The perfect storm: Security at massive scale to support the IoT & 4G/5G networks

Peter Margaris, 2016-22-02

The mobile industry is in the midst of a major transformation unlike any that we've ever seen. We all see it happening and moving forward at a neck-breaking pace as mobile service providers continue to evolve their networks to 4G, 5G and beyond to keep up with consumer demand and grow their revenues. There are more devices, more data, more applications, rapidly evolving networks, and new service delivery models evolving to leverage the cloud. More opportunities for service providers, and yet more challenges. It's really a perfect storm. A storm that opens up significant challenges for service providers to not only scale and continue to provide high quality of service, but mostly to deal with rapidly evolving security threats across their networks, across all of the new applications and services that are delivered, and across all the devices and end points that will continue to proliferate. As service providers navigate their way towards supporting a 5G connected world, security at scale has become their greatest concern.

Increasing security concerns for service providers

In a recent research study conducted by F5 and Heavy Reading, service providers from all over the world were surveyed[1]. Over 65% expressed "concern" or "extreme concern" about security impacts going forward to every single domain in their network, as well as the devices that are connecting to their networks. 83% of surveyed mobile operators are particularly concerned about securing their data centers while 76% of respondents raised concerns about securing their IMS networks, their SGi Networks, and consumer devices and endpoints.

These security concerns are well founded when you consider that service providers are literally transforming their entire network architectures on this path to 5G. They are rapidly moving into uncharted waters and battling to remain competitive and profitable while migrating their networks to accommodate a potential tidal wave of connected devices. Industry-wide projections are proclaiming that there will be as many as 7-8 connected devices per person by 2020 from the Internet of Things (IoT) – devices such as wearables, smartwatches, home appliances, sensors that monitor just about anything, and connected cars and homes. The list of devices that will connect to mobile networks is endless.

Dealing with security and massive industry growth

In addition to the large numbers of connected devices, average mobile traffic per month is also projected to grow 6-fold between 2015 and 2020 – from an average of 495 Mb/month/user to 3.3 Gb/month/user – according to the recent Cisco Visual Networking Index report[2]. So how will service providers be able to deal with such challenging circumstances in an industry that is undergoing such a massive evolution? It's not something that's years away, it's happening now, and innovative and transformative solutions are needed. Security solutions of the past cannot keep up, which will leave networks vulnerable and service provider revenues at risk. High performance platforms and virtual solutions that are specifically tailored for 4G and 5G network environments are needed that can:

- Efficiently scale to handle the extremely high concurrency from IoT devices and from the next generation of services, and

- Provide a multi-faceted security posture that mitigates new threats, DDoS attacks, and evolving vulnerabilities across all devices, all network domains, and all applications wherever they may be hosted.

F5 delivers the highest performing carrier class firewall solutions – tailored for 4G/5G environments

By leveraging F5's high-performing purpose-built platforms and highly scalable virtual network functions (VNFs), service providers can most effectively and efficiently secure devices, networks, and services in a 4G/5G connected world while maintaining the highest possible quality of service and the lowest total cost of ownership. In these future network environments the handling of very high connections per second (CPS) has become the key scaling factor. Customers deploying F5 security solutions are achieving significant performance benefits, and have paved their way to evolve and secure their networks and services.

Purpose-built platforms and Virtual Network Functions

The extensive F5 suite of security software solutions can be delivered on top of the high performance and highly programmable F5 BIG-IP platforms, and also on top of commercial off-the-shelf (COTS) platforms as virtual network functions (VNFs) in evolving virtual network architectures. F5's breadth of features, functionalities, programmability, and extensive protocol support combined with these security software modules creates a flexible, agile, and feature-rich, carrier-class network firewall (CCNFW) that's needed to mitigate all threats across all evolving network domains and also enables an effective and efficient migration of networks towards 4G, 5G, and cloud.

F5 at Mobile World Congress

Come and visit F5 at our booth while at Mobile World Congress (located in Hall 5, Stand G11) where we will be highlighting all of our solutions – showing how the breadth of these solutions can help service providers realize their operationalization goals associated with 4G, 5G, and beyond, and stay ahead of the massive mobile evolution taking place.

References:

[1] Service Provider Survey: The Future of Mobile Service Delivery:
https://f5.com/mobile-service-delivery-report (f5.com registration required)

[2] Cisco Visual Networking Index:
http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com