LIVRE BLANC

La sécurité des réseaux d'accès radio de la 4G et de la 5G

Évolution du réseau d'accès radio : un levier de croissance

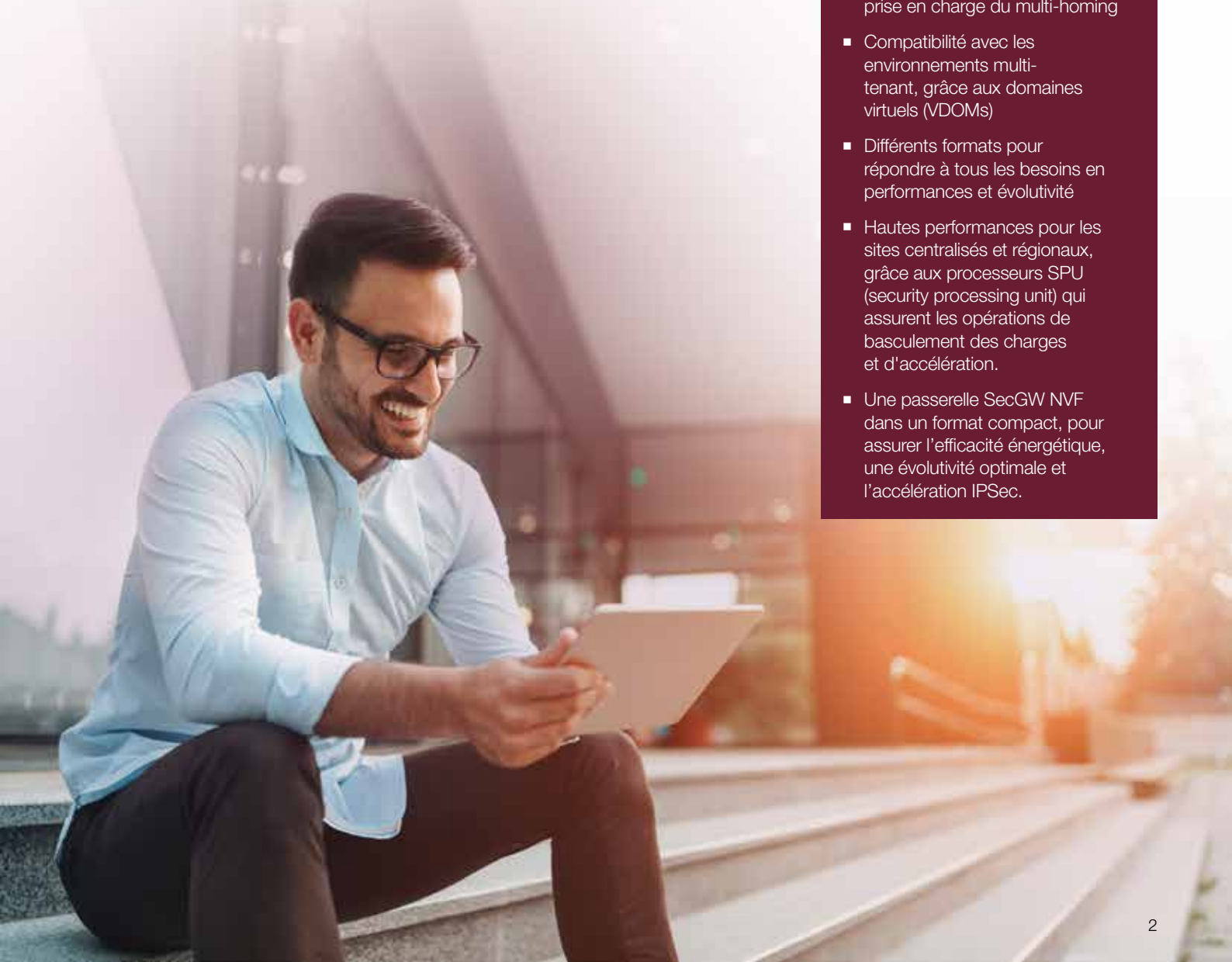
L'évolution LTE (Long Term Evolution) et le NR (New Radio) sont essentiels à la capacité d'un réseau mobile à concrétiser toutes les promesses de la 5G (bande passante renforcée, évolutivité optimale, fiabilité et faible latence) et à favoriser la croissance.

Les technologies de réseau d'accès radio (ou RAN pour Radio Access Network) pour la LTE et la 5G permettent aux opérateurs de se renforcer sur les marchés du grand public et des entreprises, tous secteurs d'activités confondus. Mais elle induisent néanmoins de la complexité, étendent la surface d'attaque et amplifient les risques qui pèsent sur l'infrastructure d'accès radio en 5G. Il est clair que l'émergence de cas d'utilisation favorisant la croissance doit s'accompagner d'une sécurité adéquate, au niveau du RAN et ailleurs dans le cloud des opérateurs.

Le 3GPP (3rd Generation Partnership Project) recommande l'utilisation d'une passerelle de sécurité (SecGW) pour protéger les accès RAN et les communications entre le RAN et le cœur mobile, ceci afin d'assurer la continuité et la confidentialité des services. La passerelle de sécurité 3GPP tire parti d'IPSec et de la gestion des certificats pour contrôler les accès via l'authentification, ainsi que la confidentialtié des données via le chiffrement. L'authentification et le chiffrement peuvent être étendus au plan utilisateur, au plan de contrôle, aux données opérationnelles et au trafic de gestion.

L'atout FortiGate pour la sécurité du RAN 5G

- Terminaison, agrégation, autorisation et authentification pour les tunnels IPsec eNB et gNB
- Segmentation pour les accès de site à site
- Sécurise les interfaces LTE S1-U et S1-MME
- Sécurise les interfaces N2 et N3 de la 5G
- Sécurise l'interface DU à CU F1-C
- Inspection DPI du trafic GTP-U encapsulé pour une protection contre les menaces connues et inconnues sur les couches L2 à L7
- Pare-feu SCTP pour inspection et application de la sécurité, avec prise en charge du multi-homing
- Compatibilité avec les environnements multi-tenant, grâce aux domaines virtuels (VDOMs)
- Différents formats pour répondre à tous les besoins en performances et évolutivité
- Hautes performances pour les sites centralisés et régionaux, grâce aux processeurs SPU (security processing unit) qui assurent les opérations de basculement des charges et d'accélération.
- Une passerelle SecGW NVF dans un format compact, pour assurer l'efficacité énergétique, une évolutivité optimale et l'accélération IPSec.



Sécurité du RAN : un besoin croissant

L'évolution du RAN, ainsi que l'ensemble des marchés et des cas d'utilisation actuels et à venir concrétisés par les technologies et infrastructures 4G/5G, font de la sécurité du RAN un impératif :

- **Toujours plus grand**
  Pour concrétiser l'évolutivité qu'offre le LTE-A et la 5G en particulier, il s'agit de déployer un réseau toujours plus important de petites cellules (small cells). Nombre de stations de base eNobeBs (eNB) et gNodeBs (gNB) femtocells, picocells et microcells sont situées dans le domaine public et dans d'autres domaines non-sécurisés. Elles sont, dans la majorité des cas, connectées aux réseaux du MNO via un rétrolien qui n'est pas de confiance. Cette perspective favorise les risques, contribue à élargir la surface d'attaque et aggrave le risque que le trafic soit détourné ou manipulé.
- **Importance et évolutivité du trafic du plan utilisateur**
  Les évolutions de la 4G et l'introduction de la 5G permettent des cas d'utilisation métiers et sectoriels qui vont au-delà de la simple connectivité sans fil. Les opérateurs peuvent ainsi définir des cas d'utilisation qui vont faire appel à différents écosystèmes pour favoriser l'innovation dans les domaines de la production industrielle, des soins de santé, des transports, de l'énergie, etc. Ces services, qui vont au-delà de la simple connectivité, mettent l'accent sur l'intégrité et la continuité du trafic du plan utilisateur dans le RAN et jusqu'au cœur. Le trafic du plan utilisateur peut devenir un levier pour permettre à un MNO d'offrir des services à valeur ajoutée (infotainment, services liés à l'Internet des objets, réalité augmentée...), alors que les services et applications utilisant les données des utilisateurs sont hébergés au sein du cloud de l'opérateur ou dans l'écosystème du cas d'utilisation.

  Ceci alimente le besoin pour davantage de sécurité, de disponibilité et de continuité pour les données du plan utilisateur. Ces données sont appelées à être plus nombreuses dans certains cas d'utilisation dans le RAN, aux côtés du trafic du plan de contrôle et du trafic opérationnel et de gestion.
- **Des architectures RAN diversifiées en place**
  La nécessité d'améliorer les performances, l'agilité, l'évolutivité et la flexibilité du RAN, associée à un objectif de maîtrise des coûts, ont incité à une évolution graduelle des technologies LTE et 5G. Il en résulte que les MNO disposeront d'un environnement RAN hybride composé de différentes architectures centralisées, distribuées et virtualisées/cloud.

  Les architectures RAN dépendront également de cas d'utilisation spécifiques à des segments de marché ou tranches réseau (slice). A titre d'exemple, les sites hébergeant les unités DU (distributed unit) et CU (centralized unit) des stations de base eNB et gNB seront choisis selon des critères de latence et de besoins en bande passante/performance.

  Dans un environnement hybride associant des architectures et composants RAN LTE -A et 5G, préserver la sécurité, l'intégrité et la visibilité sur les plans de contrôle et d'utilisateur, ainsi que sur l'environnement opérationnel et de gestion devient essentiel. Il s'agit de faire appel à des outils de sécurité suffisamment flexibles pour s'adapter aux différentes architectures, besoins et contraintes des RAN.
- **Cas d'utilisation critiques des infrastructure mobiles**
  Le LTE-A et la 5G permettent de concrétiser des cas d'utilisation innovants dans différents secteurs d'activité, comme les soins de santé, l'énergie ou encore les transports. Contrairement à la génération mobile précédente, la « normalisation » de l'infrastructure mobile et sa plus forte dépendance à ses services pour certains cas d'utilisation critiques attisent l'intérêt des cybercriminels qui voient en l'infrastructure mobile un vecteur d'attaque et une cible. La sécurité des RAN devient d'autant plus vitale.

L'évolution de l'infrastructure mobile 4G et 5G dans sa globalité et le réseau d'accès radio en particulier, encouragent un renforcement de la sécurité du RAN : des SecGW vers une infrastructure réellement sécurisée qui se veut hyper-évoltive, hybride et efficace, pour offrir des fonctions de sécurité sophistiquées SecGW et L3-L7.

Les menaces furtives au niveau du RAN

Les éléments présentés ci-dessus incitent les MNO à moderniser et renforcer la sécurité de leur RAN existant afin d'assurer la confidentialité, l'intégrité et la continuité de leurs services. Les plans de communication (contrôle, utilisateur et Opérationnel/gestion) qui ne sont pas sécurisés de manière pertinente peuvent subir différents types d'attaque :

- Introduction de stations eNB et gNB indésirables, à partir desquels des attaques vers le cœur mobile peuvent être menés
- Attaques de type Man in the Middle (MIIM) pour intercepter le trafic des plans de contrôle et d'utilisateur
- Dénis de service (DoS/DDoS)
- Injection de trafic malveillant (malware) pour attaquer et manipuler les éléments du cœur
- Erreur de configuration ou mise à jour défaillante au sein du RAN

Chacune de ces attaques peut potentiellement perturber le RAN, le cœur et la continuité des services. Les données utilisateur deviennent vulnérables tandis que les applications et services cloud de l'opérateur et des clients peuvent être impactés. Ceci nuit à la capacité du MNO à assurer sa conformité aux réglementations en matière de protection des données et de sécurité.

La plateforme FortiGate propose de nombreuses fonctions réseau physiques et virtuelles, notamment de passerelle SecGW et de pare-feu NGFW. La confidentialité des plans de contrôle et utilisateur est assurée tandis que la haute disponibilité des services et la continuité des activités sont préservés face aux cyber-attaques.

L'infrastructure de sécurité RAN de Fortinet

La solution Fortinet pour la sécurité du RAN tire parti de la plateforme FortiGate, que celle-ci soit proposée dans un format matériel ou virtuel. FortiGate apporte trois fonctionnalités clés de sécurité pour le RAN :

- **Confidentialité** – FortiGate protège le trafic utilisateur sur l'ensemble du RAN et sur le cœur du data center central ou les edges MEC (multi-access edge compute).
- **Intégrité** – FortiGate prévient toute modification prohibée des données utilisateur (injection de malware, trafic indésirable...)
- **Disponibilité et continuité** – FortiGate protège contre les attaques ciblant le RAN ou les composants du cœur et susceptibles d'entraîner une dégradation, voire une interruption des services.

FortiGate propose une plateforme unique qui offre une passerelle SecGW et un pare-feu nouvelle-génération (NGFW). Ces outils robustes fournissent des fonctions optimales et parfaitement adaptées aux environnements RAN 4G et 5G les plus étendus.

- La terminaison et l'aggrégation des tunnels IPsec pour les stations eNB et gNB, compatibles avec une autorisation et une authentification PKI (Public Key Infrastructure)
- Des fonctions de segmentation interne pour une segmentation des accès de site à site
- Sécurise les interfaces LTE S1-U et S1-MME
- Sécurise les interfaces N2 et N3 de la 5G
- Sécurise l'interface DU à CU F1-C
- L'inspection DPI du trafic GTP-U encapsulé assure une protection contre les menaces connues et inconnues sur les couches L2 à L7
- Pare-feu SCTP pour inspection et application de la sécurité, avec prise en charge du multihoming
- Compatibilité avec les environnements multi-tenant, grâce aux domaines virtuels (VDOM)
- Différents formats pour répondre à tous les besoins en performances et évolutivité
- Hautes performances pour les sites centralisés et régionaux, grâce aux processeurs SPU (Security Processing Unit) qui assurent les opérations de basculement et d'accélération
- Une passerelle SecGW NVF dans un format compact assure l'efficacité énergétique, une évolutivité optimale et une accélération IPSec
- De nombreuses API (application programming interface) et connecteurs pour faciliter l'intégration de différentes fonctions (gestion, orchestration, BSS) au sein de l'écosystème global du MNO

Architecture de l'infrastructure de sécurité RAN de Fortinet

Alors que les MNO migrent vers des environnements 5G NSA (non-autonomes) et SA (autonomes), les RAN LTE et 5G sont appélés à co-exister dans une certaine mesure. La richesse fonctionnelle de FortiGate et sa disponibilité en différents formats en font un choix idéal pour sécuriser les RAN et architectures hybrides. Avec la LTE-A et la 5G NR, il existe un lien important entre les catégories de services, la qualité de services (QoS), les accords de niveau de service (SLA) et l'environnemnet RAN, et donc un lien direct vers l'infrastructure de service et les services déployés.

À titre d'exemple, les SLA et la QoS pour les catégories de services eMBB (enhanced mobile broadband), mMTC (massive machine-type communication) et uRLLC (ultra-reliable low latency communication) sont fournis vis des tranches du réseau. Les besoins de chaque tranche de réseau sont pris en charge par un mix de composants RAN et coeur, centralisés ou distribués. Ceci détermine l'architecture et les options de déploiement pour la passerelle SecGW, comme l'indique le schéma 1 ci-dessous.

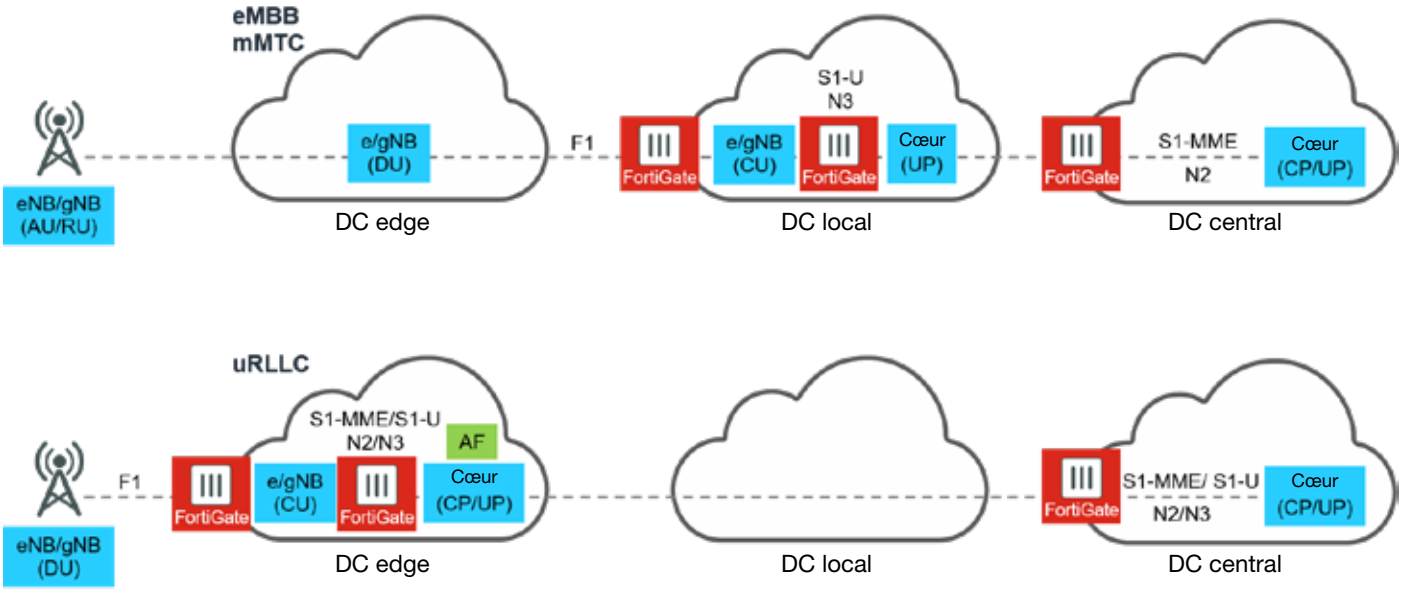


Schéma 1: Tranches réseau eMBB, mMTC et uRLLC - distribution des composants RAN

Alors que les opérateurs mobiles définissent leur infrastructure 5G, leur environnement RAN est constitué d'architectures et de technologies LTE, LTE-A et 5G NR, qui coexisteront et collaboreront au cours des années à venir. L'infrastructure de sécurité RAN en place doit fournir des outils compatibles avec le mix de technologies et d'architecture RAN, pour davantage d'agilité et de flexibilité.

Déploiement centralisé des SecGW

Dans une architecture SecGW centralisée, les éléments du plan de contrôle et utilisateur sont localisés au niveau des postes de base eNB et gNB. Ils bénéficient d'un tunnel IPSec vers la Sec GW FortiGate centrale qui prend en charge le plan de contrôle, le plan utilisateur et les services de sécurité avancés.

Pour cette passerelle SecGW centralisée, les performances et l'évolutivité de la sécurité sont d'une importance majeure, ainsi que la résilience et la haute disponibilité du service. Pour tenir ces objectifs, les appliances physiques FortiGate fournissent des performances de sécurité et IPsec accélérées par matériel, avec une latence ultra faible et des options de haute disponibilité.

Le nouveau FortiGate 4000F bénéficie de la 7eme génération des processeurs SPU de Fortinet, et offre ainsi les performances nécessaires pour la LTE-A et la 5G NR :

- Performances optimales pour le trafic, jusqu'à 110Gbps
- Performances optimales, même pour les flux volumineux de données
- Latence ultra-faible, de l'ordre du µs
- Technologie complète, sans commande supplémentaire
- Prise en charge complète de la QoS
- Mise en miroir du trafic X2/Xn
- Option de cluster évolutif et redondance
- Compatible QKD (Quantum key distribution)
- Failover et mise à jour logicielle sans interruption de service
- Efficacité énergétique et format compact

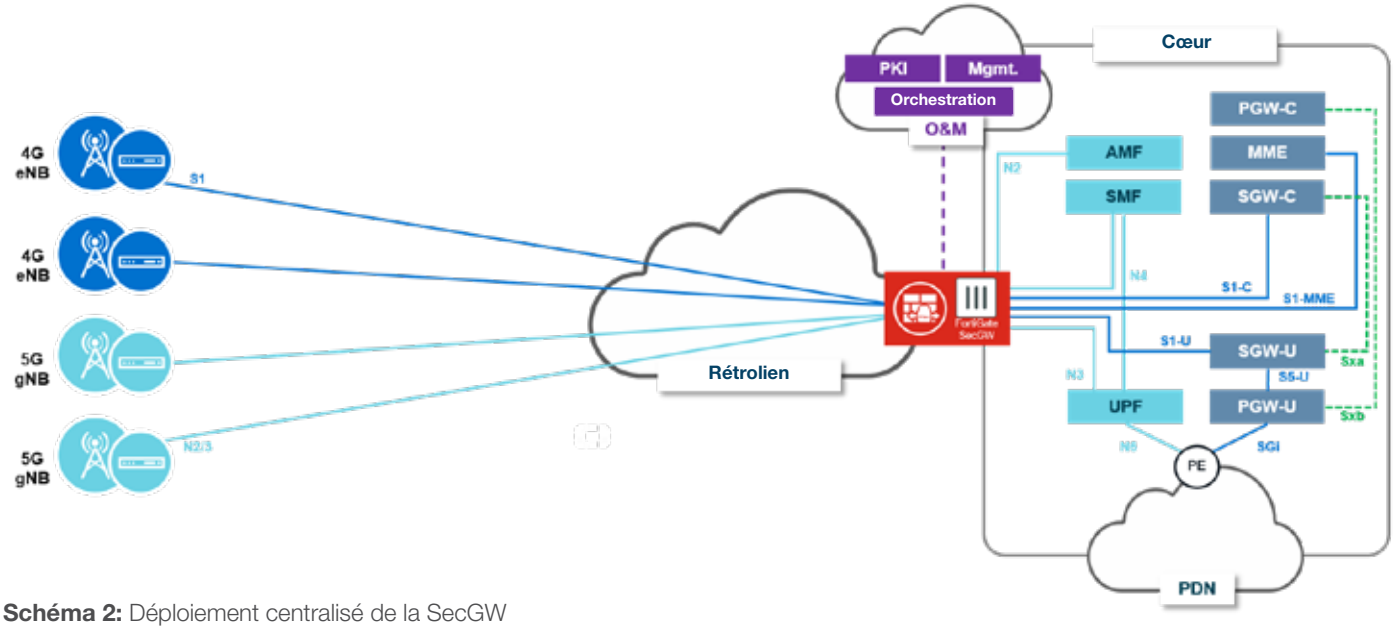


Schéma 2: Déploiement centralisé de la SecGW

FortiGate offre toutes les fonctionnalités SecGW et NGFW, au travers d'une fonction VNF (virtual network function) efficace et compacte pour les petites cellules et les sites edge. Les fonctions PNF (physical network function) de FortiGate tirent parti des processeurs SPU (security processor unit) de Fortinet, pour offrir des performances évolutives et une latence ultra faible pour les data centers régionaux et le coeur mobile.

SecGW distribué avec déploiement sur l'edge cloud

La possibilité de terminaison des liens VPN du plan utilisateur au niveau de l'edge cloud/MEC et de manière sécurisée, constitue un impératif pour les services géolocalisés, les applications critiques de l'IoT, la conduite autonome de véhicule, etc. L'edge cloud/MEC offre un PDN (packet data network) local mais peut également héberger des applications (composants IoT, applications industrielle, etc.) pour offrir le service et les fonctionnalités requises, au plus proche de l'utilisateur de ce service.

Dans cette architecture, la passerelle SecGW est le point de terminaison du lien RAN vers le cœur. La SecGW de FortiGate est rajoutée au edge cloud/MEC en tant que point de terminaison des VPN du plan utilisateur et pour sécuriser les données utilisateur du PDN local et des applications/services hébergés en local sur l'edge.

Le choix entre déployer un PNF ou une SecGW FortiGate sur l'edge cloud/DC se fera essentiellement sur des critères d'évolutivité et de latence.

- Nombre de VPN IPSec
- Volume de données du plan utilisateur
- Modèle d'utilisation (stable ou évolutif dans le temps, amélioration et diminution dans le temps)
- Exigence de la latence
- Consommation énergétique et performances

L'utilisation de FortiGate SecGW VNF est un levier de flexibilité et agilité en matière d'évolutivité des services. Pour autant, la dépendance à des ressources mutualisées VNFI (virtual network function infrastructure) dont les les performances, l'évolutivité et la latence ne sont pas optimisées, peut grever les performances de la VNFI. Dans ce contexte, FortiGate SecGW VNF n'est recommandé que pour les cas d'utilisation nécessitant des performances basses à moyenne et une latence moyenne.

L'utilisation de FortiGate SecGW PNF assure des performances optimales et une latence ultra faible, grâce aux processeurs SPU de Fortinet. L'utilisation d'un PNF est recommandée pour les cas d'utilisation qui exigent des performances et une évolutivité optimales, et/ou pour les DC régionaux/edge à forte concentration de postes eNB/gNB.

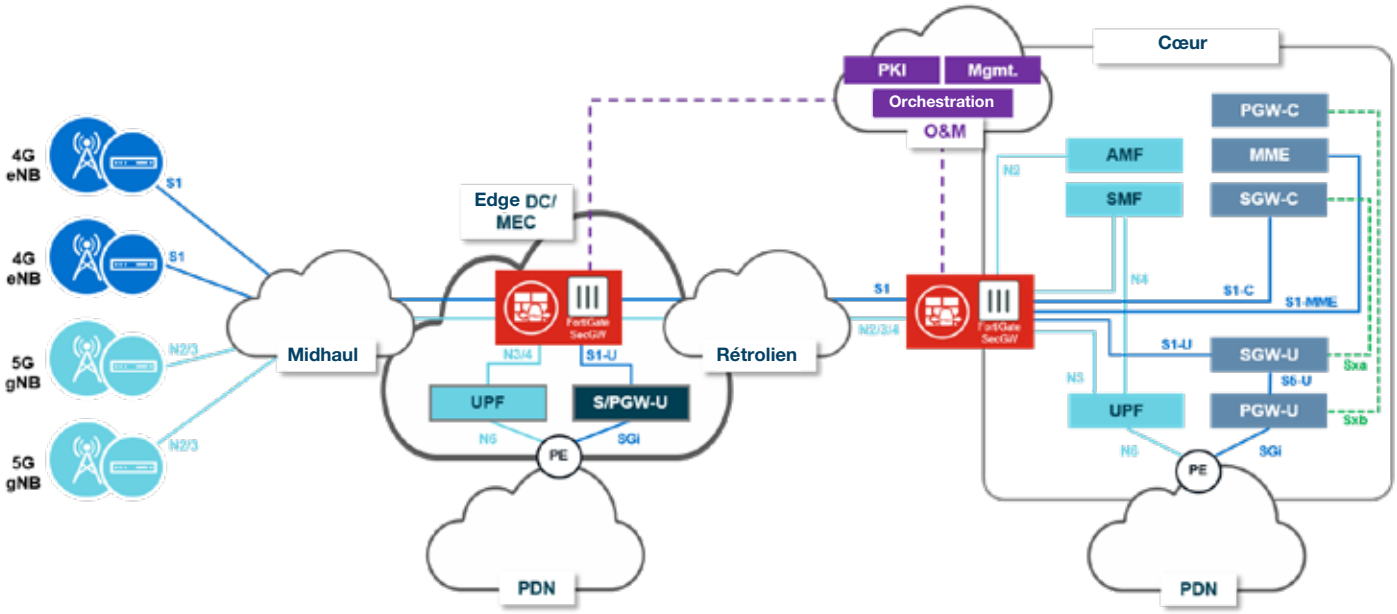


Schéma 3: SecGW distribué avec déploiement sur l'edge cloud

SecGW distribué au sein d'un RAN virtualisé et décomposé

Dans le cas d'un vRAN décomposé, la passerelle SecGW apporte des fonctions IPSec et de sécurité à la connectivité DU-CU. Comme l'illustre le schéma 4, cette connectivité est découplée et présente sur différentes parties du réseau. L'intégrité et la confidentialité des plans utilisateur et de contrôle est assurée par le protocole Packet Data Convergence Protocol (PDCP-U & PDCP-U), mais certains messages du plan de contrôle sont émis en clair. Le plan de contrôle F1 (F1-C) devient vulnérable aux menaces SCTP s'il n'est pas sécurisé et protégé par la SecGW.

Dans le cadre d'une architecture décomposée, la solution SecGW de Fortinet offre une authentification et une autorisation DU-CU avec IPSec, avec une connectivité en tunnel, une confidentialité assurée par chiffrement lorsque nécessaire et une protection contre les attaques sur la couche SCTP pour le plan F1-C.

Le volume de données du plan de contrôle étant relativement faible, FortiGate SecGW peut être déployé en amont du CU entant que VNF pour la sécurité de F1-C.

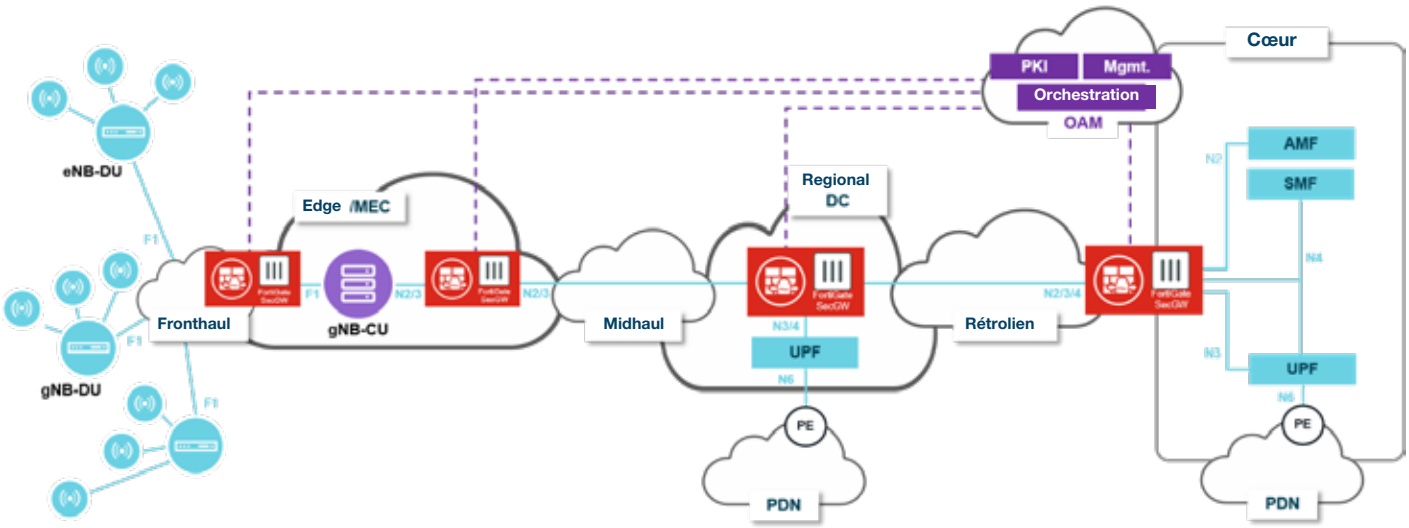


Figure 4: SecGW distribué au sein un RAN virtualisé et décomposé

Connectivité par petites cellules

Les femtocells, picocells et microcells sont déployés pour créer un réseau dense de petites cellules dédiée à l'évolutivité des capacités et du périmètre de couverture pour la LTE-A et la 5G NR.

Le déploiement et l'exploitation de ces réseaux d'envergure révèle de nombreux défis, en matière de coûts et de sécurité notamment. Certaines de ces micro-cellules peuvent également être des ressources mutualisées qui favorisent la maîtrise des coûts et amélioreront le ROI.

Les principaux défis de sécurité résultant des petites cellules sont les suivantes :

- **Un rétrolien non sécurisé :** dans la majorité des cas, les petites cellules sont connectées aux sites/data centers centraux, régionaux et même au edge du MNO, via un lien PDN qui n'est pas de confiance. Ceci expose les plans de contrôle et utilisateurs à des menaces, carences en matière de confidentialité et attaques susceptibles d'impacter la disponibilité et la qualité de service.
- **Évolutivité :** les petites cellules renforcent les besoins de la SecGW en matière d'évolutivité, avec des réseaux denses de petites cellules interconnectées via des VPN IPSec avec le cœur et les sites MEC du MNO.

L'évolutivité et les performances optimales de la SecGW de Fortinet et sa disponibilité en de nombreux formats offrent au MNO la capacité à répondre à ces défis et à sécuriser la connectivité des petites cellules à l'aide des mêmes outils et fonctionnalités communs fournies aux macro-cellules.

LE MOT DE LA FIN

La sécurité d'un réseau d'accès radio 4G et 5G versatile, hybride et évolutif est plus importante que jamais, compte tenu de la nature évolutive de la technologie et de nouveaux cas d'utilisation possibles. La sécurité du RAN exige une nouvelle infrastructure SecGW, agile et hybride, et compatible au mix d'architectures et aux différents besoins en performances, évolutivité et QoS de la LTE-A et de la 5G.

La plateforme FortiGate de Fortinet propose une plateforme SecGW flexible et hyperscale qui est déjà en production chez les principaux MNO dans le monde. Les fonctionnalités et les performances de ces passerelles SecGW et pare-feux de nouvelle génération sont sans équivalence sur le marché. Elles permettent aux MNO de se positionner sur de nouveaux cas d'utilisation de la 4G et de la 5G et sur les opportunités commerciales qui en découlent.

FORTINET

www.fortinet.fr

mars 5, 2021 12:45 PM

668851-0-1-FR