Les APNs dédiés, offre Secure Mobile Access

Sommaire

Secure Mobile Access, l'offre des APNs dédiés

Avec un APN dédié, ce point d'accès est dédié à un compte entreprise, contrairement aux autres types d'APN, qui sont mutualisés entre les différents clients de France Telecom Orange.

Les composants intermédiaires
Le raccordement est effectué directement entre le réseau Orange (la PGW, point d'accès GPRS, UMTS ou LTE) et l'intranet du client. Aucun composant applicatif intermédiaire n'intervient dans la chaîne de liaison.

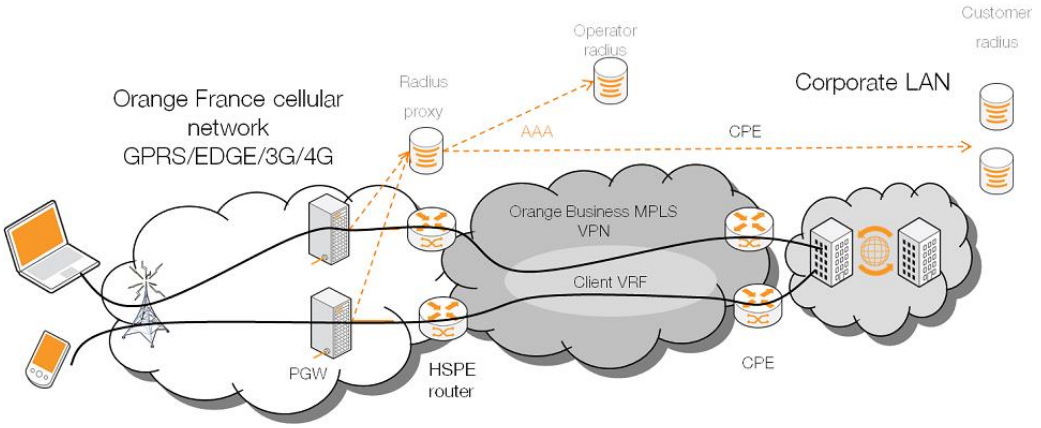
Protocoles autorisés
Sur cet APN aucun filtrage n'est appliqué. C'est l'entreprise qui en charge d'appliquer un filtrage éventuel des flux, au niveau des routeurs de son entreprise.
La rubrique 'Caractéristiques techniques des APNs et offres Orange', liste les protocoles autorisés -entrants et sortants- par APN.

Nature des adresses IP allouées
Ces accès étant de type "privés" au sens "réservés" au seul usage d'une entreprise, cette dernière choisit les plages d'adresses IP qui seront allouées à ses terminaux lors de leur connexion, dans le plan d'adressage de son Système d'Information. Tout APN dédié repose sur **deux PGWs en partage de charge pour assurer une meilleure disponibilité du service**. Les connexions se font aléatoirement sur l'une ou l'autre des deux PGWs configurés pour l'APN du Client, le Client **doit donc fournir 2 ensembles d'adresses IP de son choix** (ci-après désignés sous le terme "pools IP"). Chaque pool sera alors configuré sur un des deux PGWs utilisés par le Client.

Gestion de la sécurité
Les services de sécurité mis en œuvre sur ce type d'APN sont : réseau de données privé : confidentialité et intégrité
authentification renforcée : niveau réseau mobile (provisionning des lignes autorisées à accéder à l'APN de l'entreprise) + authentification Radius (possibilité d'authentification forte supplémentaire type Secure ID).

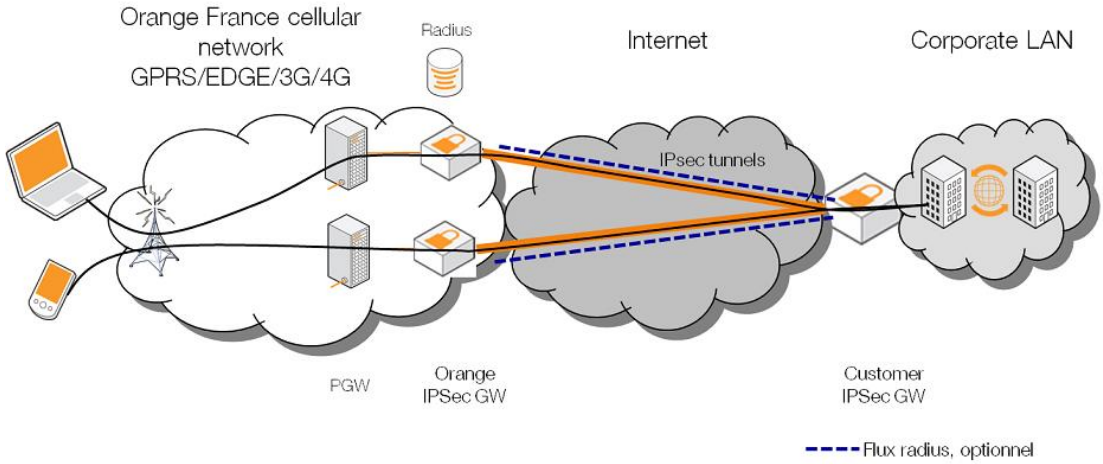
Secure Mobile Access Intranet

Dans le cas de Secure Mobile Access **Intranet**, le réseau du client est accédé par le raccord de cet APN dédié au réseau privé virtuel (VPN) mis à disposition de l'entreprise qui bénéficie de l'offre IPVPN.



Secure Mobile Access Internet

Dans le cas de Secure Mobile Access **Internet**, le site central du client est accessible grâce à la mise en place par le client d'une passerelle IPSec dans ses locaux.



Note 1 : le suffixe du nom de l'APN dépend de son type :

- "fr" (sans les guillemets) pour un APN dédié de type **intranet**
- "vp" (sans les guillemets) pour une APN dédié de type **internet**

Note 2 : Les règles d'authentification de l'entreprise peuvent varier sur un APN dédié de type intranet, suivant le serveur d'authentification (de type RADIUS uniquement) retenu par le Client :

- le serveur RADIUS proposé par Orange Business Services (par défaut), qui authentifie les utilisateurs sur le couple (login/mot de passe), avec le login de la forme user_id@entreprise1.fr.fg

ou

- son ou ses propre(s) serveur(s) RADIUS (auquel cas, le Client peut authentifier ses utilisateurs selon ses propres règles, comme par exemple le couple IMEI [identifiant unique du terminal] / MSISDN [N° data de la SIM dans le terminal])

Plus de détails sur la sécurité des réseaux mobiles dans le dossier Sécurité des réseaux mobiles.