F5 BIG-IP AFM—SERVICE PROVIDER SECURITY PLATFORM

WHAT'S INSIDE

DEFEND THE NETWORK CORE AND EDGE, AND PROTECT SERVICES

Mobile and fixed line service providers rely on their networks and data centers to drive their service-based revenues. Given their critical nature, these networks have become a major target for attack. While service providers are busy mitigating simple attacks, hackers are using more sophisticated, evolving strikes to disrupt service or steal data.

F5 BIG-IP Advanced Firewall Manager (AFM) is a high-performance, full-proxy network security solution designed to protect networks and 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 service providers a scalable, subscriber-aware platform that delivers the flexibility, performance, and control needed to mitigate aggressive distributed denial-of-service (DDoS) and protocol attacks before they overwhelm and degrade services.

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

ICSA labs CERTIFIED IPSEC

ICSA labs CERTIFIED FIREWALL - CORPORATE

KEY BENEFITS

Ensure services availability
Secure the network edge and core from DDoS and protocol threats with in-depth rules customization, and increased performance and scalability.

Protect with full proxy capabilities
Inspect all incoming subscriber connections and server-to-client responses, and mitigate threats based on security and protocol parameters before forwarding them.

Inspect SSL sessions
Decrypt SSL traffic to identify potentially hidden attacks—at high rates and with high throughput.

Automate security deployment
Simplify configuration with security policies oriented around services and protocols and an efficient rules and policy GUI.

Scale to meet network demand
Meet demands for higher bandwidth usage and concurrency rates with F5's proven virtual software editions and hardware systems to flexibly ensure performance while under attack.

Consistent protection for containerized applications
Protect container-based applications regardless of platform or location with attack detection and mitigation services to mitigate attacks and risks.

Flexible automation options for ease of integration into operations
Extensive integration with third-party and public cloud automation tools to speed BIG-IP AFM into production.

Actionable reporting and visibility
Easily understand your security status with rich telemetry that can be customizable into reports and charts to provide insight to all event types and enable effective forensic analysis.

Reduced Operational Complexity
Single platform to consolidate and deliver Firewall, CGNAT, DNS, protocol protection and deep packet inspection to reduce operational complexity and costs.

SUBSCRIBER SERVICES AND APPLICATION-CENTRIC SECURITY POLICES

FULL PROXY SECURITY

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

With these full-proxy capabilities, BIG-IP AFM has in-depth understanding of the most commonly used inbound protocols such as HTTP/S, DNS, Diameter, GTP, SSH, ICMP, and TCP, and supports a rich set of services that expand beyond traditional stateful firewall capabilities. Additionally, this security enables deep 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, east-west firewall capabilities, and other performance-related services—helping organizations address challenges in volatility inside and outside of the data center.

APPLICATION-CENTRIC SECURITY 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 security solutions, BIG-IP AFM security policies are logically aligned with the applications in specific traffic flows—streamlining security operations and heightening security effectiveness. However, similar to web application firewall solutions, BIG-IP AFM attaches network security policies to application objects. Details about the application parameters, including server addressing, SSL offload, and access policies, can be grouped together with security parameters, including policies, SSL inspection, and logging. This includes information on which layer 7 protocols are permitted for specific application port access. F5's app-centric 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 an associated network security policy, deprovisioning of applications is also streamlined. When an application is deprovisioned, the obsolete security rules are simultaneously deprovisioned. BIG-IP AFM helps ensure the effectiveness of application deployment and simplifies policy assurance above rigid zone-based or segment-based constructs.

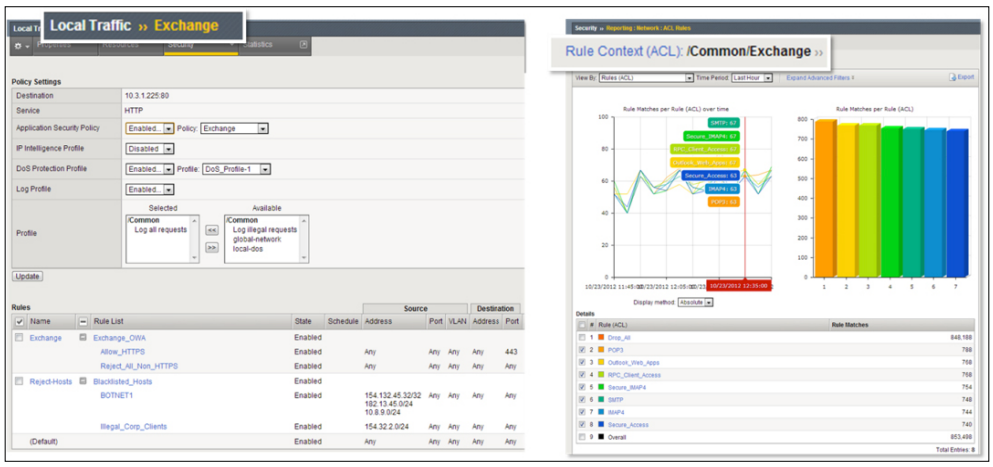

Figure 1: BIG-IP AFM orients firewall policies around the application itself–streamlining security operations.

NETWORK DDoS PROTECTION

The full-proxy architecture of BIG-IP AFM helps to ensure the application infrastructure is protected using advanced capabilities to mitigate 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. Admins can automatically or manually set DDoS threshold values. Furthermore, you can configure packet limits, percentage increases for 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 also helps to ensure clean pipes for inbound traffic. Using remotely triggered black hole filtering (RTBH), BIG-IP AFM stops attack traffic even before it leaves the ISP network realm. When activated, BIG-IP AFM automatically broadcasts malicious IPs to upstream routers to enforce denylisting through participating ISP routers, ensuring that only good traffic is routed to the data center network and applications within. RTBH functionality leverages the BIG-IP AFM IP shun category denylist that uniquely identifies and blocks malicious L3–L7 attack sources in hardware until feed lists are updated. BIG-IP AFM can also signal and redirect traffic to F5 Silverline for DDoS Protection service. Silverline's DDoS defense can be either reactive or proactive hybrid DDoS defense—ensuring always-up services by rerouting attacks away from the data center for cloud-based mitigation.

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.

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 allowlist and denylist 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.

Dynamic Denylisting

Attackers are continually changing their tactics in order to circumvent security controls. One of the more useful evasive tactics used by attackers is changing different IP addresses. By changing their IP addresses and associated domain names they can avoid being blocked and continue their attacks.

BIG-IP AFM provides IP denylisting capabilities that help organizations to minimize enforcement time of dynamic security controls that guard against known malicious IPs. IP denylisting complements existing IP intelligence services. It facilitates more immediate filtering of malicious traffic until intelligence feeds containing denylisted IP addresses are updated. Up to 100,000 entries can be denylisted almost instantaneously to enable temporary, immediate blocking (or allowlisting) of malicious IPs. IP denylisting 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.

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 anticipate, detect, and respond to threats before they hit the data center. BIG-IP AFM integrates with **F5 IP Intelligence Services** for stronger context-based security that strategically guards against evolving threats at the earliest point in the traffic flow.

IP Intelligence Services minimizes the threat window and enhances BIG-IP AFM DDoS and network defense with up-to-date network threat intelligence for stronger, context-based security. It maintains information on more than one million malicious URL and IP addresses, and can effectively block connections to and from those addresses. To minimize the threat window and keep an organization's data and reputation safe, the IP Intelligence Services database of addresses is refreshed every five minutes from the cloud. Administrators can assign default classes and behaviors to feed lists, allowing more control for each IP intelligence category by specifying response actions and default logging for each policy. IP Intelligence Services reduces risk and increases data center efficiency—eliminating the effort to process bad traffic.

IN-DEPTH INFRASTRUCTURE PROTECTION

SSH Channel Protection

BIG-IP AFM uniquely controls operations in the SSH channel and helps prevent data breaches, malware distribution, and compliance failures. When deployed in front of SSH servers, BIG-IP AFM acts as a man-in-the-middle SSH proxy—filtering SSH traffic, and controlling access to files, databases, and system information by limiting task users can perform. Unlike leading firewalls, SSH policies limit permissible actions per user or per virtual server to strengthen security on SSH channels—tracking usage and preventing misuse of SSH channels by employees and contractors and stopping east-west attacks that move throughout the infrastructure. Additionally, BIG-IP AFM prevents SSH sessions from remaining open indefinitely and ensures effective and continuous SSH key management for tighter security and compliance.

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.

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 250,000 users, collaborating and creating custom rules that mitigate fewer common threats. These rules are shared to enable other administrators to flexibly expand the functionality of BIG-IP AFM deployments.

PROTECTING NETWORK RESOURCES WITHOUT COMPROMISING FLEXIBILITY AND CONTROLLING COSTS IS A CONSTANT BATTLE. BIG-IP AFM WITH ITS UNMATCHED SUBSCRIBER AGGREGATION CAPACITY ENABLES SERVICE PROVIDERS TO PROTECT NETWORKS AND SUBSCRIBERS WHILE CONSOLIDATING NETWORK INFRASTRUCTURE WITHOUT COMPROMISING FLEXIBILITY.

N6/SGi Firewall

Mobility service providers face not only intense competitive pressure, but also continual attacks on their infrastructure designed to impact subscriber services. Protecting network resources without compromising flexibility and controlling costs is a constant battle. BIG-IP AFM with its unmatched subscriber aggregation capacity enables service providers to protect networks and subscribers while consolidating network infrastructure without compromising flexibility.

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 subscribers. It gives service providers the scalability and flexibility for advanced protocol and service enforcement. The S/Gi firewall solution takes advantage of F5's intelligent services framework, meaning service providers can consolidate additional network and security functions such as carrier-grade NAT (CGNAT)and subscriber traffic visibility—all on a single platform. The F5 iSeries and VIPRION platforms have built-in Telco-grade dependability to ensure consistent service operation under heavy workloads. For encryption/decryption, both the iSeries and VIPRION are FIPS-140 certified to ensure the highest level of protection for subscriber traffic.

CGNAT

The worldwide proliferation of wireless and Internet-enabled devices has led to the rapid depletion of IPv4 addresses. All of the five Regional Internet Registries (RIR) has exhausted its IPv4 allocations, and final pool exhaustion happened in November 2020; meanwhile, IPv6 adoption continues to grow. Service providers need a solution that will help them manage IPv4 address depletion and increase network optimization by seamlessly migrating to IPv6.

F5 BIG-IP Carrier-Grade NAT (CGNAT) offers a broad set of tools that enables service providers to successfully migrate to IPv6 while continuing to support and interoperate with existing IPv4 devices and content. BIG-IP CGNAT offers service providers tunneling solutions with Dual-Stack Lite capabilities as well as native network address translation solutions, such as NAT44 and NAT64. It provides carrier-grade scalability by offering a very high number of IP address translations, very fast NAT translation setup rates, and high throughput. Granular, high-speed Netflow logging brings visibility and control to data analytics. Data collection per protected object is configurable, and can be collected for specific time intervals to simplify analysis and reduce the time to problem resolution.

DNS Security

BIG-IP DNS DELIVERS AN INTELLIGENT AND SCALABLE DNS INFRASTRUCTURE THAT GIVES MOBILE USERS FASTER ACCESS AND SERVICE RESPONSE. THIS MAKES IT EASY FOR SERVICE PROVIDERS TO OPTIMIZE, MONETIZE, AND SECURE THEIR DNS INFRASTRUCTURES.

DNS servers are critical to any mobile or fixed line network operator. Security is paramount to operations, as the DNS protocol serves as the basis for internet infrastructure mapping of the web domains that subscribers access. BIG-IP® DNS delivers an intelligent and scalable DNS infrastructure that gives mobile users faster access and service response. This makes it easy for service providers to optimize, monetize, and secure their DNS infrastructures. F5 DNS provides carrier-grade, high-performance LDNS caching and resolving, and is a hyper-scale authoritative DNS solution that handle business growth and sudden demand spikes.

BIG-IP AFM shields the DNS infrastructure from malicious attacks designed to reduce DNS and service performance, launched by infected subscribers from undesired DNS queries and responses. F5's intelligent protection of DNS services inspects and validates traffic adherence to the DNS protocol while dropping invalid requests or refusing to accept unsolicited responses. BIG-IP AFM is an ICSA Labs certified network firewall with DDoS threshold alerting that hyper-scales across many devices using IP Anycast for DDoS absorption. It mitigates threats by blocking access to malicious IP domains.

Intrusion Prevention Security

Service provider networks operate a number of protocols that enable fixed and mobile subscriber connectivity. These protocols have weak or non-existent built-in security and can be exploited by an attacker to steal information or impact services. Protecting them is a must in order to deliver an experience that meets customers' expectations in a competitive marketplace.

BIG-IP AFM Intrusion Prevention System (IPS) delivers deep packet inspection and visibility for incoming network traffic. BIG-IP AFM IPS engine performs Layer 5-7 traffic inspection for security incidents, protocol/application violations and exploits to take appropriate action for prevention. It reviews traffic for adherence to 25+ protocol standards and matches against hundreds of known attack signatures and exploits.

For Mobility service providers, BIG-IP AFM IPS performs traffic inspection and protocol adherence for SS7, Diameter (FS.19 compliance checks), HTTP/2, GTP (FS.20 compliance checks), SCTP and SIP to ensure that these application servers are not attacked or exploited.

The Central management interface for IPS leverages the industry standard domain specific language (SNORT) to provide policies and signatures to validate traffic against. This also enables the ingestion and utilization of existing SNORT policies and signatures from other sources to ensure consistent security.

BIG-IP AFM IPS is architected upon the F5 BIG-IP platform, and designed for native multi-threaded processing, for ease of scalability—enabling it to handle traffic spikes or planned growth without compromising services. The multi-threaded architecture ensures high-availability and enables hit-less upgrades to enable non-stop business operations and risk exposure.

BIG-IP AFM IPS's architecture supports rapid visibility of threats via a BIG-IQ dashboard. High-speed logging for near real-time visibility and control is also supported to third-party SIEM platforms. To further help service providers keep up with evolving attacks and hacks, BIG-IP AFM IPS has incorporated a traffic learning capability that deeply monitors traffic and auto-develops policies. The Traffic Learning capability suggests rules based on traffic patterns that can be accepted or denied manually or automatically to easily add protection without expertise or overhead.

WHEN BIG-IP AFM IS DEPLOYED IN A SERVICE PROVIDER'S NETWORK, IT FEATURES KEY DIFFERENCES WHEN COMPARED TO TRADITIONAL NETWORK FIREWALLS, MAKING IT MORE EFFECTIVE FOR IOT SERVICES.

IoT Protection

The Internet of things (IoT) comes in all shapes and sizes: from three-ton automobiles to clothing to under-the-skin blood sugar monitors and even entire homes. With IoT, communication across the internet is enabled by services from service provider mobile and fixed-line networks. Managing IoT traffic does not come without its challenges. Threats to service provider networks and data centers must be addressed in order for IoT services to be successful.

When BIG-IP AFM is deployed in a service provider's network, it features key differences when compared to traditional network firewalls, making it more effective for IoT services. BIG-IP AFM provides device-aware, application-centric security policies. This allows service providers to offer IoT security services without the need to host the IoT application in their data centers, or directly manage the IoT application.

BIG-IP AFM as an IoT firewall mitigates threats by stopping DDoS and application-layer attacks which may disrupt the integrity and availability of the service provider's network. BIG-IP AFM also ensures that devices are only connecting to 'safe' locations and prevents devices from connecting to unknown services. This reduces the chances of devices being compromised through malware and blocks malicious 'ThingBot' C&C (command and control) communication to stop devices from being exploited remotely.

IPSEC

The explosion of applications within the data center, in the cloud, and out at the edge infrastructure creates a challenge in protecting the data from theft or hack attacks. Enabling and managing encryption and decryption on each application is prohibitive due to operational and infrastructure costs. Yet, encrypting and decrypting traffic between different application hosts and clients spread across networks and remote locations is critical to protecting data and ensuring application integrity.

BIG-IP AFM integrated IPSEC encryption and decryption enables secure data connectivity between hosts and networks to eliminate risk of data theft and application attacks. AFM supports IPsec ESP and AH connections to create secure connections for data transmission.

Protection for Container-based Apps

Application development today is based on a container infrastructure that enables faster application development with greater scale-out capabilities. Container based applications can easily grow and can become distributed; but container-based applications, and the underlying infrastructure, need to be protected just like traditional applications.

BIG-IP AFM Virtual Edition (VE) supports running in both public and private cloud environments and provides protection that readily secures container-based applications by off-loading the "North/South" decryption and encryption of traffic to and from container-based application environments. BIG-IP AFM also monitors and provides visibility for non-volumetric attacks on container-based applications and enables fast development of protection via iRules.

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.

Deep Visibility and Reporting

IT and security teams struggle to collect enough threat intelligence, and analyze enough data, to implement the right 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 BIG-IP AFM 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.

Automation and Centralized 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 CENTRALIZED MANAGEMENT PROVIDES CONSOLIDATED, CUSTOMIZABLE, AND SECURITY-SPECIFIC DASHBOARDS THAT PROVIDE NEAR REAL-TIME VISIBILITY INTO TRAFFIC FROM MULTIPLE BIG-IP AFM INSTANCES BY SOURCE AND TRAFFIC TYPE.

F5 BIG-IQ® Centralized Management enables administrators to easily manage and orchestrate F5 devices and the services they deliver, including the security services of BIG-IP AFM. F5 BIG-IQ Centralized Management provides consolidated, customizable, and security-specific dashboards that provide near real-time visibility into traffic from multiple BIG-IP AFM instances by source and traffic type. Leveraging these insights and proactive alerting capabilities, BIG-IQ makes it easy to react quickly to changes and push updated and optimized configuration and policies to many BIG-IP AFM deployments from a single, unified console. BIG-IQ also leverages simple, yet powerful REST APIs to make integrating with third-party services quick and easy. And, with its tight integration with the F5 Automation Toolchain, injecting automation into app services and infrastructure creation, provisioning, and management, you can take a programmatic approach to working with BIG-IP AFM and other F5 solutions.

BIG-IP AFM is also easily automated into production via integrations with third party integrations. F5 has built solution templates for AWS, Azure, and Google public cloud environments and API integration with third-party automation tools such as Ansible and Terraform.

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 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 than with firewalls 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 Infrastructure Platform

BIG-IP AFM is a core component of F5's solutions for application protection, which combines network security capabilities with traffic management, application security, 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 and service provider protocols. This makes it the ideal platform for security standardization for protecting Internet-facing data center and distributed edge applications.

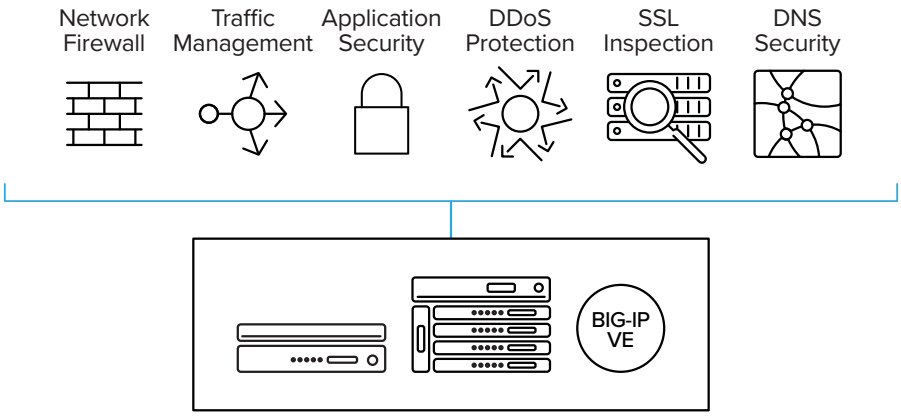

Figure 2: F5's solutions for application protection bring together key network and security functions on a single platform.

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

- **BIG-IP AFM**—This advanced network security solution forms the core of the F5 application protection solution. It provides full SSL visibility at scale, as well as network-layer and session-layer DDoS mitigation.
- **BIG-IP Advanced Web Application Firewall (Advanced WAF)**—Delivers application security, web scraping and bot prevention, and HTTP DDoS mitigation.
- **BIG-IP Local Traffic Manager (LTM)**—Provides advanced traffic management, load balancing, and application delivery.
- **BIG-IP DNS**—Hyperscales and secures the DNS infrastructure during DDoS attacks and keeps global applications online.
- **BIG-IP IPS**—Intrusion Prevention protects infrastructure and protocols and compliance verification.
- **IP Intelligence and Geolocation**—These additional services provide IP reputation and geolocation information for added context-aware security.

FEATURES AND SPECIFICATIONS

BIG-IP AFM is a stateful, full-proxy security solution that provides advanced network protection and capabilities that exceed traditional firewalls.

Protocol anomaly detection	Yes—SYN/ICMP/ACK/UDP/TCP/IP**/DNS/ARP
DoS and DDoS protection	Yes—L3, L4, SSL/TLS, HTTP, Flood, Sweep
Remotely trigger black hole filtering (RTBH)	Yes
SSH Proxy	Yes
Port-misuse protection	Yes
SSL/TLS Reverse proxy	Yes
IP reputation* and geolocations	Yes—including identifying Tor proxies, malware, and command-and-control (C&C) servers
Central management w/RBAC	Yes—with BIG-IQ Centralized Management
SNMP reporting	Yes
DDoS traffic sampling	Yes

* - licensed separately
** - IPv4 and IPv6 supported

BIG-IP AFM Availability

BIG-IP AFM is available with other modules to enable specific infrastructure, protocol and application security use cases, as follows.

NAME	AFM	IPS	LTM	ADV. WAF	APM
AFM's base service provider security platform (protocol protection, visibility and automation, and ICSA-certified firewall)	•				
AFM with Intrusion Prevention System (IPS) for advanced traffic inspection and security	•	•			
AFM with Application Delivery Controller (ADC) for load balancing of inbound subscriber traffic	•		•		
AFM with Advanced Web Application Firewall for protecting layer 7 applications from automated and manual attacks	•		•	•	
AFM with user access management	•		•	•	•
AFM with Access Policy Manager for user access management	•		•	•	•
AFM Add-on for existing LTM platforms (hardware or software)	•				

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 AFM 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 Data sheet.

PLATFORMS AND SERVICES

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 AFM 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. BIG-IP AFM VE's can be optimized against DDoS attacks and for SSL/TLS processing with Intel SmartNIC and Quick-assist Technology (QAT). Intel SmartNIC includes a FPGA which pre-processes DDoS attacks out of the traffic before it hits the Intel x86 core CPU for processing. For SSL/TLS decryption/encryption, the Intel QAT processor is supported for off-loading this intensive processing from the core CPU for improved performance.

VIPRION Platforms

BIG-IP AFM 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 enable simple scalability as your Application infrastructure grows. The VIPRION platform is NEBS Level 1 and FIPS 140-2 Level 2 compliant to ensure adherence to industry standards and compliance. See the VIPRION Data sheet for details.

BIG-IP Platforms

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. The F5 BIG-IP iSeries 15K is designed specifically to meet service providers' performance requirements in a 1U platform.

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 BIG-IP iSeries, F5 offers VIPRION modular chassis and blade systems designed specifically for performance and for true on-demand linear scalability without business disruption. 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. VIPRION systems use F5's ScaleN clustering technology to add blades without reconfiguration or rebooting.

Figure 3: BIG-IP iSeries Appliance, VIPRION Chassis, and BIG-IP Virtual Editions.

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 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.

Business-aligned Licensing

Meeting your applications' needs in a dynamic environment has never been easier. F5 BIG-IP AFM is available via F5's Good, Better, Best licensing that provides you with the flexibility to provision advanced modules on demand, at the best value.

- Provision 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

BIG-IP AFM VE can be utilized in accordance with business operational needs. F5 VE's can be purchased via Subscription, Enterprise License Agreement, Perpetual for on-premises and/or public multi-cloud architectures. Public cloud 'pay-as-you-go' (PAYG) is also supported.

F5 Professional 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.

F5 Global Support Services

F5 Global Services helps you deliver your applications with the availability, performance and security users expect. With deep expertise in F5 application services, as well as the ecosystems that they operate in, our teams can help you support new business initiatives including automation, migrating apps to the cloud, ensuring consistent security and deploying new application architectures.

F5 provides the services, support, and training you need to ensure success across the lifecycle of your deployments, from implementation to maintenance to optimization. We help you speed deployment, drive operational efficiencies and get to market as quickly as possible.

F5 offers a range of support packages that provide best in class technical expertise to help solve your challenges. You can take advantage of flexible options including our robust, self-solve knowledge repository, communities and phone. Our worldwide support centers are available 24/7 to provide help wherever and whenever you need it.

Service Provider Essentials

The F5 Service Provider Essentials technical services program (SPE) offers a specialized level of service designed for, and exclusively available to, our service provider customers in almost every country. It provides service provider operations teams with the specialized support they need to effectively manage their F5 application delivery estate. F5 SPE combines high-quality, service provider-specific technical assistance including a dedicated service provider network support team, consulting hours inside the maintenance contract, and high-urgency incident management. Learn more at f5.com/SPE.

Premium Plus

Premium Plus customers receive priority status at F5, with fast, easy access to remote assistance from a dedicated team of senior-level, F5-certified Network Support Engineers and a Service Delivery Manager. You also get proactive support for planned maintenance, advance RMA replacement, software upgrades, and help with F5 iRules scripts. Your Premium Plus team will also work with you to create an IT environment that addresses your business goals. Learn more at www.f5.com/services/support.

MORE INFORMATION

To learn more about BIG-IP AFM and complimentary solutions, visit f5.com to find these and other resources:

Data sheets

BIG-IP Advanced WAF
IP Intelligence Services
Access Policy Manager

Web pages

F5 BIG-IP AFM

Additional resources

Intelligent DNS Firewall for Service Providers
Diameter Security
Near Real-Time DNS Reporting Attack Mitigation Case Study
Carrier-Grade NAT for Service Providers
Key Use Cases for GTP

DC1120 | DS-SP-551986256