FORTINET

WHITE PAPER

Securing 5G Private Mobile Networks

Enterprises across many industries are looking to 5G technology and services as a key enabler for digital transformation and innovation.

Non-public mobile networks, aka private mobile networks, promise the benefits of 5G technology tailored for enterprise-specific needs, use cases, privacy, management, and control.

Research indicates that private mobile networks spending will experience continuous growth. ABI Research recently estimated that spending on 5G private and shared enterprise networks will surpass spending on public mobile networks in about 15 years.[1]

It is clear that private mobile networks are among 5G's critical use cases and therefore need to become important offerings from mobile network operators (MNOs), especially as enterprises and industries move forward with digital innovation and Industry 4.0.

The legal and practical ability of enterprises to build their own 5G private networks, independently of public 5G infrastructure and services, is both a threat and an opportunity for MNOs:

- **A threat** of potential revenue loss and growth slowdown if lacking a comprehensive private 5G network offering.
- **An opportunity** to create real 5G competitive differentiation alongside a revenue and growth engine with a complete, private 5G network offering and ecosystem to support it.

As private mobile networks are built, they will fuel new use cases, drive innovation and efficiency, and become one of the major connectivity technologies for Industry 4.0. Cybersecurity must be top of mind for both enterprises and MNOs to ensure the availability, continuity, privacy, and integrity of the network, its services, its applications, its data, and its ecosystem partners.

Private Mobile Architectures and Cybersecurity

5G private networks can be implemented under two principal architecture families, each with a direct impact on cybersecurity risks, ownership, and solutions. MNO-independent and MNO-dependent architectures differ in their level of dependency in public 5G infrastructure, the physical location of their components, and possible ownership and management, as outlined in Diagram 1 below.

		Private Mobile Network Architecture Family			
		MNO Independent	MNO Dependent		
		No Sharing	Public 5G RAN Sharing	Public 5G RAN and Control Plane Sharing	Public 5G Full Sharing (End-to-End Slicing)
Component	Radio Access Network (RAN)				
	Control Plane (CP)				
	Data Plane (UPF)				
	Multi-access Edge Compute (MEC)				
Private 5G network component physically isolated from public 5G network			Private 5G network component logically isolated from public 5G network		

Diagram 1: 5G private network components and relationship to public 5G network resources.

The level of dependency on public 5G network resources has a considerable impact, both for an enterprise and MNO, on factors such as complexity, agility, and control. However, these impacts may be different for enterprises and MNOs and have a role to play in the choice of the appropriate private network architecture to be implemented, in addition to the deployment's specific use-case requirements.

Diagram 2: Major private networks architectural considerations beyond use-case requirements.

5G Private Networks' Cybersecurity Risk and Solutions

There are multiple architectures for deploying private mobile networks, which vary based on the enterprise/industry requirements and use cases, along with spectrum regulations and allocation per country. Each architecture introduces cybersecurity risks that must be minimized by the MNO or the enterprise, or by both.

Regardless of the architecture, ensuring the security of a 5G private mobile network should be considered critical for both the enterprise and the MNO. The below table summarizes Fortinet security solutions for private 5G mobile networks—including security objectives and main services. Fortinet solutions deliver protection and service integrity, privacy, availability, and continuity in the face of possible cyberattacks and risks.

Security Platform	Form Factor	Objective	Security Platform Services
FortiGate	Physical (PNF) Virtual (VNF)	Secure private RAN (gNB) to core communications	▪ gNB authentication ▪ gNB to core VPN termination ▪ User plane (GTP-U) deep inspection threat protection ▪ SCTP firewalling ▪ L4-L7 firewall for core protection
		Protect against IoT signaling storms in the private network	▪ Tunnels and sessions rate limitation on N3 in conjunction to N4 monitoring ▪ Block unauthorized sessions on N3 ▪ Block reconnection storms
		Protect private network against PDN/internet-originated threats	▪ IPS and antivirus services ▪ L4-L7 firewall for PDN/internet threat protection ▪ URL filtering and application protocol ▪ Bot mitigation
		Private network to PDN address connectivity	▪ IPv4 - IPv6 Network Address Translation

Security Platform	Form Factor	Objective	Security Platform Services
FortiWeb	Physical (PNF) Virtual (VNF) Container (CNF)	Secure against MEC application-level threats and attacks	▪ OWASP Top 10 application attacks mitigation ▪ Known threat and zero-day attack protection ▪ Bot mitigation ▪ ML for false positives minimization ▪ Protocol validation
		Private network API protection against: API attacks, misbehaviour, misconfiguration Protect private network signaling plane API exposure to external application functions (AF)	▪ Native support for HTTP/2 ▪ OpenAPI 3.0 verification ▪ JSON protocol conformance, limits, and schema validation ▪ XML protocol conformance, limits, schema validation, external entities, SOAP ▪ WebSocket support: signature enforcement on WebSocket connections, frame and message limits, extensions disablement ▪ API Gateway: API key management, access rate limits and control

Table 1: Fortinet security platforms and services for 5G private networks.

MNO-independent Private Mobile Network Architecture

In this option, there are no relationships whatsoever between the private and the public 5G networks. Such a deployment can be built and managed by the enterprise, the MNO, a mobile technology vendor, or a combination of each. However, the complexity and potential lack of technical know-how will exclude, in most cases, implementation by the enterprise itself.

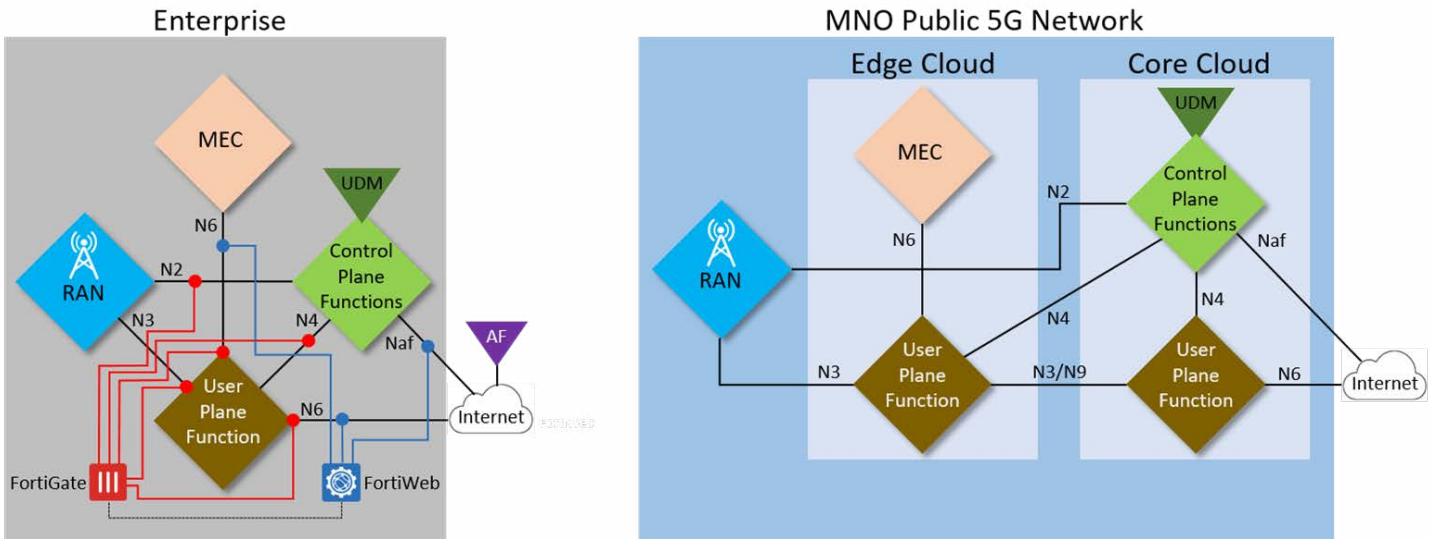

Diagram 3: MNO-independent and secured 5G private network architecture.

As depicted in Diagram 1, a fully MNO-independent and secured private network will self-contain all the required RAN, control plane, data plane, and MEC components at the enterprise premises. The 5G spectrum used can be licensed/unlicensed or use the MNO's licensed 5G spectrum in cases that the private network is built and operated/managed by the operator.

Based on the private network services and implemented use cases, connectivity to packet data networks and the internet for enterprise data center, partners and contractor systems/applications, public cloud connectivity, lawful interception, and other interworking may be required.

In a Fortinet solution, security is implemented on-premises via FortiGate and FortiWeb to safeguard:

- **Private RAN-to-core isolation and possible attack mitigation.** Although in this architecture all the private network components are completely isolated for the public 5G network, an infected UE or an internal threat must be accounted for as possible risks. (In some countries, the law dictates that even a private 5G RAN must provide access to the public 5G network. Although not depicted in this architecture, this situation would require private to public 5G network connectivity, and demands complete security isolation between private and public RAN-to-core virtual private networks [VPNs] for both control and user planes.)
- **Security against UE/IoT-originated threats**, such as signaling storms, infected/malfunctioning devices, and Internet-of-Things (IoT) bot protection.
- When external public data network (PDN) connectivity is required, **next-generation firewall (NGFW)** services are enforced to protect against known and unknown PDN/internet-originated threats.
- **Application-level protection** is provided for IoT and application ecosystem in the private network MEC and elsewhere.
- **API security** is provided for the MEC and external application programming interface (API)-based applications and third-party integration

Security can be implemented and managed by the enterprise itself, a partner, or by the MNO as part of a private mobile network delivered as a managed service.

MNO-dependent Private Mobile Network Architectures

In this family, architectures differ based on the amount of public 5G resources required, as previously outlined in Diagram 1. These architectures are most likely to be deployed by the operator and co-managed with the customer. The following describes some of the possible architectures within this category.

RAN sharing private mobile network architecture

In this architecture, RAN (gNBs located within the enterprise premise) is shared between the private and public 5G networks via the implementation of slicing at the RAN. This includes:

- **Private slice**, where all the private network UE/IoT devices' control and data plane traffic remains within the private network and is served by the private network's components
- **Public slice**, where the public network UE/IoT devices' control and data plane traffic leaves the enterprise premise and is served by the MNO's public 5G network

As in all architectures, external PDN connectivity to the private network and MEC is likely to be required.

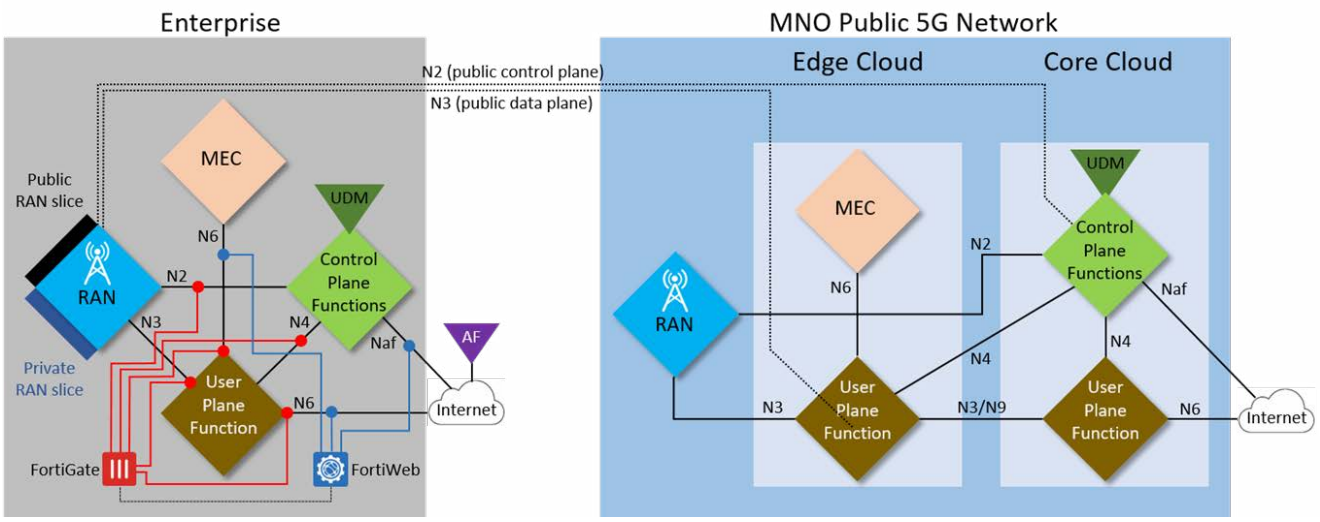

Diagram 4: RAN sharing 5G private network architecture.

On top of the security implementation described in the MNO-independent architecture, special attention must be given to the isolation and deep packet inspection of the private and public control and data plane VPNs so as to safeguard against attacks on the private networks originating from the public RAN slice, and to avoid possible data leaks.

In Fortinet solutions, the FortiGate and FortiWeb are deployed at the enterprise premises and provide the required security visibility and control as outlined in Table 1.

RAN and control plane sharing architecture

In this architecture, RAN (at the enterprise premise) and control plane are delivered via the MNO's public network and logically separated from the public RAN and control plane via a dedicated private slice. This enables the enterprise's data to be maintained within the enterprise and isolated from the public MNO network.

There is a need to secure the control plane functions' interaction with the private network components such as the UPF and any external application function (AF). This is achieved by the MNO's deployment of the FortiGate platform in its core cloud as shown in Diagram 5 below. The multitenancy support of the FortiGate allows for the implementation of RAN to core security for multiple private RAN and control plane slices with a single FortiGate VNF/PNF.

It is worth noting that because the control plane functions' are performed in the public network, they may expose some of the enterprise sensitive data, such as UE/IoT device information, which is stored in the MNO's public network core (in the UDM). Therefore, control and confidentiality must be ensured by the MNO in this architecture.

Data plane function and MEC are on enterprise premise enabling use cases and applications requiring ultralow latency.

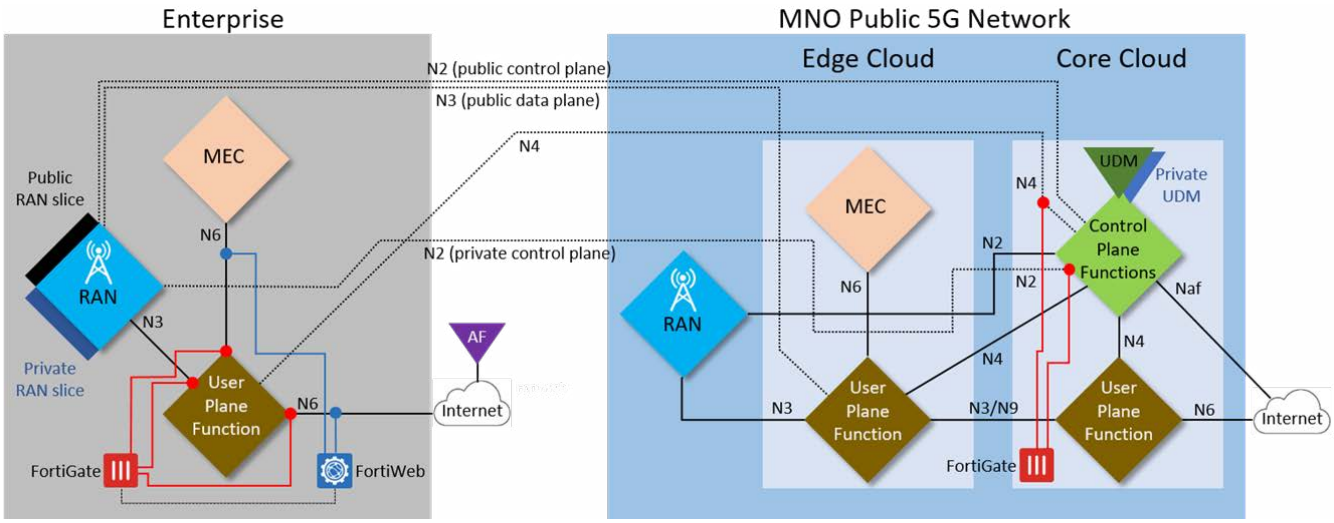

Diagram 5: RAN and control plane sharing 5G private network architecture.

End-to-end slicing private mobile network architecture

In this architecture, the enterprise's private mobile network is a logical one provided by the means of an end-to-end network slice (or multiple slices) on top of the public 5G infrastructure. Only the gNB is deployed at the enterprise premise to serve local UE/IoT devices. MEC and UPF are provided as close as possible to the enterprise, and even within the enterprise, to enable low-latency applications and use cases.

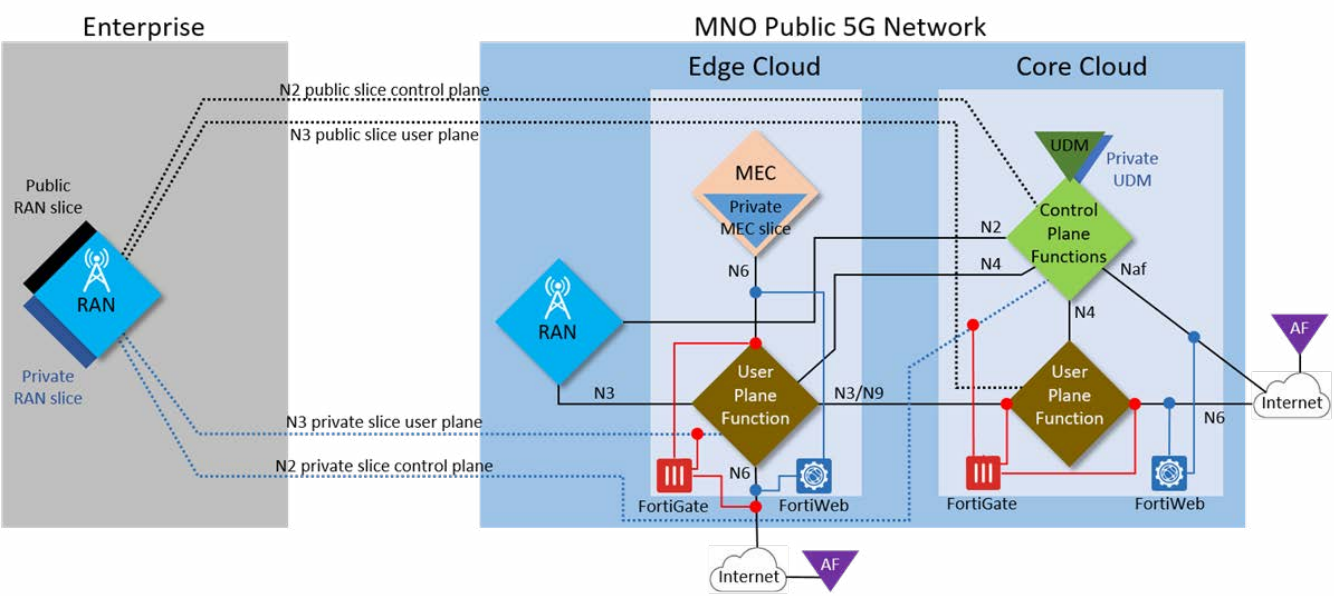

Diagram 6: 5G private network architecture with end-to-end slicing.

As the 5G private network is logically delivered on top of a publicly shared 5G network, control and data planes and any API interworking with MEC-based/external AFs should be visible and secured. (In Fortinet solutions, this is handled via FortiGate and FortiWeb.) This is critical to ensure the private network security and the security of the shared public 5G network. From a security perspective, this architecture can be considered as a "mirror image" to the MNO-independent architecture—with the MNO having the highest responsibility to secure its private 5G mobile network offering.

Summary

Private 5G networks are a clear early use case for 5G, but their growth will be hampered without the right security. To gain market share and revenue, MNOs must provide a set of flexible and secure architectures and services to meet different industries' demand for private 5G.

With a common set of security solutions applicable to a wide range of architectures and use cases, Fortinet solutions enable MNOs to meet the security requirements that are key to enterprises—either as part of a 5G private network offering or on top as a set of managed security services.

[1] ABI Research 5G Summit, July 14, 2020.

September 17, 2020 12:14 AM

771877-0-0-EN

D:\Fortinet\White Paper\Red White Paper\Security for 5G Networks\wp-FA-securing-5G-private-mobile-networks-9172020