FICHE SOLUTION

Sécuriser les infrastructures et les services 4G et 5G avec Fortinet

Synthèse

Les évolutions technologiques des réseaux mobiles 4G et l'émergence de la 5G apportent aux opérateurs mobiles (MNO - Mobile network operator) l'opportunité de changer en profondeur les marchés sur lesquels ils se positionnent, ainsi que le périmètre et la valeur de leurs services. Les fonctionnalités et services nouveaux sont essentiels pour promouvoir l'innovation dans tous les secteurs d'activité, de l'industrie manufacturière à l'énergie, des transports aux soins de santé. Les promesses de la 5G sont nombreuses, à condition de sécuriser cette technologie.

L'innovation digitale dans les réseaux mobiles engendre une dualité dans les environnements mobiles : la sécurité interne des infrastructures mobiles et, d'autre part, la sécurité et la monétisation des cas d'utilisation externes. Fortinet aide tous les secteurs d'activité à concrétiser les avantages de la 4G, et de la 5G à venir, grâce à une stratégie de réseau orienté sécurité et un accompagnement approprié pour optimiser les services et l'expérience utilisateur.

Sécurité interne des infrastructures mobiles

Les précédentes générations de technologies mobiles ciblaient essentiellement le grand public et tiraient leurs revenus d'un panel restreint de services de voix, de messagerie et Internet. Les contenus étaient, pour l'essentiel, fournis par des tiers et non pas l'opérateur lui-même.

Ce contexte a favorisé une approche minimale à la sécurité pour protéger les éléments vulnérables des infrastructures mobiles (réseau public de données, réseaux d'accès radio et connectivité en roaming) contre les menaces externes, et ainsi assurer la continuité de services. Mais compte tenu de l'évolution des infrastructures et technologies mobiles, il doit en être de même avec l'infrastructure de sécurité en place. Et la 5G s'annonce en tant que test ultime pour savoir si les réseaux peuvent garantir sécurité ET expérience utilisateur de premier rang.

Sécurité et monétisation des cas d'utilisation externes

La mise en œuvre de nouvelles technologies sur les réseaux 4G et 5G permet aux opérateurs d'offrir davantage de services à valeur ajoutée, qui vont bien au-delà de la connectivité mobile. Ce mix de fonctionnalités peut donner lieu à des services qui permettront aux opérateurs mobiles de répondre aux besoins évolutifs de différents secteurs.

La sécurité dans le cadre d'un cas d'utilisation sectoriel est importante pour les raisons suivantes :

- L'adoption et l'adaptation des cas d'utilisation dépendent de la capacité de l'opérateur à respecter les accords SLA.
- Lorsqu'un opérateur mobile fournit des services à valeur ajoutée (applications, plateformes, écosystèmes de partenaires, etc.) liés à un cas d'utilisation (au-delà de la simple connectivité), leur capacité à sécuriser ces composants devient essentielle pour concrétiser le cas d'utilisation.
- La visibilité et le contrôle sur la sécurité d'un cas d'utilisation peuvent être monétisés en fournissant un service de sécurité managé au client, contribuant ainsi aux revenus et à la croissance de l'opérateur.

Avec la disponibilité croissante de services mobiles et cas d'utilisation innovants, les cybercriminels commenceront à cibler ces cas d'utilisation. Un élément important à prendre en compte dans la stratégie globale de sécurité de l'opérateur mobile.

L'infrastructure de sécurité Fortinet pour les opérateurs mobiles : sécuriser l'innovation et favoriser la croissance

Fortinet offre un panel de solutions et d'outils de sécurité offrant une visibilité et un contrôle de bout en bout sur les infrastructures 4G et 5G, tout en assurant la monétisation et la sécurité des cas d'utilisation du secteur. Cette approche facilite le déploiement de la sécurité tout en minimisant les efforts opérationnels et de gestion. Les produits et services portent sur le pare-feu nouvelle-génération FortiGate et le pare-feu d'application Web (WAF) FortiWeb. Ensemble, ces solutions sécurisent les stratégies d'innovation des opérateurs en matière de technologie, de services et de cas d'utilisation, tant pour le grand public que pour les professionnels.

Apporter une sécurité interne agile et performante aux infrastructures et services mobiles

Le schéma ci-dessous illustre comment la solution Fortinet protège l'infrastructure des MNO contre les menaces et assure la disponibilité et la continuité de leurs services.

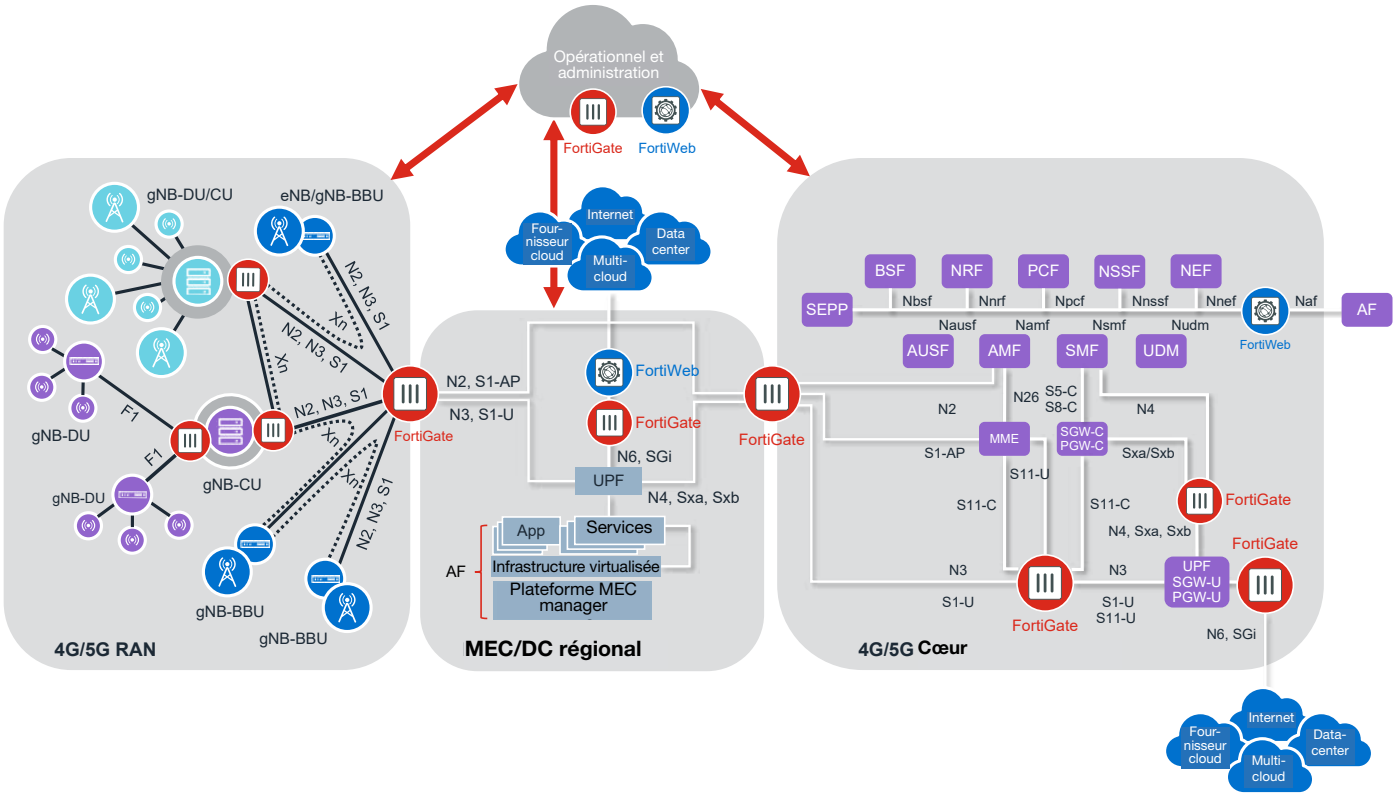

Schéma 1 : sécuriser l'écosystème MNO

Sécurité des réseaux d'accès radio

Sécuriser un réseau d'accès radio (RAN pour Radio Access Network) 4G et 5G versatile, hybride et évolutif est devenu encore plus important face aux évolutions des technologies radio et des cas d'utilisation. La sécurité du RAN implique une nouvelle infrastructure SecGW (passerelle de sécurité) qui serait agile et hybride, mais aussi adaptée à des architectures hybrides et capables de répondre aux différents besoins de la LTE-A et de la 5G en matière de performances, d'évolutivité et de qualité de service (QoS). Les fonctions PNF (physical network function) et VNF (virtual network function) de FortiGate offrent une plateforme SecGW commune, flexible et hyperscale qui est déjà en production chez les principaux MNO dans le monde. Les fonctions et performances SecGW et NGFW comptent parmi les meilleures du marché, et concrétisent ainsi une plateforme à partir de laquelle les MNO gèrent leurs réseaux privés virtuels RAN IPsec et sécurisent les plans utilisateur et de contrôle sur S1, N2, N3 et Xn.

Sécurité de l'écosystème MEC (Multi-access Edge Computing)

Le déploiement de ressources de stockage, réseau et informatiques sur les sites MEC permet aux MNO de bénéficier d'une latence ultra-faible pour les applications et les cas d'utilisation, que ces derniers soient totalement hébergés sur le site MEC ou intégrés dans un environnement cloud plus large. Ceci exige également de mettre un terme aux données associées aux utilisateurs avec une fonction UPF (user plane data) et un PDN local qui assurent la connectivité IP, ainsi que des API vers les applications et les écosystèmes de partenaires.

La plateforme VNF/PNF Fortinet offre un NAT de qualité opérateur et une visibilité sur les opérations de pare-feu sur les couches L3 à L7, pour sécuriser le trafic associé aux fonctions de contrôle et aux utilisateurs, ainsi que la connectivité PDN au niveau du MEC. La plateforme FortiGate peut également être utilisée pour monétiser la sécurité au travers de services managés proposés aux clients mobiles (sécurité des objets connectés, contrôle applicatif, protection contre les botnets et davantage).

Les fonctions PNF, VNF ou CNF (cloud-native network) offrent une sécurité applicative et des API basées sur l'intelligence artificielle pour les applications hébergées en local dans un MEC, ainsi que l'intégration et la fourniture d'applications et de services à partir de partenaires cloud.

Sécurité des accès non-3GPP

Les technologies d'accès non-3GPP, à l'instar des technologies WLAN (réseau sans fil) peuvent être interconnectées au cœur de réseau 3GPP comme EPC (evolved packet core) de différentes manières, selon le modèle économique de l'opérateur et les préférences d'architecture. Pour les accès non-3GPP non sécurisés, le dispositif de l'utilisateur se connecte dans un premier temps à la fonction N3IWF (Non-3GPP Interworking Function), puis à la fonction AMF (access and mobility management function) ou à la fonction UPF pour les accès 3GPP.

La plateforme FortiGate assure une fonction de pare-feu SCTP (Stream Control Transmission Protocol) pour le plan de contrôle N3IWF N2 et des services NGFW pour les couches L4 à L7 pour le trafic du plan utilisateur N3. Les accès qui ne sont pas de confiance sont ainsi sécurisés sur les deux plans.

Sécurité du cœur mobile

Le cœur mobile, associé au RAN, facilite la fourniture de services de base ou évolués à l'intention du grand public et des entreprises, ainsi que de nombreux cas d'utilisation. Ce constat, ainsi que différentes évolutions technologiques (dissociation entre les plans de contrôle et utilisateur, virtualisation, connectivité PDN, services roaming de partenaires, connectivité RAN, architectures orientées services..) font du cœur mobile une cible privilégiée pour les attaques.

Les même outils utilisés pour sécuriser le RAN et le MEC sont utilisés pour la sécurité du cœur mobile, ce qui offre une sécurité, une visibilité et un contrôle de bout en bout de l'infrastructure mobile.

La plateforme PNF/VNF FortiGate offre :

- Une sécurité des couches L4 à L7 des réseaux 4G/5G et des services CGNAT, avec une forte évolutivité et une latence ultra-faible sur les liens SGI et N6
- La sécurité du plan de données avec un pare-feu GTP-U et une inspection DPI sur N3 et S1-U
- Une passerelle de sécurité (SecGW) du cœur jusqu'au RAN, avec une forte évolutivité VPN et de la bande passante.
- Une sécurité du plan de données au plan de contrôle sur Sxa/Sxb et N4

Les fonctions SBA de la 5G utilisent des appels API sur HTTPv2 pour les communications sur le plan de contrôle. La plateforme FortiWeb protège contre les attaques sur la couche applicative. Elle assure également l'application des schémas API, ainsi que les fonctionnalités de l'API de la passerelle pour la fonction SBA.

Sécurité des réseaux privés 4G/5G

Les réseaux privés cellulaires offrent des avantages qui peuvent être nécessaires à nombre de cas d'utilisation : connectivité, QoS, sécurité, haute disponibilité, latence et davantage.

La fourniture et la gestion de réseaux privés cellulaires varient selon l'architecture, les services, les fonctionnalités, la complexité et les besoins de l'entreprise. Les réseaux privés peuvent être fournis au sein d'un environnement totalement privé et cloisonné sur le site d'entreprise (RAN, MEC et cœur), ou au sein d'un environnement partagé entre l'entreprise et le MNO (RAN et plan de contrôle mutualisés), ou en tant que segment du réseau.

Quelle que soient l'architecture et la solution, la sécurité doit être intégrée à différents points de l'architecture pour assurer la disponibilité du service et l'intégrité des données du plan utilisateur. Les plateformes FortiGate et FortiWeb offrent une visibilité et un contrôle sur la sécurité, quelle que soit l'architecture et les services du réseau privé, et avec une sécurisation des éléments suivants : RAN SecGW, CGNAT, L4-L7 NGFW, API et applications.

Sécurité et monétisation de cas d'utilisation sectoriels

Les services de sécurité intégrés au sein des plateformes FortiGate et FortiWeb, déjà utilisés pour sécuriser l'infrastructure mobile, peuvent également s'appliquer à des cas d'utilisation sectoriels et favoriser une monétisation de la sécurité grâce à des cas d'utilisation sectoriels. Ils permettent également la monétisation de la sécurité grâce à la fourniture de services de sécurité managés et adaptés à chaque cas d'utilisation.

Ainsi, une usine de production intelligente peut utiliser FortiGate pour son MEC ou son data center pour se protéger contre les attaques IoT et les dysfonctionnements, mais aussi déployer des services de sécurité pour le site en lui-même (antimalware, protection contre les botnets, contrôle applicatif, filtrage d'URL et davantage). FortiWeb peut offrir une sécurité des applications et des API, à l'intention des applications industrielles du site, hébergées dans le MEC et lors de leur intégration avec des applications tierces. Et avec les mêmes plateformes FortiGate et FortiWeb utilisées dans le RAN, le MEC et le cœur, la mise en œuvre de la sécurité dans le cadre de nouveaux cas d'utilisation et de la fourniture de service de sécurité aux entreprises deviennent plus rapide et économique.

Synthèse

Grâce à deux plateformes professionnelles, FortiGate et FortiWeb, Fortinet permet aux MNO de sécuriser leur infrastructure mobile 4G et 5G, de protéger des cas d'utilisation innovants en entreprise, d'offrir des réseaux privés qui intègrent des services de sécurité et de monétiser la sécurité grâce à Fortinet.

L'utilisation d'outils de sécurité communs permet aux opérateurs de simplifier le déploiement et l'exploitation de leur sécurité sur l'ensemble des infrastructures et services mobiles, de réduire leurs coûts, de renforcer leurs équipes de sécurité et d'améliorer leur agilité et capacité de manière générale, pour ainsi encourager la confiance et favoriser l'adoption parmi les clients.

mars 5, 2021 12:36 PM

734139-0-1-FR

sb-FA-securing-4G-and-5G-A4_FR