f5

# Securing Your Network with BIG-IP Security Solutions for Communications Service Providers

As mobile network operators and other communications service providers migrate to all IP-based networks such as 4G LTE, network intrusions and attacks are far more likely to occur. Service providers must constantly defend against security threats to ensure the availability of their most precious resource—the network. This increases costs and operational complexity, and has a negative effect on network performance and the subscriber experience. Traditional network elements either fail under load or are unable to respond to blended attacks. To address these challenges, F5 offers integrated, high-performance security solutions that help protect the entire infrastructure and scale to perform under the most demanding conditions. F5 brings together the network, applications, data, and users under a unified security solution that traditional firewalls and point solutions cannot offer.

## Defending Against Sophisticated and Evolving Security Threats

Attacks against service provider networks continue to increase every year. With the proliferation of mobile devices, data traffic, and cloud-based services, security threats will continue to grow. The types of threats have become more varied, and the effects of a successful attack can ripple across the entire network. For example, denial-of-service (DoS) and distributed DoS (DDoS) attacks against network resources—such as DNS systems and application servers—disrupt service availability and performance. Likewise, SYN floods and IP port scan attacks against the Radio Access Network (RAN) negatively affect the reliability and availability of mobile networks. Sensitive data is also facing new security threats. Spoofing session attacks threaten sensitive subscriber information, while multi-layer DDoS, SQL injection vulnerabilities, and JSON payload violations in AJAX widgets all pose credible risks to web applications, enterprise data, and your customers' business.

Traditional network firewalls lack the intelligence, flexibility, and scalability that you need to remain effective and responsive under this growing number of sophisticated attacks. These traditional protection methods attempt to piece together many individual point products, such as network firewalls, DDoS appliances, DNS appliances, web application firewalls, and Application Delivery Controllers (ADCs)—but this approach increases complexity and latency, and adds points of failure. Even worse, such collections of point products fail to integrate information from different attack vectors or to provide a unified defense.

### Key features

- **Unmatched Capacity and Scalability**—Better protection of your network against high-volume attacks

- **Protection from the Access Network to the Data Center**—Broad defense against DDoS, SQL injection, SYN flood, and IP port scan threats

- **Visibility, Analysis, and Compliance**—Granular view of violations, attacks, and incident correlation

- **High-Performance Network Firewall**—A stateful, full-proxy firewall protects networks and applications

### Key benefits

- **Lower Hardware Costs**—Minimizes the need for multiple devices with 640 Gbps and 288 million concurrent sessions in a 16 rack-unit system

- **Simplified Hardware**—Simplifies sparing operations through linearly scalable line cards with integrated network and security functions as well as network interfaces

- **Reduced Operational Costs**—Streamlines network operations with consolidation of network and security functions on a single platform

- **Carrier-Grade Resiliency**—Reduces network downtime through hardware platforms designed with uptime in mind plus high-availability software features

- **Greater Flexibility**—Offers customizable scripting language, iRules, for control over security policies and rapid responses to new threats
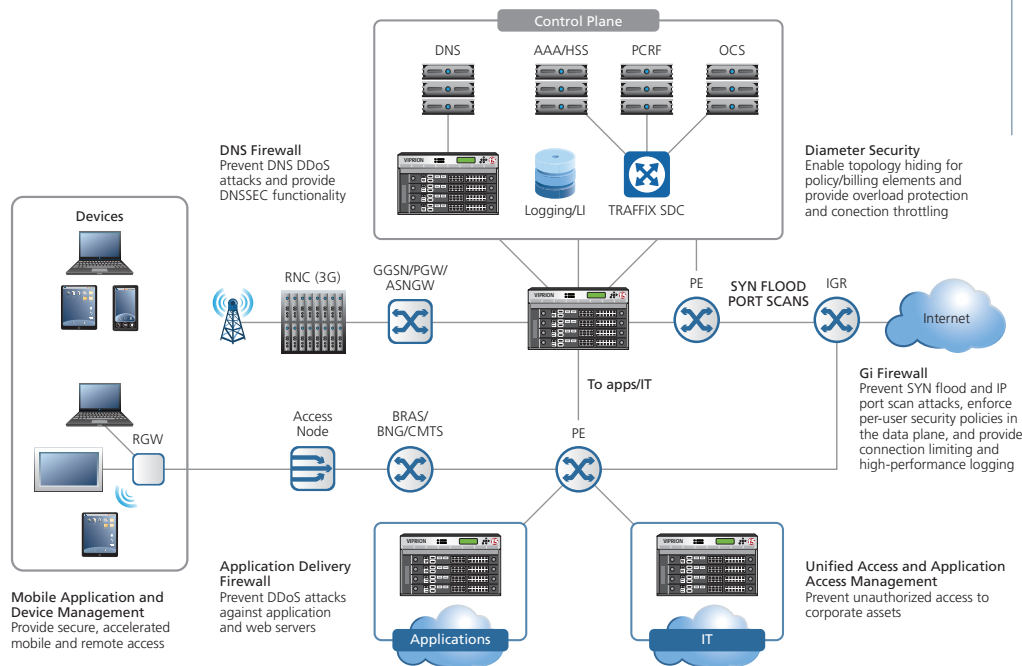
ICSAlabs
CERTIFIED FIREWALL-CORPORATE

F5's integrated, high-performance BIG-IP® security solutions for service providers, such as the F5 application delivery firewall, protect your entire infrastructure and scale to perform with intelligence and flexibility under the most demanding conditions.

BIG-IP security solutions for service providers provide:

- A stateful, full-proxy network firewall with unparalleled session scale, throughput, and connections per second.
- Defense against DDoS attacks across all layers: network, session, and application, including SYN floods and IP port scan attacks, DNS floods, and SQL injections.
- Unmatched flexibility and control of network traffic with F5® iRules®—a scripting language that enables you to create incremental security policies in a matter of hours, and to dynamically configure BIG-IP products to filter out unwanted traffic.
- Integration with leading web application scanning tools for comprehensive vulnerability assessments and automated security policy development.
- Access to the F5 DevCentral™ community of more than 100,000 developers where you can find third-party iRules enhancements, including security countermeasures.

The BIG-IP platform and application delivery firewall are ICSA Labs certified firewall solutions that simplify the network architecture, provide more flexibility for fast response to new threats, and deliver carrier-grade performance and reliability.

## Learn more

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

### Web pages

Application Delivery Firewall Solution

BIG-IP Product Suite

iRules

### Tech brief

Mitigating DDoS Attacks with F5 Technology

### Solution profiles

Securing and Scaling the Control Plane

Intelligent Traffic Management

Carrier-Grade NAT and IPv6 Services

Optimize and Monetize the Network with BIG-IP PEM



The unified F5 platform offers intelligence, flexibility, and scalability to secure multiple points in the network against a variety of threats.

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