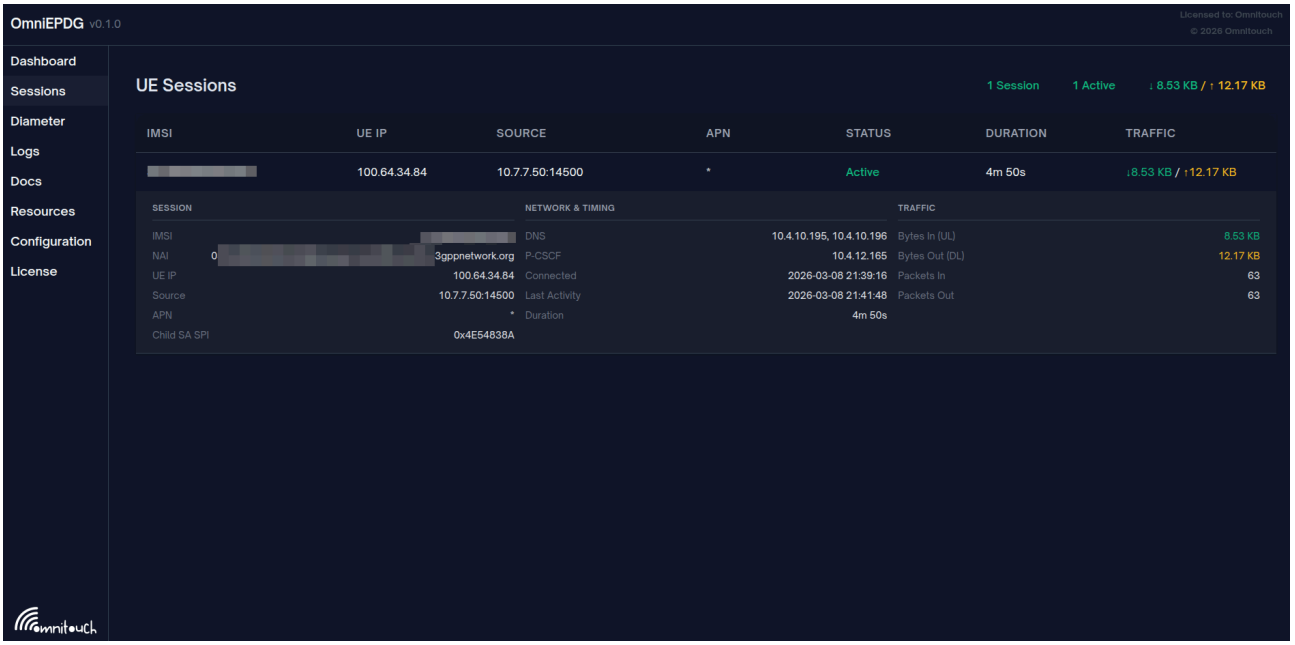
Guide d'Opérations OmniEPDG

OmniEPDG est une Passerelle de Données Évoluée (ePDG) qui permet les appels Voix sur WiFi (VoWiFi). Elle authentifie les abonnés mobiles sur des réseaux WiFi non fiables en utilisant EAP-AKA, et les connecte au réseau mobile central via un signalement Diameter vers le HSS et des tunnels GTP vers une Passerelle de Données (PGW).



Le panneau de contrôle OmniEPDG montrant une session d'abonné active avec des statistiques de trafic en temps réel.

OmniEPDG prend en charge deux modes opérationnels :

- **Mode GTP** (par défaut) - Tunnelisation complète conforme à la 3GPP via un PGW via GTPv2-C et GTP-U
- **Mode VPN Simple** - Sortie locale avec un pool IP intégré et une interface TUN Linux, sans PGW requis

OmniEPDG peut également fonctionner comme un **N3IWF** 5G sur le même écouteur IKEv2. Voir Mode N3IWF.

Documentation

Configuration & Opérations

- **Architecture & Flux d'Appels** - Architecture système, interfaces de protocole, machines d'état UE et diagrammes de séquence de messages pour les deux modes
- **Référence de Configuration** - Documentation complète des paramètres pour Diameter, GTPv2-C, GTP-U, VPN Simple et journalisation
- **Panneau de Contrôle** - Interface de surveillance basée sur le Web pour les sessions, les pairs Diameter et les journaux
- **Mode N3IWF** - Accès non 3GPP non fiable 5G : EAP-5G sur NWu, NGAP vers l'AMF et GTP-U vers l'UPF

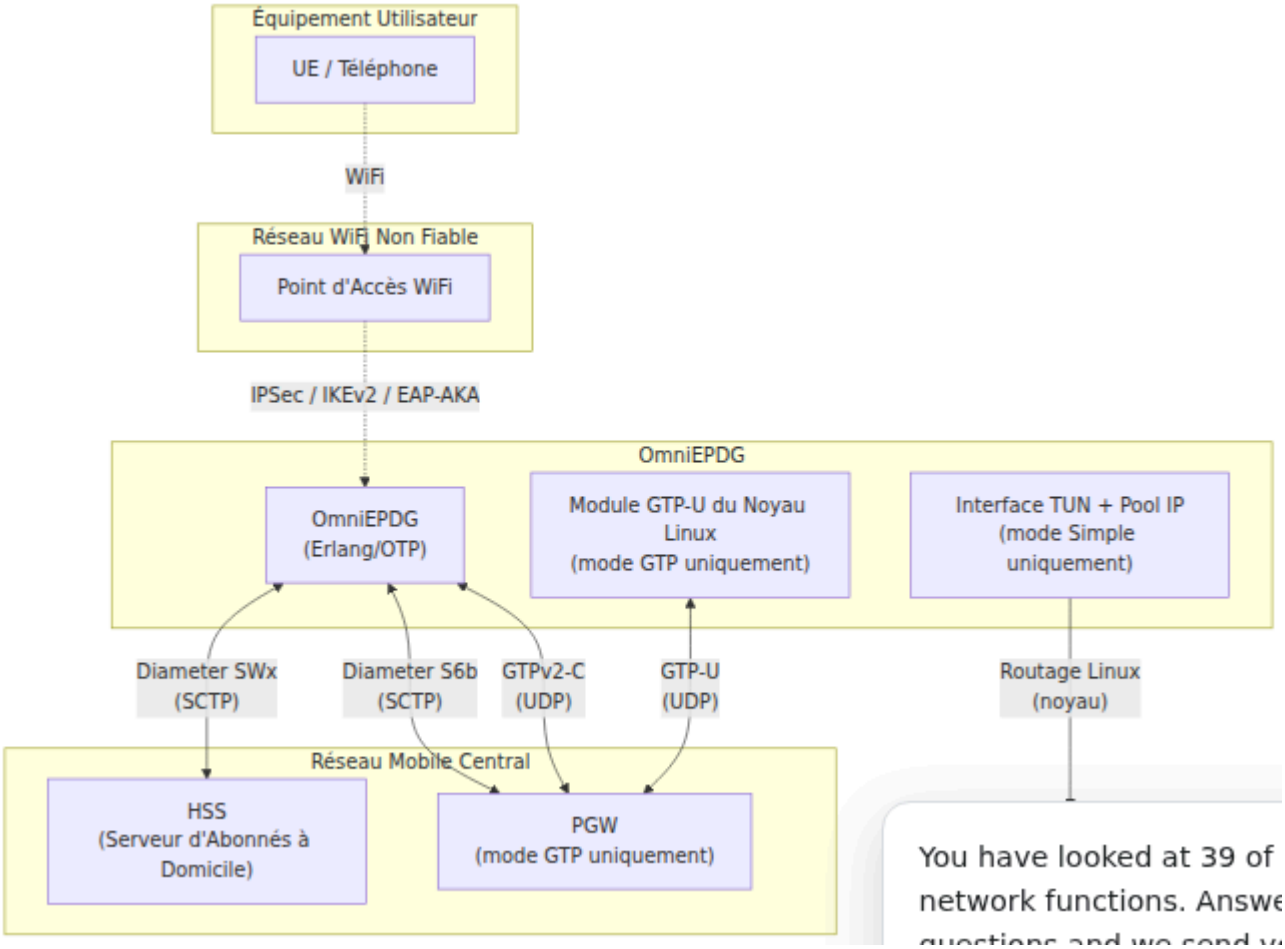
Sécurité

- **Guide de Sécurité** - Limitation du taux d'authentification et blocage des pays GeoIP

Surveillance & Dépannage

- **Référence des Métriques** - Métriques Prometheus pour surveiller l'authentification, les sessions, le signalement Diameter et la santé du système
- **Dépannage** - Problèmes courants, procédures de diagnostic et étapes de résolution

Modes Opérationnels



Mode GTP

Le mode par défaut. OmniEPDG tunnelise tout le trafic des abonnés via un PGW en utilisant GTPv2-C pour le contrôle de session et GTP-U (via le module du noyau Linux) pour le plan utilisateur. Cela est entièrement conforme à la 3GPP et convient aux déploiements d'opérateurs avec une infrastructure EPC existante.

Chemin du trafic : UE → IPSec → OmniEPDG → GTPv2-C Créer Session → tunnel GTP-U → PGW → Internet

Infrastructure requise : HSS, PGW

Mode VPN Simple

OmniEPDG alloue des adresses IP à partir d'un pool local et achemine le trafic des abonnés directement via une interface TUN Linux (`tun_epdg`) en utilisant le routage standard du noyau. Aucun PGW ou infrastructure GTP n'est nécessaire. L'authentification se fait toujours via Diameter SWx vers le HSS.

Chemin du trafic : UE → IPSec → OmniEPDG → Allocation IP locale → Interface TUN → Routage Linux → Internet

Infrastructure requise : HSS uniquement (PGW non requis)

Optimisation optionnelle : Le drapeau `skip_sar` contourne la demande/réponse d'attribution de serveur HSS, réduisant le temps de configuration de la connexion. Cela signifie que le HSS ne suivra pas quel ePDG sert l'abonné et que les procédures initiées par le HSS (désinscription, push de profil) ne fonctionneront pas. Convient aux déploiements privés sans exigences de roaming.

Comparaison des Modes

Capacité	Mode GTP	Mode VPN Simple
Conforme à la 3GPP	Oui	Non (avec `skip_sar`), Partiel (sans)
PGW requis	Oui	Non
HSS requis	Oui	Oui (authentification uniquement)
Allocation IP	Depuis PGW	Pool local (CIDR)
Plan utilisateur	Module GTP-U du noyau	TUN Linux + routage
Push de profil HSS	Oui (PPR/PPA)	Non
Désinscription HSS	Oui (RTR/RTA)	Non (avec `skip_sar`)
Teardown initié par PGW	Oui	N/A
Support de roaming	Oui	Non
IPv6 / Double pile	Oui	IPv4 uniquement

Interfaces de Protocole

Interface	Protocole	Transport	Mode	Pair	Objectif
SWu	IKEv2 / IPSec	UDP	Les deux	UE	Tunnel sécuris et authentificatio EAP-AKA
SWx	Diameter	SCTP	Les deux	HSS	Vecteurs d'authentificat et attribution d serveur
S6b	Diameter	SCTP	GTP uniquement	PGW	Autorisation de session et politique
S2b	GTPv2-C / GTP-U	UDP	GTP uniquement	PGW	Contrôle et tunnel du plan utilisateur

Fonctionnalités

Fonctionnalité de Base

- **Authentification EAP-AKA** - Authentification complète des abonnés EAP-AKA conforme à la 3GPP via le HSS
- **Gestion de Tunnel IPSec** - Tunnel sécurisé basé sur IKEv2 entre l'UE et l'ePDG
- **Modes Opérationnels Doubles** - Tunnelisation GTP vers PGW ou sortie locale avec VPN Simple
- **Machines d'État par UE** - FSM Erlang indépendante par abonné pour la gestion du cycle de vie de la session

- **Support de Double Pile** - Types d'adresses PDP IPv4, IPv6 et IPv4v6 (mode GTP)

Fonctionnalités du Mode GTP

- **Établissement de Tunnel GTP** - Création de session GTPv2-C et plan utilisateur GTP-U via le module du noyau Linux
- **Teardown Initié par PGW** - PGW envoie une Demande de Suppression de Porteuse, l'ePDG cascade le teardown vers l'UE
- **Teardown Initié par le Réseau** - HSS déclenche la désinscription via SWx RTR, l'ePDG détruit toutes les sessions
- **Ré-Authentification** - Push de profil déclenché par HSS et ré-autorisation par 3GPP TS 29.273 Section 7.1.2.5.1

Fonctionnalités du Mode VPN Simple

- **Pool IP Local** - Allocation d'adresses IPv4 basée sur CIDR avec suivi par IMSI
- **Routage par Interface TUN** - Dispositif TUN Linux standard (`tun_epdg`) avec routes hôtes par UE
- **Configuration DNS** - Serveurs DNS configurables fournis aux UE via PCO
- **Saut de SAR Optionnel** - Contourner l'enregistrement HSS pour un démarrage de connexion plus rapide

Fonctionnalités de Sécurité

- **Limitation du Taux d'Authentification** - Protection contre les attaques par force brute par IP et par IMSI avec seuils configurables
- **Blocage de Pays GeoIP** - Contrôle d'accès basé sur le pays en liste blanche ou noire utilisant MaxMind GeoLite2
- **Détection de Pair Mort** - Surveillance active de la vivacité avec sondes configurables
- **Protection Anti-Replay ESP** - Fenêtre glissante de 64 bits conforme à la RFC 4303

Intégration HSS (SWx Diameter)

- **Demande/Réponse d'Authentification Multimédia (MAR/MAA)** - Récupérer les vecteurs d'authentification EAP-AKA (les deux modes)
- **Demande/Réponse d'Attribution de Serveur (SAR/SAA)** - Télécharger le profil d'abonné et la configuration APN (sautable en mode Simple)
- **Demande/Réponse de Push de Profil (PPR/PPA)** - Recevoir des profils d'abonné mis à jour du HSS (mode GTP)
- **Demande/Réponse de Terminaison d'Inscription (RTR/RTA)** - Désinscription d'abonné initiée par HSS (mode GTP)

Intégration PGW (Mode GTP Uniquement)

S6b Diameter :

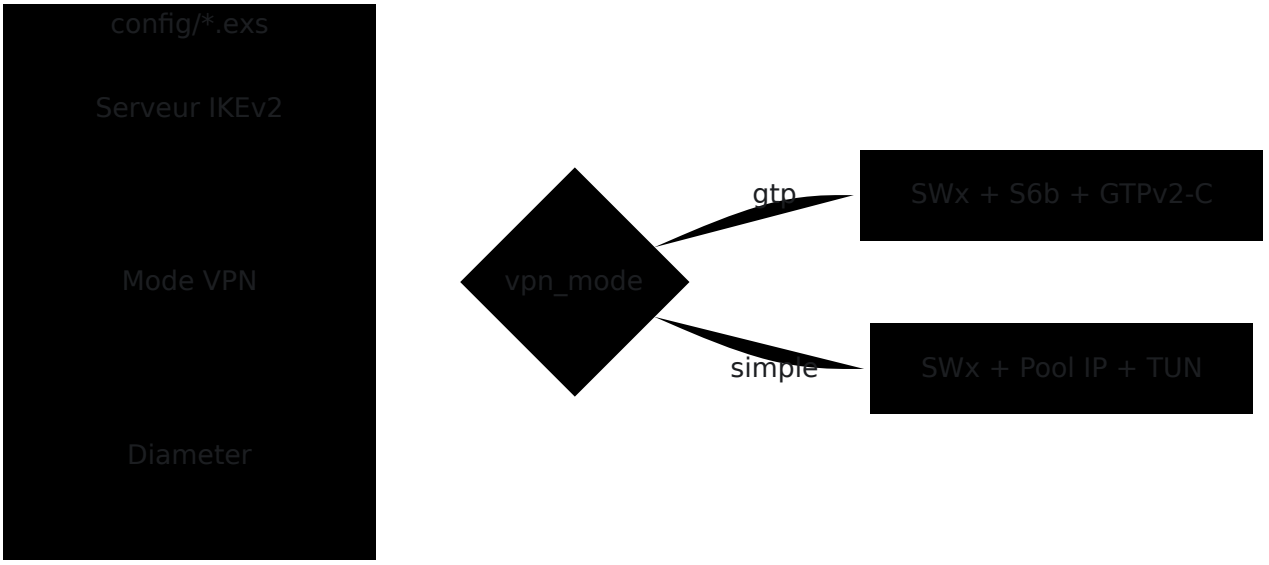
- **Demande/Réponse AA (AAR/AAA)** - Autoriser les sessions PGW
- **Demande/Réponse de Terminaison de Session (STR/STA)** - Terminer les sessions PGW
- **Demande/Réponse de Ré-Authentification (RAR/RAA)** - Ré-autoriser les sessions actives
- **Demande/Réponse d'Abandon de Session (ASR/ASA)** - Terminer les sessions de manière forcée

S2b GTPv2-C :

- **Demande/Réponse de Création de Session** - Établir des tunnels GTP avec allocation de TEID
- **Demande/Réponse de Suppression de Session** - Détruire des tunnels GTP
- **Demande/Réponse de Suppression de Porteuse** - Gestion de porteuse initiée par PGW

Démarrage Rapide

Structure de Configuration



La configuration se fait dans `config/runtime.exs` ou via des variables d'environnement. Le paramètre `vpn_mode` sélectionne entre les modes GTP et VPN Simple. Voir la Référence de Configuration pour la documentation complète des paramètres.

Adressage Réseau Typique (Mode GTP)

Composant	Adresse IP	Port	Remarques
OmniEPDG (GTP-U)	10.74.0.11	-	Point de terminaison du tunnel GTP-U
OmniEPDG (Diameter S6b)	10.74.0.12	3868	Écouteur Diameter S6b
HSS	10.74.0.21	3868	Pair Diameter SWx
PGW	10.74.0.23	2123	Pair GTPv2-C et S6b

Adressage Réseau Typique (Mode VPN Simple)

Composant	Adresse IP	Remarques
OmniEPDG (passerelle TUN)	10.44.0.1	IP de la passerelle sur l'interface `tun_epdg`
Pool IP UE	10.45.0.0/16	Pool CIDR configurable pour les IP des abonnés
HSS	10.74.0.21:3868	Pair Diameter SWx (authentification uniquement)

Spécifications 3GPP

Spécification	Titre	Pertinence
TS 29.273	Interfaces EPS AAA (SWx, S6b, SWm)	Spécification principale pour les interfaces Diameter ePDG
TS 29.274	GTPv2-C et GTP-U	Contrôle de tunnel S2b et plan utilisateur (mode GTP)
TS 33.402	Sécurité pour les accès non 3GPP	Authentification EAP-AKA pour WiFi non fiable
TS 23.402	Améliorations d'architecture pour les accès non 3GPP	Architecture ePDG globale et procédures
TS 23.003	Numérotation, adressage et identification	Format NAI, structure IMSI
TS 29.229	Cx/Dx Diameter (définitions communes)	Valeurs de Type d'Attribution de Serveur utilisées par SWx
RFC 6733	Protocole de Base Diameter	Transport Diameter, gestion des pairs, surveillance
RFC 4187	EAP-AKA	Méthode d'authentification utilisée sur IKEv2

Documentation par Rôle

Opérateurs de Réseau :

1. Commencez par Architecture & Flux d'Appels pour comprendre le système et les deux modes opérationnels

2. Consultez la Référence de Configuration pour les paramètres de déploiement
3. Consultez le Guide de Sécurité pour configurer la limitation de taux et le blocage GeoIP
4. Configurez la surveillance en utilisant la Référence des Métriques pour l'intégration Prometheus
5. Gardez le guide de Dépannage à disposition pour les opérations

Intégrateurs de Systèmes :

1. Consultez Architecture & Flux d'Appels pour les détails des interfaces et des machines d'état
2. Utilisez la Référence de Configuration pour la configuration de la connectivité des pairs
3. Configurez les alertes en utilisant la Référence des Métriques
4. Référez-vous au tableau des spécifications 3GPP ci-dessus pour la conformité des protocoles

Guide des opérations OmniEPDG

OmniEPDG est un ePDG (evolved Packet Data Gateway) conforme à la 3GPP qui permet les appels WiFi en reliant l'accès WiFi non fiable au réseau mobile central. Il prend en charge deux modes opérationnels : **mode GTP** pour le tunneling PGW et **mode VPN simple** pour le breakout IP local.

Liens rapides

Configuration & Déploiement

- **Exigences réseau** - Ports de pare-feu et entrées DNS nécessaires pour le déploiement
- **Référence de configuration** - Documentation complète des paramètres pour IKEv2, Diameter, modes VPN et tous les paramètres d'exécution
- **Aperçu de l'architecture** - Architecture système, flux d'appels, machines d'état et références de protocole

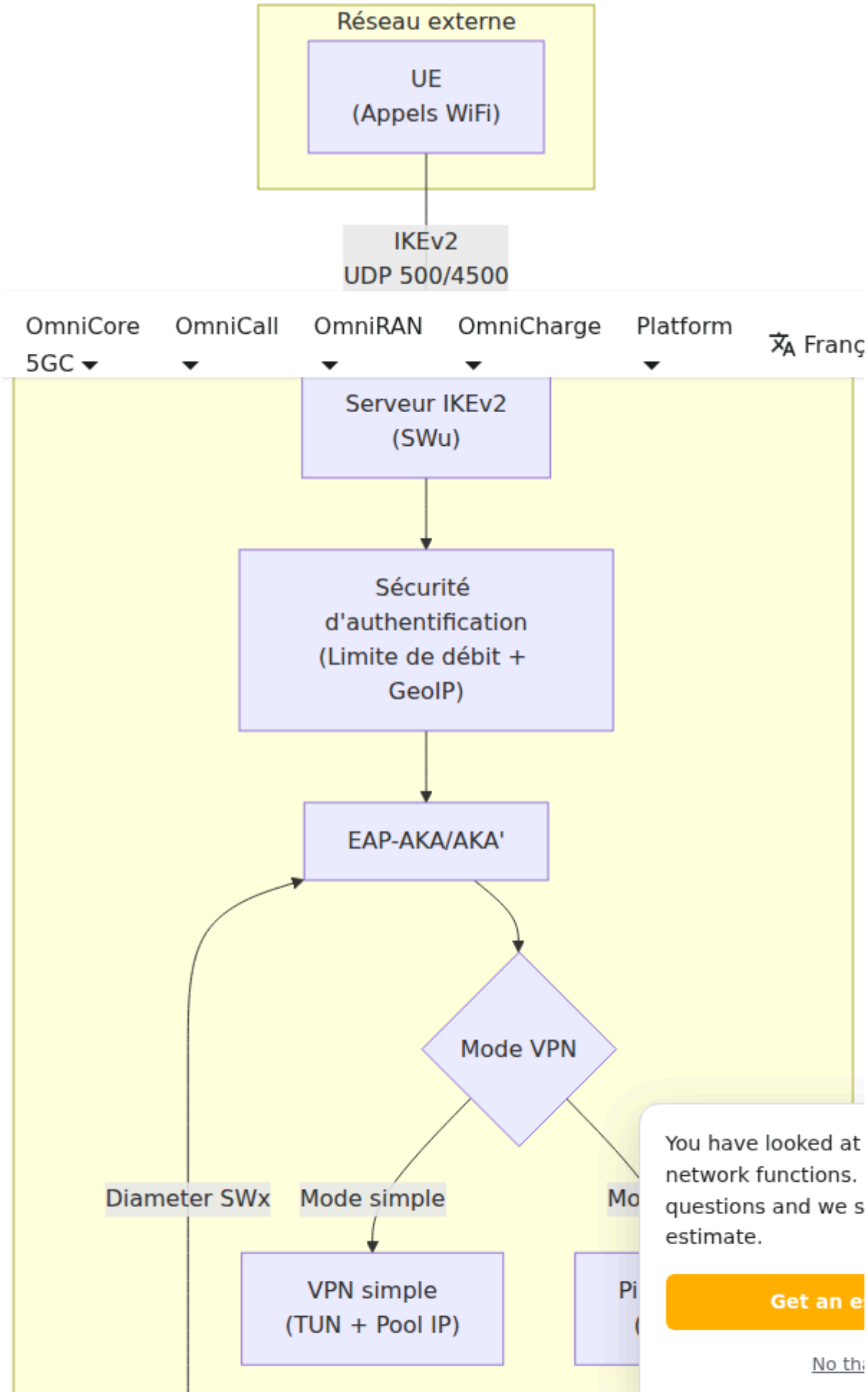
Opérations & Surveillance

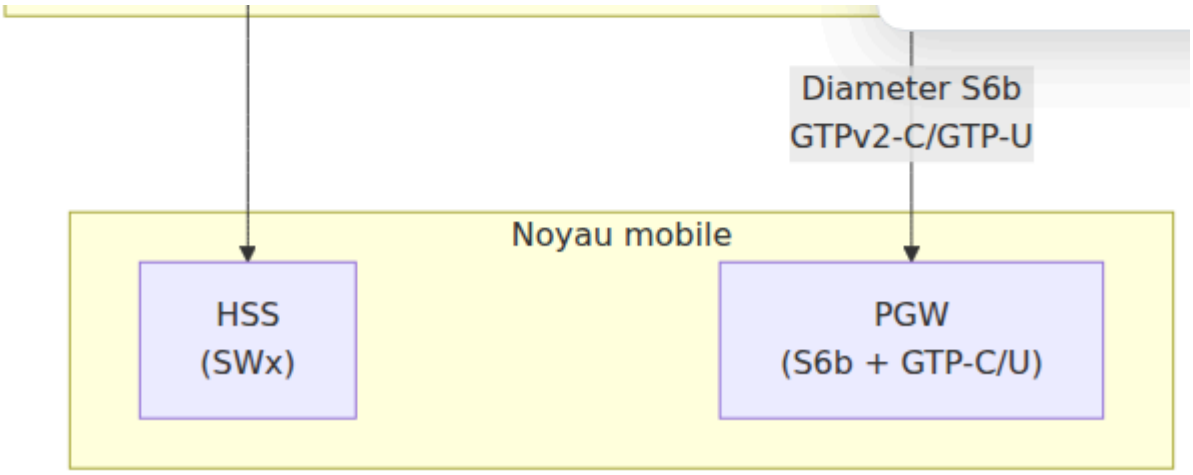
- **Panneau de contrôle** - Interface de surveillance basée sur le web pour les sessions, les pairs Diameter et les journaux
- **Référence des métriques** - Métriques Prometheus, exemples de requêtes et règles d'alerte
- **Webhooks** - Notifications de cycle de vie des sessions sortantes lors de l'attachement et du détachement
- **Dépannage** - Problèmes courants, procédures de diagnostic et étapes de résolution

Sécurité

- **Sécurité de l'authentification** - Limitation de débit et blocage par pays GeoIP

Aperçu de l'architecture


Réseau externe
UE
(Appels WiFi)
IKEv2
UDP 500/4500
OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platform
Franç
Serveur IKEv2
(SWu)
Sécurité
d'authentification
(Limite de débit +
GeoIP)
EAP-AKA/AKA'
Mode VPN
Diameter SWx
Mode simple
VPN simple
(TUN + Pool IP)
You have looked at
network functions.
questions and we s
estimate.
Get an e
No th



Modes opérationnels

OmniEPDG prend en charge deux modes opérationnels sélectionnés via le paramètre de configuration `vpn_mode`.

Mode GTP

Tunneling complet 3GPP via un PGW. Le trafic des abonnés est encapsulé dans GTP-U et acheminé à travers le noyau mobile.

Utiliser lorsque :

- Intégration avec l'infrastructure mobile centrale existante
- Politique et facturation via PCRF/PCEF
- Roaming et transfert inter-opérateur requis

Composants :

- Diameter S6b pour l'autorisation de session PGW
- GTPv2-C pour la gestion des sessions (Créer/Supprimer/Modifier la session)
- Module GTP-U du noyau Linux pour le plan utilisateur

Mode VPN simple

Breakout IP local via l'interface TUN. Le trafic des abonnés est acheminé directement à travers l'hôte OmniEPDG sans l'implication du PGW.

Utiliser lorsque :

- Déploiement autonome sans PGW
- Tests et développement
- Scénarios de breakout local

Composants :

- Gestion du pool IP local (IPv4/IPv6)
- Interface TUN (`omniepdg0`) avec des routes hôtes par abonné
- NAT/masquerade optionnel pour l'accès Internet

Sécurité de l'authentification

OmniEPDG inclut des fonctionnalités de sécurité intégrées pour se protéger contre les attaques par force brute et restreindre l'accès par localisation géographique. Consultez le guide Sécurité de l'authentification pour plus de détails.

Limitation de débit

Protège contre les attaques par force brute en suivant les tentatives d'authentification échouées :

- **Limitation par IP** - Bloque les IP après 10 échecs en 1 minute (blocage de 5 minutes)
- **Limitation par IMSI** - Bloque les IMSI après 5 échecs en 1 minute (blocage de 10 minutes)
- Algorithme de fenêtre glissante avec expiration automatique
- L'authentification réussie efface l'historique des échecs

Blocage par pays GeoIP

Contrôle d'accès géographique optionnel utilisant la base de données MaxMind GeoLite2 :

- **Mode liste blanche** - Autoriser uniquement les connexions provenant de pays spécifiés

- **Mode liste noire** - Bloquer les connexions provenant de pays spécifiés
- Gestion configurable des IP inconnues/privées
- Comportement fail-open ou fail-closed lorsque la base de données est indisponible

Configuration clé

Configuration minimale (Mode VPN simple)

```
config :omniepdg,
  vpn_mode: :simple,
  simple_vpn: [
    pool_ipv4: "10.45.0.0/16",
    dns_servers_ipv4: ["8.8.8.8", "8.8.4.4"]
  ]

config :diameter_ex,
  diameter: %{
    host: "epdg",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    peers: [
      %{host: "hss", ip: "10.74.0.21", port: 3868, transport:
:tcp}
    ]
  }
```

Activer la sécurité de l'authentification

```
config :omniepdg,
  # Limitation de débit (activée par défaut avec ces valeurs)
  auth_rate_limit_per_ip: 10,
  auth_rate_limit_ip_block_ms: 300_000,
  auth_rate_limit_per_imsi: 5,
  auth_rate_limit_imsi_block_ms: 600_000,

  # Blocage GeoIP (désactivé par défaut)
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ"]
```

Consultez la Référence de configuration pour la documentation complète des paramètres.

Surveillance

Panneau de contrôle

Accédez au panneau de contrôle web à `http://<host>:4000/dashboard` pour :

- Surveillance des sessions en temps réel
- État des pairs Diameter
- Diffusion en direct des journaux
- Configuration du système

Consultez le guide Panneau de contrôle pour plus de détails.

Métriques Prometheus

Récupérez les métriques depuis `http://<host>:9568/metrics` pour :

- Taux de succès/échec d'authentification
- Événements de cycle de vie des sessions
- Latence de signalisation Diameter

- Événements de sécurité (limitation de débit, blocs GeoIP)
- Utilisation du pool IP
- Statistiques du plan de données ESP

Consultez la Référence des métriques pour des requêtes et des règles d'alerte.

Dépannage

Problèmes courants et étapes de résolution :

Problème	Vérification rapide	Section du guide
Échecs d'authentification	Vérifiez SWx MAR/MAA dans les journaux	Échecs d'authentification
Problèmes de connexion Diameter	Vérifiez l'état des pairs dans le panneau de contrôle	Connectivité Diameter
Échecs de tunnel GTP	Vérifiez les codes de cause GTPv2-C	Échecs de tunnel GTP
Problèmes de VPN simple	Vérifiez l'interface TUN et les routes	Échecs de VPN simple
Faux positifs de limitation de débit	Ajustez les seuils	Problèmes de limitation de débit
Problèmes de blocage GeoIP	Vérifiez la base de données et les codes de pays	Problèmes GeoIP

Consultez le guide Dépannage pour des procédures de diagnostic détaillées.

Index de documentation

Document	Description
Architecture	Conception du système, machines d'état, flux d'appels, références de protocole
Configuration	Référence de configuration complète avec exemples
Panneau de contrôle	Guide de l'interface web avec captures d'écran
Métriques	Métriques Prometheus, requêtes et alertes
Exigences réseau	Ports de pare-feu et entrées DNS pour le déploiement
Sécurité	Limitation de débit et blocage par pays GeoIP
Dépannage	Problèmes courants et procédures de diagnostic

Architecture et Flux d'Appels d'OmniEPDG

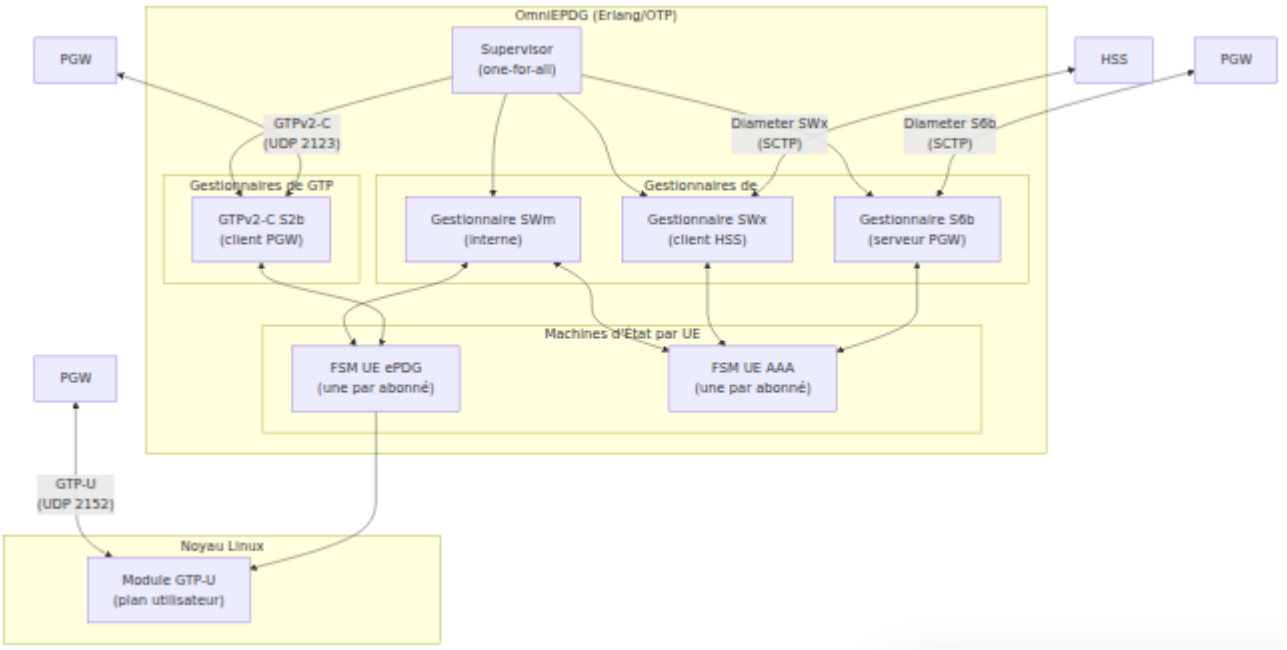
Ce document décrit l'architecture interne d'OmniEPDG, ses interfaces de protocole, les machines d'état UE et des diagrammes de séquence de messages détaillés pour les procédures clés. OmniEPDG prend en charge deux modes opérationnels : **mode GTP** (tunneling complet 3GPP via PGW) et **mode VPN Simple** (sortie locale avec interface TUN). Voir le Guide des Opérations pour une comparaison à un niveau élevé.

Architecture Système

OmniEPDG est construit sur Erlang/OTP et implémente la fonction réseau ePDG (evolved Packet Data Gateway) de la 3GPP. Il fait le pont entre l'accès WiFi non fiable et le réseau mobile central, permettant aux UEs de passer et de recevoir des appels VoWiFi.

Architecture du Mode GTP

Dans le mode GTP, le trafic des abonnés est tunnelé à travers un PGW en utilisant GTPv2-C pour le contrôle de session et le module GTP-U du noyau Linux pour le plan utilisateur.



Architecture du Mode VPN Simple

Dans le mode VPN Simple, le trafic des abonnés est routé localement via une interface TUN Linux. Aucune infrastructure PGW ou GTP n'est requise. Les composants Diameter S6b, GTPv2-C et GTP-U sont remplacés par le sous-système VPN Simple.



Arbre de Superviseur

OmniEPDG utilise une stratégie de superviseur **one-for-all**, ce qui signifie que si un processus enfant plante, tous les enfants sont redémarrés. Le superviseur démarre conditionnellement différents processus enfants en fonction du mode opérationnel.

Processus démarrés dans les deux modes :

Processus	Rôle	Description
`aaa_diameter_swx`	Client Diameter SWx	Se connecte au HSS pour l'authentification et les opérations de profil d'abonné
`aaa_diameter_swm`	Diameter SWm (Interne)	Routage des messages EAP Diameter et de session entre le ePDG et les FSM AAA
`epdg_diameter_swm`	Gestionnaire SWm ePDG	Gère le côté ePDG de la signalisation Diameter interne SWm

Processus supplémentaires en mode GTP :

Processus	Rôle	Description
`aaa_diameter_s6b`	Serveur Diameter S6b	Accepte les connexions du PGW pour l'autorisation de session
`epdg_gtpc_s2b`	Client GTPv2-C	Envoie des demandes de création/suppression de session au PGW via S2b
`gtp_u_kmod`	Gestionnaire du Noyau GTP-U	Gère les contextes PDP GTP-U dans le module du noyau Linux

Processus supplémentaires en mode VPN Simple :

Processus	Rôle	Description
`simple_vpn_supervisor`	Superviseur du Sous-système VPN	Supervise les processus de gestion de pool IP et de route
`simple_vpn_pool`	Gestionnaire de Pool IP	Alloue et libère des adresses IPv4 du pool CIDR configuré en utilisant ETS
`simple_vpn_route`	Gestionnaire de Route	Crée l'interface TUN `omniepdg0` et gère les routes hôtes par abonné

Machines d'État par UE

Pour chaque abonné actif (identifié par l'IMSI), OmniEPDG crée deux instances de machine d'état :

- **FSM UE ePDG** (`epdg_ue_fsm`) - Gère le cycle de vie de session de l'abonné du point de vue du ePDG : authentification, création de tunnel GTP et coordination de la destruction
- **FSM UE AAA** (`aaa_ue_fsm`) - Gère la signalisation côté AAA : échanges Diameter SWx avec le HSS et échanges S6b avec le PGW

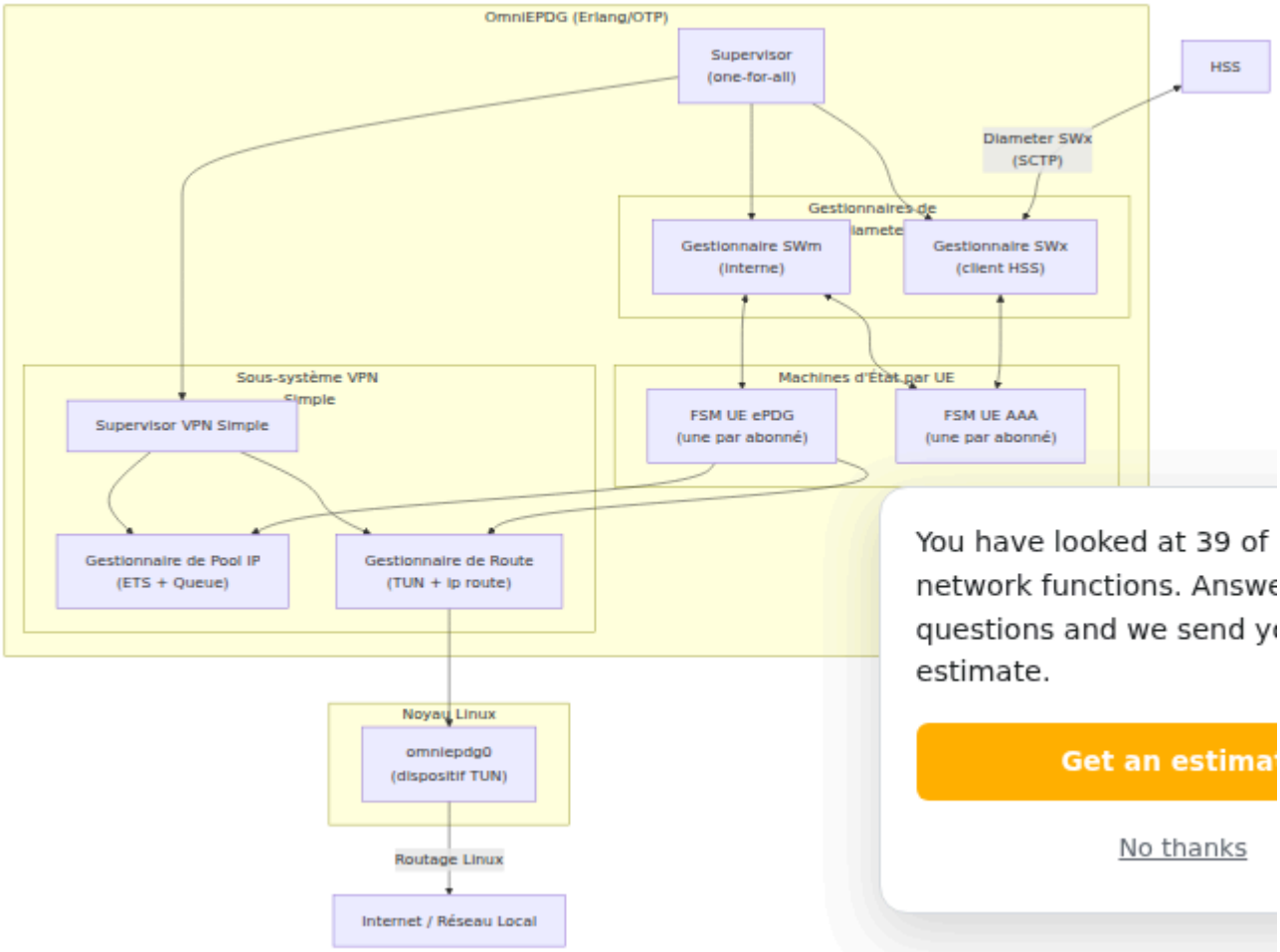
Les deux FSM sont implémentées en tant que processus Erlang `gen_statem` avec un mode de rappel de fonction d'état.

États de la FSM UE ePDG

La FSM UE ePDG suit la session d'un abonné depuis la demande d'authentification initiale jusqu'à l'état de tunnel actif jusqu'à la destruction. Le comportement de la FSM diverge à l'état `authenticated` en fonction du mode opérationnel.

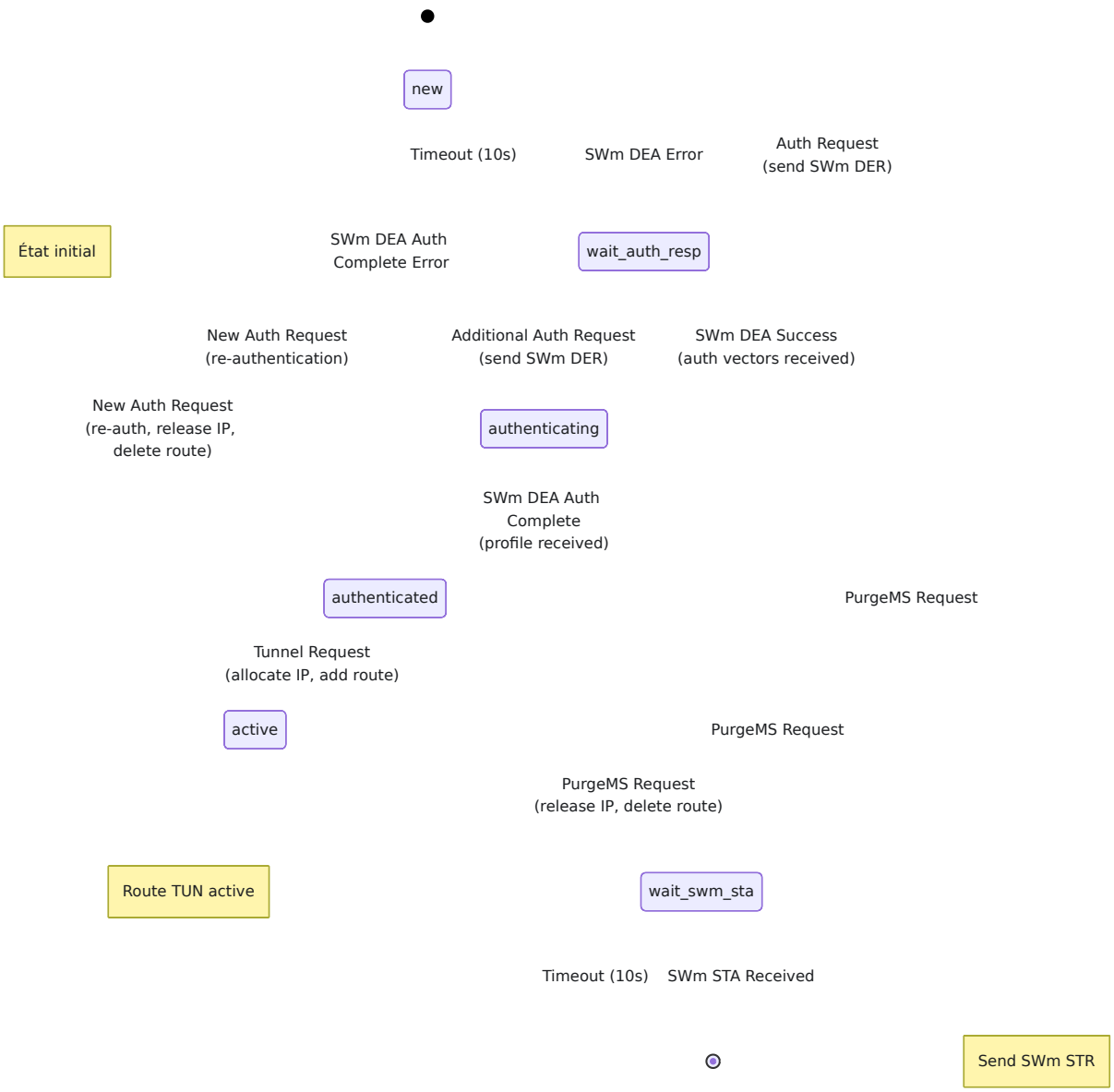
FSM en Mode GTP

Dans le mode GTP, l'établissement du tunnel passe par la création de session GTPv2-C vers le PGW, et la destruction implique la suppression de session GTPv2-C, la suppression de port initiée par le PGW et les flux de désinscription initiés par le HSS.



FSM en Mode VPN Simple

Dans le mode VPN Simple, la FSM prend un raccourci à l'état `authenticated`. Au lieu d'envoyer une demande de création de session GTPv2-C, la FSM alloue une adresse IP du pool local, crée une route hôte sur l'interface TUN et passe directement à `active`. Les états de destruction spécifiques à GTP (`wait_create_session_resp`, `wait_delete_session_resp`, `dereg_pgw_wait_cancel`, `dereg_net_wait_s2b_delete`) ne sont pas utilisés.


new
Timeout (10s)
SWm DEA Error
Auth Request
(send SWm DER)
État initial
SWm DEA Auth
Complete Error
wait_auth_resp
New Auth Request
(re-authentication)
Additional Auth Request
(send SWm DER)
SWm DEA Success
(auth vectors received)
New Auth Request
(re-auth, release IP,
delete route)
authenticating
SWm DEA Auth
Complete
(profile received)
authenticated
PurgeMS Request
Tunnel Request
(allocate IP, add route)
active
PurgeMS Request
PurgeMS Request
(release IP, delete route)
Route TUN active
wait_swm_sta
Timeout (10s)
SWm STA Received
Send SWm STR

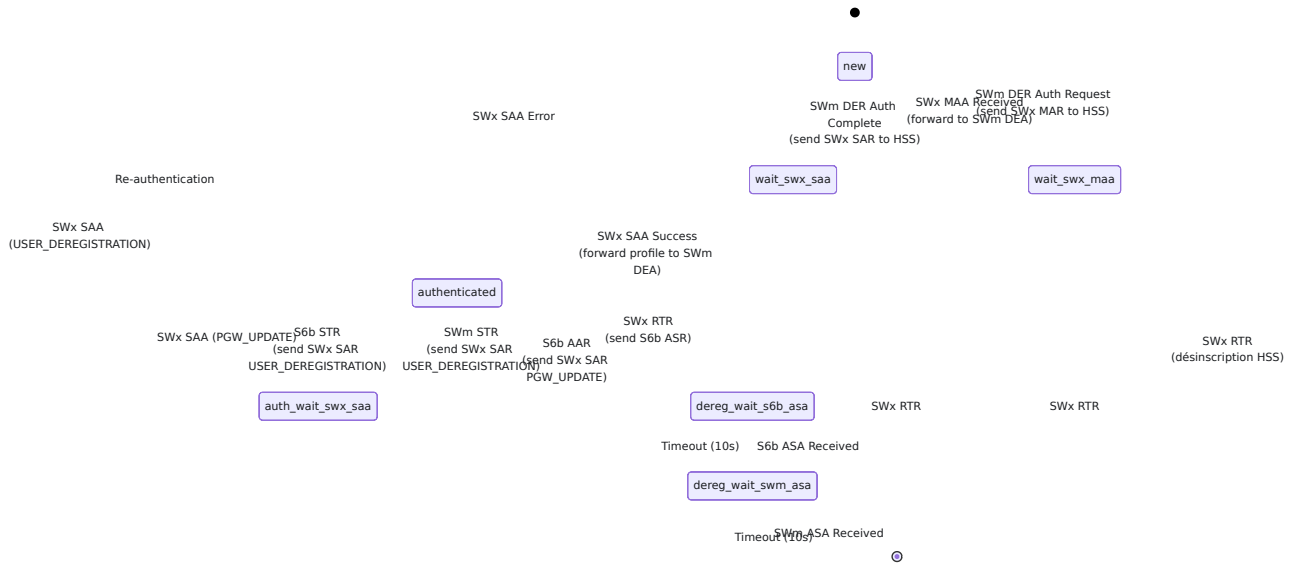
Référence des États de la FSM UE ePDG

État	Mode	Description	En Attente De
`new`	Les Deux	État initial. Pas de session active.	Demande d'authentificatio de l'UE
`wait_auth_resp`	Les Deux	Demande d'authentification envoyée via SWm DER.	SWm DEA avec vecteurs d'authentificatio ou erreur
`authenticating`	Les Deux	Vecteurs d'authentification reçus, échange EAP en cours.	Mise à jour de localisation / achèvement de l'authentificatior
`authenticated`	Les Deux	Authentification complète, profil d'abonné téléchargé.	Demande de tunnel de l'UE
`wait_create_session_resp`	GTP	Demande de création de session GTPv2-C envoyée au PGW.	Réponse de création de session du PGW
`active`	Les Deux	Tunnel/route opérationnel. Le trafic de l'abonné circule.	Déclencheur de destruction
`wait_delete_session_resp`	GTP	Demande de suppression de session GTPv2-C envoyée au PGW	Réponse de suppression de session du PGW

État	Mode	Description	En Attente De
		(destruction initiée par l'UE).	
`wait_swm_sta`	Les Deux	Demande de terminaison de session SWm envoyée.	SWm STA de AA
`dereg_pgw_wait_cancel`	GTP	Désinscription initiée par le PGW. Localisation d'annulation envoyée à l'UE.	Résultat de localisation d'annulation
`dereg_net_wait_cancel`	GTP	Désinscription initiée par le réseau/HSS. Localisation d'annulation envoyée à l'UE.	Résultat de localisation d'annulation
`dereg_net_wait_s2b_delete`	GTP	Désinscription initiée par le réseau. Suppression de session S2b envoyée au PGW.	Réponse de suppression de session

États de la FSM UE AAA

La FSM UE AAA gère la signalisation Diameter vers le HSS (SWx) et le PGW (S6b) au nom de chaque abonné.


new
SWm DER Auth
Complete
(send SWx SAR to HSS)
SWx MAA Received
(forward to SWm DEA)
SWm DER Auth Request
(send SWx MAR to HSS)
SWx SAA Error
Re-authentication
wait_swx_saa
wait_swx_maa
SWx SAA
(USER_DEREGISTRATION)
SWx SAA Success
(forward profile to SWm
DEA)
authenticated
SWx SAA (PGW_UPDATE)
S6b STR
(send SWx SAR
USER_DEREGISTRATION)
SWm STR
(send SWx SAR
USER_DEREGISTRATION)
S6b AAR
(send SWx SAR
PGW_UPDATE)
SWx RTR
(send S6b ASR)
SWx RTR
(désinscription HSS)
auth_wait_swx_saa
dereg_wait_s6b_asa
SWx RTR
SWx RTR
Timeout (10s)
S6b ASA Received
dereg_wait_swm_asa
Timeout (10s)
SWm ASA Received

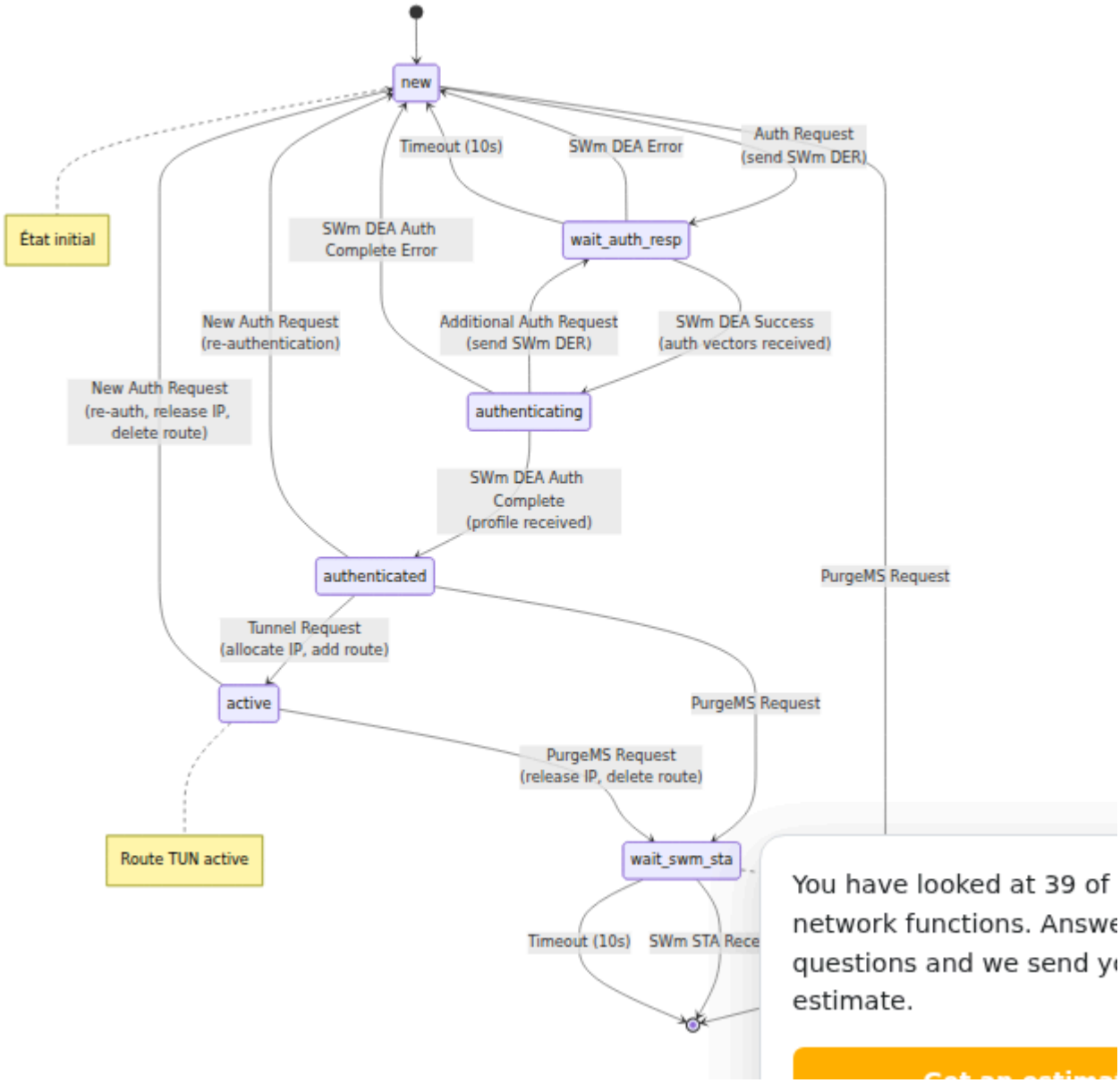
Référence des États de la FSM UE AAA

État	Description	En Attente De
`new`	État initial. Pas de session AAA active.	Demande d'authentification Diameter
`wait_swx_maa`	SWx MAR envoyé au HSS pour vecteurs EAP-AKA.	SWx MAA du HSS
`wait_swx_saa`	SWx SAR envoyé au HSS pour attribution de serveur.	SWx SAA du HSS
`authenticated`	Les sessions ePDG et PGW peuvent être actives. Suit l'état de session dual.	Événements de session
`auth_wait_swx_saa`	SWx SAR envoyé pour mise à jour PGW ou désinscription utilisateur.	SWx SAA du HSS
`dereg_net_wait_s6b_asa`	Désinscription initiée par le HSS. S6b ASR envoyé au PGW.	S6b ASA du PGW
`dereg_net_wait_swm_asa`	La destruction S6b est terminée. SWm ASR envoyé au ePDG.	SWm ASA du ePDG

Flux d'Appels

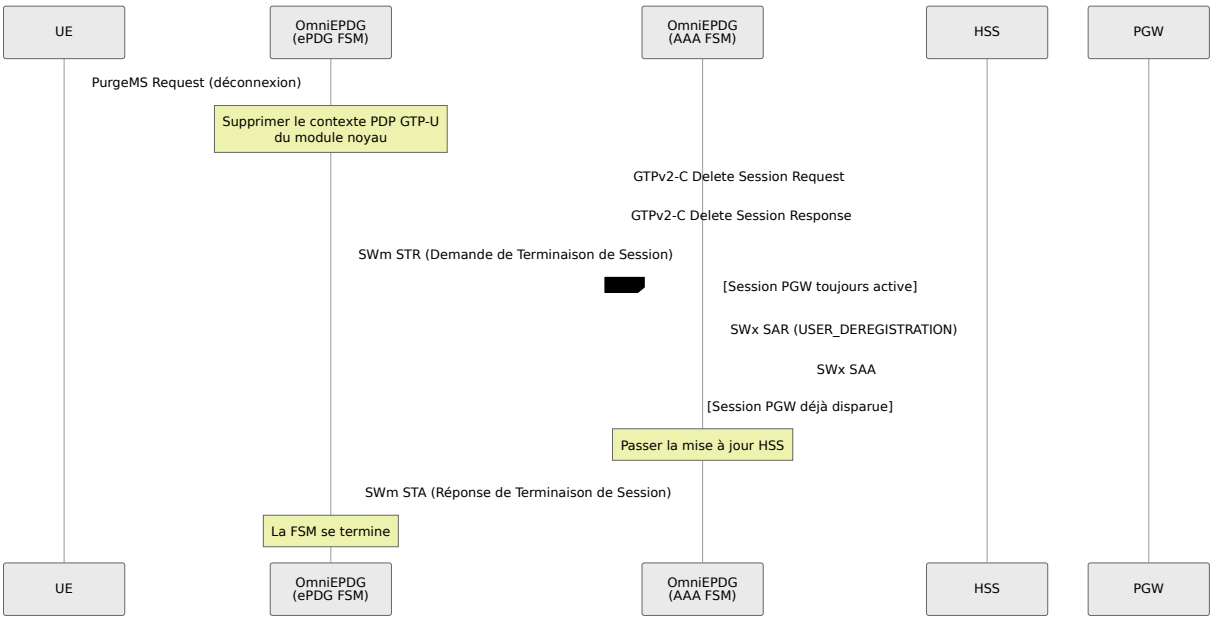
Mode GTP : Établissement de Session Réussi

Cette séquence montre une session complète réussie depuis l'authentification EAP-AKA jusqu'à un tunnel GTP actif.



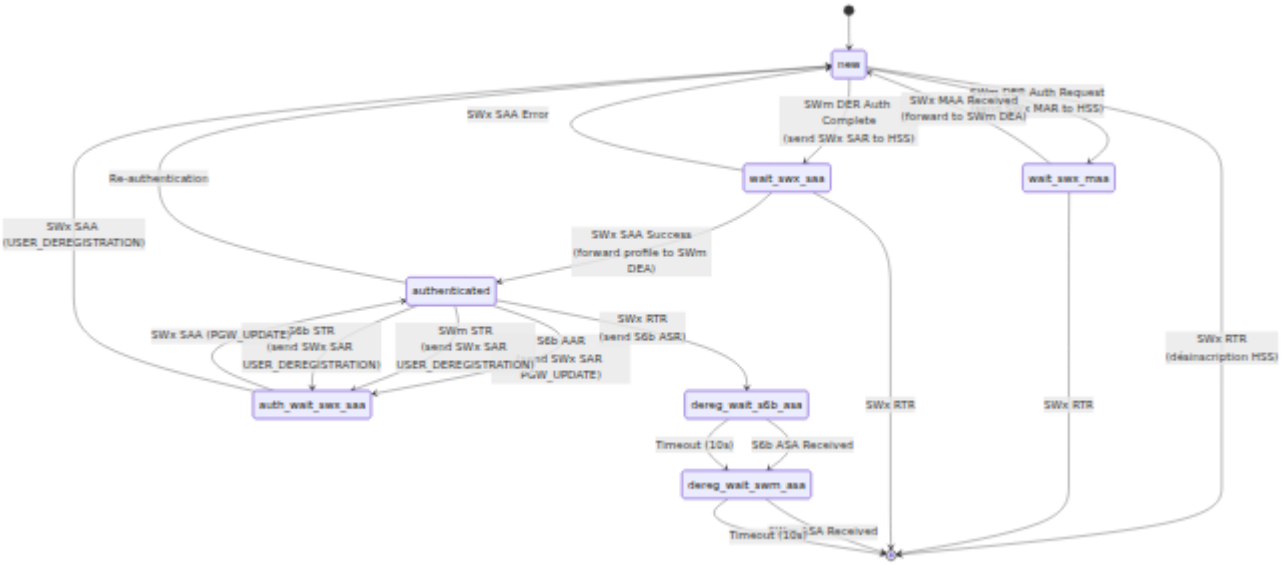
Mode GTP : Destruction de Session Initiée par l'UE

Lorsque l'UE se déconnecte (par exemple, passe de WiFi à cellulaire ou l'utilisateur raccroche).



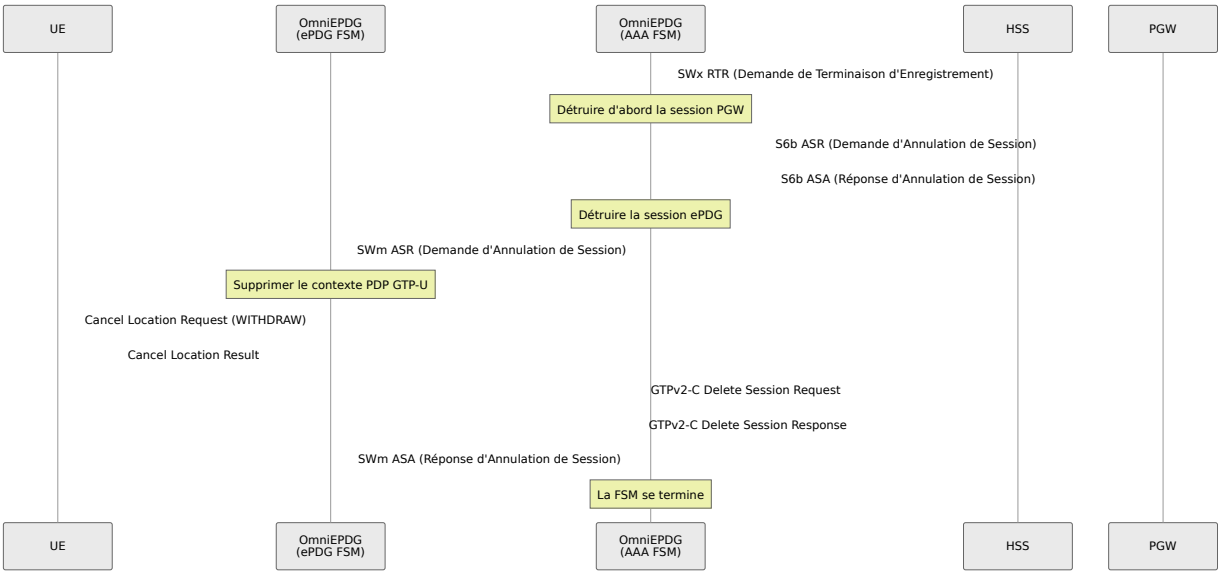
Mode GTP : Destruction de Session Initiée par le PGW

Lorsque le PGW termine la session (par exemple, violation de politique, délai d'attente ou action administrative).



Mode GTP : Désinscription Initiée par le Réseau (HSS)

Lorsque le HSS révoque l'enregistrement d'un abonné (par exemple, changement d'abonnement, détection de fraude ou action administrative).



Mode GTP : Poussée de Profil HSS et Ré-authentification

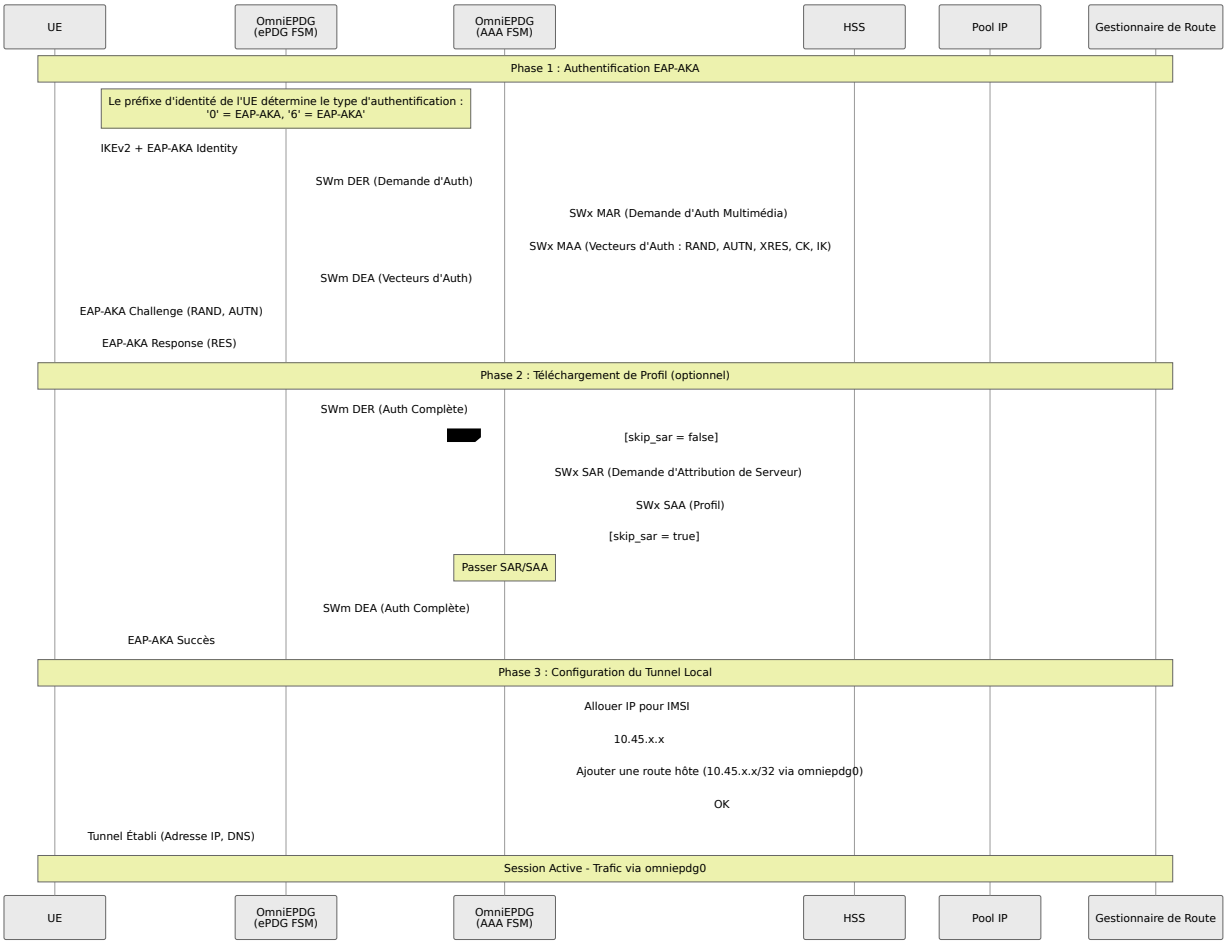
Lorsque le HSS pousse un profil d'abonné mis à jour, OmniEPDG déclenche une ré-authentification sur les sessions ePDG (SWm) et PGW (S6b) conformément à 3GPP TS 29.273 Section 8.1.2.3.3.

Parse error on line 15: ... Ré-auth session PGW AAA->>PGW: ---------- ^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW', 'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW', 'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS', 'SOLID_POINT', 'DOTTED_POINT', got 'NEWLINE'

Réessayer

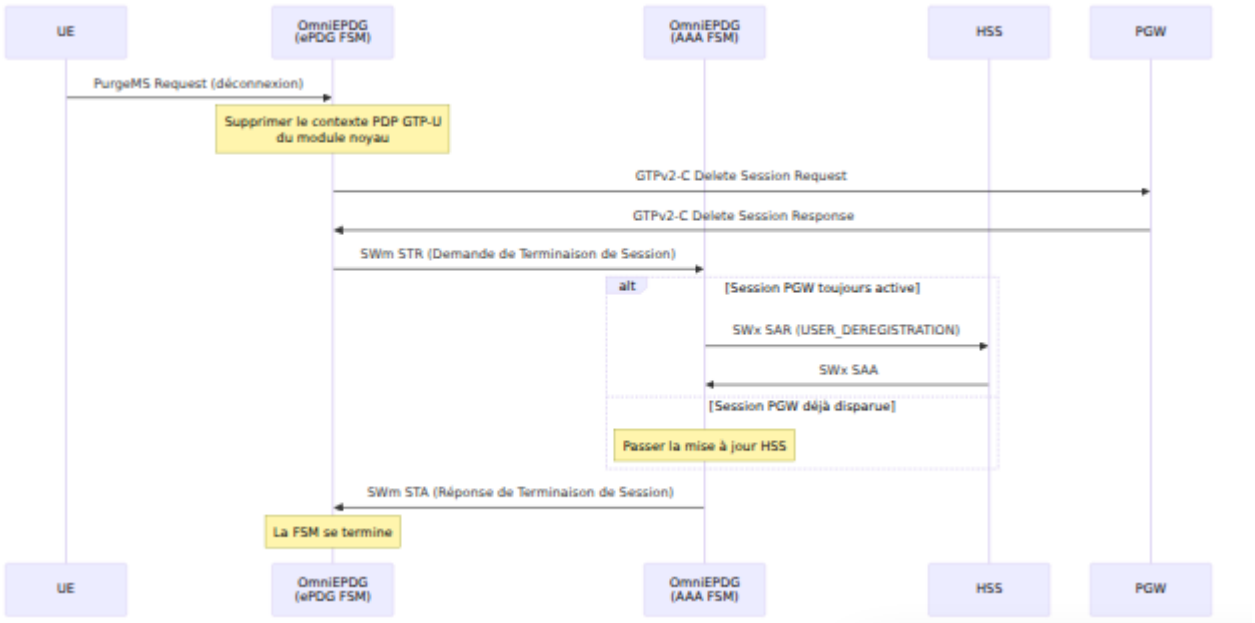
Mode VPN Simple : Établissement de Session Réussi

Dans le mode VPN Simple, l'établissement de session est plus court. Après l'authentification EAP-AKA, la FSM ePDG alloue une IP du pool local et configure une route hôte sur l'interface TUN, contournant toute interaction avec le PGW. Si `skip_sar` est activé, l'échange SAR/SAA avec le HSS est également ignoré.



Mode VPN Simple : Destruction de Session Initiée par l'UE

Lorsque l'UE se déconnecte en mode VPN Simple, la FSM libère l'adresse IP allouée et supprime la route hôte.



Identifiants d'Application Diameter

Identifiant d'Application	Interface	Identifiant de Fournisseur	Description	Référence
16777265	SWx	10415 (3GPP)	ePDG ↔ HSS authentification et gestion des abonnés	3GPP TS 29.273
16777272	S6b	10415 (3GPP)	AAA ↔ PGW autorisation de session	3GPP TS 29.273

Codes de Résultat Diameter

OmniEPDG mappe les codes de résultat Diameter aux valeurs de cause internes pour la propagation d'erreurs inter-protocoles.

Codes de Résultat Standards

Code de Résultat	Nom	Signification
2001	DIAMETER_SUCCESS	Opération complétée avec succès
2002	DIAMETER_LIMITED_SUCCESS	Opération partiellement réussie

Codes de Résultat Expérimentaux 3GPP

Code de Résultat	Nom	Significat
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	HSS ne peut temporairem pas fournir d données d'authentific
5001	DIAMETER_ERROR_USER_UNKNOWN	IMSI de l'abo non trouvé d le HSS
5002	DIAMETER_UNKNOWN_SESSION_ID	Session non trouvée (util pour STR/AA obsolètes)
5003	DIAMETER_AUTHORIZATION_REJECTED	Abonné non autorisé pou service
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	Restrictions roaming appliquées
5005	DIAMETER_MISSING_AVP	AVP requis manquant d message
5012	DIAMETER_UNABLE_TO_COMPLY	Échec de traitement générique

Code de Résultat	Nom	Significat
5420	DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION	Aucune souscription trouvée
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	Technologie d'accès non autorisée
5422	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	IMEI de l'app non reconnu

Codes de Cause GTPv2-C (Mode GTP Seulement)

OmniEPDG gère les codes de cause GTPv2-C suivants dans les réponses de création/suppression de session du PGW. Les codes 1-15 sont informatifs, 16-63 indiquent le succès, et 64+ indiquent des erreurs. Voir 3GPP TS 29.274 Section 8.4.

Causes de Succès

Code	Nom	Description
16	Request Accepted	Opération complétée avec succès
17	Request Accepted Partially	Succès partiel
18	New PDN Type (Network Preference)	Type de PDN changé en raison de la préférence du réseau
19	New PDN Type (Single Address Bearer)	Type de PDN changé en raison de la restriction de port d'adresse unique

Causes d'Erreur (Sélectionnées)

Code	Nom	Description
64	Context Not Found	Contexte de session non trouvé sur le PGW
73	No Resources Available	Épuisement des ressources PGW
78	Missing or Unknown APN	APN demandé non configuré sur le PGW
82	Denied in RAT	Technologie d'accès non autorisée
84	All Dynamic Addresses Occupied	Pool d'adresses IP épuisé sur le PGW
92	User Authentication Failed	Échec de l'authentification au PGW
93	APN Access Denied	Abonné non autorisé pour l'APN
96	IMSI/IMEI Not Known	Identité de l'abonné non reconnue
109	Invalid Peer	Échec de validation du pair
113	APN Congestion	APN surchargé
120	GTP-C Entity Congestion	Plan de contrôle PGW surchargé

Format NAI

OmniEPDG identifie les abonnés en utilisant le format d'Identifiant d'Accès au Réseau (NAI) défini dans 3GPP TS 23.003 Section 19 :

```
<prefix><IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

Préfixe d'Identité et Type d'Authentification

Le préfixe NAI détermine la méthode d'authentification EAP selon la 3GPP TS 23.003 :

Préfixe	Type d'Authentification	Description
`0`	EAP-AKA	Authentification AKA standard (la plus courante pour les appels WiFi)
`6`	EAP-AKA'	Authentification AKA améliorée avec liaison au réseau

OmniEPDG sélectionne automatiquement la méthode d'authentification en fonction du préfixe d'identité de l'UE. La plupart des UEs utilisent le préfixe `0` (EAP-AKA) pour les appels WiFi.

OmniEPDG extrait l'IMSI du NAI en analysant tout ce qui se trouve entre le préfixe et le symbole `@`. L'IMSI est ensuite utilisé comme clé principale pour toutes les machines d'état et opérations de signalisation par abonné.

Algorithmes Cryptographiques

OmniEPDG implémente des algorithmes cryptographiques conformément à 3GPP TS 33.402 et RFC 7296 (IKEv2).

Algorithmes de Chiffrement IKEv2

Algorithme	ID	Taille de Clé	Statut	Référence
AES-CBC	12	128, 192, 256 bits	Supporté (par défaut : 256)	RFC 3602
AES-GCM-16	20	128, 192, 256 bits	Supporté	RFC 5282
AES-GCM-12	19	128, 192, 256 bits	Supporté	RFC 5282
AES-GCM-8	18	128, 192, 256 bits	Supporté	RFC 5282
3DES	3	192 bits	Supporté (héritage)	RFC 2451

Algorithmes d'Intégrité IKEv2

Algorithme	ID	Taille de Clé	Taille ICV	Statut	Référence
HMAC-SHA2-256-128	12	256 bits	128 bits	Supporté (par défaut)	RFC 4868
HMAC-SHA2-384-192	13	384 bits	192 bits	Supporté	RFC 4868
HMAC-SHA2-512-256	14	512 bits	256 bits	Supporté	RFC 4868
AES-XCBC-96	5	128 bits	96 bits	Supporté	RFC 3566
HMAC-SHA1-96	2	160 bits	96 bits	Supporté (héritage)	RFC 2404
HMAC-MD5-96	1	128 bits	96 bits	Supporté (héritage)	RFC 2403

AES-XCBC-96 (`AUTH_AES_XCBC_96`) est requis par certains appareils, notamment certains clients Samsung VoWiFi, qui l'offrent comme leur seul transformateur d'intégrité. Il est implémenté conformément à la RFC 3566 avec le traitement de clé variable et la troncature du nonce SKEYSEED définie dans RFC 4434 et RFC 7296 Section 2.14.

Algorithmes PRF IKEv2

Algorithme	ID	Taille de Sortie	Statut	Référence
PRF-HMAC-SHA2-256	5	256 bits	Supporté (par défaut)	RFC 4868
PRF-HMAC-SHA2-384	6	384 bits	Supporté	RFC 4868
PRF-HMAC-SHA2-512	7	512 bits	Supporté	RFC 4868
PRF-AES128-XCBC	4	128 bits	Supporté	RFC 4434
PRF-HMAC-SHA1	2	160 bits	Supporté (héritage)	RFC 2104
PRF-HMAC-MD5	1	128 bits	Supporté (héritage)	RFC 2104

Lorsque `PRF-AES128-XCBC` est négocié, SKEYSEED est dérivé uniquement des 64 premiers bits de chacun de Ni et Nr (conformément à la section 2.14 de la RFC 7296), tandis que les nonces complets alimentent l'expansion de clé prf+.

Groupes Diffie-Hellman IKEv2

Groupe	ID	Taille	Statut	Référence
MODP-2048	14	2048 bits	Supporté (par défaut)	RFC 3526
MODP-1024	2	1024 bits	Supporté (héritage)	RFC 2409
MODP-1536	5	1536 bits	Supporté	RFC 3526
MODP-3072	15	3072 bits	Supporté	RFC 3526
MODP-4096	16	4096 bits	Supporté	RFC 3526
ECP-256	19	256 bits	Supporté	RFC 5903
ECP-384	20	384 bits	Supporté	RFC 5903
ECP-521	21	521 bits	Supporté	RFC 5903
Curve25519	31	256 bits	Supporté	RFC 8031
Curve448	32	448 bits	Supporté	RFC 8031

Algorithmes ESP (Child SA)

Les algorithmes de tunnel ESP sont négociés à partir de la proposition SA que l'UE offre dans IKE_AUTH (et dans CREATE_CHILD_SA lors du renouvellement). OmniEPDG sélectionne un transformateur que l'UE a effectivement proposé et dérive les clés Child SA avec les tailles de clé et ICV correspondantes. Il ne force pas un ensemble fixe.

Type	Algorithmes	Remarques
Chiffrement	AES-CBC-128 / 192 / 256	Le chiffre suit la longueur de clé négociée
Intégrité	HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256, AES-XCBC-96, HMAC-SHA1-96	L'ICV AES-XCBC-96 est de 12 octets (contre 16 pour HMAC-SHA2-256-128)

Fallback (uniquement lorsque la proposition de l'UE ne peut pas être analysée) :

- Chiffrement : AES-CBC-256 (clé de 32 octets, IV de 16 octets)
- Intégrité : HMAC-SHA2-256-128 (clé de 32 octets, ICV de 16 octets)

Fonctions Cryptographiques EAP-AKA

Fonction	Algorithme	Référence
Dérivation MK	SHA-1	RFC 4187 Section 7
Expansion de clé PRF+	PRF FIPS 186-2 (SHA-1)	RFC 4187 Annexe D
AT_MAC	HMAC-SHA1-128	RFC 4187 Section 10.15
Milenage (f1-f5)	AES-128	3GPP TS 35.206

Fonctions Cryptographiques EAP-AKA'

Fonction	Algorithme	Référence
Dérivation CK'/IK'	HMAC-SHA-256	RFC 5448 Section 3.3
Dérivation MK	SHA-256	RFC 5448 Section 3.4
AT_MAC	HMAC-SHA256-128	RFC 5448 Section 3.1

Conformité 3GPP

OmniEPDG implémente tous les algorithmes cryptographiques obligatoires spécifiés dans 3GPP TS 33.402 Section 8 :

Exigence	Algorithme	Statut
Chiffrement IKEv2 (obligatoire)	AES-CBC-128	✓ Supporté
Intégrité IKEv2 (obligatoire)	HMAC-SHA2-256-128	✓ Supporté (par défaut)
PRF IKEv2 (obligatoire)	PRF-HMAC-SHA-256	✓ Supporté (par défaut)
DH IKEv2 (obligatoire)	Groupe 14 (MODP-2048)	✓ Supporté (par défaut)
Chiffrement ESP (obligatoire)	AES-CBC-128/256	✓ Supporté
Intégrité ESP (obligatoire)	HMAC-SHA2-256-128	✓ Supporté (par défaut)
EAP-AKA	RFC 4187	✓ Implémenté
EAP-AKA'	RFC 5448	✓ Implémenté

Au-delà de l'ensemble obligatoire, OmniEPDG prend également en charge les transformations d'intégrité et PRF AES-XCBC (RFC 3566 / RFC 4434) pour l'interopérabilité avec les appareils qui les offrent exclusivement : par exemple certains clients Samsung VoWiFi, qui proposent AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048 et ne reviendront pas à HMAC-SHA2.

Types d'Adresse PDP (Mode GTP Seulement)

OmniEPDG prend en charge les types d'adresse PDP suivants tels que définis dans 3GPP TS 29.274 Section 8.14. En mode VPN Simple, seules les adresses

IPv4 sont allouées à partir du pool local.

Type	Description	Format PAA GTPv2-C
IPv4	Port uniquement IPv4	Adresse IPv4 de 4 octets
IPv6	Port uniquement IPv6	Longueur de préfixe de 1 octet + adresse IPv6 de 16 octets
IPv4v6	Port double pile	Longueur de préfixe de 1 octet + adresse IPv6 de 16 octets + adresse IPv4 de 4 octets

Référence de Configuration OmniEPDG

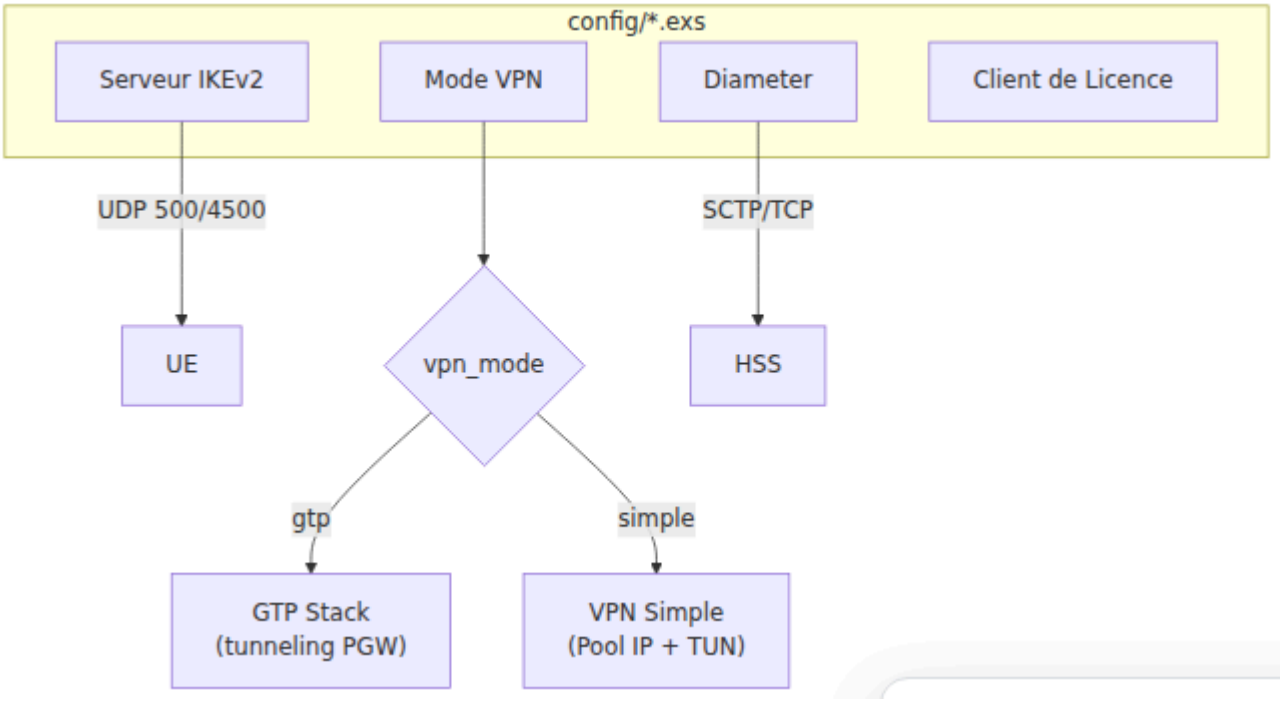
OmniEPDG est configuré via `config/runtime.exs` et des variables d'environnement. Toute la configuration accessible aux clients est effectuée à l'exécution - les valeurs par défaut à la compilation sont intégrées dans la version et ne sont pas exposées.

Pour les déploiements conteneurisés, utilisez les variables d'environnement comme documenté dans la section Référence des Variables d'Environnement.

Table des Matières

- Paramètres du Serveur IKEv2
- Paramètres de Sécurité d'Authentification
- Sélection du Mode VPN
- Paramètres VPN Simples
- Paramètres Diameter
- Configuration du Client de Licence
- Configuration du Panneau de Contrôle
- Configuration des Métriques Prometheus
- Configuration des Webhooks
- Référence des Variables d'Environnement
- Référence des Délais d'Attente

Structure de Configuration



Fichier de Configuration

Toute la configuration est effectuée dans `config/runtime.exs`. OmniEPDG lit ce fichier lors de son démarrage. Le fichier prend en charge la substitution de variables d'environnement pour les déploiements conteneurisés.

Exemple de Configuration

```
# config/runtime.exs
config :omniepdg,
  # Paramètres du serveur IKEv2
  listen_ip: {0, 0, 0, 0},
  port_500: 500,
  port_4500: 4500,

  # Mode VPN : :simple (sortie locale) ou :gtp (PGW via GTP-C)
  vpn_mode: :simple,

  # Paramètres du mode VPN simple
  simple_vpn: [
    pool_ipv4: "10.45.0.0/16",
    pool_ipv6: "2001:db8::/32",
    dns_servers_ipv4: ["8.8.8.8", "8.8.4.4"],
    dns_servers_ipv6: ["2001:4860:4860::8888",
"2001:4860:4860::8844"]
  ]

# Configuration du panneau de contrôle
config :control_panel,
  parent_application: :omniepdg,
  parent_application_readable_name: "OmniEPDG",
  use_additional_pages: [
    {OmniEpdg.Web.DashboardLive, "/", "Tableau de Bord"},
    {OmniEpdg.Web.SessionsLive, "/sessions", "Sessions"},
    {OmniEpdg.Web.DiameterLive, "/diameter", "Diameter"}
  ]

# Configuration Diameter (runtime.exs)
config :diameter_ex,
  diameter: %{
    service_name: :omniepdg,
    listen_ip: "0.0.0.0",
    listen_port: 3868,
    host: "epdg",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    product_name: "OmniEPDG",
    vendor_id: 10415,
    applications: [
      %{application_name: :swx, application_id: 16_777_265,
```

```
vendor_id: 10415},
      %{application_name: :s6b, application_id: 16_777_272,
vendor_id: 10415}
    ],
    peers: [
      %{host: "hss", ip: "127.0.0.1", port: 3868, transport: :tcp}
    ]
  }

# Configuration du client de licence (runtime.exs)
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

Paramètres du Serveur IKEv2

Le serveur IKEv2 gère l'interface SWu entre les UE et OmniEPDG. Il termine les tunnels IPSec et effectue l'authentification EAP-AKA.

Paramètre	Type	Requis	Par Défau
`listen_ip`	Tuple	Non	`{0, 0, 0, 0}`
`port_500`	Integer	Non	`500`
`port_4500`	Integer	Non	`4500`
`cert_file`	String	Oui	`/etc/omniepdg/cert`
`key_file`	String	Oui	`/etc/omniepdg/cert`

Paramètre	Type	Requis	Par Défau
`session_inactivity_timeout_ms`	Integer	Non	`300000`

Paramètres de Sécurité d'Authentification

OmniEPDG inclut une protection intégrée contre les attaques par force brute et un contrôle d'accès géographique. Consultez le Guide de Sécurité pour une documentation détaillée.

Paramètres de Limitation de Taux

```
config :omniepdg,
  # Limitation de taux par IP
  auth_rate_limit_per_ip: 10,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 300_000,

  # Limitation de taux par IMSI
  auth_rate_limit_per_imsi: 5,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 600_000
```

Paramètre	Type	Requis	Par Défaut	Descr
`auth_rate_limit_per_ip`	Integer	Non	`10`	Nombre maximur tentative d'authen échouées avant blo
`auth_rate_limit_ip_window_ms`	Integer	Non	`60000`	Fenêtre g pour com échecs IP (millisecc
`auth_rate_limit_ip_block_ms`	Integer	Non	`300000`	Durée de blocage p IP dépass seuil (5 n
`auth_rate_limit_per_imsi`	Integer	Non	`5`	Nombre maximur tentative d'authen échouées IMSI avar blocage.
`auth_rate_limit_imsi_window_ms`	Integer	Non	`60000`	Fenêtre g pour com échecs IM (millisecc
`auth_rate_limit_imsi_block_ms`	Integer	Non	`600000`	Durée de blocage p IMSI dépa

Paramètre	Type	Requis	Par Défaut	Descr
				seuil (10 minutes)

Paramètres GeoIP

```
config :omniepdg,
  geoip_enabled: false,
  geoip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ"],
  geoip_allow_unknown: false,
  geoip_fail_open: true
```

Paramètre	Type	Requis	Par Défaut	
`geoip_enabled`	Boolean	Non	`false`	
`geoip_database_path`	String	Non	`"/etc/omniepdg/GeoLite2-Country.mmdb"`	
`geoip_mode`	Atom	Non	`:whitelist`	
`geoip_countries`	List	Non	`[]`	

Paramètre	Type	Requis	Par Défaut	
`geoip_allow_unknown`	Boolean	Non	dépend du mode	
`geoip_fail_open`	Boolean	Non	`true`	

Sélection du Mode VPN

Paramètre	Type	Requis	Par Défaut	Var Env	Description
`vpn_mode`	Atom	Non	`:simple`	`EPDG_VPN_MODE`	Mode opérationnel : `:simple` pour une sortie IP locale via l'interface TUN, `:gtp` pour un tunneling à travers un PGW via GTPv2-C/GTP-U. Consultez le Guide des Opérations pour une comparaison détaillée.

Paramètres VPN Simples

Le bloc de configuration `simple_vpn` contrôle l'allocation IP et DNS pour le mode VPN Simple. OmniEPDG prend en charge à la fois les pools d'adresses IPv4 et IPv6.

```
config :omniepdg,
  simple_vpn: [
    pool_ipv4: "10.45.0.0/16",
    pool_ipv6: "2001:db8::/32",
    dns_servers_ipv4: ["8.8.8.8", "8.8.4.4"],
    dns_servers_ipv6: ["2001:4860:4860::8888",
"2001:4860:4860::8844"],
    p_cscf_ipv4: ["10.4.12.165"],
    p_cscf_ipv6: [],
    mtu: 1400,
    nat_enabled: true
  ]
```

Paramètre	Type	Requis	Par Défaut	De
`pool_ipv4`	String	Oui	`"10.45.0.0/16"`	Pool IPv4 CIDI allou abo
`pool_ipv6`	String	Non	`"2001:db8::/32"`	Pool IPv6 CIDI abo dou
`dns_servers_ipv4`	List	Non	`["8.8.8.8", "8.8.4.4"]`	Serv IPv4 UE v (Opt Con de F
`dns_servers_ipv6`	List	Non	`["2001:4860:4860::8888", "2001:4860:4860::8844"]`	Serv IPv6 UE v
`p_cscf_ipv4`	List	Non	`[]`	Adre CSC (Pro VoW aux acti l'en IMS.
`p_cscf_ipv6`	List	Non	`[]`	Adre CSC

Paramètre	Type	Requis	Par Défaut	D
				(Pro VoW
`mtu`	Integer	Non	`1400`	Vale pou de t vale bas réd frag
`nat_enabled`	Boolean	Non	`true`	Acti pou des Lors vrai de r sont pou sort

Paramètres Diameter

La configuration Diameter contrôle les interfaces SWx (HSS) et S6b (PGW). Lorsque `diameter_enabled` est `true`, OmniEPDG démarre la pile Diameter et se connecte aux pairs configurés.

```
config :diameter_ex,
  diameter: %{
    service_name: :omniepdg,
    listen_ip: "0.0.0.0",
    listen_port: 3868,
    host: "epdg",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    product_name: "OmniEPDG",
    vendor_id: 10415,
    applications: [
      %{application_name: :swx, application_id: 16_777_265,
vendor_id: 10415},
      %{application_name: :s6b, application_id: 16_777_272,
vendor_id: 10415}
    ],
    peers: [
      %{host: "hss", ip: "10.74.0.21", port: 3868, transport:
:tcp}
    ]
  }
```

Paramètres de Service

Paramètre	Type	Requis	Par Défaut
`service_name`	Atom	Non	`:omniepdg`
`listen_ip`	String	Non	`"0.0.0.0"`
`listen_port`	Integer	Non	`3868`
`host`	String	Oui	`"epdg"`

Paramètre	Type	Requis	Par Défaut
`realm`	String	Oui	`"epc.mnc001.mcc001.3gppnetwork.org"`
`product_name`	String	Non	`"OmniEPDG"`
`vendor_id`	Integer	Non	`10415`

Paramètres de Pair

Chaque entrée dans la liste `peers` définit une connexion de pair Diameter (généralement vers l'HSS).

Paramètre	Type	Requis	Par Défaut	Var Env	Description
`host`	String	Oui	-	`HSS_HOST`	Identité Diameter du pair (Origin-Host). Doit correspondre à l'identité configurée du pair.
`ip`	String	Oui	-	`HSS_IP`	Adresse IP du pair pour la connexion TCP/SCTP.
`port`	Integer	Non	`3868`	`HSS_PORT`	Port Diameter du pair.
`transport`	Atom	Non	`:tcp`	-	Protocole de transport : `:tcp` ou `:sctp`.

Identifiants d'Application

Application	ID	Vendor ID	Interface	Référence
SWx	16777265	10415	ePDG ↔ HSS	3GPP TS 29.273
S6b	16777272	10415	AAA ↔ PGW	3GPP TS 29.273

Configuration du Client de Licence

Le client de licence valide OmniEPDG auprès d'un serveur de licence.

```
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

Paramètre	Type	Requis	Par Défaut	Var Env	Des
`server_url`	String	Oui	-	`LICENSE_SERVER_URL`	URL de term API serv licer
`product`	String	Non	`"omniepdg"`	-	Iden du p pour valid de la licer

Configuration du Panneau de Contrôle

Le panneau de contrôle web fournit des capacités de surveillance et de gestion.

```
config :control_panel,
  port: 4000
```

Paramètre	Type	Requis	Par Défaut	Var Env	Descrip
`port`	Integer	Non	`4000`	`CONTROL_PANEL_PORT`	Port HT pour l'interfa web du pannea contrôle

Configuration des Métriques Prometheus

OmniEPDG expose des métriques Prometheus via HTTP pour la surveillance et l'alerte.

```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

Paramètre	Type	Requis	Par Défaut	Var Env	Descriptio
`port`	Integer	Non	`9568`	`PROMETHEUS_PORT`	Port HTTP pour le poi de terminaiso des métriques Prometheu (`/metrics`)

Métriques Exposées

Métriques de Compteur (Basées sur les événements) :

- `epdg_ikev2_session_initiated_count` - Échanges IKE_SA_INIT démarrés
- `epdg_ikev2_session_established_count` - IKE SAs établis avec succès
- `epdg_ikev2_session_failed_count` - Échecs d'établissement de l'IKE SA (par raison)
- `epdg_eap_identity_count` - Requêtes d'identité EAP
- `epdg_eap_aka_challenge_count` - Défis EAP-AKA envoyés
- `epdg_eap_aka_success_count` - Authentifications EAP-AKA réussies
- `epdg_eap_aka_failure_count` - Échecs d'authentification EAP-AKA (par raison)
- `epdg_eap_aka_sync_failure_count` - Échecs de synchronisation EAP-AKA SQN
- `epdg_diameter_swx_mar_count` - Requêtes d'authentification multimédia (par résultat)
- `epdg_diameter_swx_sar_count` - Requêtes d'attribution serveur (par résultat)
- `epdg_diameter_s6b_aar_count` - Requêtes AA traitées (par résultat)
- `epdg_diameter_s6b_str_count` - Requêtes de terminaison de session
- `epdg_session_created_count` - Sessions créées (par vpn_mode)
- `epdg_session_terminated_count` - Sessions terminées (par raison)
- `epdg_esp_packets_in_count` - Paquets ESP décryptés
- `epdg_esp_packets_out_count` - Paquets ESP chiffrés
- `epdg_ip_allocated_count` - Adresses IP allouées (par type)
- `epdg_ip_released_count` - Adresses IP libérées (par type)

Métriques de Jauge (Interrogées toutes les 5s) :

- `epdg_sessions_active_count` - Total des sessions actives
- `epdg_sessions_by_state_count` - Sessions par état FSM
- `epdg_ip_pool_allocated_count` - IPs actuellement allouées
- `epdg_ip_pool_available_count` - IPs disponibles dans le pool
- `epdg_ip_pool_utilization_ratio` - Taux d'utilisation du pool (0.0-1.0)
- `epdg_diameter_swx_pending_count` - Requêtes SWx en attente
- `epdg_diameter_s6b_active_sessions_count` - Sessions S6b actives

Métriques d'Histogramme (Suivi de la latence) :

- `epdg_auth_duration_ms` - Durée du flux d'authentification complet
- `epdg_diameter_swx_mar_latency_ms` - Temps de réponse MAR
- `epdg_diameter_swx_sar_latency_ms` - Temps de réponse SAR
- `epdg_session_duration_seconds` - Durée de la session

Métriques VM :

- `vm_memory_total` - Mémoire totale de la VM
- `vm_memory_processes` - Mémoire des processus
- `vm_memory_binary` - Mémoire binaire
- `vm_memory_ets` - Mémoire de la table ETS
- `vm_system_info_process_count` - Processus en cours d'exécution
- `vm_system_info_port_count` - Ports ouverts
- `vm_statistics_run_queue` - File d'attente d'exécution du planificateur

Configuration de Scrape Prometheus

```
scrape_configs:
  - job_name: 'omniepdg'
    static_configs:
      - targets: ['localhost:9568']
```

Configuration des Webhooks

OmniEPDG peut envoyer des webhooks sortants pour les événements du cycle de vie des sessions des abonnés. Lorsqu'il est activé, OmniEPDG envoie un `POST` HTTP avec un corps JSON à chaque point de terminaison configuré lors d'une attache réussie et lors d'une détache. Consultez Webhooks pour le modèle de livraison, le schéma de charge utile et des exemples de charges utiles.

```
config :omniepdg, :webhook,
  enabled: false,
  endpoints: ["https://127.0.0.1/webhook"],
  events: [:session_established, :session_terminated]
```

Paramètre	Type	Requis	Par Défaut	
`enabled`	Boolean	Non	`false`	Activ les w Lorsc Omn aucu
`endpoints`	List	Non	`["https://127.0.0.1/webhook"]`	La lis point Omn `POST` term évén
`events`	List	Non	`[:session_established, :session_terminated]`	La lis évén Les v sont `:ses` (atta `:ses` (déta

OmniEPDG livre les webhooks avec un modèle de type "fire-and-forget", et il ne réessaie pas une livraison échouée. Pour le modèle de livraison complet et le schéma de charge utile JSON, consultez Webhooks.

Référence des Délais d'Attente

Tous les délais d'attente internes de la FSM sont codés en dur. Ceux-ci régissent combien de temps les machines d'état attendent des réponses avant de les considérer comme échouées.

Délai d'Attente	Valeur	Mode	Contexte	Description
Réponse GTP	10,000 ms	GTP	FSM UE ePDG	Temps d'attente maximum pour la réponse Create/Delete Session GTPv2-C du PGW.
Réponse SWm	10,000 ms	Les deux	FSM UE ePDG	Temps d'attente maximum pour la réponse interne Diameter SWm (DER/DEA, STR/STA).
Réponse S6b	10,000 ms	GTP	FSM UE AAA	Temps d'attente maximum pour la réponse Diameter S6b (ASR/ASA).

Référence des Variables d'Environnement

Les variables d'environnement sont lues dans `config/runtime.exs` et remplacent les valeurs par défaut à la compilation.

Serveur IKEv2

Variable	Par Défaut	Description
`EPDG_LISTEN_IP`	`"0.0.0.0"`	Adresse de liaison du serveur IKEv2 (format décimal pointé, par exemple, `"10.0.0.1"`).
`EPDG_PORT_500`	`"500"`	Port du protocole IKE.
`EPDG_PORT_4500`	`"4500"`	Port de Traversée NAT IKE.
`EPDG_CERT_FILE`	`"/etc/omniepdg/certs/epdg.crt"`	Chemin vers le certificat du serveur IKEv2 (PEM).
`EPDG_KEY_FILE`	`"/etc/omniepdg/certs/epdg.key"`	Chemin vers la clé privée du serveur IKEv2 (PEM).
`EPDG_SESSION_TIMEOUT`	`"300000"`	Délai d'inactivité de session en millisecondes.

Mode VPN

Variable	Par Défaut	Description
`EPDG_VPN_MODE`	`"simple"`	Mode VPN : `"simple"` ou `"gtp"`.

Diameter

Variable	Par Défaut	Description
`DIA_LISTEN_IP`	`"0.0.0.0"`	Adresse de liaison du listener Diameter.
`DIA_LISTEN_PORT`	`"3868"`	Port du listener Diameter.
`DIA_HOST`	`"epdg"`	Origin-Host Diameter (sans royaume).
`DIA_REALM`	`"epc.mnc001.mcc001.3gppnetwork.org"`	Origin-Realm Diameter.

Pair HSS

Variable	Par Défaut	Description
`HSS_HOST`	`"hss"`	Identité Diameter HSS (Origin-Host).
`HSS_IP`	`"127.0.0.1"`	Adresse IP HSS.
`HSS_PORT`	`"3868"`	Port Diameter HSS.

Licence, Panneau de Contrôle et Métriques

Variable	Par Défaut	Description
`LICENSE_SERVER_URL`	-	URL de l'API du serveur de licence (requis).
`CONTROL_PANEL_PORT`	`"4000"`	Port HTTP du panneau de contrôle.
`PROMETHEUS_PORT`	`"9568"`	Port HTTP des métriques Prometheus (point de terminaison `/metrics`).

Exemple : Docker Compose

```yaml
services:
  omniepdg:
    image: omniepdg:latest
    environment:
      # IKEv2
      EPDG_LISTEN_IP: "0.0.0.0"
      EPDG_CERT_FILE: "/certs/epdg.crt"
      EPDG_KEY_FILE: "/certs/epdg.key"

      # Mode VPN
      EPDG_VPN_MODE: "simple"

      # Diameter
      DIA_HOST: "epdg"
      DIA_REALM: "epc.mnc001.mcc001.3gppnetwork.org"
      HSS_HOST: "hss"
      HSS_IP: "10.74.0.21"
      HSS_PORT: "3868"

      # Licence
      LICENSE_SERVER_URL: "https://license.example.com/api"

      # Panneau de contrôle
      CONTROL_PANEL_PORT: "4000"

      # Métriques Prometheus
      PROMETHEUS_PORT: "9568"
    ports:
      - "500:500/udp"
      - "4500:4500/udp"
      - "4000:4000"
      - "9568:9568"
    volumes:
      - ./certs:/certs:ro
    cap_add:
      - NET_ADMIN
```

Panneau de Contrôle OmniEPDG

OmniEPDG comprend un panneau de contrôle basé sur le web pour la surveillance en temps réel des sessions, des pairs Diameter et des journaux système. Le panneau de contrôle fournit des vues mises à jour en direct sans actualisation de page.

Table des Matières

- Accéder au Panneau de Contrôle
- Tableau de Bord
- Vue des Sessions
- Vue des Pairs Diameter
- Vue des Journaux
- Vue des Docs
- Vue des Ressources
- Vue de Configuration

Accéder au Panneau de Contrôle

Le panneau de contrôle est servi sur le port HTTP configuré (par défaut 4000) :

```
http://<host>:4000/dashboard
```

Navigation

Le panneau de contrôle fournit une barre latérale avec des liens vers toutes les vues :

Chemin	Vue	Description
`/dashboard`	Tableau de Bord	Vue d'ensemble du système et liens rapides
`/sessions`	Sessions	Liste des sessions UE actives
`/diameter`	Pairs Diameter	État de la connexion des pairs Diameter
`/logs`	Journaux	Diffusion en temps réel des journaux
`/docs`	Docs	Navigateur de documentation intégré
`/resources`	Ressources	Informations sur le VM BEAM et l'application
`/configuration`	Configuration	Visionneuse de configuration système

Tableau de Bord

Le Tableau de Bord fournit une vue d'ensemble de haut niveau de l'état d'OmniEPDG avec des indicateurs clés et une navigation rapide.

Cartes de Statistiques

Le tableau de bord affiche quatre statistiques principales :

Statistique	Description
Sessions Actives	Nombre actuel de sessions UE établies
Données Reçues (UL)	Total des octets reçus des UE (direction montante)
Données Envoyées (DL)	Total des octets envoyés aux UE (direction descendante)
Pairs Diameter	Pairs connectés / total des pairs configurés

Les valeurs de données s'ajustent automatiquement aux unités appropriées (B, Ko, Mo, Go).

Liens Rapides

Navigation directe vers des vues détaillées :

- **Voir les Sessions** - Naviguer vers la vue des Sessions pour des informations détaillées sur l'UE
- **Pairs Diameter** - Naviguer vers la vue des Pairs Diameter pour l'état de connectivité
- **Journaux Système** - Naviguer vers la vue des Journaux pour la diffusion en temps réel des journaux
- **Configuration** - Naviguer vers la vue de Configuration pour les paramètres système

Informations Système

Affiche la configuration opérationnelle actuelle :

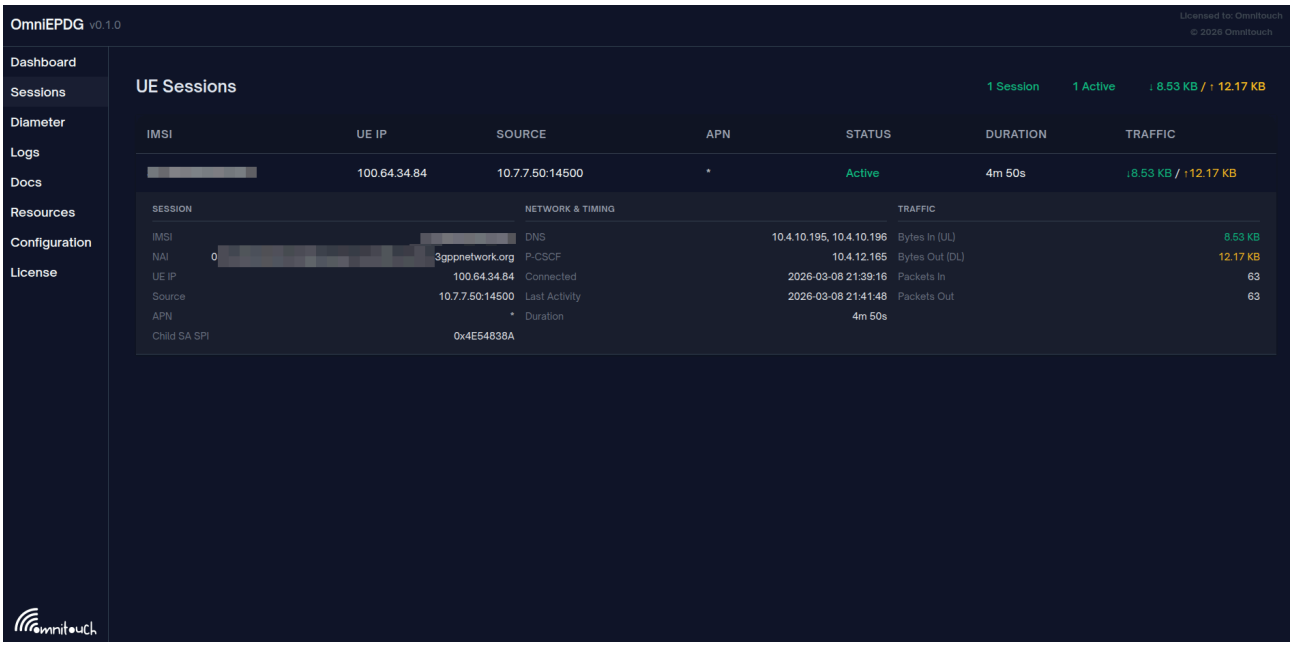
Champ	Description
Mode VPN	Mode actuel : `GTP` ou `SIMPLE`
Ports IKEv2	Ports standards : 500 (IKE), 4500 (NAT-T)
État Diameter	Indique si la signalisation Diameter est activée
Pool IP (IPv4)	CIDR du pool IP configuré (mode VPN simple uniquement)

Actualisation Automatique

Le tableau de bord se rafraîchit automatiquement chaque seconde pour afficher les statistiques actuelles.

Vue des Sessions

La vue des Sessions affiche toutes les sessions UE actives avec des informations détaillées pour chaque abonné.



La vue des Sessions montre les connexions UE actives avec des statistiques de trafic en temps réel et la durée de session.

Liste des Sessions

Chaque ligne de session affiche :

Colonne	Description
IMSI	Identité Internationale de l'Abonné Mobile de l'abonné
IP UE	Adresse IPv4/IPv6 assignée
SOURCE	IP externe et port de l'UE (adresse NAT)
APN	Nom du Point d'Accès pour la connexion
STATUT	État actuel de la session (Actif/Inactif)
DURÉE	Temps écoulé depuis l'établissement de la session
TRAFFIC	Octets reçus / envoyés (UL/DL)

Indicateurs de Statut

Les sessions affichent le statut avec des badges codés par couleur :

Statut	Couleur	Description
Actif	Vert	Session entièrement établie et opérationnelle
Connexion	Jaune	Établissement de session en cours
Inactif	Rouge	Session terminée ou échouée

Détails de la Session

Cliquez sur n'importe quelle ligne de session pour développer des informations détaillées :

Vue de session développée montrant IMSI, NAI, configuration réseau et statistiques de trafic.

Section Session

Champ	Description
IMSI	Valeur IMSI complète
NAI	Identifiant d'Accès Réseau (format 3GPP)
IP UE	Adresse IPv4/IPv6 assignée
Source	IP externe et port de l'UE (adresse NAT)
APN	Nom du Point d'Accès pour la connexion PDN
Child SA SPI	Index de Paramètre de Sécurité SA Enfant IPSec

Section Réseau & Timing

Champ	Description
DNS	Serveurs DNS fournis à l'UE
P-CSCF	Serveurs Proxy-CSCF pour la signalisation IMS
Connecté	Horodatage lorsque la session a été établie
Dernière Activité	Horodatage de la dernière activité de paquet
Durée	Temps écoulé depuis l'établissement de la session

Section Trafic

Champ	Description
Octets Entrants (UL)	Total des octets reçus de l'UE (montant)
Octets Sortants (DL)	Total des octets envoyés à l'UE (descendant)
Paquets Entrants	Total des paquets reçus de l'UE
Paquets Sortants	Total des paquets envoyés à l'UE

État Vide

Lorsque aucune session n'est active, la vue affiche :

- Message "Aucune session active"
- Indique si des connexions UE doivent être tentées

Actualisation Automatique

La liste des sessions se rafraîchit automatiquement chaque seconde.

Vue des Pairs Diameter

La vue des Pairs Diameter affiche l'état de tous les pairs Diameter configurés (HSS pour SWx, PGW pour S6b).

Liste des Pairs

Chaque ligne de pair affiche :

Colonne	Description
Pair	Identité Diameter (Origin-Host)
Royaume	Royaume Diameter (Origin-Realm)
Adresse IP	Adresse de transport au format `protocol://ip:port`
Statut	État de la connexion

Indicateurs de Statut

Statut	Couleur	Description
Connecté	Vert	Connexion du pair Diameter établie
Déconnecté	Rouge	Pair non connecté
Inconnu	Gris	Le statut ne peut pas être déterminé

Résumé du Compte des Pairs

L'en-tête affiche des comptes agrégés :

- **X Connectés** - Nombre de pairs avec des connexions actives
- **Y Déconnectés** - Nombre de pairs sans connexions

Détails du Pair

Cliquez sur n'importe quelle ligne de pair pour développer des informations détaillées :

Champ	Description
Initiation de Connexion	Qui initie : `local` (nous connectons au pair) ou `remote` (le pair se connecte à nous)
Transport	Protocole : `tcp` ou `sctp`
Nom du Produit	Nom du produit annoncé par le pair depuis CER/CEA
Applications Annoncées	Identifiants d'Application Diameter supportés par le pair

État Vide

Lorsque aucun pair n'est configuré, la vue affiche :

- "Aucun Pair Diameter configuré" si Diameter est activé
- "Diameter est désactivé" avec une indication de configuration si désactivé

Actualisation Automatique

La liste des pairs se rafraîchit automatiquement chaque seconde.

Vue des Journaux

La vue des Journaux fournit une diffusion en temps réel des journaux système avec des capacités de filtrage et de recherche.

Affichage des Journaux

Les journaux apparaissent dans un conteneur défilant avec les entrées les plus récentes en bas. Chaque entrée de journal affiche :

Élément	Description
Horodatage	Quand l'entrée de journal a été générée
Niveau	Niveau de gravité avec codage couleur
Message	Contenu du message de journal

Niveaux de Journal

Les journaux sont codés par couleur selon la gravité :

Niveau	Couleur	Description
debug	Gris	Informations de diagnostic détaillées
info	Bleu	Messages d'information généraux
warning	Jaune	Conditions d'avertissement
error	Rouge	Conditions d'erreur

Filtrage par Niveau

Filtrer les journaux par niveau de gravité minimum à l'aide du menu déroulant :

Filtre	Affiche
Tous les Niveaux	debug, info, warning, error
Info+	info, warning, error
Warning+	warning, error
Erreur Seulement	error

Recherche

La boîte de recherche filtre les journaux en temps réel :

- Entrez n'importe quel texte pour filtrer les messages de journal
- La correspondance est insensible à la casse
- Se vide lorsque la boîte de recherche est vidée

Contrôles

Contrôle	Description
Pause/Reprendre	Basculer la diffusion des journaux activée/désactivée
Effacer	Supprimer tous les journaux affichés
Défilement Automatique	Basculer le défilement automatique vers les nouvelles entrées

Tampon de Journal

- Maximum de 1000 entrées de journal sont conservées
- Les plus anciennes entrées sont supprimées lorsque la limite est atteinte
- Effacer les journaux supprime toutes les entrées de l'affichage

État Vide

Lorsque aucun journal ne correspond aux filtres actuels :

- Message "Aucun journal à afficher"
- Vérifiez les paramètres de filtre si des journaux sont attendus

Actualisation Automatique

De nouveaux journaux apparaissent automatiquement lorsqu'ils sont générés (lorsqu'ils ne sont pas en pause).

Vue des Docs

La vue des Docs fournit un navigateur de documentation intégré, permettant aux opérateurs d'accéder à toute la documentation d'OmniEPDG directement depuis le panneau de contrôle.

Sélection de Document

Sélectionnez parmi les fichiers de documentation disponibles à l'aide de la barre de boutons :

Document	Description
OPERATIONS.md	Guide des opérations avec démarrage rapide et procédures
README.md	Vue d'ensemble du projet et instructions de configuration
architecture.md	Architecture du système et flux d'appels
configuration.md	Référence complète de configuration
control-panel.md	Ce guide du panneau de contrôle
metrics.md	Référence des métriques Prometheus
troubleshooting.md	Problèmes courants et étapes de résolution

Rendu Markdown

La documentation est rendue avec un support complet de Markdown incluant :

- En-têtes et mise en forme du texte
- Blocs de code avec coloration syntaxique
- Tables
- Liens (internes et externes)
- Listes et citations

Vue des Ressources

La vue des Ressources affiche les statistiques du VM BEAM et les applications OTP en cours d'exécution.

Métriques Système

Métrique	Description
Utilisation de Mémoire	Mémoire totale utilisée par le VM BEAM
Processus BEAM	Nombre de processus Erlang/Elixir en cours d'exécution
Temps de Fonctionnement	Temps écoulé depuis le démarrage de l'application

Applications en Cours

Liste toutes les applications OTP chargées regroupées par catégorie :

Catégorie	Description
Principale	L'application OmniEPDG
Système	Applications de base Erlang/OTP et Elixir

Cliquez sur une application pour voir ses détails, y compris la version, la description et les dépendances.

Vue de Configuration

La vue de Configuration affiche la configuration d'exécution et les applications chargées.

Informations sur l'Environnement

Champ	Description
Environnement	Environnement Mix actuel (Développement/Production)
Version Elixir	Version d'Elixir en cours d'exécution

Liste des Applications

Affiche toutes les applications OTP chargées avec leurs versions. Sélectionnez une application pour voir :

- Description de l'application

- Informations sur la version
- Dépendances
- Paramètres de configuration

Configuration du Panneau de Contrôle

Port HTTP

Configurez le port du panneau de contrôle dans `config/runtime.exs` :

```
config :omniepdg, OmniEpdg.Web.Endpoint,
  http: [port: 4000]
```

Paramètre	Type	Par Défaut	Description
`port`	Entier	4000	Port HTTP pour le panneau de contrôle

Désactivation du Panneau de Contrôle

Le panneau de contrôle peut être désactivé en ne démarrant pas le point de terminaison web en production si ce n'est pas nécessaire. Contactez votre intégrateur système pour une configuration spécifique au déploiement.

Référence des métriques OmniEPDG

OmniEPDG expose des métriques Prometheus pour surveiller les flux d'authentification, le cycle de vie des sessions, la signalisation Diameter et la santé du système. Les métriques sont servies via HTTP pour le scraping par Prometheus.

Table des matières

- Point de terminaison des métriques
- Configuration
- Catégories de métriques
  - Métriques de session IKEv2
  - Métriques d'authentification EAP
  - Métriques de sécurité d'authentification
  - Métriques Diameter SWx
  - Métriques Diameter S6b
  - Métriques de cycle de vie des sessions
  - Métriques de plan de données ESP
  - Métriques de pool IP
  - Métriques VM
- Intégration Prometheus
- Exemples de requêtes
- Règles d'alerte

Point de terminaison des métriques

OmniEPDG expose des métriques à :

```
http://<host>:9568/metrics
```

Le point de terminaison renvoie des métriques au format d'exposition Prometheus, compatible avec Prometheus, Grafana et d'autres outils de surveillance.

Configuration

Configurez le point de terminaison des métriques dans `config/runtime.exs` :

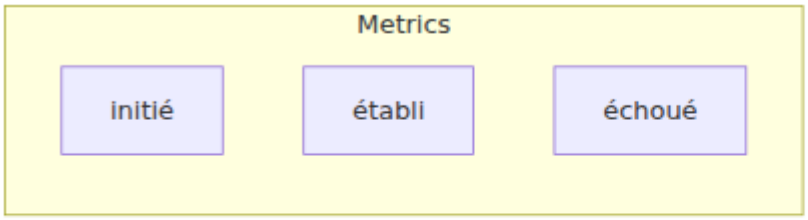
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

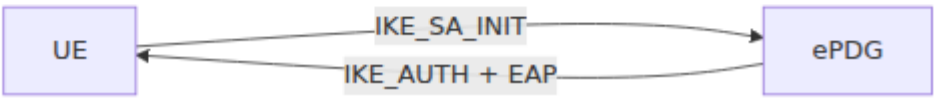
Paramètre	Type	Par défaut	Var Env	Description
`port`	Entier	`9568`	`PROMETHEUS_PORT`	Port HTTP pour le point de terminaison `/metrics`

Catégories de métriques

Métriques de session IKEv2

Métriques suivant l'établissement de tunnel IKEv2 sur l'interface SWu.





Métrique: `epdg_ikev2_session_initiated_count`
Type: Compteur
Description: Total des échanges IKE_SA_INIT initiés. S'incrémente lorsqu'un UE initie l'établissement du tunnel.

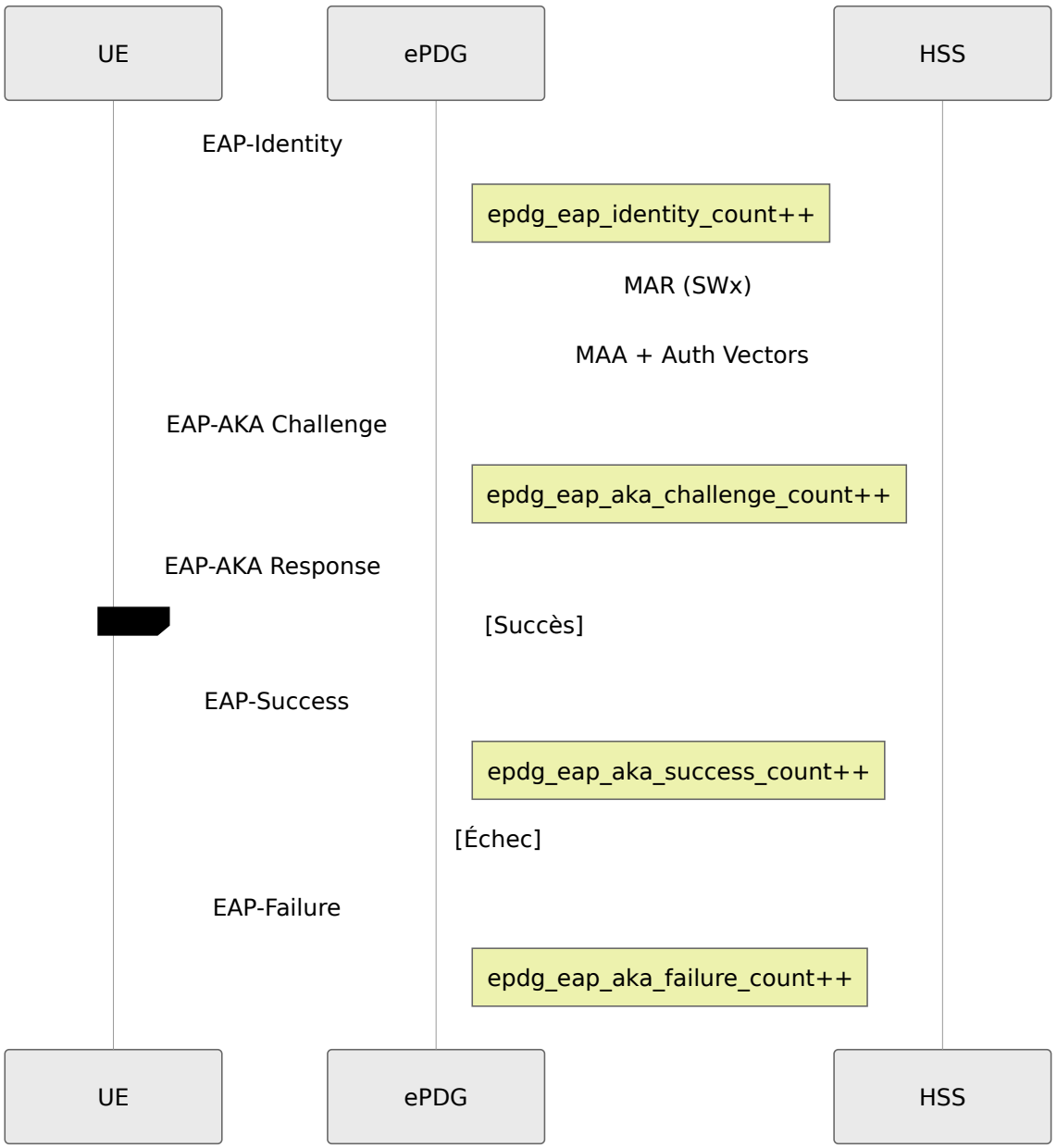
Métrique: `epdg_ikev2_session_established_count`
Type: Compteur
Description: Total des IKE SAs établis avec succès. S'incrémente après une authentification EAP-AKA réussie et la création de Child SA.

Métrique: `epdg_ikev2_session_failed_count`
Type: Compteur
Description: Total des échecs d'établissement d'IKE SA
Labels:

- `reason` - Raison de l'échec (par exemple, `auth_failed`, `timeout`, `invalid_proposal`)

Métriques d'authentification EAP

Métriques suivant les flux d'authentification EAP-AKA selon RFC 4187. OmniEPDG prend également en charge EAP-AKA' selon RFC 5448, avec le type d'authentification sélectionné automatiquement en fonction du préfixe d'identité NAI de l'UE.



Métrique: `epdg_eap_identity_count`
Type: Compteur
Description: Total des requêtes EAP-Identity reçues des UEs

Métrique: `epdg_eap_aka_challenge_count`
Type: Compteur
Description: Total des défis EAP-AKA envoyés aux UEs

Métrique: `epdg_eap_aka_success_count`
Type: Compteur
Description: Total des authentifications EAP-AKA réussies

Métrique: `epdg_eap_aka_failure_count`
Type: Compteur
Description: Total des authentifications EAP-AKA échouées
Labels:

- `reason` - Raison de l'échec (par exemple, `res_mismatch`, `invalid_identity`, `authentication_rejected`)

Métrique: `epdg_eap_aka_sync_failure_count`
Type: Compteur
Description: Total des échecs de synchronisation du numéro de séquence EAP-AKA (SQN). Indique un décalage de numéro de séquence USIM/HSS nécessitant une resynchronisation.

Métriques de sécurité d'authentification

Métriques pour la couche de sécurité d'authentification. Voir le Guide de sécurité pour les détails de configuration.

Métrique: `epdg_auth_verification_failed_count`
Type: Compteur
Description: Total des échecs de vérification de la charge utile AUTH. Indique des attaques potentielles de type homme du milieu ou des bogues d'implémentation.

Métrique: `epdg_auth_rate_limited_count`
Type: Compteur
Description: Total des tentatives d'authentification bloquées par limitation de débit
Labels:

- `type` - Raison du blocage : `ip` (seuil par IP dépassé) ou `imsi` (seuil par IMSI dépassé)

Exemples de requêtes:

```
# Tentatives limitées par minute
rate(epdg_auth_rate_limited_count[1m])

# Limité par type
sum by (type) (rate(epdg_auth_rate_limited_count[5m]))
```

Métrique: `epdg_auth_geoip_blocked_count`
Type: Compteur
Description: Total des tentatives d'authentification bloquées par filtrage de pays GeoIP
Labels:

- `country` - Code de pays ISO 3166-1 alpha-2 (par exemple, `CN`, `RU`), ou `UNKNOWN` pour les IPs qui n'ont pas pu être géolocalisées

Exemples de requêtes:

```
# Blocs GeoIP par minute
rate(epdg_auth_geoip_blocked_count[1m])

# Pays les plus bloqués
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))
```

Métrique: `epdg_esp_replay_detected_count`
Type: Compteur
Description: Total des paquets ESP rejetés en raison de la détection de répétition (selon RFC 4303). Indique des attaques potentielles de répétition ou des problèmes de réseau causant un réordonnancement des paquets.

Métriques Diameter SWx

Métriques pour l'interface SWx entre ePDG et HSS selon 3GPP TS 29.273.

Métrique: `epdg_diameter_swx_mar_count`
Type: Compteur

Description: Total des Multimedia-Auth-Requests envoyés au HSS pour la récupération des vecteurs d'authentification
Labels:

- `result` - Résultat de la requête : `success` ou `failure`

Métrique: `epdg_diameter_swx_sar_count`
Type: Compteur
Description: Total des Server-Assignment-Requests envoyés au HSS pour l'enregistrement/désenregistrement
Labels:

- `result` - Résultat de la requête : `success` ou `failure`

Métrique: `epdg_diameter_swx_mar_latency_ms`
Type: Histogramme
Description: Temps de réponse MAR en millisecondes
Seaux: 50, 100, 250, 500, 1000, 2500 ms

Métrique: `epdg_diameter_swx_sar_latency_ms`
Type: Histogramme
Description: Temps de réponse SAR en millisecondes
Seaux: 50, 100, 250, 500, 1000, 2500 ms

Métrique: `epdg_diameter_swx_pending_count`
Type: Jauge
Description: Nombre actuel de requêtes SWx en attente de réponse. Des valeurs élevées indiquent une congestion du HSS ou des problèmes de connectivité.

Métriques Diameter S6b

Métriques pour l'interface S6b entre le serveur AAA et le PGW selon 3GPP TS 29.273. Applicable uniquement en mode GTP.

Métrique: `epdg_diameter_s6b_aar_count`
Type: Compteur
Description: Total des AA-Requests traités pour l'autorisation de session
Labels:

- `result` - Résultat de la requête : `success` ou `failure`

Métrique: `epdg_diameter_s6b_str_count`
Type: Compteur
Description: Total des Session-Termination-Requests traités

Métrique: `epdg_diameter_s6b_active_sessions_count`
Type: Jauge
Description: Nombre actuel de sessions S6b actives

Métriques de cycle de vie des sessions

Métriques suivant la création et la terminaison de sessions PDN.

Métrique: `epdg_session_created_count`
Type: Compteur
Description: Total des sessions créées
Labels:

- `vpn_mode` - Mode VPN : `simple` ou `gtp`

Métrique: `epdg_session_terminated_count`
Type: Compteur
Description: Total des sessions terminées
Labels:

- `reason` - Raison de la terminaison : `user_request`, `timeout`, `error`, `admin`

Métrique: `epdg_sessions_active_count`
Type: Jauge

Description: Nombre actuel de sessions actives. Interrogé toutes les 5 secondes.

Métrique: `epdg_sessions_by_state_count`
Type: Jauge
Description: Sessions regroupées par état FSM
Labels:

- `state` - État de la session (par exemple, `init`, `eap_identity`, `eap_aka_challenge`, `authenticated`, `established`)

Métrique: `epdg_auth_duration_ms`
Type: Histogramme
Description: Durée totale du flux d'authentification de IKE_SA_INIT à session établie
Seaux: 100, 250, 500, 1000, 2500, 5000, 10000 ms

Métrique: `epdg_session_duration_seconds`
Type: Histogramme
Description: Durée de vie de la session de l'établissement à la terminaison
Seaux: 60, 300, 900, 1800, 3600, 7200, 14400 secondes (1 min à 4 heures)

Métriques de plan de données ESP

Métriques pour le traitement des paquets ESP selon RFC 4303.

Métrique: `epdg_esp_packets_in_count`
Type: Compteur
Description: Total des paquets ESP décryptés avec succès (direction UE → réseau)

Métrique: `epdg_esp_packets_out_count`
Type: Compteur
Description: Total des paquets ESP chiffrés (direction réseau → UE)

Métrique: `epdg_esp_bytes_in_total`
Type: Jauge
Description: Total des octets décryptés des paquets ESP

Métrique: `epdg_esp_bytes_out_total`
Type: Jauge
Description: Total des octets chiffrés dans les paquets ESP

Métriques de pool IP

Métriques pour la gestion du pool d'adresses IP en mode VPN simple.

Métrique: `epdg_ip_allocated_count`
Type: Compteur
Description: Total des adresses IP allouées
Labels:

- `type` - Type d'adresse : `ipv4` ou `ipv6`

Métrique: `epdg_ip_released_count`
Type: Compteur
Description: Total des adresses IP libérées
Labels:

- `type` - Type d'adresse : `ipv4` ou `ipv6`

Métrique: `epdg_ip_pool_allocated_count`
Type: Jauge
Description: Nombre actuel d'adresses IP allouées

Métrique: `epdg_ip_pool_available_count`
Type: Jauge
Description: Nombre actuel d'adresses IP disponibles dans le pool

---

Métrique: `epdg_ip_pool_utilization_ratio`
Type: Jauge
Description: Utilisation du pool IP en tant que ratio de 0.0 à 1.0. Des valeurs proches de 1.0 indiquent un risque d'épuisement du pool.

Métriques VM

Métriques de machine virtuelle Erlang/BEAM pour la surveillance de la santé du système.

Métrique: `vm_memory_total`
Type: Jauge
Unité: Octets
Description: Mémoire totale allouée par la VM

Métrique: `vm_memory_processes`
Type: Jauge
Unité: Octets
Description: Mémoire utilisée par les processus Erlang

Métrique: `vm_memory_binary`
Type: Jauge
Unité: Octets
Description: Mémoire utilisée pour les binaires (y compris les tampons de paquets)

Métrique: `vm_memory_ets`
Type: Jauge
Unité: Octets
Description: Mémoire utilisée par les tables ETS (état de session, registres)

Métrique: `vm_system_info_process_count`
Type: Jauge

Description: Nombre de processus Erlang en cours d'exécution

Métrique: `vm_system_info_port_count`
Type: Jauge
Description: Nombre de ports ouverts (sockets, descripteurs de fichiers)

Métrique: `vm_statistics_run_queue`
Type: Jauge
Description: Longueur totale des files d'attente du planificateur. Des valeurs élevées indiquent une saturation du CPU.

Intégration Prometheus

Configuration de scraping

Ajoutez OmniEPDG à votre `prometheus.yml` :

```yaml
scrape_configs:
  - job_name: 'omniepdg'
    scrape_interval: 15s
    static_configs:
      - targets: ['epdg-host:9568']
        labels:
          instance: 'epdg-01'
          environment: 'production'
```

Découverte de services

Pour les déploiements Kubernetes, utilisez la découverte de services :

```yaml
scrape_configs:
  - job_name: 'omniepdg'
    kubernetes_sd_configs:
      - role: pod
    relabel_configs:
      - source_labels: [__meta_kubernetes_pod_label_app]
        action: keep
        regex: omniepdg
      - source_labels:
[__meta_kubernetes_pod_annotation_prometheus_io_port]
        action: replace
        target_label: __address__
        regex: (.+)
        replacement: ${1}:9568
```

Exemples de requêtes

Taux de succès d'authentification

```
# Taux de succès sur 5 minutes
sum(rate(epdg_eap_aka_success_count[5m]))
/
(sum(rate(epdg_eap_aka_success_count[5m])) +
sum(rate(epdg_eap_aka_failure_count[5m])))
```

Taux d'établissement de session

```
# Sessions établies par seconde
rate(epdg_ikev2_session_established_count[5m])
```

Latence d'authentification (p95)

```
histogram_quantile(0.95,
sum(rate(epdg_auth_duration_ms_bucket[5m])) by (le))
```

Latence HSS (p99)

```
histogram_quantile(0.99,
sum(rate(epdg_diameter_swx_mar_latency_ms_bucket[5m])) by (le))
```

Sessions actives

```
epdg_sessions_active_count
```

Utilisation du pool IP

```
epdg_ip_pool_utilization_ratio * 100
```

Débit ESP

```
# Octets par seconde (entrant)
rate(epdg_esp_bytes_in_total[5m])

# Paquets par seconde (dans les deux sens)
rate(epdg_esp_packets_in_count[5m]) +
rate(epdg_esp_packets_out_count[5m])
```

Répartition des échecs par raison

```
# Échecs EAP par raison
sum by (reason) (rate(epdg_eap_aka_failure_count[5m]))

# Terminaisons de session par raison
sum by (reason) (rate(epdg_session_terminated_count[5m]))
```

Règles d'alerte

Exemples de règles d'alerte Prometheus pour OmniEPDG :

```yaml
groups:
  - name: omniepdg
    rules:
      # Taux d'échec d'authentification élevé
      - alert: OmniEPDGHighAuthFailureRate
        expr: |
          sum(rate(epdg_eap_aka_failure_count[5m]))
          /
          (sum(rate(epdg_eap_aka_success_count[5m])) +
sum(rate(epdg_eap_aka_failure_count[5m])))
          > 0.1
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Taux d'échec d'authentification EAP-AKA élevé"
          description: "Le taux d'échec d'authentification est {{
$value | humanizePercentage }} au cours des 5 dernières minutes"

      # Pool IP proche de l'épuisement
      - alert: OmniEPDGIPPoolLow
        expr: epdg_ip_pool_utilization_ratio > 0.9
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Utilisation du pool IP supérieure à 90%"
          description: "Le pool IP est {{ $value |
humanizePercentage }} utilisé"

      # Pool IP épuisé
      - alert: OmniEPDGIPPoolExhausted
        expr: epdg_ip_pool_available_count == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "Pool IP épuisé"
          description: "Aucune adresse IP disponible pour de
nouvelles sessions"

      # Latence HSS élevée
      - alert: OmniEPDGHSSLatencyHigh
```

```
        expr: |
          histogram_quantile(0.95,
sum(rate(epdg_diameter_swx_mar_latency_ms_bucket[5m])) by (le))
          > 1000
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Latence HSS (SWx) élevée"
          description: "Le 95e percentile de la latence MAR est {{
$value }}ms"

      # Arriéré de requêtes SWx en attente
      - alert: OmniEPDGSWxBacklog
        expr: epdg_diameter_swx_pending_count > 100
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "Arriéré de requêtes SWx en cours de formation"
          description: "{{ $value }} requêtes SWx en attente"

      # Mémoire VM élevée
      - alert: OmniEPDGMemoryHigh
        expr: vm_memory_total > 2147483648
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Utilisation de la mémoire OmniEPDG élevée"
          description: "L'utilisation de la mémoire VM est {{
$value | humanize1024 }}"

      # Surcharge du planificateur
      - alert: OmniEPDGSchedulerOverload
        expr: vm_statistics_run_queue > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Longueur de la file d'attente du planificateur
Erlang élevée"
          description: "La longueur de la file d'attente est {{
$value }}, indiquant une saturation du CPU"
```

```
      # Pas de sessions (problème de service potentiel)
      - alert: OmniEPDGNoSessions
        expr: epdg_sessions_active_count == 0 and
epdg_ikev2_session_initiated_count > 0
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Aucune session active malgré des tentatives de
connexion"
          description: "Des sessions sont initiées mais aucune
n'est active"

      # Activité de limitation de débit élevée (attaque
potentielle)
      - alert: OmniEPDGHighRateLimiting
        expr: rate(epdg_auth_rate_limited_count[5m]) > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Taux élevé de tentatives d'authentification
bloquées"
          description: "{{ $value | printf \"%.1f\" }} tentatives
d'authentification bloquées par seconde"

      # Pic de blocage GeoIP (attaque potentielle d'une région
spécifique)
      - alert: OmniEPDGGeoIPBlockingSpike
        expr: |
          rate(epdg_auth_geoip_blocked_count[5m]) > 5
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Activité de blocage GeoIP élevée"
          description: "{{ $value | printf \"%.1f\" }} connexions
bloquées par seconde par GeoIP"

      # Attaques de répétition ESP détectées
      - alert: OmniEPDGReplayAttack
        expr: rate(epdg_esp_replay_detected_count[5m]) > 0
        for: 2m
```

```
        labels:
          severity: warning
        annotations:
          summary: "Attaques de répétition ESP détectées"
          description: "{{ $value | printf \"%.1f\" }} tentatives
de répétition par seconde"

      # Échecs de vérification AUTH (potentiel MITM)
      - alert: OmniEPDGAuthVerificationFailures
        expr: rate(epdg_auth_verification_failed_count[5m]) > 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Échecs de vérification de la charge utile AUTH
détectés"
          description: "Attaque potentielle de type homme du
milieu ou bogue d'implémentation"
```

Mode N3IWF (Accès Non-3GPP Non Fiable 5G)

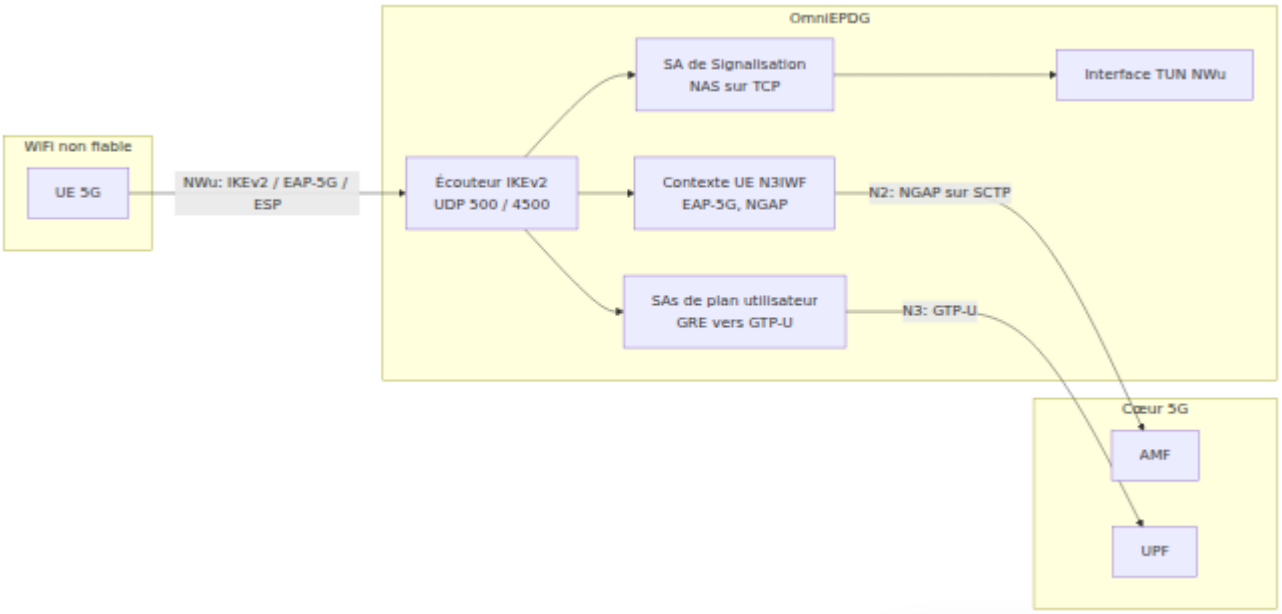
OmniEPDG peut fonctionner comme une **Fonction d'Interconnexion Non-3GPP (N3IWF)**. Dans ce mode, un UE 5G sur un réseau WiFi non fiable se connecte au cœur 5G (5GC) via OmniEPDG. Le N3IWF et l'ePDG utilisent le même écouteur IKEv2, le même chemin de données ESP et le même socket GTP-U.

Retour au Guide des Opérations.

Table des Matières

- Aperçu de l'Architecture
- Comment OmniEPDG Sélectionne le Mode N3IWF
- Interfaces
- Sélection AMF
- Flux d'Enregistrement
- Flux de Session PDU
- Flux de Libération
- Adressage Intérieur NWu
- Configuration
- Exigences d'Hôte
- Métriques
- Limitations
- Dépannage
- Spécifications 3GPP

Aperçu de l'Architecture



Le N3IWF relaie les messages NAS entre l'UE et l'AMF. Le N3IWF ne lit pas le contenu NAS. Les données utilisateur circulent dans des paquets GRE à l'intérieur des SAs enfants IPsec. Le N3IWF convertit chaque paquet GRE en un paquet GTP-U pour le UPF, et vice versa pour les données descendantes.

Comment OmniEPDG Sélectionne le Mode N3IWF

OmniEPDG examine la première demande IKE_AUTH de chaque SA IKE.

UE envoie	Comportement d'OmniEPDG
IDi de type `ID_KEY_ID` et pas de charge utile AUTH	La session fonctionne comme une session N3IWF (UE 5G).
IDi de type `ID_RFC822_ADDR` (NAI)	La session fonctionne comme une session ePDG (EAP-AKA, SWx, S2b).

Un UE 5G doit envoyer `ID_KEY_ID` dans IDi, comme le spécifient 3GPP TS 33.501 §7.2.1 et 3GPP TS 24.502 §7.3.2.1. Les sessions ePDG ne changent pas lorsque vous activez le mode N3IWF.

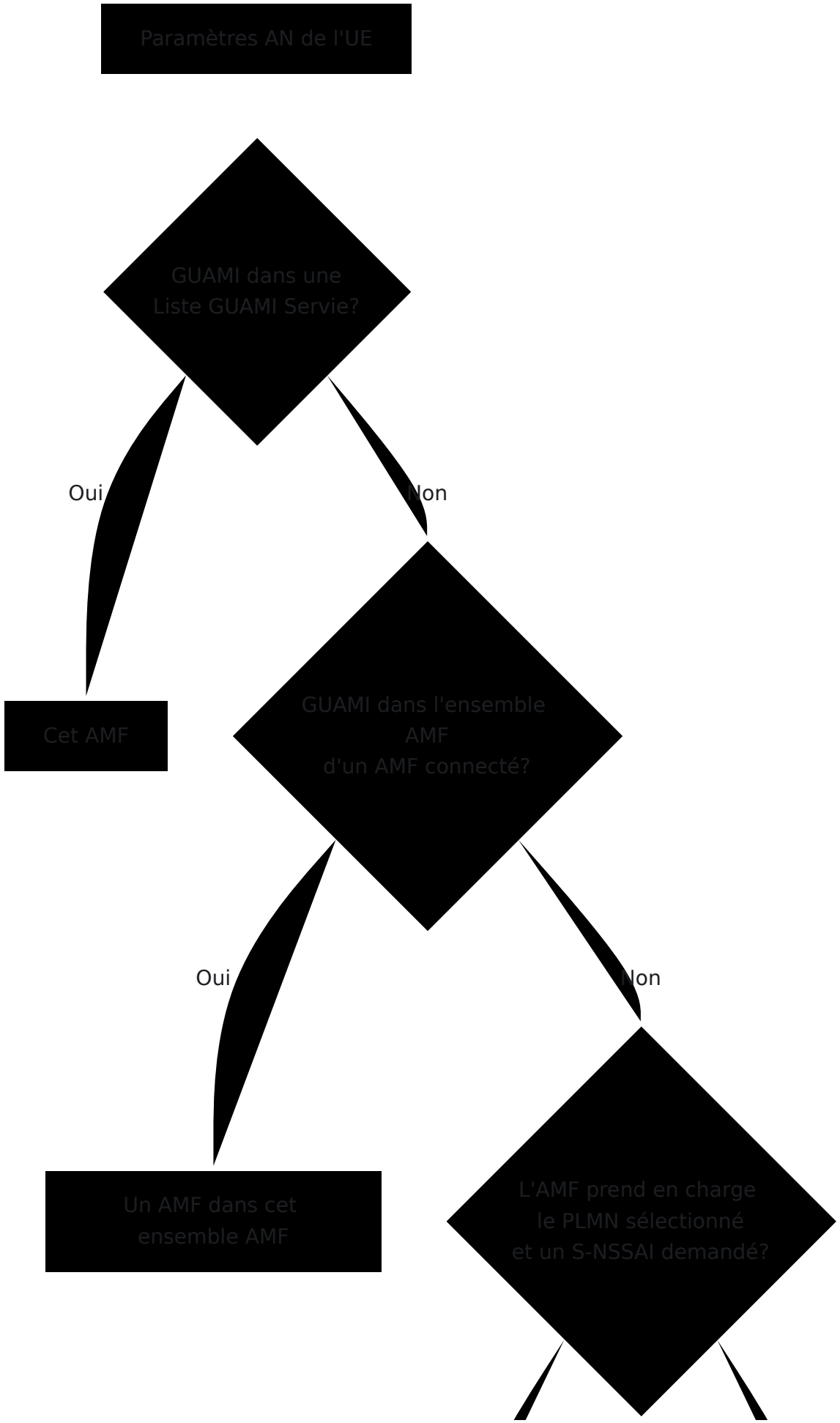
Interfaces

Interface	Pair	Transport	Protocole	Référence
NWu	UE 5G	UDP 500 / 4500	IKEv2, EAP-5G, ESP (NAT-T)	TS 24.502, RFC 7296
NWu (intérieur)	UE 5G	TCP à l'intérieur de la SA de signalisation	Enveloppe de message NAS	TS 24.502 §8.2
NWu (intérieur)	UE 5G	GRE à l'intérieur des SAs de plan utilisateur	GRE avec QFI dans la clé	TS 24.502 §8.3
N2	AMF	SCTP, PPID 60	NGAP	TS 38.412, TS 38.413
N3	UPF	UDP 2152	GTP-U avec Conteneur de Session PDU	TS 29.281, TS 38.415

Au démarrage, OmniEPDG se connecte à chaque AMF dans `amfs` et envoie à chacun une Demande de Configuration NG avec un `GlobalN3IWF-ID`. OmniEPDG accepte les UE 5G lorsque au moins un AMF a envoyé une Réponse de Configuration NG. Si une association SCTP échoue, OmniEPDG essaie à nouveau cet AMF toutes les 5 secondes. Si une association tombe, OmniEPDG libère uniquement les sessions N3IWF sur cet AMF.

Sélection AMF

Le N3IWF sélectionne un AMF pour chaque UE lorsque le premier message NAS EAP-5G arrive. Le N3IWF utilise les paramètres AN de l'UE (TS 24.502 §9.3.2.2.2) et les données que chaque AMF a envoyées dans sa Réponse de Configuration NG. L'UE reste sur cet AMF jusqu'à la libération. Voir TS 23.501 §6.3.5.


Paramètres AN de l'UE
GUAMI dans une Liste GUAMI Servie?
Oui
Non
Cet AMF
GUAMI dans l'ensemble AMF d'un AMF connecté?
Oui
Non
Un AMF dans cet ensemble AMF
L'AMF prend en charge le PLMN sélectionné et un S-NSSAI demandé?



Étape	Paramètre AN	Données AMF de la Réponse de Configuration NG	Résultat
1	GUAMI	Liste GUAMI Servie	L'AMF qui sert ce GUAMI exact. Un UE enregistré retourne à son AMF.
2	GUAMI	Liste GUAMI Servie	Un AMF avec le même PLMN, ID de Région AMF et ID de l'Ensemble AMF.
3	ID PLMN Sélectionné, NSSAI Demandé	Liste de Support PLMN	Un AMF qui prend en charge le PLMN sélectionné et au moins un S-NSSAI demandé. Si l'UE n'envoie pas de PLMN ou de NSSAI, cette vérification ne s'applique pas.

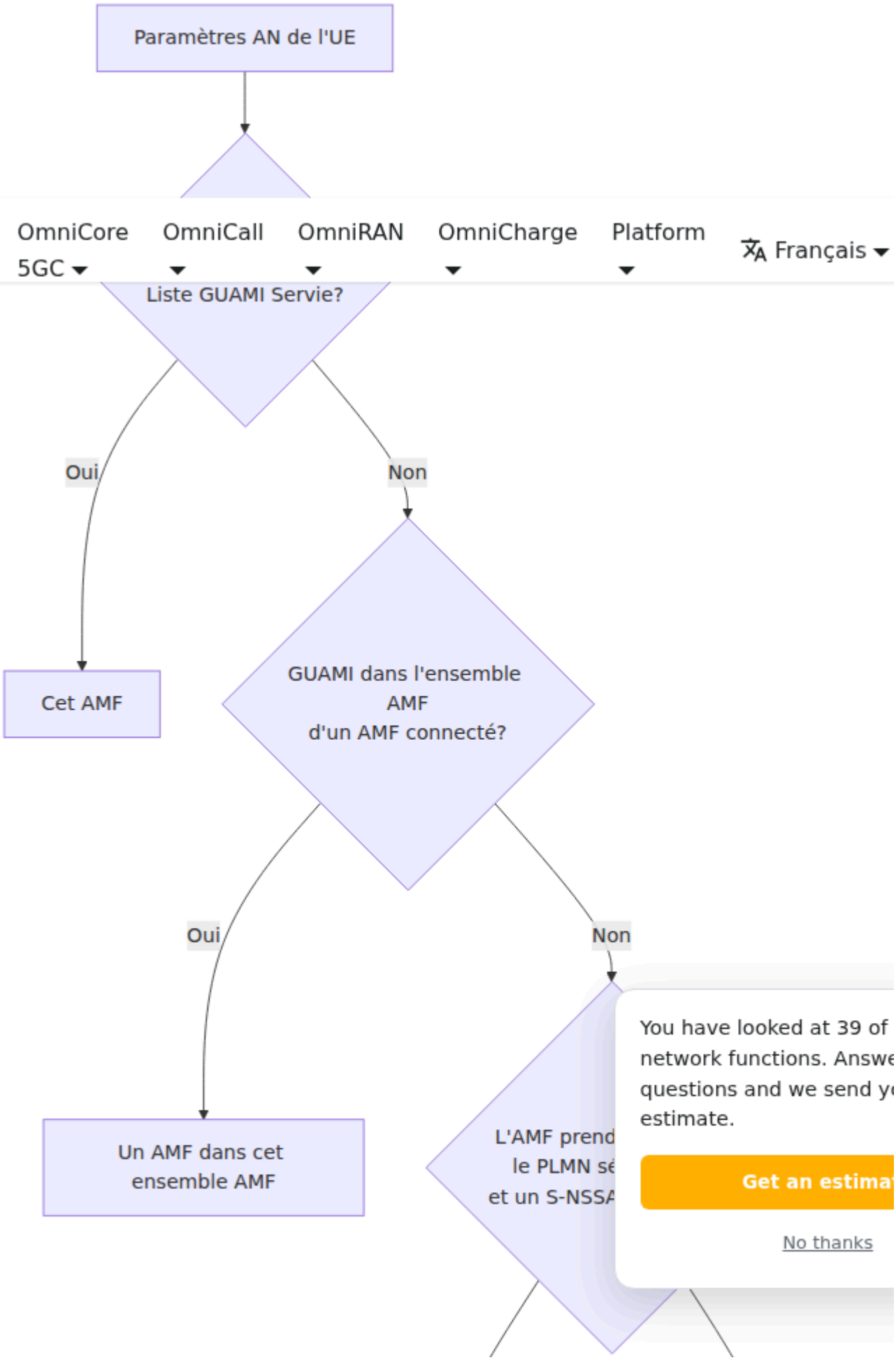
Lorsque plus d'un AMF correspond à une étape, le N3IWF en sélectionne un au hasard. La sélection est pondérée par la Capacité Relative de l'AMF de chaque AMF. Un AMF avec une capacité de 0 obtient un UE uniquement lorsque le GUAMI exact de l'UE lui correspond, ou lorsque chaque AMF correspondant a une capacité de 0.

Si aucun AMF connecté ne correspond, le N3IWF envoie EAP-Failure à l'UE et consigne `aucun AMF ne sert le GUAMI, PLMN ou tranches de l'UE`.

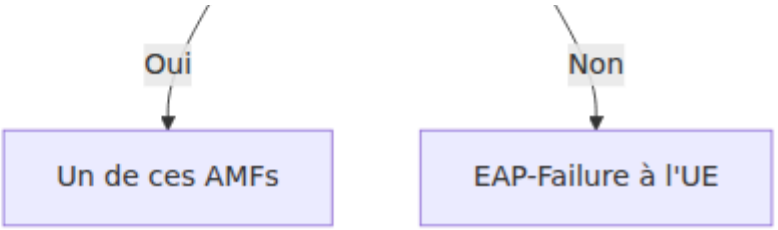
Cas d'utilisation : Utilisez un N3IWF pour des abonnés sur différents cœurs 5G. Mettez chaque AMF de cœur dans `amfs`. Les UEs qui se sont enregistrés

auparavant retournent à leur propre AMF par GUAMI. Les nouveaux UEs vont vers un AMF qui sert leur PLMN et leurs tranches.

Flux d'Enregistrement



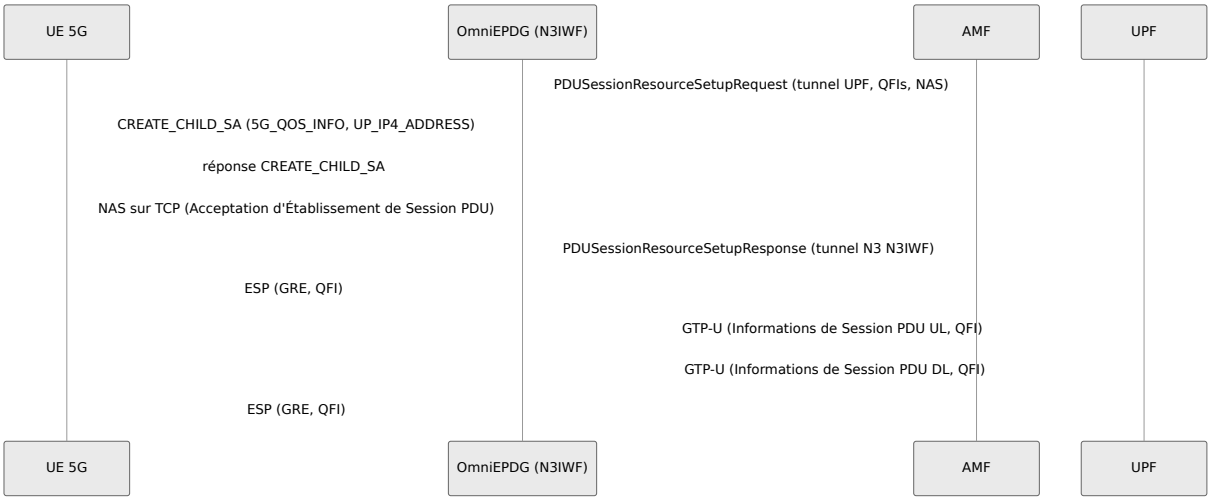
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Français
You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks



Ces points s'appliquent au flux :

- Le N3IWF signe sa première réponse IKE_AUTH avec la clé dans `key_file`. Le N3IWF inclut son certificat uniquement si l'UE envoie CERTREQ.
- Le N3IWF ne répond pas à une demande EAP-5G de l'UE tant que l'AMF n'envoie pas un message NAS descendant ou la clé N3IWF.
- L'UE et le N3IWF utilisent **Kn3iwf** de la Demande de Configuration de Contexte Initial comme EAP MSK. Les deux pairs calculent leurs charges utiles AUTH finales à partir de cette clé.
- Si l'AMF envoie un NAS descendant avant que l'UE n'ouvre la connexion TCP, le N3IWF conserve le message NAS et l'envoie lorsque la connexion s'ouvre.
- Si l'UE envoie EAP-Response/5G-Stop, le N3IWF envoie EAP-Failure et supprime la SA IKE.

Flux de Session PDU



Le N3IWF crée un SA enfant de plan utilisateur pour chaque session PDU. Ce SA enfant est le SA enfant par défaut et transporte tous les flux QoS de la session PDU. La charge utile de notification 5G_QOS_INFO indique à l'UE l'ID de session PDU et les QFIs.

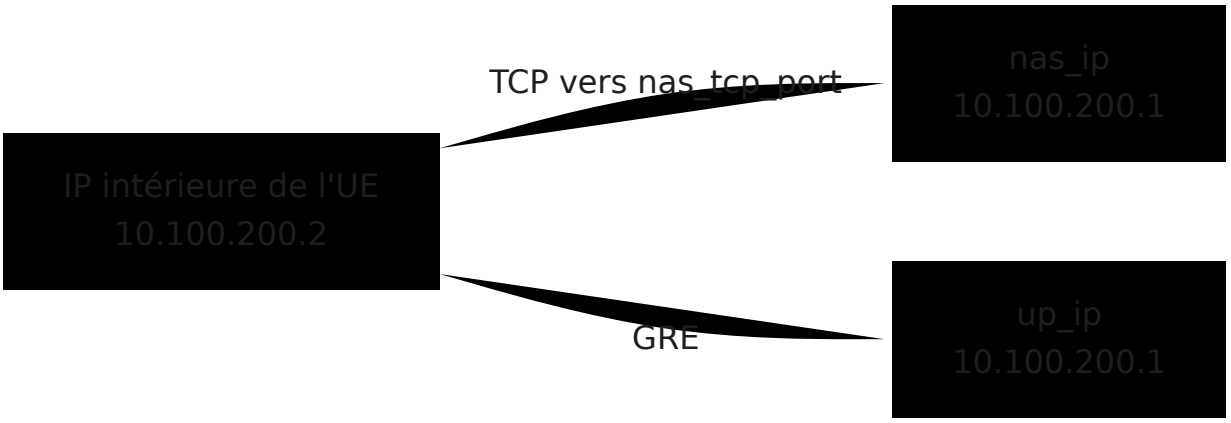
Si l'UE rejette un SA enfant, ou ne répond pas après 5 transmissions, le N3IWF signale la session PDU comme échouée dans la PDUSessionResourceSetupResponse.

Flux de Libération

Déclencheur	Action N3IWF
UEContextReleaseCommand de l'AMF	Le N3IWF supprime la SA IKE, ferme connexion NAS et envoie UEContextReleaseComplete.
L'UE supprime la SA IKE	Le N3IWF envoie UEContextReleaseRequest à l'AMF.
PDUSessionResourceReleaseCommand de l'AMF	Le N3IWF supprime le SA enfant de chaque session PDU et envoie PDUSessionResourceReleaseRespons
NG Reset de l'AMF	Le N3IWF libère les UEs nommés (ou tous les UEs) et envoie NGResetAcknowledge.
Association N2 perdue	Le N3IWF libère toutes les sessions N3IWF.
Inactivité de session	Le N3IWF libère la session après `session_inactivity_timeout_ms` sa trafic IKE ou ESP. Voir la Référence d Configuration.

Adressage Intérieur NWu

Le N3IWF attribue à chaque UE une **adresse IP intérieure** provenant de `ue_ip_pool`. L'UE utilise cette adresse à l'intérieur de ses tunnels IPsec.



- **SA de Signalisation :** L'UE ouvre une connexion TCP à `nas_ip` et `nas_tcp_port`. Le N3IWF écrit ces paquets dans l'interface TUN NWu, de sorte que la pile TCP de Linux termine la connexion.
- **SAs de Plan Utilisateur :** L'UE envoie des paquets GRE à `up_ip`. OmniEPDG décapsule GRE dans l'espace utilisateur. Le noyau ne voit pas ces paquets.

Le pool ne donne pas `nas_ip` ou `up_ip` à un UE. `nas_ip` et `up_ip` peuvent être la même adresse.

Configuration

Le mode N3IWF est désactivé par défaut. Définissez les paramètres dans `runtime.exs`.

```
config :omniepdg, :n3iwf,
  enabled: true,
  # GlobalN3IWF-ID et TA servie pour NG Setup
  n3iwf_id: 1,
  name: "OmniN3IWF",
  plmn: {"001", "01"},
  tac: 1,
  slices: [%{sst: 1, sd: nil}],
  # N2 (SCTP) vers chaque AMF
  amfs: [
    %{name: "amf1", ip: {10, 74, 0, 40}, port: 38412},
    %{name: "amf2", ip: {10, 74, 0, 41}, port: 38412}
  ],
  ngap_local_ip: {10, 74, 0, 13},
  # IDr envoyé aux UEs et le certificat/clés qui signe IKE_AUTH
  identity: "n3iwf.5gc.mnc001.mcc001.3gppnetwork.org",
  cert_file: "/etc/omniepdg/certs/n3iwf.crt",
  key_file: "/etc/omniepdg/certs/n3iwf.key",
  # Adresse N3 GTP-U annoncée au UPF
  n3_ip: {10, 74, 0, 13},
  # Adressage intérieur NWu
  ue_ip_pool: "10.100.200.0/24",
  nas_ip: {10, 100, 200, 1},
  up_ip: {10, 100, 200, 1},
  nas_tcp_port: 20000,
  tun_name: "omnin3iwf0"
```

Tous les paramètres sont requis lorsque `enabled` est `true`. Si un paramètre est manquant ou non valide, OmniEPDG ne démarre pas. L'erreur de démarrage nomme le paramètre.

Paramètres

Paramètre	Type	Requis	Par défaut	Description
`enabled`	Booléen	Oui	`false`	Active ou désactive le mode N3IWF. Lorsque `false`, OmniEPDG ignore tous les autres paramètres N3IWF.
`n3iwf_id`	Entier	Oui	-	ID N3IWF dans le `GlobalN3IWF-ID` de la Demande de Configuration NG. Plage de 0 à 65535 (16 bits). Voir TS 38.413 §9.3.1.57.
`name`	Chaîne	Oui	-	Nom du Nœud RAN dans la Demande de Configuration NG. L'AMF affiche ce nom pour le N3IWF.
`plmn`	Tuple	Oui	-	PLMN du N3IWF sous forme de chaînes de chiffres `{mcc, mnc}`. Le MNC a 2 ou 3 chiffres. L'AMF doit servir ce PLMN.
`tac`	Entier	Oui	-	Code de Zone de Suivi (24 bits) dans la Liste de TA Supportée de la Demande de Configuration NG. L'AMF doit servir ce TAC.

Paramètre	Type	Requis	Par défaut	Description
`slices`	Liste	Oui	-	S-NSSAIs que le N3IWF prend en charge. Chaque entrée est `%{sst: 0..255, sd: nil}` ou `%{sst: 0..255, sd: <<b1, b2, b3>>}`.
`amfs`	Liste	Oui	-	AMFs à connecter via N2. Chaque entrée est `%{name: chaîne, ip: tuple IPv4, port: entier}`. `name` est une étiquette unique pour les journaux. `port` est le port SCTP de l'interface N2 de l'AMF. Le port standard est 38412 (TS 38.412). Voir Sélection AMF.
`ngap_local_ip`	Tuple	Oui	-	Adresse IPv4 locale pour les associations SCTP aux AMFs.
`identity`	Chaîne	Oui	-	Identité N3IWF (FQDN) dans la charge utile IDr. L'UE compare cette valeur avec le N3IWF qu'il a sélectionné. Utilisez le FQDN dans le certificat.
`cert_file`	Chaîne	Oui	-	Chemin du certificat N3IWF (PEM). Le N3IWF

Paramètre	Type	Requis	Par défaut	Description
				envoie ce certificat lorsque l'UE envoie CERTREQ.
`key_file`	Chaîne	Oui	-	Chemin de la clé privée (PEM, non chiffrée) pour `cert_file`. Les clés RSA signent avec la méthode AUTH 1. Les clés ECDSA P-256 signent avec la méthode AUTH 9.
`n3_ip`	Tuple	Oui	-	Adresse IPv4 sur N3 que le N3IWF donne à l'AMF pour le GTP-U descendant. Le UPF envoie des données descendantes à cette adresse sur UDP 2152.
`ue_ip_pool`	Chaîne	Oui	-	CIDR IPv4 pour les adresses intérieures des UE. La longueur de préfixe doit être de 8 à 30.
`nas_ip`	Tuple	Oui	-	Adresse IPv4 intérieure pour NAS sur TCP. Le N3IWF l'envoie dans la charge utile de notification NAS_IP4_ADDRESS et l'assigne à l'interface TUN NWu. Utilisez une

Paramètre	Type	Requis	Par défaut	Description
				adresse à l'intérieur de `ue_ip_pool`.
`up_ip`	Tuple	Oui	-	Adresse IPv4 intérieure pour les données utilisateur GRE. Le N3IWF l'envoie dans la charge utile de notification UP_IP4_ADDRESS.
`nas_tcp_port`	Entier	Oui	-	Port TCP pour le transport NAS. Le N3IWF l'envoie dans la charge utile de notification NAS_TCP_PORT.
`tun_name`	Chaîne	Oui	-	Nom de l'interface TUN NWu. Utilisez un nom qu'aucun autre processus n'utilise.

Le N3IWF utilise les paramètres de l'écouteur IKEv2 (`listen_ip`, `port_500`, `port_4500`) et `session_inactivity_timeout_ms` de la configuration principale. Voir la Référence de Configuration.

Exemple de Configuration : ePDG et N3IWF sur un Hôte

```
config :omniepdg,
  listen_ip: {0, 0, 0, 0},
  port_500: 500,
  port_4500: 4500,
  vpn_mode: :gtp

config :omniepdg, :n3iwf,
  enabled: true,
  n3iwf_id: 1,
  name: "OmniN3IWF",
  plmn: {"001", "01"},
  tac: 1,
  slices: [%{sst: 1, sd: nil}],
  amfs: [%{name: "amf1", ip: {10, 74, 0, 40}, port: 38412}],
  ngap_local_ip: {10, 74, 0, 13},
  identity: "n3iwf.5gc.mnc001.mcc001.3gppnetwork.org",
  cert_file: "/etc/omniepdg/certs/n3iwf.crt",
  key_file: "/etc/omniepdg/certs/n3iwf.key",
  n3_ip: {10, 74, 0, 13},
  ue_ip_pool: "10.100.200.0/24",
  nas_ip: {10, 100, 200, 1},
  up_ip: {10, 100, 200, 1},
  nas_tcp_port: 20000,
  tun_name: "omnin3iwf0"
```

Comment ça fonctionne : Les UEs 4G (identité NAI) utilisent le flux ePDG et le PGW via S2b. Les UEs 5G (identité `ID_KEY_ID`) utilisent le flux N3IWF et l'AMF via N2. Les deux flux partagent UDP 500, UDP 4500 et le socket GTP-U sur UDP 2152.

Cas d'utilisation : Une passerelle d'appel WiFi pour les abonnés 4G et 5G.

Les paramètres dans le premier bloc se trouvent dans la Référence de Configuration. Les paramètres dans le deuxième bloc se trouvent dans Paramètres.

Exigences d'Hôte

- OmniEPDG doit avoir la permission de créer l'interface TUN NWu et d'exécuter `ip addr` et `ip link` pour celle-ci (`CAP_NET_ADMIN`). Si OmniEPDG ne peut pas créer l'interface, il ne démarre pas.
- Le noyau doit avoir le support SCTP (module `sctp`).
- Autoriser SCTP de `ngap_local_ip` à chaque AMF dans `amfs` sur son `port`.
- Autoriser UDP 2152 entre `n3_ip` et le UPF.
- Le UPF doit acheminer le trafic descendant vers `n3_ip`.

Métriques

Les sessions N3IWF utilisent les mêmes métriques de session que les sessions ePDG. Voir la Référence des Métriques.

Métrique : `epdg_session_created_count` **Type** : Compteur **Description** : Total des sessions créées. Les sessions N3IWF ont la valeur d'étiquette `vpn_mode="n3iwf"`. **Étiquettes** :

- `vpn_mode` - `simple`, `gtp` ou `n3iwf`

Exemples de requêtes :

```
# Enregistrements N3IWF par seconde
rate(epdg_session_created_count{vpn_mode="n3iwf"}[5m])
```

La page des Sessions du panneau de contrôle montre les sessions N3IWF avec l'étiquette `n3iwf-<RAN-UE-NGAP-ID>`. Le N3IWF ne connaît pas le SUPI, car les messages NAS sont chiffrés entre l'UE et l'AMF.

Limitations

- IPv4 uniquement pour les adresses intérieures, le transport NAS et N3.
- Le N3IWF envoie le même `plmn`, `tac` et `slices` dans la Demande de Configuration NG à chaque AMF. Chaque AMF dans `amfs` doit servir ce

PLMN et ce TAC.

- Le N3IWF lit uniquement la Liste GUAMI Servie, la Liste de Support PLMN et la Capacité Relative de l'AMF à partir de la Réponse de Configuration NG. Il n'applique pas une Mise à Jour de Configuration AMF.
- Un SA enfant de plan utilisateur pour chaque session PDU. Le N3IWF ne crée pas de SAs enfants supplémentaires pour des flux QoS séparés.
- Le N3IWF n'accepte pas les demandes CREATE_CHILD_SA de l'UE. Il répond par NO_ADDITIONAL_SAS, donc la réinitialisation initiée par l'UE n'est pas disponible.
- Le N3IWF consigne PDUSessionResourceModifyRequest et n'agit pas dessus.

Dépannage

Les UEs 5G ne se Connectent Pas

Symptômes : L'UE envoie IKE_AUTH et reçoit AUTHENTICATION_FAILED. Le journal montre `n2_not_ready`.

Causes possibles :

- Aucune association SCTP à un AMF n'est active.
- Les AMFs ont rejeté la Demande de Configuration NG.

Résolution :

1. Recherchez `N2 SCTP connect to AMF failed` ou `NG Setup rejected by AMF` dans le journal. Le champ de journal `amf` nomme l'entrée dans `amfs`.
2. Assurez-vous que `ip` et `port` de chaque entrée dans `amfs` sont corrects.
3. Assurez-vous que chaque AMF sert les valeurs `plmn` et `tac`.

L'UE Reçoit EAP-Failure Après le Premier Message EAP-5G

Symptômes : L'UE reçoit EAP-Failure après avoir envoyé la Demande d'Enregistrement. Le journal montre `aucun AMF ne sert le GUAMI, PLMN ou`

`tranches de l'UE`.

Causes possibles :

- Aucun AMF connecté ne sert le GUAMI, le PLMN sélectionné ou un S-NSSAI demandé de l'UE.

Résolution :

1. Comparez les champs de journal `guami`, `selected_plmn` et `requested_nssai` avec la Liste de Support PLMN de chaque AMF.
2. Assurez-vous que l'AMF pour ce cœur est dans `amfs` et que son association est active.

L'UE Rejette le Certificat N3IWF

Symptômes : L'UE s'arrête après la première réponse IKE_AUTH.

Causes possibles :

- L'UE ne fait pas confiance au certificat dans `cert_file`.
- Le FQDN du certificat n'est pas le même que `identity`.

Résolution :

1. Installez le CA racine de `cert_file` sur l'UE.
2. Assurez-vous que `identity` est le FQDN dans le certificat.

La Vérification AUTH de l'UE Échoue Après EAP-Success

Symptômes : Le journal montre `N3IWF: échec de la v��rification AUTH de l'UE`.

Causes possibles :

- L'AMF a dérivé Kn3iwf avec le mauvais discriminateur de type d'accès. Pour l'accès non-3GPP, le discriminateur est `0x02` (TS 33.501 Annexe A.9).

- L'AMF a utilisé un COUNT NAS montant qui est différent de la valeur de l'UE.

Résolution :

1. Assurez-vous que l'AMF utilise le discriminateur d'accès non-3GPP pour Kn3iwf.
2. Assurez-vous que l'AMF utilise le COUNT NAS de la connexion NAS non-3GPP.

L'Acceptation d'Enregistrement N'arrive Pas à l'UE

Symptômes : La SA IPsec est active. L'AMF envoie DownlinkNASTransport, mais l'UE ne s'enregistre pas.

Causes possibles :

- L'UE ne peut pas ouvrir la connexion TCP à `nas_ip` et `nas_tcp_port`.
- L'interface TUN NWu est inactive.

Résolution :

1. Assurez-vous que l'interface TUN `tun_name` est active et a `nas_ip`.
2. Assurez-vous qu'aucune règle de pare-feu ne bloque TCP vers `nas_tcp_port` sur l'interface TUN.

Pas de Données Utilisateur Après l'Établissement de la Session PDU

Symptômes : La session PDU est active, mais l'UE n'a pas de données.

Causes possibles :

- Le UPF ne peut pas atteindre `n3_ip` sur UDP 2152.
- Un pare-feu bloque GTP-U entre le N3IWF et le UPF.

Résolution :

1. Assurez-vous que le UPF envoie GTP-U descendant à `n3_ip`.
2. Assurez-vous que UDP 2152 est ouvert dans les deux sens.

Spécifications 3GPP

Spécification	Titre
TS 23.501	Architecture système pour le Système 5G
TS 23.502	Procédures pour le Système 5G (§4.12 : accès non-3GPP non fiable)
TS 24.502	Accès au 5GC 3GPP via des réseaux d'accès non-3GPP (EAP-5G, NWu, GRE)
TS 33.501	Architecture de sécurité et procédures pour le système 5G (§7.2.1, Annexe A.9)
TS 38.412	Transport de signalisation NG (SCTP)
TS 38.413	Protocole d'Application NG (NGAP)
TS 38.415	Protocole de plan utilisateur de session PDU
TS 29.281	GTP-U
RFC 7296	IKEv2

Exigences Réseau

Ce document couvre les ports de pare-feu et les entrées DNS nécessaires pour déployer OmniEPDG pour les appels WiFi.

Ports de Pare-feu

Ports Exposés à Internet (UE ↔ ePDG)

Ces ports doivent être ouverts à Internet pour que les appareils mobiles puissent établir des connexions d'appels WiFi.

Port	Protocole	Direction	Objectif
500	UDP	Inbound	Échange initial IKEv2 (IKE_SA_INIT, IKE_AUTH)
4500	UDP	Inbound	NAT-Traversal IKEv2 et encapsulation ESP-in-UDP

Port 500/UDP gère la négociation initiale IKEv2. Si un NAT est détecté entre l'UE et l'ePDG (ce qui est presque toujours le cas pour les appels WiFi), la connexion migre automatiquement vers le port 4500.

Port 4500/UDP transporte à la fois le signalement IKEv2 et les données utilisateur chiffrées par ESP lorsque NAT-T est actif. C'est le chemin de données principal pour tout le trafic d'appels WiFi.

Ports Réseau Internes (ePDG ↔ Noyau)

Ces ports sont utilisés pour la communication entre OmniEPDG et le réseau mobile de cœur. Ils doivent être accessibles depuis l'ePDG mais ne doivent pas être exposés à Internet.

Port	Protocole	Direction	Objectif	Pair
3868	TCP	Bidirectionnel	Diameter SWx (authentification)	HSS / DRA
3868	TCP	Bidirectionnel	Diameter S6b (autorisation de session)	PGW / AAA
2123	UDP	Bidirectionnel	Plan de contrôle GTPv2-C (S2b)	PGW
2152	UDP	Bidirectionnel	Plan utilisateur GTP-U (S2b-U)	PGW

Ports de Gestion

Ces ports sont destinés à la surveillance opérationnelle et doivent être restreints aux réseaux de gestion.

Port	Protocole	Objectif
4000	TCP	Interface web du panneau de contrôle (HTTP)
443	TCP	Interface web du panneau de contrôle (HTTPS, production)
9568	TCP	Point de terminaison des métriques Prometheus

Exigences DNS

Enregistrement DNS de Découverte ePDG

Les appareils mobiles découvrent l'ePDG en utilisant une convention de nommage DNS standardisée définie dans 3GPP TS 23.003. Le format FQDN est

:

```
epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org
```

Où :

- `<MCC>` est le code de pays mobile à 3 chiffres (par exemple, `505` pour l'Australie)
- `<MNC>` est le code de réseau mobile à 2 ou 3 chiffres, complété par des zéros à 3 chiffres (par exemple, `001`)

L'enregistrement DNS doit être un **enregistrement A** (ou AAAA pour IPv6) pointant vers l'adresse IP publique d'OmniEPDG.

```
epdg.epc.mnc999.mcc999.pub.3gppnetwork.org.  IN  A  203.0.113.10
```

Nom Commun du Certificat

Le certificat TLS de l'ePDG doit avoir un Nom Alternatif de Sujet (SAN) correspondant au FQDN de l'ePDG auquel les appareils se connecteront. Cela est validé par l'UE lors de l'authentification IKEv2.

Exigences du certificat :

- Le SAN doit inclure le FQDN de découverte de l'ePDG (par exemple, `epdg.epc.mnc001.mcc001.pub.3gppnetwork.org`)
- Le certificat doit être signé par une CA de confiance (les appareils valident la chaîne)
- RSA 2048 bits ou ECDSA P-256 minimum

DNS de Domaine Diameter

Pour un routage Diameter approprié, le domaine doit se résoudre via des enregistrements DNS NAPTR/SRV selon la RFC 6408. Le format du domaine est :

```
epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

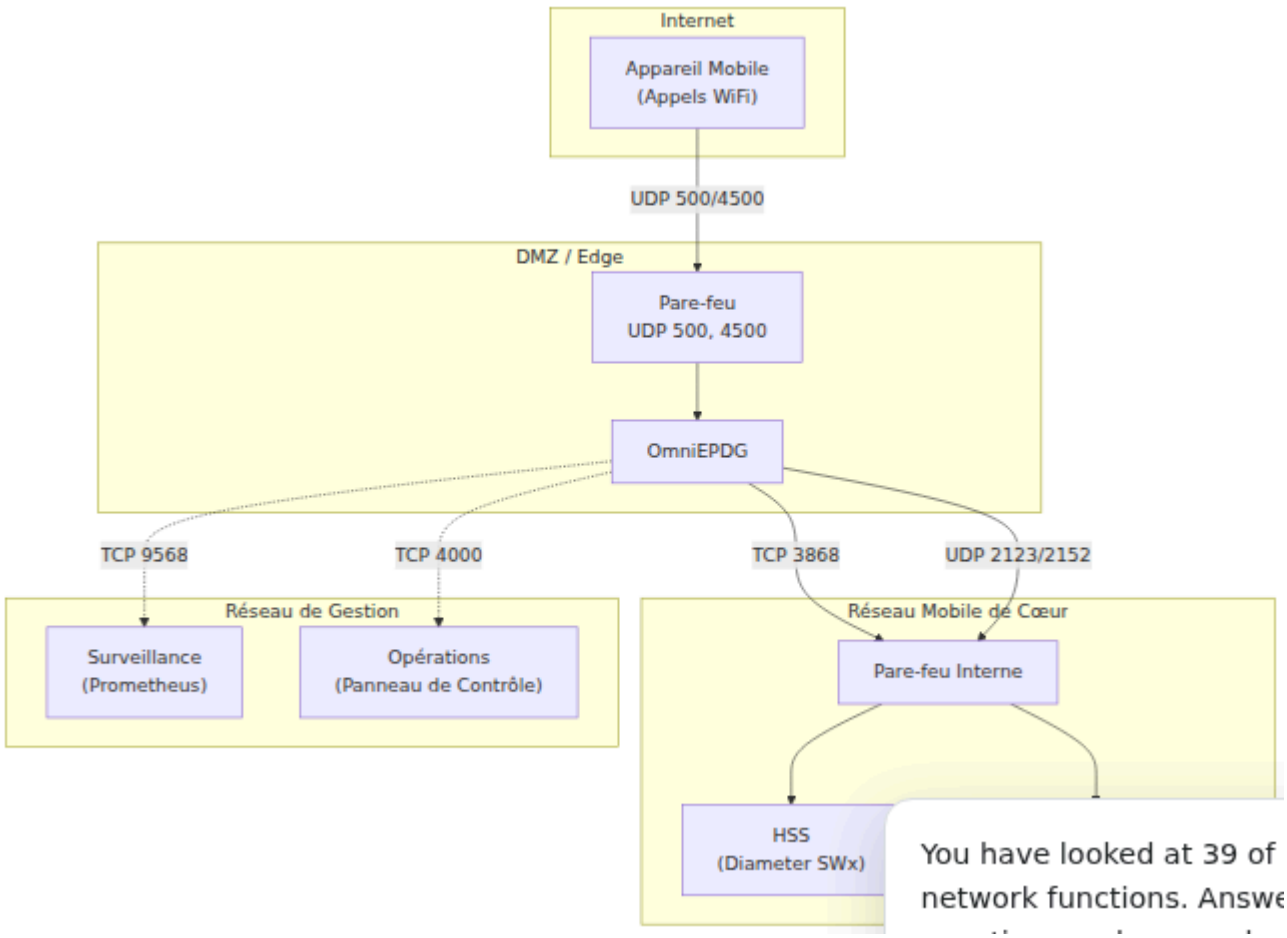
Exemple :

```
epc.mnc001.mcc001.3gppnetwork.org
```

Ce domaine est utilisé dans :

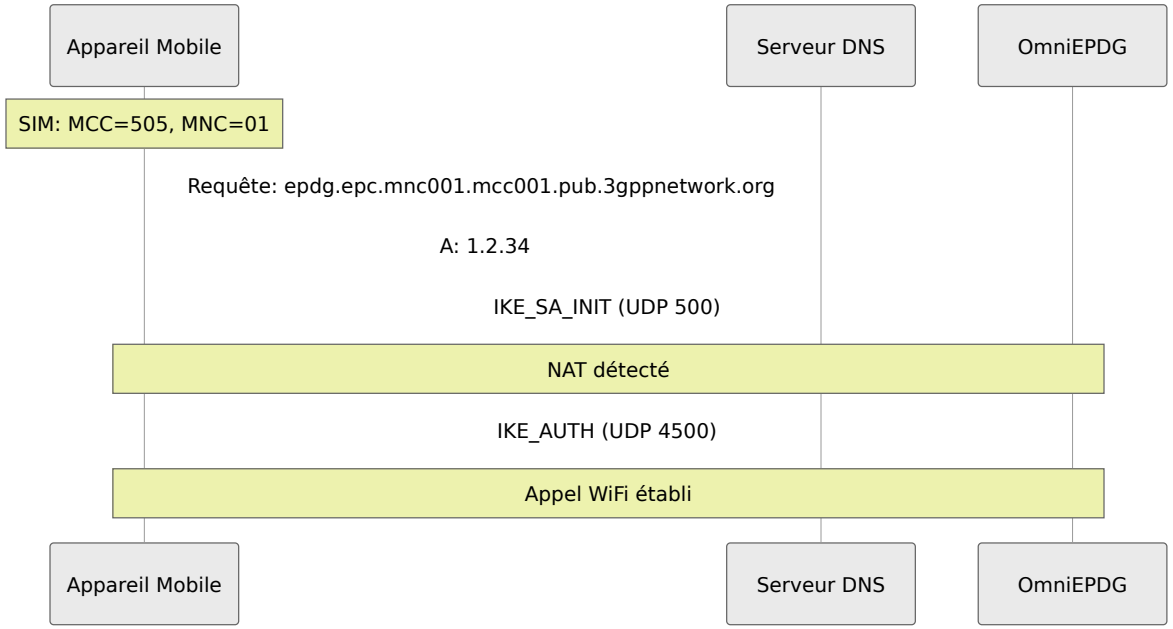
- NAI (Identifiant d'Accès Réseau) envoyé par l'UE lors de l'authentification
- AVPs Diameter Origin-Realm et Destination-Realm
- Décisions de routage Diameter

Topologie R��seau



Flux de Recherche DNS

Lorsqu'un appareil mobile initie un appel WiFi, la résolution DNS suivante se produit :



Liste de Vérification

Exigences Exposées à Internet

- [ ] UDP 500 ouvert entrant vers OmniEPDG
- [ ] UDP 4500 ouvert entrant vers OmniEPDG
- [ ] Enregistrement DNS A : `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` → IP publique de l'ePDG
- [ ] Certificat TLS avec SAN correspondant installé

Exigences du Réseau de Cœur

- [ ] TCP 3868 ouvert entre OmniEPDG et HSS/DRA
- [ ] TCP 3868 ouvert entre OmniEPDG et PGW/AAA (mode GTP uniquement)
- [ ] UDP 2123 ouvert entre OmniEPDG et PGW (mode GTP uniquement)
- [ ] UDP 2152 ouvert entre OmniEPDG et PGW (mode GTP uniquement)

Exigences de Gestion

- [ ] TCP 4000/443 accessible depuis le réseau des opérations
- [ ] TCP 9568 accessible depuis l'infrastructure de surveillance

Références

- 3GPP TS 23.003 - Numérotation, adressage et identification (format FQDN ePDG)
- 3GPP TS 23.402 - Améliorations de l'architecture pour les accès non-3GPP
- RFC 7296 - Protocole IKEv2
- RFC 3948 - Encapsulation UDP des paquets IPsec ESP (NAT-T)
- RFC 6733 - Protocole de Base Diameter

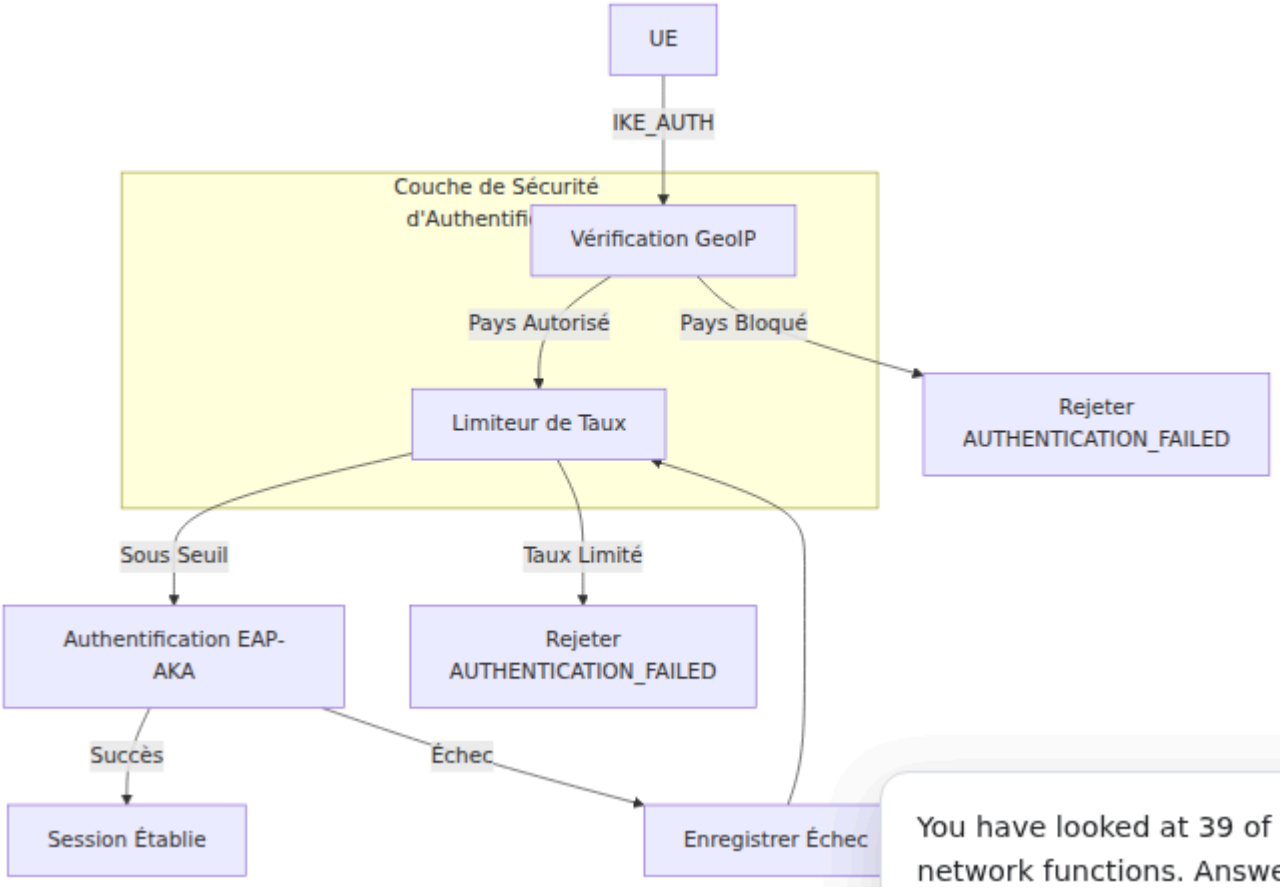
Sécurité d'Authentification OmniEPDG

OmniEPDG met en œuvre plusieurs couches de sécurité d'authentification pour se protéger contre les attaques par force brute, le credential stuffing et l'accès non autorisé depuis des régions restreintes.

Table des Matières

- Aperçu
- Limitation du Taux d'Authentification
- Blocage de Pays GeoIP
- Flux de Sécurité
- Métriques
- Dépannage

Aperçu



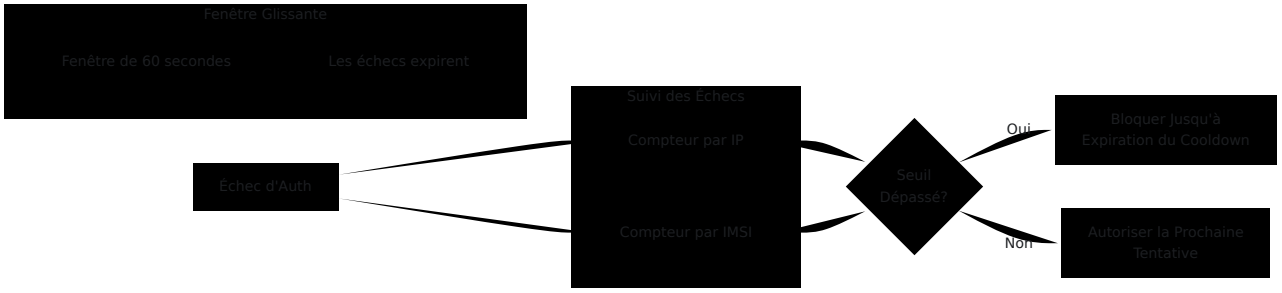
OmniEPDG effectue des vérifications de sécurité au début de l'échange IKE_AUTH, avant les opérations cryptographiques coûteuses :

1. **Vérification GeoIP** (optionnelle) - Vérifie que l'IP source provient d'un pays autorisé
2. **Vérification de Limite de Taux** - S'assure que l'IP/IMSI n'a pas dépassé les seuils d'échec
3. **Authentification EAP-AKA** - L'authentification standard 3GPP se poursuit si les vérifications réussissent

Limitation du Taux d'Authentification

La limitation de taux protège contre les attaques par force brute en suivant les tentatives d'authentification échouées par IP source et par IMSI. Lorsque les seuils sont dépassés, les tentatives ultérieures sont temporairement bloquées.

Comment Ça Marche



Le limiteur de taux utilise un **algorithme de fenêtre glissante** :

- Chaque tentative échouée est enregistrée avec un horodatage
- Les tentatives plus anciennes que la fenêtre configurée expirent automatiquement
- Lorsque les échecs dans la fenêtre dépassent le seuil, la source est bloquée
- Les blocs expirent après la période de cooldown configurée

Suivi Double

Deux limites indépendantes sont appliquées simultanément :

Type de Suivi	Objectif	Seuil par Défaut	Blocage par Défaut
Par IP	Attrape les scanners de ports et les attaques distribuées provenant de sources uniques	10 échecs / minute	5 minutes
Par IMSI	Attrape les attaques ciblées sur des abonnés spécifiques	5 échecs / minute	10 minutes

Les deux vérifications doivent réussir pour qu'une tentative d'authentification puisse se poursuivre. Si l'un ou l'autre seuil est dépassé, la tentative est rejetée.

Configuration

```
config :omniepdg,
  # Limitation de taux par IP
  auth_rate_limit_per_ip: 10,            # Max échecs avant
blocage
  auth_rate_limit_ip_window_ms: 60_000,  # Taille de la fenêtre (1
minute)
  auth_rate_limit_ip_block_ms: 300_000,  # Durée de blocage (5
minutes)

  # Limitation de taux par IMSI
  auth_rate_limit_per_imsi: 5,             # Max échecs avant
blocage
  auth_rate_limit_imsi_window_ms: 60_000,  # Taille de la fenêtre
(1 minute)
  auth_rate_limit_imsi_block_ms: 600_000   # Durée de blocage (10
minutes)
```

Paramètres par IP

Paramètre	Type	Requis	Par Défaut	Descripti
`auth_rate_limit_per_ip`	Entier	Non	`10`	Nombre maximum de tentatives d'authentific échouées autorisées d seule adress pendant la période de fenêtre avan blocage.
`auth_rate_limit_ip_window_ms`	Entier	Non	`60000`	Taille de la fenêtre gliss en millisecor pour compte échecs IP. Le échecs plus anciens que ne sont pas comptés.
`auth_rate_limit_ip_block_ms`	Entier	Non	`300000`	Durée en milliseconde pour bloquer IP après avo dépassé le s Par défaut, c 5 minutes.

Paramètres par IMSI

Paramètre	Type	Requis	Par Défaut	Descrip
`auth_rate_limit_per_imsi`	Entier	Non	`5`	Nombre maximum tentatives d'authenti échouées autorisées un seul IM pendant la période de fenêtre av blocage. P que par IP attraper le attaques c
`auth_rate_limit_imsi_window_ms`	Entier	Non	`60000`	Taille de la fenêtre gli en millisec pour comp échecs IM
`auth_rate_limit_imsi_block_ms`	Entier	Non	`600000`	Durée en millisecon pour bloqu IMSI après dépassé le Par défaut 10 minute long que l blocs IP pc protéger d

Paramètre	Type	Requis	Par Défaut	Descrip
				abonnés spécifique

Comportement en Cas de Succès

Lorsque l'authentification réussit, le limiteur de taux efface tout l'historique des échecs pour cette paire IP/IMSI. Cela permet aux utilisateurs légitimes qui ont rencontré des échecs transitoires (par exemple, des problèmes de réseau) de récupérer sans être pénalisés de manière permanente.

Exemples de Configurations

Environnement à Haute Sécurité

Limites strictes pour les environnements avec une faible tolérance aux tentatives échouées :

```
config :omniepdg,
  auth_rate_limit_per_ip: 5,
  auth_rate_limit_ip_window_ms: 120_000,   # Fenêtre de 2 minutes
  auth_rate_limit_ip_block_ms: 900_000,    # Blocage de 15 minutes

  auth_rate_limit_per_imsi: 3,
  auth_rate_limit_imsi_window_ms: 120_000,
  auth_rate_limit_imsi_block_ms: 1_800_000  # Blocage de 30
minutes
```

Comment ça fonctionne : Seules 5 échecs par IP ou 3 échecs par IMSI sont autorisés dans une fenêtre de 2 minutes. Les blocs durent respectivement 15-30 minutes.

Cas d'utilisation : Déploiements d'entreprise, bases d'abonnés à haute valeur, ou réseaux sous attaque active.

Environnement Relaxé

Limites plus permissives pour le développement ou les tests :

```
config :omniepdg,
  auth_rate_limit_per_ip: 50,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 60_000,     # Blocage de 1 minute

  auth_rate_limit_per_imsi: 20,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 120_000   # Blocage de 2 minutes
```

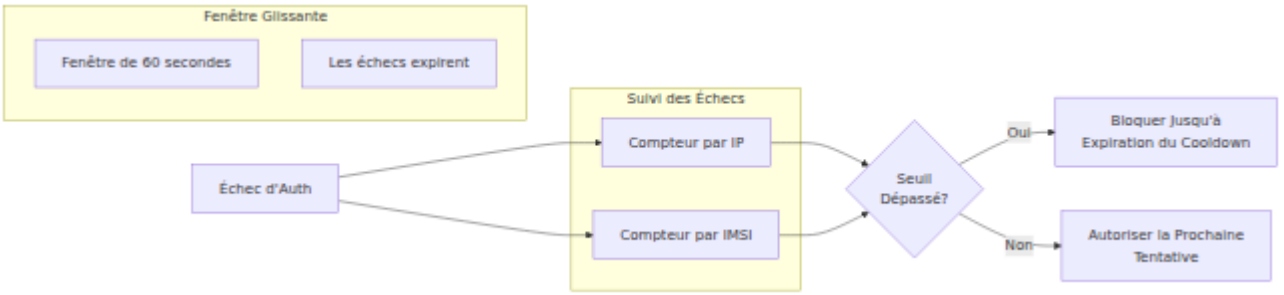
Comment ça fonctionne : Des seuils plus élevés et des blocs plus courts permettent plus de flexibilité pour les tests.

Cas d'utilisation : Environnements de développement, tests d'intégration.

Blocage de Pays GeoIP

Le blocage GeoIP restreint l'accès à l'appel WiFi en fonction de l'emplacement géographique de l'adresse IP de connexion. Cela est utile pour les opérateurs qui doivent limiter le service à des pays spécifiques pour des raisons réglementaires ou commerciales.

Aperçu



Base de Données de Géolocalisation IP

OmniEPDG utilise la base de données **DB-IP IP-to-City Lite** (CC BY 4.0. Voir `priv/geoip/ATTRIBUTION.md`). Elle n'est **pas** engagée dans git (~125 Mo). Au lieu de cela, elle est **téléchargée au moment de la construction**. `mix`

`release` exécute la tâche `geoip.fetch` comme étape de release, donc chaque package expédie une base de données actuelle. (Les environnements de développement/test la récupèrent à la demande via l'alias `mix test`.) À cause de cela :

- **Chaque session est annotée par défaut** avec le pays, la ville et les coordonnées approximatives. L'interface web ("Colonne Localisation") et la réponse `/api/sessions` montrent ces informations : `country_code`, `country_name`, `continent_code`, `geo_city`, `geo_latitude`, `geo_longitude`.
- `geoip_enabled` **contrôle uniquement** si les connexions sont *bloquées* par pays. L'annotation se produit indépendamment de ce drapeau.

Utilisation de votre propre base de données (optionnel). Définissez `geoip_database_path` sur un MaxMind GeoLite2 (`https://www.maxmind.com/en/geolite2/signup`) ou une autre DB-IP/MaxMind MMDB. Si le fichier configuré est manquant, la base de données intégrée (téléchargée) est utilisée. Remarque : L'EULA de MaxMind GeoLite2 ne permet **pas** de la redistribuer dans un produit, c'est pourquoi DB-IP Lite (CC BY 4.0) est utilisé à la place.

Pour rafraîchir la base de données manuellement (DB-IP publie mensuellement) :

```
mix geoip.fetch
```

Configuration

```
config :omniepdg,
  # Bloquer les connexions par pays (l'annotation de
géolocalisation est toujours active)
  geoip_enabled: true,

  # Optionnel : remplacer la DB intégrée par votre propre MMDB
(Pays ou Ville)
  # geoip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",

  # Mode de contrôle d'accès
  geoip_mode: :whitelist,

  # Liste des pays (codes alpha-2 ISO 3166-1)
  geoip_countries: ["AU", "NZ"],

  # Gérer les IP inconnues
  geoip_allow_unknown: false,

  # Comportement lorsque la base de données est indisponible
  geoip_fail_open: true
```

Paramètres

Paramètre	Type	Requis	Par Défaut	Description
`geoip_enabled`	Booléen	Non	`false`	Activer ou désactiver le contrôle d'accès basé sur GeoIP * (blocage). Lorsque `false`, toutes les IP sont autorisées, mais les sessions sont toujours géo-annotées.
`geoip_database_path`	Chaîne	Non	`dbip-country-lite.mmdb` intégré	Chemin vers une base de données au format MMDB (Pays ou Ville). Retombe sur la base de données DB-IP intégrée si non définie ou manquante.
`geoip_mode`	Atome	Non	`:whitelist`	Mode de contrôle d'accès : `:whitelist` (n'autoriser que les pays

Paramètre	Type	Requis	Par Défaut	Description
				listés) ou `:blacklist` (bloquer les pays listés, autoriser les autres).
`geoip_countries`	Liste	Non	`[]`	Liste des codes de pays alpha-2 ISO 3166-1. L'interprétation dépend de `geoip_mode`.
`geoip_allow_unknown`	Booléen	Non	Voir ci-dessous	Autoriser les connexions à partir d'IP qui ne peuvent pas être géolocalisées (IP privées, plages inconnues). Par défaut, c'est `false` pour le mode liste blanche, `true` pour le mode liste noire.
`geoip_fail_open`	Booléen	Non	`true`	Comportement lorsque la base de données GeoIP échoue à se charger. Lorsque `true`,

Paramètre	Type	Requis	Par Défaut	Description
				autoriser toutes les connexions (échec ouvert). Lorsque `false`, bloquer toutes les connexions (échec fermé).

Modes de Contrôle d'Accès

Mode Liste Blanche (Recommandé pour les Appels WiFi)

N'autoriser que les connexions provenant de pays spécifiés. Tous les autres pays sont bloqués.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ", "FJ"]  # Australie, Nouvelle-
Zélande, Fidji
```

Comment ça fonctionne : Seules les UE se connectant à partir d'adresses IP australiennes, néo-zélandaises ou fidjiennes peuvent s'authentifier. Tous les autres pays sont rejetés.

Cas d'utilisation : Opérateurs souhaitant restreindre les appels WiFi à leurs zones de service autorisées.

Mode Liste Noire

Bloquer les connexions provenant de pays spécifiés. Tous les autres pays sont autorisés.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :blacklist,
  geoip_countries: ["CN", "RU", "KP", "IR"]  # Chine, Russie,
Corée du Nord, Iran
```

Comment ça fonctionne : Les UE se connectant depuis les pays listés sont rejetées. Tous les autres pays peuvent s'authentifier.

Cas d'utilisation : Bloquer les régions à haut risque tout en permettant l'itinérance mondiale.

Gestion des Pays Inconnus

Certaines adresses IP ne peuvent pas être géolocalisées :

- Plages IP privées (10.x.x.x, 192.168.x.x, etc.)
- Blocs IP nouvellement alloués non encore dans la base de données
- Nœuds de sortie Tor et certains VPN

Le paramètre `geoip_allow_unknown` contrôle le comportement :

Mode	`geoip_allow_unknown` Par Défaut	Comportement
Liste Blanche	`false`	Inconnu = pas dans la liste blanche = bloqué
Liste Noire	`true`	Inconnu = pas dans la liste noire = autorisé

Pour remplacer le défaut :

```
config :omniepdg,
  geoip_mode: :whitelist,
  geoip_allow_unknown: true  # Autoriser les IP inconnues même en
mode liste blanche
```

Mises à Jour de la Base de Données

MaxMind met à jour la base de données GeoLite2 chaque semaine. Pour mettre à jour :

1. Téléchargez le nouveau fichier `GeoLite2-Country.mmdb`
2. Remplacez le fichier existant au chemin configuré
3. La base de données est automatiquement rechargée lors de la prochaine recherche (aucun redémarrage requis)

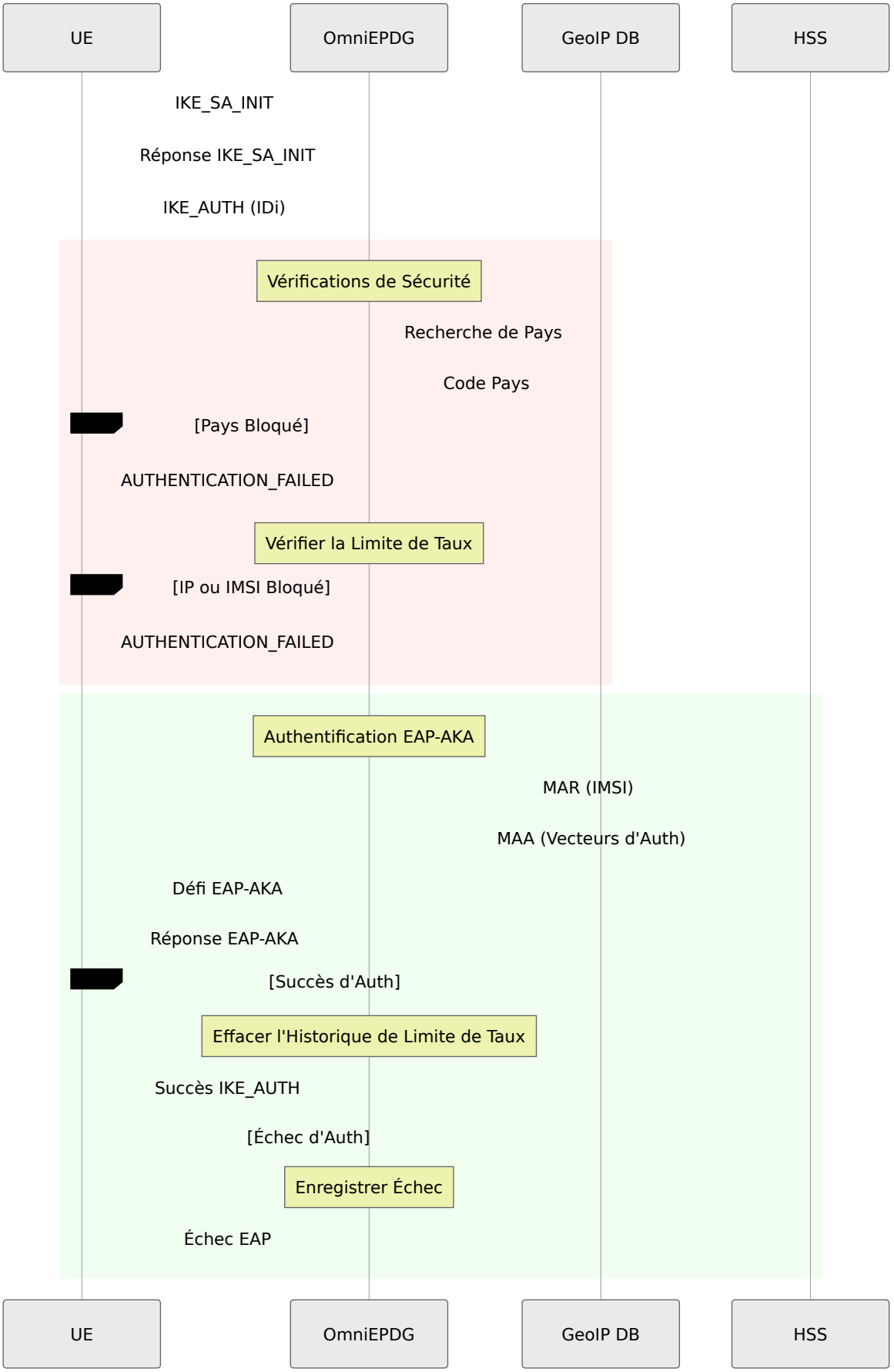
Codes de Pays Courants

Code	Pays	Code	Pays
AU	Australie	US	États-Unis
NZ	Nouvelle-Zélande	GB	Royaume-Uni
CA	Canada	DE	Allemagne
FR	France	JP	Japon
SG	Singapour	HK	Hong Kong
IN	Inde	CN	Chine

Liste complète : ISO 3166-1 alpha-2

Flux de Sécurité

Le flux complet de sécurité d'authentification :


UE
OmniEPDG
GeoIP DB
HSS
IKE_SA_INIT
Réponse IKE_SA_INIT
IKE_AUTH (IDi)
Vérifications de Sécurité
Recherche de Pays
Code Pays
[Pays Bloqué]
AUTHENTICATION_FAILED
Vérifier la Limite de Taux
[IP ou IMSI Bloqué]
AUTHENTICATION_FAILED
Authentification EAP-AKA
MAR (IMSI)
MAA (Vecteurs d'Auth)
Défi EAP-AKA
Réponse EAP-AKA
[Succès d'Auth]
Effacer l'Historique de Limite de Taux
Succès IKE_AUTH
[Échec d'Auth]
Enregistrer Échec
Échec EAP
UE
OmniEPDG
GeoIP DB
HSS

Métriques

Métriques de Limitation de Taux

Métrique: `epdg_auth_rate_limited_count` **Type**: Compteur **Description**: Nombre de tentatives d'authentification bloquées par limitation de taux **Étiquettes**:

- `type` - Raison du blocage : `ip` (seuil IP dépassé) ou `imsi` (seuil IMSI dépassé)

Exemples de requêtes :

```
# Tentatives limitées par minute
rate(epdg_auth_rate_limited_count[1m])

# Limité par type
sum by (type) (rate(epdg_auth_rate_limited_count[5m]))

# Alerte : Activité de limitation de taux élevée
rate(epdg_auth_rate_limited_count[5m]) > 10
```

Métriques GeoIP

Métrique: `epdg_auth_geoip_blocked_count` **Type**: Compteur **Description**: Nombre de tentatives d'authentification bloquées par GeoIP **Étiquettes**:

- `country` - Code de pays alpha-2 ISO 3166-1, ou `UNKNOWN` pour les IP non résolues

Exemples de requêtes :

```
# Blocs GeoIP par minute
rate(epdg_auth_geoip_blocked_count[1m])

# Pays les plus bloqués
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))

# Alerte : Pays inhabituel tentant d'accéder
increase(epdg_auth_geoip_blocked_count{country="XX"}[1h]) > 100
```

Dépannage

Problèmes de Limitation de Taux

Utilisateurs Légitimes Bloqués

Symptômes: Les utilisateurs signalent qu'ils ne peuvent pas se connecter après des tentatives échouées

Causes possibles :

- L'utilisateur a saisi de mauvaises informations d'identification plusieurs fois
- Des problèmes de réseau ont causé des délais d'authentification comptés comme des échecs
- Seuils fixés trop bas pour l'environnement

Résolution :

1. Vérifiez les métriques pour l'IP/IMSI concernée
2. Envisagez d'augmenter les seuils si les faux positifs sont fréquents
3. Après avoir corrigé la cause profonde, le bloc expirera automatiquement

Taux Élevé de Tentatives Bloquées

Symptômes: `epdg_auth_rate_limited_count` augmente rapidement

Causes possibles :

- Attaque par force brute en cours

- UE mal configurée échouant à plusieurs reprises à l'authentification
- Attaque de credential stuffing

Résolution :

1. Examinez les IP sources dans les journaux pour détecter des motifs
2. Envisagez de mettre en œuvre des règles de pare-feu au niveau IP pour les attaquants persistants
3. Vérifiez la connectivité HSS si des utilisateurs légitimes sont affectés

Problèmes GeoIP

Toutes les Connexions Sont Bloquées

Symptômes: Aucune UE ne peut se connecter après l'activation de GeoIP

Causes possibles :

- Fichier de base de données non trouvé ou corrompu
- Codes de pays incorrects dans la configuration
- `geoip_allow_unknown: false` bloquant les IP privées dans un environnement de laboratoire

Résolution :

1. Vérifiez que le fichier de base de données existe au chemin configuré
2. Vérifiez que les codes de pays sont corrects (majuscules, 2 lettres)
3. Pour le laboratoire/le développement, définissez `geoip_allow_unknown: true`
4. Vérifiez les journaux pour des avertissements liés à GeoIP

Base de Données GeoIP Ne Charge Pas

Symptômes: Avertissement dans les journaux : "Base de données GeoIP non trouvée"

Causes possibles :

- Chemin de fichier incorrect

- Les autorisations de fichier empêchent la lecture
- Le fichier n'est pas au format MMDB valide

Résolution :

1. Vérifiez que le fichier existe : `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. Vérifiez les autorisations : `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. Vérifiez l'intégrité du fichier en téléchargeant une nouvelle copie depuis MaxMind

Blocages de Pays Inattendus

Symptômes: Utilisateurs de pays autorisés étant bloqués

Causes possibles :

- VPN/proxy faisant apparaître l'IP comme provenant d'un pays différent
- Base de données GeoIP obsolète
- Sortie de réseau d'entreprise dans un emplacement inattendu

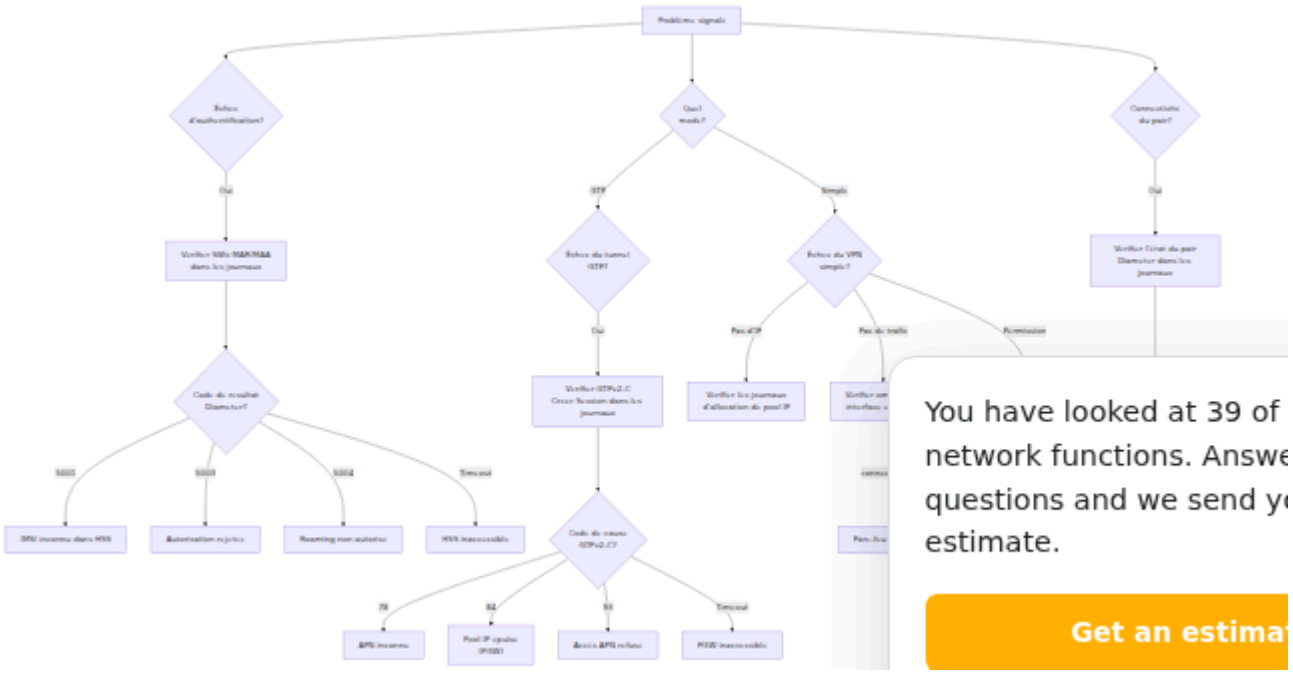
Résolution :

1. Mettez à jour la base de données GeoIP à la dernière version
2. Vérifiez l'IP de sortie réelle de l'utilisateur par rapport au pays attendu
3. Envisagez d'ajouter des pays supplémentaires si les utilisateurs passent par des réseaux d'entreprise

Dépannage OmniEPDG

Ce guide couvre les problèmes opérationnels courants, les procédures de diagnostic et les étapes de résolution pour OmniEPDG.

Aperçu du Diagnostic



Fichiers Journaux

OmniEPDG écrit des journaux dans le répertoire `log/` relatif au répertoire de travail de l'application. Voir la Référence de Configuration pour les détails de configuration des journaux.

Fichier	Objectif	Quand vérifier
`log/console.log`	Tous les messages d'application au niveau de débogage	Premier point d'investigation pour tout problème
`log/error.log`	Erreurs uniquement	Scan rapide pour les problèmes actifs
`log/crash.log`	Échecs de processus OTP	Lorsque les processus redémarrent de manière inattendue
`log/erlang.log`	Journaliseur du noyau Erlang	Problèmes Erlang/OTP de bas niveau

Modèles de Journal Clés

Événements de connexion de pair Diameter :

- `peer_up` - Pair Diameter connecté et capacités échangées
- `peer_down` - Pair Diameter déconnecté

Transitions d'état FSM UE :

- `ue_fsm state_<name> event=<event>` - FSM traitant un événement dans un état donné
- `ue_fsm init(<IMSI>)` - Nouvelle instance FSM créée pour l'abonné
- `terminating epdg_ue_fsm with reason <reason>` - FSM en cours d'arrêt

Événements de timeout :

- `Timeout swm_der_timeout` - Réponse SWm DER expirée
- `Timeout create_session_timeout` - Réponse GTPv2-C Créer Session expirée
- `Timeout s2b_delete_session_timeout` - Réponse GTPv2-C Supprimer Session expirée

- `Timeout cancel_location_timeout` - Réponse Annuler Emplacement expirée

Problèmes de Connectivité Diameter

Échec de Connexion HSS (SWx)

Symptômes : Aucun abonné ne peut s'authentifier. Les journaux montrent des tentatives de connexion répétées au HSS.

Causes possibles :

- Pare-feu bloquant le port SCTP 3868 entre OmniEPDG et HSS
- `dia_swx_remote_ip` ou `dia_swx_remote_port` incorrects dans la configuration
- HSS non opérationnel ou n'acceptant pas les connexions Diameter
- SCTP non activé sur le chemin réseau (certains pare-feu bloquent SCTP par défaut)
- Mismatch d'Origin-Host ou d'Origin-Realm causant le rejet CEA

Résolution :

1. Vérifiez la connectivité réseau vers l'IP et le port HSS
2. Confirmez que `dia_swx_remote_ip` et `dia_swx_remote_port` correspondent à la configuration HSS
3. Vérifiez que le trafic SCTP est autorisé à travers tous les pare-feu. Si SCTP est bloqué, définissez `dia_swx_proto` sur `tcp` comme solution de repli
4. Vérifiez que `dia_swx_origin_host` est un FQDN résolvable et correspond à ce que le HSS attend
5. Vérifiez les journaux HSS pour les échecs de négociation Diameter CER/CEA

Échec de Connexion PGW (S6b)

Symptômes : L'authentification réussit mais la création du tunnel GTP échoue ou S6b AAR n'arrive jamais du PGW. Les journaux ne montrent aucun événement peer_up S6b.

Causes possibles :

- PGW non configuré pour se connecter à l'écouteur S6b d'OmniEPDG
- Pare-feu bloquant le port SCTP 3868 sur l'adresse de liaison S6b d'OmniEPDG
- `dia_s6b_local_ip` non accessible depuis le PGW
- Mismatch d'Origin-Host ou d'Origin-Realm

Résolution :

1. Confirmez que le PGW est configuré pour se connecter à OmniEPDG à `dia_s6b_local_ip`:`dia_s6b_local_port`
2. Vérifiez que l'adresse de liaison S6b est accessible depuis le réseau PGW
3. Vérifiez que les règles de pare-feu autorisent le SCTP entrant sur le port 3868 à l'adresse S6b
4. Vérifiez que `dia_s6b_origin_host` et `dia_s6b_origin_realm` correspondent à ce que le PGW attend

Échecs de Watchdog Diameter

Symptômes : Les connexions Diameter établies se déconnectent de manière intermittente. Les journaux montrent des transitions de watchdog vers l'état SUSPECT ou DOWN.

Causes possibles :

- Instabilité du chemin réseau ou perte de paquets
- Pair surchargé et ne répondant pas au DWR dans `dia_swx_watchdog_timer`
- Configuration de watchdog agressive (trop peu de tentatives avant de déclarer suspect)

Résolution :

1. Vérifiez la qualité du chemin réseau (perte de paquets, latence) entre OmniEPDG et le pair
2. Si une perte de paquets est attendue, augmentez les seuils de `dia_swx_watchdog_config` / `dia_s6b_watchdog_config` (par exemple, `[{okay, 5}, {suspect, 3}]`)
3. Vérifiez la santé du système pair (CPU, mémoire, nombre de connexions)

Échecs de Négociation IKEv2

Aucune Proposition Choisie

Symptômes : L'IKE_SA_INIT de l'UE est rejeté avec `NO_PROPOSAL_CHOSEN` ; les journaux montrent `exchange error: :no_proposal_chosen`. L'UE ne passe jamais l'étape IKE_SA_INIT.

Causes possibles :

- L'UE n'offre que des transformations cryptographiques que OmniEPDG ne prend pas en charge.
- Un scanner ou un client mal configuré sonde les ports publics.

Contexte : OmniEPDG accepte le chiffrement AES-CBC et AES-GCM ; HMAC-SHA2, HMAC-SHA1 et **AES-XCBC-96** pour l'intégrité ; HMAC-SHA2, HMAC-SHA1 et **PRF-AES128-XCBC** pour les PRF ; et les groupes DH MODP/ECP/Curve25519/448. Voir Algorithmes Cryptographiques pour la liste complète. Certains téléphones (notamment certains clients Samsung VoWiFi) n'offrent que `AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048`, tous pris en charge.

Résolution :

1. Activez la journalisation `:debug` et inspectez l'événement `IKEv2 packet` pour la charge utile SA de l'UE. Les champs `payloads[].proposals[]` listent les transformations exactes offertes.
2. Confirmez que les transformations de chiffrement / d'intégrité / de PRF / de DH offertes apparaissent comme prises en charge dans les tableaux d'algorithmes.

3. Si une transformation réellement non prise en charge est requise, signalez-le à l'ingénierie.

La Connexion S'établit Puis Se Déconnecte Immédiatement (SA Enfant Supprimée)

Symptômes : IKE_AUTH se termine, la session est brièvement établie, puis l'UE envoie un `DELETE` d'INFORMATIONNEL dans ~100 ms. Aucun flux multimédia. Se répète à chaque tentative.

Causes possibles :

- Les transformations SA Enfant (ESP) dans la réponse ne correspondent pas à ce que l'UE a offert, donc l'UE détruit la SA.
- Un algorithme d'intégrité/chiffrement ESP que le plan de données ne peut pas traiter.

Contexte : OmniEPDG négocie la SA Enfant ESP à partir de la proposition offerte par l'UE (y compris AES-XCBC-96 et AES-CBC-128/192/256) plutôt que de forcer un ensemble fixe. Une réponse sélectionnant une transformation que l'UE n'a pas offerte est rejetée selon la RFC 7296.

Résolution :

1. Dans `:debug`, vérifiez la ligne de journal `child SA proposal selected`. Les champs `esp_offered`, `esp_encr` et `esp_integ` montrent ce qui a été offert et choisi.
2. Vérifiez que la longueur de la clé de chiffrement ESP sélectionnée correspond au chiffre (un mismatch se manifeste comme `Bad key size` et un paquet abandonné).
3. Confirmez que l'intégrité ESP offerte par l'UE est prise en charge par OmniEPDG (voir Algorithmes SA Enfant ESP).

Échecs d'Authentification

IMSI Inconnu (Diameter 5001)

Symptômes : Des abonnés spécifiques échouent à l'authentification EAP-AKA. Les journaux montrent SWx MAA avec le code de résultat 5001 (DIAMETER_ERROR_USER_UNKNOWN).

Causes possibles :

- Abonné non provisionné dans le HSS
- Mismatch d'IMSI entre la SIM de l'UE et la base de données HSS
- Format NAI incorrect, causant l'échec de l'extraction de l'IMSI

Résolution :

1. Vérifiez que l'IMSI de l'abonné existe dans la base de données HSS
2. Vérifiez que le format NAI dans les journaux correspond au modèle attendu : `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`
3. Confirmez que l'IMSI de la carte SIM correspond à la valeur provisionnée dans le HSS

Autorisation Rejetée (Diameter 5003)

Symptômes : L'abonné s'authentifie mais est rejeté lors de l'attribution du serveur. Les journaux montrent SWx SAA avec le code de résultat 5003.

Causes possibles :

- Abonné non autorisé pour le service d'appel WiFi
- APN non autorisé pour cet abonné
- Restrictions du profil d'abonnement

Résolution :

1. Vérifiez le profil de service de l'abonné dans le HSS
2. Vérifiez que l'accès WiFi / ePDG est activé pour l'abonné

3. Confirmez que l'APN demandé figure dans la liste des APN autorisés de l'abonné

Roaming Non Autorisé (Diameter 5004)

Symptômes : Les abonnés en roaming échouent à l'authentification. Les journaux montrent SWx MAA ou SAA avec le code de résultat 5004.

Causes possibles :

- La politique de roaming HSS rejette la localisation actuelle de l'abonné
- Appel WiFi non autorisé pour les abonnés en roaming

Résolution :

1. Examinez les politiques de roaming HSS pour la combinaison HPLMN/VPLMN de l'abonné
2. Vérifiez si l'appel WiFi est autorisé dans le cadre des accords de roaming

Timeout d'Authentification

Symptômes : L'authentification reste bloquée puis échoue après 10 secondes. Les journaux montrent `Timeout swm_der_timeout` dans `state_wait_auth_resp`.

Causes possibles :

- HSS ne répond pas à SWx MAR dans les 10 secondes
- Connexion Diameter SWx interrompue pendant la demande
- HSS surchargé

Résolution :

1. Vérifiez la réactivité et la charge du HSS
2. Vérifiez que le pair Diameter SWx est dans un état OKAY (pas SUSPECT ou DOWN)
3. Vérifiez que `dia_swx_transmit_timer` est adéquat pour la latence réseau vers le HSS

Mismatch de Type EAP-AKA

Symptômes : L'authentification échoue avec une erreur "type_mismatch" dans les journaux. Le préfixe d'identité de l'UE ne correspond pas à la méthode EAP utilisée.

Causes possibles :

- L'UE envoie une identité avec le préfixe `0` (EAP-AKA) mais le réseau attend EAP-AKA', ou vice versa
- HSS renvoie des vecteurs d'authentification pour le mauvais type EAP

Contexte : Selon 3GPP TS 23.003, le préfixe d'identité NAI indique le type d'authentification attendu :

- Le préfixe `0` indique EAP-AKA
- Le préfixe `6` indique EAP-AKA'

OmniEPDG sélectionne automatiquement la méthode d'authentification en fonction du préfixe d'identité de l'UE. La plupart des UEs d'appel WiFi utilisent le préfixe `0` (EAP-AKA).

Résolution :

1. Vérifiez l'identité NAI de l'UE dans les journaux pour vérifier le préfixe
2. Assurez-vous que le HSS est configuré pour renvoyer des vecteurs d'authentification appropriés
3. Vérifiez que la carte SIM est correctement provisionnée pour le type d'authentification attendu

Mismatch de RES EAP-AKA

Symptômes : L'authentification échoue après challenge/réponse. Les journaux montrent une erreur "RES mismatch" ou "res_mismatch".

Causes possibles :

- Échec d'authentification de la carte SIM
- Mismatch de dérivation de clé entre l'UE et le réseau

- Vecteurs d'authentification corrompus provenant du HSS

Résolution :

1. Vérifiez que la carte SIM est valide et non endommagée
2. Vérifiez que le HSS a renvoyé des vecteurs d'authentification valides (RAND, AUTN, XRES, CK, IK)
3. Activez la journalisation de débogage pour comparer le XRES attendu avec le RES reçu
4. Si vous utilisez des SIM de test, vérifiez que les valeurs Ki et OP/OPc correspondent entre la SIM et le HSS

Échecs de Tunnel GTP (Mode GTP Seulement)

Création de Session Rejetée par PGW

Symptômes : L'authentification réussit mais la création du tunnel échoue. Les journaux montrent une réponse de création de session GTPv2-C avec un code d'erreur.

Codes de cause courants et actions :

Code de Cause	Nom	Action
78	APN manquant ou inconnu	Vérifiez que l'APN est configuré sur le PGW et correspond au profil de l'abonné
82	Refusé dans RAT	Vérifiez que la politique PGW permet l'accès WiFi (type non-3GPP)
84	Tous les Adresses Dynamiques Occupées	Pool IP du PGW épuisé ; étendre le pool ou enquêter sur les fuites
92	Échec d'Authentification de l'Utilisateur	Échec d'authentification côté PGW ; vérifiez l'autorisation de session S6b
93	Accès APN Refusé	Abonné non autorisé pour l'APN sur PGW
96	IMSI/IMEI Inconnu	Abonné inconnu du PGW ; vérifiez que la session S6b a été autorisée
113	Congestion APN	APN surchargé ; réessayez ou enquêtez sur la capacité du PGW
120	Congestion de l'Entité GTP-C	Plan de contrôle PGW surchargé

Timeout de Création de Session

Symptômes : La création du tunnel reste bloquée pendant 10 secondes puis échoue. Les journaux montrent `Timeout create_session_timeout` dans `state_wait_create_session_resp`.

Causes possibles :

- PGW inaccessible à `gtpc_remote_ip`:`gtpc_remote_port`
- Pare-feu bloquant le port UDP 2123 entre OmniEPDG et PGW
- PGW surchargé et ne répond pas aux demandes GTPv2-C

Résolution :

1. Vérifiez la connectivité réseau vers le PGW sur le port UDP 2123
2. Vérifiez que les règles de pare-feu autorisent UDP 2123 entre OmniEPDG et PGW
3. Vérifiez la santé du PGW et la capacité de traitement GTPv2-C

Tunnel GTP-U Ne Transmet Pas de Trafic

Symptômes : Le tunnel est établi (la création de session réussit) mais le trafic de l'abonné ne circule pas.

Causes possibles :

- Module noyau GTP-U non chargé
- L'adresse IP du socket `gtp_u_kmod` ne correspond pas à l'adresse de point de terminaison du tunnel GTP-U signalée au PGW
- Routage non configuré pour le dispositif de tunnel GTP
- Pare-feu bloquant le port UDP 2152 (GTP-U)

Résolution :

1. Vérifiez que le module GTP du noyau Linux est chargé (`lsmod | grep gtp`)
2. Confirmez que le dispositif de tunnel GTP existe (`ip link show gtp0`)
3. Vérifiez que `gtp_u_kmod` `ip` correspond à `gtpc_local_ip` ou à l'adresse signalée dans la demande de création de session
4. Vérifiez que la table de routage inclut des routes via le dispositif de tunnel GTP
5. Vérifiez que le pare-feu autorise le port UDP 2152 entre OmniEPDG et PGW

Échecs de VPN Simple (Mode VPN Simple Seulement)

Interface TUN Non Créée

Symptômes : OmniEPDG démarre mais aucune interface `omniepdg0` n'apparaît. Les sessions échouent lors de la configuration du tunnel. Les journaux peuvent montrer des erreurs de `simple_vpn_route` lors du démarrage.

Causes possibles :

- Le processus OmniEPDG n'a pas la capacité `CAP_NET_ADMIN` ou ne s'exécute pas en tant que root
- Le module noyau TUN/TAP n'est pas chargé
- Un autre processus a déjà créé une interface nommée `omniepdg0`

Résolution :

1. Vérifiez que le module noyau TUN est disponible (`lsmod | grep tun`)
2. Confirmez qu'OmniEPDG s'exécute avec des privilèges suffisants pour créer des interfaces TUN
3. Vérifiez si `omniepdg0` existe déjà à partir d'une instance précédente (`ip link show omniepdg0`)
4. Vérifiez `log/crash.log` pour les erreurs du processus de gestion des routes

Pool IP Épuisé

Symptômes : L'authentification réussit mais la configuration du tunnel échoue. Les journaux montrent un échec d'allocation IP de `simple_vpn_pool`.

Causes possibles :

- Toutes les adresses dans le pool CIDR configuré sont allouées à des sessions actives
- Les adresses IP ne sont pas libérées après la terminaison de la session (fuite)

- Taille du pool trop petite pour le nombre d'abonnés concurrents

Résolution :

1. Vérifiez le nombre de processus `epdg_ue_fsm` actifs par rapport à la taille du pool
2. Vérifiez que les sessions sont correctement terminées (vérifiez les messages de journal `terminating`)
3. Si le pool est réellement plein, étendez-le en utilisant un préfixe CIDR plus grand dans `simple_vpn_pool_ipv4` (nécessite un redémarrage)
4. Vérifiez les plantages de FSM pendant la terminaison dans `log/crash.log` qui ont pu empêcher la libération d'IP

Trafic d'Abonné Ne Circulant Pas

Symptômes : La session est établie et l'UE reçoit une adresse IP, mais le trafic ne circule pas à travers l'interface TUN.

Causes possibles :

- Route hôte non ajoutée pour l'IP de l'abonné sur `omniepdg0`
- Le transfert IP n'est pas activé sur l'hôte OmniEPDG
- Règles de pare-feu bloquant le trafic sur l'interface `omniepdg0`
- Règles NAT/masquerade manquantes pour le trafic sortant de la plage d'IP de l'abonné

Résolution :

1. Vérifiez que la route hôte existe (`ip route show` et recherchez la route /32 de l'abonné via `omniepdg0`)
2. Confirmez que le transfert IP est activé (`sysctl net.ipv4.ip_forward`)
3. Vérifiez que les règles iptables/nftables autorisent le transfert via `omniepdg0`
4. Si les abonnés ont besoin d'un accès Internet, vérifiez que NAT/masquerade est configuré pour la plage d'IP de l'abonné (par exemple, `iptables -t nat -A POSTROUTING -s 10.45.0.0/16 -o <wan-interface> -j MASQUERADE`)

Routes Obsolètes Après Crash

Symptômes : Les routes hôtes pour les IP d'abonnés restent dans la table de routage après que OmniEPDG redémarre ou après que les sessions se terminent de manière anormale.

Causes possibles :

- FSM a planté avant que la route puisse être supprimée
- Le processus OmniEPDG a été tué sans arrêt gracieux

Résolution :

1. Vérifiez `log/crash.log` pour les plantages de processus pendant la terminaison
2. Supprimez manuellement les routes obsolètes (`ip route del <subscriber-ip>/32 dev omniepdg0`)
3. Le redémarrage d'OmniEPDG recréera l'interface `omniepdg0`, ce qui supprimera toutes les routes associées

Problèmes de Terminaison de Session

La Terminaison Reste Bloquée Pendant la Désinscription

Symptômes : La terminaison de session ne se termine pas. FSM UE bloqué dans un état `dereg_*` ou `wait_*`.

Causes possibles :

- PGW ne répond pas à la Demande de Suppression de Session
- Pair Diameter ne répond pas à STR ou ASR
- Cascade de timeout non terminée en raison de plusieurs timeouts empilés

Résolution :

1. Vérifiez les journaux pour les messages de timeout dans l'état pertinent
2. Vérifiez la connectivité PGW et HSS
3. Après 10 secondes, la FSM devrait expirer et passer à l'étape suivante de terminaison ou se terminer. Si ce n'est pas le cas, vérifiez les événements inattendus enregistrés comme `Unexpected call event`

Contextes PDP GTP-U Orphelins

Symptômes : Les entrées de tunnel GTP-U restent dans le noyau après la terminaison des sessions. `ip link show gtp0` montre que le dispositif a toujours des contextes PDP actifs.

Causes possibles :

- FSM terminée anormalement avant de supprimer le contexte PDP
- Plantage pendant la séquence de terminaison

Résolution :

1. Vérifiez `log/crash.log` pour les plantages de processus pendant la terminaison
2. Le rappel `terminate/3` de la FSM tente de nettoyer le contexte PDP. Si la FSM a été tuée (par exemple, redémarrage du superviseur), le nettoyage a pu être sauté
3. Le redémarrage d'OmniEPDG recréera le socket GTP-U et effacera les contextes obsolètes

Problèmes de Processus et Système

Boucles de Redémarrage du Superviseur

Symptômes : Les processus OmniEPDG redémarrent de manière répétée. Les journaux montrent des messages de redémarrage du superviseur et des rapports de plantage.

Causes possibles :

- Erreur de configuration persistante provoquant un plantage d'un gestionnaire au démarrage
- Dépendance externe indisponible (par exemple, bibliothèque gen_socket introuvable)
- Pair Diameter envoyant des messages malformés provoquant des plantages de gestionnaire

Résolution :

1. Vérifiez `log/crash.log` pour la cause profonde du plantage
2. Vérifiez que le chemin `libdir` de `gen_socket` est correct et que les fichiers de bibliothèque existent
3. Vérifiez que tous les paramètres de configuration requis sont présents dans `config/runtime.exs`
4. Recherchez des messages Diameter malformés dans le rapport de plantage

Utilisation Élevée de la Mémoire

Symptômes : La consommation de mémoire de la VM Erlang augmente avec le temps.

Causes possibles :

- Les processus FSM UE ne sont pas nettoyés après la terminaison de la session
- Accumulation de messages de journal dans les boîtes aux lettres
- Grand nombre de sessions concurrentes

Résolution :

1. Vérifiez le nombre de processus `epdg_ue_fsm` et `aaa_ue_fsm` en cours d'exécution (ceux-ci devraient correspondre au nombre d'abonnés actifs)
2. Vérifiez que les FSM se terminent correctement après la terminaison de la session (vérifiez les messages de journal `terminating`)
3. Examinez les paramètres de rotation des journaux pour vous assurer que les fichiers journaux sont en cours de rotation

Webhooks OmniEPDG

OmniEPDG peut envoyer des webhooks sortants pour les événements du cycle de vie des sessions des abonnés. Lorsqu'un abonné se connecte ou se déconnecte, OmniEPDG envoie un `POST` HTTP avec un corps JSON à chaque point de terminaison configuré. Utilisez les webhooks pour alimenter un système de facturation, un service de présence ou un pipeline d'analytique en temps quasi réel.

Les webhooks sont désactivés par défaut. Consultez Configuration des Webhooks pour les paramètres de configuration.

Table des Matières

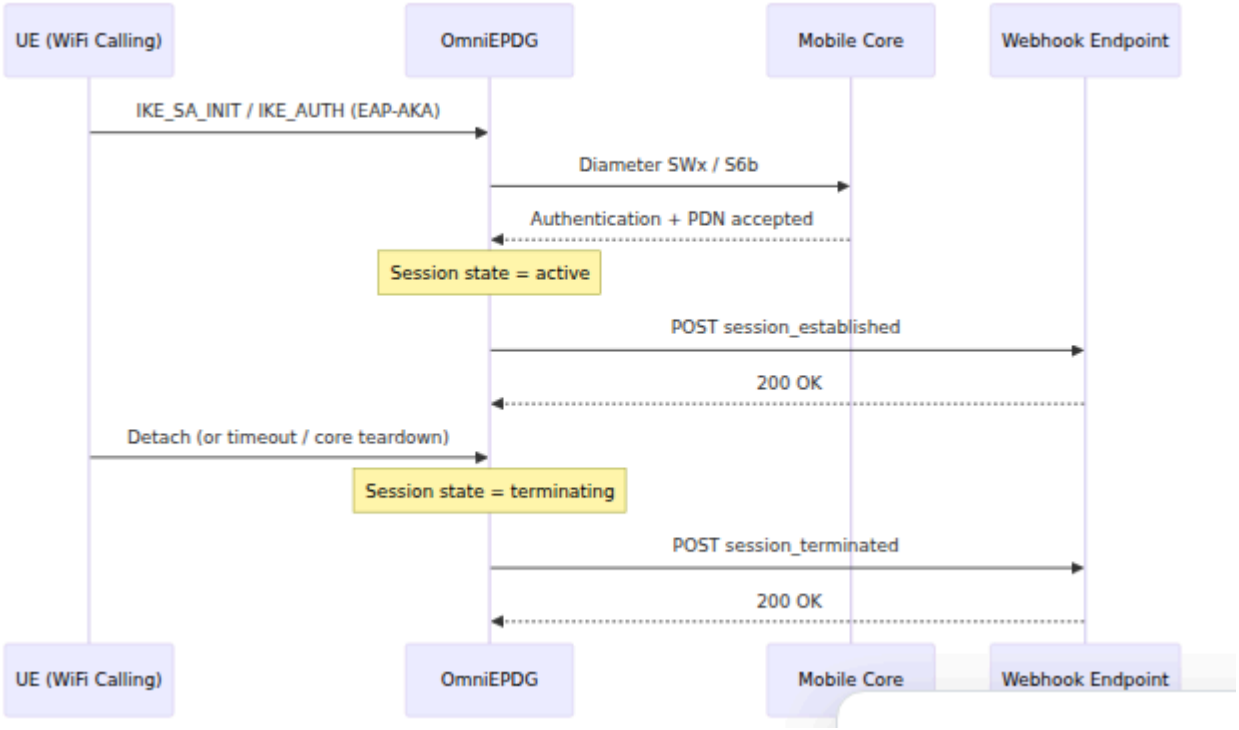
- Aperçu
- Événements
- Modèle de Livraison
- Schéma de Charge Utile
- Exemples de Charges Utiles
- Exigences du Récepteur
- Dépannage

Aperçu

OmniEPDG suit chaque session d'abonné avec une machine à états. Deux transitions produisent un webhook :

- La session atteint l'état `active` après une connexion réussie.
- La session atteint l'état `terminating` après une déconnexion.

Le diagramme suivant montre où chaque webhook est envoyé dans le cycle de vie de la session.



Événements

Événement	Déclencheur	Description
`session_established`	Connexion réussie	OmniEPDG envoie cet événement lorsque l'abonné s'authentifie et que la connexion PDN est établie. La session est prête à transporter du trafic.
`session_terminated`	Déconnexion	OmniEPDG envoie cet événement lorsqu'une session établie est interrompue. La cause est une déconnexion de l'UE, un délai d'inactivité ou une interruption initiée par le cœur.

OmniEPDG envoie `session_terminated` uniquement pour les sessions qui ont atteint l'état `active`. Une connexion qui échoue avant que la connexion PDN ne soit établie ne produit pas de webhook.

Définissez le paramètre de configuration `events` pour contrôler quels événements OmniEPDG envoie. Consultez Configuration des Webhooks.

Modèle de Livraison

OmniEPDG livre les webhooks avec un modèle de type "fire-and-forget". Chaque livraison s'exécute sur une tâche de fond supervisée. La livraison ne bloque ni ne retarde la machine à états de la session, et un point de terminaison lent ou indisponible n'affecte pas le traitement des appels.

Notez les propriétés de livraison suivantes :

- OmniEPDG envoie un `POST` par point de terminaison configuré, par événement.
- OmniEPDG ne réessaie pas une livraison échouée. Une livraison échouée est enregistrée et abandonnée.
- OmniEPDG ne garantit pas l'ordre des événements entre les deux événements. Concevez le récepteur pour gérer les événements par leur champ `timestamp`.
- OmniEPDG accepte toute réponse HTTP `2x` comme succès. Il enregistre un avertissement pour une erreur de connexion ou une réponse non `2xx`.
- OmniEPDG ne valide pas le certificat TLS d'un point de terminaison `https`. Utilisez un chemin réseau de confiance vers le récepteur.

Schéma de Charge Utile

Chaque corps de webhook est un objet JSON avec les champs suivants.

Champ	Type	Description
`event`	String	Le nom de l'événement : `session_established` ou `session_terminated`.
`timestamp`	String	L'heure de l'événement au format ISO 8601 (UTC).
`session_id`	String	L'identifiant de session interne d'OmniEPDG.
`imsi`	String	L'IMSI de l'abonné.
`apn`	String ou null	Le nom du point d'accès pour la connexion PDN.
`pdn_type`	String	Le type de PDN : `ipv4`, `ipv6`, ou `ipv4v6`.
`ue_ipv4`	String ou null	L'adresse IPv4 attribuée à l'UE.
`ue_ipv6`	String ou null	L'adresse IPv6 attribuée à l'UE.
`peer_ip`	String ou null	L'adresse IP publique de l'UE (le point d'accès WiFi).
`geoip`	Object ou null	La géolocalisation de `peer_ip`. Consultez Objet GeoIP. Il est `null` lorsque l'adresse ne peut pas être localisée.
`handover`	Boolean	`true` si la session a été créée comme un transfert LTE vers WiFi.
`bytes_in`	Integer	Le nombre de bytes uplink pour la session au moment de l'événement.

Champ	Type	Description
`bytes_out`	Integer	Le nombre de bytes downlink pour la session au moment de l'événement.
`metadata`	Object	Un objet avec un contexte d'événement supplémentaire. Il est vide pour la plupart des événements.

Les champs `bytes_in` et `bytes_out` sont `0` pour un événement `session_established`, car aucun trafic n'a encore été transmis.

Objet GeoIP

OmniEPDG annote chaque session avec la géolocalisation de l'IP publique de l'UE au moment de la connexion. L'annotation utilise la base de données DB-IP intégrée, et cela se produit indépendamment de l'activation du contrôle d'accès GeoIP. Le champ `geoip` porte cette annotation. Les champs `city`, `latitude` et `longitude` ne sont présents qu'avec une base de données de niveau Ville.

Champ	Type	Description
`country_code`	String ou null	Le code de pays ISO 3166-1 alpha-2 (par exemple `AU`).
`country_name`	String ou null	Le nom du pays.
`continent_code`	String ou null	Le code de continent à deux lettres (par exemple `OC`).
`city`	String ou null	Le nom de la ville. Présent uniquement avec une base de données de niveau Ville.
`latitude`	Number ou null	La latitude approximative. Présent uniquement avec une base de données de niveau Ville.
`longitude`	Number ou null	La longitude approximative. Présent uniquement avec une base de données de niveau Ville.

Exemples de Charges Utiles

session_established


```
{
  "event": "session_established",
  "timestamp": "2026-08-30T02:15:44.123456Z",
  "session_id": "a1b2c3d4-...",
  "imsi": "001010000000001",
  "apn": "ims",
  "pdn_type": "ipv4v6",
  "ue_ipv4": "100.64.32.5",
  "ue_ipv6": null,
  "peer_ip": "203.0.113.9",
  "geoip": {
    "country_code": "AU",
    "country_name": "Australia",
    "continent_code": "OC",
    "city": "Sydney",
    "latitude": -33.8688,
    "longitude": 151.2093
  },
  "handover": false,
  "bytes_in": 0,
  "bytes_out": 0,
  "metadata": {}
}
```

session_terminated


```
{
  "event": "session_terminated",
  "timestamp": "2026-08-30T03:42:10.998877Z",
  "session_id": "a1b2c3d4-...",
  "imsi": "001010000000001",
  "apn": "ims",
  "pdn_type": "ipv4v6",
  "ue_ipv4": "100.64.32.5",
  "ue_ipv6": null,
  "peer_ip": "203.0.113.9",
  "geoip": {
    "country_code": "AU",
    "country_name": "Australia",
    "continent_code": "OC",
    "city": "Sydney",
    "latitude": -33.8688,
    "longitude": 151.2093
  },
  "handover": false,
  "bytes_in": 154238,
  "bytes_out": 892011,
  "metadata": {}
}
```


Exigences du Récepteur

Construisez le récepteur de webhook pour répondre à ces exigences :

- Accepter un `POST` HTTP avec un corps `Content-Type: application/json`.
- Retourner une réponse `2xx` dès que vous acceptez l'événement. Ne maintenez pas la connexion ouverte pour le traitement en aval.
- Associer les événements aux sessions avec le champ `session_id`.
- Gérer un événement dupliqué. Une condition réseau peut amener OmniEPDG à envoyer le même événement plus d'une fois.
- Ordonner les événements par le champ `timestamp`, et non par l'ordre d'arrivée.

Dépannage

Aucun webhook n'arrive

Symptômes : Le récepteur ne reçoit aucune demande après une connexion ou une déconnexion.

Causes possibles :

- Les webhooks sont désactivés (`enabled: false`).
- L'événement n'est pas dans la liste `events`.
- L'URL du point de terminaison est incorrecte ou inaccessible depuis l'hôte OmniEPDG.
- Un pare-feu bloque la connexion sortante vers le point de terminaison.

Résolution :

1. Confirmez `enabled: true` dans la configuration des webhooks.
2. Confirmez que le nom de l'événement est dans la liste `events`.
3. Confirmez que l'URL du point de terminaison est correcte et accessible depuis l'hôte OmniEPDG.
4. Vérifiez les journaux d'OmniEPDG pour un avertissement de livraison de webhook.

Seul session_established arrive, pas session_terminated

Symptômes : Le récepteur reçoit des événements de connexion mais aucun événement de déconnexion.

Causes possibles :

- `session_terminated` n'est pas dans la liste `events`.
- Les sessions n'ont jamais atteint l'état `active`, donc aucun événement de déconnexion n'était dû.

Résolution :

1. Ajoutez `:session_terminated` à la liste `events`.
2. Confirmez que les sessions complètent une connexion réussie avant de se terminer.

Les livraisons sont enregistrées comme échouées

Symptômes : Les journaux d'OmniEPDG montrent un avertissement de livraison de webhook.

Causes possibles :

- Le récepteur retourne une réponse non `2xx`.
- Le récepteur est lent ou indisponible.
- L'URL du point de terminaison utilise un hôte qui ne se résout pas.

Résolution :

1. Confirmez que le récepteur retourne une réponse `2xx`.
2. Confirmez que le récepteur répond rapidement, car OmniEPDG ne réessaie pas.
3. Confirmez que l'hôte du point de terminaison se résout depuis l'hôte OmniEPDG.