FORTINET

LIVRE BLANC

Sécuriser les réseaux mobiles privés 5G

Dans de nombreux secteurs d'activité, les entreprises considèrent que les technologies et services 5G sont des moteurs de leur transformation et de leur innovation digitale.

Les réseaux mobiles privés offrent la promesse d'une technologie 5G définie sur mesure pour les besoins des entreprises, en matière de cas d'utilisation, de confidentialité, de gestion et de contrôle.

Nombre d'études indiquent que la croissance des réseaux mobiles privés s'annonce pérenne. ABI Research estime que les investissements en matière de réseaux d'entreprise 5G, privés ou mutualisés, devraient supplanter ceux des réseaux mobiles publics d'ici 15 ans.[1]

Il est évident que les réseaux mobiles privés comptent parmi les principaux cas d'utilisation de la 5G. Ils doivent donc faire l'objet d'offres clé de la part des opérateurs mobiles (ou MNO pour mobile network operators), notamment parce que les entreprises et les secteurs d'activité avancent sur le chemin de l'innovation digitale et de l'Industrie 4.0.

La possibilité légale et pratique qu'ont les entreprises de bâtir leurs propres réseaux 5G, indépendant des infrastructures et services 5G public, constitue à la fois une menace et une opportunité pour les MNO :

- **La menace** d'une perte potentielle de revenu et de ralentissement de la croissance en l'absence d'une offre commerciale de réseau 5G privé.
- **Une opportunité** de s'octroyer un réel avantage concurrentiel sur le marché de la 5G, avec un moteur de croissance et de revenus basé sur une offre intégrale de réseau 5G privé et un support associé.

L'émergence de réseaux mobiles privés favorisera de nouveaux cas d'utilisation, l'innovation et les gains de productivité. Ces réseaux sont d'ailleurs appelés à devenir l'une des principales technologies de connectivité pour l'industrie 4.0. La cybersécurité doit être une priorité pour les entreprises et les MNO, pour assurer la disponibilité, la continuité la confidentialité et l'intégrité du réseau, de ses services, de ses applications, de ses données et de son écosystème de partenaires.

Architectures mobiles privées et cybersécurité

Les réseaux privés 5G peuvent être déployés selon deux architectures principales. Chacune aura un impact en matière de risque de cybersécurité, de propriété du réseau et de solutions. Les architectures, qu'elles dépendent d'un MNO ou pas, diffèrent dans leur niveau de dépendance à l'infrastructure 5G publique, la localisation de leurs composants, ainsi que la propriété et la gestion du réseau, comme le souligne le schéma 1 ci-dessous :

		Architecture des réseaux mobiles privés			
		Indépendant du MNO	**Dépendant du MNO**		
		Non mutualisé	RAN 5G public mutualisé	RAN 5G public et plan de contrôle mutualisé	Mutualisation totale de la 5G publique (découpage de bout en bout)
Composant	Radio Access Network (RAN)				
	Plan de contrôle (CP)				
	Plan de données (UPF)				
	Multi-access Edge Compute (MEC)				
Composant réseau 5G privé cloisonné physiquement par rapport au réseau 5G public			**Composant réseau 5G privé cloisonné virtuellement par rapport au réseau 5G public**		

Diagramme 1 : composant du réseau privé 5G et relation avec les ressources du réseau 5G.

Le niveau de dépendance aux ressources réseau 5G a un impact majeur, tant pour les entreprises que pour les MNO, en matière de complexité, d'agilité et de contrôle. Cependant, ces impacts sont différents pour les entreprises et les MNO et jouent un rôle dans le choix de l'architecture de réseau privé à mettre en place, au-delà des besoins des cas d'utilisation spécifiques.

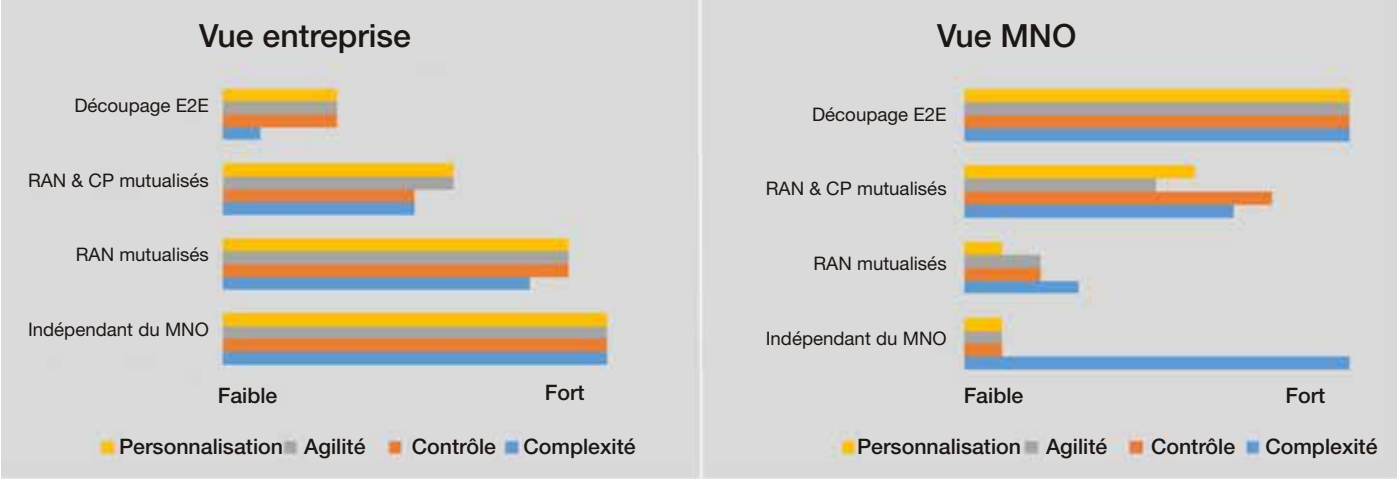

Diagramme 2 : perspectives d'architecture des réseaux privés d'envergure, au-delà des besoins des cas d'utilisation

Cybersécurité des réseaux privés 5G : risques et solutions

Les réseaux mobiles privés peuvent opter pour différentes architectures, selon les besoins de l'entreprise, les cas d'utilisation et la réglementation en vigueur en matière d'attribution des fréquences dans le pays cible. Chaque architecture présente ses propres risques en cybersécurité qui doivent être maîtrisés par l'entreprise et/ou le MNO.

Quelle que soit l'architecture en place, la sécurité d'un réseau mobile privé doit être une priorité tant pour l'entreprise que pour le MNO. Le tableau ci-dessous présente les solutions de sécurité de Fortinet à l'intention des réseaux mobiles 5G, notamment les objectifs de sécurité et les principaux services. Les solutions de Fortinet offrent une protection optimale et assurent l'intégrité, la confidentialité, la haute disponibilité et la continuité métier face aux cyberattaques et risques potentiels.

Plate-formes de sécurité	Format	Objectif	Services de la plateforme de sécurité
FortiGate	Physique (PNF) Virtuel (VNF)	RAN privé sécurisé (gNB) vers les communications du cœur	▪ Authentification gNB ▪ Terminaison du VPN reliant le gNB au cœur ▪ Protection du plan utilisateur (GTP-U) avec inspection des menaces ▪ Pare-feu SCTP ▪ Pare-feu L4-L7 pour la protection du cœur
		Protection contre les « signaling storms » IoT au sein du réseau privé	▪ Limitation du nombre de sessions et tunnels sur N3 en complément du monitoring N4 ▪ Neutralise les sessions non autorisées sur N3 ▪ Neutralise les « storms » de reconnexion
		Protège les réseaux privés contre les menaces issues des PDN/Internet	▪ Services antivirus et IPS ▪ Pare-feu L4-L7 pour la protection contre les menaces PDN/Internet ▪ Filtrage d'URL et contrôle applicatif ▪ Neutralisation des bots
		Connectivité des réseaux privés vers les PDN	▪ NAT IPv4 - IPv6

Plate-formes de sécurité	Format	Objectif	Services de la plateforme de sécurité
FortiWeb	Physique (PNF) Virtuel (VNF) Conteneur (CNF)	Protège contre les menaces et attaques sur la couche applicative du MEC	■ Protection contre les attaques applicatives du Top 10 OWASP ■ Protection contre les attaques zero-day et les menaces connues ■ Neutralisation des bots ■ Minimisation des faux-positifs par Machine Learning ■ Validation de protocole
		Protection des API des réseaux privés contre les attaques ciblant les API, les comportements suspects et les erreurs de configuration Protège l'API du plan de signaling du réseau privé vers les fonctions d'application externe (AF)	■ Support en natif de HTTP/2 ■ Vérification OpenAPI 3.0 ■ Validation du schéma, des limites et de la conformité du protocole JSON ■ Validation du schéma, des limites et de la conformité du protocole XML, entités externes, SOAP ■ Compatible WebSocket : application des signatures sur les connexions WebSockets, limites des messages et des frames, désactivation des extensions ■ Passerelle API : gestion des clés API, limites et contrôle du volume d'accès

Tableau 1 : plateformes et services de sécurité Fortinet pour les réseaux 5G privés.

Architecture d'un réseau mobile privé et indépendant des MNO

Dans cette option, il n'existe aucun lien entre les réseaux 5G privés et publics. Un tel environnement peut être déployé et géré par l'entreprise et/ou un MNO et/ou un fournisseur de technologies mobiles. Cependant, la complexité et les carences potentielles en matière de savoir-faire technique ne permettent pas, dans la majorité des cas, une mise en œuvre par l'entreprise elle-même.

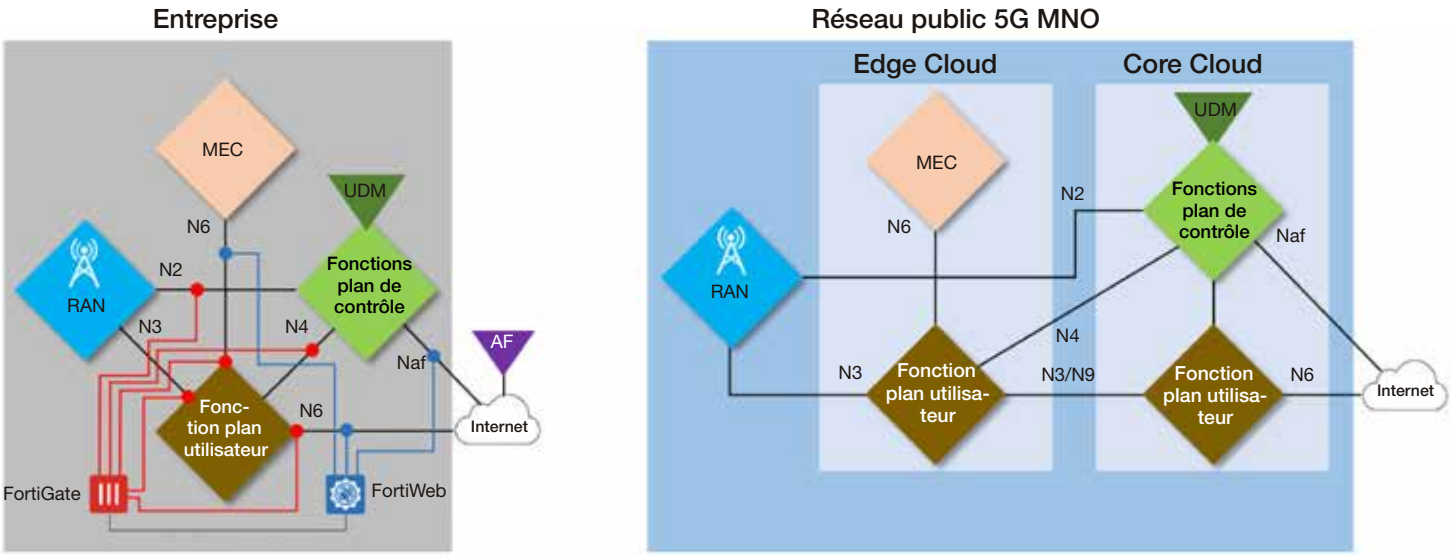

Schéma 3 : Architecture de réseau privé 5G sécurisé et indépendant des MNO

Comme l'illustre le diagramme 1, un réseau privé totalement indépendant d'un MNO dispose de ses propres caractéristiques : réseau d'accès radio (RAN), plan de contrôle, plan de données et composants MEC sur le site de l'entreprise. La fréquence 5G utilisée peut être sous licence ou pas. Il est possible d'utiliser la fréquence 5G sous licence de l'opérateur lorsque le réseau privé est conçu et géré par l'opérateur.

Selon les services du réseau privé et les cas d'utilisation, il peut être nécessaire d'établir une connexion vers les réseaux de données et Internet pour le data center d'entreprise, les partenaires, les applications et systèmes, le cloud public et certaines opérations comme l'interception autorisée du trafic de données.

Avec une solution de Fortinet, la sécurité est déployée sur site via FortiGate et FortiWeb, pour ainsi favoriser :

- **Un cloisonnement du lien vers le cœur et la maîtrise des attaques potentielles.** Dans une telle architecture, les composantes du réseau privé sont totalement isolées du réseau 5G public. Les risques potentiels associés aux menaces internes et à des utilisateurs infectés doivent être pris en compte. Dans certains pays, la réglementation exige que même les RAN 5G privés soient connectés au réseau 5G public. Cette situation exigerait une connectivité du réseau privé vers le réseau 5G public, ainsi qu'un cloisonnement total de sécurité entre les réseaux privés et les réseaux privés virtuels qui interconnectent le RAN au cœur mobile, pour les plans de contrôle et utilisateur.
- **Sécurité contre les menaces issues de l'IoT**, à l'image des « signaling storms », dispositifs infectés ou dysfonctionnants et protection contre les bots de l'IoT.
- Lorsqu'une connectivité externe est requise vers un réseau public de données, les services du **pare-feu nouvelle-génération** sont activés pour protéger contre les menaces connues et inconnues, issues d'Internet ou des réseaux PDN.
- **La protection applicative** est fournie pour les écosystèmes de l'IoT et applicatif, au sein du edge MEC du réseau privé et ailleurs.
- **La sécurité des API** est assurée pour les applications basées sur des API et pour les intégrations avec des applications tierces, au niveau du edge MEC et en externe.

La sécurité peut être déployée et gérée par l'entreprise elle-même, un partenaire ou par un MNO dans le cadre d'un réseau mobile privé fourni en tant que service managé.

Architecture d'un réseau mobile privé dépendant des MNO

Dans cette famille, les architectures diffèrent les unes des autres compte tenu du volume nécessaire de ressources 5G publiques, comme l'illustre le diagramme 1. Ces architectures sont généralement déployées par l'opérateur et gérées conjointement avec le client. Voici quelques-unes des architectures possibles pour cette catégorie.

Architecture de réseau mobile privé avec RAN mutualisé

Dans cette architecture, le RAN (postes de base gNB localisés sur le site d'entreprise) est mutualisé entre le réseau privé et le réseau 5G public, suite à un découpage du RAN. Il en résulte :

- **Une tranche privée**, où l'ensemble du trafic du plan de données et du plan de contrôle du réseau privé et des dispositifs IoT reste au sein du réseau privé et utilise les composants de ce réseau
- **Une tranche publique**, où l'ensemble du trafic du plan de données et du plan de contrôle du réseau privé quitte l'entreprise et utilise le réseau public 5G du MNO

Comme pour toutes les architectures, une connectivité doit être établie du PDN externe vers le réseau privé et le MEC.

Au-delà de l'environnement de sécurité de l'architecture indépendant du MNO, une attention spéciale doit être portée au cloisonnement et

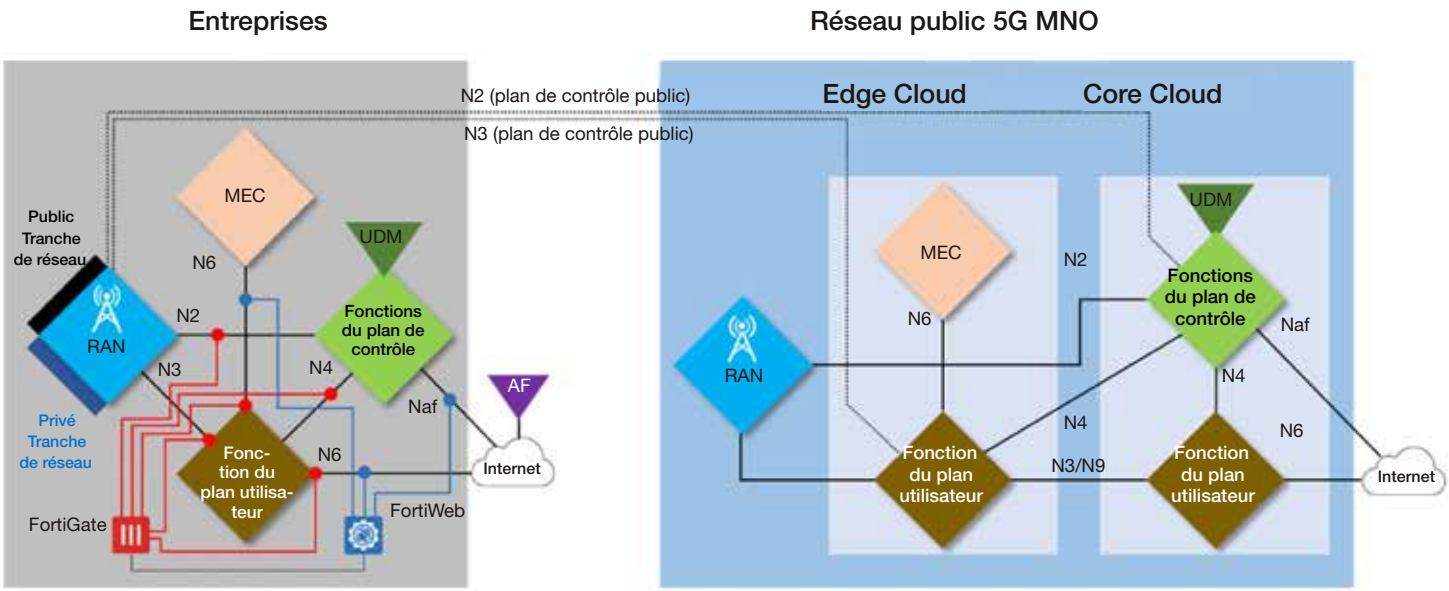

Schéma 4 : architecture de réseau privé 5G sécurisé avec RAN mutualisé.

à l'inspection DPI des VPN des plans de données et de contrôle, afin de se protéger des attaques sur les réseaux privés, celles menées à partir de la tranche publique du RAN et susceptibles d'entraîner des fuites de données.

Les solutions FortiGate et FortiWeb sont déployées sur le site d'entreprise et offrent la visibilité et le contrôle nécessaires tels que décrits dans le tableau 1.

Architecture mutualisée entre le RAN et le plan de contrôle

Au sein de cette architecture, le RAN (sur site) et le plan de contrôle sont fournis par le réseau public et dissocié du RAN public et du plan de contrôle, via une tranche dédiée de réseau privé. Ceci permet aux données de l'entreprise de rester au sein de l'entreprise tout en étant isolées du réseau public du MNO.

Il est essentiel de sécuriser les interactions entre les fonctions du plan de contrôle et les composantes du réseau privé comme l'UPF et toute autre fonction applicative. Pour cela, le MNO doit déployer une plateforme FortiGate sur le cœur de son cloud comme indiqué dans le diagramme 5 ci-dessous. La compatibilité de FortiGate aux environnements multi-tenant permet de déployer une sécurité active du RAN jusqu'au cœur, pour différentes tranches dédiées au plan de contrôle et au RAN privé, à l'aide des fonctions VNF/PNF de FortiGate.

Les fonctions du plan de contrôle sont opérées sur le réseau public et sont susceptibles d'exposer certaines données sensibles (information UE/IoT par exemple) stockées sur le cœur de réseau public du MNO (dans l'UDM). Il en résulte que le MNO doit assurer le contrôle et la confidentialité dans cette architecture.

Le plan de données et le MEC sont sur site, ce qui permet des usages et des applications exigeant une latence ultra-faible.

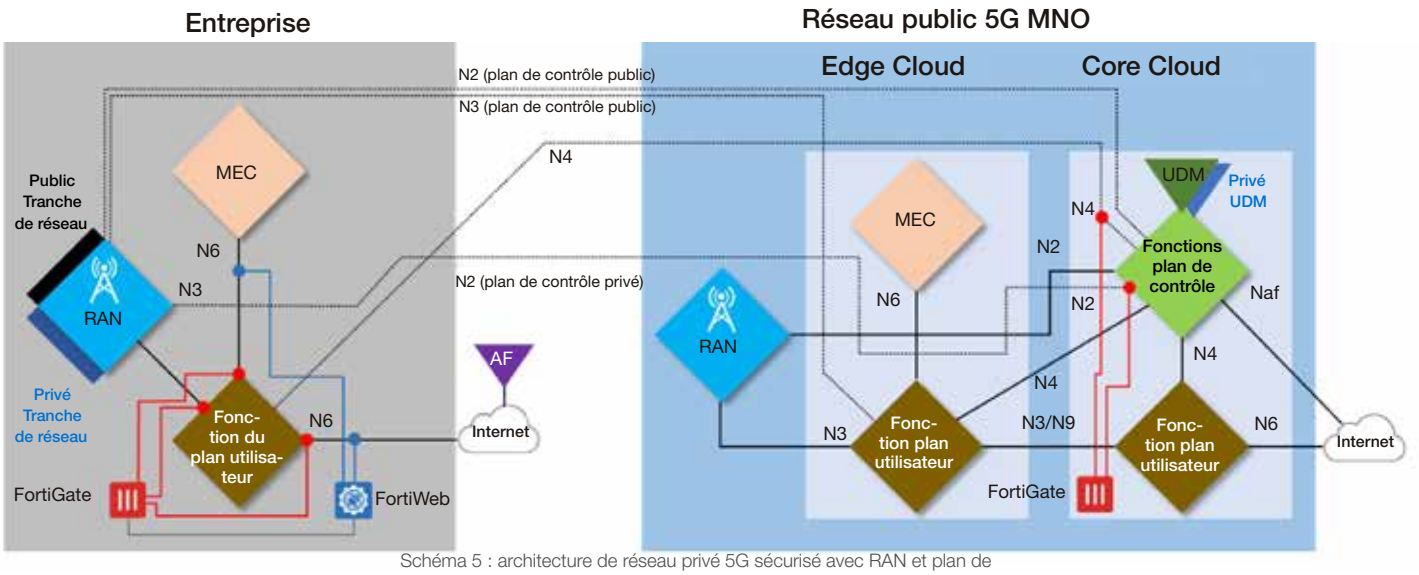

Schéma 5 : architecture de réseau privé 5G sécurisé avec RAN et plan de contrôle mutualisé.

Le découpage de bout en bout de l'architecture réseau mobile

Dans cette architecture, le réseau mobile privé de l'entreprise est un réseau virtuel issu d'un découpage de bout-en-bout et adossé à une infrastructure 5G publique. Seul le gNB est déployé sur le site d'entreprise et à disposition des dispositifs IoT/ UE. Le MEC et l'UPF sont disponibles à proximité de l'entreprise, voire au sein de l'entreprise, à disposition des usages et des applications exigeant une faible latence.

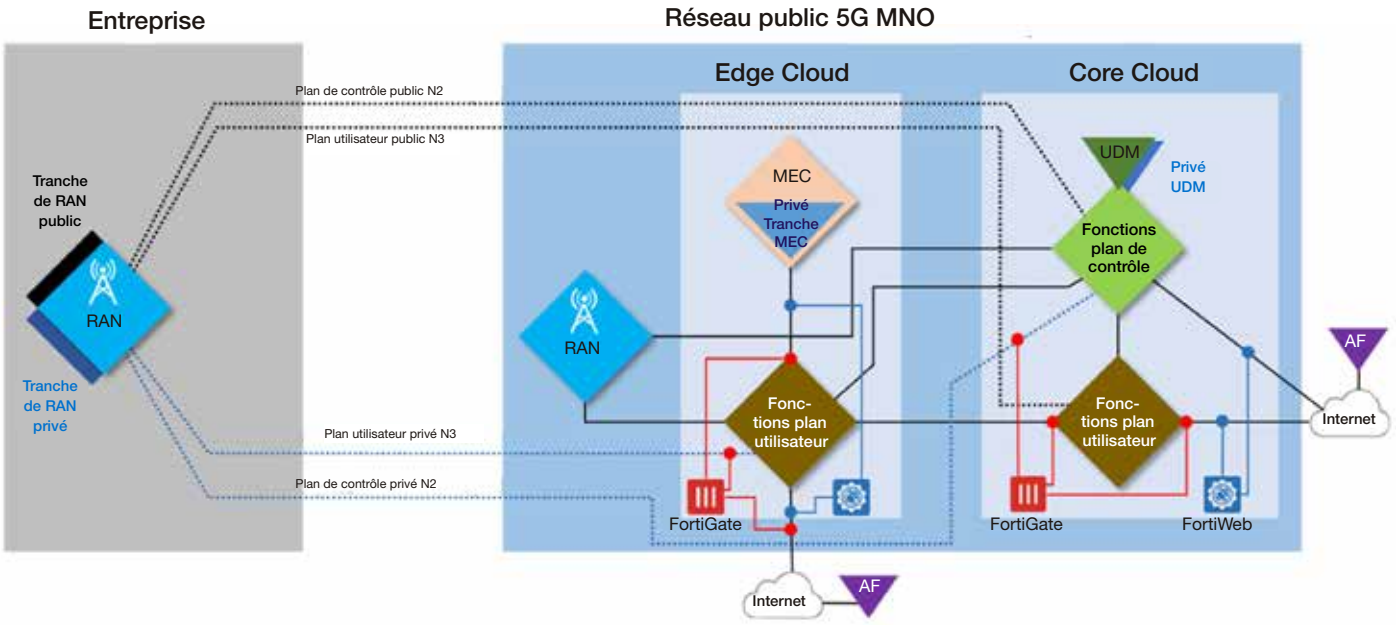

Schéma 6 : architecture de réseau privé 5G avec découpage de bout-en-bout.

Le réseau privé 5G étant adossé au réseau 5G public mutualisé, les plans de contrôle et de données, les API interagissant avec les AF externes/MEC doivent être visibles et sécurisés. Cette sécurité est offerte par FortiGate et FortiWeb de Fortinet. Ceci est essentiel pour sécuriser le réseau privé et la sécurité du réseau public 5G mutualisé. Du point de vue de la sécurité, cette architecture peut être considérée comme une « image miroir » de l'architecture indépendante du MNO—avec le MNO ayant davantage de responsabilité sur la sécurité de son offre de réseau mobile 5G.

Synthèse

Les réseaux 5G privés constituent un des premiers cas d'utilisation de la 5G, mais leur croissance reste hypothétique en l'absence d'une sécurité appropriée. Pour renforcer leurs parts de marché, les MNO doivent fournir des architectures flexibles et sécurisées qui répondent à la demande des différents secteurs d'activité pour la 5G.

Avec un panel de solutions de sécurité communes qui s'applique à de nombreuses architectures et différents cas d'utilisation, les solutions Fortinet permettent aux opérateurs de répondre aux besoins de sécurité essentiels des entreprises—soit avec une offre de réseau privé 5G ou via des services de sécurité managés.

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

mars 5, 2021 12:58 PM
771877-0-0-FR
wp-FA-securing-5G-private-mobile-networks-A4_PREP_FR