SOLUTION BRIEF

Securing 4G and 5G Infrastructure and Services with Fortinet

Executive Summary

Technology evolution in mobile networks in 4G and the introduction of 5G is presenting mobile network operators (MNOs) with the opportunity for a profound change in their addressable market segments and the scope of services and value they provide. These new capabilities and services are crucial for enabling innovation in all industries, from manufacturing and energy to transport, logistics, and healthcare. The promise of 5G especially is profound, but only if properly secured.

Digital innovation in mobile networks creates a duality in the role security plays in mobile environments: Internal mobile infrastructure security and external use-case security and monetization. Fortinet is best positioned to help industries realize the benefits of 4G and the coming 5G era through a comprehensive security-driven networking strategy and the right support for robust services and user experiences.

Internal Mobile Infrastructure Security

In previous generations of mobile technologies, the consumer market was the main addressable market where the value provided (and revenue generated) was limited to a small set of services, mainly voice, messaging, and internet connectivity. Most of the value and content was provided by third parties, not the MNO itself.

These factors led to the limited implementation of security to protect the mobile infrastructure exposure points (such as untrusted public data networks (PDNs), radio acess network (RAN) core, and roaming connectivity) from external threats as a means to help ensure service continuity. But as mobile infrastructure and technologies have continued to evolve, so must the security infrastructure in place—and 5G will be the ultimate test for networks that can stay secure while delivering world-class user experience.

External Use-case Security and Monetization

The introduction and implementation of new technologies in 4G and 5G networks enable MNOs to offer value-added services that go a long way beyond mobile connectivity. This mix of capabilities can be molded into services that are key to an MNO's ability to engage with industries and meet their evolving needs.

Security as part of an industry use case is important in the following aspects:

- Acceptance and adaptation of industry use cases will depend on the MNO's ability to ensure the appropriate security service-level agreements (SLAs).
- As MNOs provide value-added services (applications, platforms, partner ecosystems, etc.) as part of a use case (i.e., beyond just connectivity), their ability to secure these components becomes a critical part of their ability to deliver the use case.
- Security visibility and control within a use case can be monetized for delivering managed security services to the customer, thus creating additional revenue and growth for the MNO.

One can expect that with the growing availability of innovative mobile services and use cases and their corresponding customers, threat actors will turn their attention to these use cases as attack vectors or even attack targets. It is another important consideration for the MNO's overall security strategy.

Fortinet Security Infrastructure for MNOs: Securing Innovation and Enabling Growth

Fortinet provides a common set of security solutions and tools that provide end-to-end security visibility and control for 4G and 5G mobile infrastructure, while enabling industry use cases' security and monetization. This approach facilitates integration and onboarding while keeping operations and management efforts to a minimum. Products and services include the FortiGate next-generation firewall (NGFW) and the FortiWeb web application firewall (WAF). Together, they enable MNOs to securely drive innovation in technology, services, and use cases to consumer and business segments alike.

Delivering Agile and Performant Internal Security for Mobile Infrastructure and Services

The diagram below outlines the Fortinet solution for protecting the MNO's infrastructure from threats and helping to ensure service availability and continuity.

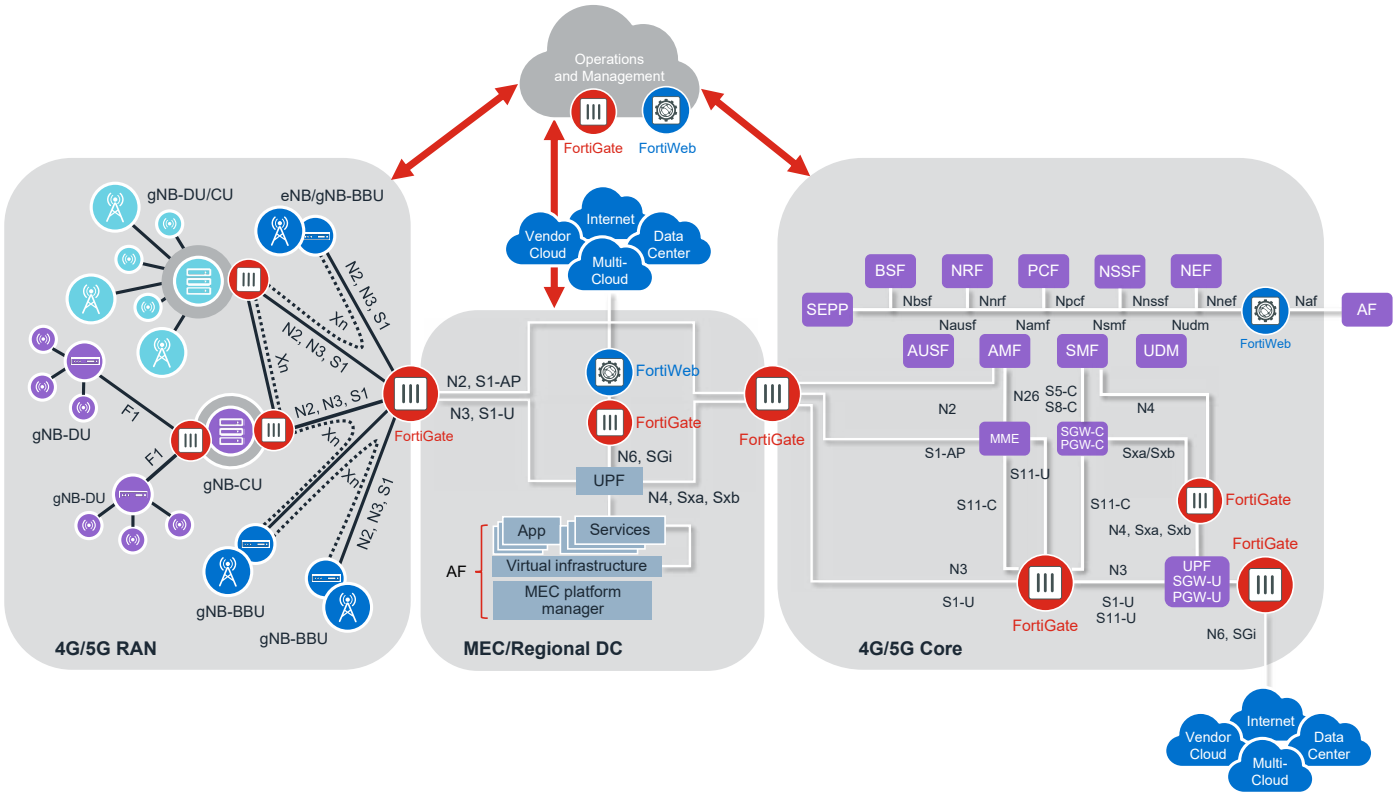

Figure 1: Securing the MNO ecosystem.

Radio Access Network (RAN) Security

Securing a versatile, hybrid, and highly scalable 4G and 5G RAN is more important than ever due to the evolving nature of radio technology and use cases. Securing the RAN mandates a new kind of security gateway (SecGW) infrastructure—one that is agile and hybrid, but also capable of supporting the mixed architectures and different performance, scalability, and quality-of-service (QoS) requirements LTE-A and 5G present. The Fortinet FortiGate physical network function (PNF) and virtual network function (VNF) offering delivers a common, flexible, and hyperscale SecGW platform that is already in production in leading tier 1 MNOs around the world. Its range of SecGW and NGFW capabilities and performance are unmatched in the industry, delivering a platform upon which MNOs can manage their RAN IPsec virtual private networks (VPNs) and secure user and control planes on S1, N2, N3, and Xn.

Multi-access Edge Computing (MEC) Ecosystem Security

The deployment of MEC sites with networking, storage, and compute resources enables MNOs to enable ultralow latency applications and use cases, weather fully hosted in the MEC site or as part of a larger ecosystem deployment in the telco cloud and partner clouds/public cloud. This also requires the ability to terminate the user plane data with local user plane function (UPF) and local PDN breakout for Internet Protocol (IP) and application programming interface (API) connectivity to applications and ecosystem partners.

The FortiGate VNF/PNF platform provides carrier-grade NAT (CGNAT) and full NGFW L3-L7 security visibility and control to secure both control and user plane traffic and PDN connectivity at the MEC. The FortiGate platform can also be used to monetize security by delivering managed security services to mobile customers, including Internet-of-Things (IoT) security, application control, botnets protection, and more.

The FortiWeb PNF, VNF, or cloud-native network function (CNF) platform provides artificial intelligence (AI)-based application and API security for MEC locally hosted applications and the integration and delivery of applications and services from partner clouds.

Non-3GPP Access Security

Non-3GPP access technologies such as wireless local-area network (WLAN) technologies can be connected to the 3GPP core network like evolved packet core (EPC) in various ways based on the operator's business models and architectural preferences. For unsecured non-3GPP access, the user equipment connects first to the Non-3GPP Interworking Function (N3IWF) and then to the access and mobility management function (AMF) and UPF, respectively, for the 3GPP access.

The FortiGate platform provides Stream Control Transmission Protocol (SCTP) firewalling for the N3IWF N2 control plane and L4-L7 NGFW services for the N3 user plane traffic, ensuring untrusted access is secured for both planes.

Mobile Core Security

The mobile core, in conjunction with the RAN, is the core enabler of a wide range of basic to advanced services and use cases for consumers and businesses. This and various technology evolutions—such as 4G and 5G control and user plane separation (CUPS), virtualization, PDN connectivity, roaming partners' connectivity, RAN connectivity, service-based architecture (SBA), application function exposure, and more—makes the mobile core a growing target for threat actors.

The same tools used to secure the RAN and the MEC are used for the mobile core security, offering a true end-to-end mobile infrastructure security visibility and control.

The FortiGate PNF/VNF platform provides:

- 4G/5G PDN L4-L7 NGFW security and CGNAT services with massive scale and ultra-low latency on SGi and N6 connectivity
- Data plane security with GTP-U firewalling and deep content inspection on N3 and S1-U
- Core-to-RAN security gateway (SecGW) with massive VPN scalability and throughput
- Control plane to data plane security on Sxa/Sxb and N4

5G's SBA functions use API calls over HTTP V2 for control plane communications. The FortiWeb platform safeguards against HTTP and application level attacks. It also provides API schema and value enforcement, and API gateway functionalities for the SBA exposure function.

Security for 4G and 5G Private Networks

Cellular private networks provide capabilities that may be needed to serve an organization's mission-critical or business-critical use cases, ranging from connectivity to QoS, security, availability, latency, and more—all specifically tailored for their needs.

Delivering and managing private cellular networks will vary based on their architecture, services and capabilities, complexity, and the needs and requirements of the enterprise. Private networks can be delivered as a fully private and close environment at the enterprise premise (including RAN, MEC, and core), as a shared environment between the enterprise and the MNO (shared RAN and control plane), or as an end-to-end network slice.

Whatever the architecture and the solution are, security must be integrated in different points of the implemented architecture to ensure the availability of the service and the user plane data integrity. The FortiGate and the FortiWeb platform provide these common security visibility and control, regardless of the private network architecture and services, inclusive of RAN SecGW, CGNAT, L4-L7 NGFW, and API and application security.

Industry Use-cases Security and Monetization

The built-in security services within the FortiGate and FortiWeb platforms that are already used to secure the mobile infrastructure can also serve to secure industry-facing use cases and enable security monetization via the delivery of managed security services appropriate to each use case.

For example, a connect smart factory use case can use the FortiGate in the factory's MEC or closest data center to protect against IoT attacks, signal storms, and malfunctions while providing security services to the plant itself, such as malware protection, botnet protection, application control, URL filtering, and more. The FortiWeb can deliver application-level security and API-level security for the plant's industrial applications residing in the MEC and to their integration with third-party applications. And with the same FortiGate and FortiWeb platforms used in the RAN, the MEC, and the core, the onboarding and operations of securing new use cases and delivering security services to the enterprise customer becomes rapid and cost-effective.

Summary

Through the use of two carrier-grade platforms, the FortiGate and FortiWeb, Fortinet enables MNOs to secure their 4G and 5G mobile infrastructure, secure a wide range of innovative enterprise use cases, provide private networks with embedded security services, and monetize their security investment with Fortinet.

The use of a common set of security tools enables operators to streamline their overall security onboarding and operational aspects across mobile infrastructure and services, reducing cost, eliminating gaps in trained security engineers, and increasing their overall agility and ability to deliver value to gain the trust and adoption of their customers.

October 17, 2020 2:06 AM

734139-0-0-EN

D:\Fortinet\Solution Brief\Red Solution Brief\4G and 5G Infrastructure Services\sb-FA-securing-4G-and-5G-Infrastructure-and-Services-with-Fortinet-10172020