Services](#)

[BIG-IP Access Policy Manger](#)

Web pages

[BIG-IP Advanced Firewall Manager](#)

Solution profile

[High-Performance Application Delivery Firewall](#)

White papers

[A New Firewall for the Data Center](#)

[Mitigating DDoS Attacks](#)

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.

