WHITE PAPER

# 4G and 5G Radio Access Network (RAN) Security

## Radio Access Network Evolution: The Cornerstone for Growth

**Long Term Evolution (LTE) and new radio (NR) evolution is a fundamental component in a mobile network operator's (MNO) ability to deliver upon the promise of 5G and growth. It is fundamental for realizing 5G's cornerstone capabilities: high bandwidth, massive scale, high reliability and low latency.**

Evolving LTE and 5G RAN technologies and architectures are also expanding the operators' customer segment from consumers to enterprises and industries – enabling new markets and growth engines. But at the same time, they introduce complexity and increase the potential attack surface and risk presented by the 5G radio access infrastructure. It is clear that the delivery of business and industry use cases to drive growth must be accompanied with the appropriate security controls – in the RAN and elsewhere in the telco cloud.

The 3rd Generation Partnership Project (3GPP) has recommended the use of Security Gateways (SecGWs) to secure the RAN and RAN to Core communications to ensure service continuity and confidentially. The 3GPP Security Gateway relies on IPSec and certificate management capabilities to provide access control through authentication, and traffic confidentiality and integrity through encryption. Authentication and encryption may be extended to the user plane, the control plane, as well as operation and management traffic.

## The Growing Need for RAN Security

### Big, bigger, biggest.

To enable the growing scalability delivered by LTE-A and especially 5G, the deployment of a growing network of small cells is required. Many of these femtocells, picocells and microcells eNobeBs (eNB) and gNodeBs (gNB) will be located in the public domain and in other non-secure locations. These will also be, in most cases, connected to the MNO network via untrusted backhaul. These combined factors represent a growing risk factor contributing to the increase in overall attack surface and risk for traffic tempering, misuse and manipulation.

### Growing importance and scale of user plane traffic.

The ongoing evolution of 4G and the introduction of 5G is gradually enabling the implementation of business and vertical use cases that provide value beyond plain wireless connectivity. MNOs can now build use cases where whole ecosystems come together to create and enable innovation in manufacturing, healthcare, transportation, energy and other sectors. Providing these "beyond connectivity" services puts a growing importance as to the integrity and continuity of user plane traffic in the RAN and onto the Core. User plane traffic will potentially become one of the most important piece of the MNO's ability to provide value added services (VAS) such as infotainment, Internet of Things (IoT) services and augmented reality (AR) services, just to name a few, as users' data target applications/ services reside within the telco cloud or within the overall use case ecosystem.

This drives the need for greater security, integrity and continuity of the user plane data, which will experience significant growth in some use cases in the RAN alongside control plane and operations and management (O&M) traffic.

## The FortiGate advantage for 5G RAN Security

- eNB and gNB IPsec tunnel termination, aggregation, authorization and authentication
- Site to site access segmentation
- Secures LTE's S1-U and S1-MME interfaces
- Secures 5G's N2 and N3 interfaces
- Secures DU to CU F1-C interface
- GTP-U encapsulated traffic deep inspection provides L2 to L7 known and unknown threat protection
- SCTP firewall for security inspection and enforcement, including multi-homing support
- Native multitenancy support with virtual domains (VDOMs)
- Flexible form factors to meet all performance and scalability requirements
- Predictable high performance for centralized and regional sites with security processing unit (SPU) for offload and acceleration
- The most efficient, smallest footprint SecGW VNF enables energy efficiency and massive scaling, including IPSec acceleration

**Diversified RAN architectures at place.**

The need for better RAN performance, agility, scalability, flexibility and cost-effectiveness, have led to its gradual evolution in LTE and 5G. As a result, MNOs will be operating a hybrid RAN environment composed of different centralized, distributed and virtualized/cloud architectures.

RAN architectures will also depend on specific use cases requirements per market segment or network slice. For example, the eNBs' and gNBs' distributed and centralized units (DU and CU) location will depend on requirements such as latency and bandwidth/performance requirements.

In such a hybrid environment consisting of LTE -A and 5G RAN architectures and components, maintaining security, integrity and visibility for control and user planes and O&M via a common set of security tools flexible enough to adapt to the RAN's different architectures, requirements and constrains is mandatory.

**Mobile infrastructure critical use cases.**

Both LTE-A and 5G bring to bear the ability to provide critical use cases and innovation in different industries, such as healthcare, energy and transportation. Unlike the previous mobile generation, mobile infrastructure "standardization" and the growing reliance on its services for some critical use cases will increase the cybercrime community's "interest" in the mobile infrastructure as an attack vector and target and will further drive the growing need for RAN security.

**The evolution of 4G and 5G mobile infrastructure as a whole, and the radio access network in particular, is driving the growing need for RAN security evolution: from SecGWs to a truly secure infrastructure that is hyper-scalable, hybrid and efficient - providing advanced SecGW and L3-L7 security capabilities.**

## Lurking threats in the RAN

The above are some of the main forces driving MNOs to modernize and strengthen their existing RAN security in order to provide confidentiality, integrity and service continuity. Failing to do so for all communication planes (control, user and O&M) may result in different types of attacks:

- Introduction of rogue eNBs and gNBs as a launch point for attacks against Core infrastructure
- Man in the middle (MIM) attack for intercepting control and user plane traffic
- Denial of service (DoS/DDoS)
- Injection of malicious traffic (malware) to attack and manipulate Core elements
- Misconfiguration or failed software updates within the RAN

Any one of the above attacks has the potential to disrupt RAN, Core and overall service continuity, expose and modify user data, impact both customers and telco cloud applications and services, and overall jeopardize the MNO's ability to comply with data privacy and security regulation.

## Fortinet RAN security infrastructure

The Fortinet solution for RAN security utilizes the FortiGate platform in its different form factors of both physical and virtual network functions (PNF and VNF). FortiGate provides three key security functions for the RAN:

- **Confidentiality** - FortiGate ensures the protection of user traffic throughout the RAN and into the distributed Core in the central data center (DC) or the multi-access edge compute (MEC) locations.
- **Integrity** - FortiGate protects against unlawful changes of user data, such as malware injections or rogue traffic
- **Availability and continuity** – FortiGate protects against attacks that can lead to RAN and Core elements' misuse to cause service degradation or interruption

FortiGate provides a single platform delivering SecGW functionality and a state-of-the-art next generation firewall (NGFW). This combination delivers a powerful tool with a rich set of versatile capabilities suitable for the largest tier-1 4G and 5G RAN deployments:

- IPsec tunnel termination and aggregation for eNB and gNB, supporting authorization and authentication with the public key infrastrure (PKI)
- Internal segmentation capabilities provide site to site access segmentation
- Secures LTE's S1-U and S1-MME interfaces
- Secures 5G's N2 and N3 interfaces
- Secures DU to CU F1 interface
- GTP-U encapsulated traffic deep inspection provides L2 to L7 known and unknown threat protection
- SCTP firewall for security inspection and enforcement, including multi-homing support
- Native multitenancy support with virtual domains (VDOMs)
- Flexible form factors to meet all performance and scalability requirements
- Predictable high performance for centralized and regional sites with security processing unit (SPU) for offload and acceleration
- The most efficient, smallest footprint SecGW VNF enables energy efficiency and massive scaling, including IPSec acceleration
- A rich ecosystem of application programming interfaces (APIs) and connectors for ease of onboarding and integration to the overall MNO's ecosystem such as operation and management, orchestration and business support system (BSS).

**As mobile network operators build their 5G infrastructure, their radio access network environment consists of a hybrid set of LTE, LTE-A and 5G NR architectures and technologies which will co exist and inter-work for years to come. The RAN security infrastructure in place should provide a common set of tools applicable to the mix of RAN technology and architectures for greater agility and flexibility.**

## Fortinet's RAN security infrastructure architecture

As MNOs gradually migrate from 5G non-standalone (NSA) and 5G standalone (SA) deployments, LTE and 5G RANs will co-exist to some degree or another. FortiGate's functionality and flexible form factors makes it the logical choice for securing mixed RANs and architectures. With LTE-A and 5G NR, there is a strong relationship between service categories/quality of service (QoS)/service level agreements (SLA) and RAN deployment and therefore a direct relationship to the security infrastructure and services deployed.

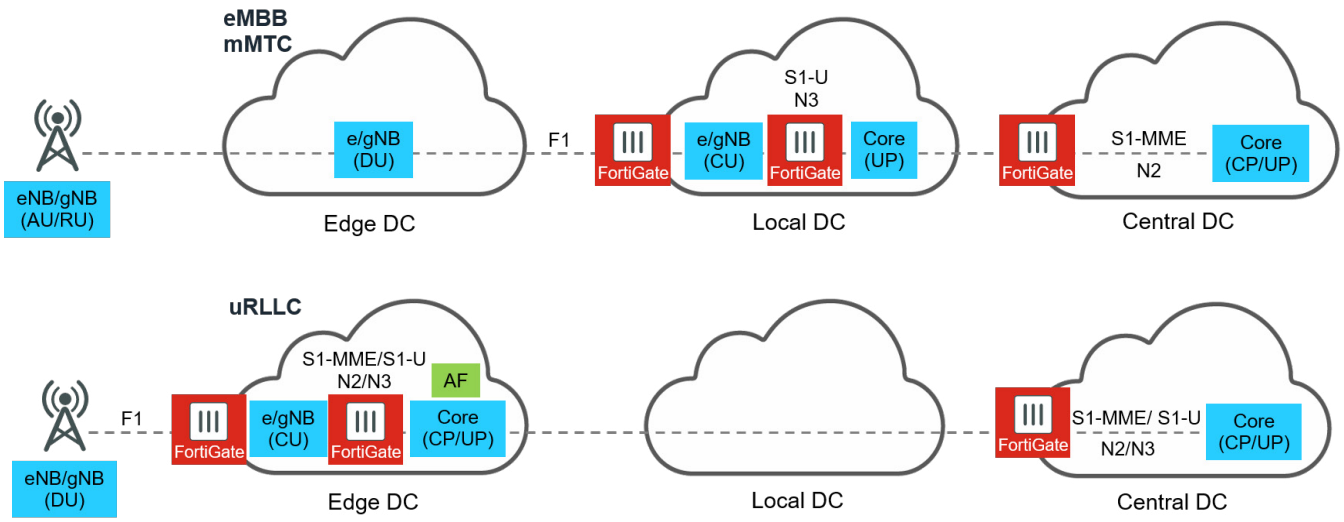


FIGURE 1: POSSIBLE EMBB, MMTC AND URLLC NETWORK SLICES - RAN COMPONENTS DISTRIBUTION

For example, enhanced mobile broadband (eMBB), massive machine-type communication (mMTC) and ultra-reliable low latency communication (uRLLC) service categories SLAs/QoS are delivered via network slices where each slice's requirements are met by a mix of centralized and distributed RAN and Core components. These will determine the SecGW architecture and deployment options, as seen in figure 1 above.

## Centralized SecGW deployment

In a centralized SecGW architecture, control and user plane elements are all located at the eNB and gNB locations with IPSec tunnel connectivity to the central FortiGate SecGW supporting control plane, user plane and O&M traffic and advanced security services.

As a centralized SecGW, IPSec and security performance and scalability are of paramount importance, along with service resiliency and availability. With these considerations in mind, the FortiGate physical appliances are the most suitable choice as they provide predictable, hardware accelerated IPSec and security performance with ultra-low latency and flexible high availability options.

The all new FortiGate 4000F series is equipped with the new 7th generation of Fortinet's network processor SPU technology, delivering the performance required for LTE-A and 5G NR:

- Massive single tunnel throughput performance - up to 110Gbbps
- High elephant stream performance
- Ultra-low, µs-level latency
- "Re-ordering avoidance" technology
- Comprehensive QoS Support
- X2/Xn Traffic mirroring
- Horizontally Scalable Cluster Options and Geo redundancy
- QKD (Quantum key distribution) support
- Hitless site failover and in-service software upgrade
- Highly Energy efficient and compact form-factor

**The FortiGate provides full SecGW and NGFW capabilities in what is the industry's mot compact and efficient virtual network function (VNF) for small cells and edge compute sites. FortiGate range of physical network functions (PNF) utilizes Fortinet's secuity processor units (SPU), providing hyper-scale performance with ultra low latency for large regional data centers and the mobile core.**

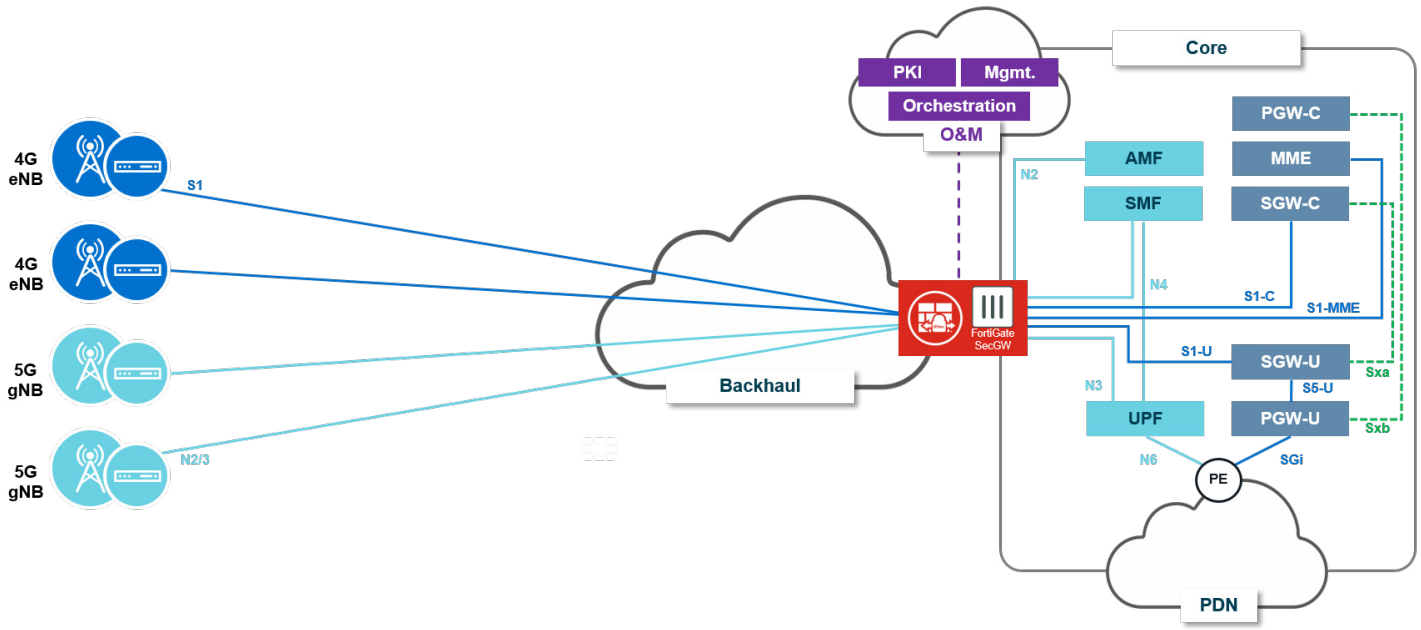


FIGURE 2: CENTRALIZED SECGW DEPLOYMENT

## Distributed SecGW with edge cloud deployment

The ability to terminate the IPSec user plane virtual private network (VPN) connections with the appropriate security controls at the edge cloud/MEC is a must in use cases ranging from location-based services, critical IoT applications, autonomous driving and more. The edge cloud/MEC offers a local packet data network (PDN) breakout but can also host applications such as IoT platform components and industrial applications to deliver the required service and functionality as close as possible to the service consumer.

In this architecture and in addition to the central SecGW terminating RAN connectivity to the Core, the FortiGate SecGW is added to the edge cloud/MEC, terminating user plane VPNs and securing user data for local PDN breakout and for applications/services residing locally at the edge.

Whether deploying a PNF or a VNF FortiGate SecGW in the edge cloud/DC will depend mostly on scale and latency considerations:

- Number of terminated IPSec VPNs
- Expected volume of terminated user plane data
- Usage pattern (stable or changing through time, predictable upscale and down scale)
- Latency requirements
- Energy consumption and performance efficiency

The use of FortiGate SecGW VNF will enable high flexibility and agility in service scaling but with relying on shared virtual network function infrastructure (VNFI) resources with limited high performance, scalability and latency per VNF, performance optimization of the VNFI may not be possible. Therefore, the use of FortiGate SecGW VNFs is recommended for use cases with low to medium performance and latency requirements.

The use of FortiGate SecGW PNF will deliver predictable high performance and ultra-low latency via the use of Fortinet SPU technology. The use of a PNF is recommended for use cases requiring high to very high levels of performance and scalability and/or for regional/edge DC environments with large eNB/gNB concentration.

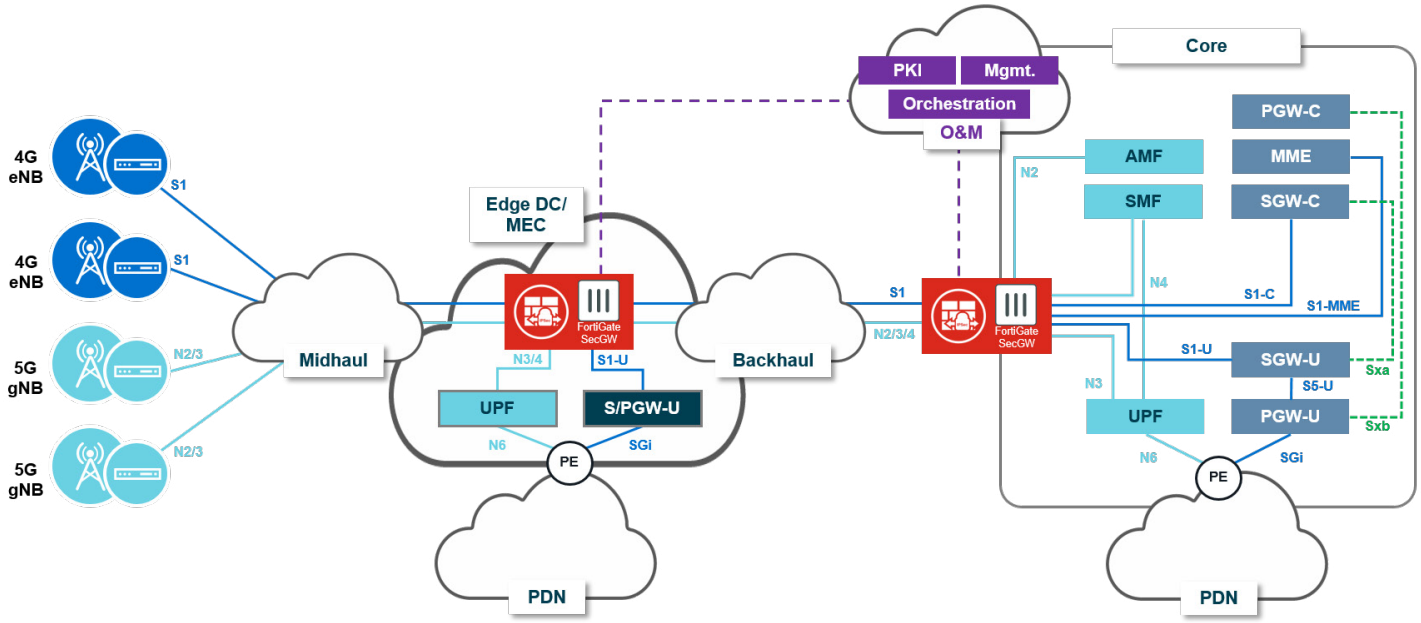


FIGURE 3: DISTRIBUTED SECGW WITH EDGE CLOUD DEPLOYMENT

## Distributed SecGW in decomposed virtual RAN

In the case of decomposed vRAN, SecGW provides IPSec and security functionality to the DU-CU connectivity split as they are decoupled and reside in different parts of the network, as outlined in figure 4. Integrity and privacy are assured for the user and control planes by the Packet Data Convergence Protocol (PDCP-U & PDCP-U), but some control plane messages are sent in the clear, which leaves the F1 control (F1-C) plane open to SCTP threats and attacks if not secured and protected by a SecGW. Specific to the decomposed architecture, Fortinet SecGW solution provides DU-CU authentication and authorization with IPSec including tunnelled connectivity, confidentiality using encryption where required and protection against attacks at the SCTP layer for F1-C.

Due to the relative low volume of control plane data, the FortiGate SecGW can be deployed before the CU as a VNF for F1-C security.

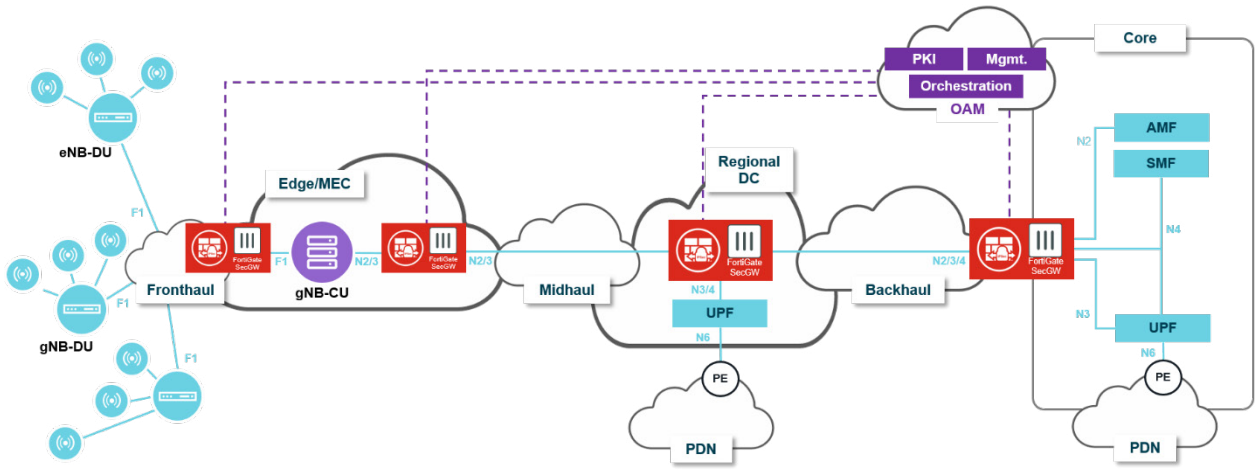


FIGURE 4: DISTRIBUTED SECGW DEPLOYMENT IN DECOMPOSED VIRTUAL RAN

## Small cell connectivity

Femtocells, picocells and microcells are being deployed to create a dense network of small cells required to achieve both capacity and coverage scalability for LTE-A and 5G NR.

Deploying and operating such a large network is a challenge in several aspects, including cost and security. Some of these microcells can also be shared, multi-tenant assets that allow overall cost reduction/better RoI.

The main unique security challenges rising from small cells can be summarized as:

- **Unsecure backhaul connectivity:** as in most cases small cells will be connected to the MNO's central, regional or even edge DC/sites via an untrusted PDN, which opens both control and user planes to a multitude of threats, privacy concerns and attacks that can impact service availability and quality.
- **Scalability:** Small cells add to SecGW scalability requirements with the potential addition of dense small cells networks all connected via IPSec VPNs to the MNO Core/regional/MEC sites.

Fortinet's massive SecGW scalability and performance and its wide range of physical and virtual form factors provides the MNO the capacity to meet these challenges and secure small cells connectivity with the same common tools and functionalities provided to macrocells.

## The Final Word

Securing a versatile, hybrid and highly scalable 4G and 5G radio access network is more important than ever due to the evolving nature of technology and new possible use cases. Securing the RAN mandates a new kind of SecGW infrastructure, one is the agile and hybrid, and yet capable of supporting the mixed architectures and different performance, scalability and QoS requirements LTE-A and 5G present.

Fortinet's FortiGate platform 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 next generation firewall capabilities and performance are unmatched in the industry and deliver a platform upon which MNOs can securely drive revenue and growth with new 4G and 5G use cases.





July 8, 2021 12:51 PM

1039305-A-0-EN