Scalable, Intelligent DDoS Protection

F5 application delivery firewall and traffic management solutions are built on high-scale/high-performance architectures, with full-proxy, deep-application fluency. At the same time, F5 solutions have always existed at the strategic point of control within the network, making them ideally suited to protect against on-premises distributed denial-of-service (DDoS) attacks at all layers: protecting the network, session, and application.

DDoS Threats

DDoS attacks have changed over the last few years. Increasingly, the motivations for attacks are either financial or political, but the objective is the same: to cause a service outage. And while we still see traditional large-scale attacks aimed at filling Internet pipes, attacks intended to exhaust application server resources gradually are becoming more prevalent.

High-profile businesses, such as financial institutions, governments, and service providers, continue to be targets. But a rising number of everyday businesses are also reporting being under attack. The most basic line of defense—the network firewall—has failed to keep up with the volume and intelligence of attacks—especially when attacks involve SSL encryption. The result is that the DDoS attacks get through the firewall line of defense.

Additionally, traditional firewalls' limited capacity to employ contextual data means they are unable to make an intelligent decision about how to deliver application traffic while also keeping services available for valid requests during a DDoS attack.

Cloud-based Services Are Not Enough

Comprehensive DDoS protection must include not only cloud-based scrubbers to handle volumetric attacks, but also strong on-premises security to mitigate attacks targeted at application servers (such as business logic attacks) and DNS servers, as well as attacks hidden in SSL-encrypted communication. This last point is key—in order to scrub SSL-encrypted data for DDoS threats, the communication must be decrypted. Most organizations are unwilling (or even legally forbidden) to upload SSL private keys to a cloud-based service, so on-premises security is the only option.

The F5 DDoS Protection Solution

F5® DDoS solutions provide the security, scale, and intelligence to protect network and application infrastructure in the most demanding deployments. With advanced software and specialized DDoS mitigation hardware available, F5 keeps the attackers at bay while allowing valid employees and customers access to applications.

Key features

- **Scalability and Performance**—Built on the market's highest-performing application delivery firewall
- **Intelligence and Context**—Ability to pull in additional information about incoming connections and monitor for anomalous latency to distinguish attackers from valid users
- **Protection at All Layers**—DDoS mitigation at the network, session, and application layers, including hardware-accelerated SYN flood protection on certain platforms, high-scale SSL inspection, DNS security, and web application protection
- **Dynamic Threat Defense**—Enforced protocol functions on both standard and emerging or custom protocols via iRules

Key benefits

- **Maintain Application Availability**—High scale and performance combine with intelligent and contextual defense to ensure applications remain available, even in the face of attacks
- **Protect Network Infrastructure**—Dedicated hardware and a purpose-built full-proxy architecture mitigate attacks before they reach your network
- **Defend Against Targeted Attacks**—Protection against a breadth of DoS attack vectors, providing administrators with the optimal tools to mitigate crafted attacks
- **Stay One Step Ahead**—Scales to handle hundreds of millions of connections and hundreds of Gbps to defend both wireline and wireless resources

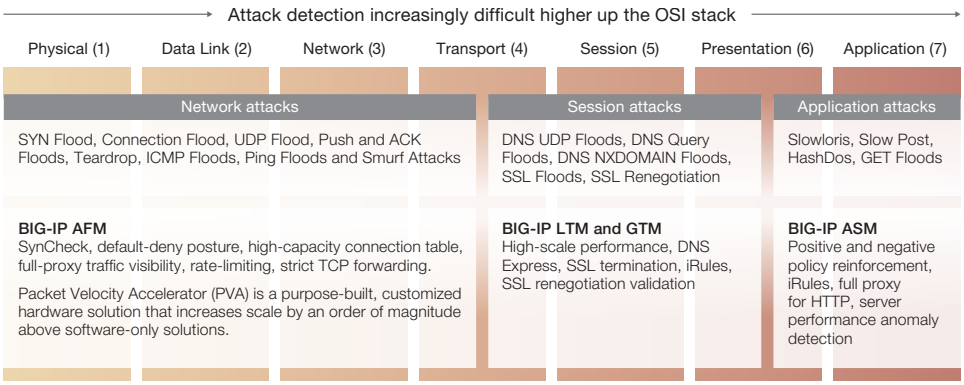
BIG-IP® Advanced Firewall Manager™ (AFM) is a high-performance, stateful, full-proxy network firewall that defends against network-layer DDoS attacks such as SYN floods, as well as session-layer attacks such as SSL floods. BIG-IP® Application Security Manager™ (ASM), an advanced web application firewall, uses F5's deep application fluency to detect and mitigate HTTP-based attacks. BIG-IP® Global Traffic Manager™ (GTM) is a scalable DNS and DNSSEC solution that mitigates DNS-based attacks. BIG-IP® Local Traffic Manager™ (LTM), an application delivery solution, adds intelligent traffic management.

Scale and performance: BIG-IP AFM and BIG-IP LTM scale to up to 576 million concurrent connections, 640 Gbps of throughput, and 8 million connections per second—performance that can mitigate even the largest volumetric attacks.

DDoS protection for all layers: network, session, and application: F5 DDoS solutions provide security at all layers, protecting not only protocols (such as UDP, TCP, SIP, DNS, HTTP, and SSL), but also applications. This includes the ability to mitigate even new and advanced DDoS vectors with custom signatures.

SSL termination: The BIG-IP system excels at offloading and inspecting SSL traffic, making it the only place in the network where early content analysis and mitigation can be performed for SSL attacks. The high-scale SSL proxy also means F5 solutions can mitigate SSL floods and renegotiation attacks.

Extensible security and dynamic threat mitigation: F5 iRules® scripting language provides a flexible means of enforcing protocol functions and scanning payloads to create a zero-day dynamic security context to react to DDoS threats and vulnerabilities for which an associated patch has not yet been released.



F5 DDoS protection solutions provide security at all layers: network, session, and application—all on a single platform.

Learn more

For more information about F5 DDoS protection solutions, please see the following resources or use the search function on f5.com.

Solution pages

F5 DDoS Protection

F5 Application Delivery Firewall

Product pages

BIG-IP Advanced Firewall Manager

BIG-IP Local Traffic Manager

BIG-IP Global Traffic Manager

BIG-IP Application Security Manager

Datasheet

BIG-IP Advanced Firewall Manager

BIG-IP Local Traffic Manager

BIG-IP Global Traffic Manager

BIG-IP Application Security Manager

White papers

The DDoS Threat Spectrum

Mitigating DDoS Attacks with F5 Technology

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

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

F5 Networks
Asia-Pacific
apacinfo@f5.com

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

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