# Arquitectura y Flujos de Llamadas de OmniEPDG

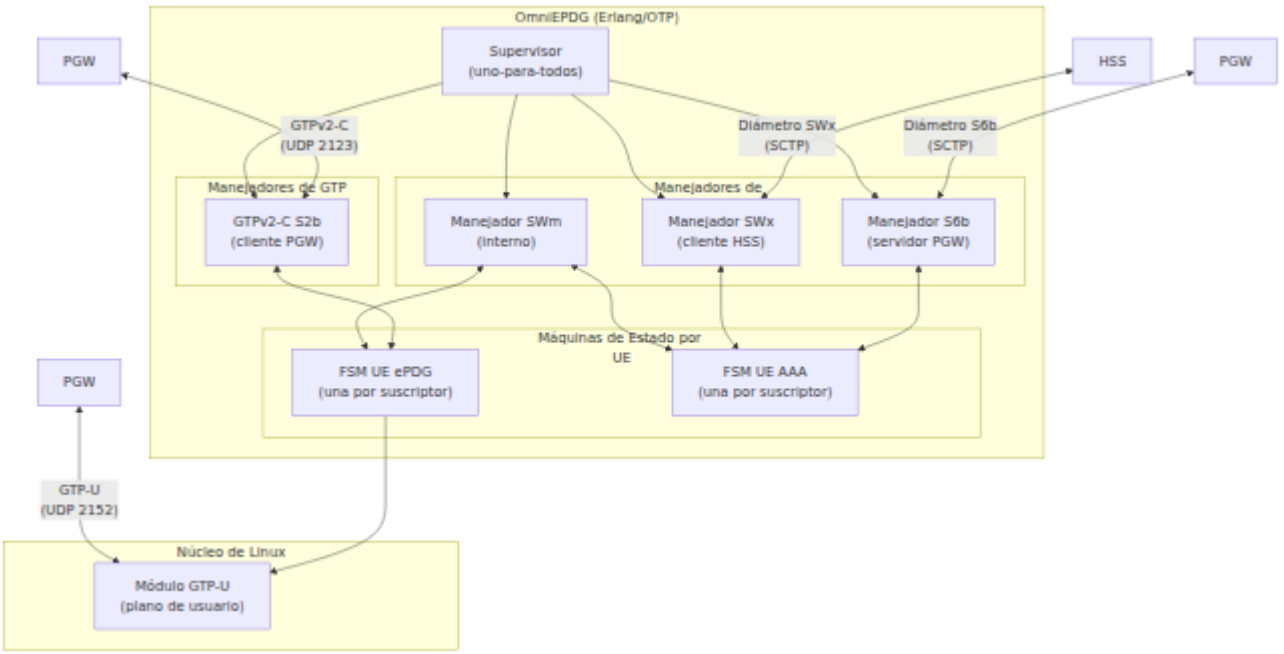
Este documento describe la arquitectura interna de OmniEPDG, sus interfaces de protocolo, máquinas de estado de UE y diagramas de secuencia de mensajes detallados para procedimientos clave. OmniEPDG admite dos modos operativos: **modo GTP** (túnel completo 3GPP a través de PGW) y **modo VPN Simple** (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 que los UEs realicen y reciban llamadas VoWiFi.

### Arquitectura del Modo GTP

En el modo GTP, el tráfico de suscriptores se tunela 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 algún 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 operaciones de autenticación y 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 de la señalización interna de Diámetro 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 gestor de IP y del gestor de rutas |
| `simple_vpn_pool` | Gestor de IPs | Asigna y libera direcciones IPv4 del grupo CIDR configurado utilizando ETS |
| `simple_vpn_route` | Gestor 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 máquinas 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 la señalización del lado AAA: intercambios de Diámetro SWx con el HSS e intercambios S6b con el PGW.

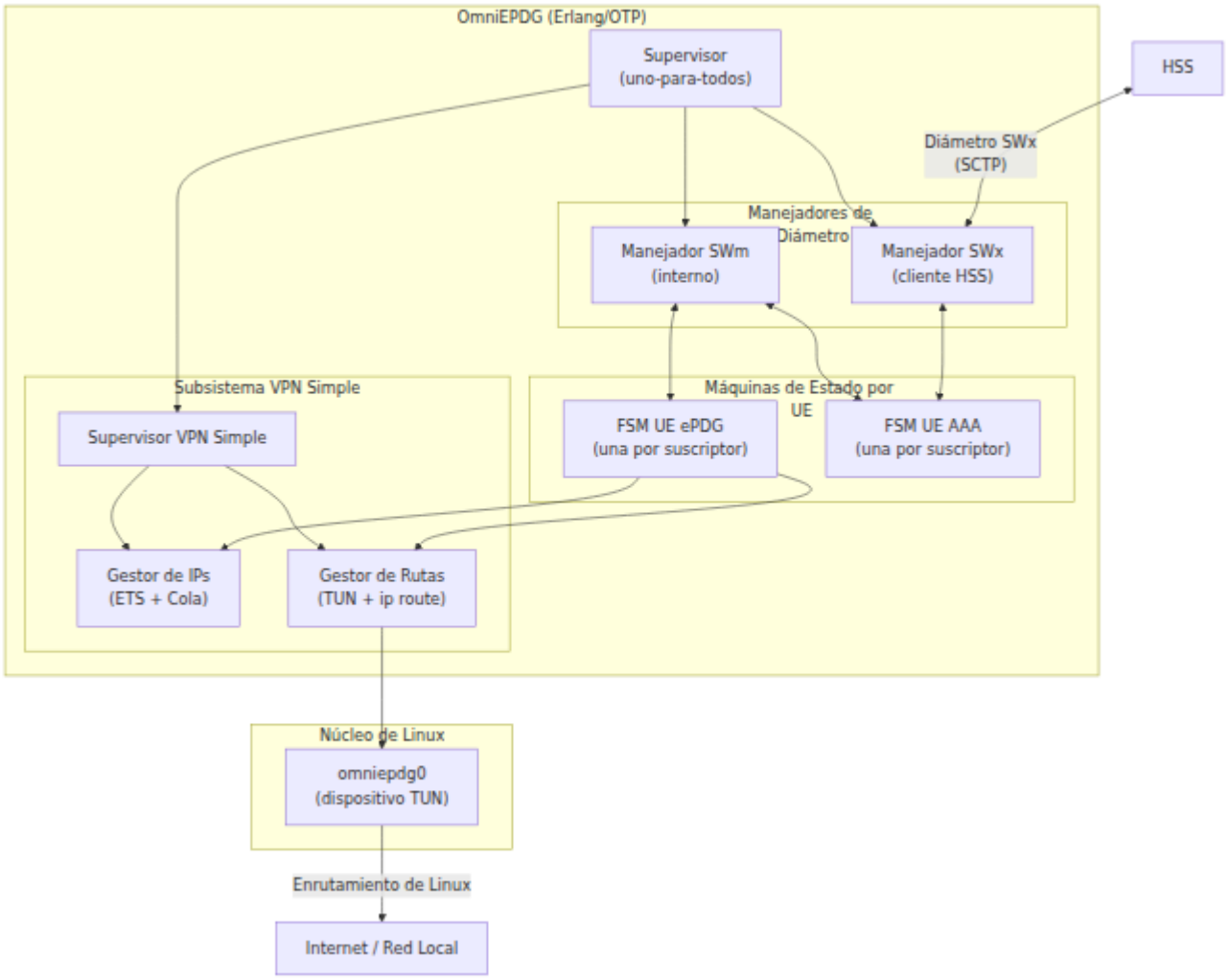
Ambas FSM se implementan como procesos `gen_statem` de Erlang con modo de devolución de llamada de función de estado.

# 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.

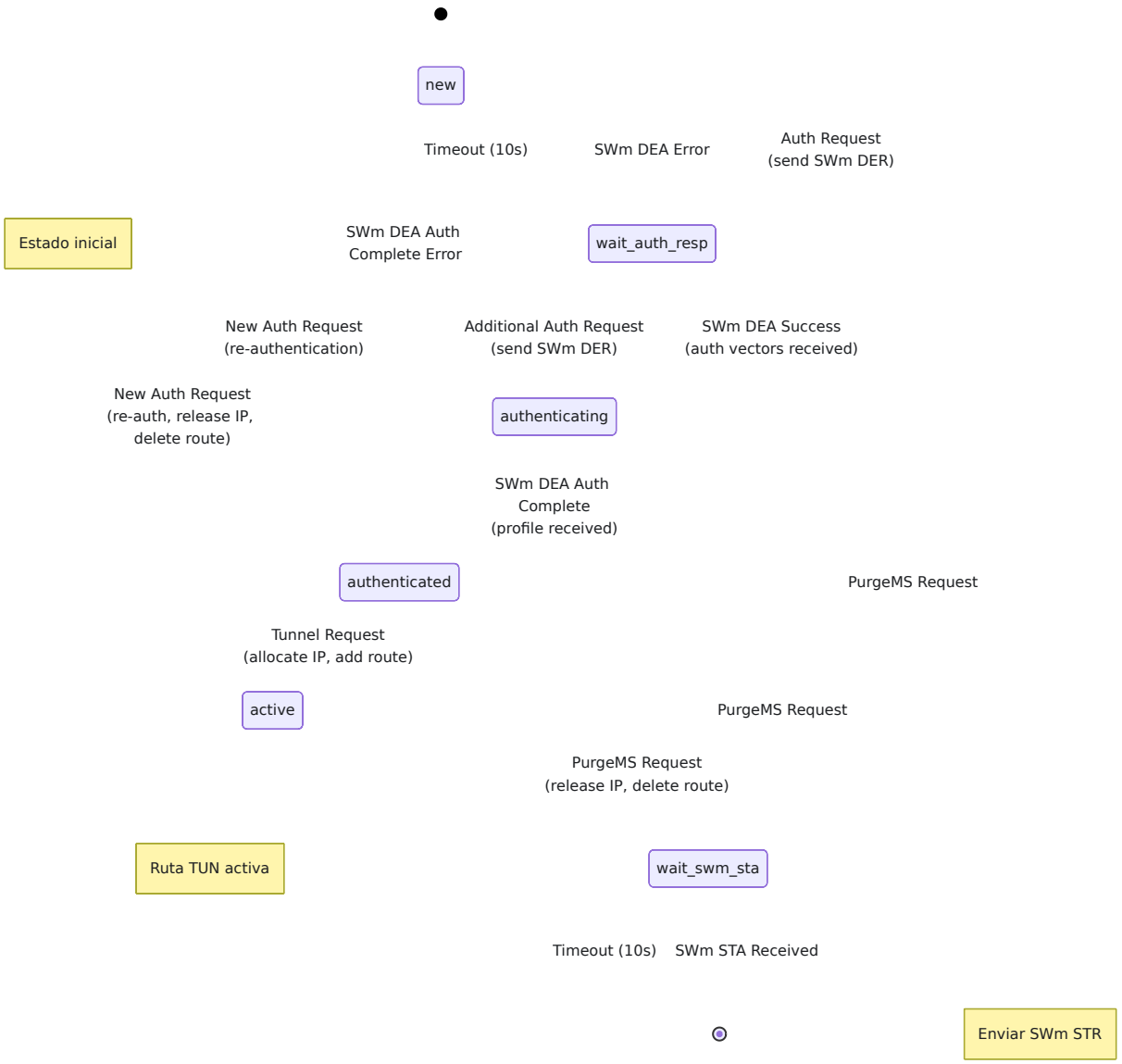
# FSM del Modo GTP

En el modo GTP, el establecimiento del túnel pasa por la creación de sesión GTPv2-C hacia el PGW, y el desmantelamiento implica la eliminación de sesión GTPv2-C, eliminación de portadora iniciada por PGW y flujos de desregistro 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 grupo 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

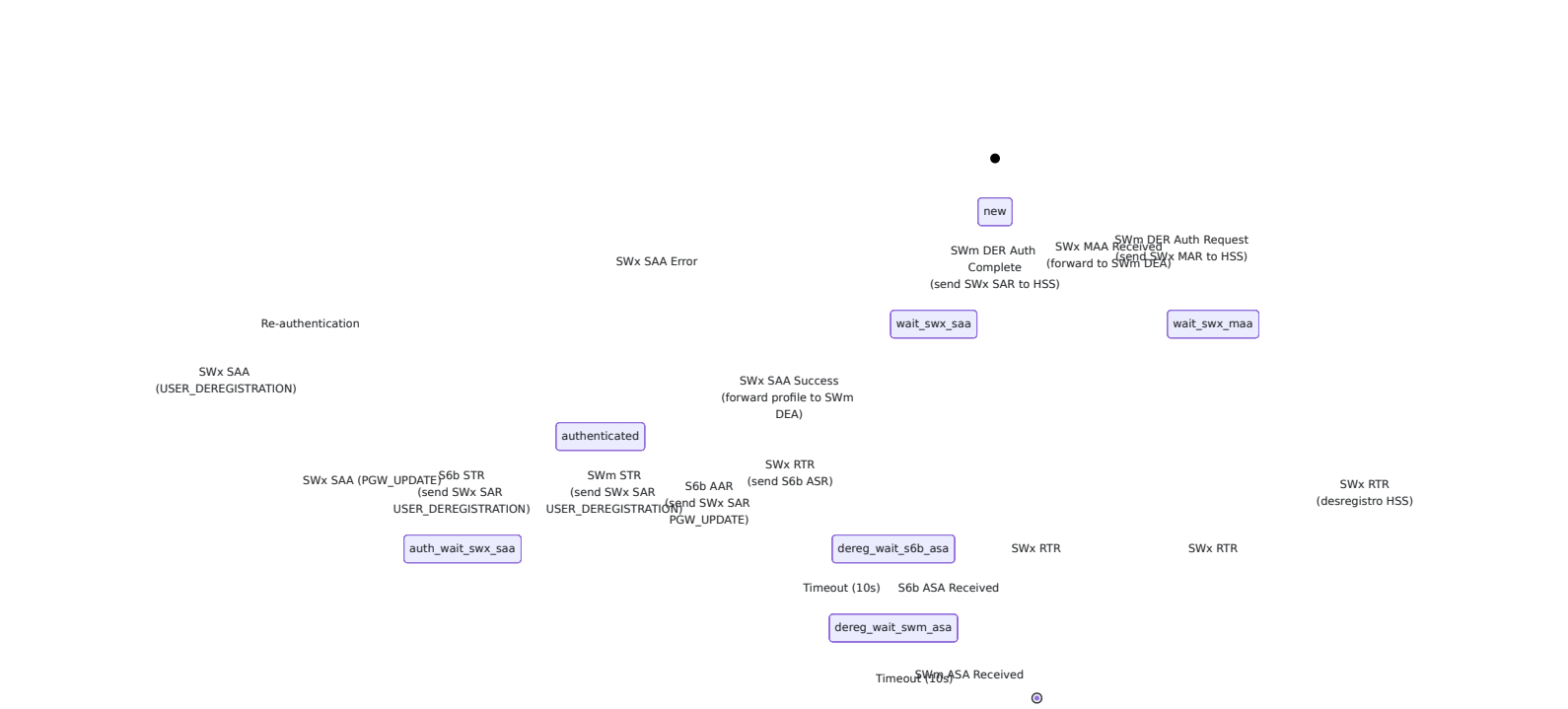
# Referencia de Estados de la FSM UE ePDG

| Estado | Modo | Descripción | Esperand |
|---|---|---|---|
| `new` | Ambos | Estado inicial. No hay 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. | Disparador 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 | Desregistro iniciado por PGW. Ubicación de cancelación enviada a UE. | Resultado de ubicación de cancelación |
| `dereg_net_wait_cancel` | GTP | Desregistro iniciado por la red/HSS. Ubicación de cancelación enviada a UE. | Resultado de ubicación de cancelación |
| `dereg_net_wait_s2b_delete` | GTP | Desregistro 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 la señalización de Diámetro hacia el HSS (SWx) y el PGW (S6b) en nombre de cada suscriptor.


new
SWx SAA Error
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)
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
(desregistro 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

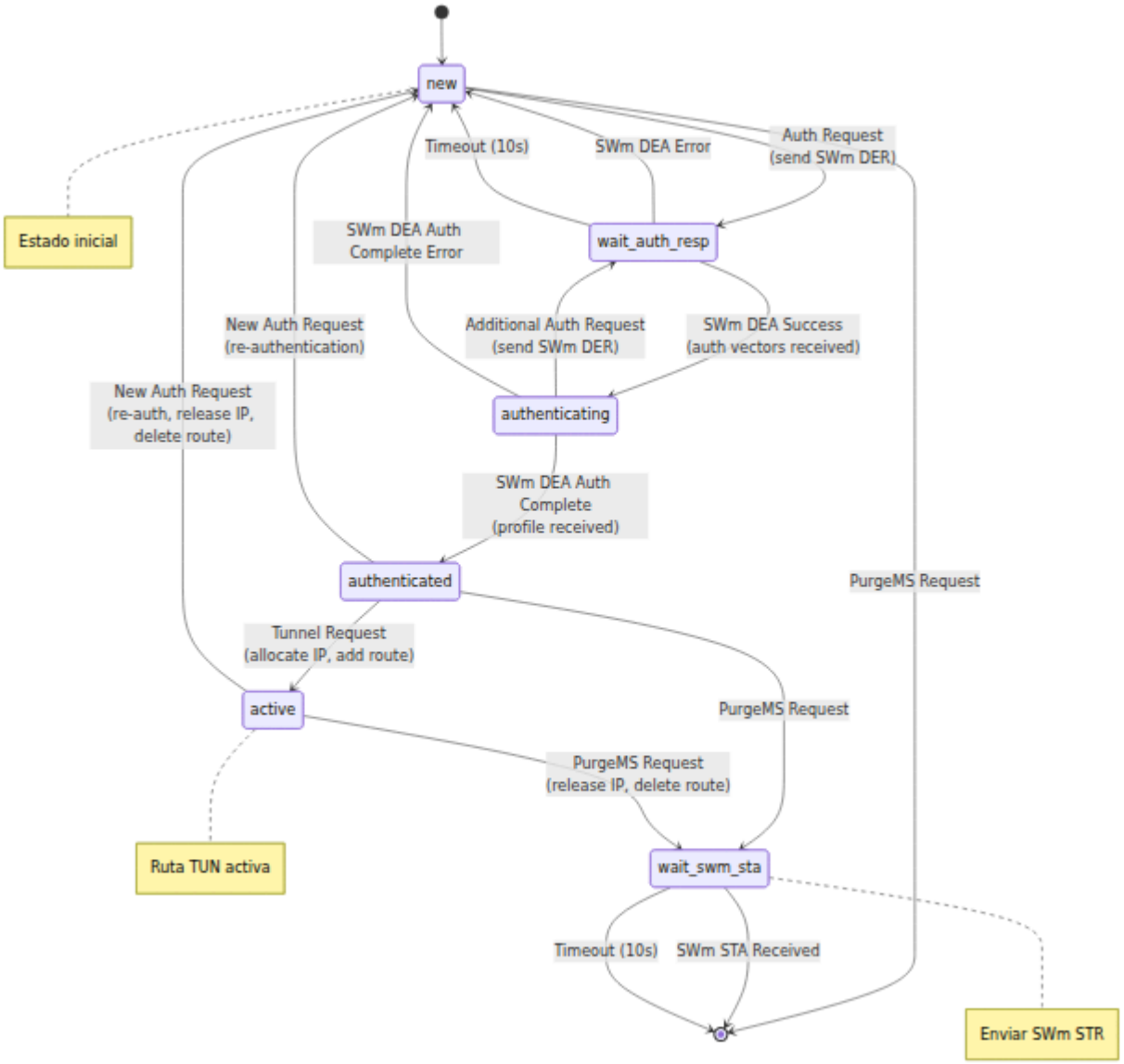
# Referencia de Estados de la FSM UE AAA

| Estado | Descripción | Esperando |
|---|---|---|
| `new` | Estado inicial. No hay 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. Rastreando el estado de sesión dual. | Eventos de sesión |
| `auth_wait_swx_saa` | SWx SAR enviado para actualización de PGW o desregistro de usuario. | SWx SAA del HSS |
| `dereg_net_wait_s6b_asa` | Desregistro 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

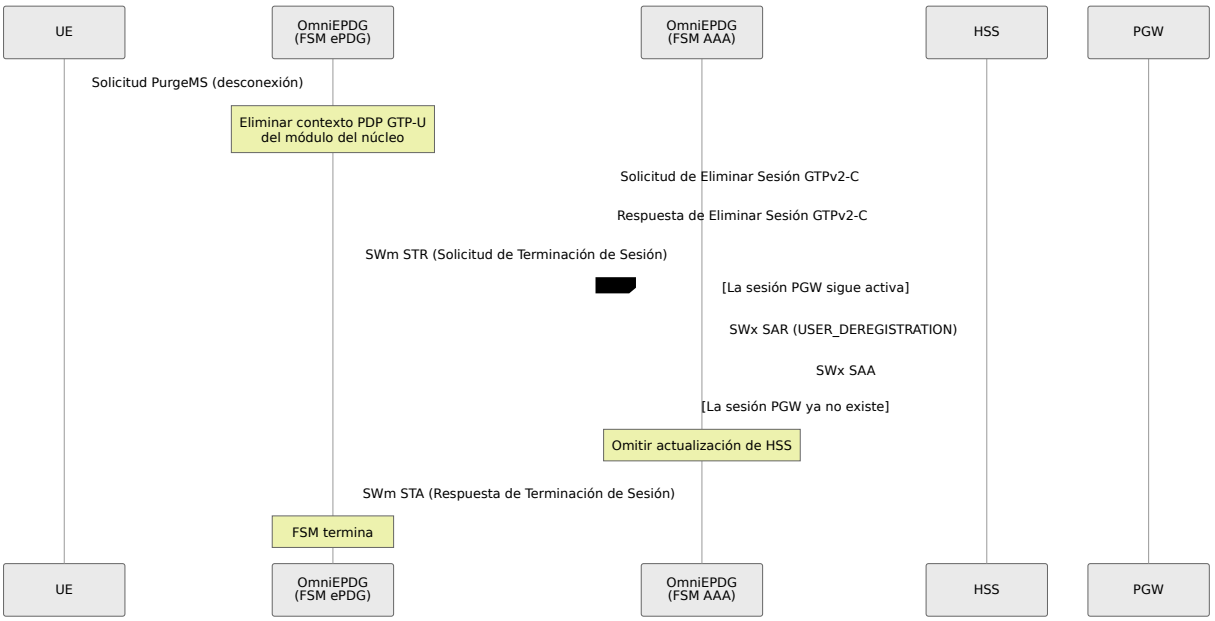
## Modo GTP: Establecimiento de Sesión Exitoso

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



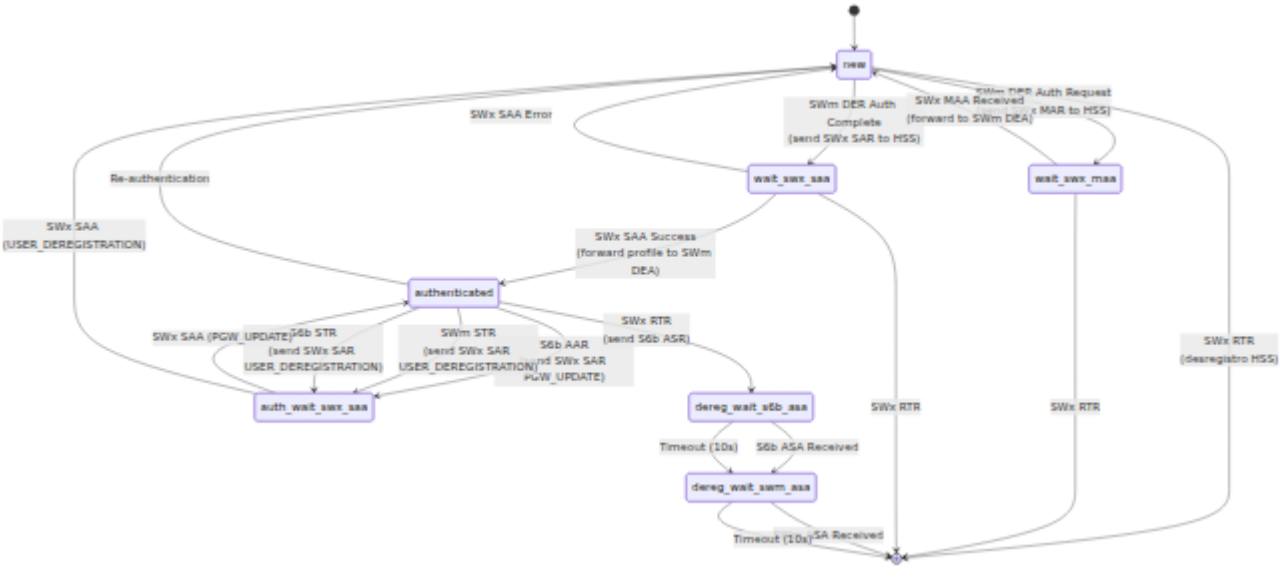

## Modo GTP: Desmantelamiento de Sesión Iniciado por UE

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



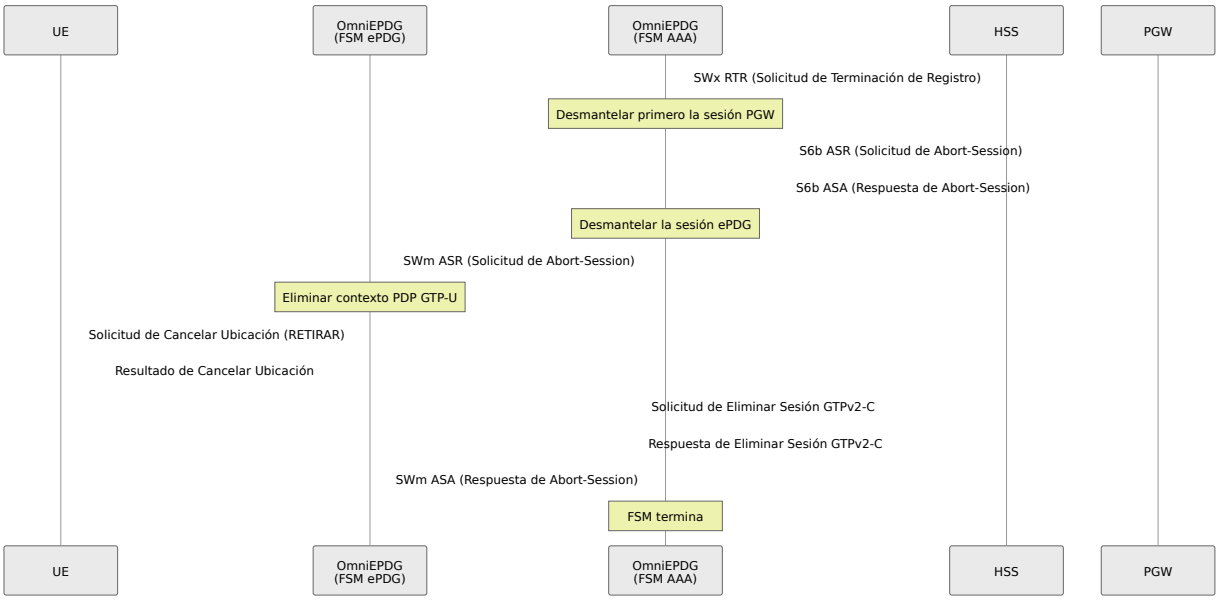

# Modo GTP: Desmantelamiento de Sesión Iniciado por PGW

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



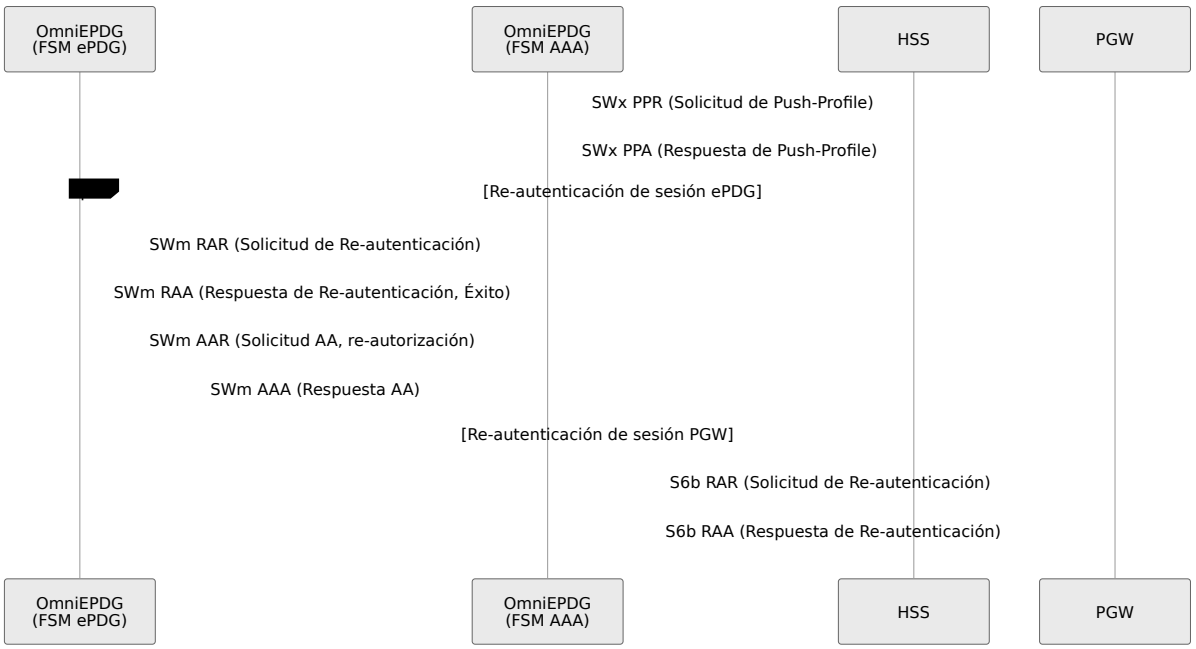

# Modo GTP: Desregistro Iniciado por la Red (HSS)

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



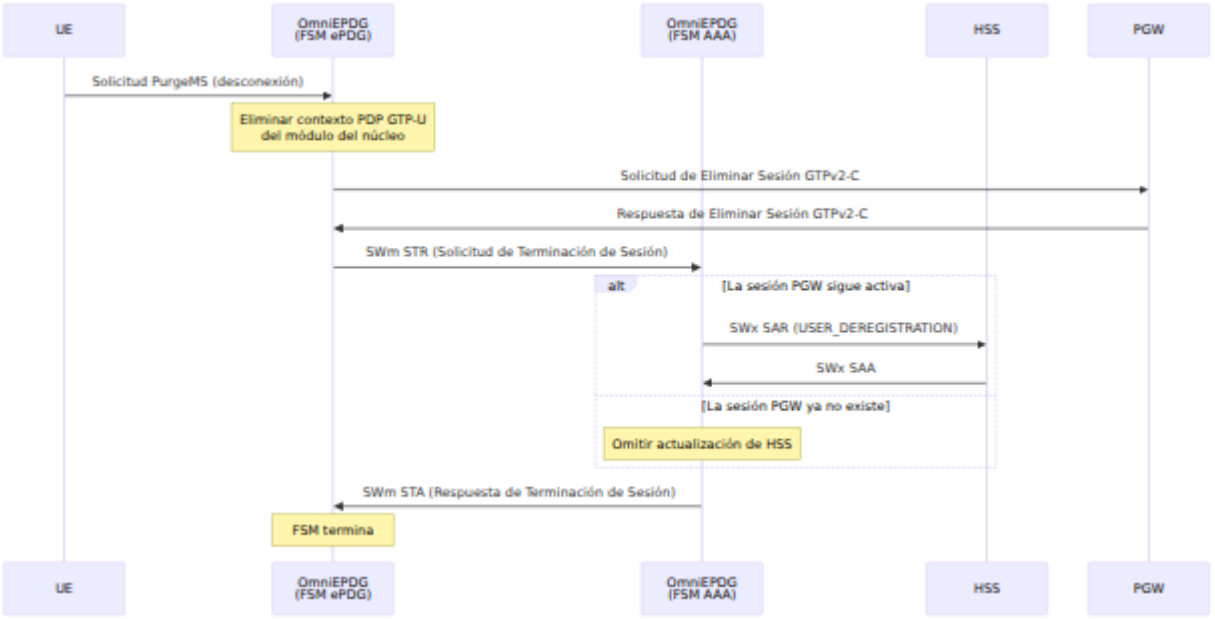

# Modo GTP: Push de Perfil HSS y Re-autenticación

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.



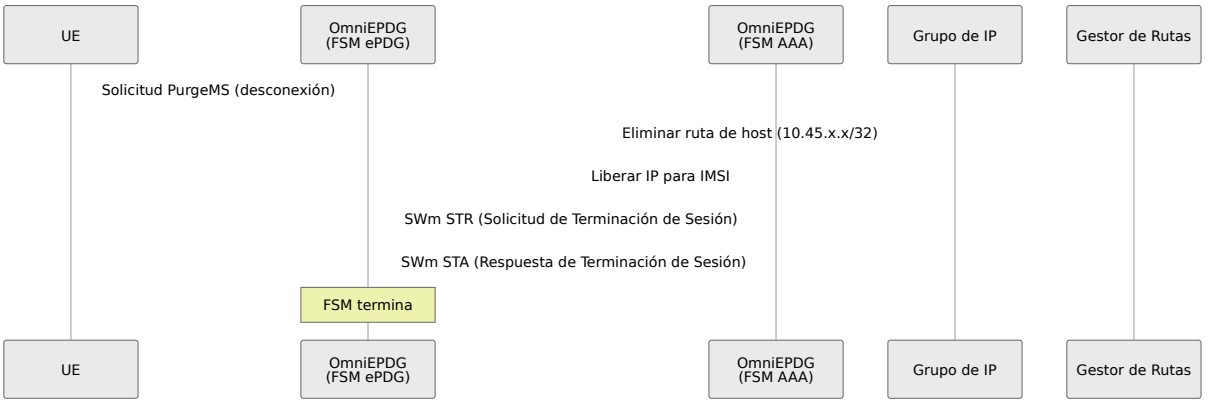
# Modo VPN Simple: Establecimiento de Sesión Exitoso

En el modo VPN Simple, el establecimiento de la sesión es más corto. Después de la autenticación EAP-AKA, la FSM ePDG asigna una IP del grupo local y configura una ruta de host en la interfaz TUN, eludiendo toda interacción con 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 el 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 Aplicaci��n | 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 no pu proporcion datos de autenticac temporalm |
| 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 genér de procesami |

| Código de Resultado | Nombre | Significa |
|---|---|---|
| 5420 | DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION | No se enc suscripció EPS |
| 5421 | DIAMETER_ERROR_RAT_NOT_ALLOWED | Tecnología acceso no permitida |
| 5422 | DIAMETER_ERROR_EQUIPMENT_UNKNOWN | Dispositivo IMEI no 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 del 1 al 15 son informativos, del 16 al 63 indican éxito y del 64 en adelante 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 portadora 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 | Grupo 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 | Fallo en la validación del par |
| 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 del UE. La mayoría de los 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 |
| HMAC-SHA1-96 | 2 | 160 bits | 96 bits | Soportado (legado) | RFC 2404 |
| HMAC-MD5-96 | 1 | 128 bits | 96 bits | Soportado (legado) | RFC 2403 |

# 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-HMAC-SHA1 | 2 | 160 bits | Soportado (legado) | RFC 2104 |
| PRF-HMAC-MD5 | 1 | 128 bits | Soportado (legado) | RFC 2104 |

## 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 (SA Hijo)

El túnel ESP utiliza los mismos algoritmos de cifrado e integridad negociados durante IKEv2 CREATE_CHILD_SA.

**Configuración predeterminada de ESP:**

- 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+ | FIPS 186-2 PRF (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 |

# 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 grupo local.

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

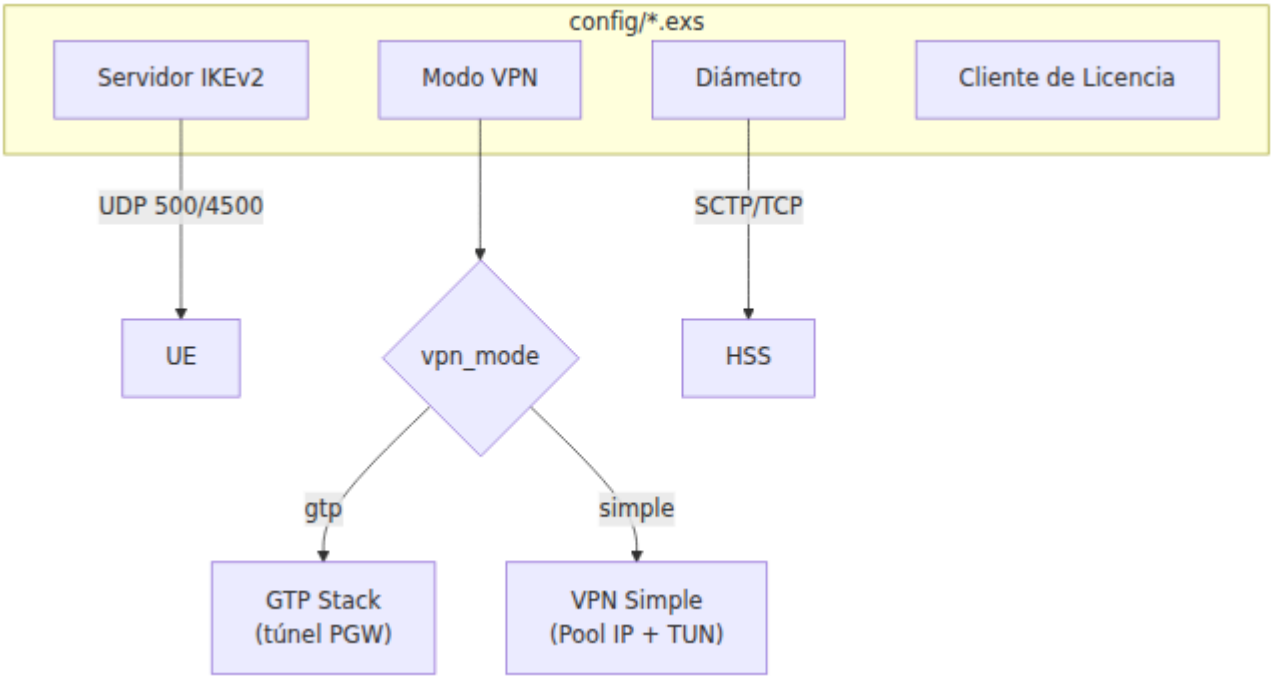
# Referencia de Configuración de OmniEPDG

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 en tiempo de compilación están integrados en la versión y no se exponen.

Para implementaciones en contenedores, utiliza 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`. Este archivo se lee cuando OmniEPDG se inicia y admite la sustitución de variables de entorno para implementaciones en contenedores.

## Ejemplo de Configuración

```
# config/runtime.exs
config :omniepdg,
  # Configuración 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,

  # Configuración 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 UE 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/` |

| Parámetro | Tipo | Requerido | Predete |
|---|---|---|---|
| `key_file` | Cadena | Sí | `/etc/omniepdg/` |
| `session_inactivity_timeout_ms` | Entero | No | `300000` |

## Parámetros de Seguridad de Autenticación

OmniEPDG incluye protección incorporada contra ataques de fuerza bruta y control de acceso geográfico. Consulta 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 pools 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"` |

| Parámetro | Tipo | Requerido | Predeterminado |
|---|---|---|---|
| `realm` | Cadena | Sí | `"epc.mnc001.mcc001.3gppnetwork.` |
| `product_name` | Cadena | No | `"OmniEPDG"` |
| `vendor_id` | Entero | No | `10415` |

### Parámetros de Pares

Cada entrada en la lista de `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 Host 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` - SAs IKE establecidos con éxito

- `epdg_ikev2_session_failed_count` - Fallos en el establecimiento de SA IKE (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 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 descifrados
- `epdg_esp_packets_out_count` - Paquetes ESP cifrados
- `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 pool
- `epdg_ip_pool_utilization_ratio` - Utilización del pool (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 total del flujo de autenticación

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

**Métricas de VM:**

- `vm_memory_total` - Memoria total de VM
- `vm_memory_processes` - Memoria de procesos
- `vm_memory_binary` - Memoria binaria
- `vm_memory_ets` - Memoria de 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 programador

**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 de FSM internos 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 en tiempo de compilación.

## Servidor IKEv2

| Variable | Predeterminado | Descripción |
|---|---|---|
| `EPDG_LISTEN_IP` | `"0.0.0.0"` | Dirección de vinculación 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 Traversal NAT 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 por inactividad de 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 vinculación del oyente de Diámetro. |
| `DIA_LISTEN_PORT` | `"3868"` | Puerto del oyente de Diámetro. |
| `DIA_HOST` | `"epdg"` | Host de origen de Diámetro (sin dominio). |
| `DIA_REALM` | `"epc.mnc001.mcc001.3gppnetwork.org"` | Dominio de origen de Diámetro. |

## Par HSS

| Variable | Predeterminado | Descripción |
|---|---|---|
| `HSS_HOST` | `"hss"` | Identidad de Diámetro HSS (Origin-Host). |
| `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
```

# OmniEPDG Panel de Control

OmniEPDG incluye un panel de control basado en la web para el monitoreo en tiempo real de sesiones, pares 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 Diameter | Estado de conexión de pares 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 Diameter** | Pares conectados / total de pares configurados |

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 Diameter** - Navegar a la vista de Pares Diameter para 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 Diameter** | Si la señalización Diameter está habilitada |
| **Pool de IP (IPv4)** | CIDR del pool de IP configurado (solo modo VPN Simple) |

## Auto-Actualización

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

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

*Vista de sesión expandida mostrando 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 SA Hijo IPSec |

**Sección de Red y Tiempos**

| 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 UE

## Auto-Actualización

La lista de sesiones se actualiza automáticamente cada segundo.

# Vista de Pares Diameter

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

## Lista de Pares

Cada fila de par muestra:

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

## Indicadores de Estado

| Estado | Color | Descripción |
| --- | --- | --- |
| **Conectado** | Verde | Conexión de par Diameter establecida |
| **Desconectado** | Rojo | Par no conectado |
| **Desconocido** | Gris | El estado no puede ser determinado |

## 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

Haga 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 Diameter soportadas por el par |

## Estado Vacío

Cuando no hay pares configurados, la vista muestra:

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

## Auto-Actualización

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 recientes 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

Filtrar 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 |
| **Error Solo** | error |

## Búsqueda

El cuadro de búsqueda filtra registros en tiempo real:

- Ingrese 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"
- Verifique la configuración de filtros si se esperan registros

## Auto-Actualización

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

Seleccione 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 para Markdown, incluyendo:

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

# 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 Erlang/Elixir en ejecución |
| **Tiempo de Actividad** | Tiempo desde que se inició la aplicación |

## Aplicaciones en Ejecuci��n

Lista todas las aplicaciones OTP cargadas agrupadas por categoría:

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

Haga 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 Mix actual (Desarrollo/Producción) |
| **Versión de Elixir** | Versión de Elixir en ejecución |

## Lista de Aplicaciones

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

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

# Configuración del Panel de Control

## Puerto HTTP

Configure 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 |

## Deshabilitar el Panel de Control

El panel de control se puede deshabilitar al no iniciar el punto final web en producción si no es necesario. Comuníquese con su integrador de sistemas para obtener 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`:

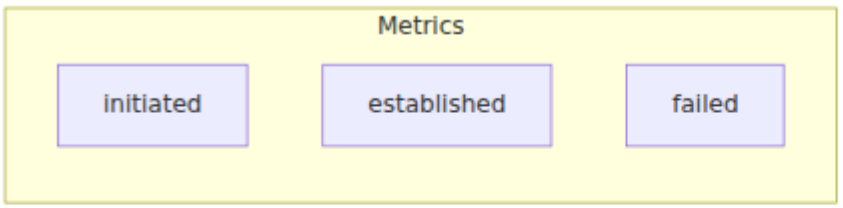
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

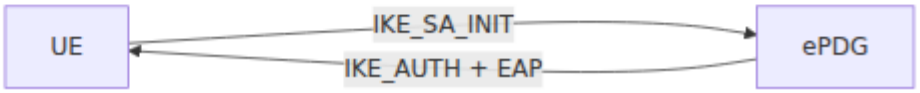
| Parámetro | Tipo | Predeterminado | Var. de Entorno | Descripció |
|---|---|---|---|---|
| `port` | Entero | `9568` | `PROMETHEUS_PORT` | Puerto HTTP para el endpoint `/metrics` |

# 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.

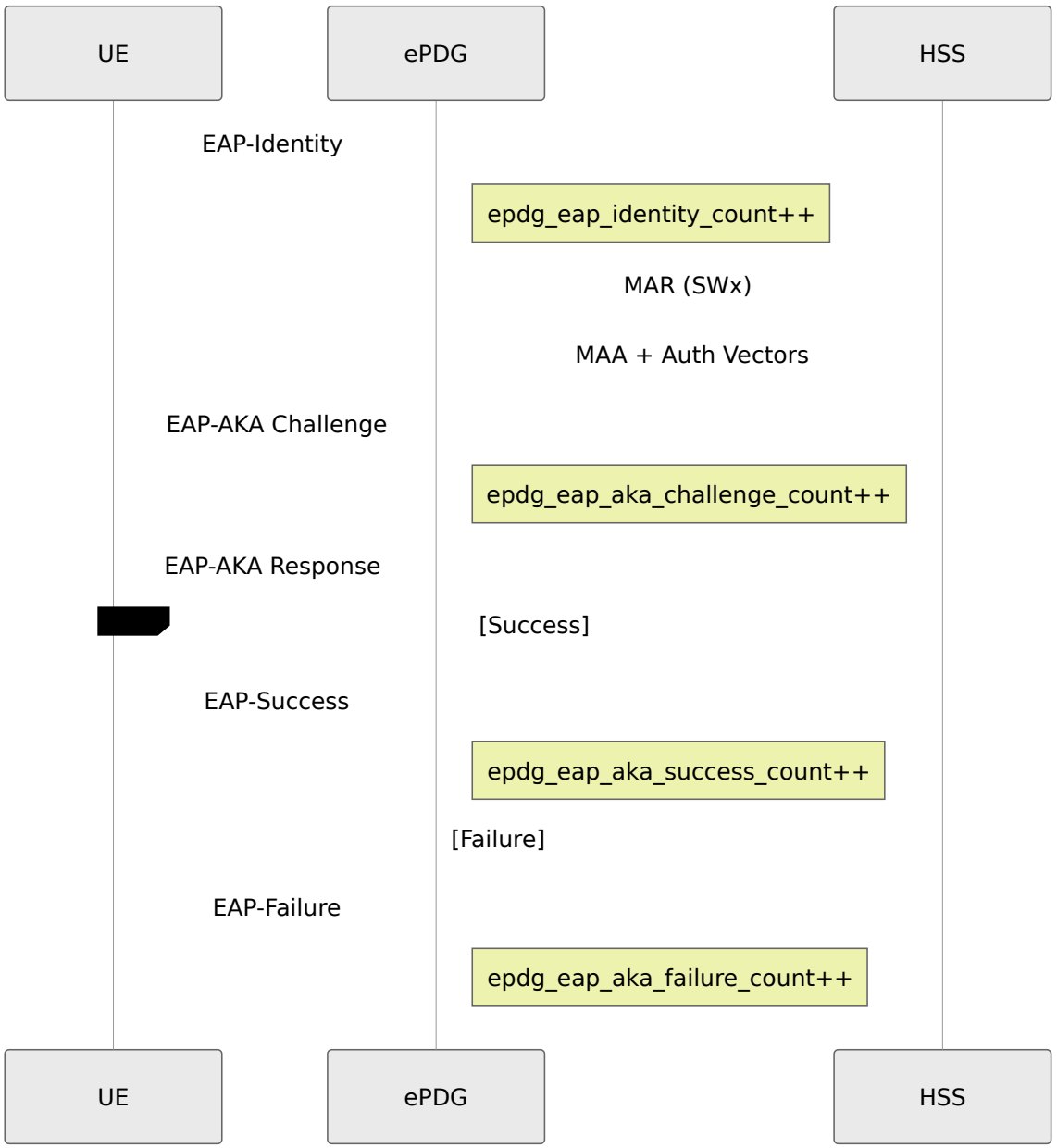
---

**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 los flujos de autenticación EAP-AKA según RFC 4187. OmniEPDG también soporta EAP-AKA' según RFC 5448, con el tipo de autenticación seleccionado automáticamente en función del 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 en el número de secuencia USIM/HSS que requiere resincronización.

## 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 la 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` (límite por IP excedido) o `imsi` (límite 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 en el 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. Se consulta 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 la 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 cercanos 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**: Total de memoria 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 (incluidos los 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 (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"

      # Alta memoria de VM
      - 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 de GeoIP (posible ataque desde una
región específica)
      - alert: OmniEPDGGeoIPBlockingSpike
        expr: |
          rate(epdg_auth_geoip_blocked_count[5m]) > 5
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Actividad de bloqueo GeoIP elevada"
          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 la carga útil
AUTH detectados"
          description: "Posible ataque de hombre en el medio o
error de implementación"
```

# Requisitos de Red

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

# Puertos del Firewall

## Puertos de 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 llamadas WiFi), la conexión se migra automáticamente al puerto 4500.

**Puerto 4500/UDP** transporta tanto la señalización IKEv2 como los datos de usuario cifrados 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 ↔ Núcleo)

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 d��gitos, con ceros a la izquierda hasta 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

# Dominio DNS de Diameter

Para un enrutamiento adecuado de Diameter, 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
```

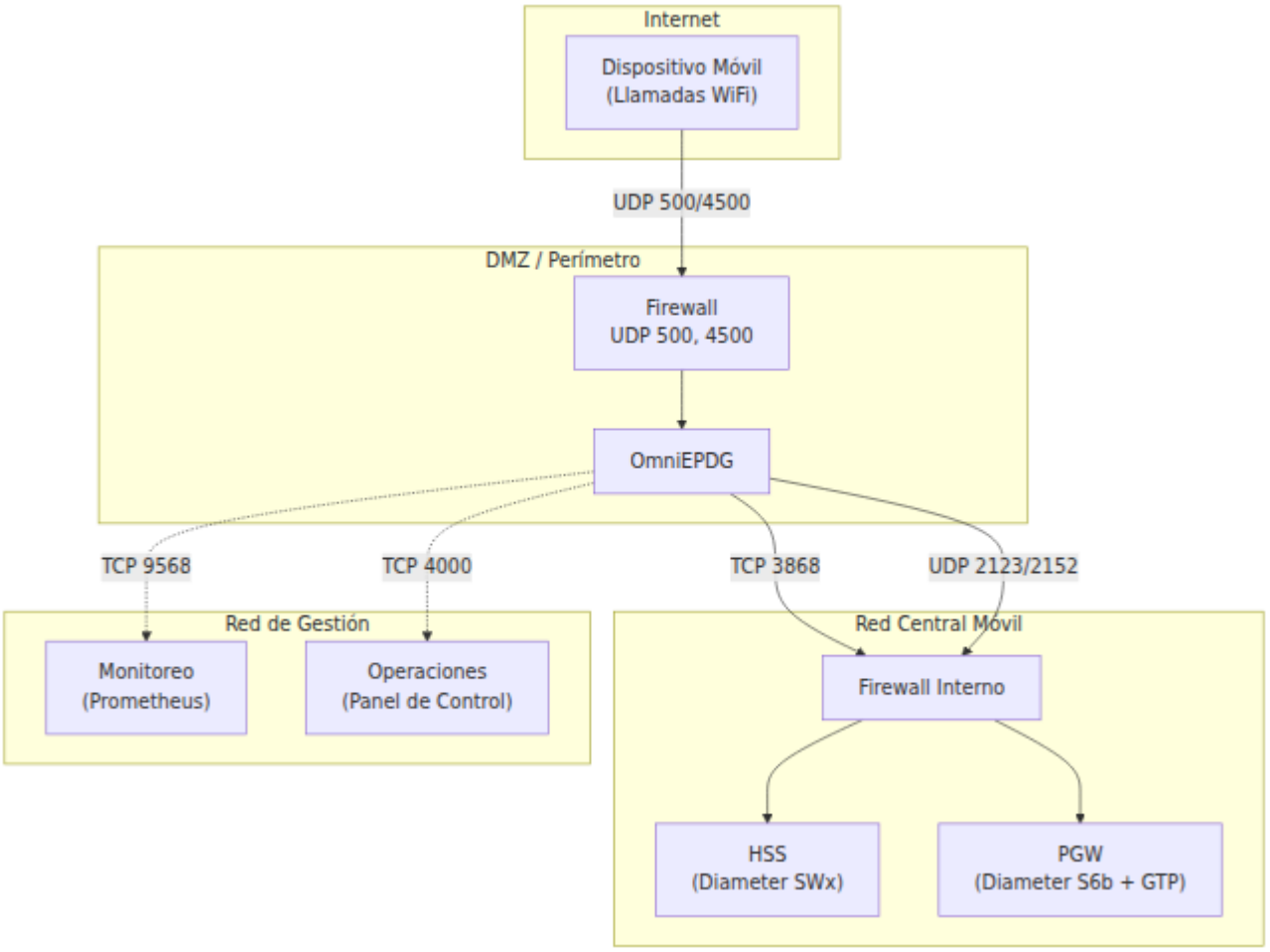
**Ejemplo:**

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

Este dominio se utiliza en:

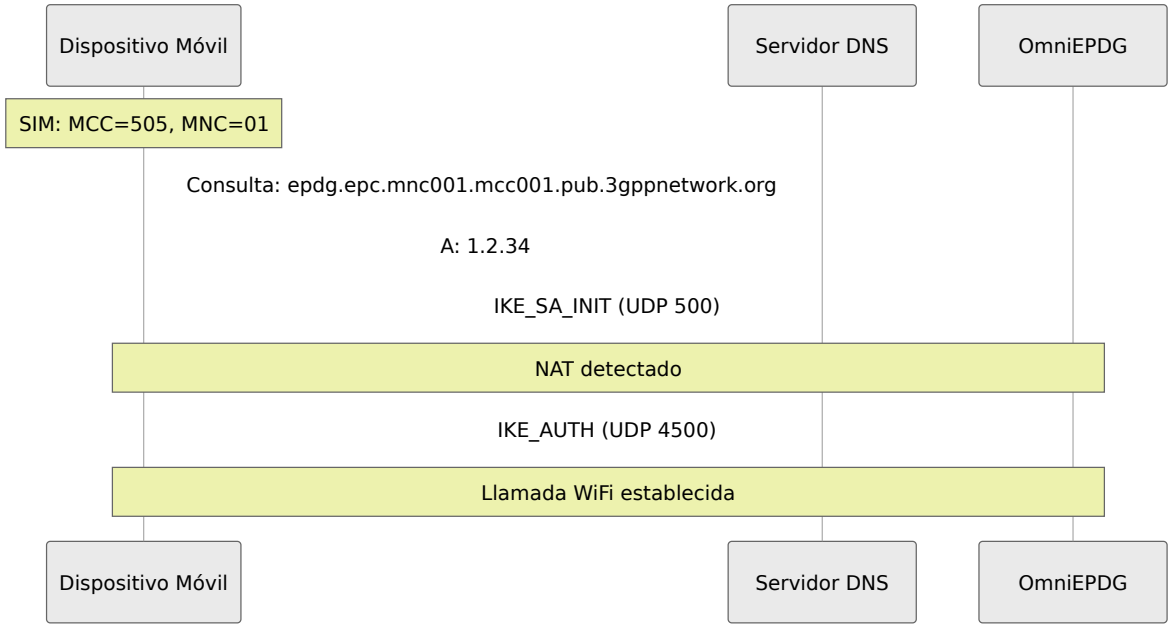
- NAI (Identificador de Acceso a la Red) enviado por el UE durante la autenticación
- AVPs de Diameter Origin-Realm y Destination-Realm
- Decisiones de enrutamiento de Diameter

# 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 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 (solo modo GTP)
- [ ] UDP 2123 abierto entre OmniEPDG y PGW (solo modo GTP)
- [ ] UDP 2152 abierto entre OmniEPDG y PGW (solo modo GTP)

## 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 de Diameter

# Guía de Operaciones de OmniEPDG

OmniEPDG es un ePDG (evolved Packet Data Gateway) compatible con 3GPP que permite llamadas por WiFi al conectar el acceso WiFi no confiable a la red central móvil. Soporta dos modos operativos: **modo GTP** para túneles 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 de la Arquitectura** - Arquitectura del sistema, flujos de llamadas, máquinas de estado y referencias de protocolo

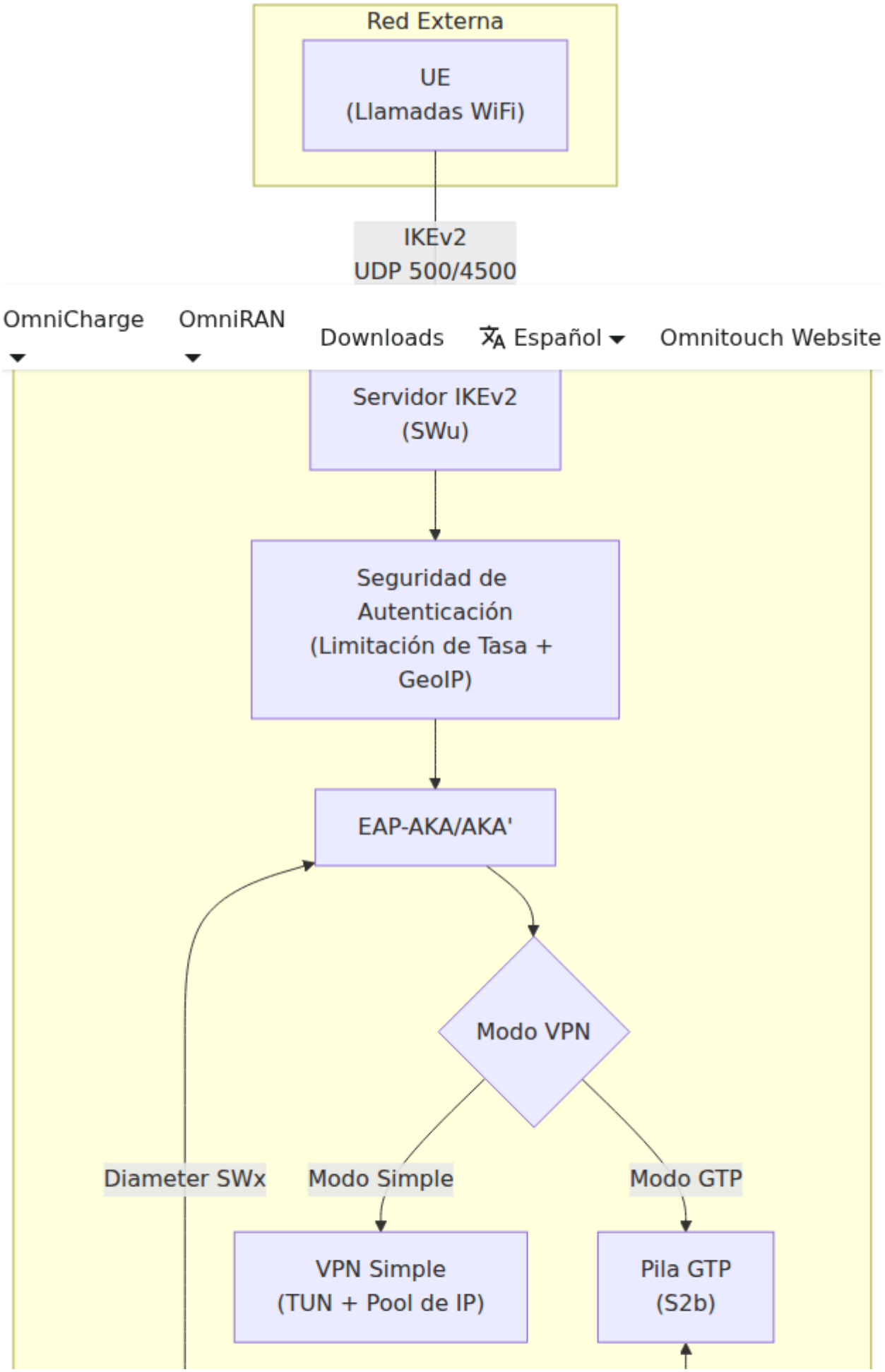
### Operaciones y Monitoreo

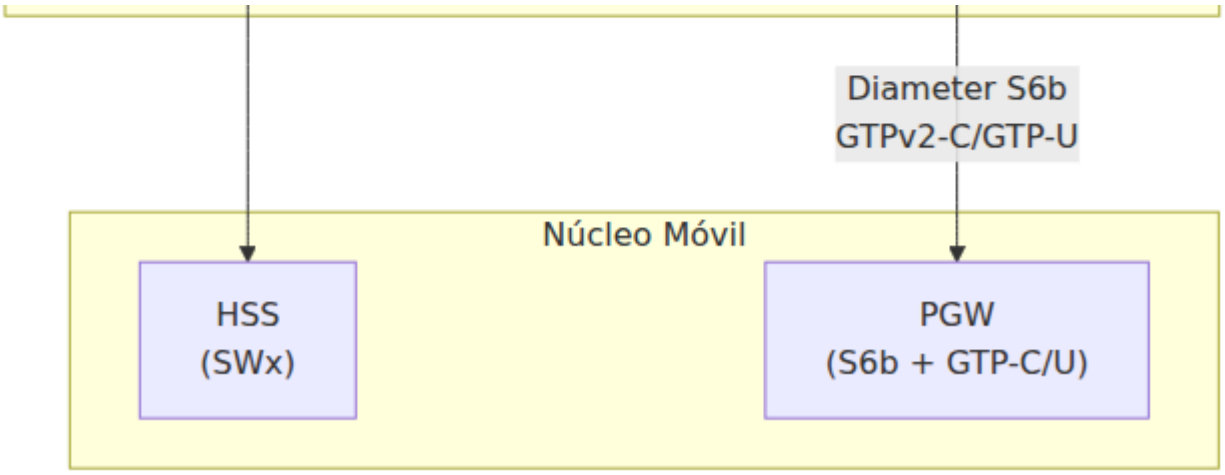
- **Panel de Control** - Interfaz de monitoreo basada en web para sesiones, pares Diameter y registros
- **Referencia de Métricas** - Métricas de Prometheus, consultas de ejemplo y reglas de alerta
- **Solución de Problemas** - Problemas comunes, procedimientos de diagnóstico y pasos de resolución

### Seguridad

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

# Descripción de la Arquitectura


Red Externa
UE
(Llamadas WiFi)
IKEv2
UDP 500/4500
OmniCharge
OmniRAN
Downloads
Español
Omnitouch Website
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

Túnel completo 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 cobro a través de PCRF/PCEF
- Se requiere roaming y traspaso 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 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 desde países especificados
- **Modo de lista negra** - Bloquea conexiones desde 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 de 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 de 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

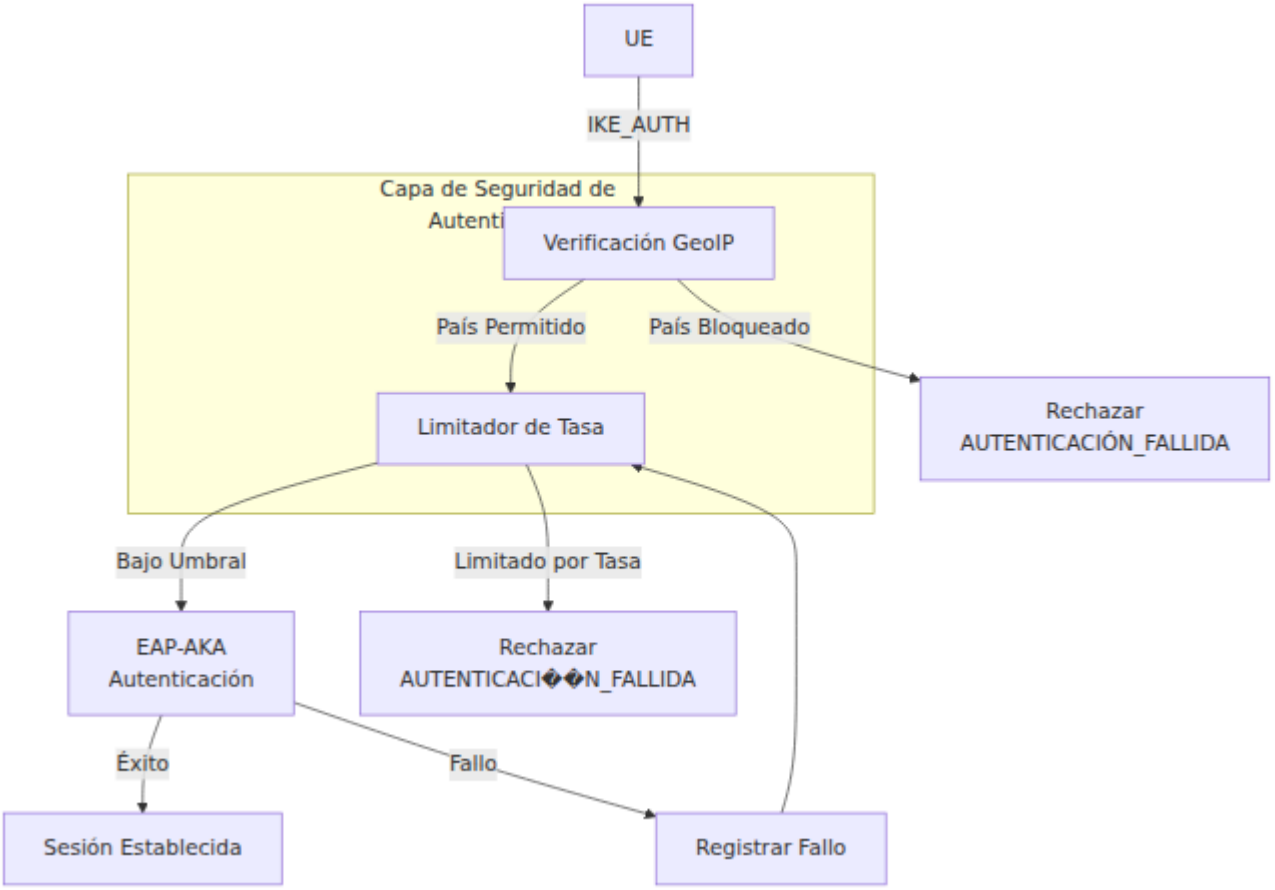
| Documento | Descripción |
|---|---|
| Arquitectura | Diseño del sistema, máquinas de estado, flujos de llamadas, referencias de protocolo |
| Configuración | Referencia completa de configuración con ejemplos |
| Panel de Control | Guía de interfaz web con capturas de pantalla |
| Métricas | Métricas 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 |

# Seguridad de Autenticación de OmniEPDG

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

## Tabla de Contenidos

# Descripción General



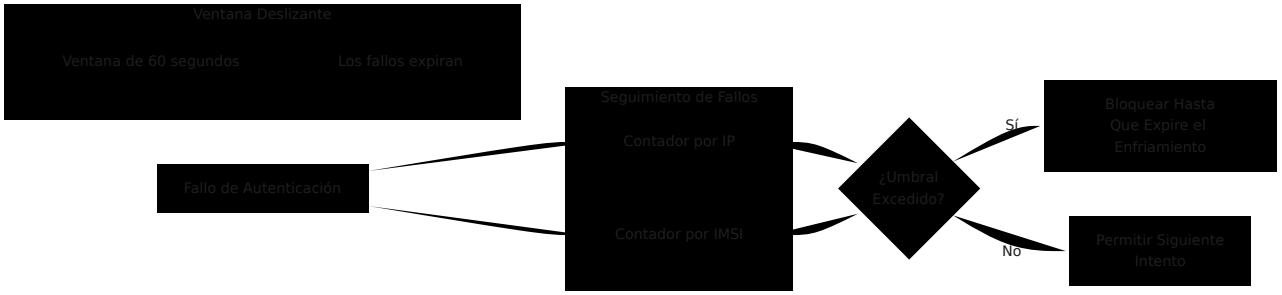

OmniEPDG realiza verificaciones de seguridad al inicio del intercambio IKE_AUTH, antes de operaciones criptográficas costosas:

1. **Verificación 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 excedido los umbrales de fallo
3. **Autenticación EAP-AKA** - La autenticación estándar 3GPP procede si las verificaciones son satisfactorias

# Limitación de Tasa de Autenticación

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

# 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 escáneres de puertos y ataques distribuidos de 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 cualquiera de los umbrales, el intento es rechazado.

## 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 de 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 de 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 a los usuarios legítimos que experimentaron fallos transitorios (por ejemplo, problemas de red) recuperarse sin ser penalizados permanentemente.

## Ejemplos de Configuración

### 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
```

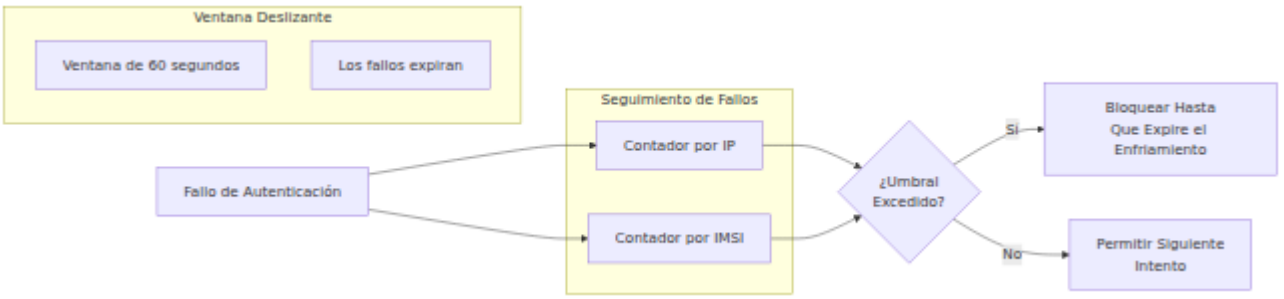
**Cómo funciona:** Umbrales más altos y bloqueos más cortos permiten mayor flexibilidad en las pruebas.

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

# Bloqueo de Países GeoIP

El bloqueo GeoIP restringe el acceso a llamadas WiFi según 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 MaxMind GeoLite2

Las verificaciones GeoIP utilizan la base de datos de País GeoLite2 de MaxMind, una base de datos de geolocalización IP gratuita con actualizaciones semanales.

**Para habilitar el bloqueo GeoIP:**

1. Regístrate para obtener una cuenta gratuita en MaxMind GeoLite2 Signup
2. Descarga el archivo de base de datos `GeoLite2-Country.mmdb`
3. Coloca el archivo en la ruta configurada (predeterminado: `/etc/omniepdg/GeoLite2-Country.mmdb`)
4. Habilita GeoIP en la configuración

# Configuración

```
config :omniepdg,
  # Habilitar bloqueo GeoIP
  geoip_enabled: true,

  # Ruta a la base de datos de MaxMind
  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 |
|---|---|---|---|
| `geoip_enabled` | Booleano | No | `false` |
| `geoip_database_path` | Cadena | No | `"/etc/omniepdg/GeoLite2 Country.mmdb"` |
| `geoip_mode` | Átomo | No | `:whitelist` |
| `geoip_countries` | Lista | No | `[]` |

| Parámetro | Tipo | Requerido | Predeterminado |
| --- | --- | --- | --- |
| `geoip_allow_unknown` | Booleano | No | Ver a continuación |
| `geoip_fail_open` | Booleano | No | `true` |

# Modos de Control de Acceso

### Modo de Lista Blanca (Recomendado para Llamadas WiFi)

Solo se permiten 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 las UEs 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 son permitidos.

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

**Cómo funciona:** Las UEs que se conectan desde los países listados son rechazadas. 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 se pueden geolocalizar:

- 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 VPNs

El parámetro `geoip_allow_unknown` controla el comportamiento:

| Modo | Valor Predeterminado de `geoip_allow_unknown` | 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 valor 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. Descarga el nuevo archivo `GeoLite2-Country.mmdb`
2. Reemplaza el archivo existente en la ruta configurada
3. La base de datos se recarga automáticamente en la próxima verificación (no se requiere reinicio)

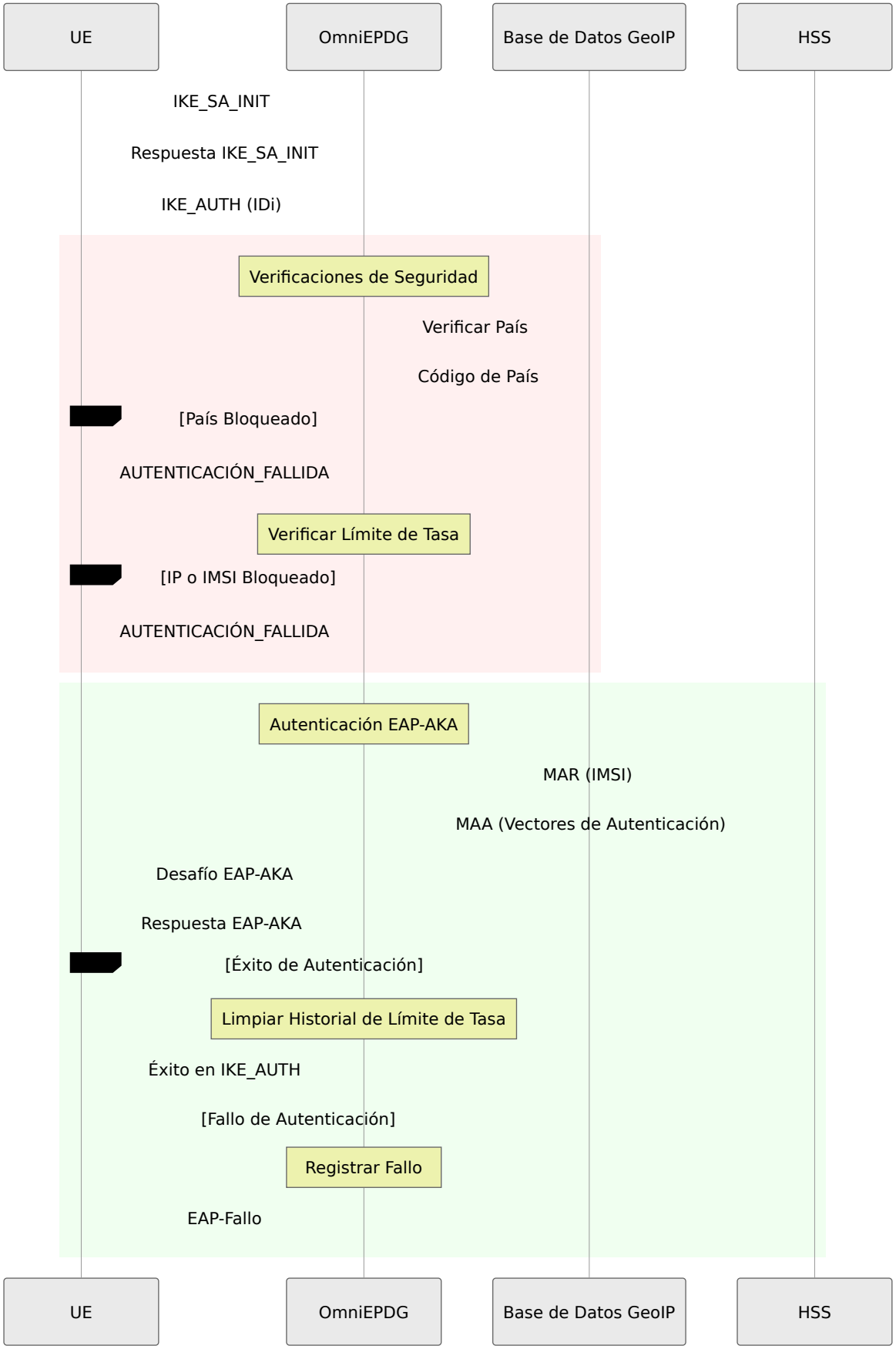
## Códigos de País Comunes

| 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
Verificar 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 en 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 excedido) o `imsi` (umbral de 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]))

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

## Métricas 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 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. Verificar métricas para la IP/IMSI afectada
2. Considerar 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 configurada fallando repetidamente la autenticación
- Ataque de relleno de credenciales

**Resolución**:

1. Revisar IPs de origen en los registros para patrones
2. Considerar implementar reglas de firewall a nivel de IP para atacantes persistentes
3. Verificar conectividad HSS si los usuarios legítimos se ven afectados

# Problemas GeoIP

### Todas las Conexiones Siendo Bloqueadas

**Síntomas**: Ninguna 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 entorno de laboratorio

**Resolución**:

1. Verificar que el archivo de base de datos exista en la ruta configurada
2. Comprobar que los códigos de país sean correctos (mayúsculas, 2 letras)
3. Para laboratorio/desarrollo, establecer `geoip_allow_unknown: true`
4. Revisar registros para 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 que impiden la lectura

- El archivo no es un formato MMDB válido

**Resolución**:

1. Verificar que el archivo exista: `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. Comprobar permisos: `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. Verificar 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 ubicación inesperada

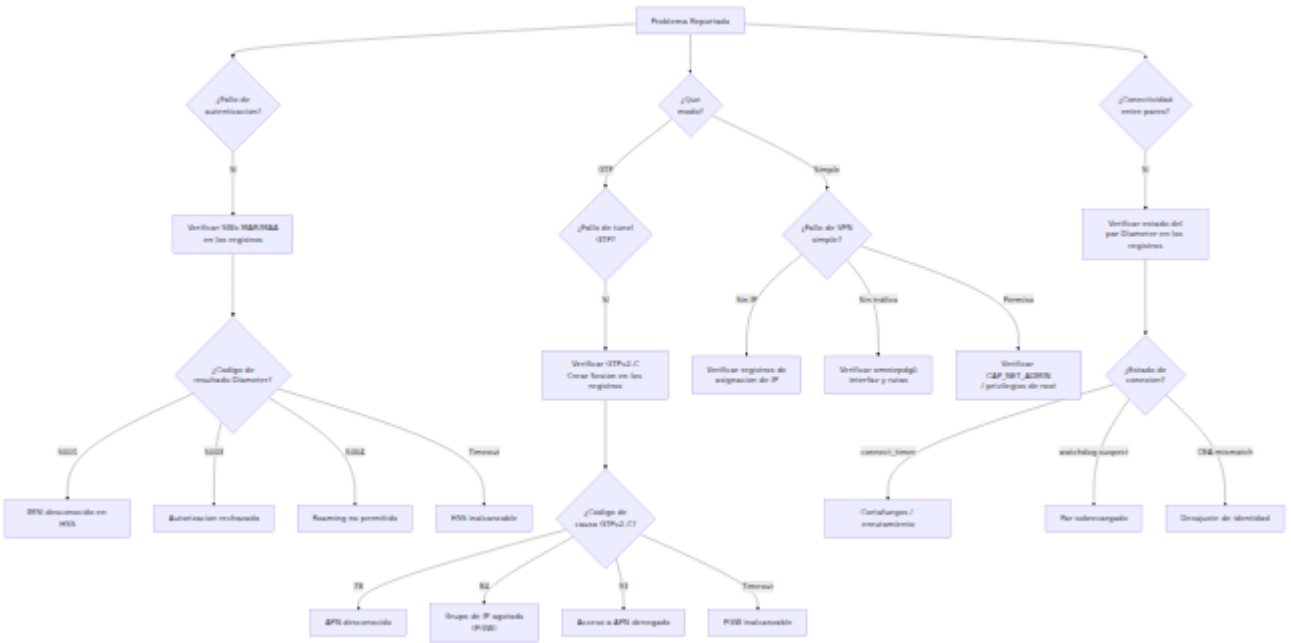
**Resolución**:

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

# OmniEPDG Solución de Problemas

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 en 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 en los Registros

**Eventos de conexión de pares Diameter:**

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

**Transiciones de estado de FSM de UE:**

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

**Eventos de tiempo de espera:**

- `Timeout swm_der_timeout` - Tiempo de espera de respuesta SWm DER agotado
- `Timeout create_session_timeout` - Tiempo de espera de respuesta GTPv2-C Crear Sesión agotado

- `Timeout s2b_delete_session_timeout` - Tiempo de espera de respuesta GTPv2-C Eliminar Sesión agotado
- `Timeout cancel_location_timeout` - Tiempo de espera de respuesta Cancelar Ubicación agotado

# 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**:

- Cortafuegos bloqueando el puerto SCTP 3868 entre OmniEPDG y HSS
- `dia_swx_remote_ip` o `dia_swx_remote_port` incorrectos en la configuración
- HSS no funcionando o no aceptando conexiones Diameter
- SCTP no habilitado en la ruta de red (algunos cortafuegos 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 cortafuegos. 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 nunca llega un AAR S6b del PGW. Los registros no muestran ningún evento peer_up de S6b.

**Causas posibles**:

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

**Resolución**:

1. Confirmar que el PGW esté configurado para conectarse a OmniEPDG en `dia_s6b_local_ip`:`dia_s6b_local_port`
2. Verificar que la dirección de enlace S6b sea accesible desde la red del PGW
3. Comprobar que las reglas del cortafuegos 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 Vigilante Diameter

**Síntomas**: Las conexiones Diameter establecidas se caen intermitentemente. Los registros muestran transiciones del vigilante a estado SUSPECT o DOWN.

**Causas posibles**:

- Inestabilidad en la ruta de red o pérdida de paquetes
- Par sobrecargado y no respondiendo a DWR dentro de `dia_swx_watchdog_timer`
- Configuración agresiva del vigilante (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 par
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 par (CPU, memoria, conteo de conexiones)

# 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 la SIM de 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 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 de SWx caída durante la solicitud
- HSS sobrecargado

**Resolución**:

1. Verificar la capacidad de respuesta y carga del HSS
2. Confirmar que el par Diameter de 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 de UE no coincide con el método EAP utilizado.

**Causas posibles**:

- 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 de la UE. La mayoría de los UEs de llamadas WiFi utilizan el prefijo `0` (EAP-AKA).

**Resolución**:

1. Verificar la identidad NAI de la UE en los registros para confirmar 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 error "RES mismatch" o "res_mismatch".

**Causas posibles**:

- Fallo de autenticación de la tarjeta SIM
- Desajuste en la derivación de claves entre UE y 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 devolvió 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 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 creación de 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 | Comprobar que la política del PGW permita el tipo de acceso WiFi (no-3GPP) |
| 84 | Todos los 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 el APN en el PGW |
| 96 | IMSI/IMEI Desconocido | Suscriptor desconocido para el 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 accesible en `gtpc_remote_ip`:`gtpc_remote_port`
- Cortafuegos 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 cortafuegos 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 núcleo 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 del túnel GTP
- Cortafuegos bloqueando el puerto UDP 2152 (GTP-U)

**Resolución**:

1. Verificar que el módulo GTP del núcleo de Linux esté cargado (`lsmod | grep gtp`)
2. Confirmar que el dispositivo del 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 del túnel GTP
5. Verificar que el cortafuegos 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 núcleo TUN/TAP no cargado
- Otro proceso ya ha creado una interfaz llamada `omniepdg0`

**Resolución**:

1. Verificar que el módulo del núcleo 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 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 están cerrando 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 pueden 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 del cortafuegos 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 Crash

**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**:

- FSM se bloqueó antes de que la ruta pudiera ser eliminada
- El proceso de OmniEPDG fue asesinado sin un apagado ordenado

**Resolución**:

1. Revisar `log/crash.log` en busca de caídas de procesos 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 Detiene Durante la Desregistración

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

**Causas posibles**:

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

- Tiempo de espera en cascada no completándose debido a múltiples tiempos de espera acumulándose

**Resolución**:

1. Verificar los registros para mensajes de tiempo de espera en el estado relevante
2. Verificar la conectividad con 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 núcleo después de que las sesiones terminan. `ip link show gtp0` muestra que el dispositivo aún tiene contextos PDP activos.

**Causas posibles**:

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

**Resolución**:

1. Revisar `log/crash.log` en busca de caídas de procesos 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 se bloquee al iniciar
- Dependencia externa no disponible (por ejemplo, biblioteca gen_socket no encontrada)
- Par Diameter enviando mensajes malformados que causan bloqueos de 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 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 (estos deberían 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

# Guía de Operaciones de OmniEPDG

OmniEPDG es un Gateway de Datos por Paquete (ePDG) evolucionado 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 un Gateway de Paquete (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 compatible con 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

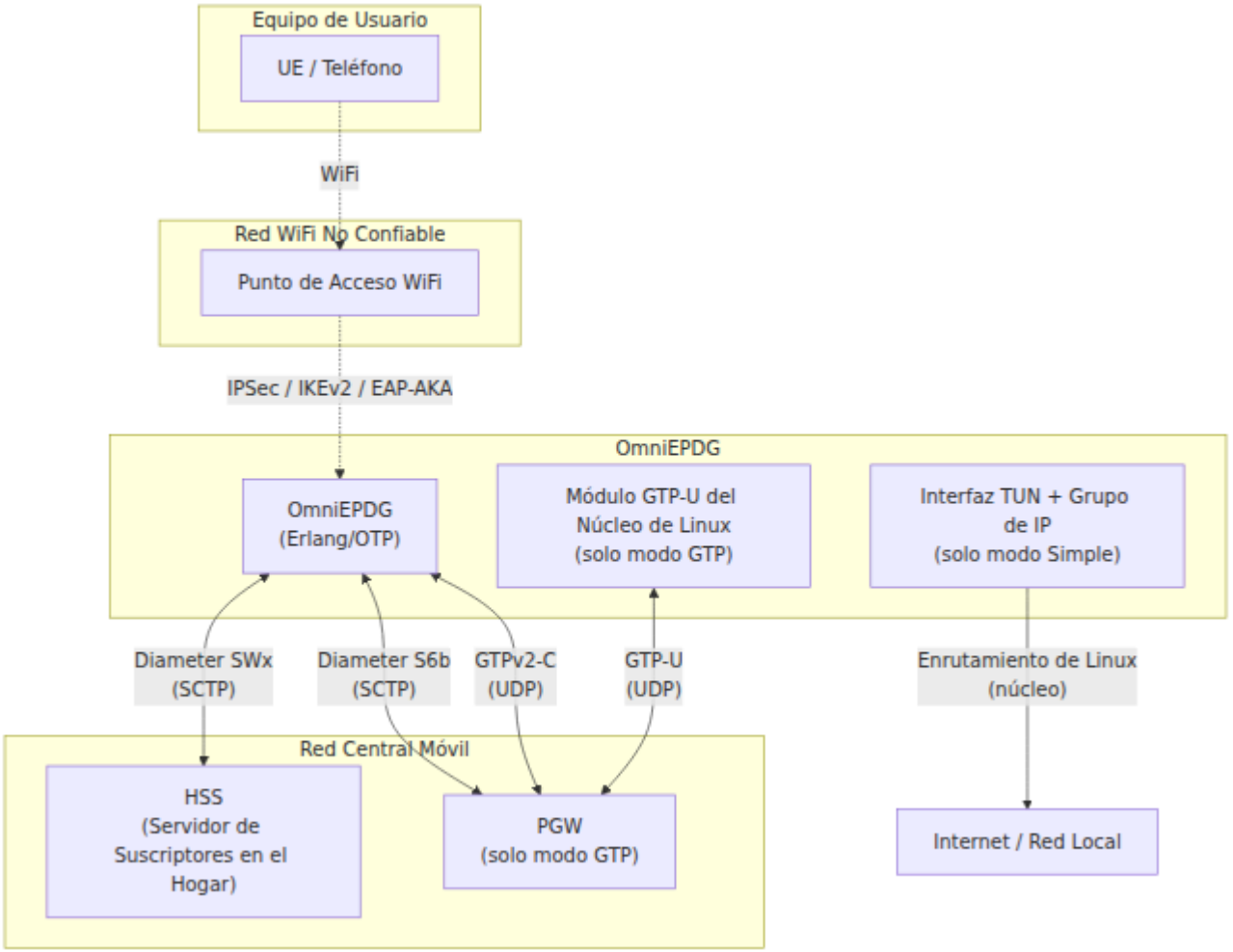
## Seguridad

- **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 canaliza todo el tráfico de suscriptores 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 compatible con 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 de suscriptores 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 ocurre 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 del Servidor HSS, reduciendo el tiempo de configuración de la conexión. Esto significa que el HSS no rastreará qué ePDG sirve al suscriptor y los procedimientos iniciados por el HSS (deregistro, envío de perfil) no funcionarán. Adecuado para implementaciones privadas sin requisitos de roaming.

## Comparación de Modos

| Capacidad | Modo GTP | Modo VPN Simple |
|---|---|---|
| Compatible con 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`) |
| Desmontaje iniciado por PGW | Sí | N/A |
| Soporte para roaming | 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 Principal

- **Autenticación EAP-AKA** - Autenticación de suscriptores EAP-AKA completamente compatible con 3GPP a través de HSS
- **Gestión de Túneles IPSec** - Túnel seguro basado en IKEv2 entre UE y ePDG
- **Dos Modos Operativos** - Túnel GTP hacia 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 y 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
- **Desmontaje Iniciado por PGW** - PGW envía Solicitud de Eliminación de Bearer, ePDG cascada el desmontaje hacia UE
- **Desmontaje Iniciado por la Red** - HSS desencadena el deregistro a través de SWx RTR, ePDG desmonta todas las sesiones
- **Re-Autenticación** - Envío de perfil y re-autorización desencadenados 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 de Linux estándar (`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 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 en lista blanca o negra utilizando MaxMind GeoLite2
- **Detección de Pares Muertos** - Monitoreo activo de vitalidad con sondas configurables
- **Protección Anti-Repetición ESP** - Ventana deslizante de 64 bits conforme a RFC 4303

# Integración 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 PGW (Solo Modo GTP)

**S6b Diameter:**

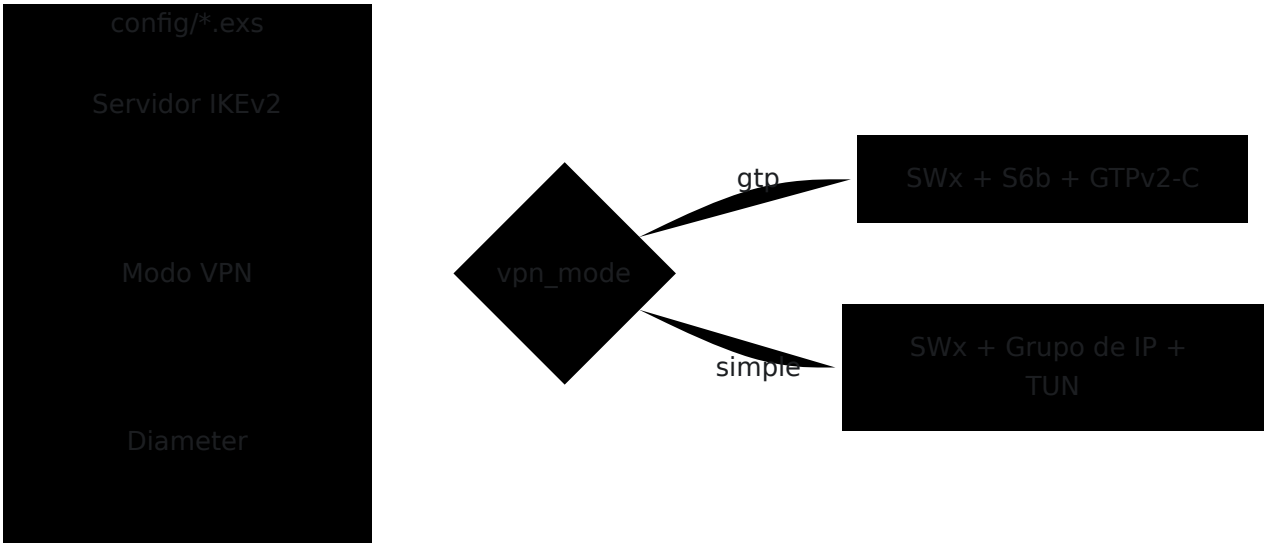
- **Solicitud/Respuesta AA (AAR/AAA)** - Autorizar sesiones PGW
- **Solicitud/Respuesta de Terminación de Sesión (STR/STA)** - Terminar sesiones PGW
- **Solicitud/Respuesta de Re-Autenticación (RAR/RAA)** - Re-autorizar sesiones activas
- **Solicitud/Respuesta de Abort-Session (ASR/ASA)** - Terminar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

**S2b GTPv2-C:**

- **Solicitud/Respuesta de Crear Sesión** - Establecer túneles GTP con asignación de TEID
- **Solicitud/Respuesta de Eliminar Sesión** - Desmontar túneles GTP
- **Solicitud/Respuesta de Eliminar Bearer** - Gestión de bearer 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 de enlace TUN) | 10.44.0.1 | IP de puerta de enlace 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 | Diameter Cx/Dx (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 parámetros de implementación
3. Revise la Guía de Seguridad para configurar limitación de tasa y bloqueo por GeoIP
4. Configure el monitoreo utilizando la Referencia de Métricas para la integración de 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 cumplimiento de protocolos