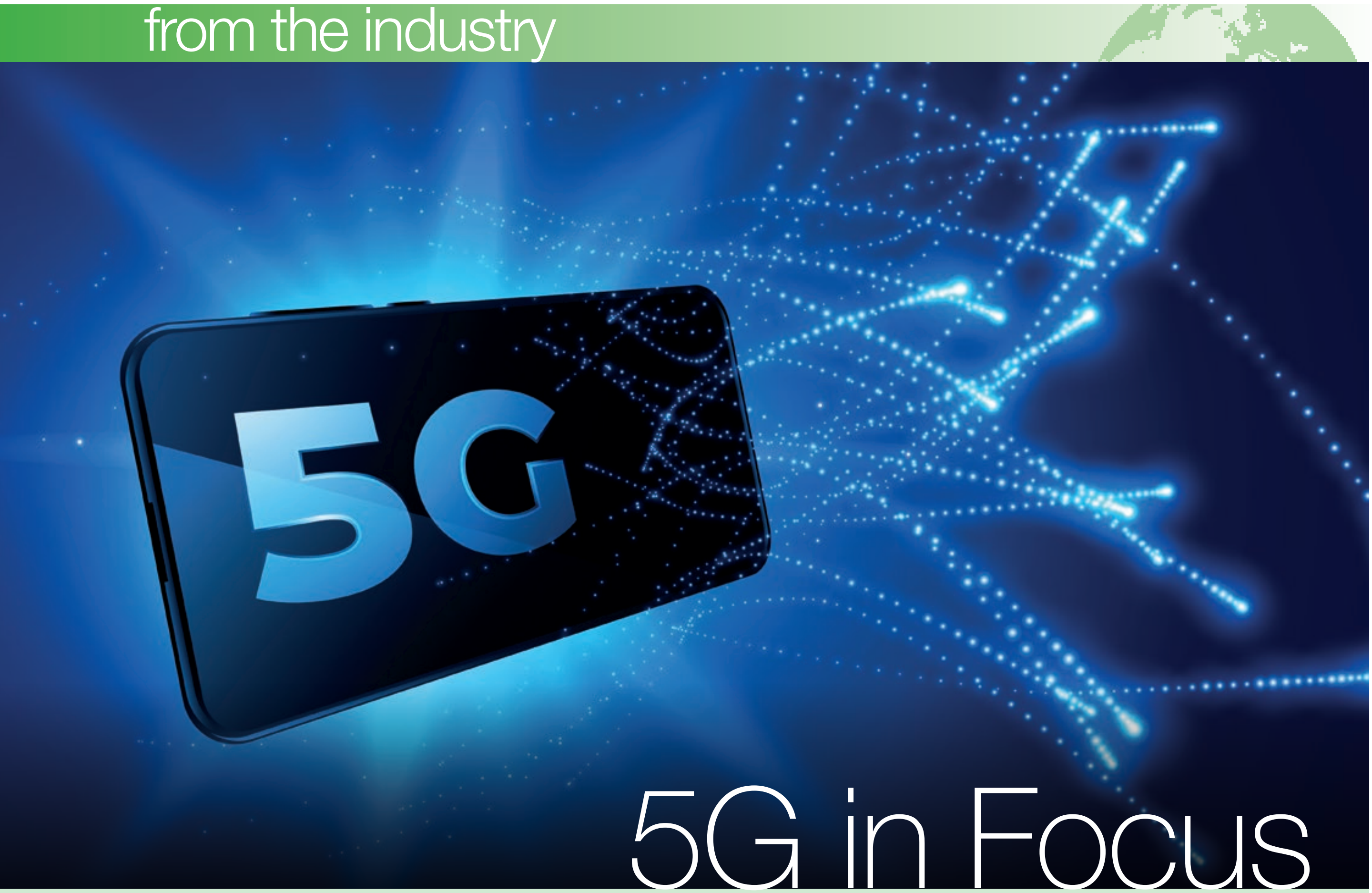

5G in Focus

By Adrian Taylor, Regional VP of Sales, A10 Networks

According to a new report, it is security (not COVID-19), that challenges the commercial deployment of 5G. Five key solutions are presented to ensure that migration to 5G is smooth and, more importantly, secure.

Since the beginning of the current pandemic, false and unsubstantiated rumours of 5G and its impact on people's health have been prevalent on social media. Phone masts have reportedly been damaged or destroyed in several European countries. The problem has been particularly acute in the UK, where dozens of towers were targeted and engineers abused as they worked, according to media reports.

The scale of the problem prompted the World Health Organisation (WHO), the UN agency which is leading the response to the pandemic, to add the 5G conspiracy to its COVID-19 myth busters article, which highlighted that "viruses cannot travel on radio waves/mobile networks. COVID-19 is spreading in many countries that do not have 5G mobile networks."

In the midst of this controversy, A10 Networks released a report entitled, "Toward a More Secure 5G World," which highlighted how COVID-19 may result in some short-term delays for operators, but ultimately it demonstrates a global need for higher speed, higher capacity 5G networks and the applications and use cases that they enable. The study also found that 81% believe industry progress toward 5G is moving rapidly, mostly in major markets or at least in line with expectations.

An eye on security

Whilst the report shows that 5G adoption is scaling rapidly, one of the main concerns from the report surrounded cybersecurity. As 5G networks expand, so does the explosive growth in network traffic, connected devices and mission-critical IoT use cases. This will impact network security and reliability more than ever. The report supported this view, with 99% respondents expecting 5G networks to increase security and reliability concerns and 93% having or expecting to change security investments in light of 5G.

To address this challenge, service providers need highly cost-efficient security solutions that offer flexibility, scalability and protection as they evolve their networks to 5G and integrate cloud and edge capabilities. This means a comprehensive security stack at service provider scale with other functions

> **“Operators must meet growing security challenges while also providing a seamless subscriber experience.”**

most needed in mobile networks, including a firewall for all network peering points, deep packet inspection (DPI), carrier-grade network address translation (CGNAT) and IPv6 migration, integrated distributed denial of service (DDoS) threat protection, intelligent traffic steering and analytics.

Below is a blueprint of five of the key solutions required for a successful migration to 5G.

1. Gi-LAN Security – Gi/SGi Firewall

Significant threats to mobile subscribers and networks come through the internet interface – the Gi/SGi. As traffic volume, devices and cybercriminal expertise increases, so do these threats. An integrated Gi/SGi firewall protects infrastructure and subscribers as well as delivering the performance required by mobile carriers. The Gi/SGi firewall solution meets both current and future traffic requirements for any service provider. This comprehensive and consolidated approach provides strong performance, efficiency and scale to protect the mobile infrastructure while reducing OPEX and CAPEX costs. Service providers can also use a Gi/SGi firewall solution in a virtual form factor for flexible, easy-to-deploy and on-demand, software-based deployment.

2. Mobile Roaming Security – GTP Firewall

The GTP protocol used in the roaming and other EPC interfaces has known vulnerabilities that can be readily exploited by malicious actors. Operators must meet growing security challenges while also providing a seamless subscriber experience – wherever they travel, whatever devices are used and whichever network is accessed.

A GTP firewall provides extensive capabilities including stateful inspection, rate limiting and filtering of traffic for protocol abnormalities, invalid messages and other suspicious indicators. It protects against GTP protocol vulnerabilities such as fraudulent use, confidentiality breaches, DDoS attacks by malicious peers and other threats.

A GTP firewall can be inserted into multiple interfaces carrying the GTP traffic. In the primary use case, it is inserted on S5-Gn and S8-Gp (roaming) interfaces. The GTP firewall provides scalability and supports uninterrupted operations while protecting subscribers and the mobile core against GTP-based threats such as information leaks, malicious packet attacks, fraud and DDoS attacks through GTP interfaces in the access networks and GRX/IPX interconnect.

3. Network Slicing – Intelligent Traffic Steering

Network slicing will allow mobile operators to offer security and other capabilities tailored to each vertical application and to capture revenue from these diverse use cases, without losing the economies of scale of common infrastructure. Network slicing isolates each use case or service from one another so that the services can be independently deployed, managed securely and delivered in a robust way.

This solution identifies specific types of traffic by multiple criteria including radio access type, IP address, DNS address, device type, destination, subscriber ID and other parameters and then redirects these “slices” of traffic to value-added service platforms, such as protection platforms for deeper threat analysis and scrubbing.

This re-direction can be based on either static policy or dynamic factors. This solution enables differentiated treatment to the developing 5G use cases, deepens the security posture and boosts revenue opportunity without adding unnecessary inspection load on the entire network.

4. Network Wide DDoS Detection and Mitigation System

Mobile operators must maintain high network availability at all times. DDoS attacks target mobile networks and their subscribers with high-volume message floods that overwhelm infrastructure and can cause service degradation and network outages.

Now, targeted attacks can also come from any network peering point and include both volumetric and lower volume, sophisticated attacks against specific network elements or important applications of key enterprise customers.

Over-provisioning of network elements to meet rising threat volume or simply blocking traffic during an attack increases costs and can result in service denial for critical traffic. Operators need a more cost-efficient and comprehensive approach that quickly detects and mitigates DDoS and infrastructure attacks across the entire mobile network without denying service to important traffic. Service providers can achieve full DDoS resilience and improve security by using a layered approach for detecting and mitigating attacks of all types and sizes before attackers take down their targets.

5. Secure, Efficient MEC

Multi-Access Edge Compute (MEC) architecture is often part of the 5G transition plan. In a MEC architecture, network traffic processing functions move from a centralised data centre or mobile core to several distribution points that are located closer to the user at the "edge". A distributed architecture with thousands of nodes increases management difficulty and requires a high level of automation and analytics for deployment, management and security and operational changes. A10 Networks offers a Thunder CFW solution in a software-based or hardware form factor for firewall, CGNAT and IPv6 migration, traffic steering and other functions.

As we reach the halfway point of 2020, the study indicates that major mobile carriers around the world are on track with their 5G plans, and more expect to begin commercial buildouts in the coming months. Mobile operators globally therefore need to proactively prepare for the demands of a new virtualised and secure 5G world.

This means boosting security at key protection points like the mobile edge, deploying a cloud-native infrastructure, consolidating network functions, leveraging new CI/CD integrations and DevOps automation tools, and moving to an agile and hyperscale service-based architecture as much as possible.

All these improvements will pay dividends immediately with existing networks and move carriers closer to their ultimate goals for broader 5G adoption.

For more information, see https://www.a10networks.com/