High-Performance Application Delivery Firewall

F5 solutions sit at the strategic point of control in the network to deliver applications, which is also the ideal place to perform security functions such as network firewalling, advanced authentication, web application firewalling, availability monitoring, SSL termination, and distributed denial-of-service (DDoS) mitigation. The F5 application delivery firewall solution combines scalability, application fluency, and intelligence to deliver data and applications safely.

Evolving Threats

Internet data centers and public-facing web properties are constant targets for large-scale attacks by hacker/hacktivist communities and others looking to grab intellectual property or cause a service outage. Organizations must prepare for the normal load of users, but they also must defend their infrastructures from the daily barrage of malicious attackers.

Traditional firewalls are not meeting fundamental functional requirements, let alone performance needs. Dynamic and layered attacks that necessitate multiple point solutions add to administrative distress. Traditional firewalls can be overwhelmed by their limited ability to scale under a DDoS attack while keeping peak connection performance for valid users, which renders not only the firewalls themselves unresponsive, but the websites they are supposed to protect. Additionally, traditional firewalls' limited capacity to interpret context means they may be unable to make an intelligent decision about how to deliver the application while also keeping services available for valid requests during a DDoS attack.

Traditional firewalls also lack specialized capabilities like SSL offload, which not only helps reduce the load on the web servers, but enables inspection, re-encryption (perhaps with a different key strength), and certificate storage. Most traditional firewalls lack the agility to react quickly to changes and emerging threats, and many have only limited ability to provide new services such as IP geolocation, traffic redirection, traffic manipulation, content scrubbing, and connection limiting.

There are several point solutions in the market that concentrate on specific problem areas, but this creates security silos that only make management and maintenance more costly, more cumbersome, and less effective.

Solution

The foundation of the application delivery firewall solution is BIG-IP® Local Traffic Manager™ (LTM). BIG-IP LTM is a purpose-built, high-performance Application Delivery Controller (ADC) designed to protect Internet data centers. The BIG-IP® system is an ICSA-certified network firewall, and the BIG-IP® Advanced Firewall Manager (AFM) module brings layer 4 network control. BIG-IP® Global Traffic Manager™ (GTM) and BIG-IP LTM high-performance SSL

Key features

- **Scalability and Performance**—Provides optimal scalability because it is built on the highest-performing ADC on the market
- **Stateful Firewall**—Maintains security with a network firewall certified by ICSA
- **Protocol Security**—Appears as a TCP peer to both client and server
- **Application Security**—Protects applications with the industry-leading web application firewall, BIG-IP® Application Security Manager™
- **DDoS Attack Prevention**—Protects against both network and application attacks, including DNS DDoS, while delivering uninterrupted service for legitimate connections
- **Dynamic Threat Defense**—Enforces protocol functions on both standard and emerging or custom protocols through F5® iRules®

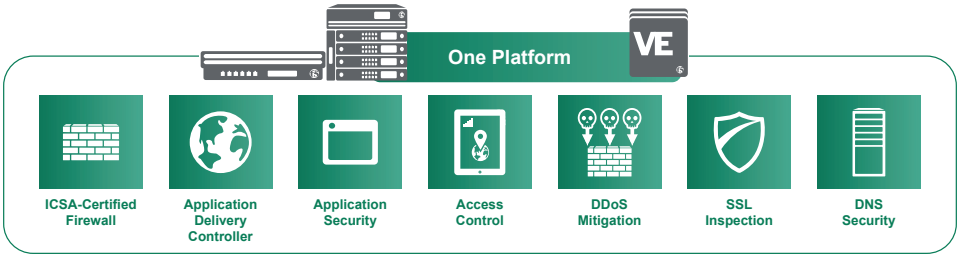
Key benefits

- **Unified Platform**—Consolidates security functions for DNS, web, access, and firewall onto a single platform, streamlining operations and lowering TCO
- **Extensible and Adaptable**—Allows multiple application services to be managed on one device and responds to new threats instantly
- **Service Provider Scale**—Scales to handle millions of connections
- **Context Aware**—Understands user context to intelligently deliver critical applications

offload protect the session at layers 5 and 6. The BIG-IP Application Security Manager (ASM) module protects the applications at layer 7, and F5 iRules provides extensibility across all layers.

The F5 application delivery firewall solution provides the following benefits:

- **Streamlined security**—BIG-IP AFM introduces an application-centric security model to firewall policies. Rather than forcing a mapping between applications and artificial constructs such as security zones, BIG-IP AFM firewall policies are oriented around the applications they protect. This reduces operational complexity and minimizes overhead between the applications team and network/security team.
- **Performance**—BIG-IP LTM manages up to 192 million concurrent connections and 320 Gbps of throughput with various timeout behaviors, buffer sizes, and other security-focused options when under attack.
- **Protocol security**—The BIG-IP system natively decodes IPv4, IPv6, TCP, HTTP, SPDY, SIP, DNS, SMTP, FTP, Diameter, and RADIUS. Organizations can control almost every element of the protocols they're deploying.
- **DDoS mitigations**—The BIG-IP system protects UDP, TCP, SIP, DNS, HTTP, SSL, and other network and application attack targets while delivering uninterrupted service for legitimate connections.
- **SSL termination**—BIG-IP LTM 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.
- **Dynamic threat mitigation**—Organizations can use iRules to create a zero day dynamic security context to react to vulnerabilities for which an associated patch has not yet been released.
- **Resource cloaking and content security**—BIG-IP LTM with iRules prevents error codes and sensitive content from being leaked.
- **Application monitoring and control**—The application delivery firewall monitors the health of applications, and has the ability to act on behavior, not just specifications and standards.



The F5 application delivery firewall brings an application-centric view to firewall security.

Learn more

For more information about BIG-IP DNS solutions, please see the following resources or search f5.com.

Product pages

BIG-IP Local Traffic Manager

BIG-IP Global Traffic Manager

BIG-IP Application Security Manager

BIG-IP Access Policy Manager

Datasheet

BIG-IP Modules

White paper

The New Data Center Firewall Paradigm

ICSA labs CERTIFIED FIREWALL - CORPORATE

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

©2012 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS23-00014 1212