High-Performance Network Firewall for Data Centers

Internet threats are widely varied and multi-layered. Although applications and their data are attackers' primary targets, many attackers gain entry at the network layer. F5® BIG-IP® Local Traffic Manager™ (LTM) has numerous security features that enable it to serve as a network firewall, so Internet data centers can deliver applications while protecting the infrastructure that supports their clients. The BIG-IP system is an ICSA Certified Network Firewall.

Evolving Threats

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

Security administrators who manage large web properties are struggling with security because traditional firewalls are not meeting fundamental 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 web sites 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, 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. An organization's inability to respond to these threats dynamically, and to minimize the exposure window, means the risk to the overall business is massive.

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 BIG-IP platform provides a unified view of layer 3 through 7 for both general and ICSA-required reporting and alerts, as well as integration with SIEM vendors. BIG-IP LTM offers native, high-performance firewall services to protect the entire infrastructure.

Key features

- **Scalable Performance**—Enables scalability with the highest performing ADC on the market
- **Stateful Firewall**—Maintains security with network firewall certified by ICSA
- **Protocol Security**—Appears as a TCP peer to both client and server
- **DDoS Attack Prevention**—Protects against DoS, SYN floods, and other network attacks while delivering uninterrupted service for legitimate connections
- **Dynamic Threat Defense**—Enforces protocol functions on both standard and emerging or custom protocols via iRules

Key benefits

- **Unified Platform**—Enables consolidation of DNS, web, access, and security functions onto a single platform
- **Business Integrity**—Keeps Internet resources safe and protects the business and brand
- **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

BIG-IP LTM is a purpose-built, high-performance Application Delivery Controller (ADC) designed to protect Internet data centers. In many instances, BIG-IP LTM can replace an existing firewall while also offering scale, performance, and persistence.

Performance: BIG-IP LTM manages up to 48 million concurrent connections and 72 Gbps of throughput with various timeout behaviors, buffer sizes, and more when under attack.

Protocol security: The BIG-IP system natively decodes IPv4, IPv6, TCP, HTTP, SIP, DNS, SMTP, FTP, Diameter, and RADIUS. Organizations can control almost every element of the protocols they're deploying.

DDoS prevention capabilities: An integrated architecture enables organizations to combine traditional firewall layers 3 and 4 with application layers 5 through 7.

DDoS mitigations: The BIG-IP system protects UDP, TCP, SIP, DNS, HTTP, SSL, and other network attack targets while delivering uninterrupted service for legitimate connections.

SSL termination: Offload computationally intensive SSL to the BIG-IP system and gain visibility into potentially harmful encrypted payloads.

Dynamic threat mitigation: iRules® provide a flexible way to enforce protocol functions on both standard and emerging or custom protocols. With iRules, organizations can 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: Prevent leaks of error codes and sensitive content.

Learn more

For more information about BIG-IP firewall solutions, please see the following resources or use the search function on f5.com.

Product page

BIG-IP Local Traffic Manager

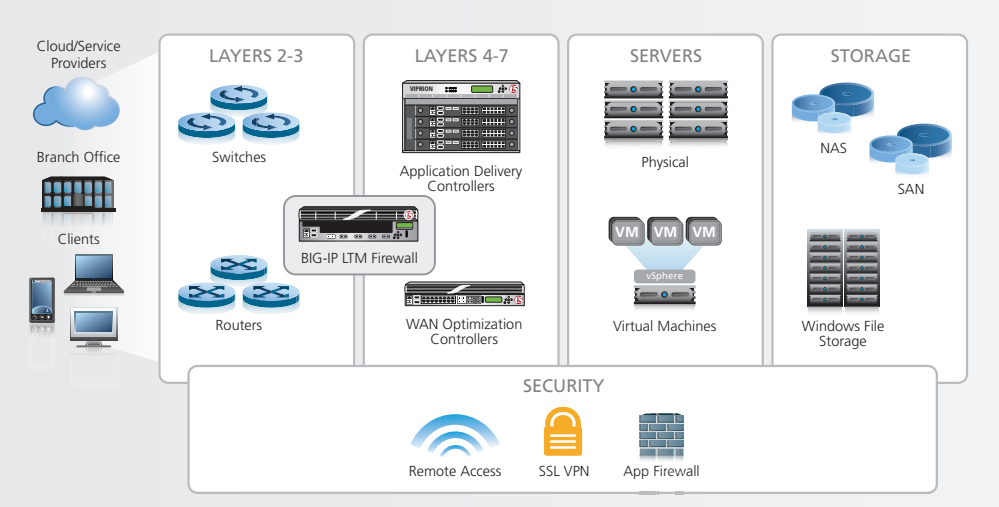
Datasheet

BIG-IP Modules

White paper

The New Data Center Firewall Paradigm

ICSA labs CERTIFIED FIREWALL - CORPORATE



Replacing stateful firewall services with BIG-IP LTM in the data center architecture.

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