# LEADING SERVICE PROVIDER DELIVERS OUTSTANDING 5G NETWORK PERFORMANCE

**The combination of high-performance hardware and advanced virtualization software has been the key to unlocking new 5G services for this major Service Provider.**

## NEW 5G MARKETS REQUIRE MASSIVE NETWORK SCALING.

The potential of 5G has transcended mobile devices. Supported by F5, a major Service Provider recently launched fixed-mobile services that directly compete with in-home cable providers. This eliminates the need to run coaxial or fiber optic cable to a residence and is being offered to consumers to compete with cable services. Other possible 5G service offerings under consideration include virtual reality viewing at sporting events, 5G-enabled autonomous vehicles and drones, improved driver safety, and enhanced emergency services.

Launching these new services, especially in high-density population areas, requires massive scaling of existing networks in addition to deployment of new network resources. Rather than just ripping and replacing older network components, this Service Provider was able to utilize a combination of software and hardware upgrades, coupled with increased automation, to efficiently and economically enable massive scaling. This made it possible for them to deliver the extraordinary number of connections per second, high bandwidth, and low latency required for these new 5G services.

## MAXIMIZE NETWORK THROUGHPUT WITH HIGH-PERFORMANCE HARDWARE AND SOFTWARE INNOVATIONS.

The Service Provider was able to upgrade its existing F5® VIPRION® platform with higher performance 100G interfaces, eliminating the need to replace chassis that were still usable. Furthermore, Field Programmable Gate Array (FPGA) technology provides hardware accelerated flow processing to provide low latency processing and reduced CPU usage. Enhancements will soon be introduced that enable prioritized flow processing, programmed to reserve FPGA processing for higher priority flows. This feature is software configured and significantly reduces CPU usage, adding to overall efficiencies and performance enhancements.

F5 network functions virtualization (NFV) is used in test environments. This makes it possible to test numerous solutions quickly, identify those that work well, and discard the solutions that don't. This greatly speeds up new services creation while minimizing costs.

## SECURITY IS STILL PARAMOUNT.

5G promises to deliver 100 times the bandwidth of existing networks. These high-performance networks must be adequately protected against both targeted and automated threats. Proper scaling to ensure high-performance security for the 5G forwarding plane requires the use of high-performance hardware. This is especially true for firewall and distributed denial-of-service (DDoS) mitigation functionality that protects infrastructure from threats.

The Service Provider adopted an F5 security solution that can support 3G, 4G, and 5G on the same platform. It instituted granular controls enabling users to set thresholds by maximum packets per second, both manually and through auto tuning. Based on these thresholds, machine learning is used to handle attacks more intelligently. The Service Provider installed 5G-ready DDoS mitigation in an always-on (in-line) configuration versus a traffic-redirect solution. This minimizes the time between when an attack is detected, when mitigation starts, and when the attacks are fully mitigated. This helps reduce downtime and ensure network availability.

F5 BIG-IQ® Centralized Management is used to measure device health and investigate DDoS attacks. In Figure 1, DNS DDoS attack details can be observed by all managed F5 BIG-IP® products. It shows attack type, size, flow history, source and destination IP address, Geo IP map, and status. The Attack Type details show In/Drop requests (the amount of traffic that has been filtered); Status (whether the attack is ongoing or has been mitigated); Start/End Time (the event start and end date of the attack); and how much traffic has been observed by each BIG-IP module.

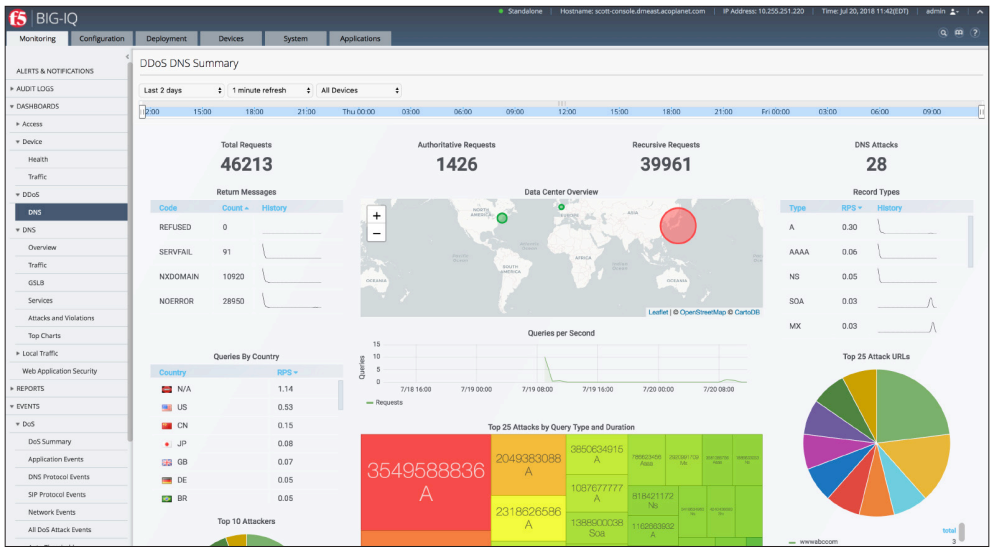


**Figure 1:** F5 BIG-IQ DNS and DDoS Traffic Dashboard

This solution also provides a holistic view of the infrastructure as shown in Figure 2. Service Providers typically prefer a high-level, at-a-glance view of DNS and DDoS traffic details from which they can drill down into a specific attack or review current traffic trends.

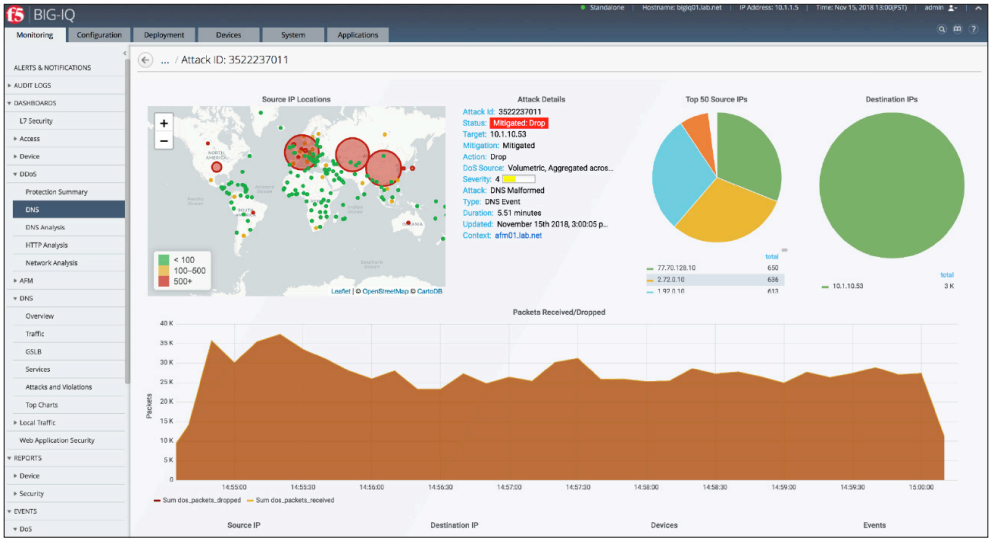


**Figure 2:** F5 BIG-IQ Infrastructure Dashboard

## COLLABORATION LEADS TO SUCCESS.

F5 technical and service delivery teams have collaborated with this Service Provider for many years, helping it to implement cost effective, flexible, and scalable network solutions. This close collaboration helped deliver the high-throughput, high-bandwidth, and low-latency solutions required for its new 5G services, and enabled it to extend the life of its existing equipment. The Service Provider was also able to implement a best-in-class 5G DDoS security solution, helping it defend both its network infrastructure and mobile subscribers from attacks, regardless of the source.

**For more information visit: f5.com/5G**