SecurityGen
Telecom Security. Transcending Generations.

PRIVATE 5G NETWORKS (AND HOW TO SECURE THOSE)

Wi-Fi has been ubiquitous on Enterprise and Industrial environments. Fast evolution a great promise in fact made some MNOs and Fixed Service Providers to build their own "complementary" Wi-Fi networks, especially due to the high costs on 3G deployment.

During the 4G rollout, technology evolution has tilted the scale back for MNOs, but Wi-Fi was still the standard for enterprises. Enhanced-LTE and 5G are now challenging this reality.

The specifications for reliability, high speed, low latency, high density, and power efficiency meet or surpass corporate and industrial requirements, and research companies announce the dawning of the Private 4G and 5G era. In fact, some researchers point out that the market for private 5G shall be bigger than public 5G. But this should be taken with caution, as networks are built and players evolve, there are still no winners on this race.

Focusing on 5G, the first decision for Corporate Management is not a simple "Make or Buy", but rather how much responsibility I want on the network deployment and management and how much segregation does my business require?

Enterprise migration to a much more flexible wireless network which may be built and optimized for latency, low energy consumption or throughput (not the main motivator) according to specific requirements is expected. Next step is planning this migration.

Main options so far are:

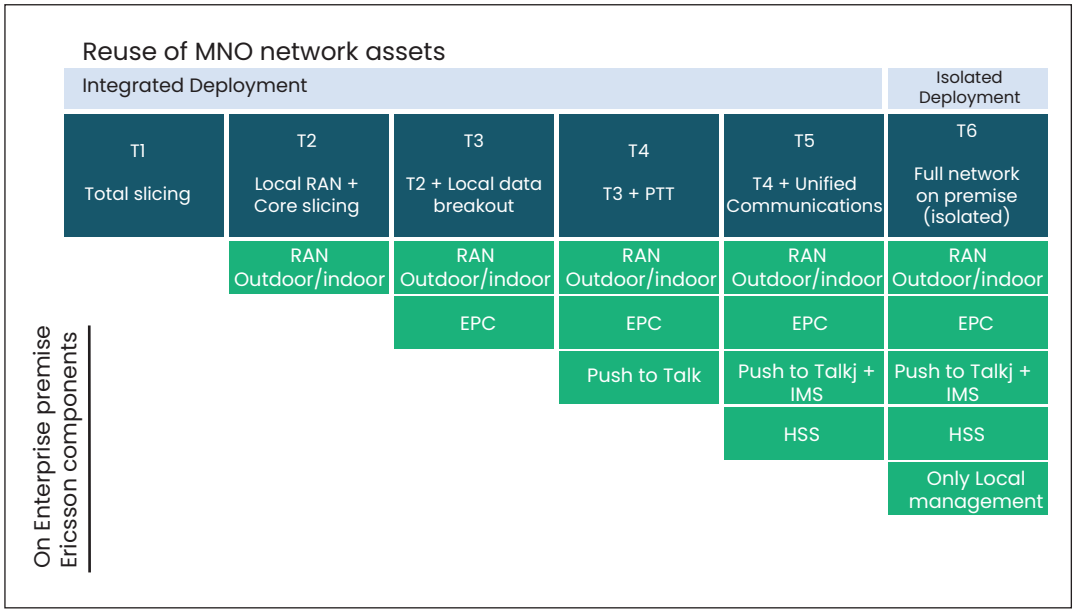
- Procure a Private Network from a local MNO (which has several models on itself)
- Procure a "NPN As a Service" from a Vendor/Hyperscaler and deploy only 5G NR elements, possibly using public spectrum
- Buy a full Private Network which will be deployed on premises and require 24x7 support with a good SLA.

Each one brings security challenges and, as a minimum, companies need to follow their due diligence towards their supply chain, validating that service providers' security measures are in place and any breaches must be reported to customer, on contract.

Model	Enterprise Responsibilities	Provider Responsibilities	Security
PNI-NPN	Enterprise or industrial endpoints, evaluating and monitoring Security of MNO	All Mobile Network Infrastructure, availability, Security Lifecycle and endpoint activation. This is the only option where spectrum is already paid for. The others may incur on additional costs or use of shared frequency bands	100% on MNO to provide the Security but Enterprise must validate and, when applicable, audit.
NPN as A Service	Enterprise or industrial endpoints, evaluating and monitoring Security of Service Provider. Also Management and Operation of RAN elements and some Core elements (e.g.: UPF) depending on the integration scenario.	Usually, 5G Core Functions and RAN control. This may not be the best fit for big plants or company campuses, but rather useful for smaller business.	Shared, according to the integration level.
NPN	Both IT/OT and Telco solutions	Software/Hardware Delivery and Support	100% on Enterprise

MNO Private Network Offer (PNI-NPN)

This is for sure the fastest and low-touch option in case your site already has 5G coverage. Used for both industry and logistics companies (warehouses and ports, for instance), the level of delegation may vary from 100% as a Service to just the 5G radio part, as shown in Ericsson's value proposition reproduced below.



One company may just pay for a slice using dedicated resources from the MNO (T1), might decide to build its own RAN (T2) and so on. Even on T6 model, the company may buy project, operation and support from the Operator, which in some countries act as the solution Integrator as well.

5G As a Service (or NPNaAS)

Hyperscalers proposals roam between T2 and T3 models, depending on the company requirements, especially local data breakout for accessing internal systems and/or Internet with low latency and high capacity.
In some cases, Hyperscalers might try also to host those systems as an additional service.

Private 5G Network (NPN)

The case for T6 may be somewhat rare because just a few scenarios that really require it:

- Law enforcement communication networks for events: Available independent of public network load, specific privacy requirements, etc.
- Agricultural plants so big that are poorly covered or even not covered by public networks. Although those might be surprised by some specific initiatives from both MNOs and heavy machinery vendors
- Mining plants which require kilometers of indoor coverage

Owning a network means Operational Costs that may be equivalent or bigger than paying for it "as a service".

Also, depending on the country, companies must pay for a spectrum license or use shared spectrum subject to future interference as new networks and services are implemented. When you consider the logistics use case, spectrum licensing across many sites may become a burden as well.

Security of a Private 5G Network

There are many security features available from the specification. Enterprise and industry must assure they are enabled on their environments. For a non-exhaustive list:

SUPI concealing, meaning that the unique Id of a subscription and its keys are not openly transmitted on the air interface.

IPSec enabled for Backhaul to assure no interception is possible between RAN and Core. Even more relevant if your Core is hosted externally.

Encrypt both Control and User Plane on the Air Interface to assure confidentiality and integrity of transmitted data.

Our research has identified threats to the 5G Core not covered by the Standards and that must be taken in consideration. We may support MNOs for a safer 5G Service

Telco Cloud Security recommendations also apply since 5G is Cloud Native.

In a nutshell, Telco Cloud is the base virtualization infrastructure that makes 5G viable. It supports all Core Functions and recently a huge part of the RAN, in case Open RAN is implemented. Nevertheless, technologies were not re-created but instead absorbed from IT Virtualization vendors, as well as COTS x86 servers and Data Switches.

All those parts and its Management and Orchestration layers add complexity to the 5G ecosystem as well as further domains for Vulnerability Management.

For details and additional insights, specific articles we have written on the subject are available.

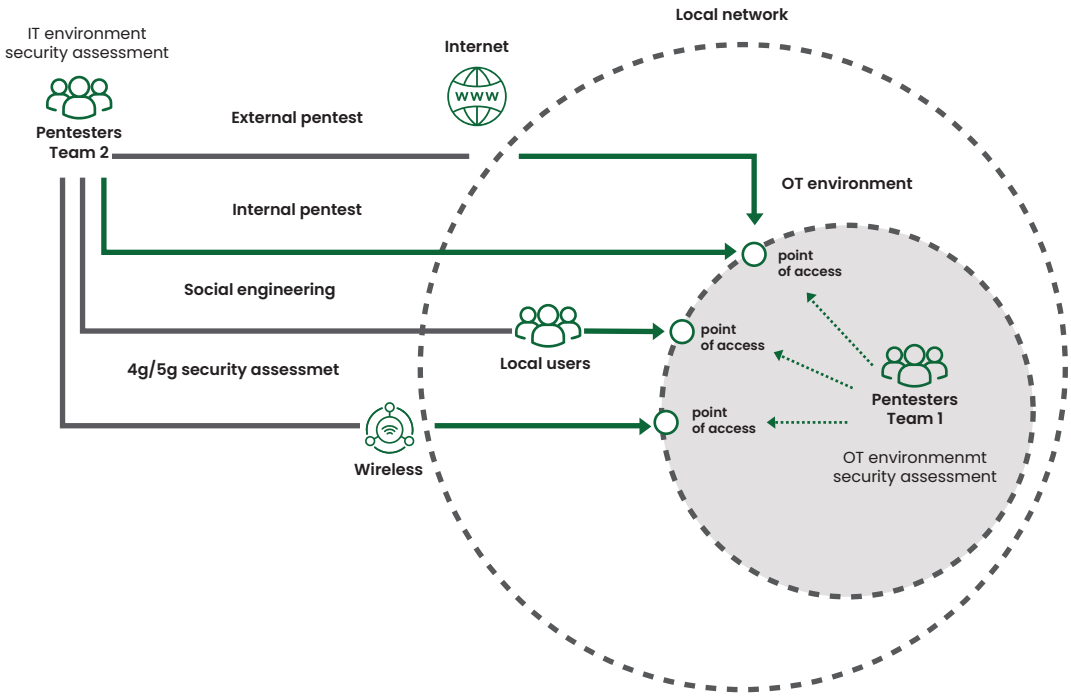
Security Process

Possibly the hardest part on private networks is to keep those safe for the entire lifecycle. This may become a relevant argument for PNI-NPN and NPNaAS, since the technology keeper must assure the integrity and availability of assets from:

- Onboarding of new Functions or releases
- Hardening of OS, Hypervisors, Management Systems and VNFs
- Assuring the designed Network Architecture is kept and evolve according to new requirements
- SOC integration and active monitoring
- Robust Change Management and Vulnerability Management processes

All those tasks are complex, and even more because several vendors are used on the building of a 5G Network. Not all companies might want to build a new team or specialize a current one in Telecom Networks and Telecom Security. The latter is so rare that we are usually requested to recommend or support on the hiring of new professionals even for MNOs.

The usage of Private 4G/5G in Industry includes new elements and borders to be Assessed for Security:



Industrial risks

The usual temprary glimpse on service or traffic speed noticed sometimes in heavily loaded Public Networks are a nuisance for subscriber during special events such as New Year's Eve or huge concerts. While serving an industrial plant, the lack of availability or capacity for Real-time transmission could impact on profits and create physical hazards for the plant itself and its workers.

Security Assessment on the RAN and its redundancy comes as a minimum set of actions to be considered to mitigate attacks on that layer. Constant monitoring of RAN exceptions is also recommended.

Additional Assessments such as pentesting through the external connections (5GaAS, for instance) and internal testing must be performed to ensure the network was built securely and mitigate attack risks.

Any external access must be performed through VPNs and authenticated for both users and endpoints.

Whenever MQTT is used, MQTTS is advised and a MQTT firewall may prevent an attacker of introducing harming conditions into the environment, bad data into controlling application and cause damages.

And as it cannot be stressed enough: ICS should not have a straight unfiltered connection to Corporate Datacenter. No matter the costs or use cases.

IoT devices are numerous and must be cost-effective according to each application. That being said, they are unlikely to support EDRs or other IT-positioned solutions. Each device must be secured on design phase and assessed before usage on an industrial network.

Known threats for OT/ICS:

Management and Control Plane Attack	Mngt networks are exposed to the same advanced threats and attacks as business system
Zero day and DdoS attacks	Plethora of devices are subject to unknown threats
Lateral Movement and Malware attack	Compromise host by host, typical from malware
Usage of unsecure protocols	Non secured sessions i.e. DNP3, Modbus, IEC 1xx are non secure by design.
Network Hardware vulnerabilities	Plenty of devices with non mitigated / patched vulnerabilities
Network Perimeter vulnerabilities	Inadequate physical protection of network equipment
Equipment pivoting	Plenty of devices with non mitigated / patched vulnerabilities
Transmission Poisoning / altering	Industrial devices used as tele command to control other processes / devices

Recommendations for MNOs

The base for Private Networks in PNI-NPN model is about slicing, isolation, and secure integration to enterprise customers.

To achieve those, besides following the best practices and 5G standards, a relevant font of information is NESAS (Network Equipment Security Assurance Scheme) from GSMA. According to it, some key Network Functions must be verified against previously undealt threats.

AMF

- Authentication and key agreement procedure (Synchronization handling, RES* verification failure)
- Security mode command procedure (Replay protection of NAS, NAS integrity algorithm selection)
- 5G-GUTI allocation
- Invalid or unacceptable UE security capabilities handling
- Validation of S-NSSAIs in PDU session establishment request

UPF

- Confidentiality, integrity, replay protection of user data transported over N3 interface

NRF

- NF discovery authorization for specific slice

The eUICC/eSIM enrollment procedure and physical cards procedures for Private Networks must be monitored and controlled. Preferably using different provisioning chains and with much more limited access control. SIM Swapping on enterprise or an industrial plant may turn into huge losses for customers.

MNOs must perform periodic security assessments related to elements that serve the NPN slices and provide evidence for customers' due diligence.