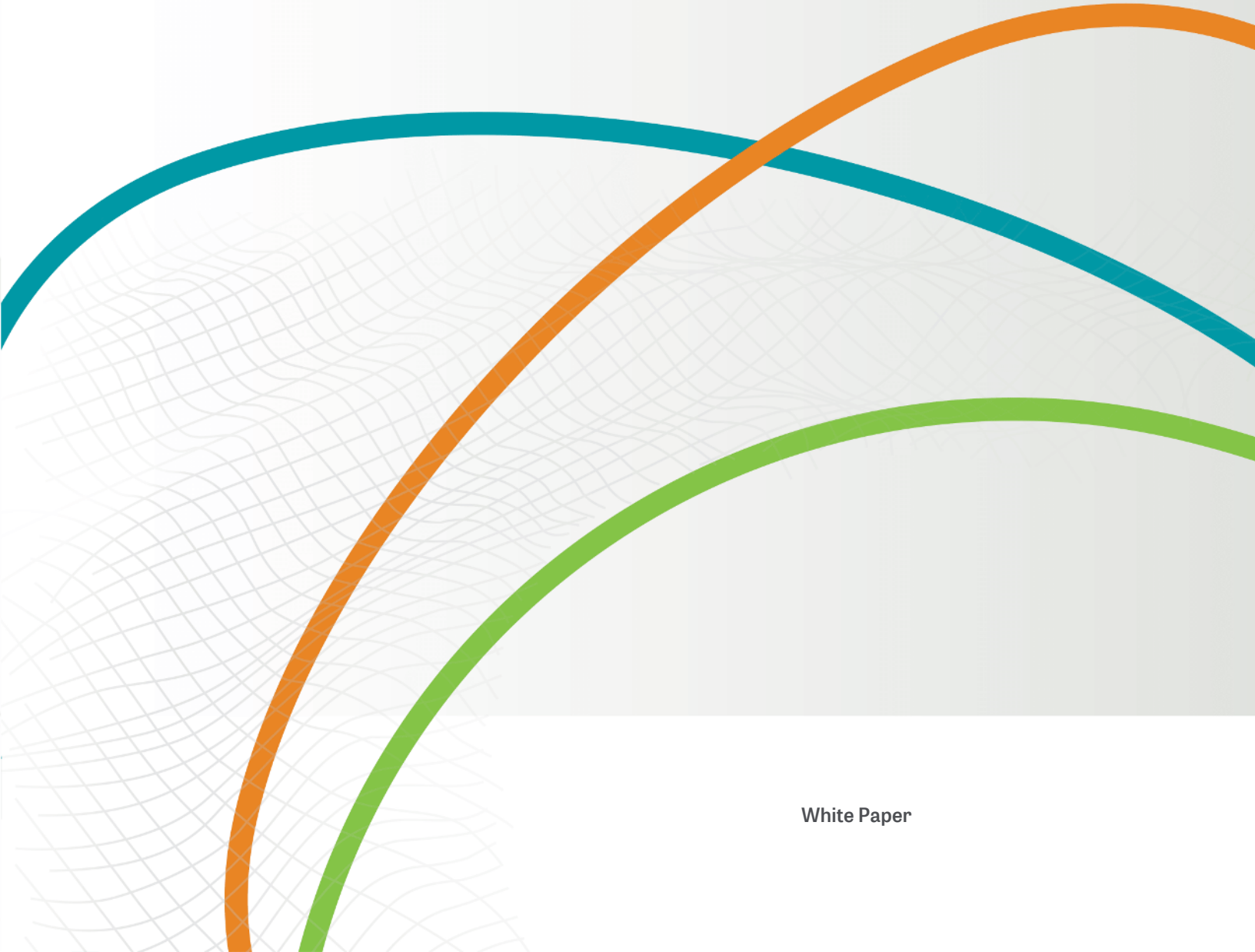
The F5 Security for Service Providers Reference Architecture

Optimize, secure, and monetize your CSP network by simplifying your delivery architecture and operations, boosting service availability and reliability, and providing application awareness and control.



White Paper

Introduction

Communications service providers (CSPs) must ensure that customers can successfully make calls and use their smartphone apps with reliable connectivity, and provide differentiated services that enhance competitiveness and can boost relatively flat revenue streams. Service providers therefore need to guarantee superior network quality without adding complexity or cost. Because security threats have a directly detrimental impact on network quality and customer experiences, security is a top priority, and CSPs must constantly defend against a growing number of threats.

Meanwhile, service providers are grappling with explosive data growth while competitive and industry pressures drive them to embark on time-consuming and costly upgrades for 4G LTE. This transition is changing the security threat landscape dramatically. In addition, IPv6 migrations and network functions virtualization (NFV) technology also are imminent or already underway. As a result, CSPs need multi-faceted support to ensure that their networks remain predictable, reliable, and available.

F5 offers a suite of dynamic, multi-layered security solutions capable of meeting these CSP needs across the entire service delivery architecture. This solution breadth, which is necessary to protect the entire CSP infrastructure, cannot be provided by traditional firewalls and point products. F5 security solutions help CSPs to optimize, secure, and monetize their networks by simplifying their delivery architectures and operations, boosting service availability and reliability, and providing application awareness and control while reducing costs.

Challenges

The security landscape for service providers is changing dramatically as the transition to 4G LTE makes the service delivery architecture flatter, more open, and all IP-based. As a result, service providers are facing increasingly complex, multi-faceted, blended, and large attacks on subscribers and the services infrastructure. Malicious behavior such as DoS attacks, botnets, identity theft, and compromised systems must be prevented from affecting the network, as must unintentional security-related issues such as signaling storms and misconfigured systems.

At the same time, to enhance business performance CSPs need to reduce costs and improve the operational efficiency of their networks—just as they are incurring significant expenses to deploy 4G LTE services and securely manage exploding traffic, which continues to strain the entire infrastructure. Finally, in the new 4G LTE architectures, strategic network elements like policy management, DNS addressing, and IMS services rely on a new signaling infrastructure that must also be protected.

In this environment, the security challenges that service providers face include:

- Threats to service availability such as DoS and distributed denial-of-service (DDoS) attacks, IP port sweeps, and signaling storms.
- Theft of data ranging from personal and banking information to corporate assets and passwords.
- Malware on the device and server side that degrades performance or interferes with service.
- Advanced persistent threats (APT) that compromise network and data center assets due to insufficient access controls.
- Web application attacks such as the OWASP Top 10.

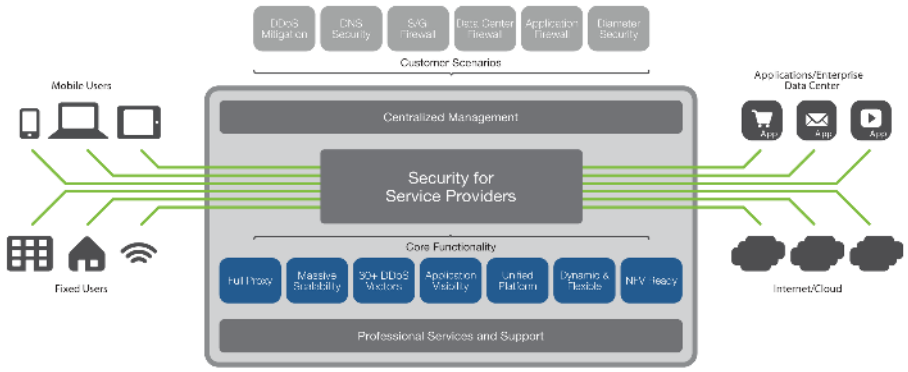
Traditional network firewalls cannot provide the needed scalability, flexibility, and intelligence, nor are they easy to manage. CSPs need to remain responsive to provide effective security under a growing number of increasingly sophisticated attacks. In addition, threats do not originate solely from the Internet; attacks by DDoS botnets, malware, and other sources now originate from mobile devices, too. Because the threats are now bi-directional, security solutions also must be able to provide bi-directional protection to the network infrastructure.

Other traditional protection methods attempt to piece together many individual products, such as DDoS appliances, DNS appliances, web application firewalls, and load balancers—but this approach increases architectural complexity and latency and adds points of failure into the network. In addition, from an operations perspective, managing and supporting the products of multiple security vendors with disparate systems and technologies is extremely difficult and resource intensive. Even worse, collections of point products fail to integrate information from different attack vectors or provide a unified defense. Comprehensive intelligence about attacks is critical, because when the network experiences unresolved security issues, service calls increase and customer satisfaction drops, increasing churn.

Solutions

Successful security demands a multi-layered solutions approach. CSPs need to design service delivery architectures that implement broad-spectrum security throughout their networks, on their users' devices, and within their data centers. Within the network, solutions need to offer protection in both the data and control planes: in the data plane to safeguard the mobile packet core infrastructure, and in the control plane to protect the messaging and signaling infrastructure. In the data center, solutions need to offer application- level protection for the data infrastructure as well as hosted applications themselves.

F5 offers a suite of dynamic, multi-layered security solutions that help service providers protect the entire infrastructure and scale to perform with intelligence and flexibility under the most demanding conditions. Unlike competing point products that resolve only a limited set of security issues, F5 security solutions rely on a unified platform and unmatched capabilities that can address threats throughout the CSP infrastructure. As a result, these solutions help service providers to secure, optimize, and monetize their networks.



The F5 Security for Service Providers solution

F5 platforms are certified firewall solutions that simplify the network architecture, provide more flexibility for fast response to new threats, and deliver carrier-grade performance and reliability. These universal platform capabilities are implemented across F5 solutions that are intended to achieve different functions in CSPs' core infrastructure:

- Packet core (S/Gi) network security
- Messaging and signaling protocol security
- Internet data center security

The solutions fit within a single service delivery architecture that delivers the highest security posture and optimal experiences for subscribers.

F5 does not offer a single security product for this architecture. Instead, the solution is delivered by the combination of intelligent and scalable components within the F5 security portfolio: a unified platform that comprises F5 BIG-IP Advanced Firewall Manager (AFM), BIG-IP Application Security Manager (ASM), BIG-IP Global Traffic Manager (GTM), BIG-IP Local Traffic Manager (LTM), and the F5 Traffix Signaling Delivery Controller (SDC).

- BIG-IP 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 ASM, an advanced web application firewall, uses F5's deep application fluency to detect and mitigate HTTP-based attacks.
- BIG-IP GTM is a scalable DNS and DNSSEC solution that mitigates DNS-based network and session attacks on the DNS infrastructure.
- BIG-IP LTM is an application delivery solution that adds content-based, intelligent traffic management.
- Traffix SDC is a Diameter routing solution that provides topology hiding and signaling storm protection from third-party partners.

Why This Solution Works

F5 security solutions offer important capabilities that extend throughout the service architecture: scalability, flexibility, application visibility, manageability, and performance. As a result, CSPs can avoid supporting multiple point products from disparate vendors in different parts of the service delivery architecture. This enables broad-spectrum s ecurity without the cost and operational complexity of a multi-vendor environment.

Rather, by delivering dynamic, multi-layered security capabilities from a unified platform, F5 solutions simplify CSP architectures and operations, boost service availability and reliability, provide application awareness, and reduce capital and operating costs. The result is the superior network quality that can directly improve customer satisfaction.

Key Capabilities and Benefits

F5 security solutions offer a number of important capabilities to meet the needs of CSPs across their service delivery architectures. These capabilities are inherent in the unified platform to enable wide realization of their benefits.

- A full-proxy architecture: This architecture enables F5 devices to terminate, inspect, and forward sessions to deliver the highest visibility and control.
- Scale and performance: 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.
- A unified platform: The F5 platform delivers multiple security solutions as

software- enabled services on a common system architecture to simplify operations and reduce total costs of ownership.

- Flexibility and programmability: The F5 platform offers the flexibility of customized security policy through the F5 iRules scripting language. It also provides automated programmability and orchestration integration through the F5 iControl and F5 iCall APIs. A user-customizable framework simplifies and speeds security deployments throughout the network via F5 iApps Templates.
- Hardware and software virtual editions: F5 platforms are supported on dedicated, high-performance hardware and software-enabled virtual editions that are NFV- ready to provide the ultimate operational flexibility.
- Availability and reliability: The system provides high availability and reliability with hardware redundancy, synchronization, health monitoring, and automatic failover/ failback capabilities.
- Manageability: A sophisticated management suite enables CSPs to centrally manage firewall policies, orient security policies logically around specific applications, monitor the effectiveness of policies across all devices, and audit policy changes.
- DDoS awareness and protection for all layers: BIG-IP AFM is DDoS aware and can automatically prevent floods and handle dozens of Layer 2 through 4 attacks in hardware deployments at line rates. F5 DDoS solutions provide security at the network, session, and application layers.

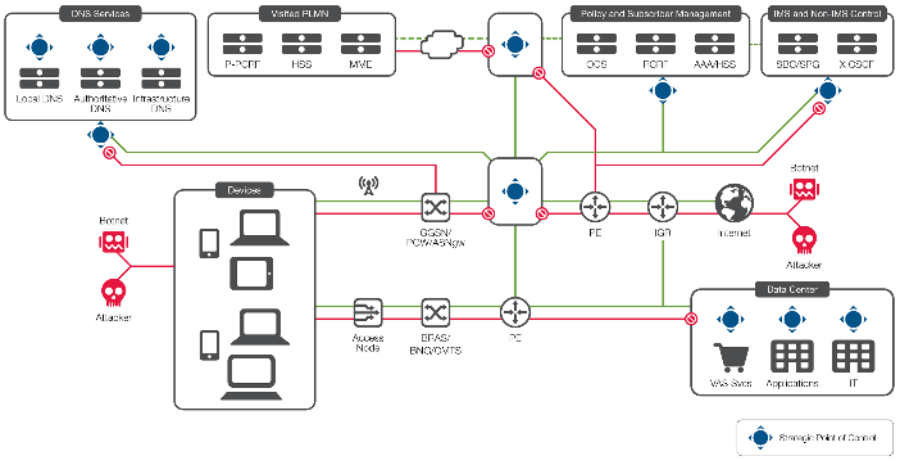
Business Benefits

F5 security solutions offer a number of benefits to CSPs.

- Simplify the architecture and operations: The F5 unified platform encompasses a range of security solutions for the data and signaling networks as well as for the data center, enabling service providers to simplify their security architectures with fewer point products and vendors. The comprehensive nature of the solution platform also enables reduced sparing, reduced training and troubleshooting, and centralized security policy control across the entire delivery infrastructure.
- Enhance performance: F5 products consolidate security functions into a unified, high-capacity platform that reduces the number of network hops and latency and delivers hardware- accelerated security performance.
- Defend against volumetric attacks with unparalleled scalability: F5 security solutions provide service providers with a highly scalable platform that enables superior throughput, connections per second, and concurrent sessions to protect high traffic environments against volumetric attacks.
- Improve service experiences: F5 solutions enable service providers to deploy per-user (rather than per-IP address) policies to protect against attacks and threats and ensure better service availability and reliability. As a result, service providers can maintain subscriber trust and protect their service quality, subscriber data, and reputations from damaging security attacks.
- Reduce costs: The F5 platform consolidates security functions into a unified framework to reduce CapEx and OpEx. In addition, the high scalability and

capacity of the F5 platform deliver a lower total cost of ownership because they reduce overall device management time, footprint costs, and power costs.

- Increase operational flexibility: Service providers can respond to zero-day attacks and other threats via the iRules scripting language, without signature updates or new software upgrades. With iRules, F5 solutions can communicate and interact with orchestration systems for policy updates and external monitoring, while the iControl API provides a smooth interface with logging and reporting systems.
- Choose hardware or virtual editions: F5 security services can be provided from dedicated hardware—from a range of appliances to chassis-based systems—as well as from software- based virtual editions. The combination provides pay-as-you-grow flexibility to match systems to needs and budgets. F5 also offers multi-tenancy Virtual Clustered Multiprocessing (vCMP) for resource sharing on appliances and chassis blades.



The F5 Security for Service Providers architecture

Conclusion

F5 security for service providers delivers a dynamic, multi-layered security architecture for CSPs grappling with expanding security threats—not to mention explosive data growth, flat revenue streams, 4G LTE upgrades, and rapidly shifting standards and technologies. To provide superior and differentiated customer experiences in this challenging environment, CSPs must operate high-quality networks that are predictable, reliable, available, and neither complex nor too costly. The F5 suite for service providers helps protect the entire infrastructure and scales to perform with intelligence and flexibility under the most demanding conditions.

Unlike competitive products that resolve only a limited set of security issues, F5 security solutions rely on a unified, scalable platform that can address threats throughout the CSP infrastructure. F5 security solutions also offer important capabilities across the service architecture to enhance scalability, flexibility, application visibility, manageability, and performance. As a result, CSPs can simplify the service delivery architecture and provide broad-spectrum security without the complexity or cost of a multi-vendor environment built on point solutions.

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com