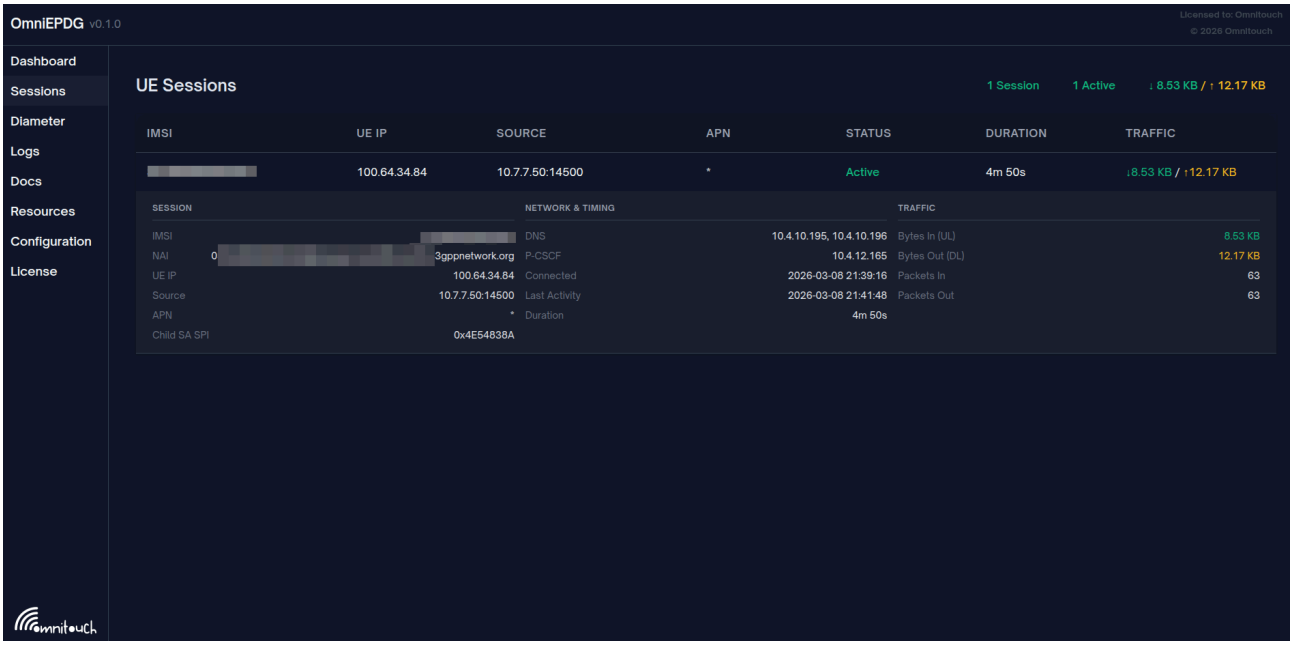
Guía de Operaciones de OmniEPDG

OmniEPDG es una Puerta de Datos de Paquetes Evolucionada (ePDG) que permite llamadas de Voz sobre WiFi (VoWiFi). Autentica a los suscriptores móviles a través de redes WiFi no confiables utilizando EAP-AKA, y los conecta a la red central móvil a través de señalización Diameter hacia el HSS y túneles GTP hacia una Puerta de Datos de Paquetes (PGW).



El panel de control de OmniEPDG mostrando una sesión de suscriptor activa con estadísticas de tráfico en tiempo real.

OmniEPDG soporta dos modos operativos:

- **Modo GTP** (predeterminado) - Túnel completamente conforme a 3GPP a través de un PGW mediante GTPv2-C y GTP-U
- **Modo VPN Simple** - Salida local con un grupo de IP incorporado y una interfaz TUN de Linux, sin necesidad de PGW

Documentación

Configuración y Operaciones

- **Arquitectura y Flujos de Llamadas** - Arquitectura del sistema, interfaces de protocolo, máquinas de estado de UE y diagramas de secuencia de mensajes para ambos modos
- **Referencia de Configuración** - Documentación completa de parámetros para Diameter, GTPv2-C, GTP-U, VPN Simple y registro
- **Panel de Control** - Interfaz de monitoreo basada en web para sesiones, pares Diameter y registros

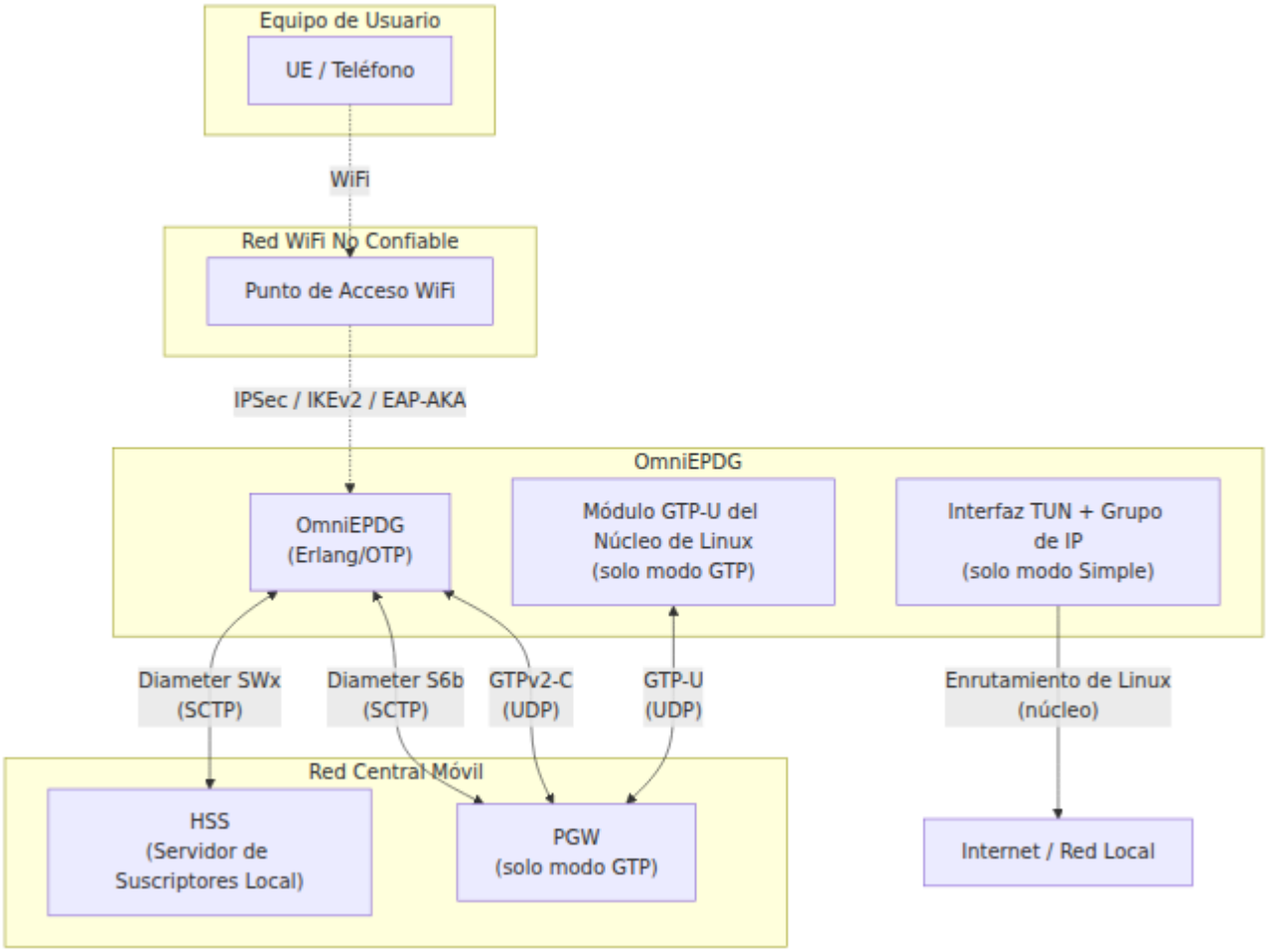
Seguridad

- **Guía de Seguridad** - Limitación de tasa de autenticación y bloqueo de países por GeoIP

Monitoreo y Solución de Problemas

- **Referencia de Métricas** - Métricas de Prometheus para monitorear autenticación, sesiones, señalización Diameter y salud del sistema
- **Solución de Problemas** - Problemas comunes, procedimientos de diagnóstico y pasos de resolución

Modos Operativos



Modo GTP

El modo predeterminado. OmniEPDG envía todo el tráfico del suscriptor a través de un PGW utilizando GTPv2-C para el control de sesiones y GTP-U (a través del módulo del núcleo de Linux) para el plano de usuario. Esto es completamente conforme a 3GPP y adecuado para implementaciones de operadores con infraestructura EPC existente.

Ruta de tráfico: UE → IPSec → OmniEPDG → GTPv2-C Crear Sesión → túnel GTP-U → PGW → Internet

Infraestructura requerida: HSS, PGW

Modo VPN Simple

OmniEPDG asigna direcciones IP de un grupo local y enruta el tráfico del suscriptor directamente a través de una interfaz TUN de Linux (`tun_epdg`) utilizando enrutamiento estándar del núcleo. No se necesita infraestructura de PGW o GTP. La autenticación aún se realiza a través de Diameter SWx hacia el HSS.

Ruta de tráfico: UE → IPSec → OmniEPDG → Asignación de IP local → interfaz TUN → enrutamiento de Linux → Internet

Infraestructura requerida: Solo HSS (no se necesita PGW)

Optimización opcional: La bandera `skip_sar` omite la Solicitud/Respuesta de Asignación de Servidor del HSS, reduciendo el tiempo de configuración de conexión. Esto significa que el HSS no rastreará qué ePDG atiende al suscriptor y los procedimientos iniciados por el HSS (deregistro, envío de perfil) no funcionarán. Adecuado para implementaciones privadas sin requisitos de itinerancia.

Comparación de Modos

Capacidad	Modo GTP	Modo VPN Simple
Conforme a 3GPP	Sí	No (con `skip_sar`), Parcial (sin)
PGW requerido	Sí	No
HSS requerido	Sí	Sí (solo autenticación)
Asignación de IP	Desde PGW	Grupo local (CIDR)
Plano de usuario	Módulo GTP-U del núcleo	Linux TUN + enrutamiento
Envío de perfil HSS	Sí (PPR/PPA)	No
Deregistro HSS	Sí (RTR/RTA)	No (con `skip_sar`)
Desmantelamiento iniciado por PGW	Sí	N/A
Soporte de itinerancia	Sí	No
IPv6 / Doble pila	Sí	Solo IPv4

Interfaces de Protocolo

Interfaz	Protocolo	Transporte	Modo	Par	Propósito	Re
SWu	IKEv2 / IPSec	UDP	Ambos	UE	Túnel seguro y autenticación EAP-AKA	3G 33.
SWx	Diameter	SCTP	Ambos	HSS	Vectores de autenticación y asignación de servidor	3G 29. Sec
S6b	Diameter	SCTP	Solo GTP	PGW	Autorización de sesión y política	3G 29. Sec
S2b	GTPv2-C / GTP-U	UDP	Solo GTP	PGW	Control y túnel de plano de usuario	3G 29.

Características

Funcionalidad Central

- **Autenticación EAP-AKA** - Autenticación de suscriptores EAP-AKA completamente conforme a 3GPP a través del HSS
- **Gestión de Túneles IPSec** - Túnel seguro basado en IKEv2 entre UE y ePDG
- **Dos Modos Operativos** - Túnel GTP a PGW o salida local con VPN Simple
- **Máquinas de Estado por UE** - FSM de Erlang independiente por suscriptor para la gestión del ciclo de vida de la sesión

- **Soporte de Doble Pila** - Tipos de dirección PDP IPv4, IPv6 e IPv4v6 (modo GTP)

Características del Modo GTP

- **Establecimiento de Túnel GTP** - Creación de sesión GTPv2-C y plano de usuario GTP-U a través del módulo del núcleo de Linux
- **Desmantelamiento Iniciado por PGW** - PGW envía Solicitud de Eliminación de Portadora, ePDG cascada desmantela a UE
- **Desmantelamiento Iniciado por la Red** - HSS activa el deregistro a través de SWx RTR, ePDG desmantela todas las sesiones
- **Re-Autenticación** - Envío de perfil y re-autorización activados por HSS según 3GPP TS 29.273 Sección 7.1.2.5.1

Características del Modo VPN Simple

- **Grupo de IP Local** - Asignación de direcciones IPv4 basada en CIDR con seguimiento por IMSI
- **Enrutamiento de Interfaz TUN** - Dispositivo TUN estándar de Linux (`tun_epdg`) con rutas de host por UE
- **Configuración de DNS** - Servidores DNS configurables proporcionados a los UEs a través de PCO
- **Opción de Omitir SAR** - Omitir el registro en el HSS para una configuración de conexión más rápida

Características de Seguridad

- **Limitación de Tasa de Autenticación** - Protección contra fuerza bruta por IP y por IMSI con umbrales configurables
- **Bloqueo de Países por GeoIP** - Control de acceso basado en países mediante lista blanca o negra utilizando MaxMind GeoLite2
- **Detección de Pares Muertos** - Monitoreo activo de disponibilidad con sondas configurables
- **Protección Anti-Repetición ESP** - Ventana deslizante de 64 bits conforme a RFC 4303

Integración con HSS (SWx Diameter)

- **Solicitud/Respuesta de Autenticación Multimedia (MAR/MAA)** - Recuperar vectores de autenticación EAP-AKA (ambos modos)
- **Solicitud/Respuesta de Asignación de Servidor (SAR/SAA)** - Descargar perfil de suscriptor y configuración de APN (omitible en modo Simple)
- **Solicitud/Respuesta de Envío de Perfil (PPR/PPA)** - Recibir perfiles de suscriptor actualizados del HSS (modo GTP)
- **Solicitud/Respuesta de Terminación de Registro (RTR/RTA)** - Deregistro de suscriptor iniciado por HSS (modo GTP)

Integración con PGW (Solo Modo GTP)

S6b Diameter:

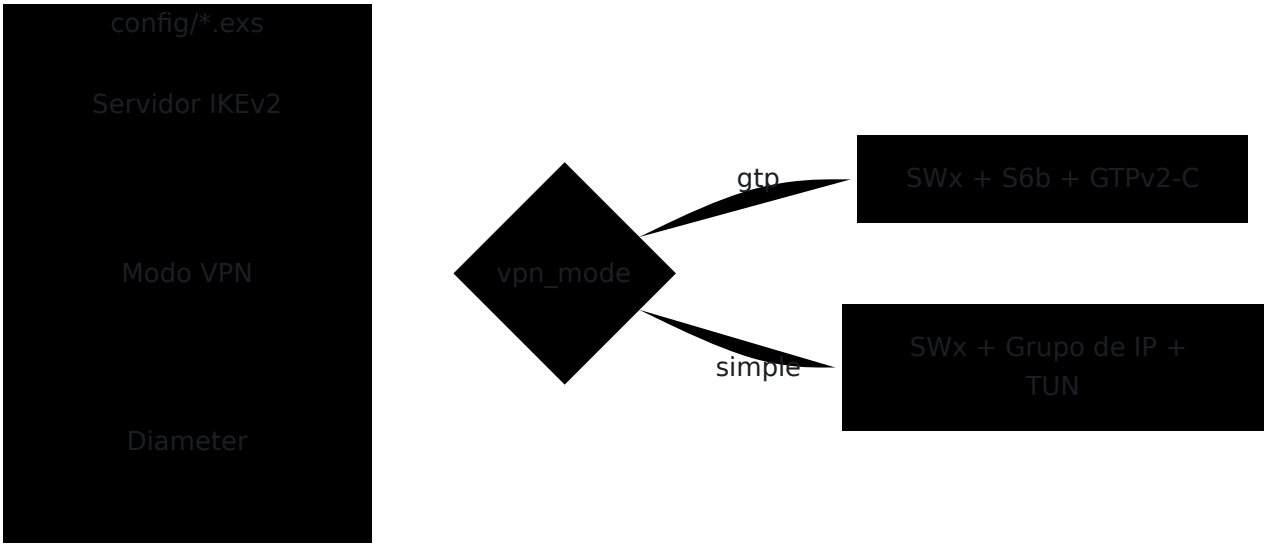
- **Solicitud/Respuesta de AA (AAR/AAA)** - Autorizar sesiones PGW
- **Solicitud/Respuesta de Terminación de Sesión (STR/STA)** - Terminar sesiones PGW
- **Solicitud/Respuesta de Re-Autorización (RAR/RAA)** - Re-autorizar sesiones activas
- **Solicitud/Respuesta de Abort-Session (ASR/ASA)** - Terminar sesiones de forma forzada

S2b GTPv2-C:

- **Solicitud/Respuesta de Crear Sesión** - Establecer túneles GTP con asignación de TEID
- **Solicitud/Respuesta de Eliminar Sesión** - Desmantelar túneles GTP
- **Solicitud/Respuesta de Eliminar Portadora** - Gestión de portadora iniciada por PGW

Inicio Rápido

Estructura de Configuración



La configuración se realiza en `config/runtime.exs` o a través de variables de entorno. El parámetro `vpn_mode` selecciona entre los modos GTP y VPN Simple. Consulte la Referencia de Configuración para la documentación completa de parámetros.

Direccionamiento de Red Típico (Modo GTP)

Componente	Dirección IP	Puerto	Notas
OmniEPDG (GTP-U)	10.74.0.11	-	Punto final del túnel GTP-U
OmniEPDG (Diameter S6b)	10.74.0.12	3868	Escucha Diameter S6b
HSS	10.74.0.21	3868	Par Diameter SWx
PGW	10.74.0.23	2123	Par GTPv2-C y S6b

Direccionamiento de Red Típico (Modo VPN Simple)

Componente	Dirección IP	Notas
OmniEPDG (puerta TUN)	10.44.0.1	IP de puerta en la interfaz `tun_epdg`
Grupo de IP de UE	10.45.0.0/16	Grupo CIDR configurable para IPs de suscriptores
HSS	10.74.0.21:3868	Par Diameter SWx (solo autenticación)

Especificaciones 3GPP

Especificación	Título	Relevancia
TS 29.273	Interfaces EPS AAA (SWx, S6b, SWm)	Especificación principal para interfaces Diameter de ePDG
TS 29.274	GTPv2-C y GTP-U	Control de túnel S2b y plano de usuario (modo GTP)
TS 33.402	Seguridad para accesos no 3GPP	Autenticación EAP-AKA para WiFi no confiable
TS 23.402	Mejoras de arquitectura para accesos no 3GPP	Arquitectura y procedimientos generales de ePDG
TS 23.003	Numeración, direccionamiento e identificación	Formato NAI, estructura IMSI
TS 29.229	Cx/Dx Diameter (definiciones comunes)	Valores de tipo de asignación de servidor utilizados por SWx
RFC 6733	Protocolo Base Diameter	Transporte Diameter, gestión de pares, watchdog
RFC 4187	EAP-AKA	Método de autenticación utilizado sobre IKEv2

Documentación por Rol

Operadores de Red:

1. Comience con la Arquitectura y Flujos de Llamadas para entender el sistema y ambos modos operativos
2. Revise la Referencia de Configuración para los parámetros de implementación
3. Revise la Guía de Seguridad para configurar la limitación de tasa y el bloqueo por GeoIP
4. Configure el monitoreo utilizando la Referencia de Métricas para la integración con Prometheus
5. Mantenga disponible la guía de Solución de Problemas para operaciones

Integradores de Sistemas:

1. Revise la Arquitectura y Flujos de Llamadas para detalles de interfaz y máquinas de estado
2. Utilice la Referencia de Configuración para la configuración de conectividad de pares
3. Configure alertas utilizando la Referencia de Métricas
4. Consulte la tabla de especificaciones 3GPP anterior para el cumplimiento de protocolos

Guía de Operaciones de OmniEPDG

OmniEPDG es un ePDG (evolved Packet Data Gateway) conforme a 3GPP que habilita la llamada por WiFi al conectar el acceso WiFi no confiable a la red central móvil. Soporta dos modos operativos: **modo GTP** para tunelización PGW y **modo VPN Simple** para salida de IP local.

Enlaces Rápidos

Configuración y Despliegue

- **Requisitos de Red** - Puertos de firewall y entradas DNS requeridas para el despliegue
- **Referencia de Configuración** - Documentación completa de parámetros para IKEv2, Diameter, modos VPN y todas las configuraciones en tiempo de ejecución
- **Descripción General de la Arquitectura** - Arquitectura del sistema, flujos de llamadas, máquinas de estado y referencias de protocolo

Operaciones y Monitoreo

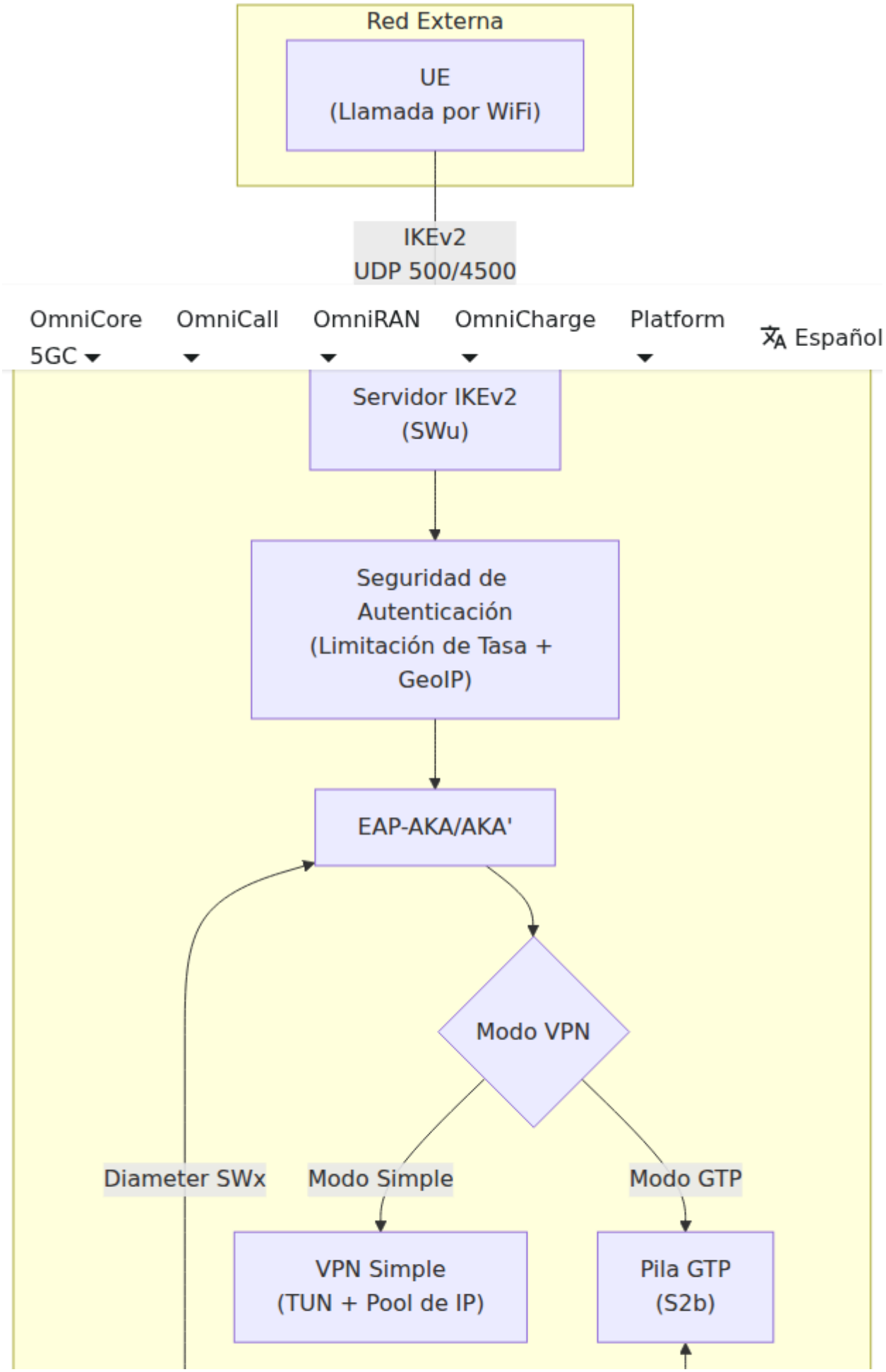
- **Panel de Control** - Interfaz de monitoreo basada en web para sesiones, pares Diameter y registros
- **Referencia de Métricas** - Métricas de Prometheus, consultas de ejemplo y reglas de alerta
- **Solución de Problemas** - Problemas comunes, procedimientos de diagnóstico y pasos de resolución

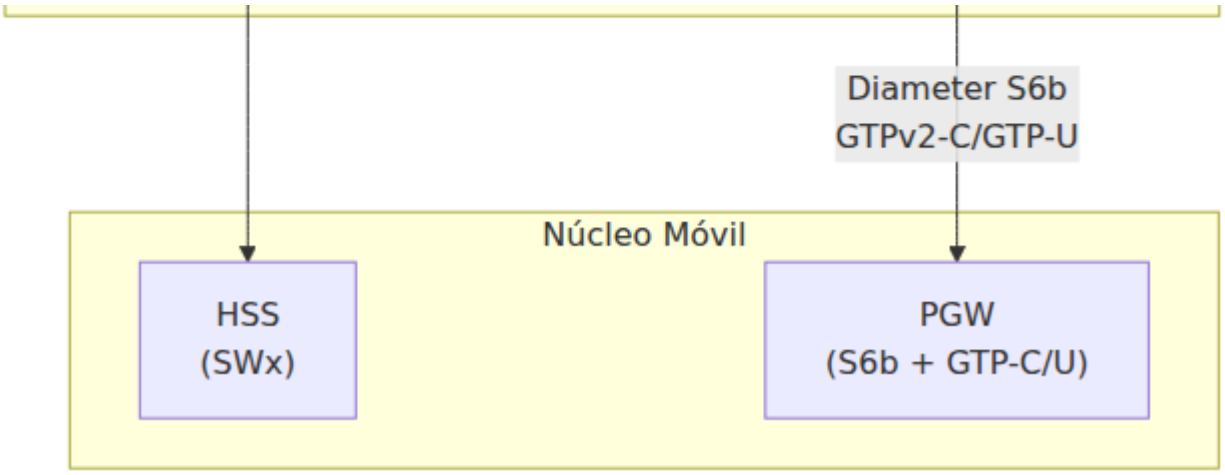
Seguridad

- **Seguridad de Autenticación** - Limitación de tasa y bloqueo de países por GeoIP

Descripción General de la

Arquitectura


Red Externa
UE
(Llamada por WiFi)
IKEv2
UDP 500/4500
OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platform
Español
Servidor IKEv2
(SWu)
Seguridad de
Autenticación
(Limitación de Tasa +
GeoIP)
EAP-AKA/AKA'
Modo VPN
Diameter SWx
Modo Simple
Modo GTP
VPN Simple
(TUN + Pool de IP)
Pila GTP
(S2b)



Modos Operativos

OmniEPDG soporta dos modos operativos seleccionados a través del parámetro de configuración `vpn_mode`.

Modo GTP

Tunelización completa 3GPP a través de un PGW. El tráfico del suscriptor se encapsula en GTP-U y se enruta a través del núcleo móvil.

Usar cuando:

- Integración con infraestructura de núcleo móvil existente
- Políticas y cobros a través de PCRF/PCEF
- Se requiere roaming y transferencia entre operadores

Componentes:

- Diameter S6b para autorización de sesión PGW
- GTPv2-C para gestión de sesiones (Crear/Eliminar/Modificar Sesión)
- Módulo GTP-U del kernel de Linux para el plano de usuario

Modo VPN Simple

Salida de IP local a través de la interfaz TUN. El tráfico del suscriptor se enruta directamente a través del host de OmniEPDG sin la participación del PGW.

Usar cuando:

- Despliegue independiente sin PGW
- Pruebas y desarrollo
- Escenarios de salida local

Componentes:

- Gestión de pool de IP local (IPv4/IPv6)
- Interfaz TUN (`omniepdg0`) con rutas de host por suscriptor
- NAT/mascarada opcional para acceso a internet

Seguridad de Autenticación

OmniEPDG incluye características de seguridad integradas para proteger contra ataques de fuerza bruta y restringir el acceso por ubicación geográfica. Consulte la guía de Seguridad de Autenticación para más detalles.

Limitación de Tasa

Protege contra ataques de fuerza bruta al rastrear intentos de autenticación fallidos:

- **Limitación por IP** - Bloquea IPs después de 10 fallos en 1 minuto (bloqueo de 5 minutos)
- **Limitación por IMSI** - Bloquea IMSIs después de 5 fallos en 1 minuto (bloqueo de 10 minutos)
- Algoritmo de ventana deslizante con expiración automática
- La autenticación exitosa borra el historial de fallos

Bloqueo de Países por GeoIP

Control de acceso geográfico opcional utilizando la base de datos MaxMind GeoLite2:

- **Modo de lista blanca** - Solo permite conexiones de países especificados
- **Modo de lista negra** - Bloquea conexiones de países especificados
- Manejo configurable de IPs desconocidas/privadas

- Comportamiento de falla abierta o cerrada cuando la base de datos no está disponible

Configuración Clave

Configuración Mínima (Modo 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}
    ]
  }
```

Habilitar Seguridad de Autenticación

```
config :omniepdg,
  # Limitación de tasa (habilitada por defecto con estos valores)
  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,

  # Bloqueo por GeoIP (deshabilitado por defecto)
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ"]
```

Consulte la Referencia de Configuración para la documentación completa de parámetros.

Monitoreo

Panel de Control

Acceda al panel de control web en `http://<host>:4000/dashboard` para:

- Monitoreo de sesiones en tiempo real
- Estado de pares Diameter
- Transmisión de registros en vivo
- Configuración del sistema

Consulte la guía del Panel de Control para más detalles.

Métricas de Prometheus

Recopile métricas de `http://<host>:9568/metrics` para:

- Tasas de éxito/fallo de autenticación
- Eventos del ciclo de vida de la sesión
- Latencia de señalización Diameter
- Eventos de seguridad (limitación de tasa, bloqueos por GeoIP)
- Utilización del pool de IP
- Estadísticas del plano de datos ESP

Consulte la Referencia de Métricas para consultas y reglas de alerta.

Solución de Problemas

Problemas comunes y pasos de resolución:

Problema	Verificación Rápida	Sección de la Guía
Fallos de autenticación	Verifique SWx MAR/MAA en los registros	Fallos de Autenticación
Problemas de conexión Diameter	Verifique el estado de los pares en el panel de control	Conectividad Diameter
Fallos de túnel GTP	Verifique los códigos de causa GTPv2-C	Fallos de Túnel GTP
Problemas de VPN Simple	Verifique la interfaz TUN y las rutas	Fallos de VPN Simple
Falsos positivos de limitación de tasa	Ajuste los umbrales	Problemas de Limitación de Tasa
Problemas de bloqueo por GeoIP	Verifique la base de datos y los códigos de país	Problemas de GeoIP

Consulte la guía de Solución de Problemas para procedimientos de diagnóstico detallados.

Índice de Documentación

Documento	Descripción
Arquitectura	Diseño del sistema, máquinas de estado, flujos de llamadas, referencias de protocolo
Configuración	Referencia de configuración completa con ejemplos
Panel de Control	Guía de interfaz web con capturas de pantalla
Métricas	Métricas de Prometheus, consultas y alertas
Requisitos de Red	Puertos de firewall y entradas DNS para el despliegue
Seguridad	Limitación de tasa y bloqueo de países por GeoIP
Solución de Problemas	Problemas comunes y procedimientos de diagnóstico

Arquitectura y Flujos de Llamadas de OmniEPDG

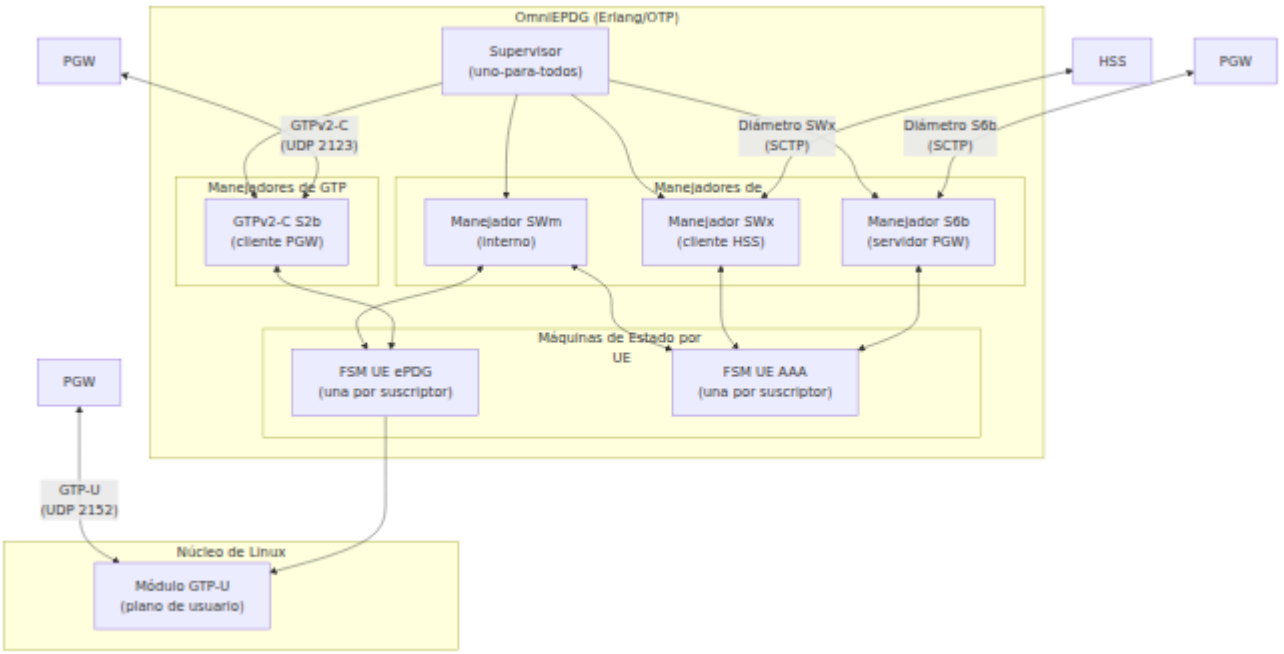
Este documento describe la arquitectura interna de OmniEPDG, sus interfaces de protocolo, máquinas de estado de UE y diagramas de secuencia de mensajes detallados para procedimientos clave. OmniEPDG admite dos modos operativos: **modo GTP** (túnel completo 3GPP a través de PGW) y **modo VPN Simple** (salida local con interfaz TUN). Consulte la Guía de Operaciones para una comparación de alto nivel.

Arquitectura del Sistema

OmniEPDG está construido sobre Erlang/OTP e implementa la función de red ePDG (evolved Packet Data Gateway) de 3GPP. Conecta el acceso WiFi no confiable a la red central móvil, permitiendo a las UEs realizar y recibir llamadas VoWiFi.

Arquitectura del Modo GTP

En el modo GTP, el tráfico de suscriptores se encapsula a través de un PGW utilizando GTPv2-C para el control de sesión y el módulo GTP-U del núcleo de Linux para el plano de usuario.



Arquitectura del Modo VPN Simple

En el modo VPN Simple, el tráfico de suscriptores se enruta localmente a través de una interfaz TUN de Linux. No se requiere infraestructura de PGW o GTP. Los componentes de Diámetro S6b, GTPv2-C y GTP-U son reemplazados por el subsistema VPN Simple.

Árbol de Supervisores

OmniEPDG utiliza una estrategia de supervisor **uno-para-todos**, lo que significa que si cualquier proceso hijo falla, todos los hijos se reinician. El supervisor inicia condicionalmente diferentes procesos hijos dependiendo del modo operativo.

Procesos iniciados en ambos modos:

Proceso	Rol	Descripción
`aaa_diameter_swx`	Cliente Diámetro SWx	Se conecta al HSS para autenticación y operaciones de perfil de suscriptor
`aaa_diameter_swm`	Diámetro SWm (Interno)	Enruta mensajes EAP de Diámetro y de sesión entre el ePDG y las FSM de AAA
`epdg_diameter_swm`	Manejador SWm ePDG	Maneja el lado ePDG del señalamiento de Diámetro interno SWm

Procesos adicionales en modo GTP:

Proceso	Rol	Descripción
`aaa_diameter_s6b`	Servidor Diámetro S6b	Acepta conexiones del PGW para autorización de sesión
`epdg_gtpc_s2b`	Cliente GTPv2-C	Envía solicitudes de Crear/Eliminar Sesión al PGW a través de S2b
`gtp_u_kmod`	Manejador del Núcleo GTP-U	Gestiona los contextos PDP GTP-U en el módulo del núcleo de Linux

Procesos adicionales en modo VPN Simple:

Proceso	Rol	Descripción
`simple_vpn_supervisor`	Supervisor del Subsistema VPN	Supervisa los procesos del administrador de IP pool y del administrador de rutas
`simple_vpn_pool`	Administrador de IP Pool	Asigna y libera direcciones IPv4 del pool CIDR configurado utilizando ETS
`simple_vpn_route`	Administrador de Rutas	Crea la interfaz TUN `omniepdg0` y gestiona las rutas de host por suscriptor

Máquinas de Estado por UE

Para cada suscriptor activo (identificado por IMSI), OmniEPDG crea dos instancias de máquina de estado:

- **FSM UE ePDG** (`epdg_ue_fsm`) - Gestiona el ciclo de vida de la sesión del suscriptor desde la perspectiva del ePDG: autenticación, creación de túneles GTP y coordinación de desmantelamiento
- **FSM UE AAA** (`aaa_ue_fsm`) - Gestiona el señalamiento del lado AAA: intercambios de Diámetro SWx con el HSS y intercambios S6b con el PGW

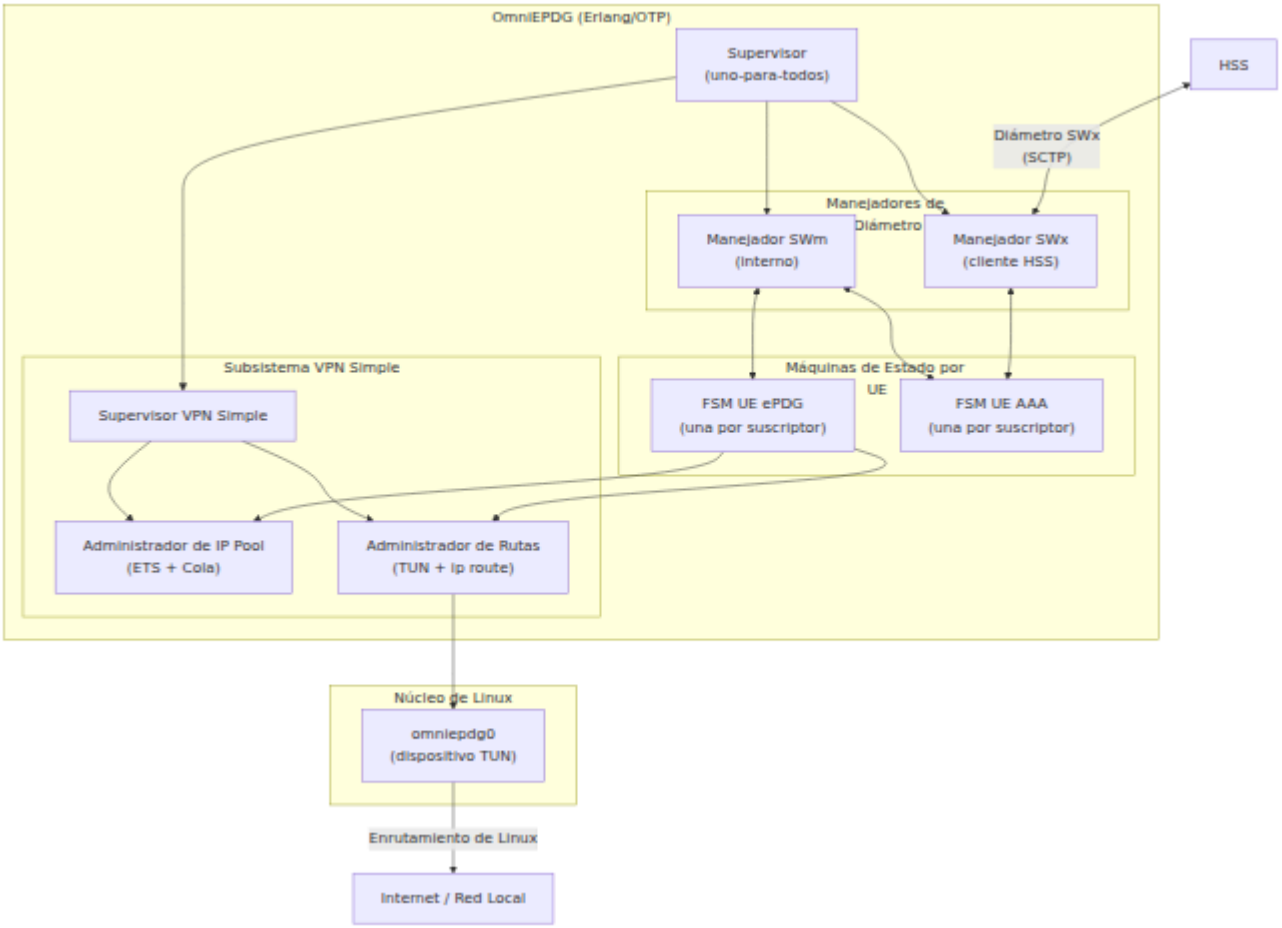
Ambas FSM se implementan como procesos `gen_statem` de Erlang con modo de devolución de llamada de función de estado.

Estados de la FSM UE ePDG

La FSM UE ePDG rastrea la sesión de un suscriptor desde la solicitud de autenticación inicial hasta el estado de túnel activo y el desmantelamiento. El comportamiento de la FSM diverge en el estado `authenticated` según el modo operativo.

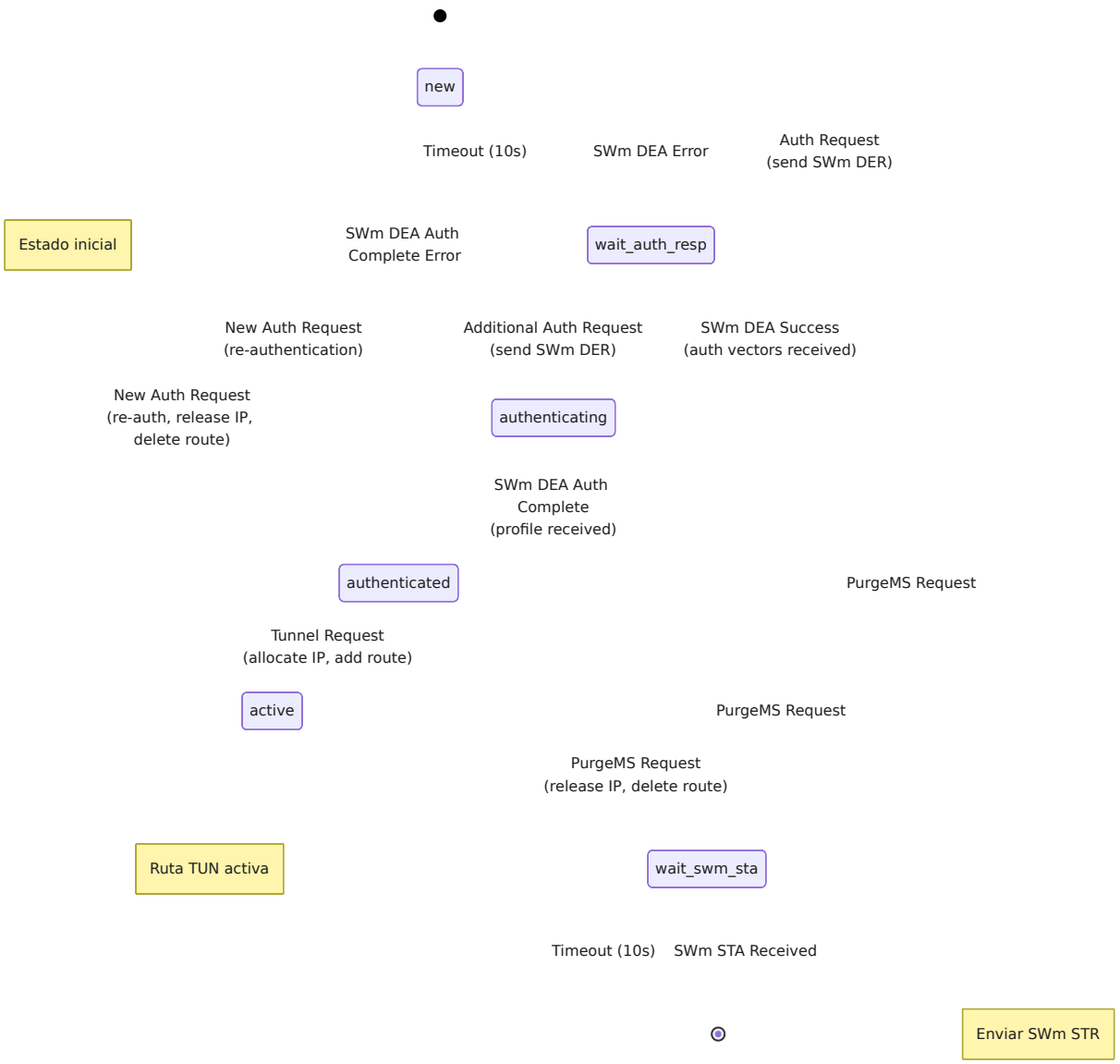
FSM del Modo GTP

En el modo GTP, el establecimiento del túnel pasa por la creación de sesión GTPv2-C al PGW, y el desmantelamiento implica la eliminación de sesión GTPv2-C, eliminación de bearer iniciada por PGW y flujos de deregistro iniciados por HSS.



FSM del Modo VPN Simple

En el modo VPN Simple, la FSM toma un atajo en el estado `authenticated`. En lugar de enviar una solicitud de creación de sesión GTPv2-C, la FSM asigna una dirección IP del pool local, crea una ruta de host en la interfaz TUN y transita directamente a `active`. Los estados de desmantelamiento específicos de GTP (`wait_create_session_resp`, `wait_delete_session_resp`, `dereg_pgw_wait_cancel`, `dereg_net_wait_s2b_delete`) no se utilizan.


new
Timeout (10s)
SWm DEA Error
Auth Request
(send SWm DER)
Estado inicial
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)
Ruta TUN activa
wait_swm_sta
Timeout (10s)
SWm STA Received
Enviar SWm STR

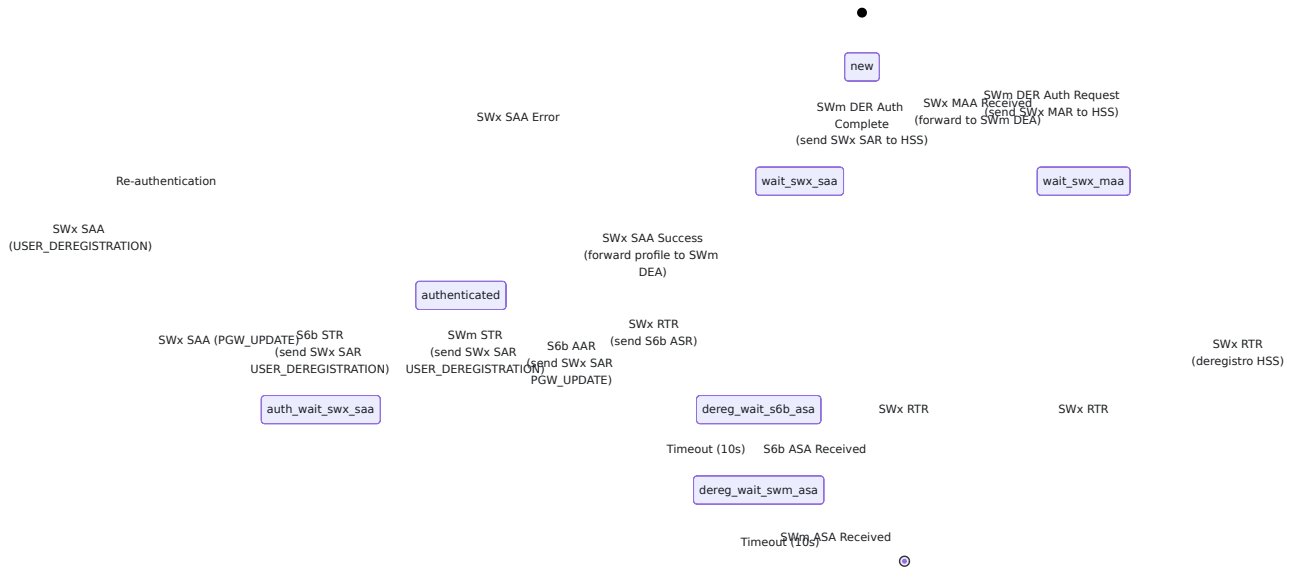
Referencia de Estados de la FSM UE ePDG

Estado	Modo	Descripción	Esperand
`new`	Ambos	Estado inicial. Sin sesión activa.	Solicitud de autenticación UE
`wait_auth_resp`	Ambos	Solicitud de autenticación enviada a través de SWm DER.	SWm DEA cor vectores de autenticación error
`authenticating`	Ambos	Vectores de autenticación recibidos, intercambio EAP en progreso.	Actualización ubicación / finalización de autenticación
`authenticated`	Ambos	Autenticación completa, perfil de suscriptor descargado.	Solicitud de tú de UE
`wait_create_session_resp`	GTP	Solicitud de creación de sesión GTPv2-C enviada al PGW.	Respuesta de creación de se del PGW
`active`	Ambos	Túnel/ruta operativo. El tráfico del suscriptor está fluyendo.	Activador de desmantelam
`wait_delete_session_resp`	GTP	Solicitud de eliminación de	Respuesta de eliminación de

Estado	Modo	Descripción	Esperand
		sesión GTPv2-C enviada al PGW (desmantelamiento iniciado por UE).	sesión del PG
`wait_swm_sta`	Ambos	Solicitud de terminación de sesión SWm enviada.	SWm STA de A
`dereg_pgw_wait_cancel`	GTP	Deregistro iniciado por PGW. Ubicación de cancelación enviada a UE.	Resultado de ubicación de cancelación
`dereg_net_wait_cancel`	GTP	Deregistro iniciado por la red/HSS. Ubicación de cancelación enviada a UE.	Resultado de ubicación de cancelación
`dereg_net_wait_s2b_delete`	GTP	Deregistro iniciado por la red. S2b Delete Session enviado al PGW.	Respuesta de eliminación de sesión

Estados de la FSM UE AAA

La FSM UE AAA gestiona el señalamiento de Diámetro hacia el HSS (SWx) y PGW (S6b) en nombre de cada suscriptor.


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
(deregistro 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

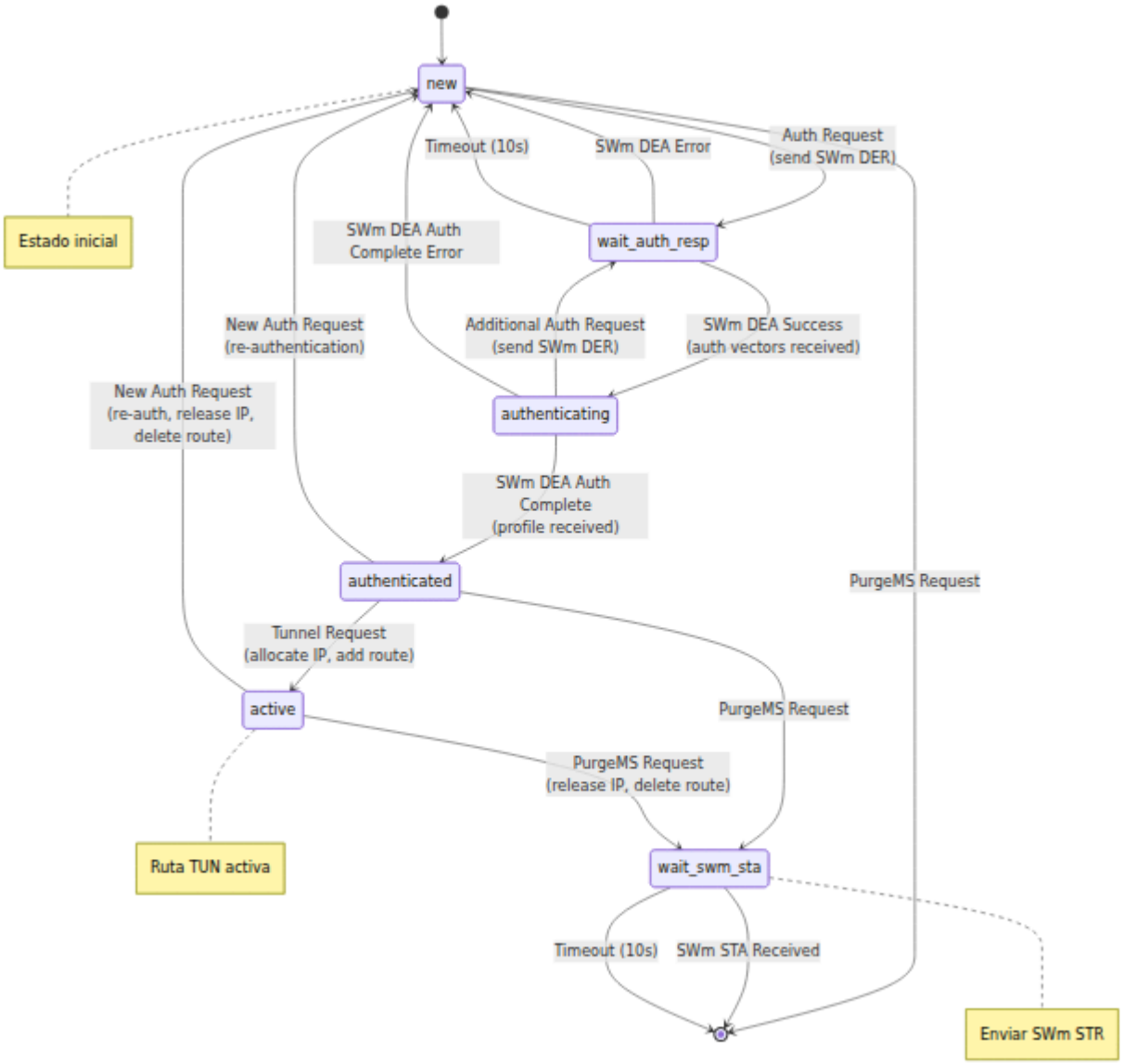
Referencia de Estados de la FSM UE AAA

Estado	Descripción	Esperando
`new`	Estado inicial. Sin sesión AAA activa.	Solicitud de autenticación de Diámetro
`wait_swx_maa`	SWx MAR enviado al HSS para vectores EAP-AKA.	SWx MAA del HSS
`wait_swx_saa`	SWx SAR enviado al HSS para asignación de servidor.	SWx SAA del HSS
`authenticated`	Ambas sesiones ePDG y PGW pueden estar activas. Rastrea el estado de sesión dual.	Eventos de sesión
`auth_wait_swx_saa`	SWx SAR enviado para actualización de PGW o deregistro de usuario.	SWx SAA del HSS
`dereg_net_wait_s6b_asa`	Deregistro iniciado por HSS. S6b ASR enviado al PGW.	S6b ASA del PGW
`dereg_net_wait_swm_asa`	Desmantelamiento de S6b completo. SWm ASR enviado al ePDG.	SWm ASA del ePDG

Flujos de Llamadas

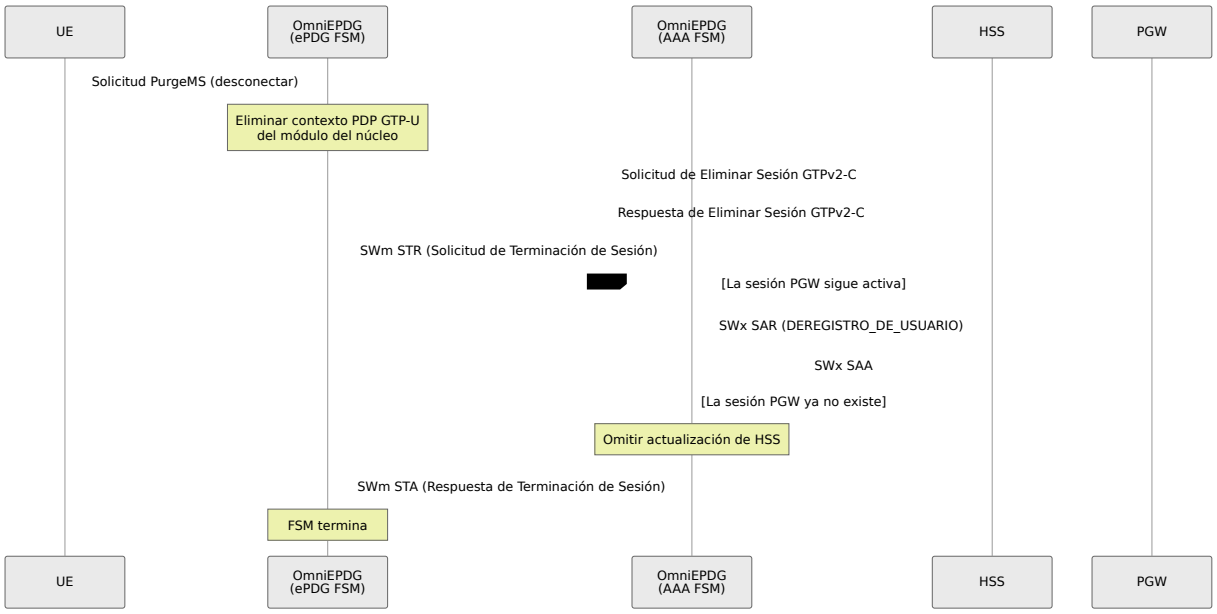
Modo GTP: Establecimiento de Sesión Exitoso

Esta secuencia muestra una sesión completa exitosa desde la autenticación EAP-AKA hasta un túnel GTP activo.



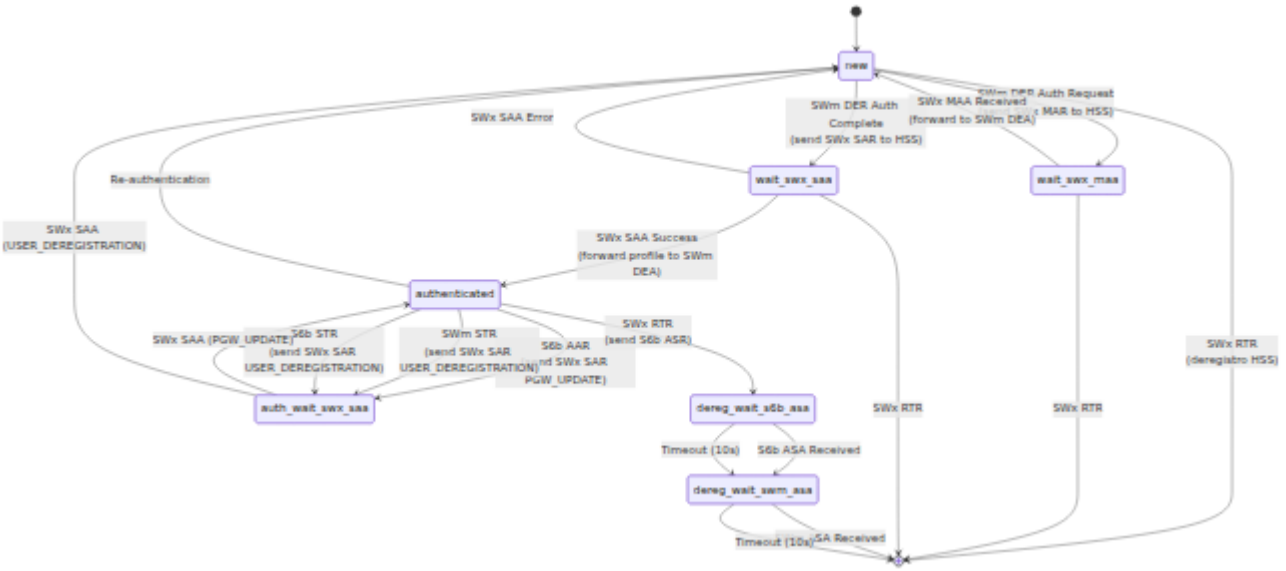
Modo GTP: Desmantelamiento de Sesión Iniciado por UE

Cuando la UE se desconecta (por ejemplo, cambia de WiFi a celular o el usuario cuelga).



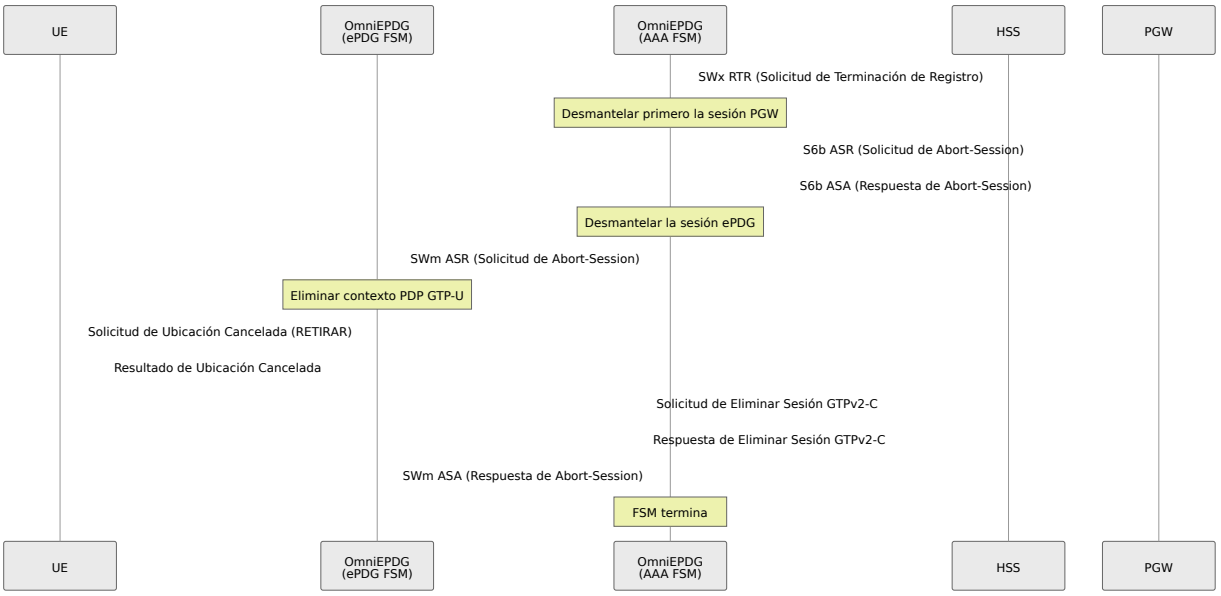
Modo GTP: Desmantelamiento de Sesión Iniciado por PGW

Cuando el PGW termina la sesión (por ejemplo, violación de políticas, tiempo de espera o acción administrativa).



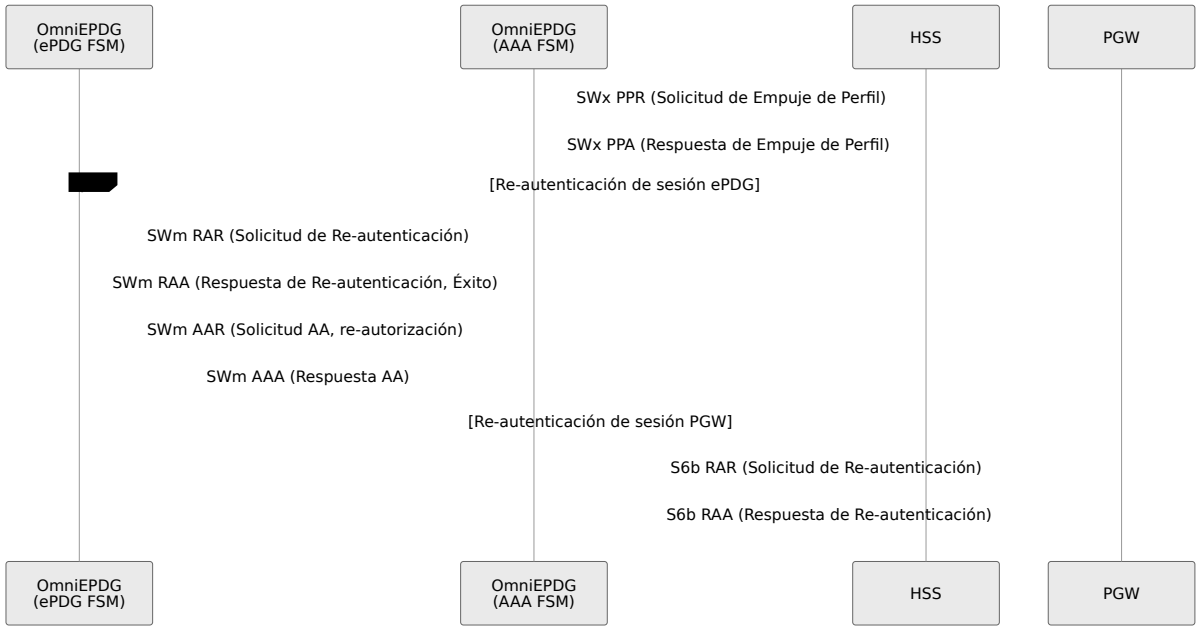
Modo GTP: Deregistro Iniciado por la Red (HSS)

Cuando el HSS revoca el registro de un suscriptor (por ejemplo, cambio de suscripción, detección de fraude o acción administrativa).



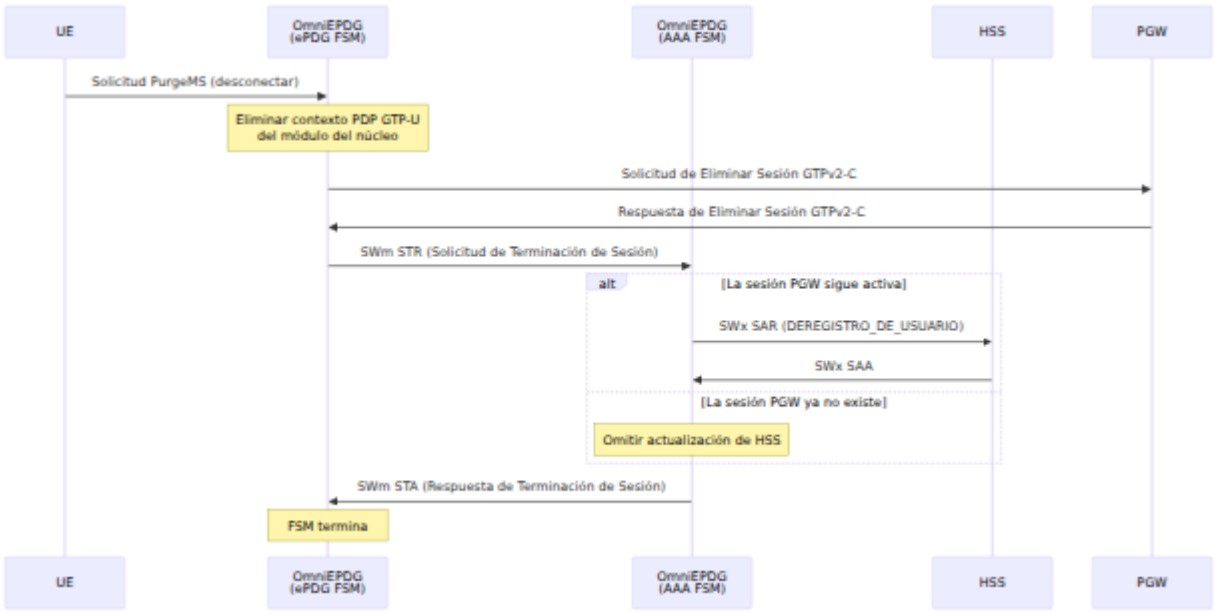
Modo GTP: Empuje de Perfil HSS y Re-autenticación

Cuando el HSS envía un perfil de suscriptor actualizado, OmniEPDG activa la re-autenticación en ambas sesiones ePDG (SWm) y PGW (S6b) según 3GPP TS 29.273 Sección 8.1.2.3.3.



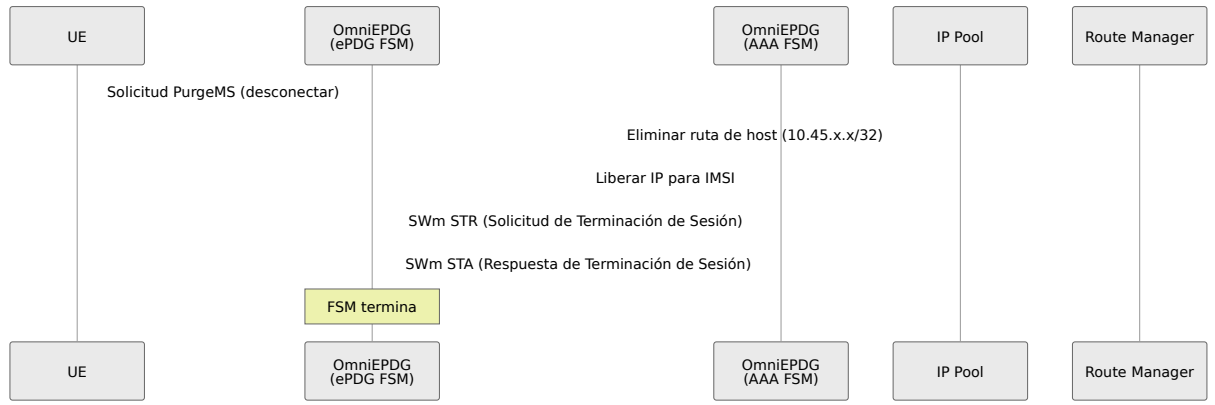
Modo VPN Simple: Establecimiento de Sesión Exitoso

En el modo VPN Simple, el establecimiento de sesión es más corto. Después de la autenticación EAP-AKA, la FSM ePDG asigna una IP del pool local y configura una ruta de host en la interfaz TUN, eludiendo toda interacción con el PGW. Si `skip_sar` está habilitado, el intercambio SAR/SAA con el HSS también se omite.



Modo VPN Simple: Desmantelamiento de Sesión Iniciado por UE

Cuando la UE se desconecta en modo VPN Simple, la FSM libera la dirección IP asignada y elimina la ruta de host.



Identificadores de Aplicación de Diámetro

Identificador de Aplicación	Interfaz	Identificador de Proveedor	Descripción	Referencia
16777265	SWx	10415 (3GPP)	ePDG ↔ HSS autenticación y gestión de suscriptores	3GPP TS 29.273
16777272	S6b	10415 (3GPP)	AAA ↔ PGW autorización de sesión	3GPP TS 29.273

Códigos de Resultado de Diámetro

OmniEPDG mapea los códigos de resultado de Diámetro a valores de causa internos para la propagación de errores entre protocolos.

Códigos de Resultado Estándar

Código de Resultado	Nombre	Significado
2001	DIAMETER_SUCCESS	Operación completada con éxito
2002	DIAMETER_LIMITED_SUCCESS	Operación parcialmente exitosa

Códigos de Resultado Experimentales de 3GPP

Código de Resultado	Nombre	Significa
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	HSS temporalm no puede proporcion datos de autenticac
5001	DIAMETER_ERROR_USER_UNKNOWN	IMSI del suscriptor encontrad HSS
5002	DIAMETER_UNKNOWN_SESSION_ID	Sesión no encontrad (utilizada p STR/AAR obsoletos)
5003	DIAMETER_AUTHORIZATION_REJECTED	Suscriptor autorizado para el ser
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	Se aplican restriccion de roamin
5005	DIAMETER_MISSING_AVP	AVP reque faltante er mensaje
5012	DIAMETER_UNABLE_TO_COMPLY	Fallo gené de

Código de Resultado	Nombre	Significa
		procesami
5420	DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION	No se enc ninguna suscripció EPS
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	Tecnología acceso no permitida
5422	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	IMEI del dispositivo reconocid

Códigos de Causa GTPv2-C (Solo Modo GTP)

OmniEPDG maneja los siguientes códigos de causa GTPv2-C en las respuestas de Crear/Eliminar Sesión del PGW. Los códigos 1-15 son informativos, 16-63 indican éxito y 64+ indican errores. Consulte 3GPP TS 29.274 Sección 8.4.

Causas de Éxito

Código	Nombre	Descripción
16	Request Accepted	Operación completada con éxito
17	Request Accepted Partially	Éxito parcial
18	New PDN Type (Network Preference)	Tipo de PDN cambiado debido a preferencia de red
19	New PDN Type (Single Address Bearer)	Tipo de PDN cambiado debido a restricción de bearer de dirección única

Causas de Error (Seleccionadas)

Código	Nombre	Descripción
64	Context Not Found	Contexto de sesión no encontrado en PGW
73	No Resources Available	Agotamiento de recursos en PGW
78	Missing or Unknown APN	APN solicitado no configurado en PGW
82	Denied in RAT	Tecnología de acceso no permitida
84	All Dynamic Addresses Occupied	Pool de direcciones IP agotado en PGW
92	User Authentication Failed	Fallo de autenticación en PGW
93	APN Access Denied	Suscriptor no autorizado para APN
96	IMSI/IMEI Not Known	Identidad del suscriptor no reconocida
109	Invalid Peer	Validación de par fallida
113	APN Congestion	APN sobrecargado
120	GTP-C Entity Congestion	Sobrecarga del plano de control del PGW

Formato NAI

OmniEPDG identifica a los suscriptores utilizando el formato de Identificador de Acceso a la Red (NAI) definido en 3GPP TS 23.003 Sección 19:

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

Prefijo de Identidad y Tipo de Autenticación

El prefijo NAI determina el método de autenticación EAP según 3GPP TS 23.003:

Prefijo	Tipo de Autenticación	Descripción
`0`	EAP-AKA	Autenticación AKA estándar (más común para llamadas WiFi)
`6`	EAP-AKA'	Autenticación AKA mejorada con vinculación a la red

OmniEPDG selecciona automáticamente el método de autenticación basado en el prefijo de identidad de la UE. La mayoría de las UEs utilizan el prefijo `0` (EAP-AKA) para llamadas WiFi.

OmniEPDG extrae el IMSI del NAI analizando todo entre el prefijo y el símbolo `@`. El IMSI se utiliza como la clave principal para todas las máquinas de estado y operaciones de señalización por suscriptor.

Algoritmos Criptográficos

OmniEPDG implementa algoritmos criptográficos según 3GPP TS 33.402 y RFC 7296 (IKEv2).

Algoritmos de Cifrado IKEv2

Algoritmo	ID	Tamaño de Clave	Estado	Referencia
AES-CBC	12	128, 192, 256 bits	Soportado (predeterminado: 256)	RFC 3602
AES-GCM-16	20	128, 192, 256 bits	Soportado	RFC 5282
AES-GCM-12	19	128, 192, 256 bits	Soportado	RFC 5282
AES-GCM-8	18	128, 192, 256 bits	Soportado	RFC 5282
3DES	3	192 bits	Soportado (legado)	RFC 2451

Algoritmos de Integridad IKEv2

Algoritmo	ID	Tamaño de Clave	Tamaño de ICV	Estado	Referencia
HMAC-SHA2-256-128	12	256 bits	128 bits	Soportado (predeterminado)	RFC 4868
HMAC-SHA2-384-192	13	384 bits	192 bits	Soportado	RFC 4868
HMAC-SHA2-512-256	14	512 bits	256 bits	Soportado	RFC 4868
AES-XCBC-96	5	128 bits	96 bits	Soportado	RFC 3566
HMAC-SHA1-96	2	160 bits	96 bits	Soportado (legado)	RFC 2404
HMAC-MD5-96	1	128 bits	96 bits	Soportado (legado)	RFC 2403

AES-XCBC-96 (`AUTH_AES_XCBC_96`) es requerido por algunos teléfonos, notablemente ciertos clientes Samsung VoWiFi, que lo ofrecen como su único transformador de integridad. Se implementa según RFC 3566 con el manejo de clave variable y la truncación de nonce SKEYSEED definidas en RFC 4434 y RFC 7296 Sección 2.14.

Algoritmos PRF IKEv2

Algoritmo	ID	Tamaño de Salida	Estado	Referencia
PRF-HMAC-SHA2-256	5	256 bits	Soportado (predeterminado)	RFC 4868
PRF-HMAC-SHA2-384	6	384 bits	Soportado	RFC 4868
PRF-HMAC-SHA2-512	7	512 bits	Soportado	RFC 4868
PRF-AES128-XCBC	4	128 bits	Soportado	RFC 4434
PRF-HMAC-SHA1	2	160 bits	Soportado (legado)	RFC 2104
PRF-HMAC-MD5	1	128 bits	Soportado (legado)	RFC 2104

Cuando se negocia `PRF-AES128-XCBC`, SKEYSEED se deriva solo de los primeros 64 bits de cada uno de Ni y Nr (según RFC 7296 Sección 2.14), mientras que los nonce completos alimentan la expansión de clave prf+.

Grupos de Diffie-Hellman IKEv2

Grupo	ID	Tamaño	Estado	Referencia
MODP-2048	14	2048 bits	Soportado (predeterminado)	RFC 3526
MODP-1024	2	1024 bits	Soportado (legado)	RFC 2409
MODP-1536	5	1536 bits	Soportado	RFC 3526
MODP-3072	15	3072 bits	Soportado	RFC 3526
MODP-4096	16	4096 bits	Soportado	RFC 3526
ECP-256	19	256 bits	Soportado	RFC 5903
ECP-384	20	384 bits	Soportado	RFC 5903
ECP-521	21	521 bits	Soportado	RFC 5903
Curve25519	31	256 bits	Soportado	RFC 8031
Curve448	32	448 bits	Soportado	RFC 8031

Algoritmos ESP (Child SA)

Los algoritmos de túnel ESP se negocian a partir de la propuesta de SA que la UE ofrece en IKE_AUTH (y en CREATE_CHILD_SA en rekey). OmniEPDG selecciona un transformador que la UE realmente ofreció y deriva las claves de Child SA con los tamaños de clave y ICV coincidentes. No impone un conjunto fijo.

Tipo	Algoritmos	Notas
Cifrado	AES-CBC-128 / 192 / 256	El cifrado sigue la longitud de clave negociada
Integridad	HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256, AES-XCBC-96, HMAC-SHA1-96	El ICV de AES-XCBC-96 es de 12 bytes (frente a 16 para HMAC-SHA2-256-128)

Fallback (solo cuando la propuesta de la UE no puede ser analizada):

- Cifrado: AES-CBC-256 (clave de 32 bytes, IV de 16 bytes)
- Integridad: HMAC-SHA2-256-128 (clave de 32 bytes, ICV de 16 bytes)

Funciones Criptográficas EAP-AKA

Función	Algoritmo	Referencia
Derivación de MK	SHA-1	RFC 4187 Sección 7
Expansión de clave PRF+	PRF de FIPS 186-2 (SHA-1)	RFC 4187 Apéndice D
AT_MAC	HMAC-SHA1-128	RFC 4187 Sección 10.15
Milenage (f1-f5)	AES-128	3GPP TS 35.206

Funciones Criptográficas EAP-AKA'

Función	Algoritmo	Referencia
Derivación de CK'/IK'	HMAC-SHA-256	RFC 5448 Sección 3.3
Derivación de MK	SHA-256	RFC 5448 Sección 3.4
AT_MAC	HMAC-SHA256-128	RFC 5448 Sección 3.1

Cumplimiento de 3GPP

OmniEPDG implementa todos los algoritmos criptográficos obligatorios especificados en 3GPP TS 33.402 Sección 8:

Requisito	Algoritmo	Estado
Cifrado IKEv2 (obligatorio)	AES-CBC-128	✓ Soportado
Integridad IKEv2 (obligatorio)	HMAC-SHA2-256-128	✓ Soportado (predeterminado)
PRF IKEv2 (obligatorio)	PRF-HMAC-SHA-256	✓ Soportado (predeterminado)
DH IKEv2 (obligatorio)	Grupo 14 (MODP-2048)	✓ Soportado (predeterminado)
Cifrado ESP (obligatorio)	AES-CBC-128/256	✓ Soportado
Integridad ESP (obligatorio)	HMAC-SHA2-256-128	✓ Soportado (predeterminado)
EAP-AKA	RFC 4187	✓ Implementado
EAP-AKA'	RFC 5448	✓ Implementado

Más allá del conjunto obligatorio, OmniEPDG también admite los transformadores de integridad y PRF AES-XCBC (RFC 3566 / RFC 4434) para interoperabilidad con teléfonos que los ofrecen exclusivamente: por ejemplo, ciertos clientes Samsung VoWiFi, que proponen AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048 y no retrocederán a HMAC-SHA2.

Tipos de Dirección PDP (Solo Modo GTP)

OmniEPDG admite los siguientes tipos de dirección PDP según lo definido en 3GPP TS 29.274 Sección 8.14. En el modo VPN Simple, solo se asignan

direcciones IPv4 del pool local.

Tipo	Descripción	Formato PAA GTPv2-C
IPv4	Bearer solo IPv4	Dirección IPv4 de 4 bytes
IPv6	Bearer solo IPv6	Longitud de prefijo de 1 byte + dirección IPv6 de 16 bytes
IPv4v6	Bearer de doble pila	Longitud de prefijo de 1 byte + dirección IPv6 de 16 bytes + dirección IPv4 de 4 bytes

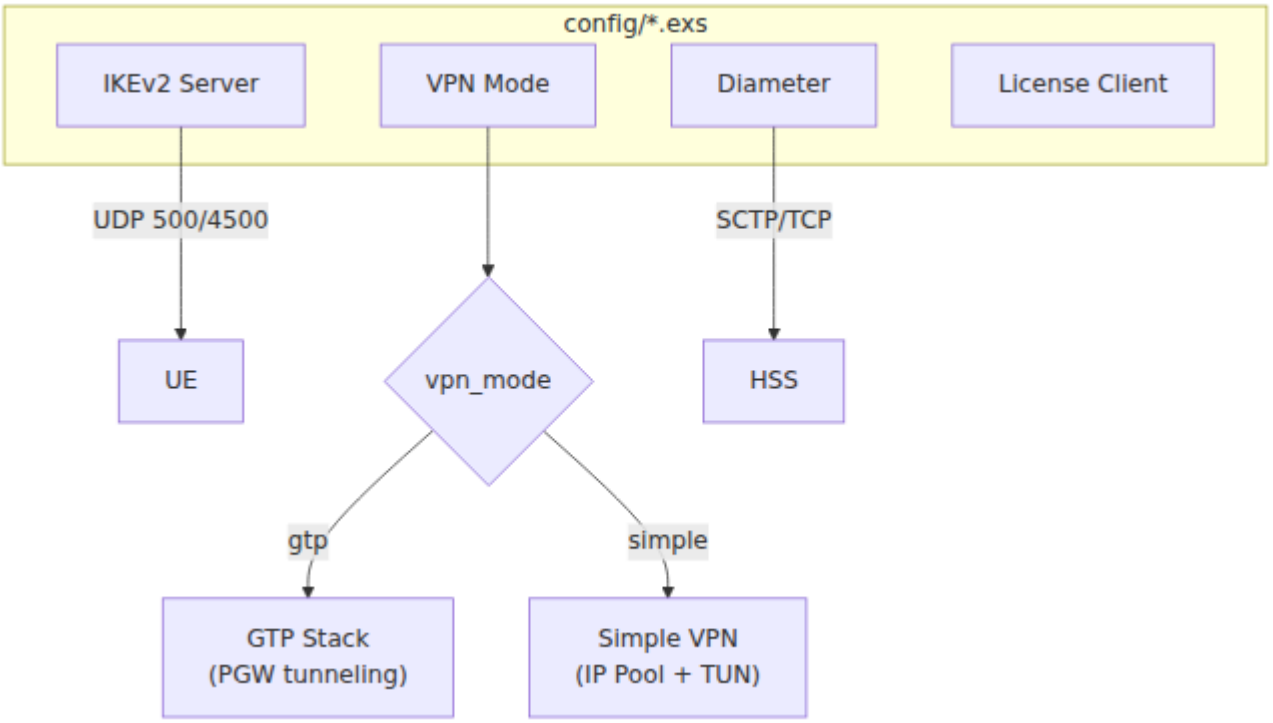
Referencia de Configuración de OmniEPDG

OmniEPDG se configura a través de `config/runtime.exs` y variables de entorno. Toda la configuración orientada al cliente se realiza en tiempo de ejecución; los valores predeterminados de tiempo de compilación están integrados en la versión y no se exponen.

Para implementaciones en contenedores, use las variables de entorno como se documenta en la sección de Referencia de Variables de Entorno.

Tabla de Contenidos

Estructura de Configuración



Archivo de Configuración

Toda la configuración se realiza en `config/runtime.exs`. OmniEPDG lee este archivo cuando se inicia. El archivo admite la sustitución de variables de entorno para implementaciones en contenedores.

Ejemplo de Configuración

```
# config/runtime.exs
config :omniepdg,
  # Configuraciones del servidor IKEv2
  listen_ip: {0, 0, 0, 0},
  port_500: 500,
  port_4500: 4500,

  # Modo VPN: :simple (salida local) o :gtp (PGW a través de GTP-
C)
  vpn_mode: :simple,

  # Configuraciones del modo 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"]
  ]

# Configuración del panel de control
config :control_panel,
  parent_application: :omniepdg,
  parent_application_readable_name: "OmniEPDG",
  use_additional_pages: [
    {OmniEpdg.Web.DashboardLive, "/", "Dashboard"},
    {OmniEpdg.Web.SessionsLive, "/sessions", "Sessions"},
    {OmniEpdg.Web.DiameterLive, "/diameter", "Diameter"}
  ]

# Configuración de Diámetro (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}
    ]
  }

# Configuración del cliente de licencia (runtime.exs)
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

Parámetros del Servidor IKEv2

El servidor IKEv2 maneja la interfaz SWu entre los UEs y OmniEPDG. Termina túneles IPSec y realiza autenticación EAP-AKA.

Parámetro	Tipo	Requerido	Predeter
`listen_ip`	Tupla	No	`{0, 0, 0, 0}`
`port_500`	Entero	No	`500`
`port_4500`	Entero	No	`4500`
`cert_file`	Cadena	Sí	`/etc/omniepdg/`
`key_file`	Cadena	Sí	`/etc/omniepdg/`

Parámetro	Tipo	Requerido	Predete
`session_inactivity_timeout_ms`	Entero	No	`300000`

Parámetros de Seguridad de Autenticación

OmniEPDG incluye protección integrada contra ataques de fuerza bruta y control de acceso geográfico. Consulte la Guía de Seguridad para obtener documentación detallada.

Parámetros de Limitación de Tasa

```
config :omniepdg,
  # Limitación de tasa por IP
  auth_rate_limit_per_ip: 10,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 300_000,

  # Limitación de tasa por IMSI
  auth_rate_limit_per_imsi: 5,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 600_000
```

Parámetro	Tipo	Requerido	Predeterminad
`auth_rate_limit_per_ip`	Entero	No	`10`
`auth_rate_limit_ip_window_ms`	Entero	No	`60000`
`auth_rate_limit_ip_block_ms`	Entero	No	`300000`
`auth_rate_limit_per_imsi`	Entero	No	`5`
`auth_rate_limit_imsi_window_ms`	Entero	No	`60000`
`auth_rate_limit_imsi_block_ms`	Entero	No	`600000`

Parámetro	Tipo	Requerido	Predeterminad

Parámetros de 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
```

Parámetro	Tipo	Requerido	Predeterminado
`geoip_enabled`	Booleano	No	`false`
`geoip_database_path`	Cadena	No	`"/etc/omniepdg/GeoLite2 Country.mmdb"`
`geoip_mode`	Átomo	No	`:whitelist`
`geoip_countries`	Lista	No	`[]`
`geoip_allow_unknown`	Booleano	No	dependiente del modo

Parámetro	Tipo	Requerido	Predeterminado
`geoip_fail_open`	Booleano	No	`true`

Selección del Modo VPN

Parámetro	Tipo	Requerido	Predeterminado	Var de Entorno
`vpn_mode`	Átomo	No	`:simple`	`EPDG_VPN_MODE`

Parámetros de VPN Simple

El bloque de configuración `simple_vpn` controla la asignación de IP y DNS para el modo VPN Simple. OmniEPDG admite tanto grupos de direcciones IPv4 como 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
  ]
```

Parámetro	Tipo	Requerido	Predeterminado
`pool_ipv4`	Cadena	Sí	`"10.45.0.0/16"`
`pool_ipv6`	Cadena	No	`"2001:db8::/32"`
`dns_servers_ipv4`	Lista	No	`["8.8.8.8", "8.8.4.4"]`
`dns_servers_ipv6`	Lista	No	`["2001:4860:4860::8888", "2001:4860:4860::8844"]`
`p_cscf_ipv4`	Lista	No	`[]`

Parámetro	Tipo	Requerido	Predeterminado
`p_cscf_ipv6`	Lista	No	`[]`
`mtu`	Entero	No	`1400`
`nat_enabled`	Booleano	No	`true`

Parámetros de Diámetro

La configuración de Diámetro controla las interfaces SWx (HSS) y S6b (PGW). Cuando `diameter_enabled` es `true`, OmniEPDG inicia la pila de Diámetro y se conecta a los pares configurados.

```
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}
    ]
  }
```

Parámetros del Servicio

Parámetro	Tipo	Requerido	Predeterminado
`service_name`	Átomo	No	`:omniepdg`
`listen_ip`	Cadena	No	`"0.0.0.0"`
`listen_port`	Entero	No	`3868`
`host`	Cadena	Sí	`"epdg"`
`realm`	Cadena	Sí	`"epc.mnc001.mcc001.3gppnetwork.`

Parámetro	Tipo	Requerido	Predeterminado
`product_name`	Cadena	No	`"OmniEPDG"`
`vendor_id`	Entero	No	`10415`

Parámetros de Pares

Cada entrada en la lista `peers` define una conexión de par de Diámetro (típicamente al HSS).

Parámetro	Tipo	Requerido	Predeterminado	Var de Entorno	Des
`host`	Cadena	Sí	-	`HSS_HOST`	Iden Diár par Orig Deb coin la id conf del
`ip`	Cadena	Sí	-	`HSS_IP`	Dire del la c TCP/
`port`	Entero	No	`3868`	`HSS_PORT`	Puer Diár par.
`transport`	Átomo	No	`:tcp`	-	Prot tran `:tc` `:sc`

Identificadores de Aplicación

Aplicación	ID	Vendor ID	Interfaz	Referencia
SWx	16777265	10415	ePDG ↔ HSS	3GPP TS 29.273
S6b	16777272	10415	AAA ↔ PGW	3GPP TS 29.273

Configuración del Cliente de Licencia

El cliente de licencia valida OmniEPDG contra un servidor de licencias.

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

Parámetro	Tipo	Requerido	Predeterminado	Var de Entor
`server_url`	Cadena	Sí	-	`LICENSE_SERVER_`
`product`	Cadena	No	`"omniepdg"`	-

Configuración del Panel de Control

El panel de control web proporciona capacidades de monitoreo y gestión.

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

Parámetro	Tipo	Requerido	Predeterminado	Var de Entorn
`port`	Entero	No	`4000`	`CONTROL_PANEL_PO`

Configuración de Métricas de Prometheus

OmniEPDG expone métricas de Prometheus a través de HTTP para monitoreo y alertas.

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

Parámetro	Tipo	Requerido	Predeterminado	Var de Entorno
`port`	Entero	No	`9568`	`PROMETHEUS_PORT`

Métricas Expuestas

Métricas de Contador (Impulsadas por eventos):

- `epdg_ikev2_session_initiated_count` - Intercambios IKE_SA_INIT iniciados
- `epdg_ikev2_session_established_count` - IKE SAs establecidos con éxito

- `epdg_ikev2_session_failed_count` - Fallos en el establecimiento de IKE SA (por razón)
- `epdg_eap_identity_count` - Solicitudes de identidad EAP
- `epdg_eap_aka_challenge_count` - Desafíos EAP-AKA enviados
- `epdg_eap_aka_success_count` - Autenticaciones EAP-AKA exitosas
- `epdg_eap_aka_failure_count` - Fallos en las autenticaciones EAP-AKA (por razón)
- `epdg_eap_aka_sync_failure_count` - Fallos de sincronización de SQN EAP-AKA
- `epdg_diameter_swx_mar_count` - Solicitudes de autenticación multimedia (por resultado)
- `epdg_diameter_swx_sar_count` - Solicitudes de asignación del servidor (por resultado)
- `epdg_diameter_s6b_aar_count` - Solicitudes AA manejadas (por resultado)
- `epdg_diameter_s6b_str_count` - Solicitudes de terminación de sesión
- `epdg_session_created_count` - Sesiones creadas (por vpn_mode)
- `epdg_session_terminated_count` - Sesiones terminadas (por razón)
- `epdg_esp_packets_in_count` - Paquetes ESP desencriptados
- `epdg_esp_packets_out_count` - Paquetes ESP encriptados
- `epdg_ip_allocated_count` - Direcciones IP asignadas (por tipo)
- `epdg_ip_released_count` - Direcciones IP liberadas (por tipo)

Métricas de Medición (Sondeadas cada 5s):

- `epdg_sessions_active_count` - Total de sesiones activas
- `epdg_sessions_by_state_count` - Sesiones por estado de FSM
- `epdg_ip_pool_allocated_count` - IPs actualmente asignadas
- `epdg_ip_pool_available_count` - IPs disponibles en el grupo
- `epdg_ip_pool_utilization_ratio` - Utilización del grupo (0.0-1.0)
- `epdg_diameter_swx_pending_count` - Solicitudes SWx pendientes
- `epdg_diameter_s6b_active_sessions_count` - Sesiones S6b activas

Métricas de Histograma (Seguimiento de latencia):

- `epdg_auth_duration_ms` - Duración del flujo de autenticación completo

- `epdg_diameter_swx_mar_latency_ms` - Tiempo de respuesta MAR
- `epdg_diameter_swx_sar_latency_ms` - Tiempo de respuesta SAR
- `epdg_session_duration_seconds` - Tiempo de vida de la sesión

Métricas de VM:

- `vm_memory_total` - Memoria total de la VM
- `vm_memory_processes` - Memoria del proceso
- `vm_memory_binary` - Memoria binaria
- `vm_memory_ets` - Memoria de la tabla ETS
- `vm_system_info_process_count` - Procesos en ejecución
- `vm_system_info_port_count` - Puertos abiertos
- `vm_statistics_run_queue` - Cola de ejecución del planificador

Configuración de Sondeo de Prometheus

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

Referencia de Tiempo de Espera

Todos los tiempos de espera internos de FSM están codificados. Estos determinan cuánto tiempo las máquinas de estado esperan respuestas antes de considerarlas fallidas.

Tiempo de Espera	Valor	Modo	Contexto	Descripción
Respuesta GTP	10,000 ms	GTP	FSM UE ePDG	Máximo tiempo de espera para la respuesta de creación/eliminación de sesión GTPv2-C del PGW.
Respuesta SWm	10,000 ms	Ambos	FSM UE ePDG	Máximo tiempo de espera para la respuesta interna de Diámetro SWm (DER/DEA, STR/STA).
Respuesta S6b	10,000 ms	GTP	FSM UE AAA	Máximo tiempo de espera para la respuesta de Diámetro S6b (ASR/ASA).

Referencia de Variables de Entorno

Las variables de entorno se leen en `config/runtime.exs` y sobrescriben los valores predeterminados de tiempo de compilación.

Servidor IKEv2

Variable	Predeterminado	Descripción
`EPDG_LISTEN_IP`	`"0.0.0.0"`	Dirección de enlace del servidor IKEv2 (formato decimal con puntos, por ejemplo, `"10.0.0.1"`).
`EPDG_PORT_500`	`"500"`	Puerto del protocolo IKE.
`EPDG_PORT_4500`	`"4500"`	Puerto de NAT-Traversal de IKE.
`EPDG_CERT_FILE`	`"/etc/omniepdg/certs/epdg.crt"`	Ruta al certificado del servidor IKEv2 (PEM).
`EPDG_KEY_FILE`	`"/etc/omniepdg/certs/epdg.key"`	Ruta a la clave privada del servidor IKEv2 (PEM).
`EPDG_SESSION_TIMEOUT`	`"300000"`	Tiempo de espera de inactividad de la sesión en milisegundos.

Modo VPN

Variable	Predeterminado	Descripción
`EPDG_VPN_MODE`	`"simple"`	Modo VPN: `"simple"` o `"gtp"`.

Diámetro

Variable	Predeterminado	Descripción
`DIA_LISTEN_IP`	`"0.0.0.0"`	Dirección de enlace del oyente de Diámetro.
`DIA_LISTEN_PORT`	`"3868"`	Puerto del oyente de Diámetro.
`DIA_HOST`	`"epdg"`	Host de origen de Diámetro (sin reino).
`DIA_REALM`	`"epc.mnc001.mcc001.3gppnetwork.org"`	Reino de origen de Diámetro.

Par HSS

Variable	Predeterminado	Descripción
`HSS_HOST`	`"hss"`	Identidad de Diámetro del HSS (Host de Origen).
`HSS_IP`	`"127.0.0.1"`	Dirección IP del HSS.
`HSS_PORT`	`"3868"`	Puerto de Diámetro del HSS.

Licencia, Panel de Control y Métricas

Variable	Predeterminado	Descripción
`LICENSE_SERVER_URL`	-	URL de la API del servidor de licencias (requerido).
`CONTROL_PANEL_PORT`	`"4000"`	Puerto HTTP del panel de control.
`PROMETHEUS_PORT`	`"9568"`	Puerto HTTP de métricas de Prometheus (punto final `/metrics`).

Ejemplo: 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"

      # Modo VPN
      EPDG_VPN_MODE: "simple"

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

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

      # Panel de control
      CONTROL_PANEL_PORT: "4000"

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

Panel de Control de OmniEPDG

OmniEPDG incluye un panel de control basado en la web para el monitoreo en tiempo real de sesiones, pares de Diameter y registros del sistema. El panel de control proporciona vistas que se actualizan en vivo sin necesidad de refrescar la página.

Tabla de Contenidos

Accediendo al Panel de Control

El panel de control se sirve en el puerto HTTP configurado (por defecto 4000):

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

Navegación

El panel de control proporciona una barra lateral con enlaces a todas las vistas:

Ruta	Vista	Descripción
`/dashboard`	Tablero	Resumen del sistema y enlaces rápidos
`/sessions`	Sesiones	Lista de sesiones UE activas
`/diameter`	Pares de Diameter	Estado de conexión de pares de Diameter
`/logs`	Registros	Transmisión de registros en tiempo real
`/docs`	Documentos	Navegador de documentación integrada
`/resources`	Recursos	Información sobre BEAM VM y aplicaciones
`/configuration`	Configuración	Visor de configuración del sistema

Tablero

El Tablero proporciona una visión general de alto nivel del estado de OmniEPDG con métricas clave y navegación rápida.

Tarjetas de Estadísticas

El tablero muestra cuatro estadísticas principales:

Estadística	Descripción
Sesiones Activas	Número actual de sesiones UE establecidas
Datos Recibidos (UL)	Total de bytes recibidos de UEs (dirección de subida)
Datos Enviados (DL)	Total de bytes enviados a UEs (dirección de bajada)
Pares de Diameter	Pares conectados / pares configurados totales

Los valores de datos se escalan automáticamente a las unidades apropiadas (B, KB, MB, GB).

Enlaces Rápidos

Navegación directa a vistas detalladas:

- **Ver Sesiones** - Navegar a la vista de Sesiones para información detallada de UE
- **Pares de Diameter** - Navegar a la vista de Pares de Diameter para el estado de conectividad
- **Registros del Sistema** - Navegar a la vista de Registros para transmisión de registros en tiempo real
- **Configuración** - Navegar a la vista de Configuración para ajustes del sistema

Información del Sistema

Muestra la configuración operativa actual:

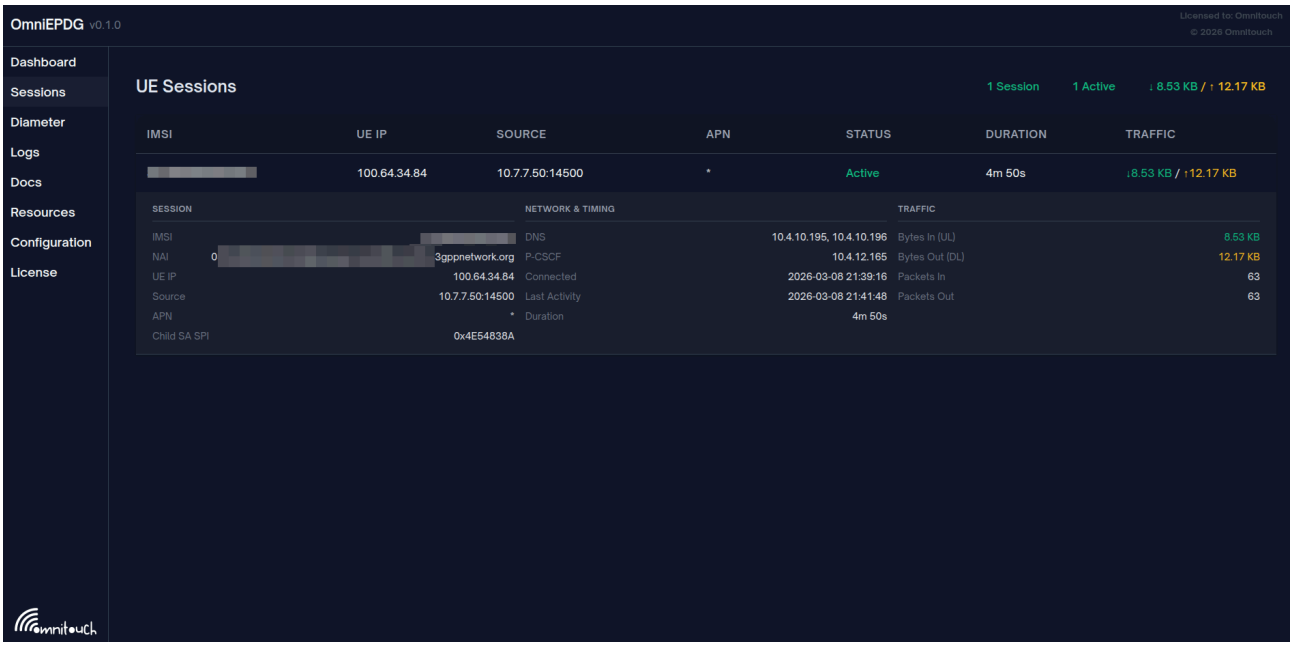
Campo	Descripción
Modo VPN	Modo actual: `GTP` o `SIMPLE`
Puertos IKEv2	Puertos estándar: 500 (IKE), 4500 (NAT-T)
Estado de Diameter	Si el señalamiento de Diameter está habilitado
Pool de IP (IPv4)	CIDR del pool de IP configurado (solo modo VPN Simple)

Actualización Automática

El tablero se actualiza automáticamente cada segundo para mostrar estadísticas actuales.

Vista de Sesiones

La vista de Sesiones muestra todas las sesiones UE activas con información detallada para cada suscriptor.



La vista de Sesiones muestra conexiones UE activas con estadísticas de tráfico en tiempo real y duración de la sesión.

Lista de Sesiones

Cada fila de sesión muestra:

Columna	Descripción
IMSI	Identidad Internacional del Suscriptor Móvil del suscriptor
UE IP	Dirección IPv4/IPv6 asignada
FUENTE	IP y puerto externos del UE (dirección NAT)
APN	Nombre del Punto de Acceso para la conexión
ESTADO	Estado actual de la sesión (Activa/Inactiva)
DURACIÓN	Tiempo desde el establecimiento de la sesión
TRÁFICO	Bytes recibidos / enviados (UL/DL)

Indicadores de Estado

Las sesiones muestran el estado con insignias codificadas por colores:

Estado	Color	Descripción
Activa	Verde	Sesión completamente establecida y operativa
Conectando	Amarillo	Establecimiento de sesión en progreso
Inactiva	Rojo	Sesión terminada o fallida

Detalles de la Sesión

Haz clic en cualquier fila de sesión para expandir información detallada:

Vista de sesión expandida que muestra IMSI, NAI, configuración de red y estadísticas de tráfico.

Sección de Sesión

Campo	Descripción
IMSI	Valor completo de IMSI
NAI	Identificador de Acceso a la Red (formato 3GPP)
UE IP	Dirección IPv4/IPv6 asignada
Fuente	IP y puerto externos del UE (dirección NAT)
APN	Nombre del Punto de Acceso para la conexión PDN
Child SA SPI	Índice de Parámetro de Seguridad de la SA Hijos de IPSec

Sección de Red y Tiempo

Campo	Descripción
DNS	Servidores DNS proporcionados al UE
P-CSCF	Servidores Proxy-CSCF para señalización IMS
Conectado	Marca de tiempo cuando se estableció la sesión
Última Actividad	Marca de tiempo de la actividad de paquete más reciente
Duración	Tiempo desde el establecimiento de la sesión

Sección de Tráfico

Campo	Descripción
Bytes Entrantes (UL)	Total de bytes recibidos del UE (subida)
Bytes Salientes (DL)	Total de bytes enviados al UE (bajada)
Paquetes Entrantes	Total de paquetes recibidos del UE
Paquetes Salientes	Total de paquetes enviados al UE

Estado Vacío

Cuando no hay sesiones activas, la vista muestra:

- Mensaje "No hay sesiones activas"
- Indica si se deben intentar conexiones de UE

Actualización Automática

La lista de sesiones se actualiza automáticamente cada segundo.

Vista de Pares de Diameter

La vista de Pares de Diameter muestra el estado de todos los pares de Diameter configurados (HSS para SWx, PGW para S6b).

Lista de Pares

Cada fila de par muestra:

Columna	Descripción
Par	Identidad de Diameter (Origin-Host)
Dominio	Dominio de Diameter (Origin-Realm)
Dirección IP	Dirección de transporte en formato `protocolo://ip:puerto`
Estado	Estado de conexión

Indicadores de Estado

Estado	Color	Descripción
Conectado	Verde	Conexión de par de Diameter establecida
Desconectado	Rojo	Par no conectado
Desconocido	Gris	No se puede determinar el estado

Resumen de Conteo de Pares

El encabezado muestra conteos agregados:

- **X Conectados** - Número de pares con conexiones activas
- **Y Desconectados** - Número de pares sin conexiones

Detalles del Par

Haz clic en cualquier fila de par para expandir información detallada:

Campo	Descripción
Iniciación de Conexión	Quién inicia: `local` (nosotros conectamos al par) o `remoto` (el par se conecta a nosotros)
Transporte	Protocolo: `tcp` o `sctp`
Nombre del Producto	Nombre del producto publicitado del par desde CER/CEA
Aplicaciones Publicitadas	IDs de Aplicación de Diameter soportadas por el par

Estado Vacío

Cuando no hay pares configurados, la vista muestra:

- "No hay Pares de Diameter configurados" si Diameter está habilitado
- "Diameter está deshabilitado" con sugerencia de configuración si está deshabilitado

Actualización Automática

La lista de pares se actualiza automáticamente cada segundo.

Vista de Registros

La vista de Registros proporciona transmisión en tiempo real de los registros del sistema con capacidades de filtrado y búsqueda.

Visualización de Registros

Los registros aparecen en un contenedor de desplazamiento con las entradas más nuevas en la parte inferior. Cada entrada de registro muestra:

Elemento	Descripción
Marca de tiempo	Cuándo se generó la entrada de registro
Nivel	Nivel de severidad con codificación de color
Mensaje	Contenido del mensaje de registro

Niveles de Registro

Los registros están codificados por colores según la severidad:

Nivel	Color	Descripción
debug	Gris	Información diagnóstica detallada
info	Azul	Mensajes informativos generales
warning	Amarillo	Condiciones de advertencia
error	Rojo	Condiciones de error

Filtrado por Nivel

Filtra los registros por nivel de severidad mínimo usando el menú desplegable:

Filtro	Muestra
Todos los Niveles	debug, info, warning, error
Info+	info, warning, error
Warning+	warning, error
Solo Error	error

Búsqueda

El cuadro de búsqueda filtra los registros en tiempo real:

- Ingresa cualquier texto para filtrar mensajes de registro
- La coincidencia no distingue entre mayúsculas y minúsculas
- Se borra cuando se vacía el cuadro de búsqueda

Controles

Control	Descripción
Pausar/Reanudar	Alternar transmisión de registros encendido/apagado
Limpiar	Eliminar todos los registros mostrados
Desplazamiento automático	Alternar desplazamiento automático a las entradas más nuevas

Búfer de Registros

- Se retienen un máximo de 1000 entradas de registro
- Las entradas más antiguas se eliminan cuando se alcanza el límite
- Limpiar registros elimina todas las entradas de la visualización

Estado Vacío

Cuando no hay registros que coincidan con los filtros actuales:

- Mensaje "No hay registros para mostrar"
- Verifica la configuración de filtros si se esperan registros

Actualización Automática

Los nuevos registros aparecen automáticamente a medida que se generan (cuando no están en pausa).

Vista de Documentos

La vista de Documentos proporciona un navegador de documentación integrada, permitiendo a los operadores acceder a toda la documentación de OmniEPDG directamente desde el panel de control.

Selección de Documentos

Selecciona entre los archivos de documentación disponibles usando la barra de botones:

Documento	Descripción
OPERATIONS.md	Guía de operaciones con inicio rápido y procedimientos
README.md	Resumen del proyecto e instrucciones de configuración
architecture.md	Arquitectura del sistema y flujos de llamadas
configuration.md	Referencia completa de configuración
control-panel.md	Esta guía del panel de control
metrics.md	Referencia de métricas de Prometheus
troubleshooting.md	Problemas comunes y pasos de resolución

Renderización de Markdown

La documentación se renderiza con soporte completo de Markdown incluyendo:

- Encabezados y formato de texto
- Bloques de código con resaltado de sintaxis
- Tablas
- Enlaces (internos y externos)
- Listas y citas en bloque

Vista de Recursos

La vista de Recursos muestra estadísticas de BEAM VM y aplicaciones OTP en ejecución.

Métricas del Sistema

Métrica	Descripción
Uso de Memoria	Memoria total utilizada por BEAM VM
Procesos BEAM	Número de procesos de Erlang/Elixir en ejecución
Tiempo de Actividad	Tiempo desde que se inició la aplicación

Aplicaciones en Ejecución

Lista todas las aplicaciones OTP cargadas agrupadas por categoría:

Categoría	Descripción
Principal	La aplicación OmniEPDG
Sistema	Aplicaciones centrales de Erlang/OTP y Elixir

Haz clic en una aplicación para ver sus detalles, incluyendo versión, descripción y dependencias.

Vista de Configuración

La vista de Configuración muestra la configuración en tiempo de ejecución y las aplicaciones cargadas.

Información del Entorno

Campo	Descripción
Entorno	Entorno de Mix actual (Desarrollo/Producción)
Versión de Elixir	Versión de Elixir en ejecución

Lista de Aplicaciones

Muestra todas las aplicaciones OTP cargadas con sus versiones. Selecciona una aplicación para ver:

- Descripción de la aplicación
- Información de versión
- Dependencias
- Parámetros de configuración

Configuración del Panel de Control

Puerto HTTP

Configura el puerto del panel de control en `config/runtime.exs`:

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

Parámetro	Tipo	Predeterminado	Descripción
`port`	Entero	4000	Puerto HTTP para el panel de control

Deshabilitando el Panel de Control

El panel de control se puede deshabilitar al no iniciar el punto final web en producción si no es necesario. Contacta a tu integrador de sistemas para la configuración específica de implementación.

Referencia de Métricas de OmniEPDG

OmniEPDG expone métricas de Prometheus para monitorear flujos de autenticación, ciclo de vida de sesiones, señalización de Diameter y salud del sistema. Las métricas se sirven a través de HTTP para la recolección por parte de Prometheus.

Tabla de Contenidos

Endpoint de Métricas

OmniEPDG expone métricas en:

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

El endpoint devuelve métricas en formato de exposición de Prometheus, compatible con Prometheus, Grafana y otras herramientas de monitoreo.

Configuración

Configura el endpoint de métricas en `config/runtime.exs`:

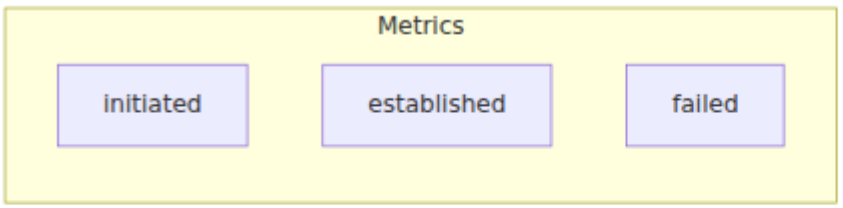
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

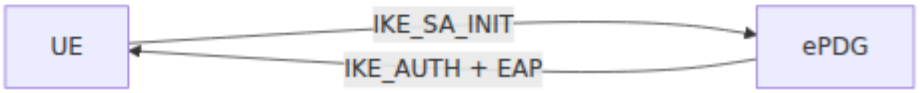
Parámetro	Tipo	Predeterminado	Var de Entorno	Descripció
`port`	Entero	`9568`	`PROMETHEUS_PORT`	Puerto HTTP para el endpoint `/metrics`

Categorías de Métricas

Métricas de Sesión IKEv2

Métricas que rastrean el establecimiento de túneles IKEv2 en la interfaz SWu.





Métrica: `epdg_ikev2_session_initiated_count`
Tipo: Contador
Descripción: Total de intercambios IKE_SA_INIT iniciados. Se incrementa cuando un UE inicia el establecimiento del túnel.

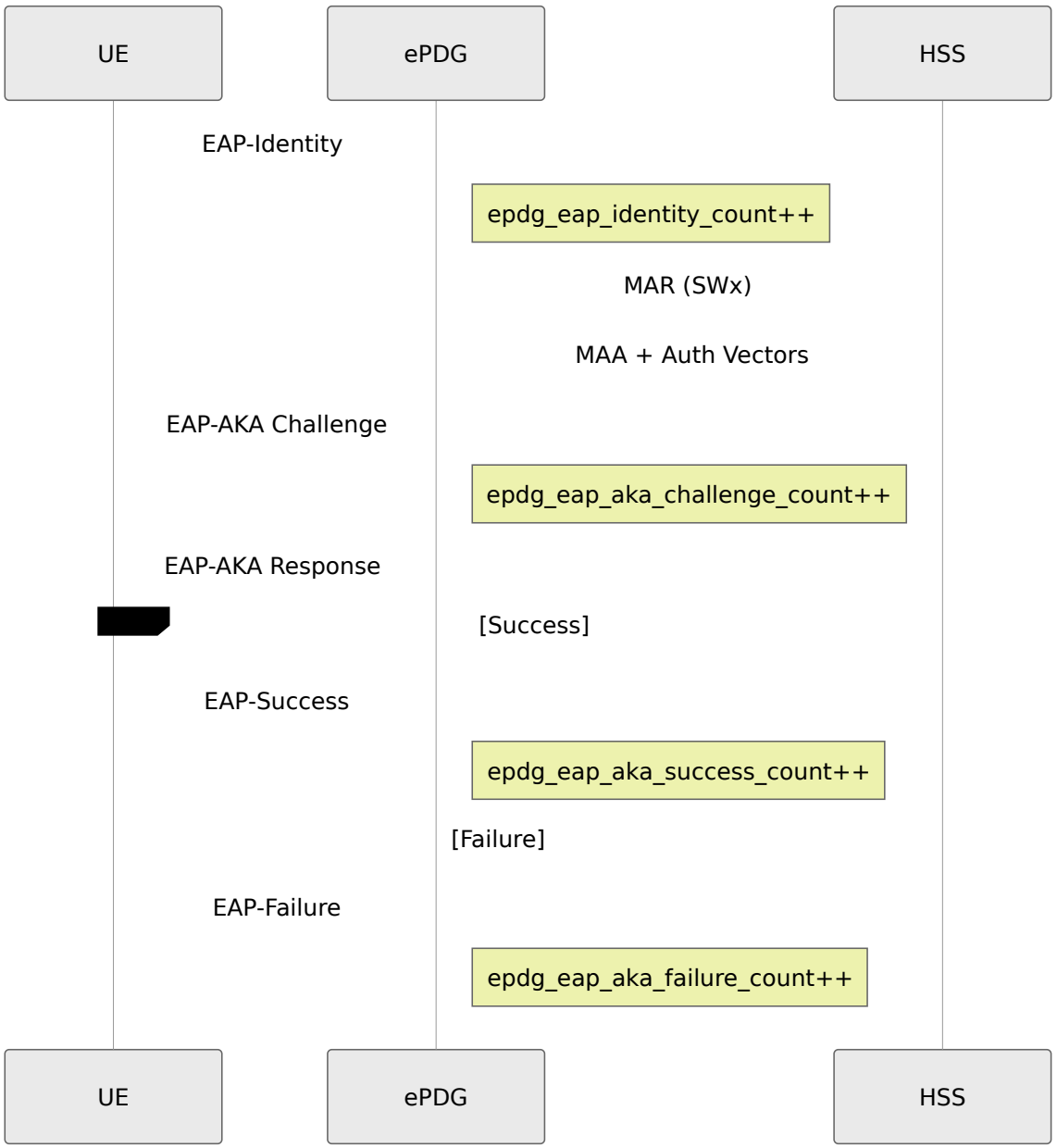
Métrica: `epdg_ikev2_session_established_count`
Tipo: Contador
Descripción: Total de IKE SAs establecidos con éxito. Se incrementa después de una autenticación EAP-AKA exitosa y la creación de Child SA.

Métrica: `epdg_ikev2_session_failed_count`
Tipo: Contador
Descripción: Total de fallos en el establecimiento de IKE SA
Etiquetas:

- `reason` - Razón de la falla (por ejemplo, `auth_failed`, `timeout`, `invalid_proposal`)

Métricas de Autenticación EAP

Métricas que rastrean flujos de autenticación EAP-AKA según RFC 4187. OmniEPDG también soporta EAP-AKA' según RFC 5448, con el tipo de autenticación seleccionado automáticamente según el prefijo de identidad NAI del UE.



Métrica: `epdg_eap_identity_count`
Tipo: Contador
Descripción: Total de solicitudes EAP-Identity recibidas de los UEs

---

Métrica: `epdg_eap_aka_challenge_count`
Tipo: Contador
Descripción: Total de desafíos EAP-AKA enviados a los UEs

Métrica: `epdg_eap_aka_success_count`
Tipo: Contador
Descripción: Total de autenticaciones EAP-AKA exitosas

Métrica: `epdg_eap_aka_failure_count`
Tipo: Contador
Descripción: Total de autenticaciones EAP-AKA fallidas
Etiquetas:

- `reason` - Razón de la falla (por ejemplo, `res_mismatch`, `invalid_identity`, `authentication_rejected`)

Métrica: `epdg_eap_aka_sync_failure_count`
Tipo: Contador
Descripción: Total de fallos de sincronización del número de secuencia (SQN) EAP-AKA. Indica un desajuste del número de secuencia USIM/HSS que requiere re-sincronización.

Métricas de Seguridad de Autenticación

Métricas para la capa de seguridad de autenticación. Consulta la Guía de Seguridad para detalles de configuración.

Métrica: `epdg_auth_verification_failed_count`
Tipo: Contador
Descripción: Total de fallos en la verificación de carga útil AUTH. Indica posibles ataques de hombre en el medio o errores de implementación.

Métrica: `epdg_auth_rate_limited_count`
Tipo: Contador
Descripción: Total de intentos de autenticación bloqueados por limitación de tasa
Etiquetas:

- `type` - Razón del bloqueo: `ip` (umbral por IP excedido) o `imsi` (umbral por IMSI excedido)

Consultas de ejemplo:

```
# Intentos limitados por tasa por minuto
rate(epdg_auth_rate_limited_count[1m])

# Limitados por tipo
sum by (type) (rate(epdg_auth_rate_limited_count[5m]))
```

Métrica: `epdg_auth_geoip_blocked_count`
Tipo: Contador
Descripción: Total de intentos de autenticación bloqueados por filtrado de país GeoIP
Etiquetas:

- `country` - Código de país ISO 3166-1 alpha-2 (por ejemplo, `CN`, `RU`), o `UNKNOWN` para IPs que no pudieron ser geolocalizadas

Consultas de ejemplo:

```
# Bloqueos GeoIP por minuto
rate(epdg_auth_geoip_blocked_count[1m])

# Principales países bloqueados
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))
```

Métrica: `epdg_esp_replay_detected_count`
Tipo: Contador
Descripción: Total de paquetes ESP rechazados debido a la detección de repetición (según RFC 4303). Indica posibles ataques de repetición o problemas de red que causan reordenamiento de paquetes.

Métricas de Diameter SWx

Métricas para la interfaz SWx entre ePDG y HSS según 3GPP TS 29.273.

Métrica: `epdg_diameter_swx_mar_count`
Tipo: Contador

Descripción: Total de Multimedia-Auth-Requests enviados al HSS para la recuperación de vectores de autenticación
Etiquetas:

- `result` - Resultado de la solicitud: `success` o `failure`

Métrica: `epdg_diameter_swx_sar_count`
Tipo: Contador
Descripción: Total de Server-Assignment-Requests enviados al HSS para registro/deregistro
Etiquetas:

- `result` - Resultado de la solicitud: `success` o `failure`

Métrica: `epdg_diameter_swx_mar_latency_ms`
Tipo: Histograma
Descripción: Tiempo de respuesta MAR en milisegundos
Buckets: 50, 100, 250, 500, 1000, 2500 ms

Métrica: `epdg_diameter_swx_sar_latency_ms`
Tipo: Histograma
Descripción: Tiempo de respuesta SAR en milisegundos
Buckets: 50, 100, 250, 500, 1000, 2500 ms

Métrica: `epdg_diameter_swx_pending_count`
Tipo: Gauge
Descripción: Número actual de solicitudes SWx pendientes a la espera de respuesta. Valores altos indican congestión del HSS o problemas de conectividad.

Métricas de Diameter S6b

Métricas para la interfaz S6b entre el servidor AAA y el PGW según 3GPP TS 29.273. Solo aplicable en modo GTP.

Métrica: `epdg_diameter_s6b_aar_count`
Tipo: Contador
Descripción: Total de AA-Requests manejados para autorización de sesión
Etiquetas:

- `result` - Resultado de la solicitud: `success` o `failure`

Métrica: `epdg_diameter_s6b_str_count`
Tipo: Contador
Descripción: Total de Session-Termination-Requests procesados

---

Métrica: `epdg_diameter_s6b_active_sessions_count`
Tipo: Gauge
Descripción: Número actual de sesiones S6b activas

Métricas de Ciclo de Vida de Sesiones

Métricas que rastrean la creación y terminación de sesiones PDN.

Métrica: `epdg_session_created_count`
Tipo: Contador
Descripción: Total de sesiones creadas
Etiquetas:

- `vpn_mode` - Modo VPN: `simple` o `gtp`

Métrica: `epdg_session_terminated_count`
Tipo: Contador
Descripción: Total de sesiones terminadas
Etiquetas:

- `reason` - Razón de la terminación: `user_request`, `timeout`, `error`, `admin`

Métrica: `epdg_sessions_active_count`
Tipo: Gauge

Descripción: Número actual de sesiones activas. Consultado cada 5 segundos.

Métrica: `epdg_sessions_by_state_count`
Tipo: Gauge
Descripción: Sesiones agrupadas por estado de FSM
Etiquetas:

- `state` - Estado de la sesión (por ejemplo, `init`, `eap_identity`, `eap_aka_challenge`, `authenticated`, `established`)

Métrica: `epdg_auth_duration_ms`
Tipo: Histograma
Descripción: Duración del flujo de autenticación completo desde IKE_SA_INIT hasta sesión establecida
Buckets: 100, 250, 500, 1000, 2500, 5000, 10000 ms

Métrica: `epdg_session_duration_seconds`
Tipo: Histograma
Descripción: Tiempo de vida de la sesión desde el establecimiento hasta la terminación
Buckets: 60, 300, 900, 1800, 3600, 7200, 14400 segundos (1 min a 4 horas)

Métricas de Plano de Datos ESP

Métricas para el procesamiento de paquetes ESP según RFC 4303.

Métrica: `epdg_esp_packets_in_count`
Tipo: Contador
Descripción: Total de paquetes ESP descifrados con éxito (dirección UE → red)

Métrica: `epdg_esp_packets_out_count`
Tipo: Contador
Descripción: Total de paquetes ESP cifrados (dirección red → UE)

Métrica: `epdg_esp_bytes_in_total`
Tipo: Gauge
Descripción: Total de bytes descifrados de paquetes ESP

Métrica: `epdg_esp_bytes_out_total`
Tipo: Gauge
Descripción: Total de bytes cifrados en paquetes ESP

Métricas de Pool de IP

Métricas para la gestión de direcciones IP en modo VPN Simple.

Métrica: `epdg_ip_allocated_count`
Tipo: Contador
Descripción: Total de direcciones IP asignadas
Etiquetas:

- `type` - Tipo de dirección: `ipv4` o `ipv6`

Métrica: `epdg_ip_released_count`
Tipo: Contador
Descripción: Total de direcciones IP liberadas
Etiquetas:

- `type` - Tipo de dirección: `ipv4` o `ipv6`

Métrica: `epdg_ip_pool_allocated_count`
Tipo: Gauge
Descripción: Número actual de direcciones IP asignadas

Métrica: `epdg_ip_pool_available_count`
Tipo: Gauge
Descripción: Número actual de direcciones IP disponibles en el pool

---

Métrica: `epdg_ip_pool_utilization_ratio`
Tipo: Gauge
Descripción: Utilización del pool de IP como una proporción de 0.0 a 1.0. Valores que se acercan a 1.0 indican riesgo de agotamiento del pool.

Métricas de VM

Métricas de la máquina virtual Erlang/BEAM para el monitoreo de la salud del sistema.

Métrica: `vm_memory_total`
Tipo: Gauge
Unidad: Bytes
Descripción: Memoria total asignada por la VM

Métrica: `vm_memory_processes`
Tipo: Gauge
Unidad: Bytes
Descripción: Memoria utilizada por procesos Erlang

Métrica: `vm_memory_binary`
Tipo: Gauge
Unidad: Bytes
Descripción: Memoria utilizada para binarios (incluyendo búferes de paquetes)

Métrica: `vm_memory_ets`
Tipo: Gauge
Unidad: Bytes
Descripción: Memoria utilizada por tablas ETS (estado de sesión, registros)

Métrica: `vm_system_info_process_count`
Tipo: Gauge
Descripción: Número de procesos Erlang en ejecución

Métrica: `vm_system_info_port_count`
Tipo: Gauge
Descripción: Número de puertos abiertos (sockets, manejadores de archivos)

Métrica: `vm_statistics_run_queue`
Tipo: Gauge
Descripción: Longitud total de las colas de ejecución del programador. Valores altos indican saturación de CPU.

Integración con Prometheus

Configuración de Recolección

Agrega OmniEPDG a tu `prometheus.yml` de Prometheus:

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

Descubrimiento de Servicios

Para implementaciones en Kubernetes, utiliza el descubrimiento de servicios:

```
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
```

Consultas de Ejemplo

Tasa de Éxito de Autenticación

```
# Tasa de éxito durante 5 minutos
sum(rate(epdg_eap_aka_success_count[5m]))
/
(sum(rate(epdg_eap_aka_success_count[5m])) +
sum(rate(epdg_eap_aka_failure_count[5m])))
```

Tasa de Establecimiento de Sesiones

```
# Sesiones establecidas por segundo
rate(epdg_ikev2_session_established_count[5m])
```

Latencia de Autenticación (p95)

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

Latencia de HSS (p99)

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

Sesiones Activas

```
epdg_sessions_active_count
```

Utilización del Pool de IP

```
epdg_ip_pool_utilization_ratio * 100
```

Rendimiento de ESP

```
# Bytes por segundo (entrante)
rate(epdg_esp_bytes_in_total[5m])

# Paquetes por segundo (en ambas direcciones)
rate(epdg_esp_packets_in_count[5m]) +
rate(epdg_esp_packets_out_count[5m])
```

Desglose de Fallos por Razón

```
# Fallos EAP por razón
sum by (reason) (rate(epdg_eap_aka_failure_count[5m]))

# Terminaciones de sesión por razón
sum by (reason) (rate(epdg_session_terminated_count[5m]))
```

Reglas de Alerta

Ejemplo de reglas de alerta de Prometheus para OmniEPDG:

```yaml
groups:
  - name: omniepdg
    rules:
      # Alta tasa de fallos de autenticación
      - 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: "Alta tasa de fallos de autenticación EAP-AKA"
          description: "La tasa de fallos de autenticación es {{
$value | humanizePercentage }} durante los últimos 5 minutos"

      # Pool de IP cerca del agotamiento
      - alert: OmniEPDGIPPoolLow
        expr: epdg_ip_pool_utilization_ratio > 0.9
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Utilización del pool de IP por encima del 90%"
          description: "El pool de IP está {{ $value |
humanizePercentage }} utilizado"

      # Pool de IP agotado
      - alert: OmniEPDGIPPoolExhausted
        expr: epdg_ip_pool_available_count == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "Pool de IP agotado"
          description: "No hay direcciones IP disponibles para
nuevas sesiones"

      # Latencia alta de HSS
      - 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: "Alta latencia de HSS (SWx)"
          description: "La latencia del percentil 95 de MAR es {{
$value }}ms"

      # Acumulación de solicitudes SWx pendientes
      - alert: OmniEPDGSWxBacklog
        expr: epdg_diameter_swx_pending_count > 100
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "Acumulación de solicitudes SWx en aumento"
          description: "{{ $value }} solicitudes SWx pendientes"

      # Memoria de VM alta
      - alert: OmniEPDGMemoryHigh
        expr: vm_memory_total > 2147483648
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Uso de memoria de OmniEPDG alto"
          description: "El uso de memoria de la VM es {{ $value |
humanize1024 }}"

      # Sobrecarga del programador
      - alert: OmniEPDGSchedulerOverload
        expr: vm_statistics_run_queue > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Cola de ejecución del programador Erlang alta"
          description: "La longitud de la cola de ejecución es {{
$value }}, indicando saturación de CPU"
```

```
      # Sin sesiones (posible problema de servicio)
      - alert: OmniEPDGNoSessions
        expr: epdg_sessions_active_count == 0 and
epdg_ikev2_session_initiated_count > 0
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Sin sesiones activas a pesar de los intentos
de conexión"
          description: "Se están iniciando sesiones pero ninguna
está activa"

      # Alta actividad de limitación de tasa (posible ataque)
      - alert: OmniEPDGHighRateLimiting
        expr: rate(epdg_auth_rate_limited_count[5m]) > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta tasa de intentos de autenticación
bloqueados"
          description: "{{ $value | printf \"%.1f\" }} intentos de
autenticación bloqueados por segundo"

      # Aumento en el bloqueo por GeoIP (posible ataque de una
región específica)
      - alert: OmniEPDGGeoIPBlockingSpike
        expr: |
          rate(epdg_auth_geoip_blocked_count[5m]) > 5
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Actividad elevada de bloqueo por GeoIP"
          description: "{{ $value | printf \"%.1f\" }} conexiones
bloqueadas por segundo por GeoIP"

      # Ataques de repetición de ESP detectados
      - alert: OmniEPDGReplayAttack
        expr: rate(epdg_esp_replay_detected_count[5m]) > 0
        for: 2m
        labels:
          severity: warning
```

```
        annotations:
          summary: "Ataques de repetición de ESP detectados"
          description: "{{ $value | printf \"%.1f\" }} intentos de
repetición por segundo"

      # Fallos en la verificación de AUTH (posible MITM)
      - alert: OmniEPDGAuthVerificationFailures
        expr: rate(epdg_auth_verification_failed_count[5m]) > 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Fallos en la verificación de carga útil AUTH
detectados"
          description: "Posible ataque de hombre en el medio o
error de implementación"
```

Requisitos de Red

Este documento cubre los puertos de firewall y las entradas DNS requeridas para implementar OmniEPDG para llamadas WiFi.

Puertos de Firewall

Puertos de Cara a Internet (UE ↔ ePDG)

Estos puertos deben estar abiertos a Internet para que los dispositivos móviles establezcan conexiones de llamadas WiFi.

Puerto	Protocolo	Dirección	Propósito
500	UDP	Entrante	Intercambio inicial IKEv2 (IKE_SA_INIT, IKE_AUTH)
4500	UDP	Entrante	NAT-Traversal IKEv2 y encapsulación ESP-en-UDP

Puerto 500/UDP maneja la negociación inicial de IKEv2. Si se detecta NAT entre el UE y el ePDG (lo cual es casi siempre el caso para las llamadas WiFi), la conexión migra automáticamente al puerto 4500.

Puerto 4500/UDP transporta tanto la señalización IKEv2 como los datos de usuario encriptados por ESP cuando NAT-T está activo. Este es el camino de datos principal para todo el tráfico de llamadas WiFi.

Puertos de Red Interna (ePDG ↔ Core)

Estos puertos se utilizan para la comunicación entre OmniEPDG y la red central móvil. Deben ser accesibles desde el ePDG pero no expuestos a Internet.

Puerto	Protocolo	Dirección	Propósito	Par
3868	TCP	Bidireccional	Diameter SWx (autenticación)	HSS / DRA
3868	TCP	Bidireccional	Diameter S6b (autorización de sesión)	PGW / AAA
2123	UDP	Bidireccional	Plano de control GTPv2-C (S2b)	PGW
2152	UDP	Bidireccional	Plano de usuario GTP-U (S2b-U)	PGW

Puertos de Gestión

Estos puertos son para monitoreo operativo y deben estar restringidos a redes de gestión.

Puerto	Protocolo	Propósito
4000	TCP	Interfaz web del panel de control (HTTP)
443	TCP	Interfaz web del panel de control (HTTPS, producción)
9568	TCP	Punto final de métricas de Prometheus

Requisitos DNS

Registro DNS de Descubrimiento de ePDG

Los dispositivos móviles descubren el ePDG utilizando una convención de nomenclatura DNS estandarizada definida en 3GPP TS 23.003. El formato FQDN

es:

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

Donde:

- `<MCC>` es el código de país móvil de 3 dígitos (por ejemplo, `505` para Australia)
- `<MNC>` es el código de red móvil de 2 o 3 dígitos, rellenado con ceros a 3 dígitos (por ejemplo, `001`)

El registro DNS debe ser un **registro A** (o AAAA para IPv6) que apunte a la dirección IP pública de OmniEPDG.

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

Nombre Común del Certificado

El certificado TLS del ePDG debe tener un Nombre Alternativo del Sujeto (SAN) que coincida con el FQDN del ePDG al que se conectarán los dispositivos. Esto es validado por el UE durante la autenticación IKEv2.

Requisitos del certificado:

- El SAN debe incluir el FQDN de descubrimiento del ePDG (por ejemplo, `epdg.epc.mnc001.mcc001.pub.3gppnetwork.org`)
- El certificado debe estar firmado por una CA de confianza (los dispositivos validan la cadena)
- Mínimo RSA de 2048 bits o ECDSA P-256

DNS del Dominio Diameter

Para un enrutamiento Diameter adecuado, el dominio debe resolverse a través de registros DNS NAPTR/SRV según RFC 6408. El formato del dominio es:

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

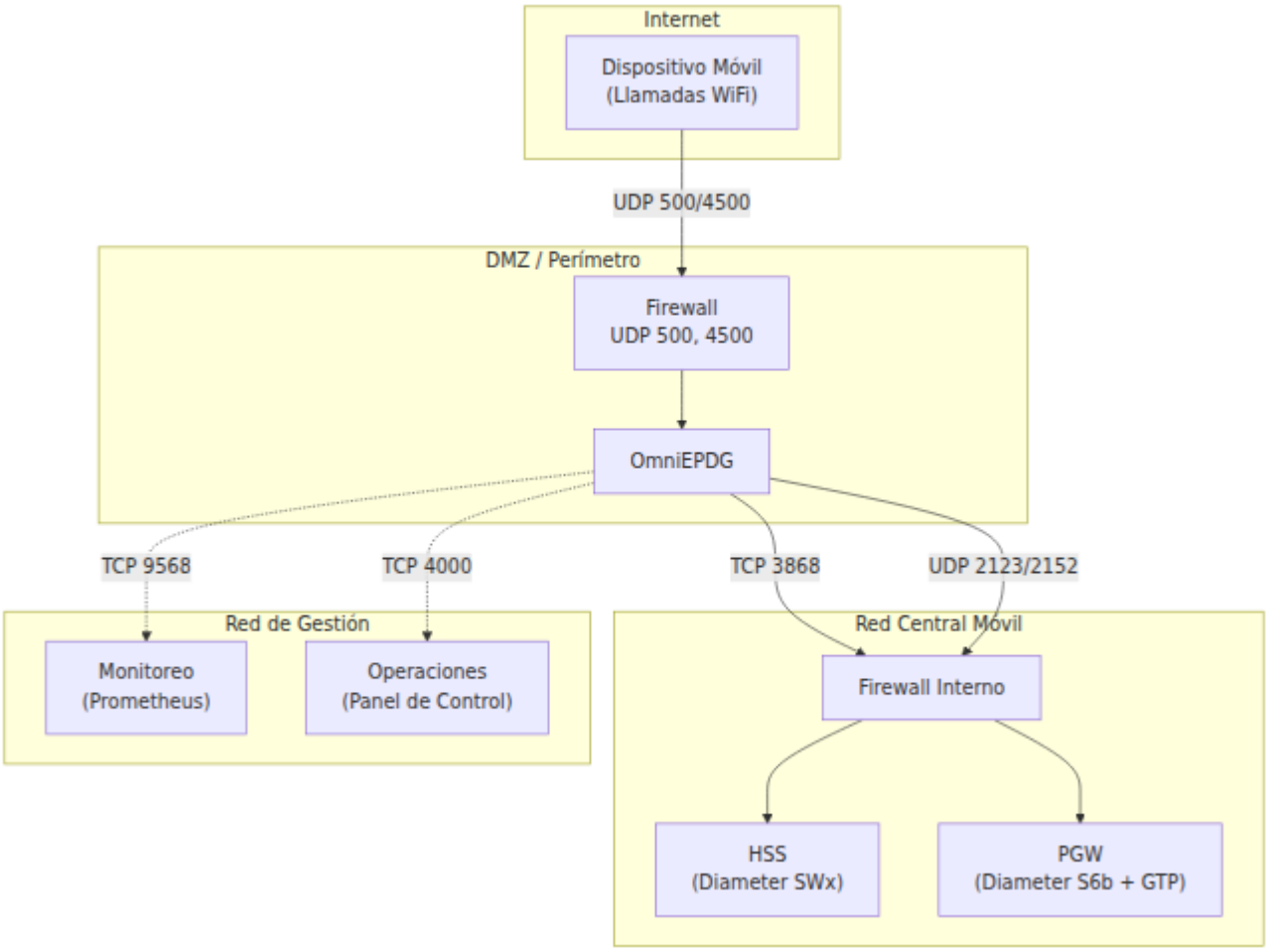
Ejemplo:

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

Este dominio se utiliza en:

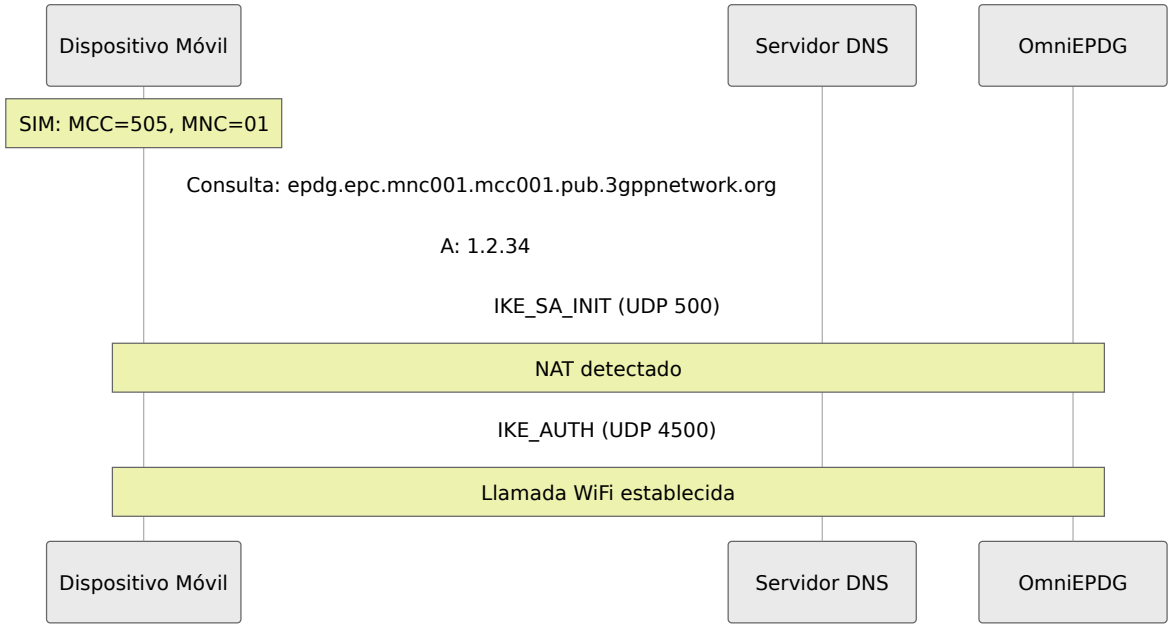
- NAI (Identificador de Acceso a la Red) enviado por el UE durante la autenticación
- AVPs de Diameter Origin-Realm y Destination-Realm
- Decisiones de enrutamiento Diameter

Topología de Red



Flujo de Búsqueda DNS

Cuando un dispositivo móvil inicia una llamada WiFi, se produce la siguiente resolución DNS:



Lista de Verificación

Requisitos de Cara a Internet

- [ ] UDP 500 abierto entrante a OmniEPDG
- [ ] UDP 4500 abierto entrante a OmniEPDG
- [ ] Registro DNS A: `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` → IP pública de ePDG
- [ ] Certificado TLS con SAN coincidente instalado

Requisitos de la Red Central

- [ ] TCP 3868 abierto entre OmniEPDG y HSS/DRA
- [ ] TCP 3868 abierto entre OmniEPDG y PGW/AAA (modo GTP solo)
- [ ] UDP 2123 abierto entre OmniEPDG y PGW (modo GTP solo)
- [ ] UDP 2152 abierto entre OmniEPDG y PGW (modo GTP solo)

Requisitos de Gestión

- [ ] TCP 4000/443 accesible desde la red de operaciones
- [ ] TCP 9568 accesible desde la infraestructura de monitoreo

Referencias

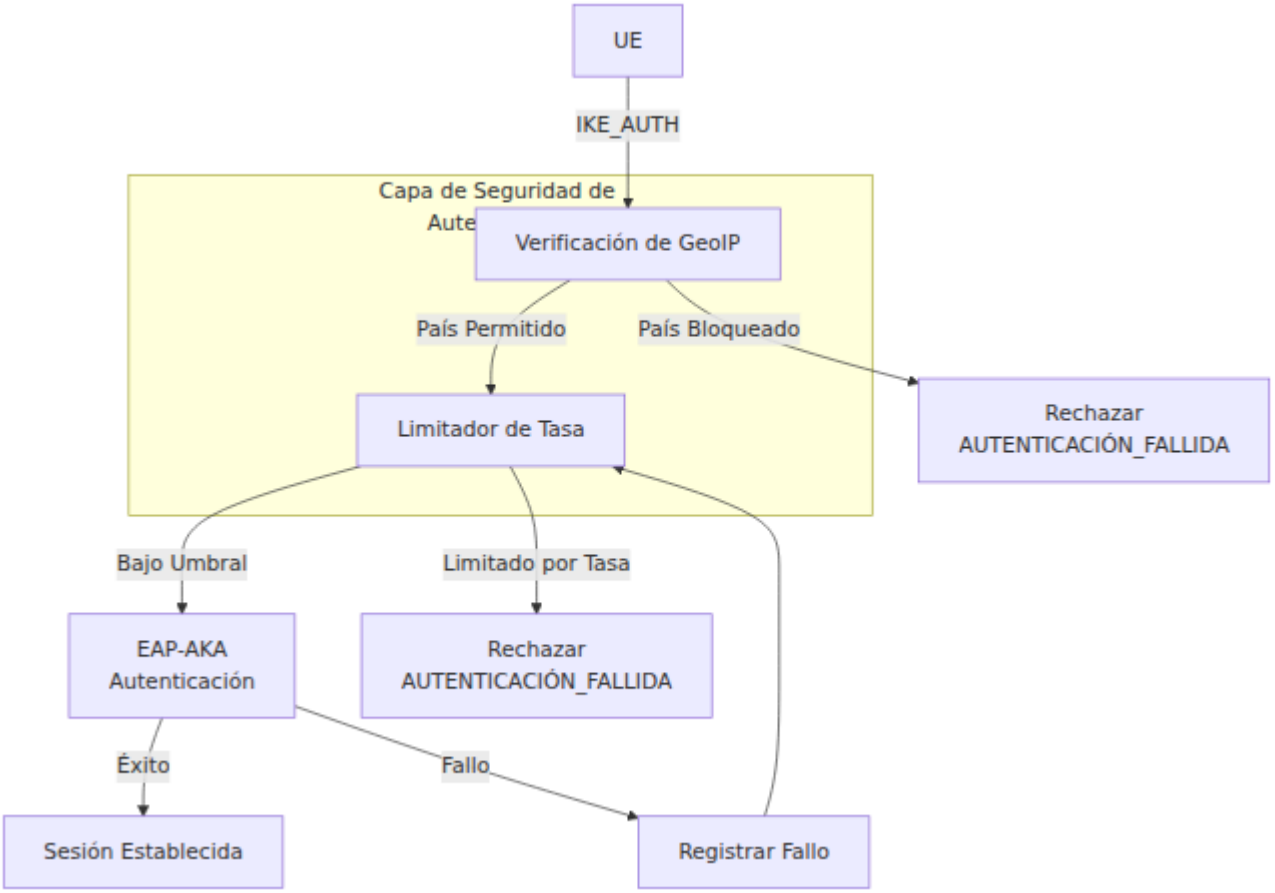
- 3GPP TS 23.003 - Numeración, direccionamiento e identificación (formato FQDN de ePDG)
- 3GPP TS 23.402 - Mejoras de arquitectura para accesos no 3GPP
- RFC 7296 - Protocolo IKEv2
- RFC 3948 - Encapsulación UDP de paquetes ESP de IPsec (NAT-T)
- RFC 6733 - Protocolo Base Diameter

Seguridad de Autenticación de OmniEPDG

OmniEPDG implementa múltiples capas de seguridad de autenticación para protegerse contra ataques de fuerza bruta, relleno de credenciales y acceso no autorizado desde regiones restringidas.

Tabla de Contenidos

Descripción General



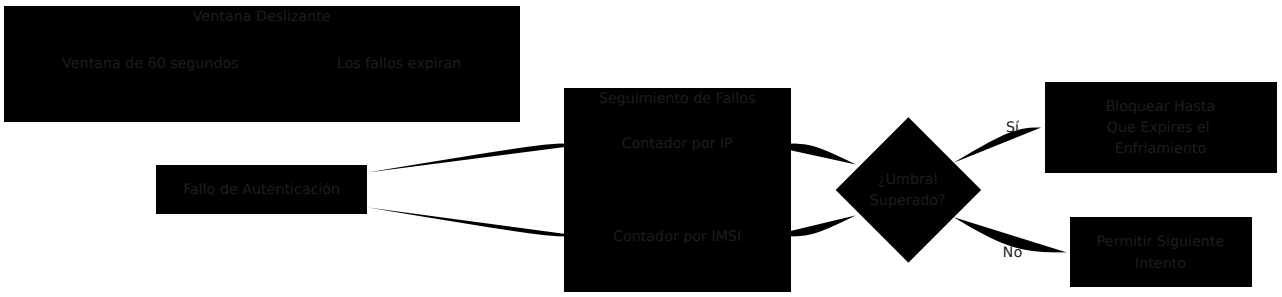
OmniEPDG realiza verificaciones de seguridad al inicio del intercambio IKE_AUTH, antes de las costosas operaciones criptográficas:

1. **Verificación de GeoIP** (opcional) - Verifica que la IP de origen sea de un país permitido
2. **Verificación de Límite de Tasa** - Asegura que la IP/IMSI no haya superado los umbrales de fallo
3. **Autenticación EAP-AKA** - La autenticación estándar 3GPP procede si las verificaciones son exitosas

Limitación de Tasa de Autenticación

La limitación de tasa protege contra ataques de fuerza bruta al rastrear los intentos de autenticación fallidos por IP de origen y por IMSI. Cuando se superan los umbrales, los intentos adicionales se bloquean temporalmente.

Cómo Funciona



El limitador de tasa utiliza un **algoritmo de ventana deslizante**:

- Cada intento fallido se registra con una marca de tiempo
- Los intentos más antiguos que la ventana configurada se expiran automáticamente
- Cuando los fallos en la ventana superan el umbral, se bloquea la fuente
- Los bloqueos expiran después del período de enfriamiento configurado

Seguimiento Dual

Se aplican simultáneamente dos límites independientes:

Tipo de Seguimiento	Propósito	Umbral Predeterminado	Bloqueo Predeterminado
Por IP	Captura escaneadores de puertos y ataques distribuidos desde fuentes únicas	10 fallos / minuto	5 minutos
Por IMSI	Captura ataques dirigidos a suscriptores específicos	5 fallos / minuto	10 minutos

Ambas verificaciones deben pasar para que un intento de autenticación proceda. Si se supera alguno de los umbrales, se rechaza el intento.

Configuración

```
config :omniepdg,
  # Limitación de tasa por IP
  auth_rate_limit_per_ip: 10,            # Máx. fallos antes de
bloquear
  auth_rate_limit_ip_window_ms: 60_000,  # Tamaño de ventana (1
minuto)
  auth_rate_limit_ip_block_ms: 300_000,  # Duración del bloqueo (5
minutos)

  # Limitación de tasa por IMSI
  auth_rate_limit_per_imsi: 5,             # Máx. fallos antes de
bloquear
  auth_rate_limit_imsi_window_ms: 60_000,  # Tamaño de ventana (1
minuto)
  auth_rate_limit_imsi_block_ms: 600_000   # Duración del bloqueo
(10 minutos)
```

Parámetros por IP

Parámetro	Tipo	Requerido	Predeterminado
`auth_rate_limit_per_ip`	Entero	No	`10`
`auth_rate_limit_ip_window_ms`	Entero	No	`60000`
`auth_rate_limit_ip_block_ms`	Entero	No	`300000`

Parámetros por IMSI

Parámetro	Tipo	Requerido	Predeterminad
`auth_rate_limit_per_imsi`	Entero	No	`5`
`auth_rate_limit_imsi_window_ms`	Entero	No	`60000`
`auth_rate_limit_imsi_block_ms`	Entero	No	`600000`

Parámetro	Tipo	Requerido	Predeterminad

Comportamiento en Caso de Éxito

Cuando la autenticación tiene éxito, el limitador de tasa borra todo el historial de fallos para ese par IP/IMSI. Esto permite que los usuarios legítimos que experimentaron fallos transitorios (por ejemplo, problemas de red) se recuperen sin ser penalizados permanentemente.

Ejemplos de Configuraciones

Entorno de Alta Seguridad

Límites estrictos para entornos con baja tolerancia a intentos fallidos:

```
config :omniepdg,
  auth_rate_limit_per_ip: 5,
  auth_rate_limit_ip_window_ms: 120_000,   # Ventana de 2 minutos
  auth_rate_limit_ip_block_ms: 900_000,    # Bloqueo de 15 minutos

  auth_rate_limit_per_imsi: 3,
  auth_rate_limit_imsi_window_ms: 120_000,
  auth_rate_limit_imsi_block_ms: 1_800_000  # Bloqueo de 30
minutos
```

Cómo funciona: Solo se permiten 5 fallos por IP o 3 fallos por IMSI dentro de una ventana de 2 minutos. Los bloqueos duran de 15 a 30 minutos respectivamente.

Caso de uso: Implementaciones empresariales, bases de suscriptores de alto valor o redes bajo ataque activo.

Entorno Relajado

Límites más permisivos para desarrollo o pruebas:

```
config :omniepdg,
  auth_rate_limit_per_ip: 50,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 60_000,     # Bloqueo de 1 minuto

  auth_rate_limit_per_imsi: 20,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 120_000   # Bloqueo de 2 minutos
```

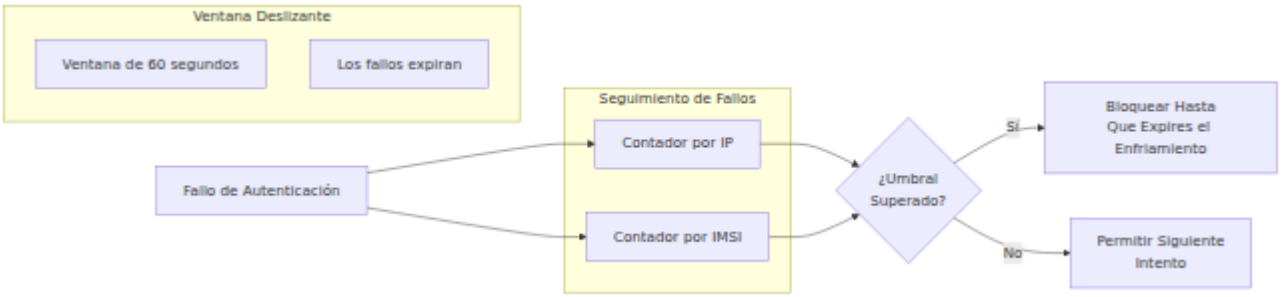
Cómo funciona: Umbrales más altos y bloqueos más cortos permiten mayor flexibilidad en las pruebas.

Caso de uso: Entornos de desarrollo, pruebas de integración.

Bloqueo de Países por GeoIP

El bloqueo por GeoIP restringe el acceso a llamadas WiFi en función de la ubicación geográfica de la dirección IP de conexión. Esto es útil para operadores que necesitan limitar el servicio a países específicos por razones regulatorias o comerciales.

Descripción General



Base de datos de geolocalización IP

OmniEPDG utiliza la base de datos **DB-IP IP-to-City Lite** (CC BY 4.0. Ver `priv/geoip/ATTRIBUTION.md`). No está comprometida en git (~125 MB). En su lugar, se **descarga en el momento de la construcción**. `mix release`

ejecuta la tarea `geoip.fetch` como un paso de liberación, por lo que cada paquete envía una base de datos actual. (Desarrollo/pruebas la obtienen bajo demanda a través del alias `mix test`.) Debido a esto:

- **Cada sesión está anotada automáticamente** con país, ciudad y coordenadas aproximadas. La interfaz web ("Columna de Ubicación") y la respuesta de `/api/sessions` muestran estos: `country_code`, `country_name`, `continent_code`, `geo_city`, `geo_latitude`, `geo_longitude`.
- `geoip_enabled` **solo** controla si las conexiones son *bloqueadas* por país. La anotación ocurre independientemente de esta bandera.

Uso de su propia base de datos (opcional). Establezca `geoip_database_path` a un MaxMind GeoLite2 (`https://www.maxmind.com/en/geolite2/signup`) u otro DB-IP/MaxMind MMDB. Si el archivo configurado falta, se utiliza la base de datos empaquetada (descargada). Nota: El EULA de MaxMind GeoLite2 **no** permite redistribuirlo dentro de un producto, por lo que se utiliza DB-IP Lite (CC BY 4.0) en su lugar.

Para actualizar la base de datos manualmente (DB-IP publica mensualmente):

```
mix geoip.fetch
```

Configuración

```
config :omniepdg,
  # Bloquear conexiones por país (la anotación de geolocalización
siempre está activa)
  geoip_enabled: true,

  # Opcional: sobrescribir la base de datos empaquetada con su
propio MMDB (País o Ciudad)
  # geoip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",

  # Modo de control de acceso
  geoip_mode: :whitelist,

  # Lista de países (códigos ISO 3166-1 alpha-2)
  geoip_countries: ["AU", "NZ"],

  # Manejar IPs desconocidas
  geoip_allow_unknown: false,

  # Comportamiento cuando la base de datos no está disponible
  geoip_fail_open: true
```

Parámetros

Parámetro	Tipo	Requerido	Predeterminado	De
`geoip_enabled`	Booleano	No	`false`	Habi desh acce en G (bloq Cuar se pe toda pero sesic está anot
`geoip_database_path`	Cadena	No	base de datos empaquetada `dbip-country-lite.mmdb`	Ruta de da form (País Reca base DB-IP empa no se o falt
`geoip_mode`	Átomo	No	`:whitelist`	Modo de ac `:whi` (solo país o `:b` (bloq listad perm

Parámetro	Tipo	Requerido	Predeterminado	De
`geoip_countries`	Lista	No	`[]`	Lista de pa 3166 La inter depe `geoi`
`geoip_allow_unknown`	Booleano	No	Ver abajo	Perm cone desd no pu geolo (IPs p rang desc El pred es `fa` mod blan para lista
`geoip_fail_open`	Booleano	No	`true`	Com cuan de da no se Cuar se pe toda cone (falla Cuar se bl

Parámetro	Tipo	Requerido	Predeterminado	De
				toda cone (falla

Modos de Control de Acceso

Modo de Lista Blanca (Recomendado para Llamadas WiFi)

Solo permitir conexiones desde países especificados. Todos los demás países son bloqueados.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ", "FJ"]  # Australia, Nueva Zelanda,
Fiyi
```

Cómo funciona: Solo los UE que se conectan desde direcciones IP australianas, neozelandesas o fijianas pueden autenticarse. Todos los demás países son rechazados.

Caso de uso: Operadores que desean restringir las llamadas WiFi a sus áreas de servicio licenciadas.

Modo de Lista Negra

Bloquear conexiones desde países especificados. Todos los demás países están permitidos.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :blacklist,
  geoip_countries: ["CN", "RU", "KP", "IR"]  # China, Rusia, Corea
del Norte, Irán
```

Cómo funciona: Los UE que se conectan desde los países listados son rechazados. Todos los demás países pueden autenticarse.

Caso de uso: Bloquear regiones de alto riesgo mientras se permite el roaming global.

Manejo de Países Desconocidos

Algunas direcciones IP no pueden ser geolocalizadas:

- Rangos de IP privadas (10.x.x.x, 192.168.x.x, etc.)
- Bloques de IP recién asignados que aún no están en la base de datos
- Nodos de salida de Tor y algunas VPN

El parámetro `geoip_allow_unknown` controla el comportamiento:

Modo	`geoip_allow_unknown` Predeterminado	Comportamiento
Lista Blanca	`false`	Desconocido = no está en la lista blanca = bloqueado
Lista Negra	`true`	Desconocido = no está en la lista negra = permitido

Para anular el predeterminado:

```
config :omniepdg,
  geoip_mode: :whitelist,
  geoip_allow_unknown: true  # Permitir IPs desconocidas incluso
en modo de lista blanca
```

Actualizaciones de Base de Datos

MaxMind actualiza la base de datos GeoLite2 semanalmente. Para actualizar:

1. Descargue el nuevo archivo `GeoLite2-Country.mmdb`

2. Reemplace el archivo existente en la ruta configurada
3. La base de datos se recarga automáticamente en la próxima búsqueda (no se requiere reinicio)

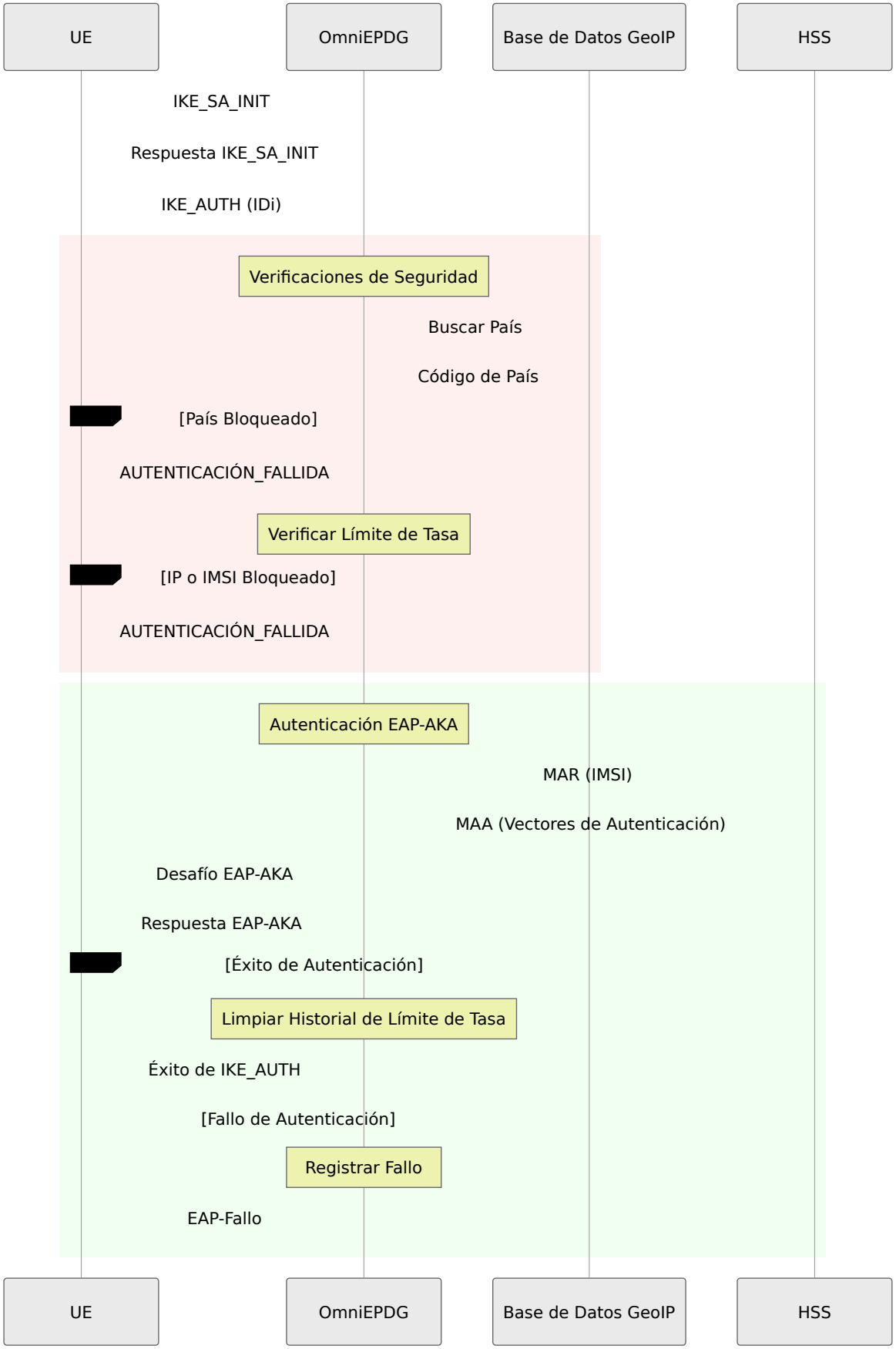
Códigos de País Comunes

Código	País	Código	País
AU	Australia	US	Estados Unidos
NZ	Nueva Zelanda	GB	Reino Unido
CA	Canadá	DE	Alemania
FR	Francia	JP	Japón
SG	Singapur	HK	Hong Kong
IN	India	CN	China

Lista completa: ISO 3166-1 alpha-2

Flujo de Seguridad

El flujo completo de seguridad de autenticación:


UE
OmniEPDG
Base de Datos GeoIP
HSS
IKE_SA_INIT
Respuesta IKE_SA_INIT
IKE_AUTH (IDi)
Verificaciones de Seguridad
Buscar País
Código de País
[País Bloqueado]
AUTENTICACIÓN_FALLIDA
Verificar Límite de Tasa
[IP o IMSI Bloqueado]
AUTENTICACIÓN_FALLIDA
Autenticación EAP-AKA
MAR (IMSI)
MAA (Vectores de Autenticación)
Desafío EAP-AKA
Respuesta EAP-AKA
[Éxito de Autenticación]
Limpiar Historial de Límite de Tasa
Éxito de IKE_AUTH
[Fallo de Autenticación]
Registrar Fallo
EAP-Fallo
UE
OmniEPDG
Base de Datos GeoIP
HSS

Métricas

Métricas de Limitación de Tasa

Métrica: `epdg_auth_rate_limited_count` **Tipo**: Contador **Descripción**: Número de intentos de autenticación bloqueados por limitación de tasa **Etiquetas**:

- `type` - Razón del bloqueo: `ip` (umbral de IP superado) o `imsi` (umbral de IMSI superado)

Consultas de ejemplo:

```
# Intentos limitados por tasa por minuto
rate(epdg_auth_rate_limited_count[1m])

# Limitados por tipo
sum by (type) (rate(epdg_auth_rate_limited_count[5m]))

# Alerta: Alta actividad de limitación de tasa
rate(epdg_auth_rate_limited_count[5m]) > 10
```

Métricas de GeoIP

Métrica: `epdg_auth_geoip_blocked_count` **Tipo**: Contador **Descripción**: Número de intentos de autenticación bloqueados por GeoIP **Etiquetas**:

- `country` - Código de país ISO 3166-1 alpha-2, o `UNKNOWN` para IPs no resolubles

Consultas de ejemplo:

```
# Bloqueos de GeoIP por minuto
rate(epdg_auth_geoip_blocked_count[1m])

# Principales países bloqueados
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))

# Alerta: País inusual intentando acceso
increase(epdg_auth_geoip_blocked_count{country="XX"}[1h]) > 100
```

Solución de Problemas

Problemas de Limitación de Tasa

Usuarios Legítimos Siendo Bloqueados

Síntomas: Los usuarios informan que no pueden conectarse después de intentos fallidos

Causas posibles:

- El usuario ingresó credenciales incorrectas varias veces
- Problemas de red causaron tiempos de espera de autenticación contados como fallos
- Umbrales configurados demasiado bajos para el entorno

Resolución:

1. Verifique las métricas para la IP/IMSI afectada
2. Considere aumentar los umbrales si los falsos positivos son comunes
3. Después de solucionar la causa raíz, el bloqueo expirará automáticamente

Alta Tasa de Intentos Bloqueados

Síntomas: `epdg_auth_rate_limited_count` aumentando rápidamente

Causas posibles:

- Ataque de fuerza bruta en progreso

- UE mal configurado fallando repetidamente la autenticación
- Ataque de relleno de credenciales

Resolución:

1. Revise las IPs de origen en los registros en busca de patrones
2. Considere implementar reglas de firewall a nivel de IP para atacantes persistentes
3. Verifique la conectividad HSS si los usuarios legítimos se ven afectados

Problemas de GeoIP

Todas las Conexiones Siendo Bloqueadas

Síntomas: Ningún UE puede conectarse después de habilitar GeoIP

Causas posibles:

- Archivo de base de datos no encontrado o corrupto
- Códigos de país incorrectos en la configuración
- `geoip_allow_unknown: false` bloqueando IPs privadas en el entorno de laboratorio

Resolución:

1. Verifique que el archivo de base de datos exista en la ruta configurada
2. Verifique que los códigos de país sean correctos (mayúsculas, 2 letras)
3. Para laboratorio/desarrollo, establezca `geoip_allow_unknown: true`
4. Verifique los registros en busca de advertencias relacionadas con GeoIP

Base de Datos GeoIP No Cargando

Síntomas: Advertencia en los registros: "Base de datos GeoIP no encontrada"

Causas posibles:

- Ruta del archivo incorrecta
- Permisos de archivo impiden la lectura

- El archivo no es un formato MMDB válido

Resolución:

1. Verifique que el archivo exista: `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. Verifique los permisos: `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. Verifique la integridad del archivo descargando una copia nueva de MaxMind

Bloqueos de Países Inesperados

Síntomas: Usuarios de países permitidos siendo bloqueados

Causas posibles:

- VPN/proxy haciendo que la IP aparezca de un país diferente
- Base de datos GeoIP desactualizada
- Salida de red corporativa en una ubicación inesperada

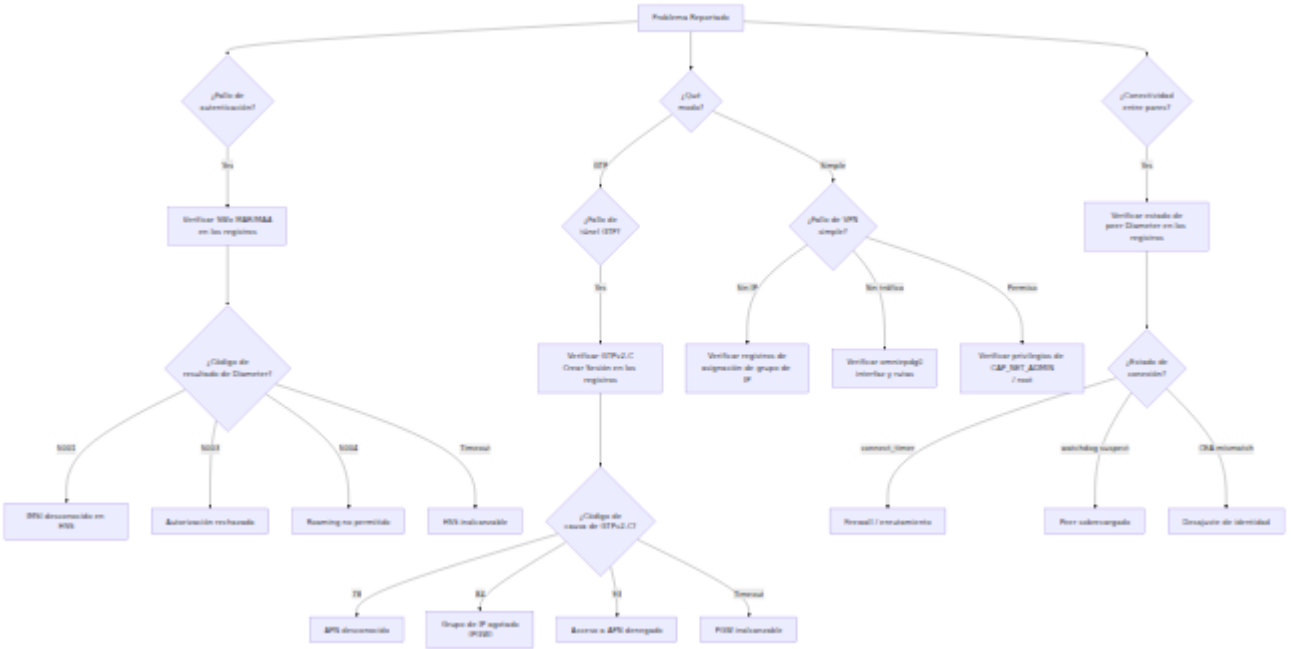
Resolución:

1. Actualice la base de datos GeoIP a la última versión
2. Verifique la IP de salida real del usuario frente al país esperado
3. Considere agregar países adicionales si los usuarios navegan a través de redes corporativas

Resolución de Problemas de OmniEPDG

Esta guía cubre problemas operativos comunes, procedimientos de diagnóstico y pasos de resolución para OmniEPDG.

Visión General del Diagnóstico



Archivos de Registro

OmniEPDG escribe registros en el directorio `log/` relativo al directorio de trabajo de la aplicación. Consulte la Referencia de Configuración para obtener detalles sobre la configuración de registros.

Archivo	Propósito	Cuándo Verificar
`log/console.log`	Todos los mensajes de la aplicación a nivel de depuración	Primer punto de investigación para cualquier problema
`log/error.log`	Solo errores	Escaneo rápido para problemas activos
`log/crash.log`	Caídas del proceso OTP	Cuando los procesos se reinician inesperadamente
`log/erlang.log`	Registrador del núcleo Erlang	Problemas de bajo nivel de Erlang/OTP

Patrones Clave de Registro

Eventos de conexión de peer Diameter:

- `peer_up` - Peer Diameter conectado y capacidades intercambiadas
- `peer_down` - Peer Diameter desconectado

Transiciones de estado de FSM de UE:

- `ue_fsm state_<nombre> event=<evento>` - FSM procesando un evento en un estado dado
- `ue_fsm init(<IMSI>)` - Nueva instancia de FSM creada para el suscriptor
- `terminating epdg_ue_fsm with reason <razón>` - FSM apagándose

Eventos de tiempo de espera:

- `Timeout swm_der_timeout` - Respuesta SWm DER agotada
- `Timeout create_session_timeout` - Respuesta GTPv2-C Crear Sesión agotada
- `Timeout s2b_delete_session_timeout` - Respuesta GTPv2-C Eliminar Sesión agotada

- `Timeout cancel_location_timeout` - Respuesta Cancelar Ubicación agotada

Problemas de Conectividad Diameter

Fallo de Conexión HSS (SWx)

Síntomas: Ningún suscriptor puede autenticarse. Los registros muestran intentos de conexión repetidos al HSS.

Causas posibles:

- Firewall bloqueando el puerto SCTP 3868 entre OmniEPDG y HSS
- `dia_swx_remote_ip` o `dia_swx_remote_port` incorrectos en la configuración
- HSS no está en funcionamiento o no acepta conexiones Diameter
- SCTP no habilitado en la ruta de red (algunos firewalls bloquean SCTP por defecto)
- Desajuste de Origin-Host o Origin-Realm causando rechazo de CEA

Resolución:

1. Verificar la conectividad de red a la IP y puerto del HSS
2. Confirmar que `dia_swx_remote_ip` y `dia_swx_remote_port` coinciden con la configuración del HSS
3. Verificar que el tráfico SCTP esté permitido a través de todos los firewalls. Si SCTP está bloqueado, establecer `dia_swx_proto` a `tcp` como alternativa
4. Verificar que `dia_swx_origin_host` sea un FQDN resolvible y coincida con lo que espera el HSS
5. Revisar los registros del HSS para fallos de negociación Diameter CER/CEA

Fallo de Conexión PGW (S6b)

Síntomas: La autenticación tiene éxito pero la creación del túnel GTP falla o el AAR S6b nunca llega del PGW. Los registros no muestran ningún evento peer_up de S6b.

Causas posibles:

- PGW no configurado para conectarse al listener S6b de OmniEPDG
- Firewall bloqueando el puerto SCTP 3868 en la dirección de enlace S6b de OmniEPDG
- `dia_s6b_local_ip` no es alcanzable desde el PGW
- Desajuste de Origin-Host o Origin-Realm

Resolución:

1. Confirmar que el PGW está configurado para conectarse a OmniEPDG en `dia_s6b_local_ip`:`dia_s6b_local_port`
2. Verificar que la dirección de enlace S6b sea alcanzable desde la red del PGW
3. Comprobar que las reglas del firewall permitan SCTP entrante en el puerto 3868 en la dirección S6b
4. Verificar que `dia_s6b_origin_host` y `dia_s6b_origin_realm` coincidan con lo que espera el PGW

Fallos del Watchdog de Diameter

Síntomas: Las conexiones Diameter establecidas se desconectan intermitentemente. Los registros muestran transiciones del watchdog al estado SUSPECT o DOWN.

Causas posibles:

- Inestabilidad en la ruta de red o pérdida de paquetes
- Peer sobrecargado y no respondiendo a DWR dentro de `dia_swx_watchdog_timer`
- Configuración agresiva del watchdog (demasiados pocos reintentos antes de declarar sospechoso)

Resolución:

1. Verificar la calidad de la ruta de red (pérdida de paquetes, latencia) entre OmniEPDG y el peer
2. Si se espera pérdida de paquetes, aumentar los umbrales de `dia_swx_watchdog_config` / `dia_s6b_watchdog_config` (por ejemplo, `[{okay, 5}, {suspect, 3}]`)
3. Verificar la salud del sistema peer (CPU, memoria, conteo de conexiones)

Fallos de Negociación IKEv2

Ninguna Propuesta Elegida

Síntomas: El IKE_SA_INIT del UE es rechazado con `NO_PROPOSAL_CHOSEN`; los registros muestran `exchange error: :no_proposal_chosen`. El UE nunca avanza más allá de IKE_SA_INIT.

Causas posibles:

- El UE solo ofrece transformaciones criptográficas que OmniEPDG no soporta.
- Un escáner o cliente mal configurado sondeando los puertos públicos.

Antecedentes: OmniEPDG acepta cifrado AES-CBC y AES-GCM; integridad HMAC-SHA2, HMAC-SHA1 y **AES-XCBC-96**; PRFs HMAC-SHA2, HMAC-SHA1 y **PRF-AES128-XCBC**; y grupos DH MODP/ECP/Curve25519/448. Consulte Algoritmos Criptográficos para la lista completa. Algunos teléfonos (notablemente ciertos clientes Samsung VoWiFi) solo ofrecen `AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048`, todos soportados.

Resolución:

1. Habilitar el registro `:debug` e inspeccionar el evento `IKEv2 packet` para la carga útil SA del UE. Los campos `payloads[].proposals[]` enumeran las transformaciones exactas ofrecidas.
2. Confirmar que el cifrado ofrecido / integridad / PRF / transformaciones DH aparezcan como Soportadas en las tablas de algoritmos.

3. Si se requiere una transformación genuinamente no soportada, plantearlo con ingeniería.

La Conexión Se Establece y Luego Se Desconecta Inmediatamente (Child SA Eliminado)

Síntomas: IKE_AUTH se completa, la sesión se establece brevemente, luego el UE envía un `DELETE` INFORMACIONAL dentro de ~100 ms. No hay flujos de medios. Se repite en cada intento.

Causas posibles:

- Las transformaciones Child SA (ESP) en la respuesta no coinciden con lo que ofreció el UE, por lo que el UE elimina la SA.
- Un algoritmo de integridad/cifrado ESP que el plano de datos no puede procesar.

Antecedentes: OmniEPDG negocia la Child SA ESP a partir de la propuesta ofrecida por el UE (incluyendo AES-XCBC-96 y AES-CBC-128/192/256) en lugar de forzar un conjunto fijo. Una respuesta que selecciona una transformación que el UE no ofreció es rechazada según el RFC 7296.

Resolución:

1. En `:debug`, verificar la línea de registro `child SA proposal selected`. Los campos `esp_offered`, `esp_encr` y `esp_integ` muestran lo que se ofreció y lo que se eligió.
2. Verificar que la longitud de la clave de cifrado ESP seleccionada coincida con el cifrado (un desajuste se presenta como `Bad key size` y un paquete descartado).
3. Confirmar que la integridad ESP ofrecida por el UE es una que OmniEPDG soporta (ver Algoritmos de Child SA ESP).

Fallos de Autenticación

IMSI Desconocido (Diameter 5001)

Síntomas: Suscriptores específicos fallan en la autenticación EAP-AKA. Los registros muestran SWx MAA con código de resultado 5001 (DIAMETER_ERROR_USER_UNKNOWN).

Causas posibles:

- Suscriptor no provisionado en el HSS
- Desajuste de IMSI entre el SIM del UE y la base de datos del HSS
- Formato NAI incorrecto, causando que la extracción de IMSI falle

Resolución:

1. Verificar que el IMSI del suscriptor exista en la base de datos del HSS
2. Comprobar que el formato NAI en los registros coincida con el patrón esperado: `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`
3. Confirmar que el IMSI de la tarjeta SIM coincida con el valor provisionado en el HSS

Autorización Rechazada (Diameter 5003)

Síntomas: El suscriptor se autentica pero es rechazado durante la asignación del servidor. Los registros muestran SWx SAA con código de resultado 5003.

Causas posibles:

- Suscriptor no autorizado para el servicio de llamadas WiFi
- APN no permitido para este suscriptor
- Restricciones en el perfil de suscripción

Resolución:

1. Verificar el perfil de servicio del suscriptor en el HSS

2. Confirmar que el acceso a llamadas WiFi / ePDG esté habilitado para el suscriptor
3. Verificar que el APN solicitado esté en la lista de APN permitidos del suscriptor

Roaming No Permitido (Diameter 5004)

Síntomas: Suscriptores en roaming fallan en la autenticación. Los registros muestran SWx MAA o SAA con código de resultado 5004.

Causas posibles:

- La política de roaming del HSS rechaza la ubicación actual del suscriptor
- Llamadas WiFi no permitidas para suscriptores en roaming

Resolución:

1. Revisar las políticas de roaming del HSS para la combinación HPLMN/VPLMN del suscriptor
2. Verificar si las llamadas WiFi están permitidas bajo acuerdos de roaming

Tiempo de Espera de Autenticación

Síntomas: La autenticación se queda colgada y luego falla después de 10 segundos. Los registros muestran `Timeout swm_der_timeout` en `state_wait_auth_resp`.

Causas posibles:

- HSS no responde a SWx MAR dentro de 10 segundos
- Conexión Diameter SWx caída durante la solicitud
- HSS sobrecargado

Resolución:

1. Verificar la capacidad de respuesta y carga del HSS
2. Confirmar que el peer Diameter SWx esté en estado OKAY (no SUSPECT o DOWN)

3. Comprobar que `dia_swx_transmit_timer` sea adecuado para la latencia de red hacia el HSS

Desajuste de Tipo EAP-AKA

Síntomas: La autenticación falla con un error "type_mismatch" en los registros. El prefijo de identidad del UE no coincide con el método EAP utilizado.

Causas posibles:

- El UE envía identidad con prefijo `0` (EAP-AKA) pero la red espera EAP-AKA', o viceversa
- HSS devuelve vectores de autenticación para el tipo EAP incorrecto

Antecedentes: Según 3GPP TS 23.003, el prefijo de identidad NAI indica el tipo de autenticación esperado:

- El prefijo `0` indica EAP-AKA
- El prefijo `6` indica EAP-AKA'

OmniEPDG selecciona automáticamente el método de autenticación basado en el prefijo de identidad del UE. La mayoría de los UEs de llamadas WiFi utilizan el prefijo `0` (EAP-AKA).

Resolución:

1. Verificar la identidad NAI del UE en los registros para verificar el prefijo
2. Asegurarse de que el HSS esté configurado para devolver vectores de autenticación apropiados
3. Verificar que la tarjeta SIM esté provisionada correctamente para el tipo de autenticación esperado

Desajuste de RES EAP-AKA

Síntomas: La autenticación falla después del desafío/respuesta. Los registros muestran "RES mismatch" o "res_mismatch" error.

Causas posibles:

- Fallo de autenticación de la tarjeta SIM
- Desajuste en la derivación de claves entre el UE y la red
- Vectores de autenticación corruptos del HSS

Resolución:

1. Verificar que la tarjeta SIM sea válida y no esté dañada
2. Comprobar que el HSS haya devuelto vectores de autenticación válidos (RAND, AUTN, XRES, CK, IK)
3. Habilitar el registro de depuración para comparar el XRES esperado con el RES recibido
4. Si se utilizan SIMs de prueba, verificar que los valores de Ki y OP/OPc coincidan entre la SIM y el HSS

Fallos de Túnel GTP (Solo Modo GTP)

Crear Sesión Rechazada por PGW

Síntomas: La autenticación tiene éxito pero la creación del túnel falla. Los registros muestran Respuesta de Crear Sesión GTPv2-C con código de error.

Códigos de causa comunes y acciones:

Código de Causa	Nombre	Acción
78	APN Faltante o Desconocido	Verificar que el APN esté configurado en el PGW y coincida con el perfil del suscriptor
82	Denegado en RAT	Verificar que la política del PGW permita el tipo de acceso WiFi (no-3GPP)
84	Todas las Direcciones Dinámicas Ocupadas	Grupo de IP del PGW agotado; expandir grupo o investigar fugas
92	Fallo de Autenticación del Usuario	Fallo de autenticación del lado del PGW; verificar autorización de sesión S6b
93	Acceso a APN Denegado	Suscriptor no autorizado para APN en PGW
96	IMSI/IMEI Desconocido	Suscriptor desconocido para PGW; verificar que la sesión S6b fue autorizada
113	Congestión de APN	APN sobrecargado; reintentar o investigar capacidad del PGW
120	Congestión de Entidad GTP-C	Plano de control del PGW sobrecargado

Tiempo de Espera para Crear Sesión

Síntomas: La creación del túnel se queda colgada durante 10 segundos y luego falla. Los registros muestran `Timeout create_session_timeout` en `state_wait_create_session_resp`.

Causas posibles:

- PGW no es alcanzable en `gtpc_remote_ip`:`gtpc_remote_port`
- Firewall bloqueando el puerto UDP 2123 entre OmniEPDG y PGW
- PGW sobrecargado y no respondiendo a solicitudes GTPv2-C

Resolución:

1. Verificar la conectividad de red al PGW en el puerto UDP 2123
2. Comprobar que las reglas del firewall permitan UDP 2123 entre OmniEPDG y PGW
3. Verificar la salud del PGW y la capacidad de procesamiento GTPv2-C

Túnel GTP-U No Transmite Tráfico

Síntomas: El túnel está establecido (Crear Sesión tiene éxito) pero el tráfico del suscriptor no fluye.

Causas posibles:

- Módulo del kernel GTP-U no cargado
- La IP del socket `gtp_u_kmod` no coincide con la dirección del punto final del túnel GTP-U señalada al PGW
- Enrutamiento no configurado para el dispositivo de túnel GTP
- Firewall bloqueando el puerto UDP 2152 (GTP-U)

Resolución:

1. Verificar que el módulo GTP del kernel de Linux esté cargado (`lsmod | grep gtp`)
2. Confirmar que el dispositivo de túnel GTP exista (`ip link show gtp0`)
3. Verificar que `gtp_u_kmod` `ip` coincida con `gtpc_local_ip` o la dirección señalada en la Solicitud de Crear Sesión
4. Comprobar que la tabla de enrutamiento incluya rutas a través del dispositivo de túnel GTP
5. Verificar que el firewall permita el puerto UDP 2152 entre OmniEPDG y PGW

Fallos de VPN Simple (Solo Modo VPN Simple)

Interfaz TUN No Creada

Síntomas: OmniEPDG se inicia pero no aparece ninguna interfaz `omniepdg0`. Las sesiones fallan en la configuración del túnel. Los registros pueden mostrar errores de `simple_vpn_route` durante el inicio.

Causas posibles:

- El proceso de OmniEPDG carece de la capacidad `CAP_NET_ADMIN` o no se está ejecutando como root
- Módulo del kernel TUN/TAP no cargado
- Otro proceso ya ha creado una interfaz llamada `omniepdg0`

Resolución:

1. Verificar que el módulo del kernel TUN esté disponible (`lsmod | grep tun`)
2. Confirmar que OmniEPDG se esté ejecutando con privilegios suficientes para crear interfaces TUN
3. Comprobar si `omniepdg0` ya existe de una instancia anterior (`ip link show omniepdg0`)
4. Revisar `log/crash.log` en busca de errores del proceso del administrador de rutas

Grupo de IP Agotado

Síntomas: La autenticación tiene éxito pero la configuración del túnel falla. Los registros muestran fallo de asignación de IP de `simple_vpn_pool`.

Causas posibles:

- Todas las direcciones en el grupo CIDR configurado están asignadas a sesiones activas
- Las direcciones IP no se están liberando después de la finalización de la sesión (fuga)

- El tamaño del grupo es demasiado pequeño para el número de suscriptores concurrentes

Resolución:

1. Verificar el número de procesos `epdg_ue_fsm` activos en comparación con el tamaño del grupo
2. Confirmar que las sesiones se estén finalizando correctamente (comprobar mensajes de registro de `terminating`)
3. Si el grupo está realmente lleno, expandirlo utilizando un prefijo CIDR más grande en `simple_vpn_pool_ipv4` (requiere reinicio)
4. Comprobar si hay caídas de FSM durante la finalización en `log/crash.log` que puedan haber impedido la liberación de IP

Tráfico del Suscriptor No Fluye

Síntomas: La sesión está establecida y el UE recibe una dirección IP, pero el tráfico no fluye a través de la interfaz TUN.

Causas posibles:

- Ruta de host no añadida para la IP del suscriptor en `omniepdg0`
- El reenvío de IP no está habilitado en el host de OmniEPDG
- Reglas de firewall bloqueando el tráfico en la interfaz `omniepdg0`
- Faltan reglas de NAT/mascarado para el tráfico saliente del rango de IP del suscriptor

Resolución:

1. Verificar que la ruta de host exista (`ip route show` y buscar la ruta /32 del suscriptor a través de `omniepdg0`)
2. Confirmar que el reenvío de IP esté habilitado (`sysctl net.ipv4.ip_forward`)
3. Comprobar que las reglas de iptables/nftables permitan el reenvío a través de `omniepdg0`
4. Si los suscriptores necesitan acceso a internet, verificar que NAT/mascarado esté configurado para el rango de IP del suscriptor (por

ejemplo, `iptables -t nat -A POSTROUTING -s 10.45.0.0/16 -o <wan-interface> -j MASQUERADE`)

Rutas Obsoletas Después de un Fallo

Síntomas: Las rutas de host para las IP de los suscriptores permanecen en la tabla de enrutamiento después de que OmniEPDG se reinicia o después de que las sesiones terminan anormalmente.

Causas posibles:

- La FSM falló antes de que se pudiera eliminar la ruta
- El proceso de OmniEPDG fue asesinado sin un apagado ordenado

Resolución:

1. Revisar `log/crash.log` en busca de fallos de proceso durante la finalización
2. Eliminar manualmente rutas obsoletas (`ip route del <subscriber-ip>/32 dev omniepdg0`)
3. Reiniciar OmniEPDG recreará la interfaz `omniepdg0`, lo que eliminará todas las rutas asociadas

Problemas de Finalización de Sesión

La Finalización Se Queda Colgada Durante la Desregistración

Síntomas: La finalización de la sesión no se completa. La FSM del UE se queda atascada en un estado `dereg_*` o `wait_*`.

Causas posibles:

- PGW no responde a la Solicitud de Eliminar Sesión
- El peer Diameter no responde a STR o ASR

- La cascada de tiempo de espera no se completa debido a múltiples tiempos de espera acumulados

Resolución:

1. Revisar los registros en busca de mensajes de tiempo de espera en el estado relevante
2. Verificar la conectividad entre PGW y HSS
3. Después de 10 segundos, la FSM debería agotar el tiempo y proceder al siguiente paso de finalización o terminar. Si no lo hace, verificar eventos inesperados registrados como `Unexpected call event`

Contextos PDP GTP-U Huérfanos

Síntomas: Las entradas del túnel GTP-U permanecen en el kernel después de que las sesiones terminan. `ip link show gtp0` muestra que el dispositivo aún tiene contextos PDP activos.

Causas posibles:

- La FSM terminó anormalmente antes de eliminar el contexto PDP
- Fallo durante la secuencia de finalización

Resolución:

1. Revisar `log/crash.log` en busca de fallos de proceso durante la finalización
2. La devolución de llamada `terminate/3` de la FSM intenta limpiar el contexto PDP. Si la FSM fue asesinada (por ejemplo, reinicio del supervisor), la limpieza puede haberse omitido
3. Reiniciar OmniEPDG recreará el socket GTP-U y limpiará los contextos obsoletos

Problemas de Proceso y Sistema

Bucles de Reinicio del Supervisor

Síntomas: Los procesos de OmniEPDG se reinician repetidamente. Los registros muestran mensajes de reinicio del supervisor e informes de fallos.

Causas posibles:

- Error de configuración persistente que causa que un controlador falle al iniciar
- Dependencia externa no disponible (por ejemplo, biblioteca gen_socket no encontrada)
- Peer Diameter enviando mensajes malformados que causan fallos en los controladores

Resolución:

1. Revisar `log/crash.log` para encontrar la causa raíz del fallo
2. Verificar que la ruta `libdir` de `gen_socket` sea correcta y que los archivos de la biblioteca existan
3. Comprobar que todos los parámetros de configuración requeridos estén presentes en `config/runtime.exs`
4. Buscar mensajes Diameter malformados en el informe de fallos

Alto Uso de Memoria

Síntomas: El consumo de memoria de la VM de Erlang crece con el tiempo.

Causas posibles:

- Procesos de FSM de UE no se están limpiando después de la finalización de la sesión
- Acumulación de mensajes de registro en los buzones
- Gran número de sesiones concurrentes

Resolución:

1. Verificar el número de procesos `epdg_ue_fsm` y `aaa_ue_fsm` en ejecución (deben coincidir con el conteo de suscriptores activos)
2. Confirmar que las FSM se estén terminando correctamente después de la finalización de la sesión (comprobar mensajes de registro de `terminating`)
3. Revisar la configuración de rotación de registros para asegurar que los archivos de registro se estén rotando