Securing LTE Networks—What, Why, and How

As security threats evolve, service providers must implement comprehensive security for both their LTE network infrastructures and connected devices to protect network and service performance, customer satisfaction, and revenue growth.

White Paper

by F5

Introduction

Service providers are faced with a number of complex challenges today as they seek to evolve and "future-proof" their networks to accommodate increasing network traffic, massive scaling requirements, virtualization and orchestration needs, cost controls, and expansion into new revenue sources.

At the same time, operators are experiencing security incidents and attacks resembling those that Internet service providers have been experiencing for years. Network congestion, service degradation or complete outage, and exposure of user information and signaling messages are serious concerns. Core network elements and support infrastructure are more prone to outside threats than ever before. Advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and DNS-level attacks threaten network and service availability and performance. Ensuring the security, performance, and availability of high-speed mobile networks is thus of critical importance to both the service providers who own and operate them and their subscribers. Furthermore, it is now critical to protect the network itself as well as the consumer devices connected to it.

F5's carrier-grade security solutions protect both the long-term evolution (LTE) network and its subscribers from the threats they face today. These solutions can provide service providers with security in a changing landscape, safeguard their brand reputations, protect against next-generation attacks, and enable expansion into new revenue sources.

Network Evolution and the Evolving Threat Landscape

Traditionally, service provider security has focused almost entirely upon protecting the network infrastructure, with little or no thought given to subscriber endpoint devices. However, as network technologies evolve and performance increases through 3G, 4G, 5G, and beyond, the legacy operational viewpoint—that simply protecting the network itself is enough—must change.

Legacy operational models designed for fixed network infrastructure and low performance subscriber devices are no longer sufficient as service provider architectures evolve to dynamic, virtualized, and orchestrated infrastructure models. Service provider networks, especially the evolving LTE networks, must now be designed to remain secure everywhere so they can deliver reliable, high performance service in virtualized, cloud, and software-defined networking (SDN) environments. In addition, delivering infrastructure security in the twenty-first century requires service providers to take a new focus on consumer device protection, as those devices represent a new and very serious risk vector.

F5 provides the solutions to these critical challenges—via purpose-built hardware as well as virtual offerings—to deliver the security, performance, and availability operators need as their networks grow and evolve.

Evolving subscriber devices and why they matter

Mobile telephony devices have evolved over the years and are now every bit as powerful and ubiquitous as regular computers. At the same time, the volume and variety of data they can store have increased dramatically, making these devices themselves an attractive target for attackers. Similarly, the threat landscape facing mobile networks has broadened from the earlier SMS-based attacks to now include risks at the device, application, and network levels.

With more than two thirds of online adults using free, unsecured public WiFi services, the security threat becomes obvious. As Bryan Sartin, director at Verizon Business, states, "In two years, more data will be stolen from mobile devices than from servers and applications."

Another risk to consider in addition to malicious attacker traffic is chatty applications and the load they can generate on signaling and ancillary support systems. With a single connection request for popular applications, including mail, news, and social media, often producing 30 or more connection and signaling events, the potential for millions of subscriber devices to overload service provider signaling and support infrastructure is also a very real concern. If it's not designed and built with sufficient capacity and security, there is significant potential for a small number of bad actors to disrupt the carrier's signalling and support infrastructure.

The threat landscape targeting consumers and their devices also continues to evolve. With the increasing variety and sophistication of threat vectors, including social engineering, malware, DDoS attacks, and more, it is now becoming critical for modern LTE network operators to protect their clients from potential attacks in order to protect themselves.

Why Is Security So Important to the Operator?

As technologies evolve and network cost/performance ratios improve, operators must seek to defray the projected decline in revenues from pure connectivity and legacy services. While most operators are seeking to reduce the costs of their network infrastructure, this alone will not ensure profitable growth, so operators are seeking sources of additional service revenue.

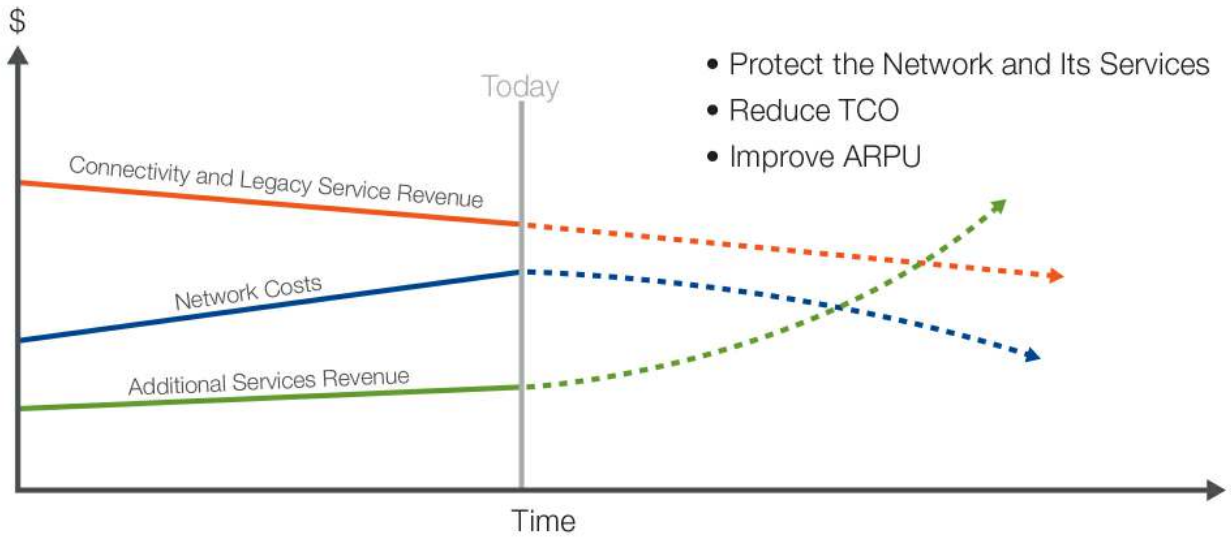

Figure 1: Network security is critical to ensure positive customer experience and profitable growth.

By protecting the network itself, operators can improve the quality of experience (QoE) provided by the network to subscribers, thus protecting both existing and new services the network supports. This in turn will protect operators from subscriber churn and declines in average revenue per user (ARPU). Thus by strengthening the security of the network, operators may boost overall revenues and reduce their total cost of ownership (TCO).

What risks do LTE networks face?

Mobile operators face unique risks due to the multitude of threat vectors involved; threats exist at the device, network, and application layers, and each must be considered and secured against to protect both the network and subscribers from attack.

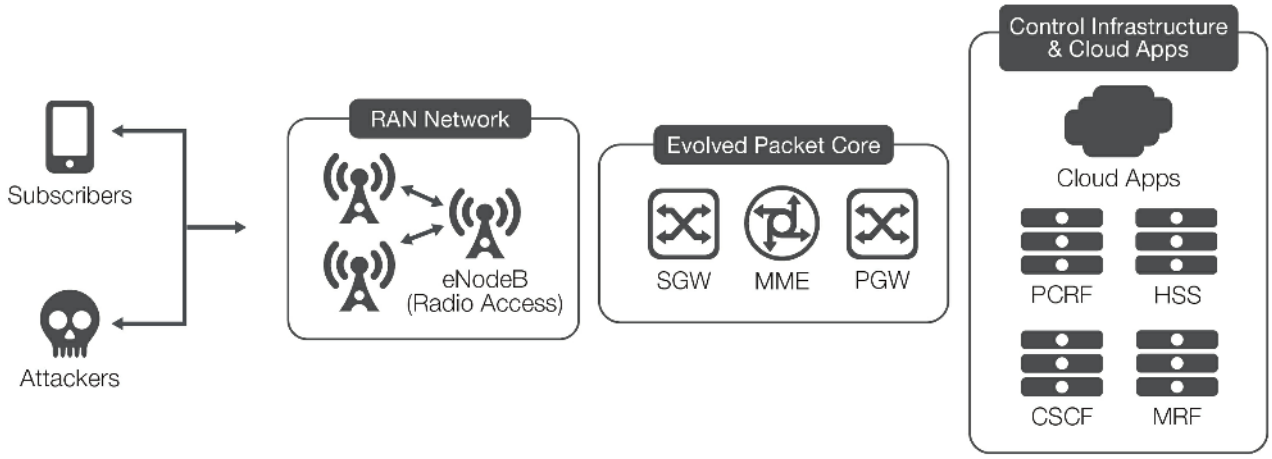

Figure 2: Mobile networks may be attacked from many sources at multiple locations.

Device-level attacks, which may be caused by malware or bots infecting subscribers' devices, can generate spurious or attack traffic, create signaling storms into the network, and drain device batteries. The network itself may be subject to radio access network (RAN) and core network resource exhaustion, terms and conditions (T&C) violations, and attacks on DNS, billing, and signaling infrastructure. Additionally, attacks targeted at the application layer may include server-side malware, application-level (protocol-specific) DDoS attacks, or layer 7, web application level threats.

All these risk factors must be considered for the operator to ensure stable and secure network operation, to protect the infrastructure, and to protect and satisfy customers. More specifically, operators must put controls and security policies into place in multiple domains to protect each aspect of the mobile network.

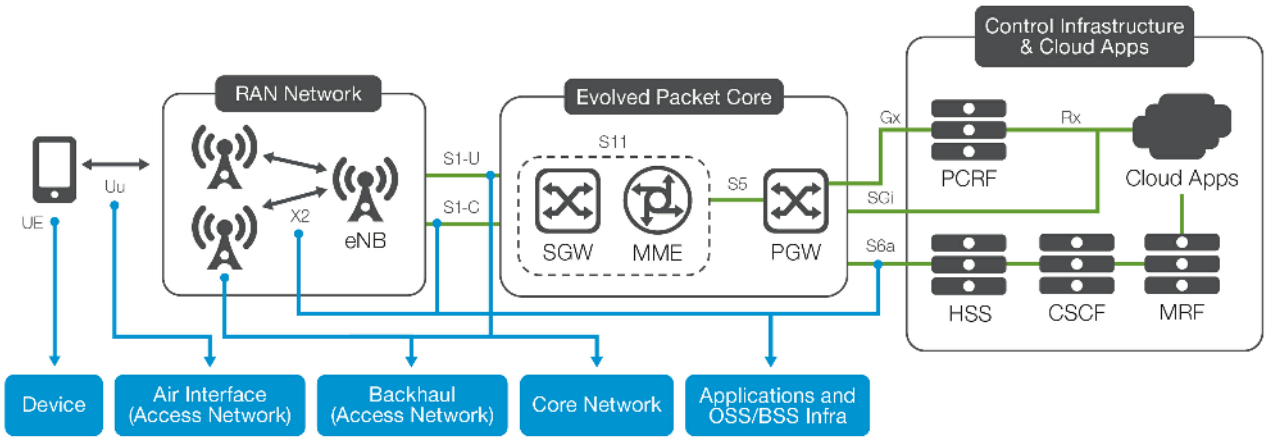

Figure 3: LTE networks contain multiple attack surfaces.

To protect the network fully requires a policy of true multi-layer, multi-domain security. Security at the mobile device, air interface, access network, core network—and also at the applications, operational support systems (OSS), and business support systems (BSS)—must all be protected. Until all of these layers are secure, operators face the risk of attack via multiple, evolving threat vectors.

Attack Scenarios and Associated Impacts

There are many potential attacks that can harm LTE networks and their subscribers, and it is critical to design and implement a holistic security architecture to protect against them all. While the damage from many of the various attacks types, such as that of a DDoS attack, will be both broad and immediately apparent, several attack types will only produce localized service degradation and are thus much more difficult to troubleshoot.

Examples of this latter type of attack include RAN connection exhaustion, which leads to localized outages, and consumer device battery drain problems, which may lead to device returns. Similarly, attacks on the billing infrastructure will cause customer dissatisfaction and service calls.

All types of attack—if successful—will decrease customer satisfaction and increase operator costs, so it is critical to both understand the risks and develop an end-to-end mitigation strategy.

Scenario 1: Attacks from the Internet side

If operators do not pay sufficient attention to inbound security from their upstream Internet connection, attackers can launch flooding or DoS/DDoS attacks toward network subscribers. The diagram below shows such an attack scenario, with mobile subscribers attacked from upstream.

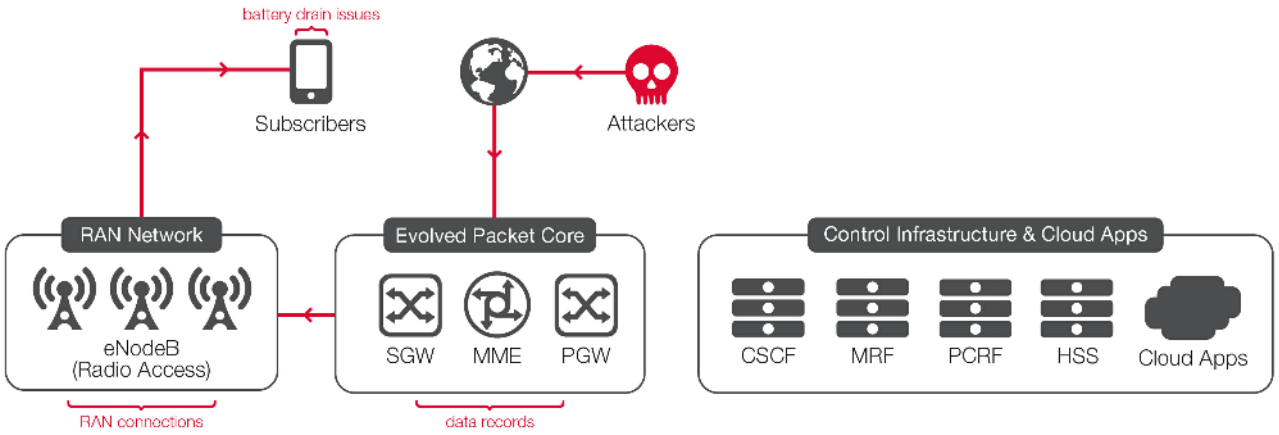

Figure 4: Devices may be attacked from the Internet side of the mobile network.

The potential damage of such an attack could include:

- Mobile device battery drain.
- Data volume use and resulting billing complaints.
- RAN connection exhaustion.

Scenario 2: Attacks from the mobile side

Attackers may also target other mobile device users from the mobile side of a single operator's network. In this scenario, one or more mobile attackers can target network subscribers with DoS, flooding or DDoS attacks across the operator's access and core network infrastructure.

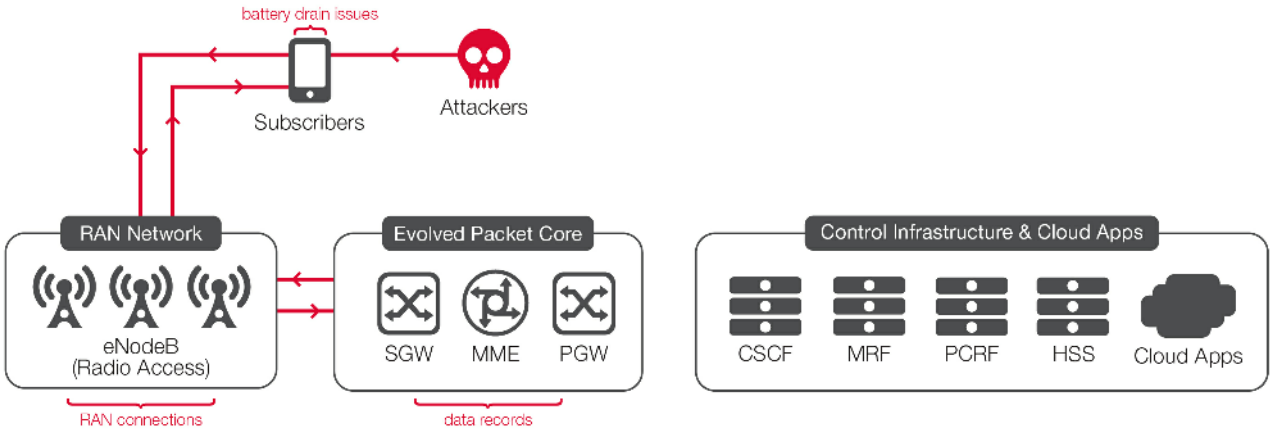

Figure 5: Devices also may be attacked from the mobile side of the network.

As with an Internet-side attack, this attack also potentially could cause multiple problems, including:

1. Mobile device battery drain.
2. Data volume use leading to billing complaints.
3. RAN connection exhaustion.

Scenario 3: DNS/Signaling attacks from the mobile side

Rather than targeting devices, attacks from the mobile side may instead target the operator's signaling infrastructure, including DNS and charging and billing systems.

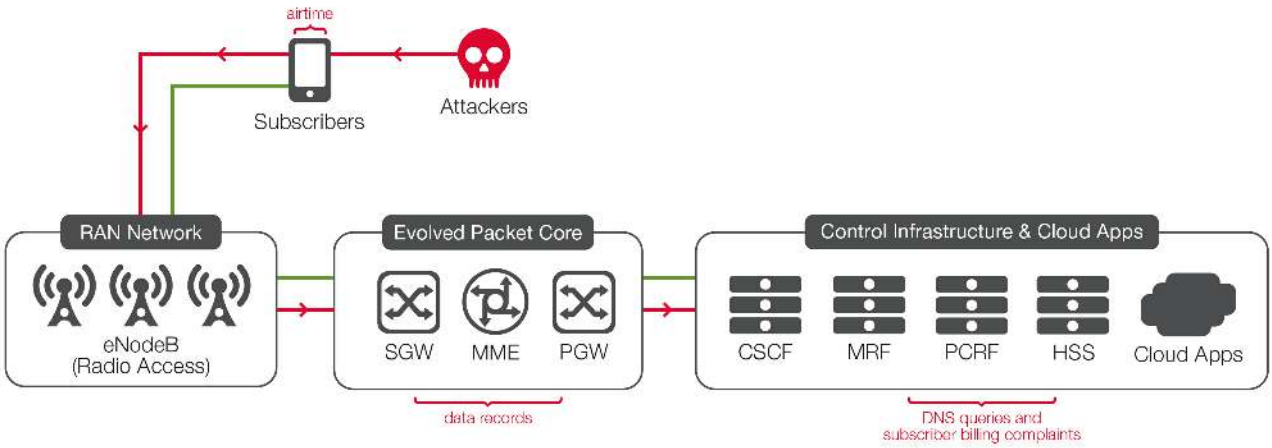

Figure 6: Intensive DNS and signaling attacks can originate from a mobile device.

The risks of an attack of this nature include:

1. Airtime/RAN resource exhaustion.
2. Subscriber data volume use and billing complaints.
3. DNS infrastructure overload and collapse.
4. Subscriber data record errors.

As you can see, it can indeed be a complex task to understand and address all the potential security risks faced by an LTE network operator. Fortunately, F5 can offer tailored, carrier-grade solutions to mitigate these risks.

Protect Your LTE Network—Everywhere—with F5

The world's largest communication service providers trust F5 to help them secure and simplify their networks, improve their quality of service, and increase profitability. Today, F5 is in a unique position to help service providers manage the data explosion and seamlessly migrate to IPv6 with a broad portfolio of carrier-grade solutions that deliver multiple services, including security, on a unified platform. The F5 platform enables service providers to decrease time to market, reduce capital and operating costs, improve service delivery performance and security, and monetize network services.

F5's service provider solution set is composed of solutions for security, network functions virtualization (NFV), data traffic management, and Diameter and DNS signaling. All F5 solutions are available either on purpose-built, high-performance physical hardware platforms or on a variety of virtual or cloud platforms. In addition, management and orchestration for these solutions is available via the F5® BIG-IQ® management platform as well as APIs from each product.

As networks continue to grow and scale massively, the characteristics of the traffic running on them also evolve, leading to a greater number of TCP connections, with shorter and more frequent connections becoming dominant. The implication of this evolution of application traffic is that the service provider network now requires infrastructure solutions that support very high TCP connection scaling**.** Legacy security solutions can't scale and don't deliver the performance needed for modern, high-performance networks and applications; they will not be sufficient to deliver security, performance, and reliability in today's environment.

Virtual or overlay networks and virtualized network services, as used to create over-the-top (OTT) or wholesale network services also create another level of complexity as scalability requirements increase and new services and applications with strict latency requirements are run across these networks.

All of this transformation drives the critical requirement for security and traffic management solutions that can deliver massive scale and high performance. F5 solutions, which do both, are perfectly suited to these new service and operating environments.

F5 solutions for LTE security

Carrier-grade service provider solutions from F5 enable operators to secure their LTE infrastructures, subscriber devices, and OSS applications from potential attackers. Specifically, deploying local and global traffic management solutions such as F5 BIG-IP® Local Traffic Manager™ (LTM) and BIG-IP® DNS inside the carrier data center—along with F5 firewall solutions for layer 4 and layer 7, such as BIG-IP® Advanced Firewall Manager™ (AFM) and BIG-IP® Application Security Manager™ (ASM)—will protect mobile customers from attacks from the Internet while protecting the data center from attacks from the mobile side.

Within the data center itself, the layer 4 firewall from F5 can offload security functions from the operator's core infrastructure, increasing security and lowering costs. Additionally, BIG-IP® Carrier-Grad NAT (CGNAT) provides the carrier-grade NAT scalability and performance required to support millions of users. User traffic payload visibility and enforcement can also be provided by BIG-IP® Policy Enforcement Manager™ (PEM) to secure and monetize service traffic.

The BIG-IP physical and virtual platforms also provide a high-performance and highly scalable SSL encryption and decryption endpoint to enable and enforce secure connections to and from the operator core, thus securing the access network infrastructure. Using the security platforms of BIG-IP AFM and BIG-IP ASM at peering junctions protects both the network infrastructure and mobile customers against attacks from roaming network partners.

Finally, OSS and BSS systems, including subscriber databases, DNS, and other signaling and charging systems within the operator's network can be protected against attack from rogue employees or Internet and mobile threats by BIG-IP AFM, BIG-IP DNS, and the F5 Traffix® Signaling Delivery Controller™ (SDC). F5 also offers a full suite of management and orchestration options for next-generation architectures like SDN and NFV, including northbound APIs and the BIG-IQ management platform.

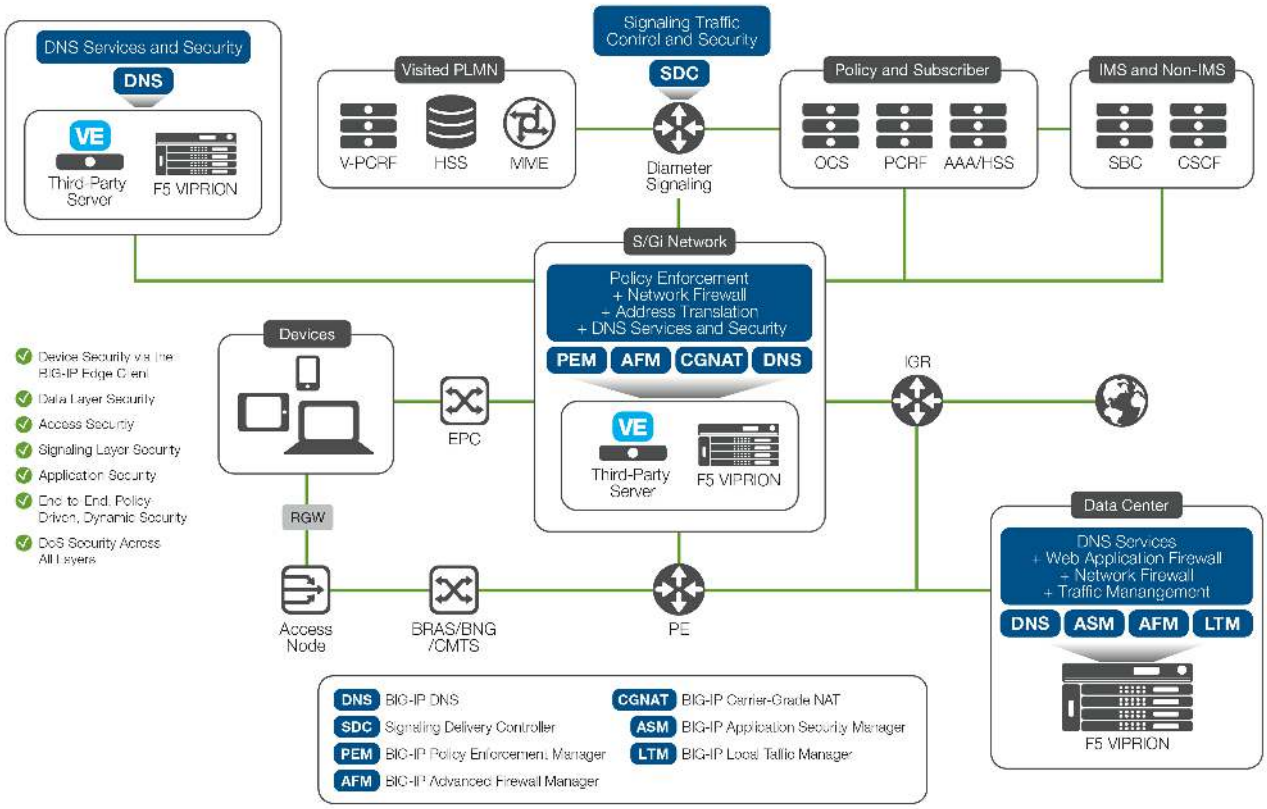

Figure 7: The suite of F5 carrier-grade solutions can ensure comprehensive security from the core network to user devices.

In short, F5 offers comprehensive service provider security solutions that can secure:

1. Subscriber mobile devices.
2. The data layer of the S/Gi network itself, as well as data center and peering connections.
3. The access network for both wireless and wireline connections.
4. The signalling layer with the Traffix SDC plus BIG-IP DNS services.
5. Applications for the virtualed network functions (VNFs) within the data center.

All of the above services can be matched end-to-end across the network and enforced with a consistent set of policies. Finally, DDoS protection can be delivered across all layers of the network, on all BIG-IP hardware or virtual edition platforms.

Benefits of security solutions from F5

Service provider security and traffic management solutions from F5 enable network operators to:

- **Maintain service provider security in a changing landscape.** F5 offers service providers a comprehensive, security solution with massive scalability, programmability, and extensibility.
- **Simplify.** Since all the above functions (except the Traffix SDC) are available on a single BIG-IP platform, an operator can collapse and simplify its data center infrastructure and network operations, thus reducing CapEx,

OpEx, and TCO.

- **Protect the service provider's brand.** F5 security solutions fit within a single service delivery architecture that delivers a proactive security posture and optimal experiences for subscribers.
- **Secure against next-generation attacks.** F5 security solutions provide service providers with a highly scalable platform that enables superior throughput, connection rates, and concurrent sessions while protecting against the next generation of attacks.
- **Secure expansion into new revenue sources.** F5 protects and ensures availability of service provider networks and application infrastructure under the most demanding conditions, empowering secure delivery of new network applications and services that drive revenue growth.

Conclusion

Service providers' primary concern continues to be protecting all their critical network infrastructure from attacks, but user equipment attacks are now also firmly within the scope of concern. While in the past some service providers may have categorized attacks on mobile devices as being outside the realm of their responsibilities, most now fully understand the potential harm of those attacks, and that they must have tools to prevent these incidents from occurring.

Compounding the service providers' challenge to ensure end-to-end security for all service delivery is that the line between user equipment attacks and network element attacks continues to blur. This drives the need for service providers to implement a scalable, advanced, and comprehensive security framework that protects their networks and customers while providing tools and capabilities to address new sophisticated threats as they emerge. Implementing a strong security posture is now more critical than ever, and mobile service providers can best secure their evolving LTE networks with the extensive service provider security capabilities that only F5 can provide.

Learn more about the F5 service provider solution set at f5.com/solutions/service-provider.

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