Architecture et Flux d'Appels OmniEPDG

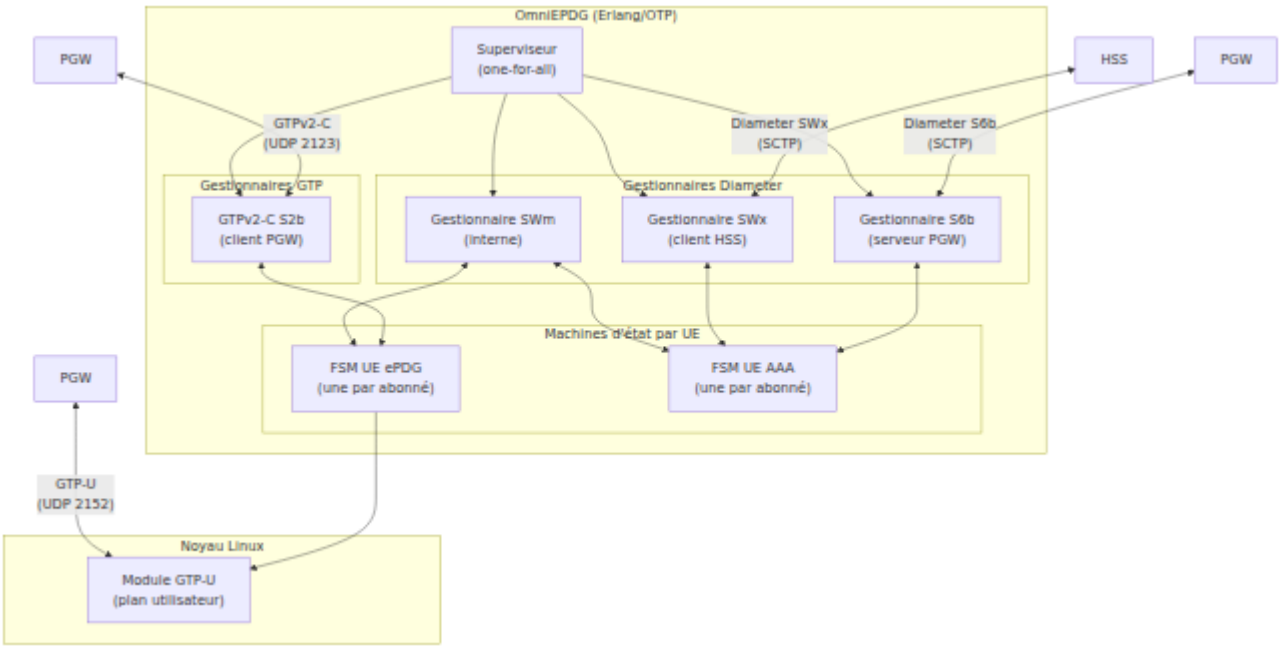
Ce document décrit l'architecture interne d'OmniEPDG, ses interfaces de protocole, les machines d'état UE et les diagrammes de séquence de messages détaillés pour les procédures clés. OmniEPDG prend en charge deux modes opérationnels : **mode GTP** (tunneling complet 3GPP via PGW) et **mode VPN Simple**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

Architecture du Système

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

Architecture du Mode GTP

En mode GTP, le trafic des abonnés est tunnelé à travers un PGW 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

En 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)	Route les messages EAP Diameter et de session entre les FSM ePDG et 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 du pool IP et de route
`simple_vpn_pool`	Gestionnaire de Pool IP	Alloue et libère des adresses IPv4 à partir 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 machines d'état :

- **FSM UE ePDG** (`epdg_ue_fsm`) - Gère le cycle de vie de la session de l'abonné du point de vue de l'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

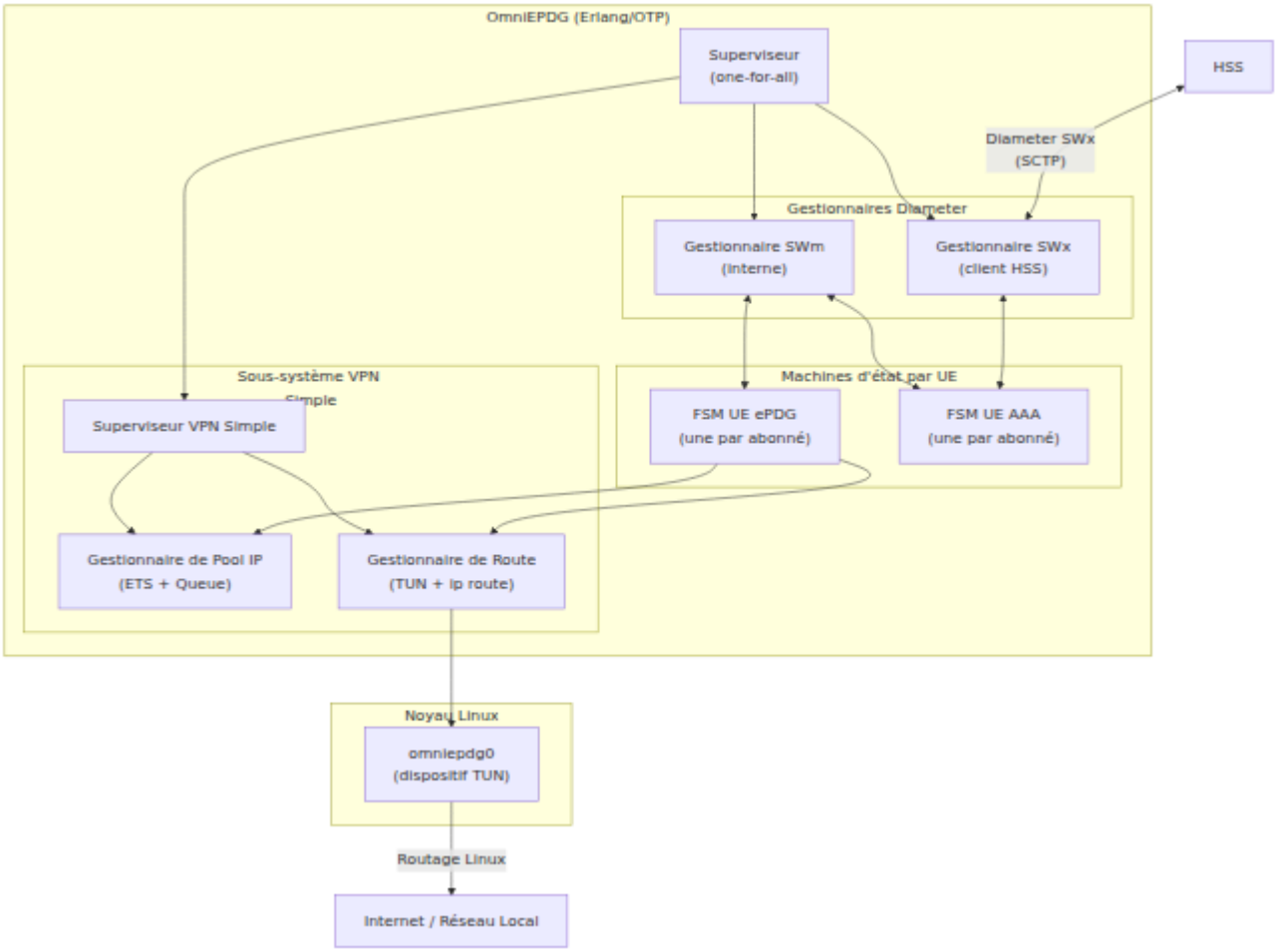
Les deux FSM sont implémentées comme des processus Erlang `gen_statem` avec un mode de rappel de fonction d'état.

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 et à la destruction. Le comportement de la FSM diverge à l'état `authenticated` en fonction du mode opérationnel.

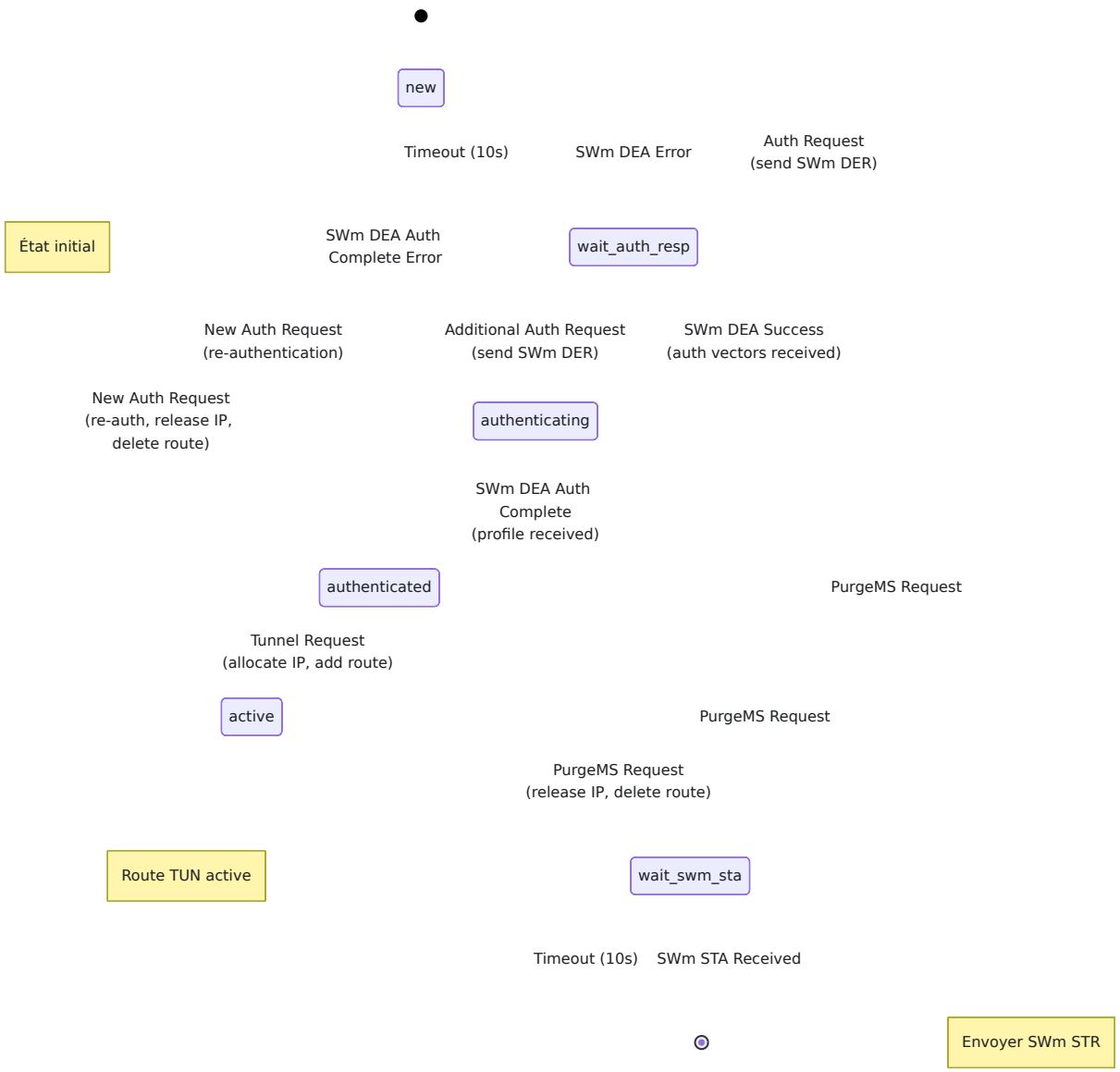
FSM en Mode GTP

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



FSM en Mode VPN Simple

En 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 à partir du pool local, crée une route hôte sur l'interface TUN et passe directement à `active`. Les états de destruction spécifiques au 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
Envoyer SWm STR

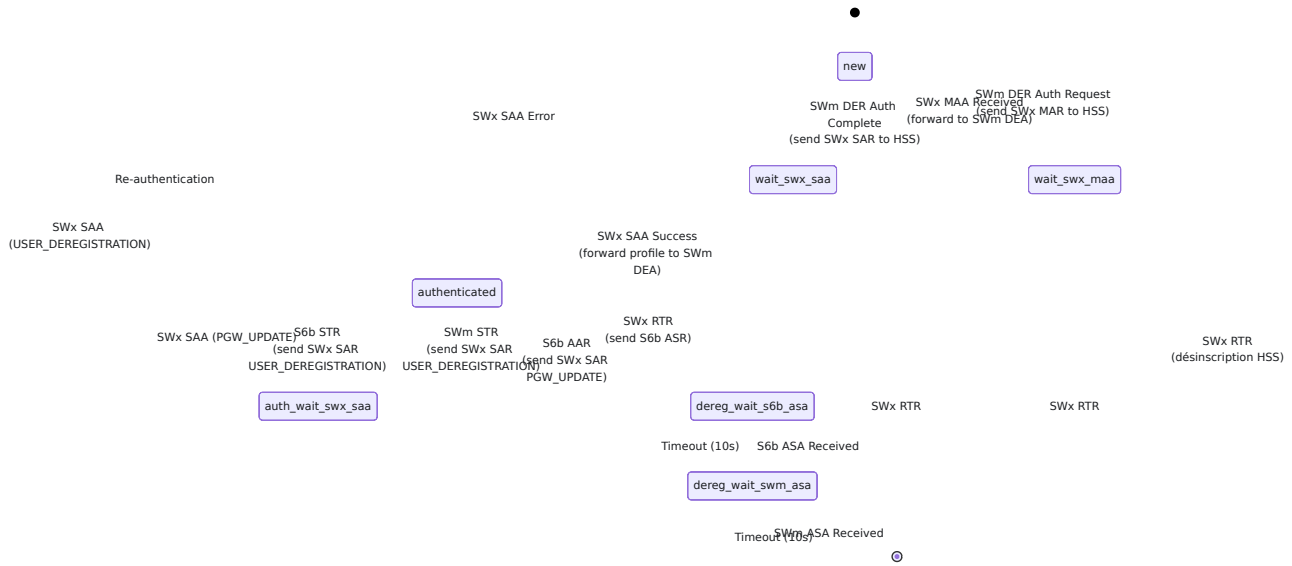
Référence d'État de la FSM UE ePDG

État	Mode	Description	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 terminée, 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	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. Annulation de l'emplacement envoyée à l'UE.	Résultat d'annulation de l'emplacement
`dereg_net_wait_cancel`	GTP	Désinscription initiée par le réseau/HSS. Annulation de l'emplacement envoyée à l'UE.	Résultat d'annulation de l'emplacement
`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

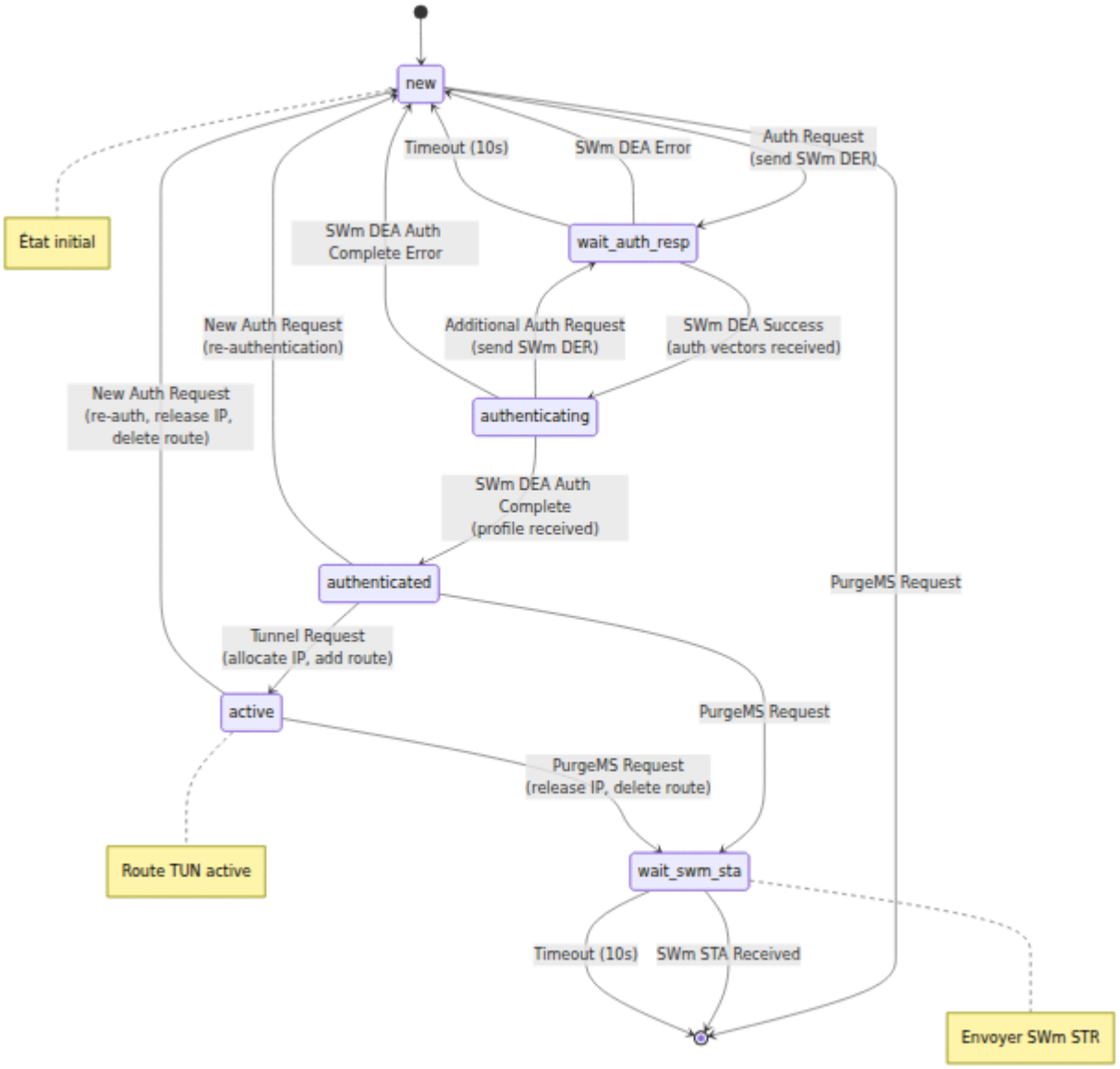
Référence d'État de la FSM UE AAA

État	Description	Attente de
`new`	État initial. Pas de session AAA active.	Demande d'authentification Diameter
`wait_swx_maa`	SWx MAR envoyé au HSS pour les vecteurs EAP-AKA.	SWx MAA du HSS
`wait_swx_saa`	SWx SAR envoyé au HSS pour l'attribution du 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 du PGW ou désinscription de l'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 à l'ePDG.	SWm ASA de l'ePDG

Flux d'Appels

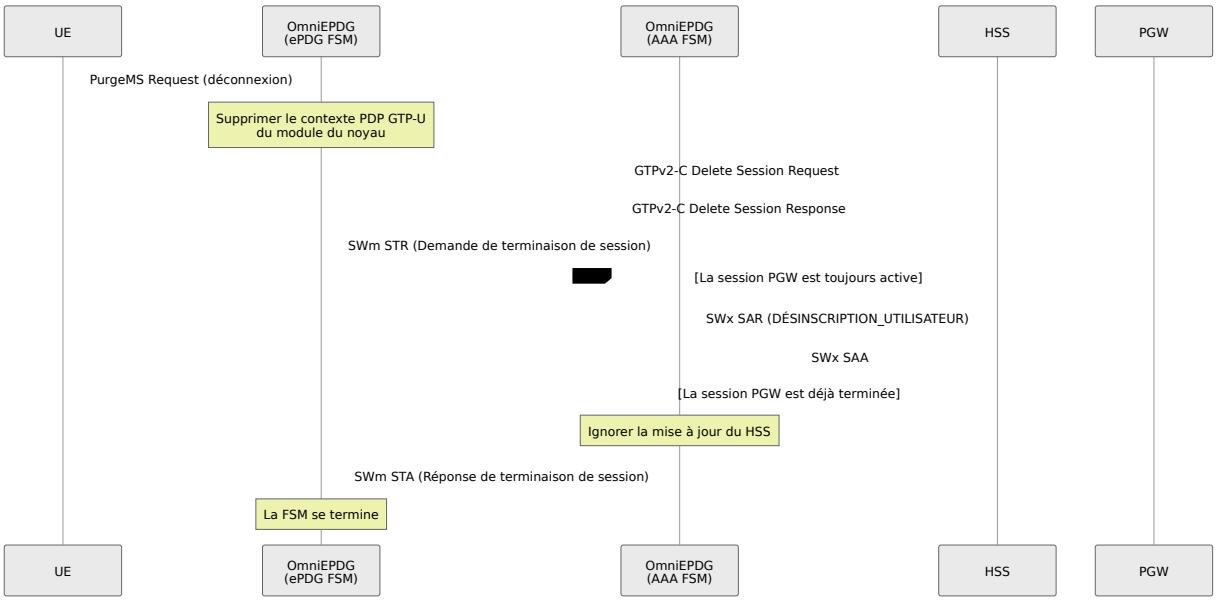
Mode GTP : Établissement de Session Réussi

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



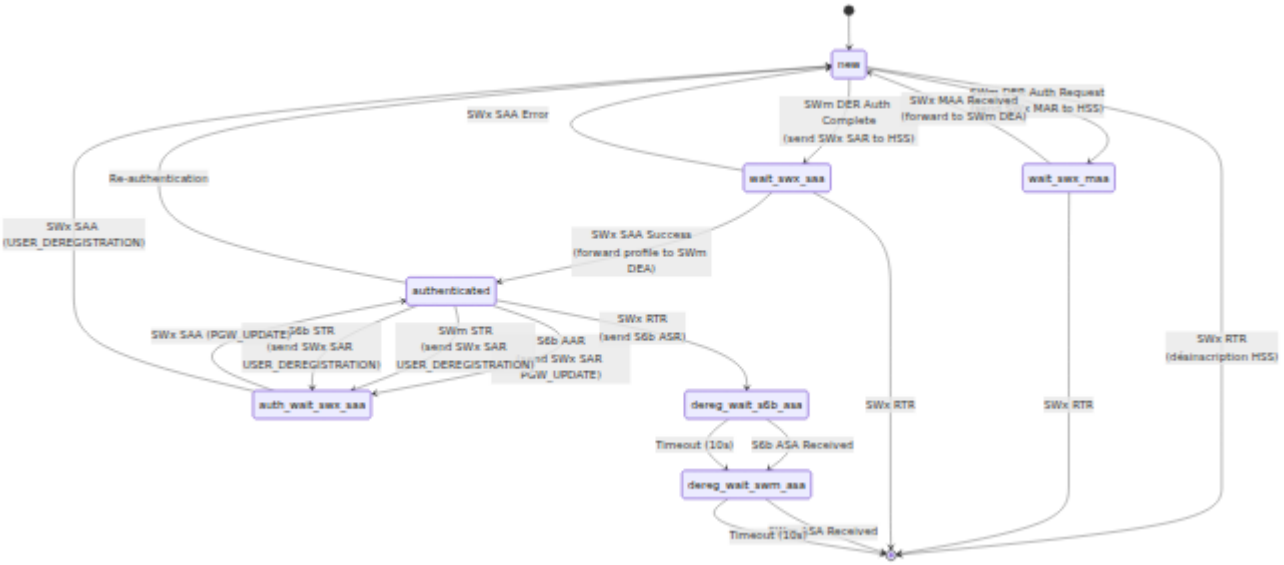
Mode GTP : Destruction de Session Initiée par l'UE

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



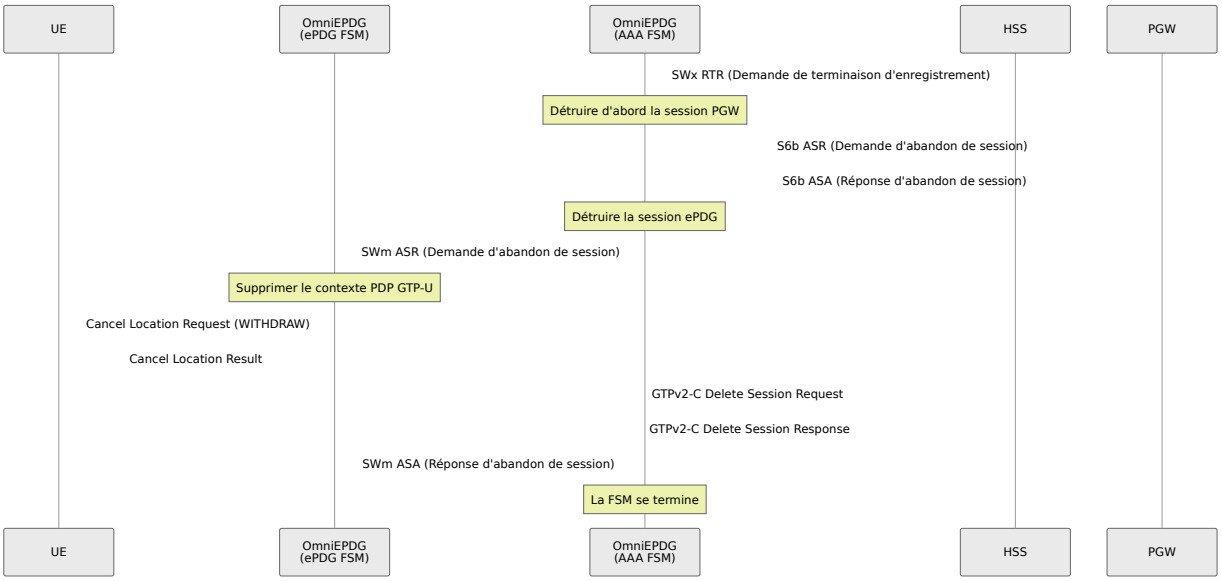
Mode GTP : Destruction de Session Initiée par le PGW

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



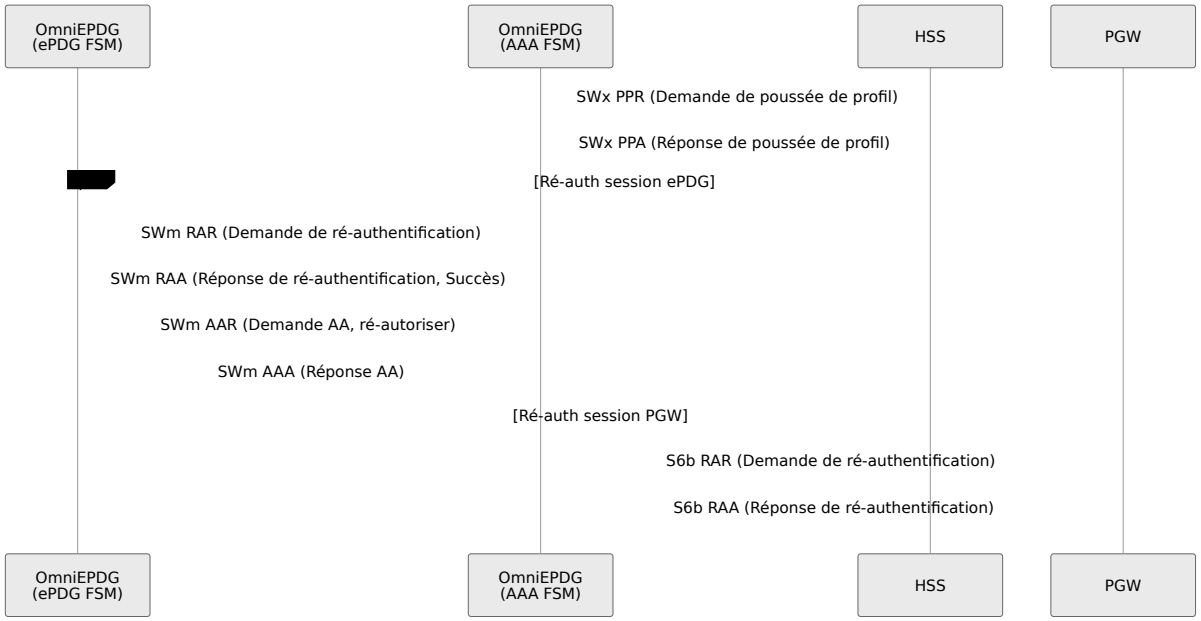
Mode GTP : Désinscription Initiée par le Réseau (HSS)

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



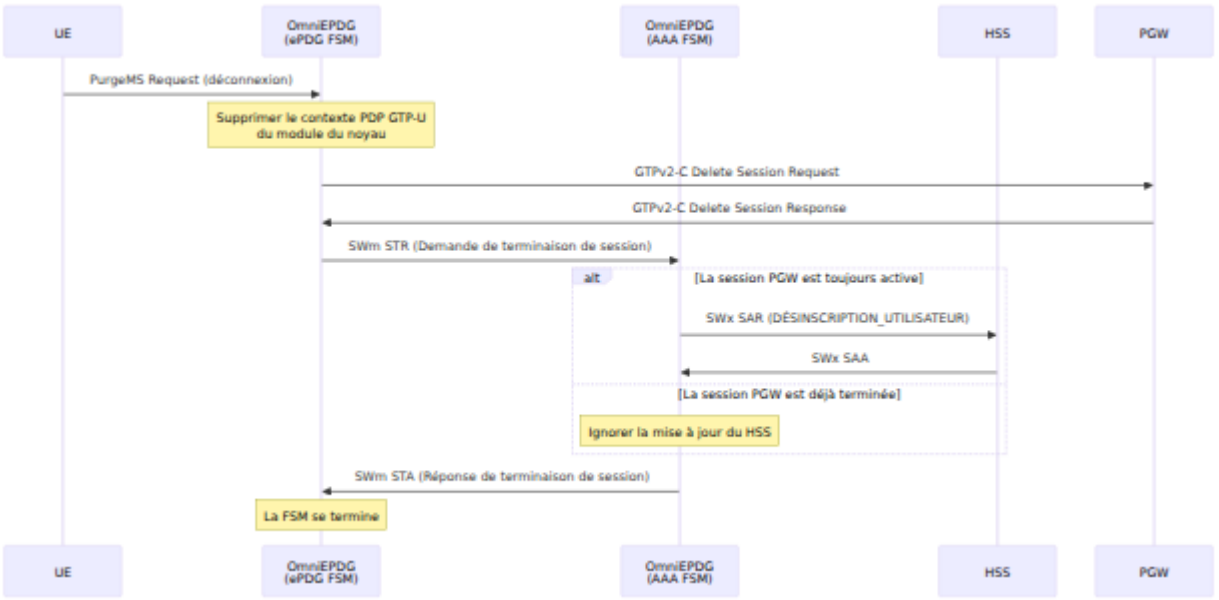
Mode GTP : Poussée de Profil HSS et Ré-authentification

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.



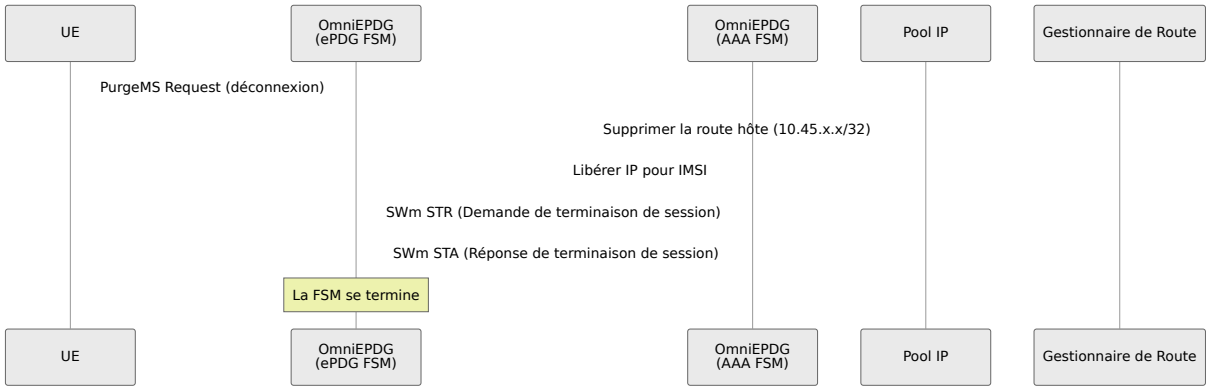
Mode VPN Simple : Établissement de Session Réussi

En mode VPN Simple, l'établissement de session est plus court. Après l'authentification EAP-AKA, la FSM ePDG alloue une IP à partir 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)	Authentification ePDG ↔ HSS et gestion des abonnés	3GPP TS 29.273
16777272	S6b	10415 (3GPP)	Autorisation de session AAA ↔ PGW	3GPP TS 29.273

Codes de Résultat Diameter

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

Codes de Résultat Standards

Code de Résultat	Nom	Signification
2001	DIAMETER_SUCCESS	Opération terminée 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 le 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 (Uniquement en Mode GTP)

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 terminée 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 d'un porteur 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 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
HMAC-SHA1-96	2	160 bits	96 bits	Supporté (héritage)	RFC 2404
HMAC-MD5-96	1	128 bits	96 bits	Supporté (héritage)	RFC 2403

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-HMAC-SHA1	2	160 bits	Supporté (héritage)	RFC 2104
PRF-HMAC-MD5	1	128 bits	Supporté (héritage)	RFC 2104

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 (SA Enfant)

Le tunnel ESP utilise les mêmes algorithmes de chiffrement et d'intégrité négociés lors de la création de SA_ENFANT IKEv2.

Configuration ESP par défaut :

- 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+	FIPS 186-2 PRF (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

Types d'Adresse PDP (Uniquement en Mode GTP)

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	Porteur uniquement IPv4	Adresse IPv4 de 4 octets
IPv6	Porteur uniquement IPv6	Longueur de préfixe de 1 octet + adresse IPv6 de 16 octets
IPv4v6	Porteur double pile	Longueur de préfixe de 1 octet + adresse IPv6 de 16 octets + adresse IPv4 de 4 octets

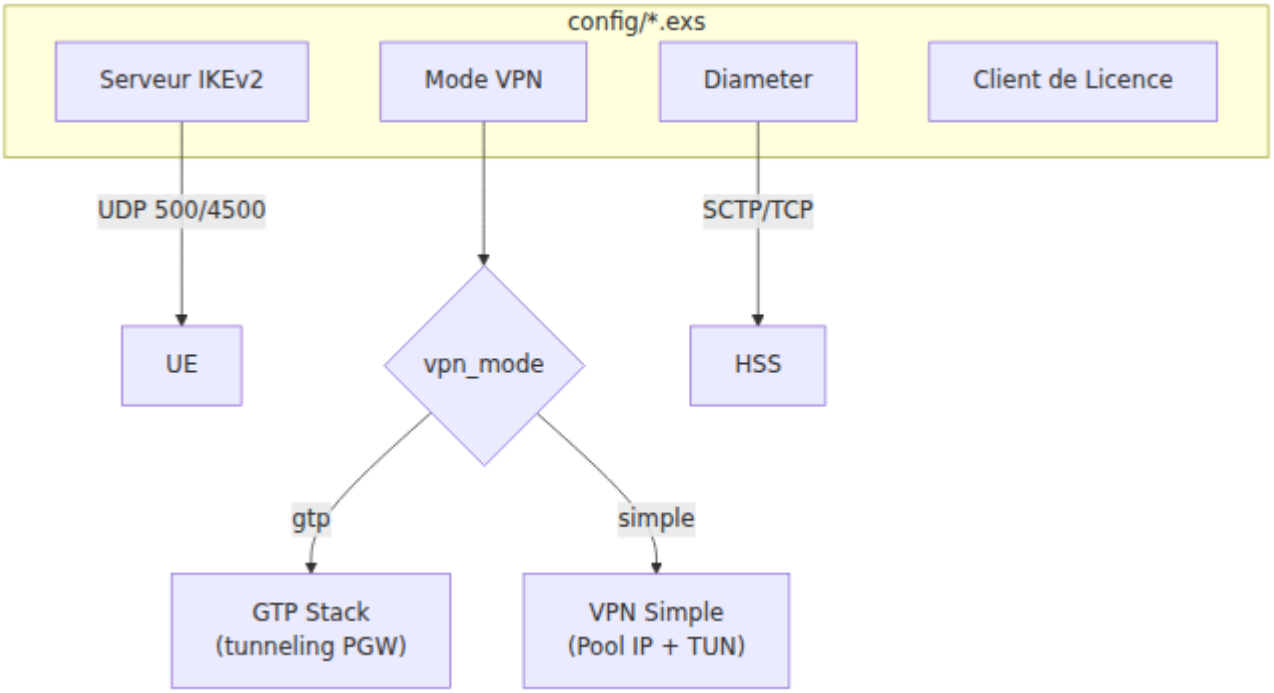
Référence de Configuration OmniEPDG

OmniEPDG est configuré via `config/runtime.exs` et des variables d'environnement. Toute la configuration destinée 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

Structure de Configuration



Fichier de Configuration

Toute la configuration se fait dans `config/runtime.exs`. Ce fichier est lu lorsque OmniEPDG démarre et 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`	Entier	Non	`500`
`port_4500`	Entier	Non	`4500`
`cert_file`	Chaîne	Oui	`/etc/omniepdg/cert`
`key_file`	Chaîne	Oui	`/etc/omniepdg/cert`

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

Paramètres de Sécurité d'Authentification

OmniEPDG inclut une protection intégrée contre les attaques par force brute et le 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	Descrip
`auth_rate_limit_per_ip`	Entier	Non	`10`	Nombre maximum tentatives d'authenti échouées avant bloc
`auth_rate_limit_ip_window_ms`	Entier	Non	`60000`	Fenêtre gl pour comp échecs IP (millisecor
`auth_rate_limit_ip_block_ms`	Entier	Non	`300000`	Durée de blocage p IP dépassa seuil (5 mi
`auth_rate_limit_per_imsi`	Entier	Non	`5`	Nombre maximum tentatives d'authenti échouées IMSI avant blocage.
`auth_rate_limit_imsi_window_ms`	Entier	Non	`60000`	Fenêtre gl pour comp échecs IM (millisecor
`auth_rate_limit_imsi_block_ms`	Entier	Non	`600000`	Durée de blocage p IMSI dépas

Paramètre	Type	Requis	Par Défaut	Descrip
				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`	Booléen	Non	`false`	
`geoip_database_path`	Chaîne	Non	`"/etc/omniepdg/GeoLite2-Country.mmdb"`	
`geoip_mode`	Atome	Non	`:whitelist`	
`geoip_countries`	Liste	Non	`[]`	

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

Sélection du Mode VPN

Paramètre	Type	Requis	Par Défaut	Var Env	Description
`vpn_mode`	Atome	Non	`:simple`	`EPDG_VPN_MODE`	Mode opérationnel : `:simple` pour une sortie IP locale via l'interface TUN, `:gtp` pour le 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	D
`pool_ipv4`	Chaîne	Oui	`"10.45.0.0/16"`	Pool IPv4 CIDI allo abo
`pool_ipv6`	Chaîne	Non	`"2001:db8::/32"`	Pool IPv6 CIDI abo dou
`dns_servers_ipv4`	Liste	Non	`["8.8.8.8", "8.8.4.4"]`	Serv IPv4 UE v (Opt Con de F
`dns_servers_ipv6`	Liste	Non	`["2001:4860:4860::8888", "2001:4860:4860::8844"]`	Serv IPv6 UE v
`p_cscf_ipv4`	Liste	Non	`[]`	Adre CSC (Pro VoW aux acti l'en IMS.
`p_cscf_ipv6`	Liste	Non	`[]`	Adre CSC

Paramètre	Type	Requis	Par Défaut	D
				(Pro VoW
`mtu`	Entier	Non	`1400`	Vale pou de t vale bas réd frag
`nat_enabled`	Booléen	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`	Atome	Non	`:omniepdg`
`listen_ip`	Chaîne	Non	`"0.0.0.0"`
`listen_port`	Entier	Non	`3868`
`host`	Chaîne	Oui	`"epdg"`

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

Paramètres de Pair

Chaque entrée dans la liste `peers` définit une connexion de pair Diameter (typiquement vers le HSS).

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

Identifiants d'Application

Application	ID	Identifiant du Fournisseur	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 par rapport à un serveur de licence.

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

Paramètre	Type	Requis	Par Défaut	Var Env	De
`server_url`	Chaîne	Oui	-	`LICENSE_SERVER_URL`	URI de ter API ser lice
`product`	Chaîne	Non	`"omniepdg"`	-	Ide du pou val de

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	Descript
`port`	Entier	Non	`4000`	`CONTROL_PANEL_PORT`	Port HTTI pour l'interfac web du panneau 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	Description
`port`	Entier	Non	`9568`	`PROMETHEUS_PORT`	Port HTTP pour le point de terminaison des métriques Prometheus (`/metrics`).

Métriques Exposées

Métriques de Compteur (Basées sur les Événements) :

- `epdg_ikev2_session_initiated_count` - Échanges IKE_SA_INIT commencés
- `epdg_ikev2_session_established_count` - IKE SAs établis avec succès
- `epdg_ikev2_session_failed_count` - Échecs d'établissement de SA IKE (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` - Authentifications EAP-AKA échouées (par raison)
- `epdg_eap_aka_sync_failure_count` - Échecs de synchronisation SQN EAP-AKA
- `epdg_diameter_swx_mar_count` - Requêtes Multimedia-Auth (par résultat)
- `epdg_diameter_swx_sar_count` - Requêtes Server-Assignment (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 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 Scraping Prometheus

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

Référence des Délai d'Attente

Tous les délais d'attente internes de 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 maximum d'attente pour la réponse Create/Delete Session GTPv2-C du PGW.
Réponse SWm	10,000 ms	Les Deux	FSM UE ePDG	Temps maximum d'attente pour la réponse Diameter SWm interne (DER/DEA, STR/STA).
Réponse S6b	10,000 ms	GTP	FSM UE AAA	Temps maximum d'attente 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 de l'écoute Diameter.
`DIA_LISTEN_PORT`	`"3868"`	Port d'écoute Diameter.
`DIA_HOST`	`"epdg"`	Host d'origine Diameter (sans domaine).
`DIA_REALM`	`"epc.mnc001.mcc001.3gppnetwork.org"`	Domaine d'origine Diameter.

Pair HSS

Variable	Par Défaut	Description
`HSS_HOST`	`"hss"`	Identité Diameter HSS (Host d'origine).
`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
```

OmniEPDG Panneau de Contrôle

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

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 connexion des pairs Diameter
`/logs`	Journaux	Diffusion de journaux en temps réel
`/docs`	Docs	Navigateur de documentation intégré
`/resources`	Ressources	Informations sur le VM BEAM et l'application
`/configuration`	Configuration	Visualiseur 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'échelonnent 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 de journaux en temps réel
- **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 le signalement Diameter est activé
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
ÉTAT	État actuel de la session (Active/Inactif)
DURÉE	Temps écoulé depuis l'établissement de la session
TRAFFIC	Octets reçus / envoyés (UL/DL)

Indicateurs d'État

Les sessions affichent l'état avec des badges codés par couleur :

État	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 de 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 de l'Enfant IPSec

Section Réseau & Timing

Champ	Description
DNS	Serveurs DNS fournis à l'UE
P-CSCF	Serveurs Proxy-CSCF pour le signalement 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`
État	État de connexion

Indicateurs d'État

État	Couleur	Description
Connecté	Vert	Connexion de pair Diameter établie
Déconnecté	Rouge	Pair non connecté
Inconnu	Gris	L'état ne peut pas être déterminé

Résumé du Nombre de 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 pris en charge 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 un indice 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 nouvelles entrées 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 de 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 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 formatage de 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 de la VM BEAM et les applications OTP en cours d'exécution.

Métriques Système

Métrique	Description
Utilisation de Mémoire	Mémoire totale utilisée par la 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
Principal	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

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` :

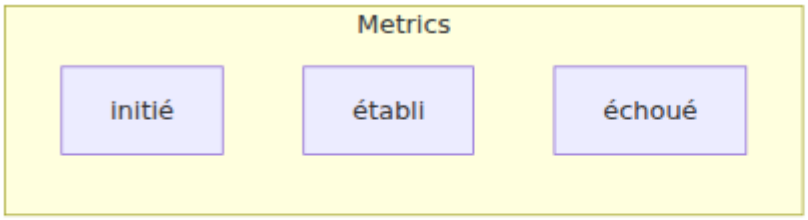
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

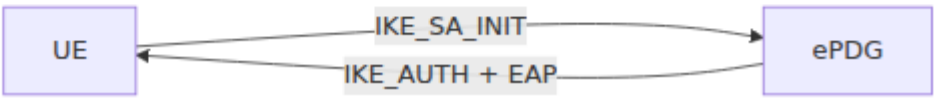
Paramètre	Type	Par défaut	Var Env	Description
`port`	Entier	`9568`	`PROMETHEUS_PORT`	Port HTTP pour le point de terminaison `/metrics`

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.

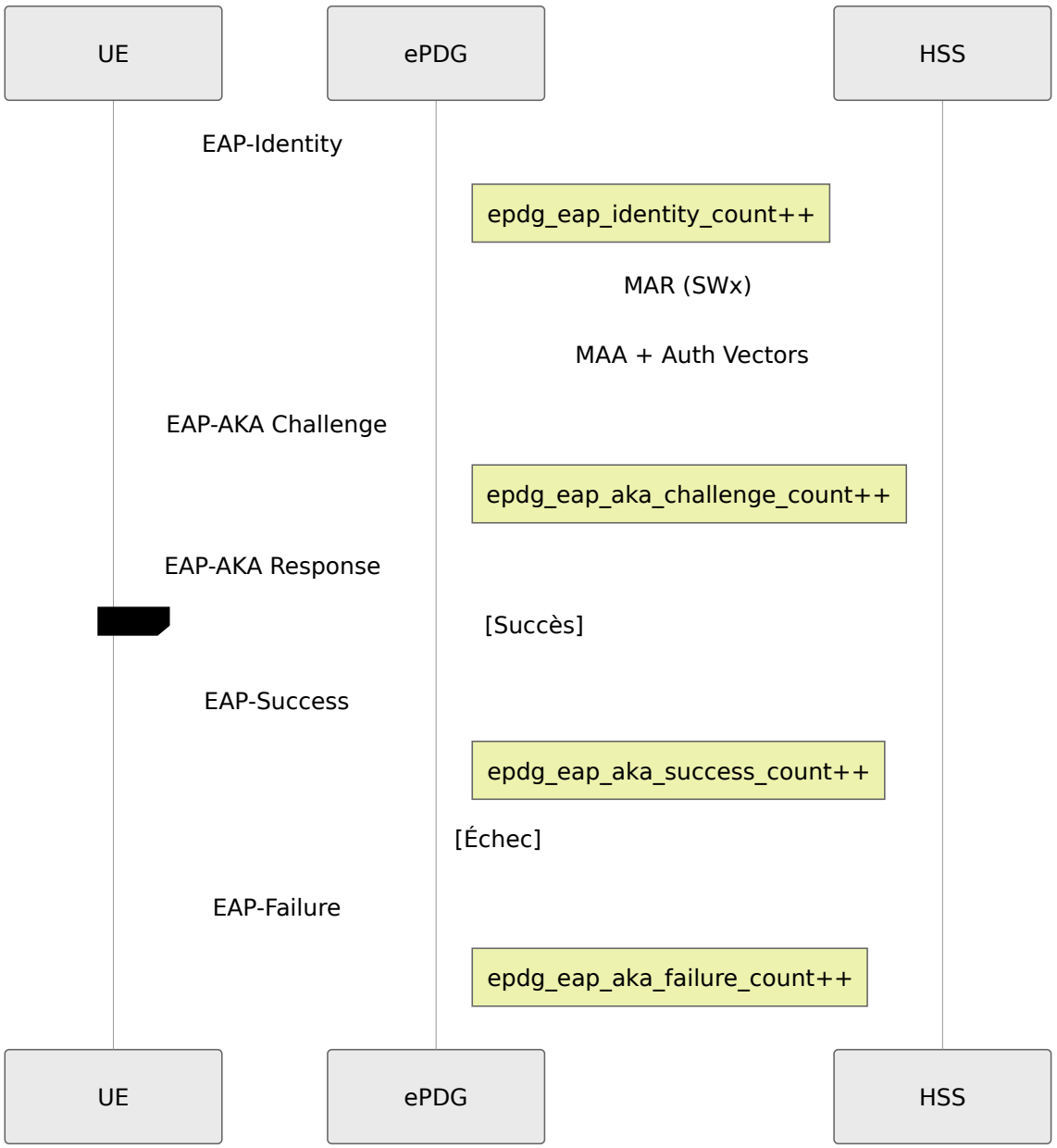
Métrique: `epdg_ikev2_session_established_count`
Type: Compteur
Description: Total des SAs IKE établis avec succès. S'incrémente après une authentification EAP-AKA réussie et la création de Child SA.

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

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

Métriques d'authentification EAP

Métriques suivant les flux d'authentification EAP-AKA par RFC 4187. OmniEPDG prend également en charge EAP-AKA' par 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
Étiquettes:

- `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
Étiquettes:

- `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
Étiquettes:

- `country` - Code de pays ISO 3166-1 alpha-2 (par exemple, `CN`, `RU`), ou `UNKNOWN` pour les IP 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 relecture (par RFC 4303). Indique des attaques potentielles de relecture ou des problèmes de réseau causant un réarrangement 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 de vecteurs d'authentification
Étiquettes:

- `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
Étiquettes:

- `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 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
Étiquettes:

- `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
Étiquettes:

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

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

- `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
Étiquettes:

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

Métrique: `epdg_auth_duration_ms`
Type: Histogramme
Description: Durée du flux d'authentification complet 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 du 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 de pool d'adresses IP en mode VPN simple.

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

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

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

- `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 approchant 1.0 indiquent un risque d'épuisement du pool.

Métriques VM

Métriques de la 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 d'exécution du planificateur. Des valeurs élevées indiquent une saturation du CPU.

Intégration Prometheus

Configuration de Scrape

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 Service

Pour les déploiements Kubernetes, utilisez la découverte de service :

```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 directions)
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 95ème 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
constitution"
          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: "File d'attente d'exécution du planificateur
Erlang élevée"
          description: "La longueur de la file d'attente
```

```
d'exécution est {{ $value }}, indiquant une saturation du CPU"

      # Aucune session (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 relecture ESP détectées
      - alert: OmniEPDGReplayAttack
        expr: rate(epdg_esp_replay_detected_count[5m]) > 0
```

```
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "Attaques de relecture ESP détectées"
          description: "{{ $value | printf \"%.1f\" }} tentatives
de relecture 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"
```

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 ↔ Core)

Ces ports sont utilisés pour la communication entre OmniEPDG et le réseau central mobile. Ils doivent être accessibles depuis l'ePDG mais ne 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 pour atteindre 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

Domaine Diameter DNS

Pour un routage Diameter correct, 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
```

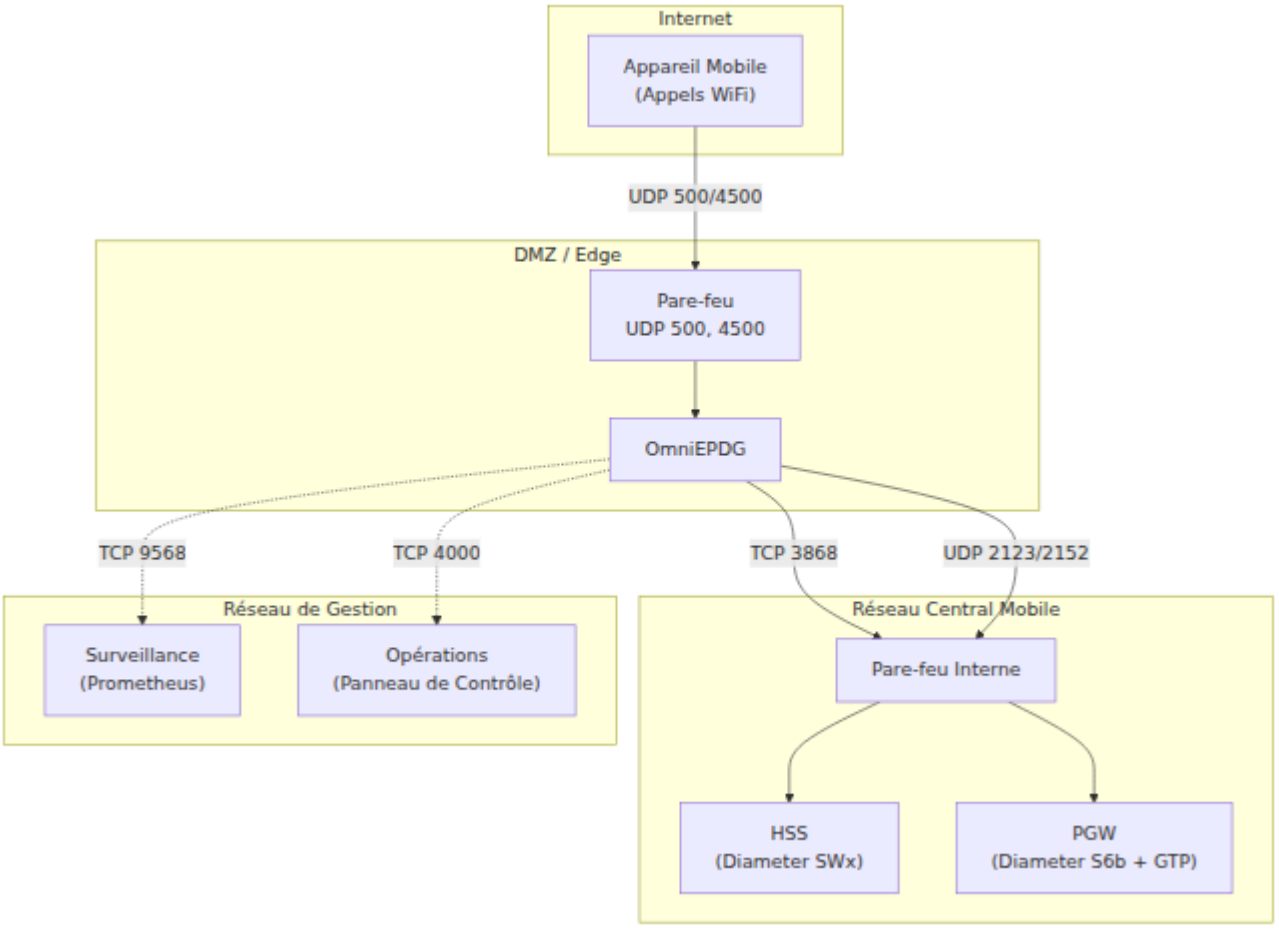
Exemple :

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

Ce domaine est utilisé dans :

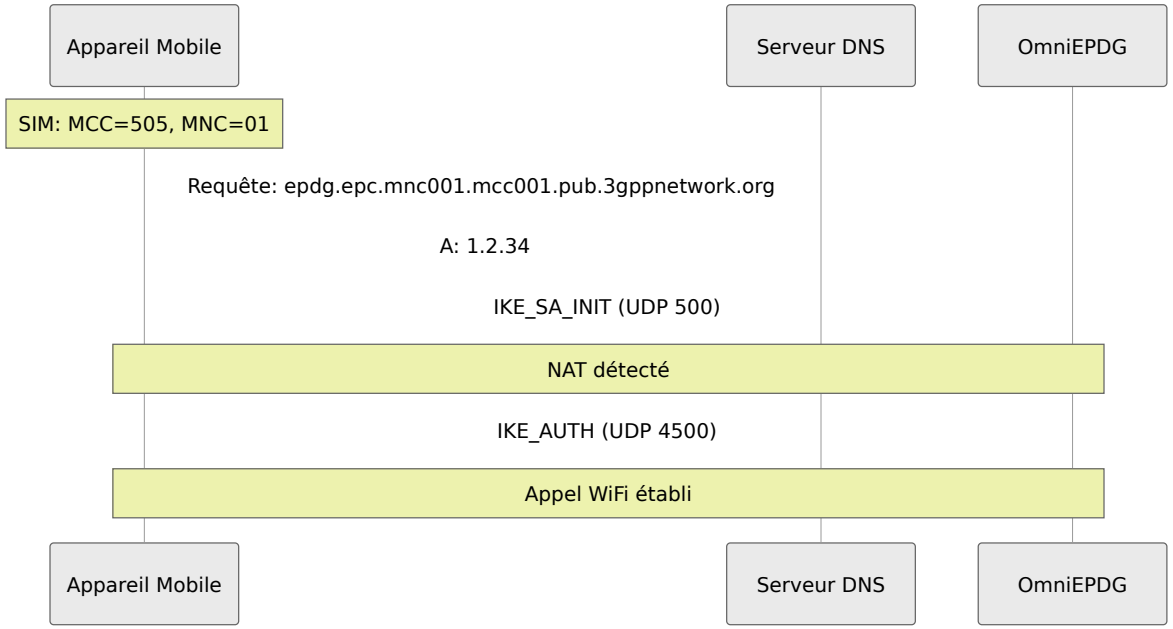
- NAI (Identifiant d'Accès au Réseau) envoyé par l'UE lors de l'authentification
- AVPs Diameter Origin-Realm et Destination-Realm
- Décisions de routage Diameter

Topologie Réseau



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

Exigences du Réseau Central

- [ ] 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 de l'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

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 débranchement IP local.

Liens rapides

Configuration et 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

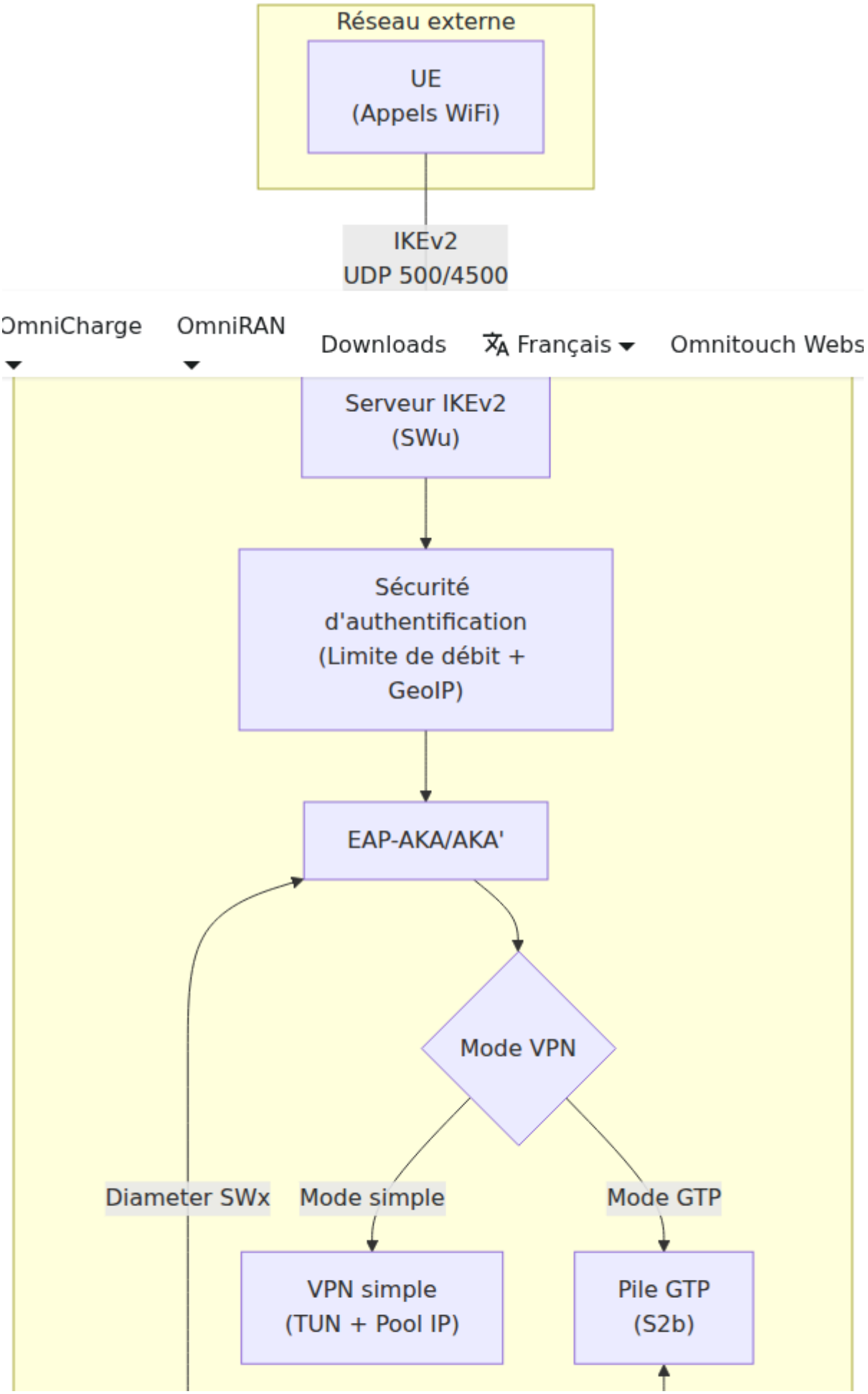
Opérations et surveillance

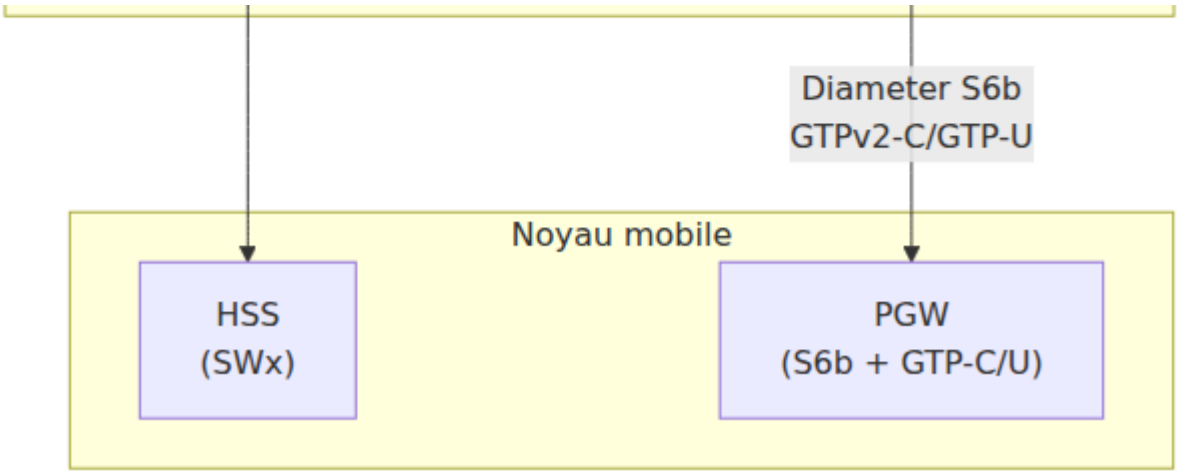
- **Panneau de contrôle** - Interface de surveillance basée sur le web pour les sessions, les pairs Diameter et les journaux
- **Référence des métriques** - Métriques Prometheus, exemples de requêtes et règles d'alerte
- **Dépannage** - Problèmes courants, procédures de diagnostic et étapes de résolution

Sécurité

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

Aperçu de l'architecture


Réseau externe
UE
(Appels WiFi)
IKEv2
UDP 500/4500
OmniCharge
OmniRAN
Downloads
Français
Omnitouch Webs
Serveur IKEv2
(SWu)
Sécurité
d'authentification
(Limite de débit +
GeoIP)
EAP-AKA/AKA'
Mode VPN
Diameter SWx
Mode simple
Mode GTP
VPN simple
(TUN + Pool IP)
Pile GTP
(S2b)



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.

Utilisez 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

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

Utilisez lorsque :

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

Composants :

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

Sécurité d'authentification

OmniEPDG comprend des fonctionnalités de sécurité intégrées pour se protéger contre les attaques par force brute et restreindre l'accès par emplacement géographique. Consultez le guide Sécurité d'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 de pays GeoIP

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

- **Mode liste blanche** - N'autorise que les connexions provenant de pays spécifiés

- **Mode liste noire** - Bloque les connexions provenant de pays spécifiés
- Gestion configurable des IP inconnues/privées
- Comportement de 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 d'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
- Statut des pairs Diameter
- Diffusion en direct des journaux
- Configuration 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 du 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 le statut 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

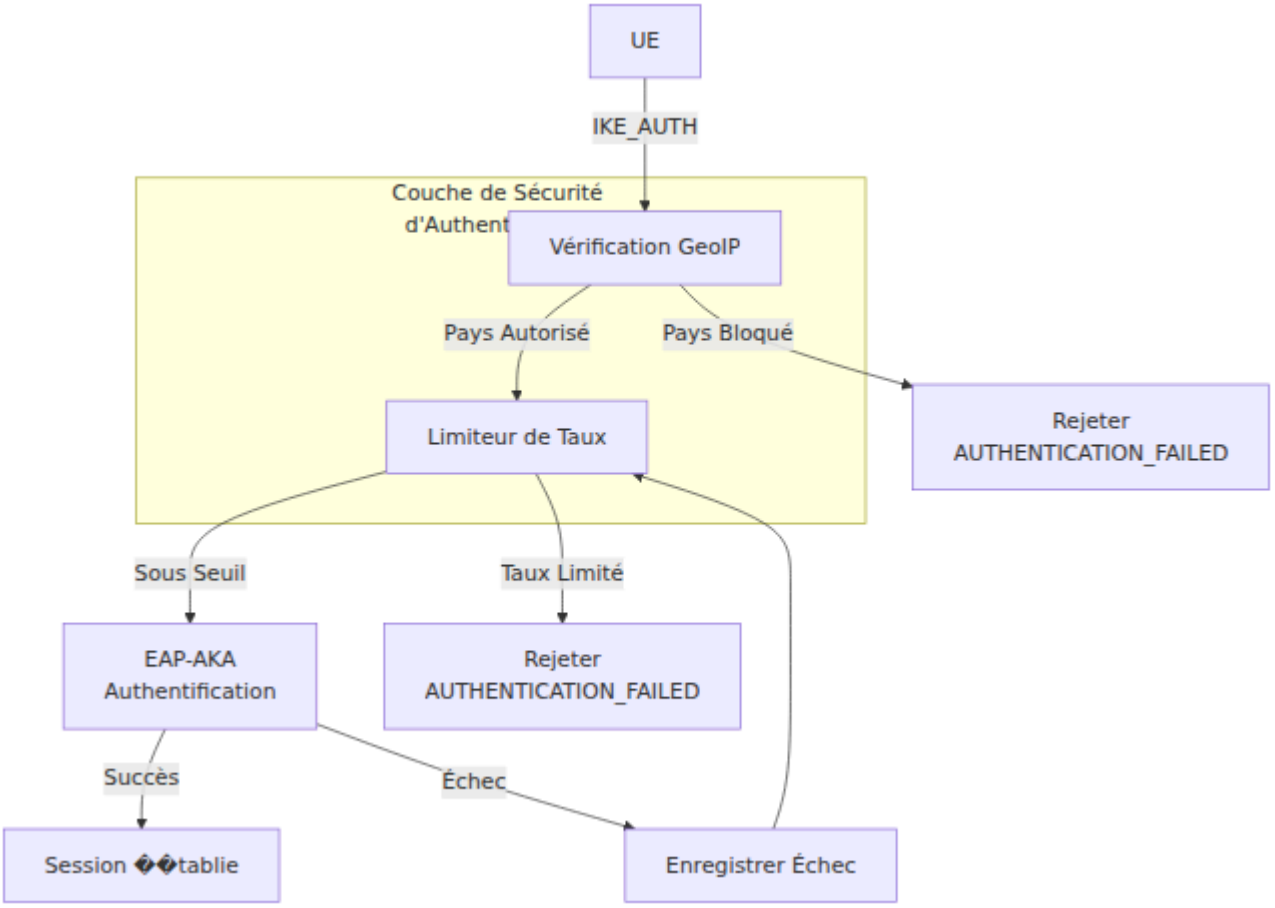
Document	Description
Architecture	Conception du système, machines d'état, flux d'appels, références de protocole
Configuration	Référence de configuration complète avec exemples
Panneau de contrôle	Guide de l'interface web avec captures d'écran
Métriques	Métriques Prometheus, requêtes et alertes
Exigences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

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



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

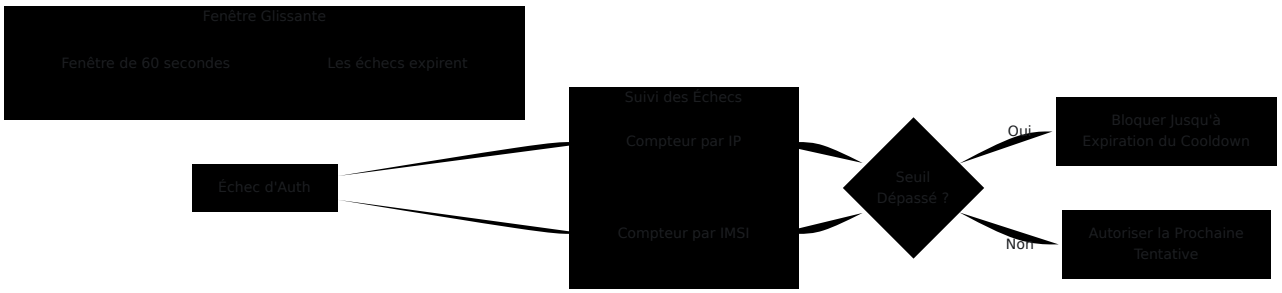
1. **Vérification GeoIP** (optionnelle) - Vérifie que l'IP source provient d'un pays autorisé
2. **Vérification de Limite de Taux** - S'assure que l'IP/IMSI n'a pas dépassé les seuils d'échec
3. **Authentification EAP-AKA** - L'authentification standard 3GPP se poursuit si les vérifications passent

Limitation de 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, d'autres tentatives sont temporairement bloquées.

Comment Cela Fonctionne



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 port 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 passer pour qu'une tentative d'authentification puisse se poursuivre. Si l'un des seuils 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 depuis une s adresse IP 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. Inférieur à pour attra 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 cela fonctionne : Seulement 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 de 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
```

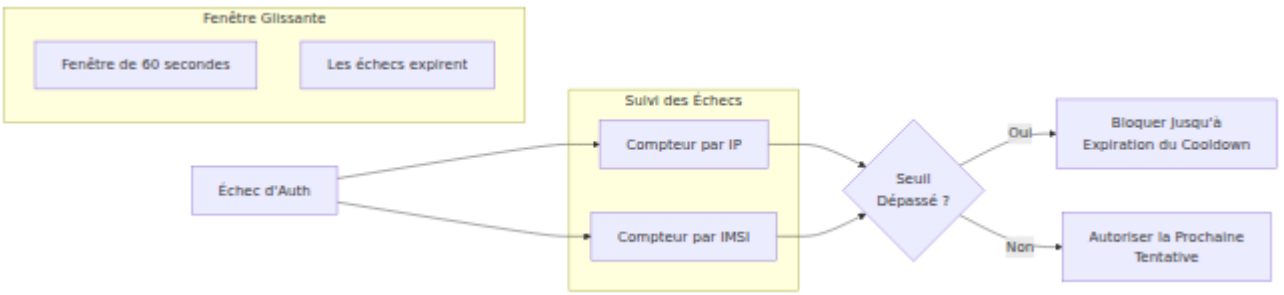
Comment cela fonctionne : Seuils plus élevés et blocs plus courts permettent plus de flexibilité pour les tests.

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 la localisation 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 MaxMind GeoLite2

Les recherches GeoIP utilisent la base de données MaxMind GeoLite2 Country, une base de données de géolocalisation IP gratuite avec des mises à jour hebdomadaires.

Pour activer le blocage GeoIP :

1. Inscrivez-vous pour un compte gratuit sur MaxMind GeoLite2 Signup
2. Téléchargez le fichier de base de données `GeoLite2-Country.mmdb`
3. Placez le fichier au chemin configuré (par défaut : `/etc/omniepdg/GeoLite2-Country.mmdb`)
4. Activez GeoIP dans la configuration

Configuration

```
config :omniepdg,
  # Activer le blocage GeoIP
  geoip_enabled: true,

  # Chemin vers la base de données MaxMind
  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	
`geoip_enabled`	Booléen	Non	`false`	
`geoip_database_path`	Chaîne	Non	`"/etc/omniepdg/GeoLite2-Country.mmdb"`	
`geoip_mode`	Atome	Non	`:whitelist`	

Paramètre	Type	Requis	Par Défaut	
`geoip_countries`	Liste	Non	`[]`	
`geoip_allow_unknown`	Booléen	Non	Voir ci-dessous	
`geoip_fail_open`	Booléen	Non	`true`	

Paramètre	Type	Requis	Par Défaut	
				t c (

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 cela 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 cela 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 le roaming mondial.

Gestion des Pays Inconnus

Certaines adresses IP ne peuvent pas être géolocalisées :

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

Le paramètre `geoip_allow_unknown` contrôle le comportement :

Mode	Valeur par Défaut de `geoip_allow_unknown`	Comportement
Liste Blanche	`false`	Inconnu = non dans la liste blanche = bloqué
Liste Noire	`true`	Inconnu = non dans la liste noire = autorisé

Pour remplacer la valeur par 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)

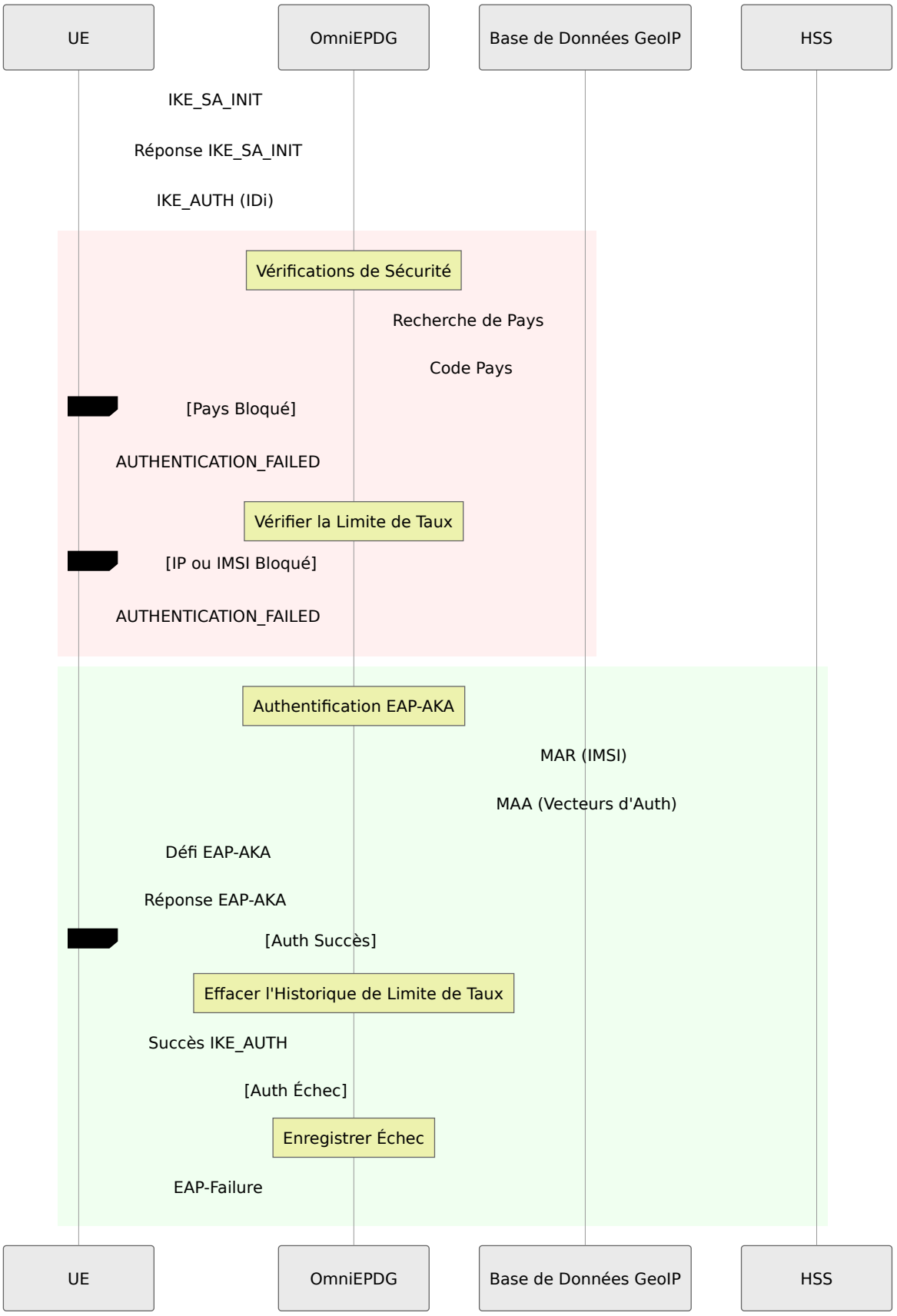
Codes de Pays Courants

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
Base de Données GeoIP
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
[Auth Succès]
Effacer l'Historique de Limite de Taux
Succès IKE_AUTH
[Auth Échec]
Enregistrer Échec
EAP-Failure
UE
OmniEPDG
Base de Données GeoIP
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 réglés trop bas pour l'environnement

Résolution :

1. Vérifiez les métriques pour l'IP/IMSI affectée
2. Envisagez d'augmenter les seuils si des 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 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 avoir activé GeoIP

Causes possibles :

- Fichier de base de données introuvable ou corrompu
- Mauvais codes de pays 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 un laboratoire/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 introuvable"

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

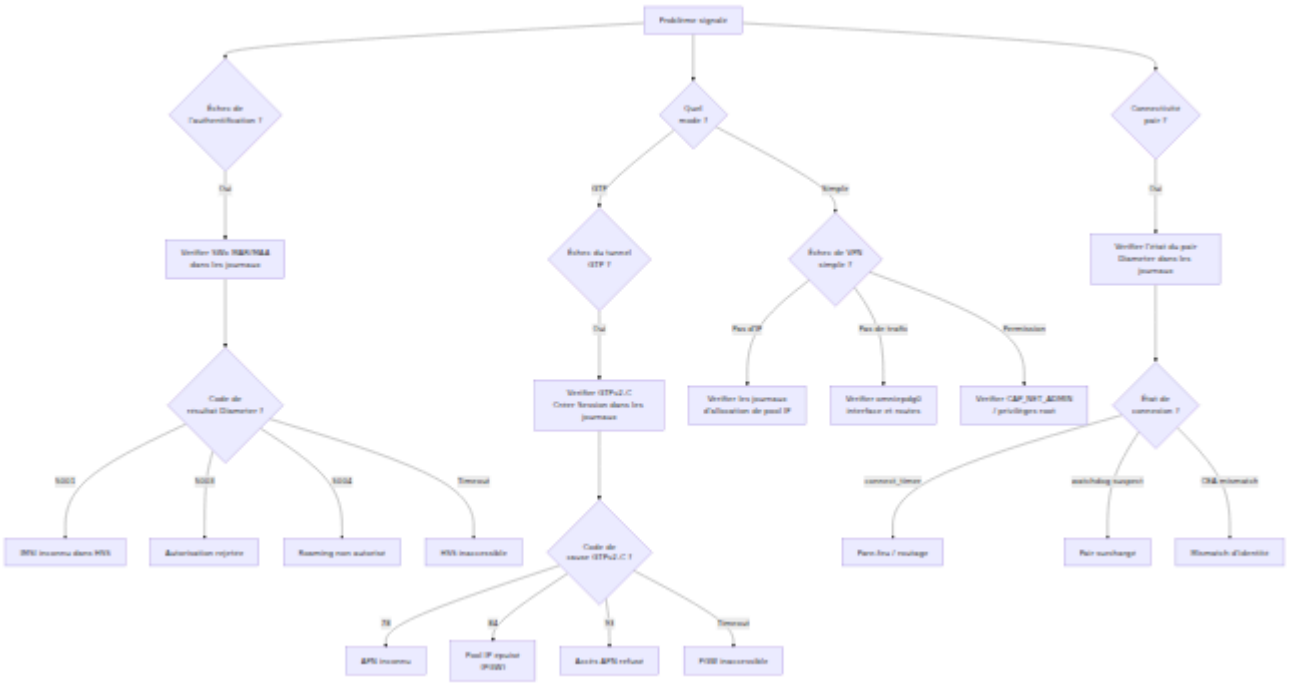
Résolution :

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 des utilisateurs parcourent des réseaux d'entreprise

OmniEPDG Dépannage

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	But	Quand vérifier
`log/console.log`	Tous les messages de l'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`	Crashes du processus OTP	Lorsque les processus redémarrent de manière inattendue
`log/erlang.log`	Journaliseur du noyau Erlang	Problèmes Erlang/OTP de bas niveau

Modèles de Journaux 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(&lt;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 en cours d'exécution 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. Vérifier la connectivité réseau vers l'IP et le port HSS
2. Confirmer que `dia_swx_remote_ip` et `dia_swx_remote_port` correspondent à la configuration HSS
3. Vérifier que le trafic SCTP est autorisé à travers tous les pare-feu. Si SCTP est bloqué, définir `dia_swx_proto` sur `tcp` comme solution de secours
4. Vérifier que `dia_swx_origin_host` est un FQDN résolvable et correspond à ce que le HSS attend
5. Vérifier les journaux HSS pour des échecs de négociation Diameter CER/CEA

Échec de Connexion PGW (S6b)

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

Causes possibles :

- PGW non configuré pour se connecter à l'auditeur 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. Confirmer que le PGW est configuré pour se connecter à OmniEPDG à `dia_s6b_local_ip`:`dia_s6b_local_port`
2. Vérifier que l'adresse de liaison S6b est accessible depuis le réseau PGW
3. Vérifier que les règles de pare-feu autorisent le SCTP entrant sur le port 3868 à l'adresse S6b
4. Vérifier 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 répond pas au DWR dans `dia_swx_watchdog_timer`
- Configuration de watchdog agressive (trop peu de tentatives avant de déclarer suspect)

Résolution :

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

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 carte SIM UE et la base de données HSS
- Format NAI incorrect, causant un échec d'extraction de l'IMSI

Résolution :

1. Vérifier que l'IMSI de l'abonné existe dans la base de données HSS
2. Vérifier que le format NAI dans les journaux correspond au modèle attendu : `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`
3. Confirmer 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 de profil d'abonnement

Résolution :

1. Vérifier le profil de service de l'abonné dans le HSS
2. Confirmer que l'accès WiFi / ePDG est activé pour l'abonné
3. Vérifier que l'APN demandé est 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 l'emplacement actuel de l'abonné
- Appel WiFi non autorisé pour les abonnés en roaming

Résolution :

1. Examiner les politiques de roaming HSS pour la combinaison HPLMN/VPLMN de l'abonné
2. Vérifier 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. Vérifier la réactivité et la charge du HSS
2. Vérifier que le pair Diameter SWx est dans l'état OKAY (pas SUSPECT ou DOWN)
3. Vérifier 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 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 retourne des vecteurs d'authentification pour un 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. Vérifier l'identité NAI de l'UE dans les journaux pour vérifier le préfixe
2. S'assurer que le HSS est configuré pour retourner des vecteurs d'authentification appropriés
3. Vérifier 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. Vérifier que la carte SIM est valide et non endommagée
2. Vérifier que le HSS a retourné des vecteurs d'authentification valides (RAND, AUTN, XRES, CK, IK)
3. Activer la journalisation de débogage pour comparer le XRES attendu avec le RES reçu
4. Si des cartes SIM de test sont utilisées, vérifier 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 de tunnel échoue. Les journaux montrent une réponse GTPv2-C Créer Session avec un code d'erreur.

Codes de cause courants et actions :

Code de Cause	Nom	Action
78	APN manquant ou inconnu	Vérifier que l'APN est configuré sur le PGW et correspond au profil de l'abonné
82	Refusé dans RAT	Vérifier que la politique PGW autorise le type d'accès WiFi (non-3GPP)
84	Tous les adresses dynamiques occupées	Pool IP PGW épuisé ; étendre le pool ou enquêter sur les fuites
92	Échec d'authentification utilisateur	Échec d'authentification côté PGW ; vérifier 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 ; vérifier que la session S6b a été autorisée
113	Congestion APN	APN surchargé ; réessayer ou enquêter 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 de tunnel reste bloquée pendant 10 secondes puis échoue. Les journaux montrent `Timeout create_session_timeout` dans `state_wait_create_session_resp`.

Causes possibles :

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

Tunnel GTP-U Ne Transmet Pas de Trafic

Symptômes : Le tunnel est établi (Création de session réussie) mais le trafic de l'abonné ne passe 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. Vérifier que le module GTP du noyau Linux est chargé (`lsmod | grep gtp`)
2. Confirmer que le dispositif de tunnel GTP existe (`ip link show gtp0`)
3. Vérifier que `gtp_u_kmod` `ip` correspond à `gtpc_local_ip` ou à l'adresse signalée dans la demande de création de session
4. Vérifier que la table de routage inclut des routes à travers le dispositif de tunnel GTP
5. Vérifier 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
- Module noyau TUN/TAP non chargé
- Un autre processus a déjà créé une interface nommée `omniepdg0`

Résolution :

1. Vérifier que le module noyau TUN est disponible (`lsmod | grep tun`)
2. Confirmer qu'OmniEPDG s'exécute avec des privilèges suffisants pour créer des interfaces TUN
3. Vérifier si `omniepdg0` existe déjà d'une instance précédente (`ip link show omniepdg0`)
4. Vérifier `log/crash.log` pour des erreurs du processus gestionnaire de 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 destruction de la session (fuite)
- Taille du pool trop petite pour le nombre d'abonnés simultanés

Résolution :

1. Vérifier le nombre de processus `epdg_ue_fsm` actifs par rapport à la taille du pool
2. Vérifier que les sessions sont correctement détruites (vérifier les messages de journal `terminating`)
3. Si le pool est réellement plein, l'étendre en utilisant un préfixe CIDR plus grand dans `simple_vpn_pool_ipv4` (nécessite un redémarrage)
4. Vérifier les crashes de FSM lors de la destruction dans `log/crash.log` qui auraient 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. Vérifier que la route hôte existe (`ip route show` et chercher la route /32 de l'abonné via `omniepdg0`)
2. Confirmer que le transfert IP est activé (`sysctl net.ipv4.ip_forward`)
3. Vérifier que les règles iptables/nftables permettent le transfert à travers `omniepdg0`
4. Si les abonnés ont besoin d'accès à Internet, vérifier 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 des abonnés restent dans la table de routage après le redémarrage d'OmniEPDG ou après que les sessions se terminent anormalement.

Causes possibles :

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

Résolution :

1. Vérifier `log/crash.log` pour des crashes de processus lors de la destruction
2. Supprimer 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 Démontage de Session

Démontage Bloque Pendant la Désinscription

Symptômes : Le démontage 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. Vérifier les journaux pour des messages de timeout dans l'état pertinent
2. Vérifier la connectivité PGW et HSS
3. Après 10 secondes, la FSM devrait expirer et passer à l'étape suivante de démontage ou se terminer. Si ce n'est pas le cas, vérifier 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
- Crash pendant la séquence de démontage

Résolution :

1. Vérifier `log/crash.log` pour des crashes de processus lors de la destruction
2. Le callback `terminate/3` de la FSM tente de nettoyer le contexte PDP. Si la FSM a été tuée (par exemple, redémarrage du superviseur), le nettoyage peut avoir été 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 crash.

Causes possibles :

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

Résolution :

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

Utilisation Élevée de 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 destruction de la session
- Accumulation de messages de journal dans les boîtes aux lettres
- Grand nombre de sessions simultanées

Résolution :

1. Vérifier 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. Vérifier que les FSM se terminent correctement après la destruction de la session (vérifier les messages de journal `terminating`)

3. Examiner les paramètres de rotation des journaux pour s'assurer que les fichiers journaux sont en cours de rotation

Guide des opérations OmniEPDG

OmniEPDG est une passerelle de données par paquet 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 paquets (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) - Tunneling complet 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

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

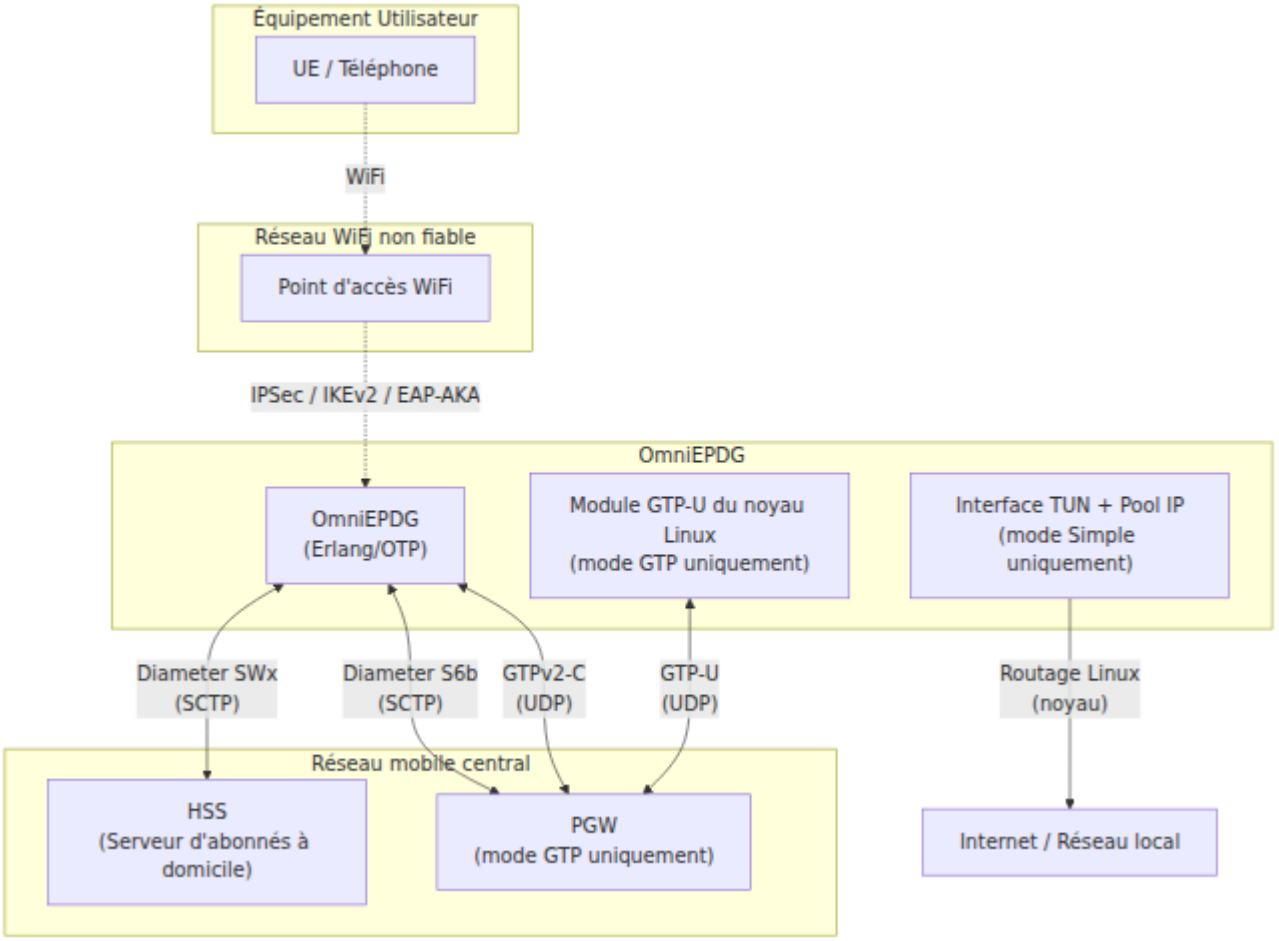
Sécurité

- **Guide de sécurité** - Limitation du taux d'authentification et blocage de 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 des 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 nécessaire)

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 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	À partir du 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 du 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 de plan utilisateur

Fonctionnalités

Fonctionnalité principale

- **Authentification EAP-AKA** - Authentification complète des abonnés EAP-AKA conforme à la 3GPP via HSS
- **Gestion de tunnel IPSec** - Tunnel sécurisé basé sur IKEv2 entre UE et ePDG
- **Deux modes opérationnels** - Tunneling 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 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 module du noyau Linux
- **Teardown initié par PGW** - PGW envoie une demande de suppression de porteur, ePDG cascade le teardown vers l'UE
- **Teardown initié par le réseau** - HSS déclenche la désinscription via SWx RTR, 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 de l'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 des sondes configurables
- **Protection anti-rejeu 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'abonnés mis à jour du HSS (mode GTP)
- **Demande/Réponse de terminaison d'enregistrement (RTR/RTA)** - Désinscription d'abonné initiée par HSS (mode GTP)

Intégration PGW (mode GTP uniquement)

S6b Diameter :

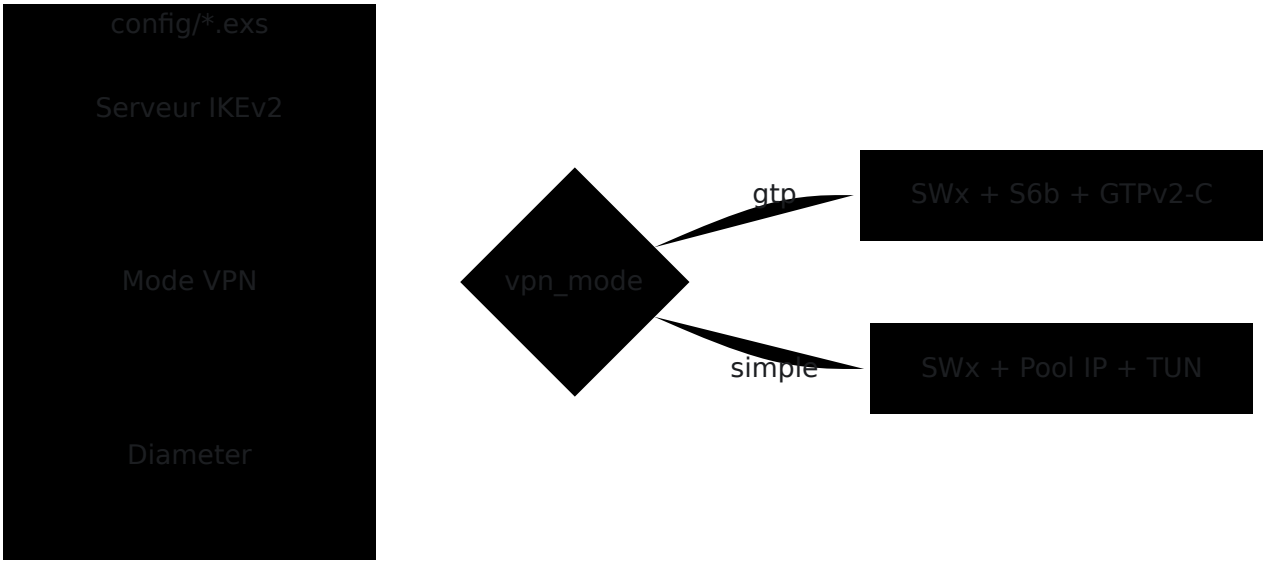
- **Demande/Réponse AA (AAR/AAA)** - Autoriser les sessions PGW
- **Demande/Réponse de terminaison de session (STR/STA)** - Terminer les sessions PGW
- **Demande/Réponse de ré-authentification (RAR/RAA)** - Ré-autoriser les sessions actives
- **Demande/Réponse d'abandon de session (ASR/ASA)** - Terminer de force les sessions

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 porteur** - Gestion des porteurs 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. Consultez 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 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 de l'architecture pour les accès non 3GPP	Architecture globale ePDG 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 l'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 système :

1. Consultez l'Architecture & Flux d'appels pour les détails d'interface et les machines d'état
2. Utilisez la Référence de configuration pour la configuration de 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 aux protocoles