5G SECURITY SOLUTION GUIDE

SECURE AND SCALE THE MOBILE NETWORK DURING 5G TRANSITION

YOUR GUIDE TO 5G SECURITY

5G promises higher speeds, lower latency, a multitude of new IoT applications and new 5G revenue opportunities for the mobile network operator. However, security is a top concern for operators as they approach 5G roll-outs. Malicious attacks on mission-critical applications and infrastructure could disrupt service and cause network outages. This could derail revenue potential and cause significant damage to both brand and reputation when they occur. The expected volume of IoT devices, increased efficacy of cyber criminals, and high-risk botnets make protection of evolving mobile networks strategically important. Mobile operators must balance security needs with other business requirements such as network performance and costs.

The A10 Networks 5G security portfolio provides highly cost-efficient security solutions with the flexibility, scalability and protection mobile operators need as they evolve their networks to 5G and integrate cloud and edge capabilities. The portfolio provides a comprehensive security stack at service provider scale with other functions 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.

This guide provides a blueprint of five of the key solutions offered by A10 Networks for successful migration to 5G. Solutions covered in this guide include:

- Gi-LAN Security
- Mobile Roaming Security
- Network Slicing
- Network Wide DDoS Protection
- Secure, Efficient MEC

Visit **www.a10networks.com/5G** for information on additional solutions in the 5G Security Portfolio.

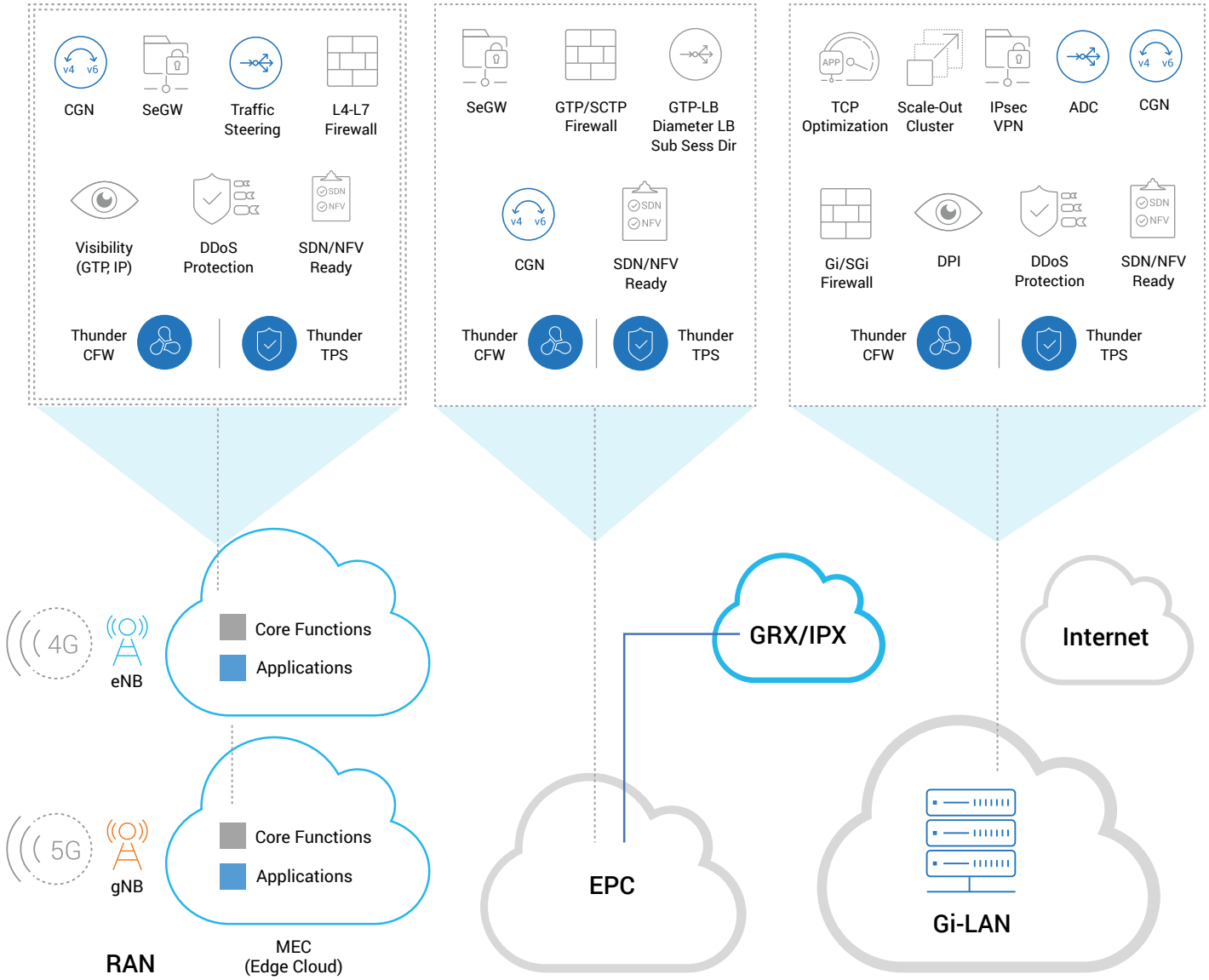

Figure 1: A10 Networks provides a comprehensive security portfolio for 4G, MEC and 5G networks

Gi-LAN Security – Gi/SGi Firewall

USE CASE #1

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.

The A10 Thunder® Convergent Firewall (CFW), with an integrated Gi/SGi firewall, protects infrastructure and subscribers and delivers the performance that mobile carriers require. The Gi/SGi firewall solution meets both current and future traffic requirements for any service provider.

This comprehensive and consolidated approach provides best-in-class performance, efficiency and scale to protect the mobile infrastructure while reducing OPEX and CAPEX costs.

Service providers can also use the Gi/SGi firewall solution in a virtual form factor with the A10 Networks vThunder® to gain a flexible, easy-to-deploy and on-demand, software-based deployment.

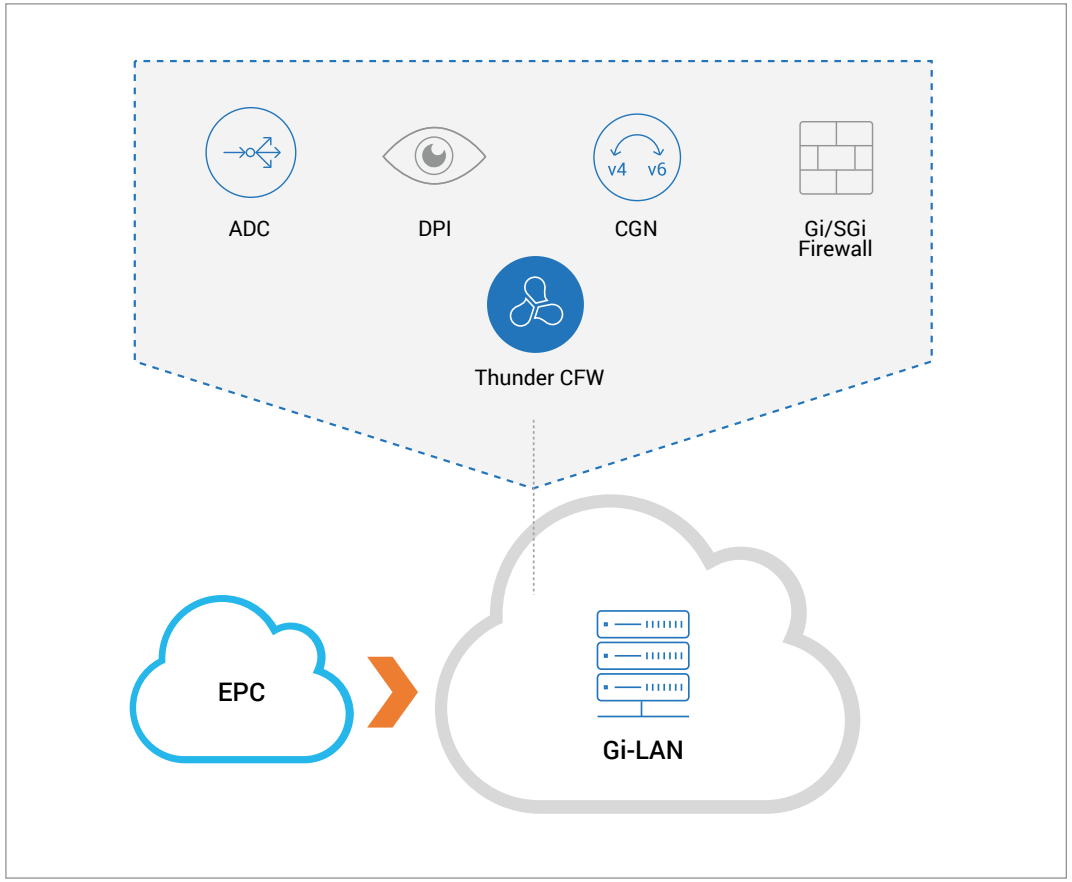

Figure 2: The Gi-LAN solution protects network infrastructure

Mobile Roaming Security – GTP Firewall

USE CASE #2

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 the growing security challenges while also providing a seamless subscriber experience – wherever they travel whatever devices they use, whatever network is accessed.

The A10 Networks 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.

GTP firewall is part of the A10 Networks 5G solution portfolio. The 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.

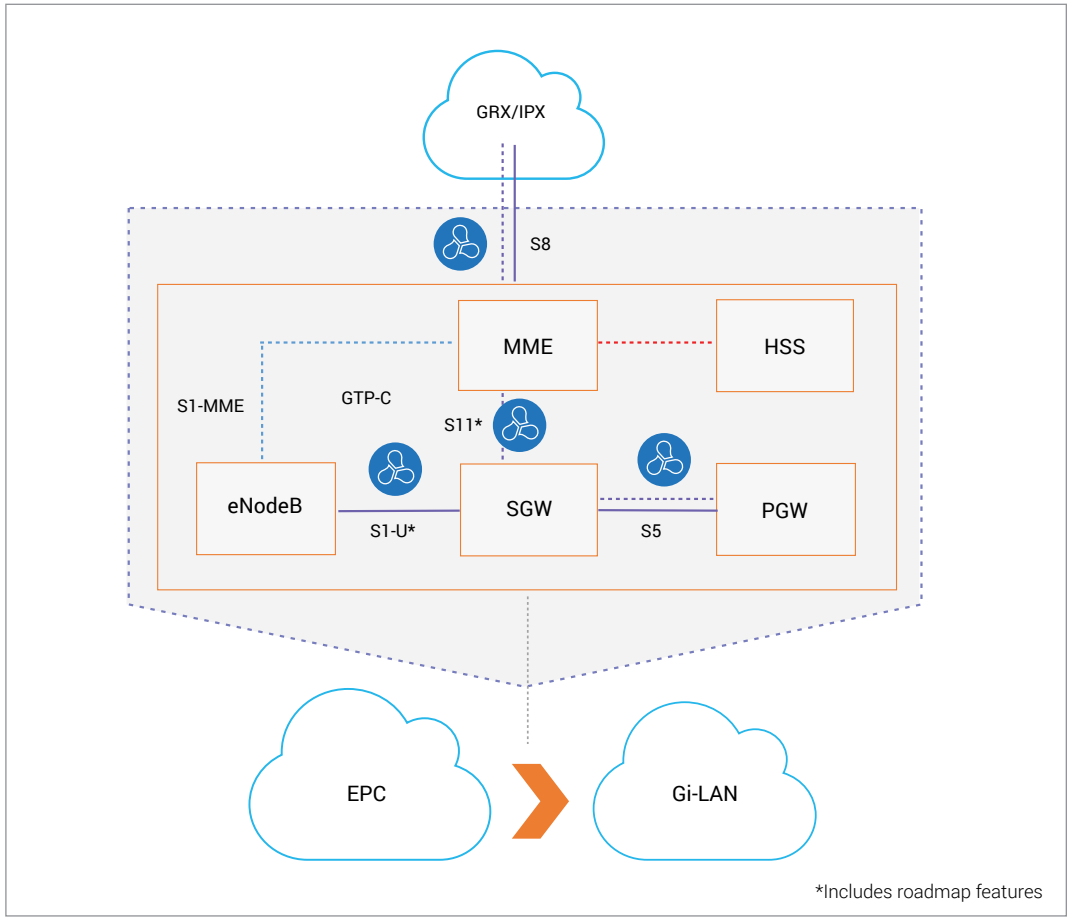

Figure 3: GTP firewall protects subscribers and network from GTP-based attacks

Network Slicing – Intelligent Traffic Steering

USE CASE #3

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.

The A10 Networks 5G solution portfolio provides highly scalable security solutions for 5G network slicing scenarios. Operators can begin using the concepts of network slicing now as they prepare for 5G.

The A10 Networks 5G solution portfolio provides intelligent traffic steering and distribution. 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.

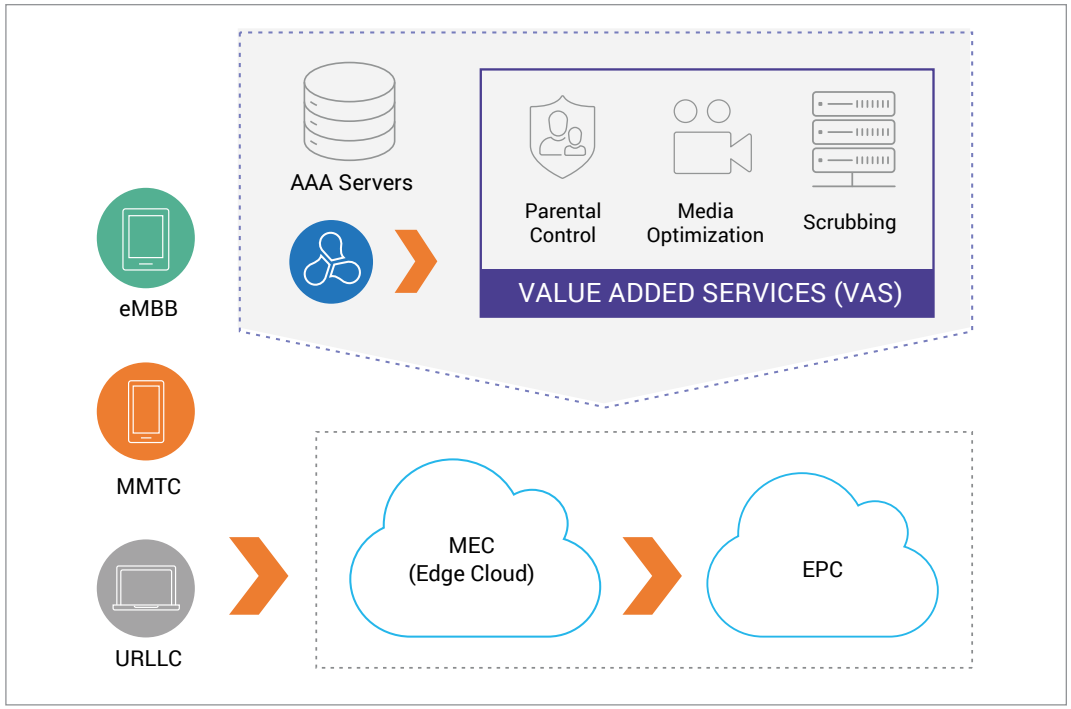

Figure 4: Intelligent traffic steering directs slices of traffic to value added services.

Network Wide DDoS Detection and Mitigation System

USE CASE #4

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.

A10 Networks' comprehensive strategy includes One-DDoS capabilities which provide layered distributed detection coupled with protection capabilities across key networks elements. Thunder CFW works in concert with A10 Thunder Threat Protection System (TPS) edge flow-based detection and centralized mitigation to enable service providers to achieve full spectrum resilience against DDoS. CFW also contains integrated functions that protect against signaling floods and targeted infrastructure attacks.

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.

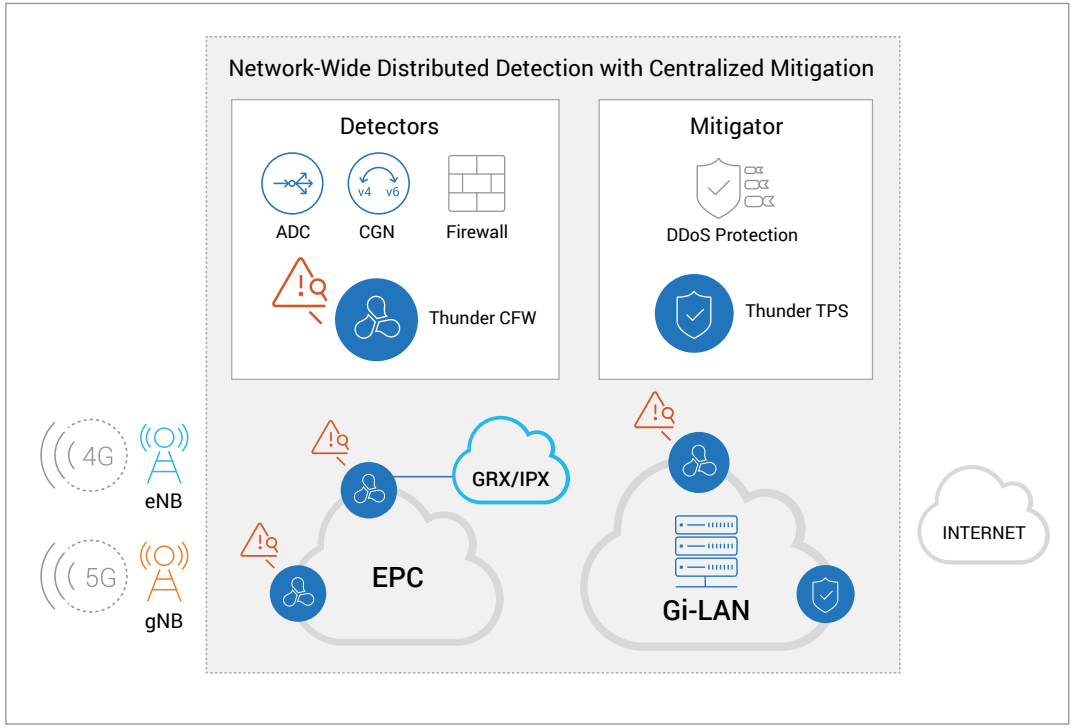

Figure 5: Thunder TPS and Thunder CFW provide industry leading DDoS detection and mitigation

Secure, Efficient MEC

USE CASE #5

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 centralized data center or mobile core to a number of 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 Thunder CFW offers high performance, low latency in a software-based or hardware form factor for firewall, CGNAT and IPv6 migration, traffic steering and other functions. Many functions that may have been provided by single point appliances are combined into one appliance, virtual instance, bare metal or container.

Cost-efficient, high-performance security is ensured without exceeding space and power limitations. The A10 Networks ACOS operating system ensures maximum flexibility and consistent deployment across all form factors. Centralized management and analytics simplify operations for lower TCO.

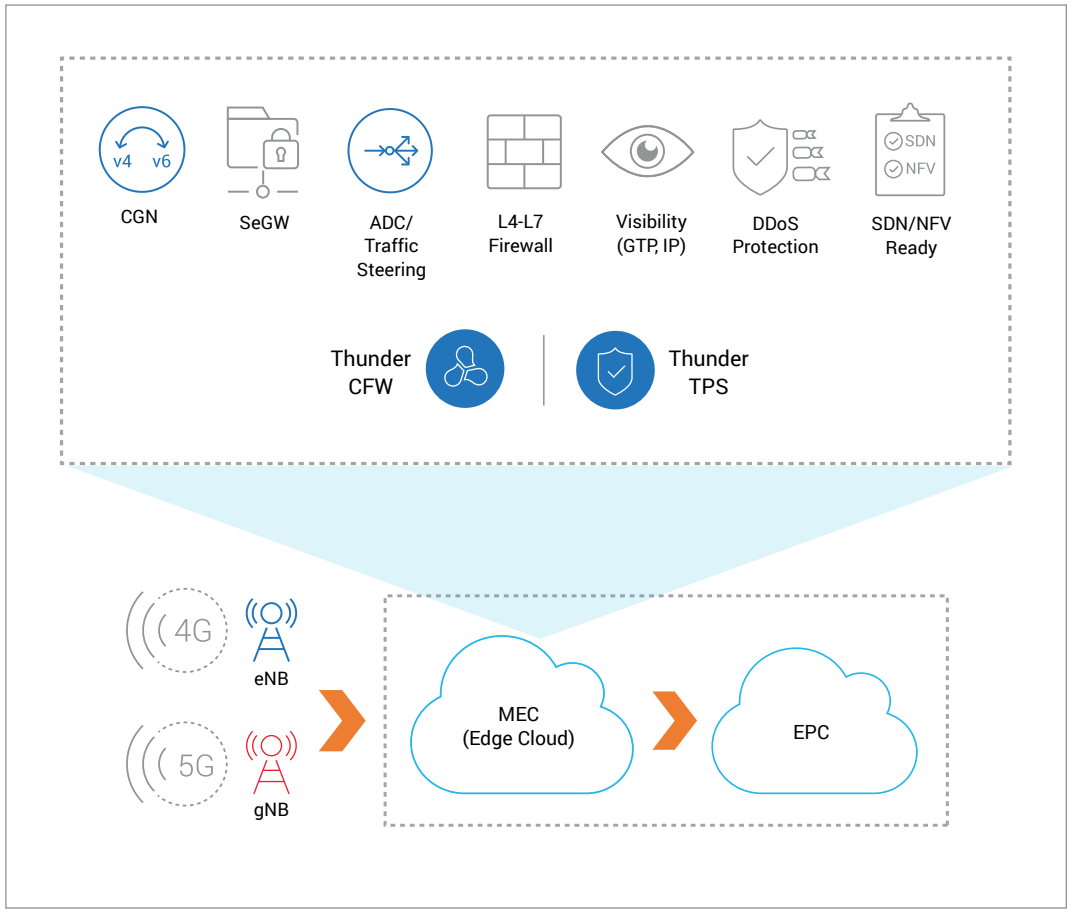

Figure 6. Thunder CFW and Thunder TPS provide space and power efficient solutions for MEC environments

A10 NETWORKS – YOUR PARTNER IN THE 5G JOURNEY

A10 Networks provides highly scalable security solutions for 5G network scenarios. Its robust firewall and DDoS mitigation and detection technologies can be deployed in physical, virtual, bare metal, and container form factors to suit individual network topologies, including 4G, 5G-NSA, MEC and 5G SA.

The A10 Networks Thunder CFW provides exceptionally high firewall connection rates, low latency, throughput and concurrent sessions for the most demanding 5G use cases in compact and flexible form factors.

The A10 Networks Thunder TPS™ is an automated multi-vector DDoS protection solution that ensures availability of business services at any scale or type of network.

By combining a firewall with deep packet inspection, carrier-grade network address translation, intelligent traffic steering and analytics with industry leading DDoS solution, the A10 Networks 5G security portfolio provides the highest flexibility, scalability and protection for mobile operators as they evolve their networks for 5G.

This Solution Guide describes five of the key solutions in A10 Networks 5G Solution Portfolio. For more comprehensive information on solutions for service providers, please visit **www.a10networks.com/solutions/service-provider/**

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information visit: a10networks.com
or tweet **@A10Networks.**

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-BR-20111-EN-01 AUG 2019