Simplifying Security for Mobile Networks

Communications service providers face an array of complex challenges, from network growth and increasing security threats to technology transitions. The comprehensive F5 S/Gi firewall solution ensures security and high availability, provides insight for new services and revenues to protect margins, and positions CSPs for more growth in the future.

White Paper

by Geoffrey Huang

Introduction

At a time of growing demand on their mobile networks, communications service providers (CSPs) are increasingly challenged to provide highly available service and excellent subscriber experiences—without further eroding service margins. Several trends are working against CSPs: the exploding number of subscriber devices, the expanding use of bandwidth-intensive applications such as video streaming, and two significant and simultaneous technology transitions—the IPv4 to IPv6 migration and the 3G to 4G/LTE migration.

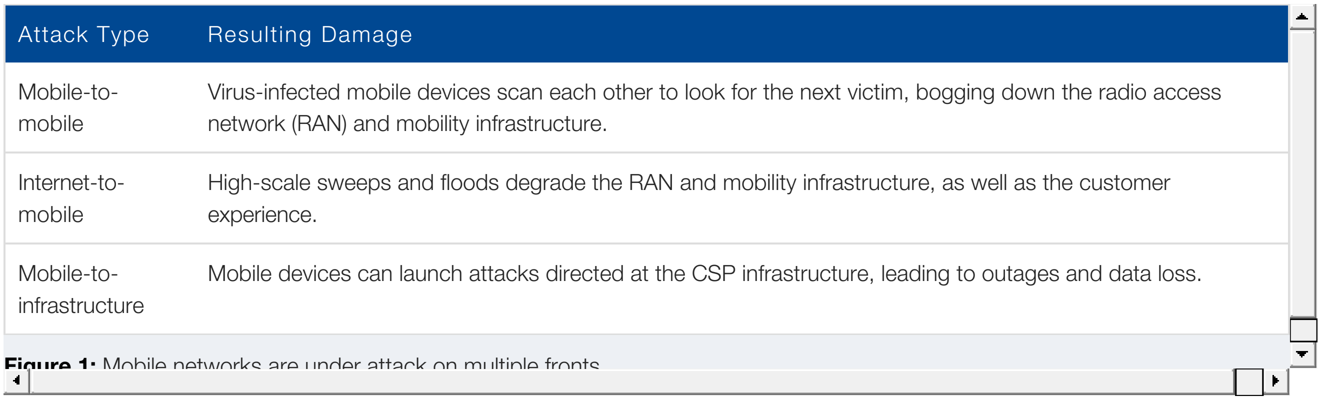
In the face of these challenges, CSPs still need to plan for growth. The shift to LTE —which provides higher bandwidth and more reliable connections—virtually guarantees additional bandwidth consumption by subscribers, as well as a substantial increase in the number of connections per subscriber. Meanwhile, malicious attackers are advancing on another front, threatening the availability of the mobility infrastructure itself.

Providing security for the mobility infrastructure and for mobile subscriber connections has been the task of network firewalls deployed at the Gi interface for 3G networks and at the SGi interface for 4G/LTE networks. Until now, the only options have been legacy firewalls with limited scale and performance. While some of these legacy firewalls offer new line cards with better scaling, they still only represent incremental scale improvement—not the generational shift in architecture needed to match the generational shift in mobile network standards. As a consequence of the limitations of such legacy systems, CSPs planning for growth must include additional instances of firewalls to keep pace with demands while maintaining secure services. This leads to not only a significant increase in capital expenditures, but also additional strain on the network operations team—and the resulting increase in operational costs.

Fortunately, there is another solution that incorporates high availability, security, and immense scalability, while positioning CSPs with the flexibility and unified management necessary to ease technology transitions and infrastructure changes. That answer is the F5 S/Gi firewall solution.

Ensuring Network Availability

The first challenge to network availability is malicious activity. The IP infrastructure of mobile CSP networks is subject to the same increase in attacks endured by wire-line and application networks today. With mobile networks, attacks can be mobile-to-mobile, Internet-to-mobile, or mobile-to-infrastructure.



Attack Type	Resulting Damage
Mobile-to-mobile	Virus-infected mobile devices scan each other to look for the next victim, bogging down the radio access network (RAN) and mobility infrastructure.
Internet-to-mobile	High-scale sweeps and floods degrade the RAN and mobility infrastructure, as well as the customer experience.
Mobile-to-infrastructure	Mobile devices can launch attacks directed at the CSP infrastructure, leading to outages and data loss.

Figure 1: Mobile networks are under attack on multiple fronts

In all cases, the result is the same as in any distributed denial-of-service (DDoS) attack: the network degrades or becomes unavailable.

Just as with a wire-line infrastructure, the first line of defense for a mobility infrastructure is the firewall. Basic perimeter protection is necessary to separate the mobility infrastructure from the Internet. For GSM networks, this perimeter is protected at the Gi interface, and CDMA networks are similarly protected at an analogous part of the mobile network. In 4G/LTE networks, perimeter protection is done at the SGi interface.

Preparing for the Future

In the face of increasing attacks, CSPs still need to run their businesses: securing subscribers today while simultaneously planning for the future. As part of a CSP's day-to-day network operations, standard functions such as service enforcement are critical. For instance, a CSP must segment its IP network, allowing only specific devices on its mobile infrastructure to gain access to or from internal and external applications and services. Such segmentation commonly:

- Defines security policies that enforce the acceptable-use policy for different subscriber plans.
- Customizes security policies for enterprise customers.
- Provides restricted network access for over-the-air firmware updates.
- Restricts Internet endpoints connecting to mobile devices.
- Limits abusive applications and services.

Aside from these standard aspects of the mobility infrastructure, CSPs are busy rolling out (or planning the roll out of) 4G/LTE. Without a doubt, LTE has significant implications for CSP operations. On the one hand, the technology brings increased bandwidth per subscriber, but on the other, modern devices consume more concurrent connections due to their increased processing power and high-bandwidth network access. CSPs that already have LTE networks need to execute their deployments efficiently—controlling expenses while deploying long-life equipment that can scale as needed. CSPs that have not yet rolled out LTE need to begin planning today for tomorrow's network. This means deploying 3G infrastructure equipment that not only has the capacity for scaling vertically to accommodate the higher bandwidth and connection needs of 4G/LTE, but also the ability to scale horizontally to add additional functionality without more equipment.

With all this going on, CSPs must also manage IPv4 address exhaustion and the migration to IPv6. This migration pressure is exacerbated by the increasing number of subscriber devices and the demands of all-IP LTE infrastructure deployments. Migration to a voice-over-LTE (VoLTE) approach makes the problem even worse, as it requires always-on connectivity. CSPs must protect their security infrastructure investments and minimize operational impacts by deploying systems that handle IPv6 with minimal performance or scale degradation compared to IPv4. These systems must also handle the transition from IPv4 to IPv6 seamlessly.

Beyond the need to support IPv6, CSPs are also looking for ways to maximize the efficiency of routing traffic within their networks. Visibility into subscriber traffic patterns is essential for this kind of efficiency, which helps reduce costs by gaining the maximum utilization of existing network resources. Paramount to maximizing efficiency is the insight that comes from visibility into subscriber traffic patterns. CSPs can use this insight to offer new types of services that can increase the revenue per subscriber.

Massive Density: The F5 Way

The F5 solution to these issues is the S/Gi firewall, which separates the mobility infrastructure from threats on the Internet as well as threats from other subscribers. The F5 S/Gi firewall is so named because it is ideal for both 3G deployments at the Gi interface and 4G/LTE deployments at the SGi interface. The foundation of this solution is F5 BIG-IP Advanced Firewall Manager (AFM), the highest scaling, highest performing network firewall on the market. The S/Gi firewall solution optionally includes BIG-IP Carrier-Grade NAT (CGNAT), which enables high-scale, seamless migration of IPv4 to IPv6 on a single platform. To manage firewall policies across the network, F5 offers BIG-IQ Security, a central management solution built on top of the extensible BIG-IQ platform, which facilitates the federation of application network and delivery services across clouds, regardless of their underlying network standards frameworks. Finally, CSPs can take advantage of the F5 intelligent services framework, which enables the deployment of additional network and security functions on the same BIG-IP platform.

The World's Most Scalable, Highest Performing Firewall

Handling up to 576 million concurrent connections on a single, unified device, BIG-IP AFM has the capacity to meet the future needs of the most demanding networks. BIG-IP AFM also has the performance, with up to 640 Gbps of throughput and the ability to process 8 million connections per second. When deployed on F5 VIPRION chassis platforms, BIG-IP AFM provides exceptional linear scalability. When CSPs need more capacity or performance, they simply add a blade to the chassis. At the same time, the VIPRION platform streamlines network operations with a single type of blade that provides network interface ports, security, and management services. This not only simplifies expansion, but also eases the management of spare blades for contingency planning.

As part of its core functionality, the BIG-IP AFM network firewall enables operators to delineate network boundaries based on the common security building blocks: prefixes, protocols, ports, VLANs, route domains, and virtual servers. Thus CSPs can secure service offerings and implement flexible security models with the lowest cost.

Defense Against Attacks

BIG-IP AFM defends the mobility infrastructure and mobile subscribers from attacks, regardless of the source of the attacks. This capability includes mitigation of large-scale DDoS attacks such as network floods, port scans and sweeps, or connection floods. By detecting and stopping these types of attacks, BIG-IP AFM can prevent congestion and overloading of the control and bearer planes of the radio access network. BIG-IP AFM protection against DDoS attack vectors continues to increase with each version released, and with many BIG-IP platforms, DDoS protection functions are accelerated with specialized hardware.

BIG-IP AFM offers the protection of a full-proxy firewall, meaning that it fully terminates and inspects incoming client connections for threats. The end result, and the benefit to CSPs, is the assurance of network availability and an improved subscriber experience.

Built with Availability in Mind

As with all F5 solutions, BIG-IP AFM, BIG-IP CGNAT, and the other modules that comprise F5's S/Gi firewall solution are built with availability in mind. At the platform level, F5 hardware architectures provide redundant power supplies that can be hot-swapped. On the multi-line-card VIPRION chassis, the line cards can also be hot-swapped.

At the system level, BIG-IP solutions provide active/active and active/standby high availability, with multiple levels of redundancy. At layer 2, BIG-IP devices support link aggregation technologies such as LACP. At layer 3, the BIG-IP system achieves redundancy by monitoring next-hop status, routing table information, and ICMP probes.

Finally, at the software level, the F5 TMOS operating system that forms the basis of the BIG-IP system provides configuration and session synchronization. Advanced functionality such as automatic failback—the ability to revert to the primary system in a high-availability cluster—is also supported.

High-Scale, Seamless IPv4 to IPv6 Transition

Since the network perimeter separates the "inside" of the mobility infrastructure from the "outside" Internet, it makes an ideal location to handle address translation. Networks that currently run IPv4 addressing are faced with a dwindling pool of available public addresses—but the number of subscriber devices these networks need to support is increasing. BIG-IP CGNAT solves this problem, and it does so at a high scale.

At the same time, the BIG-IP system natively supports IPv6 while minimizing degradation in scale. BIG-IP CGNAT simplifies the migration from IPv4 to IPv6, supporting a variety of transition technologies: NAT64, DNS64, DS-Lite, and deterministic NAT. This means that CSPs can deploy the S/Gi firewall solution for both IPv4 and IPv6 on a single platform. Combine this advantage with massive scalability, and the network investment is protected for years to come.

Centralized Management with BIG-IQ Security

To manage policies for a network of multiple firewalls, F5 offers BIG-IQ Security, an advanced central management solution. BIG-IQ Security provides several key features to simplify the management of distributed network security:

- Management authority over BIG-IP AFM instances.
- Firewall policy management, including policy search, viewing, creation, editing, and deployment, with a contextually aware, modern user interface.
- Audit logging that delivers the ability to track changes for compliance and troubleshooting. The log includes information about who made a change, when the change was made, and what the change was.
- Monitoring that enables administrators to view the activity across policies and provides a useful way to tune policies.

Simplify and Secure the Network

The F5 S/Gi firewall solution takes advantage of the F5 intelligent services framework. This means that CSPs can layer additional functionality within a common architecture, simplifying the network even further. This additional functionality is available as licensable solution modules, eliminating the need for, and administrative challenges of, separate hardware from different vendors. Optional modules include networking functions such as:

- **BIG-IP Policy Enforcement Manager** (PEM), providing carrier-class subscriber and application visibility, policy enforcement, and traffic steering. This module helps CSPs not only maximize the efficiency of the existing infrastructure, but also delivers insights into new types of subscriber services to offer.
- **BIG-IP Local Traffic Manager** (LTM), providing high-scale traffic management and load balancing.
- **BIG-IP Global Traffic Manager** (GTM), providing a complete DNS-based infrastructure solution including DNS DDoS protection.

Security for the Next-Generation Mobile Network

Available security modules include:

- **BIG-IP Application Security Manager** (ASM), providing security for web-based applications as well as application-layer DDoS protection.

- **BIG-IP Access Policy Manager** (APM), providing flexible application access management and user access management.

Additionally, added contextual information is available through IP intelligence and geolocation, which gives CSPs the ability to make policy decisions based on IP address reputations and location information.

Conclusion

CSPs are under consistent pressure to streamline operations and increase service margins. Yet the simultaneous complexities of defending against attacks while preparing for disruptive technology shifts are complicating matters. The F5 S/Gi firewall solution enables CSPs to protect their mobility infrastructures and subscribers with BIG-IP AFM, the highest-scaling, highest-performing network firewall on the market. Likewise, CSPs can deploy BIG-IP CGNAT for high-scale IPv4 address management and IPv4 to IPv6 migration.

The results of this unmatched service performance and density are significant cost reduction and network simplification, with room to grow to meet future scale demands. The vertical scalability of the S/Gi firewall solution is matched by the solution's horizontal scalability—that is, its ability to add functionality within a common solution architecture. This flexibility is made possible by the F5 intelligent services framework, which consolidates multiple network and security functions within one unified framework.

With the S/Gi firewall solution, F5 enables CSPs to deliver an excellent subscriber experience by ensuring the security and availability of the mobile network. The massive scalability and excellent programmability of F5 products protect providers from an unknown future full of complex threats, bringing certainty of highly available security, at scale, to that future.

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