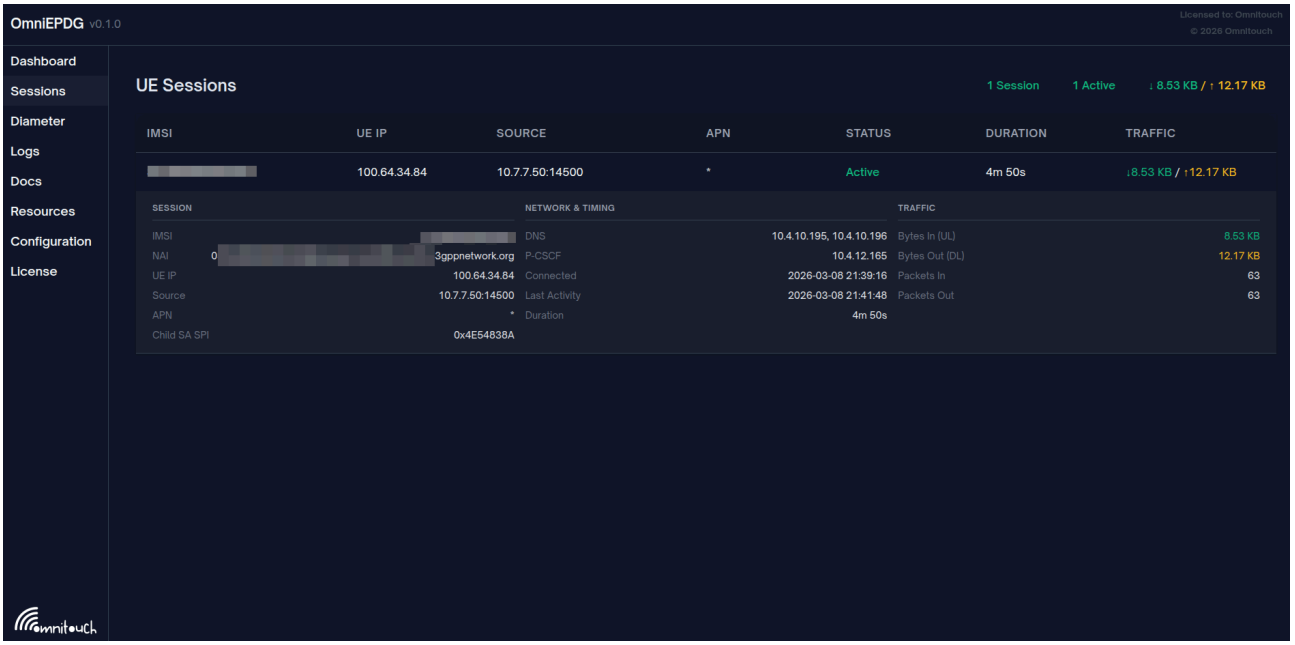
Guia de Operações do OmniEPDG

OmniEPDG é um Gateway de Dados de Pacote Evoluído (ePDG) que permite chamadas de Voz sobre WiFi (VoWiFi). Ele autentica assinantes móveis em redes WiFi não confiáveis usando EAP-AKA e os conecta à rede central móvel através de sinalização Diameter para o HSS e túneis GTP para um Gateway de Pacote (PGW).



O painel de controle do OmniEPDG mostrando uma sessão de assinante ativa com estatísticas de tráfego em tempo real.

OmniEPDG suporta dois modos operacionais:

- **Modo GTP** (padrão) - Tunelamento totalmente compatível com 3GPP através de um PGW via GTPv2-C e GTP-U
- **Modo VPN Simples** - Saída local com um pool de IP embutido e interface TUN do Linux, sem necessidade de PGW

Documentação

Configuração e Operações

- **Arquitetura e Fluxos de Chamadas** - Arquitetura do sistema, interfaces de protocolo, máquinas de estado do UE e diagramas de sequência de mensagens para ambos os modos
- **Referência de Configuração** - Documentação completa dos parâmetros para Diameter, GTPv2-C, GTP-U, VPN Simples e registro
- **Painel de Controle** - UI de monitoramento baseada na web para sessões, pares Diameter e logs

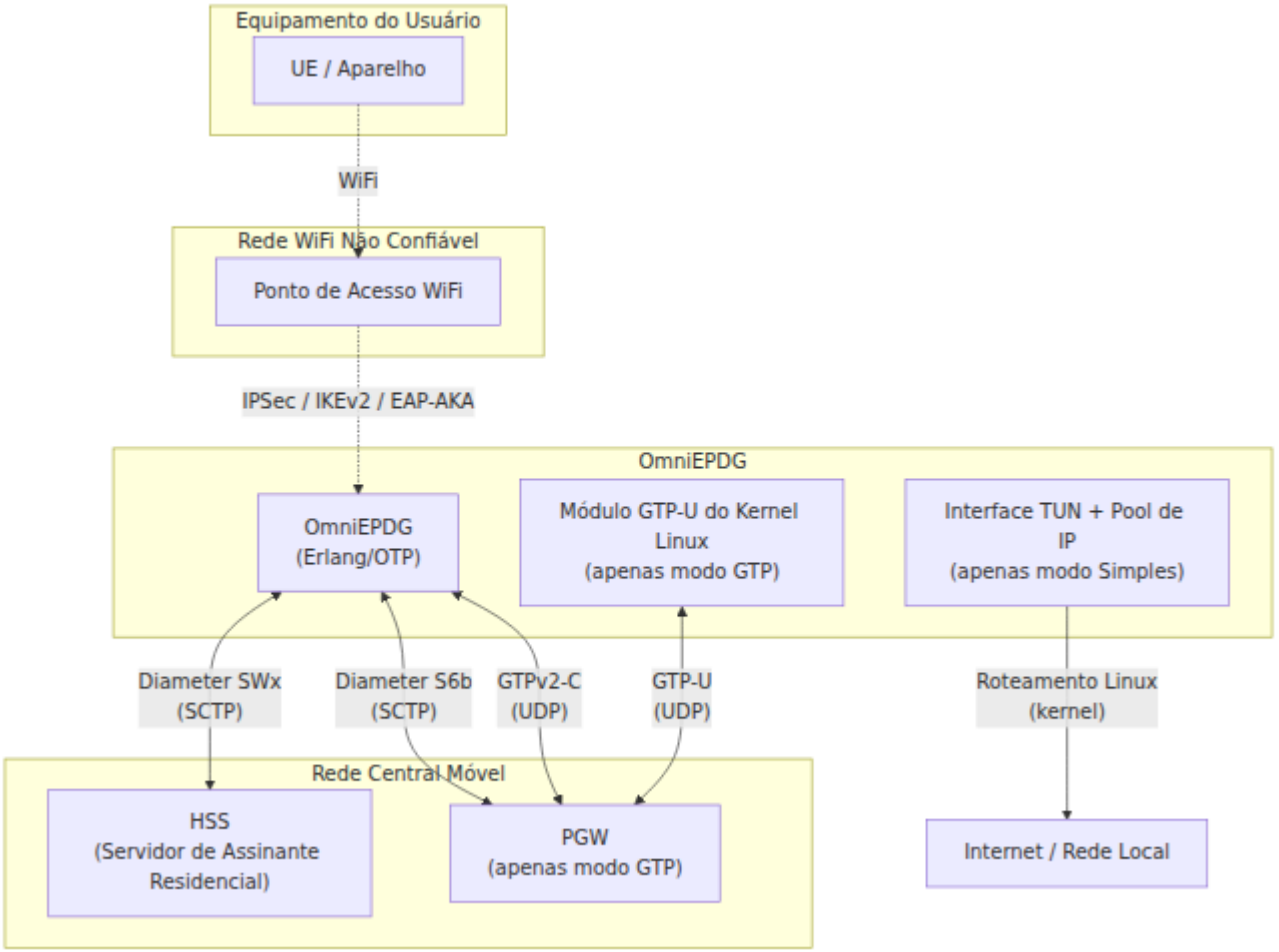
Segurança

- **Guia de Segurança** - Limitação da taxa de autenticação e bloqueio de países GeoIP

Monitoramento e Solução de Problemas

- **Referência de Métricas** - Métricas Prometheus para monitoramento de autenticação, sessões, sinalização Diameter e saúde do sistema
- **Solução de Problemas** - Problemas comuns, procedimentos de diagnóstico e etapas de resolução

Modos Operacionais



Modo GTP

O modo padrão. OmniEPDG tunela todo o tráfego do assinante através de um PGW usando GTPv2-C para controle de sessão e GTP-U (via módulo do kernel Linux) para o plano do usuário. Isso é totalmente compatível com 3GPP e adequado para implantações de operadoras com infraestrutura EPC existente.

Caminho do tráfego: UE → IPSec → OmniEPDG → GTPv2-C Criar Sessão → túnel GTP-U → PGW → Internet

Infraestrutura necessária: HSS, PGW

Modo VPN Simples

OmniEPDG aloca endereços IP de um pool local e roteia o tráfego do assinante diretamente através de uma interface TUN do Linux (`tun_epdg`) usando roteamento padrão do kernel. Nenhuma infraestrutura de PGW ou GTP é necessária. A autenticação ainda ocorre via Diameter SWx para o HSS.

Caminho do tráfego: UE → IPSec → OmniEPDG → Alocação de IP local → interface TUN → roteamento Linux → Internet

Infraestrutura necessária: Apenas HSS (PGW não necessário)

Otimização opcional: O flag `skip_sar` ignora a Solicitação/Resposta de Atribuição de Servidor do HSS, reduzindo o tempo de configuração da conexão. Isso significa que o HSS não rastreará qual ePDG atende o assinante e procedimentos iniciados pelo HSS (desregistro, push de perfil) não funcionarão. Adequado para implantações privadas sem requisitos de roaming.

Comparação de Modos

Capacidade	Modo GTP	Modo VPN Simples
Compatível com 3GPP	Sim	Não (com `skip_sar`), Parcial (sem)
PGW necessário	Sim	Não
HSS necessário	Sim	Sim (apenas autenticação)
Alocação de IP	Do PGW	Pool local (CIDR)
Plano do usuário	Módulo GTP-U do kernel	Linux TUN + roteamento
Push de perfil do HSS	Sim (PPR/PPA)	Não
Desregistro do HSS	Sim (RTR/RTA)	Não (com `skip_sar`)
Desmontagem iniciada pelo PGW	Sim	N/A
Suporte a roaming	Sim	Não
IPv6 / Dual-stack	Sim	Apenas IPv4

Interfaces de Protocolo

Interface	Protocolo	Transporte	Modo	Par	Propósito	R
SWu	IKEv2 / IPSec	UDP	Ambos	UE	Tunnel seguro e autenticação EAP-AKA	3 3
SWx	Diameter	SCTP	Ambos	HSS	Vetores de autenticação e atribuição de servidor	3 2 S
S6b	Diameter	SCTP	Apenas GTP	PGW	Autorização de sessão e política	3 2 S
S2b	GTPv2-C / GTP-U	UDP	Apenas GTP	PGW	Controle de túnel e plano do usuário	3 2

Recursos

Funcionalidade Principal

- **Autenticação EAP-AKA** - Autenticação completa de assinantes EAP-AKA via HSS
- **Gerenciamento de Tunnel IPSec** - Tunnel seguro baseado em IKEv2 entre UE e ePDG
- **Dois Modos Operacionais** - Tunelamento GTP para PGW ou saída local com VPN Simples
- **Máquinas de Estado por UE** - FSM Erlang independente por assinante para gerenciamento do ciclo de vida da sessão

- **Suporte a Dual-Stack** - Tipos de endereços PDP IPv4, IPv6 e IPv4v6 (modo GTP)

Recursos do Modo GTP

- **Estabelecimento de Tunnel GTP** - Criação de sessão GTPv2-C e plano do usuário GTP-U via módulo do kernel Linux
- **Desmontagem Iniciada pelo PGW** - PGW envia Solicitação de Exclusão de Bearer, ePDG cascata a desmontagem para UE
- **Desmontagem Iniciada pela Rede** - HSS aciona desregistro via SWx RTR, ePDG desmonta todas as sessões
- **Re-Autenticação** - Push de perfil acionado pelo HSS e re-autorização por 3GPP TS 29.273 Seção 7.1.2.5.1

Recursos do Modo VPN Simples

- **Pool de IP Local** - Alocação de endereços IPv4 baseada em CIDR com rastreamento por IMSI
- **Roteamento da Interface TUN** - Dispositivo TUN padrão do Linux (`tun_epdg`) com rotas de host por UE
- **Configuração de DNS** - Servidores DNS configuráveis fornecidos aos UEs via PCO
- **Otimização SAR Opcional** - Ignorar registro HSS para configuração de conexão mais rápida

Recursos de Segurança

- **Limitação da Taxa de Autenticação** - Proteção contra força bruta por IP e por IMSI com limites configuráveis
- **Bloqueio de Países GeoIP** - Controle de acesso baseado em países em lista branca ou negra usando MaxMind GeoLite2
- **Detecção de Peer Morto** - Monitoramento ativo de vivacidade com sondas configuráveis
- **Proteção Anti-Replay ESP** - Janela deslizante de 64 bits compatível com RFC 4303

Integração com HSS (SWx Diameter)

- **Solicitação/Resposta de Autenticação Multimídia (MAR/MAA)** - Recuperar vetores de autenticação EAP-AKA (ambos os modos)
- **Solicitação/Resposta de Atribuição de Servidor (SAR/SAA)** - Baixar perfil de assinante e configuração de APN (pode ser ignorado no modo Simples)
- **Solicitação/Resposta de Push de Perfil (PPR/PPA)** - Receber perfis de assinante atualizados do HSS (modo GTP)
- **Solicitação/Resposta de Término de Registro (RTR/RTA)** - Desregistro de assinante iniciado pelo HSS (modo GTP)

Integração com PGW (Apenas Modo GTP)

S6b Diameter:

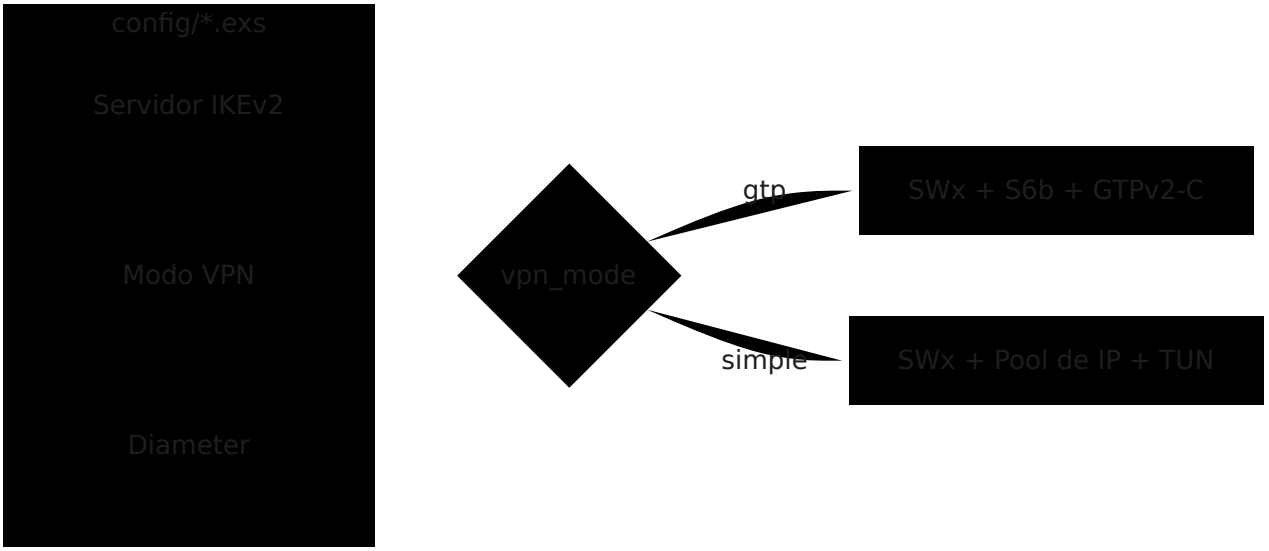
- **Solicitação/Resposta AA (AAR/AAA)** - Autorizar sessões PGW
- **Solicitação/Resposta de Término de Sessão (STR/STA)** - Terminar sessões PGW
- **Solicitação/Resposta de Re-Autenticação (RAR/RAA)** - Re-autorizar sessões ativas
- **Solicitação/Resposta de Abortar Sessão (ASR/ASA)** - Terminar sessões forçadamente

S2b GTPv2-C:

- **Solicitação/Resposta de Criar Sessão** - Estabelecer túneis GTP com alocação de TEID
- **Solicitação/Resposta de Excluir Sessão** - Desmontar túneis GTP
- **Solicitação/Resposta de Excluir Bearer** - Gerenciamento de bearer iniciado pelo PGW

Início Rápido

Estrutura de Configuração



A configuração é feita em `config/runtime.exs` ou através de variáveis de ambiente. O parâmetro `vpn_mode` seleciona entre os modos GTP e VPN Simples. Consulte a Referência de Configuração para a documentação completa dos parâmetros.

Endereçamento de Rede Típico (Modo GTP)

Componente	Endereço IP	Porta	Notas
OmniEPDG (GTP-U)	10.74.0.11	-	Endpoint do túnel GTP-U
OmniEPDG (Diameter S6b)	10.74.0.12	3868	Ouvinte Diameter S6b
HSS	10.74.0.21	3868	Par Diameter SWx
PGW	10.74.0.23	2123	Par GTPv2-C e S6b

Endereçamento de Rede Típico (Modo VPN Simples)

Componente	Endereço IP	Notas
OmniEPDG (gateway TUN)	10.44.0.1	IP do gateway na interface `tun_epdg`
Pool de IP do UE	10.45.0.0/16	Pool CIDR configurável para IPs de assinantes
HSS	10.74.0.21:3868	Par Diameter SWx (apenas autenticação)

Especificações 3GPP

Especificação	Título	Relevância
TS 29.273	Interfaces EPS AAA (SWx, S6b, SWm)	Especificação principal para interfaces Diameter do ePDG
TS 29.274	GTPv2-C e GTP-U	Controle de túnel S2b e plano do usuário (modo GTP)
TS 33.402	Segurança para acessos não 3GPP	Autenticação EAP-AKA para WiFi não confiável
TS 23.402	Melhorias de arquitetura para acessos não 3GPP	Arquitetura e procedimentos gerais do ePDG
TS 23.003	Numeração, endereçamento e identificação	Formato NAI, estrutura IMSI
TS 29.229	Cx/Dx Diameter (definições comuns)	Valores de Tipo de Atribuição de Servidor usados pelo SWx
RFC 6733	Protocolo Base Diameter	Transporte Diameter, gerenciamento de pares, watchdog
RFC 4187	EAP-AKA	Método de autenticação usado sobre IKEv2

Documentação por Função

Operadores de Rede:

1. Comece com a Arquitetura e Fluxos de Chamadas para entender o sistema e ambos os modos operacionais

2. Revise a Referência de Configuração para parâmetros de implantação
3. Revise o Guia de Segurança para configurar limitação de taxa e bloqueio GeoIP
4. Configure o monitoramento usando a Referência de Métricas para integração com Prometheus
5. Mantenha o guia de Solução de Problemas disponível para operações

Integradores de Sistemas:

1. Revise a Arquitetura e Fluxos de Chamadas para detalhes de interface e máquinas de estado
2. Use a Referência de Configuração para configuração de conectividade de pares
3. Configure alertas usando a Referência de Métricas
4. Consulte a tabela de especificações 3GPP acima para conformidade de protocolo

Guia de Operações do OmniEPDG

OmniEPDG é um ePDG (evolved Packet Data Gateway) compatível com 3GPP que permite chamadas via WiFi, conectando acesso WiFi não confiável à rede central móvel. Ele suporta dois modos operacionais: **modo GTP** para tunelamento PGW e **modo VPN Simples** para saída de IP local.

Links Rápidos

Configuração & Implantação

- **Requisitos de Rede** - Portas de firewall e entradas DNS necessárias para a implantação
- **Referência de Configuração** - Documentação completa dos parâmetros para IKEv2, Diameter, modos VPN e todas as configurações em tempo de execução
- **Visão Geral da Arquitetura** - Arquitetura do sistema, fluxos de chamadas, máquinas de estado e referências de protocolo

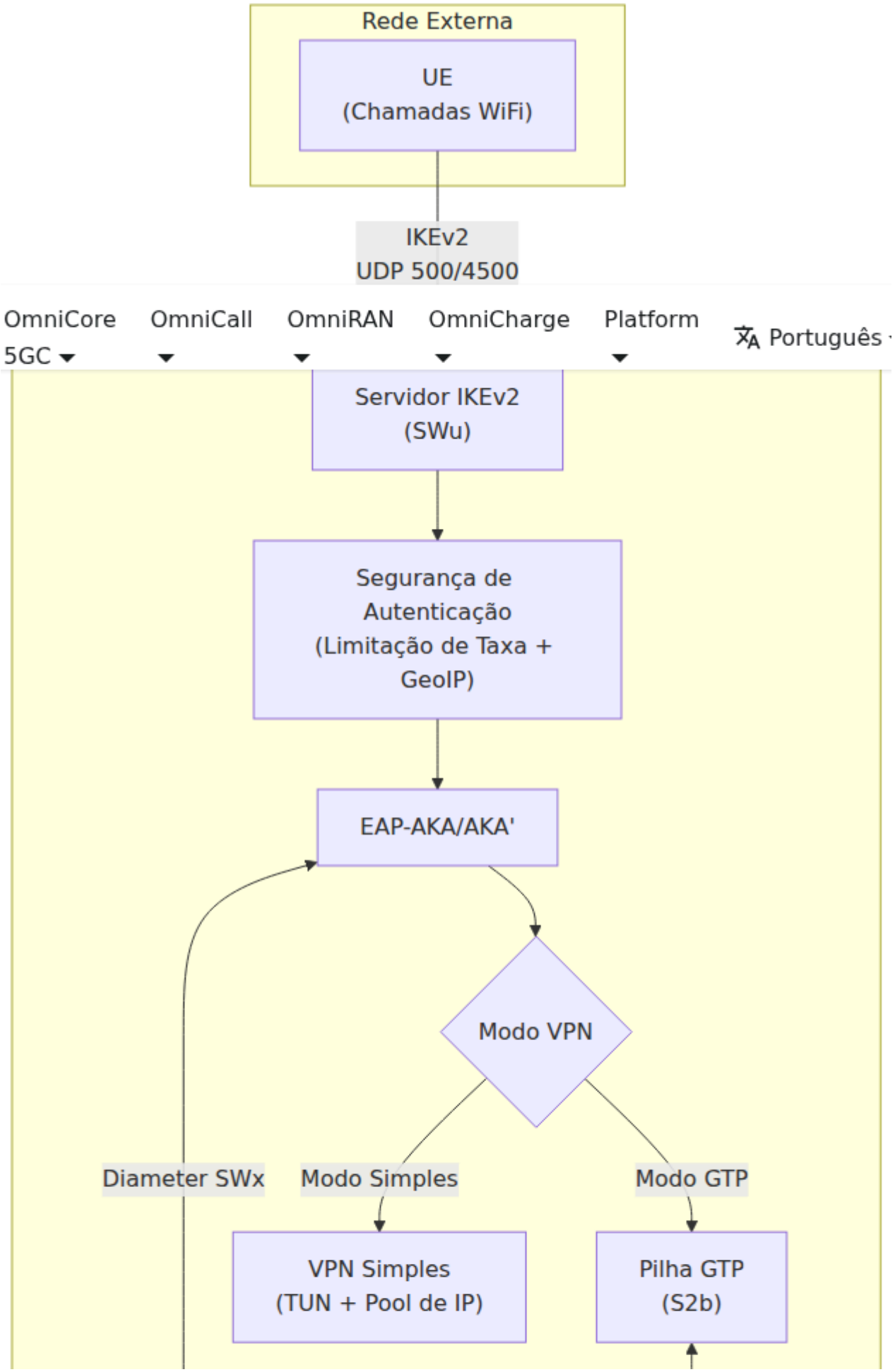
Operações & Monitoramento

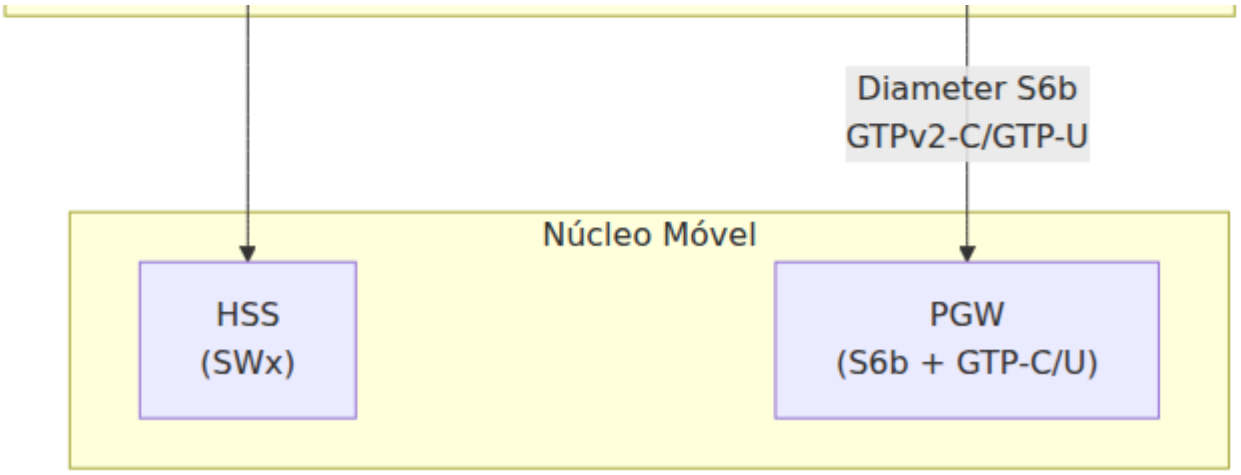
- **Painel de Controle** - Interface de monitoramento baseada na web para sessões, pares Diameter e logs
- **Referência de Métricas** - Métricas Prometheus, consultas de exemplo e regras de alerta
- **Webhooks** - Notificações de ciclo de vida de sessão de saída ao anexar e desanexar
- **Solução de Problemas** - Problemas comuns, procedimentos de diagnóstico e etapas de resolução

Segurança

- **Segurança de Autenticação** - Limitação de taxa e bloqueio de países por GeoIP

Visão Geral da Arquitetura


Rede Externa
UE
(Chamadas WiFi)
IKEv2
UDP 500/4500
OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platform
Português
Servidor IKEv2
(SWu)
Segurança de
Autenticação
(Limitação de Taxa +
GeoIP)
EAP-AKA/AKA'
Modo VPN
Diameter SWx
Modo Simples
Modo GTP
VPN Simples
(TUN + Pool de IP)
Pilha GTP
(S2b)



Modos Operacionais

OmniEPDG suporta dois modos operacionais selecionados através do parâmetro de configuração `vpn_mode`.

Modo GTP

Tunelamento completo 3GPP através de um PGW. O tráfego do assinante é encapsulado em GTP-U e roteado através do núcleo móvel.

Usar quando:

- Integração com infraestrutura central móvel existente
- Política e cobrança através de PCRF/PCEF
- Roaming e transferência entre operadores necessárias

Componentes:

- Diameter S6b para autorização de sessão PGW
- GTPv2-C para gerenciamento de sessão (Criar/Excluir/Modificar Sessão)
- Módulo GTP-U do kernel Linux para plano de usuário

Modo VPN Simples

Saída de IP local via interface TUN. O tráfego do assinante é roteado diretamente através do host OmniEPDG sem envolvimento do PGW.

Usar quando:

- Implantação independente sem PGW
- Testes e desenvolvimento
- Cenários de saída local

Componentes:

- Gerenciamento de pool de IP local (IPv4/IPv6)
- Interface TUN (`omniepdg0`) com rotas de host por assinante
- NAT/mascaramento opcional para acesso à internet

Segurança de Autenticação

OmniEPDG inclui recursos de segurança integrados para proteger contra ataques de força bruta e restringir o acesso por localização geográfica. Consulte o guia de Segurança de Autenticação para detalhes.

Limitação de Taxa

Protege contra ataques de força bruta rastreando tentativas de autenticação falhadas:

- **Limitação por IP** - Bloqueia IPs após 10 falhas em 1 minuto (bloqueio de 5 minutos)
- **Limitação por IMSI** - Bloqueia IMSIs após 5 falhas em 1 minuto (bloqueio de 10 minutos)
- Algoritmo de janela deslizante com expiração automática
- Autenticação bem-sucedida limpa o histórico de falhas

Bloqueio de Países por GeoIP

Controle de acesso geográfico opcional usando o banco de dados MaxMind GeoLite2:

- **Modo de Lista Branca** - Permitir apenas conexões de países especificados
- **Modo de Lista Negra** - Bloquear conexões de países especificados

- Manipulação configurável de IPs desconhecidos/privados
- Comportamento de falha aberta ou fechada quando o banco de dados não está disponível

Configuração Chave

Configuração Mínima (Modo VPN Simples)

```
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}
    ]
  }
```

Ativar Segurança de Autenticação

```
config :omniepdg,
  # Limitação de taxa (ativada por padrão com esses 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,

  # Bloqueio GeoIP (desativado por padrão)
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ"]
```

Consulte a Referência de Configuração para documentação completa dos parâmetros.

Monitoramento

Painel de Controle

Acesse o painel de controle web em `http://<host>:4000/dashboard` para:

- Monitoramento de sessão em tempo real
- Status dos pares Diameter
- Streaming de logs ao vivo
- Configuração do sistema

Consulte o guia do Painel de Controle para detalhes.

Métricas Prometheus

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

- Taxas de sucesso/falha de autenticação
- Eventos de ciclo de vida da sessão
- Latência de sinalização Diameter

- Eventos de segurança (limitação de taxa, bloqueios GeoIP)
- Utilização do pool de IP
- Estatísticas do plano de dados ESP

Consulte a Referência de Métricas para consultas e regras de alerta.

Solução de Problemas

Problemas comuns e etapas de resolução:

Problema	Verificação Rápida	Seção do Guia
Falhas de autenticação	Verifique SWx MAR/MAA nos logs	Falhas de Autenticação
Problemas de conexão Diameter	Verifique o status do par no painel de controle	Conectividade Diameter
Falhas de túnel GTP	Verifique os códigos de causa GTPv2-C	Falhas de Túnel GTP
Problemas de VPN Simples	Verifique a interface TUN e rotas	Falhas de VPN Simples
Falsos positivos de limitação de taxa	Ajuste os limites	Problemas de Limitação de Taxa
Problemas de bloqueio GeoIP	Verifique o banco de dados e códigos de país	Problemas GeoIP

Consulte o guia de Solução de Problemas para procedimentos de diagnóstico detalhados.

Índice de Documentação

Documento	Descrição
Arquitetura	Design do sistema, máquinas de estado, fluxos de chamadas, referências de protocolo
Configuração	Referência de configuração completa com exemplos
Painel de Controle	Guia da interface web com capturas de tela
Métricas	Métricas Prometheus, consultas e alertas
Requisitos de Rede	Portas de firewall e entradas DNS para implantação
Segurança	Limitação de taxa e bloqueio de países por GeoIP
Solução de Problemas	Problemas comuns e procedimentos de diagnóstico

Arquitetura e Fluxos de Chamadas do OmniEPDG

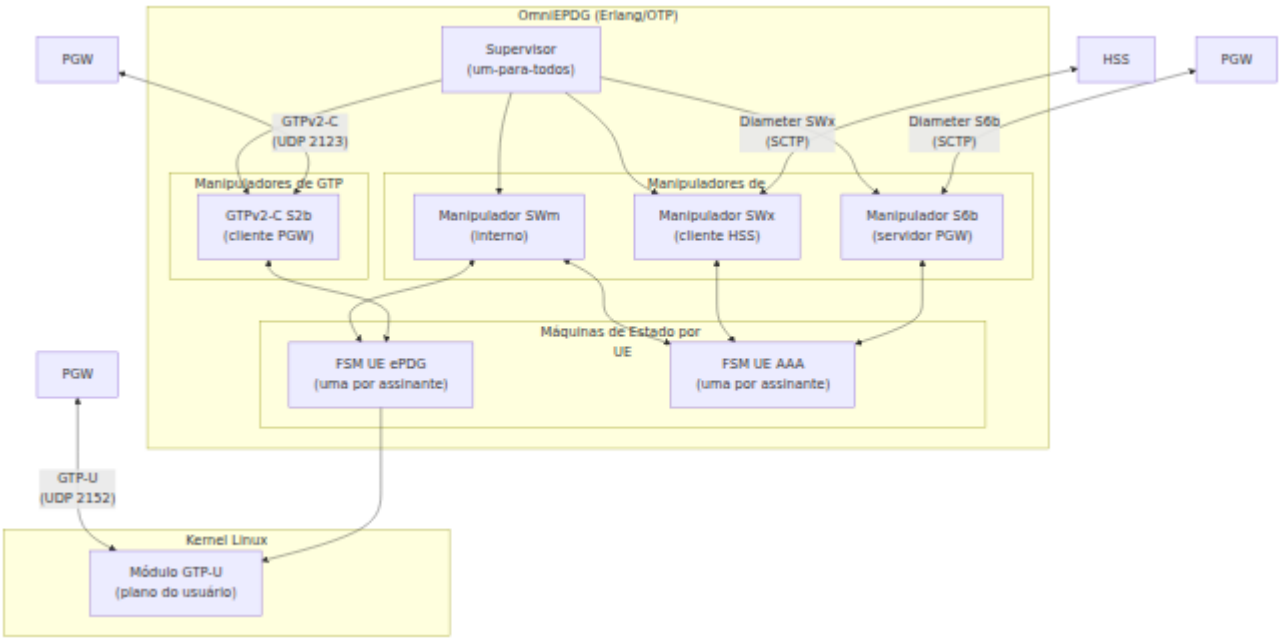
Este documento descreve a arquitetura interna do OmniEPDG, suas interfaces de protocolo, máquinas de estado do UE e diagramas de sequência de mensagens detalhados para procedimentos-chave. O OmniEPDG suporta dois modos operacionais: **Modo GTP** (túnel completo 3GPP via PGW) e **Modo VPN Simples** (quebra local com interface TUN). Consulte o Guia de Operações para uma comparação de alto nível.

Arquitetura do Sistema

O OmniEPDG é construído sobre Erlang/OTP e implementa a função de rede ePDG (evolved Packet Data Gateway) do 3GPP. Ele conecta o acesso WiFi não confiável à rede central móvel, permitindo que os UEs façam e recebam chamadas VoWiFi.

Arquitetura do Modo GTP

No modo GTP, o tráfego do assinante é encapsulado através de um PGW usando GTPv2-C para controle de sessão e o módulo GTP-U do kernel Linux para o plano do usuário.



Arquitetura do Modo VPN Simples

No modo VPN Simples, o tráfego do assinante é roteado localmente através de uma interface TUN do Linux. Nenhuma infraestrutura de PGW ou GTP é necessária. Os componentes Diameter S6b, GTPv2-C e GTP-U são substituídos pelo subsistema VPN Simples.

Árvore de Supervisores

O OmniEPDG utiliza uma estratégia de supervisor **um-para-todos**, o que significa que se qualquer processo filho falhar, todos os filhos são reiniciados. O supervisor inicia condicionalmente diferentes processos filhos dependendo do modo operacional.

Processos iniciados em ambos os modos:

Processo	Função	Descrição
`aaa_diameter_swx`	Cliente Diameter SWx	Conecta-se ao HSS para autenticação e operações de perfil de assinante
`aaa_diameter_swm`	Diameter SWm (Interno)	Roteia mensagens EAP Diameter e de sessão entre o ePDG e as FSMs AAA
`epdg_diameter_swm`	Manipulador SWm ePDG	Trata do lado ePDG da sinalização Diameter interna SWm

Processos adicionais no modo GTP:

Processo	Função	Descrição
`aaa_diameter_s6b`	Servidor Diameter S6b	Aceita conexões do PGW para autorização de sessão
`epdg_gtpc_s2b`	Cliente GTPv2-C	Envia solicitações de Criação/Exclusão de Sessão para o PGW via S2b
`gtp_u_kmod`	Manipulador Kernel GTP-U	Gerencia contextos PDP GTP-U no módulo do kernel Linux

Processos adicionais no modo VPN Simples:

Processo	Função	Descrição
`simple_vpn_supervisor`	Supervisor do Subsistema VPN	Supervisiona os processos do gerente de pool de IP e do gerente de rota
`simple_vpn_pool`	Gerente de Pool de IP	Aloca e libera endereços IPv4 do pool CIDR configurado usando ETS
`simple_vpn_route`	Gerente de Rota	Cria a interface TUN `omniepdg0` e gerencia rotas de host por assinante

Máquinas de Estado por UE

Para cada assinante ativo (identificado pelo IMSI), o OmniEPDG cria duas instâncias de máquinas de estado:

- **FSM UE ePDG** (`epdg_ue_fsm`) - Gerencia o ciclo de vida da sessão do assinante do ponto de vista do ePDG: autenticação, criação de túnel GTP e coordenação de encerramento
- **FSM UE AAA** (`aaa_ue_fsm`) - Gerencia a sinalização do lado AAA: trocas Diameter SWx com o HSS e trocas S6b com o PGW

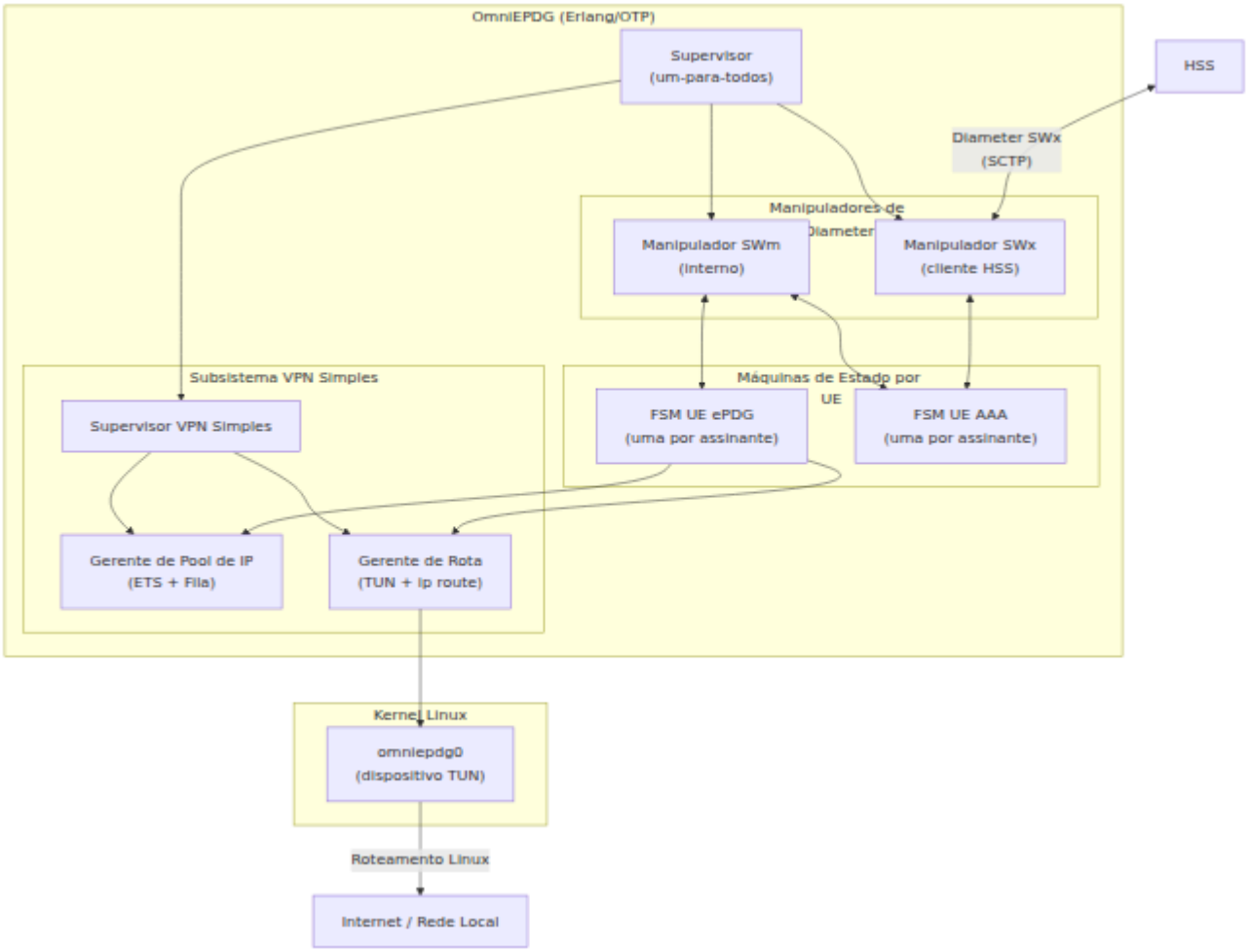
Ambas as FSMs são implementadas como processos `gen_statem` do Erlang com modo de callback de função de estado.

Estados da FSM UE ePDG

A FSM UE ePDG rastreia a sessão de um assinante desde a solicitação inicial de autenticação até o estado de túnel ativo e ao encerramento. O comportamento da FSM diverge no estado `authenticated` com base no modo operacional.

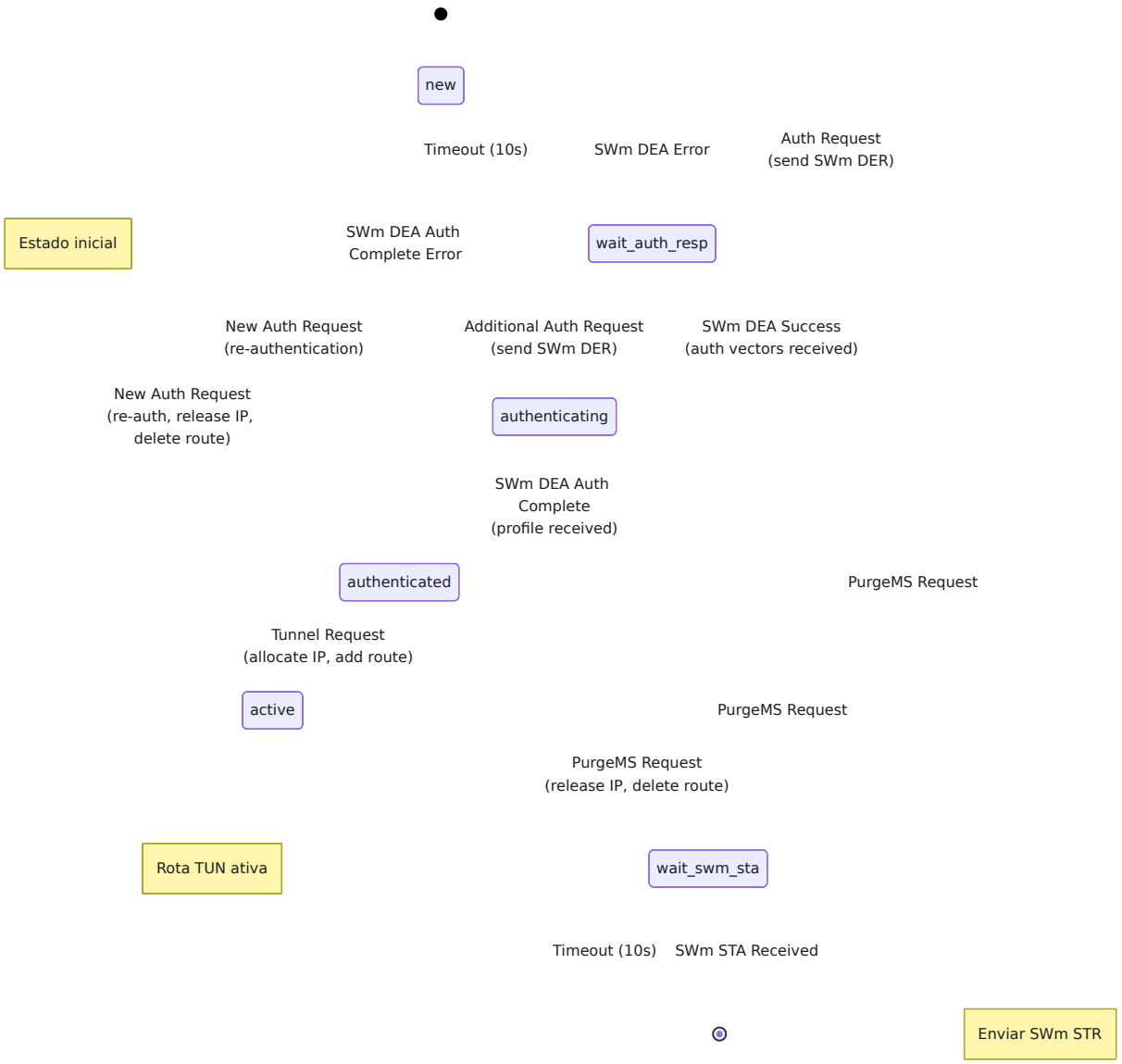
FSM do Modo GTP

No modo GTP, o estabelecimento do túnel passa pela Criação de Sessão GTPv2-C para o PGW, e o encerramento envolve a Exclusão de Sessão GTPv2-C, Exclusão de Bearer iniciada pelo PGW e fluxos de desregistro iniciados pelo HSS.



FSM do Modo VPN Simples

No modo VPN Simples, a FSM toma um atalho no estado `authenticated`. Em vez de enviar uma Solicitação de Criação de Sessão GTPv2-C, a FSM aloca um endereço IP do pool local, cria uma rota de host na interface TUN e transita diretamente para `active`. Os estados de encerramento específicos do GTP (`wait_create_session_resp`, `wait_delete_session_resp`, `dereg_pgw_wait_cancel`, `dereg_net_wait_s2b_delete`) não são utilizados.


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)
Rota TUN ativa
wait_swm_sta
Timeout (10s)
SWm STA Received
Enviar SWm STR

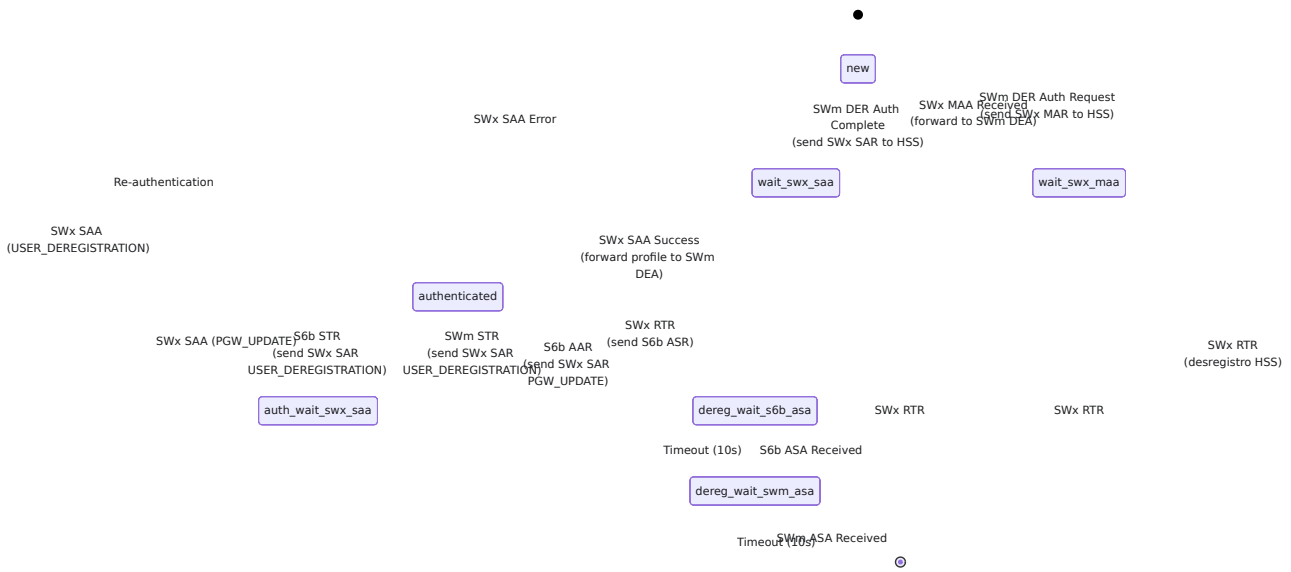
Referência de Estados da FSM UE ePDG

Estado	Modo	Descrição	Aguardando
`new`	Ambos	Estado inicial. Nenhuma sessão ativa.	Solicitação de autenticação do UE
`wait_auth_resp`	Ambos	Solicitação de autenticação enviada via SWm DER.	SWm DEA com vetores de autenticação ou erro
`authenticating`	Ambos	Vetores de autenticação recebidos, troca EAP em andamento.	Atualização de localização / conclusão de autenticação
`authenticated`	Ambos	Autenticação concluída, perfil do assinante baixado.	Solicitação de túnel do UE
`wait_create_session_resp`	GTP	Solicitação de Criação de Sessão GTPv2-C enviada ao PGW.	Resposta de Criação de Sessão do PGW
`active`	Ambos	Túnel/rota operacional. O tráfego do assinante está fluindo.	Gatilho de encerramento

Estado	Modo	Descrição	Aguardando
`wait_delete_session_resp`	GTP	Solicitação de Exclusão de Sessão GTPv2-C enviada ao PGW (encerramento iniciado pelo UE).	Resposta de Exclusão de Sessão do PGW
`wait_swm_sta`	Ambos	Solicitação de Término de Sessão SWm enviada.	SWm STA do AAA
`dereg_pgw_wait_cancel`	GTP	Desregistro iniciado pelo PGW. Localização de Cancelamento enviada ao UE.	Resultado de Cancelamento de Localização
`dereg_net_wait_cancel`	GTP	Desregistro iniciado pela rede/HSS. Localização de Cancelamento enviada ao UE.	Resultado de Cancelamento de Localização
`dereg_net_wait_s2b_delete`	GTP	Desregistro iniciado pela rede. S2b Delete Session enviada ao PGW.	Resposta de Exclusão de Sessão

Estados da FSM UE AAA

A FSM UE AAA gerencia a sinalização Diameter em direção ao HSS (SWx) e ao PGW (S6b) em nome de cada assinante.



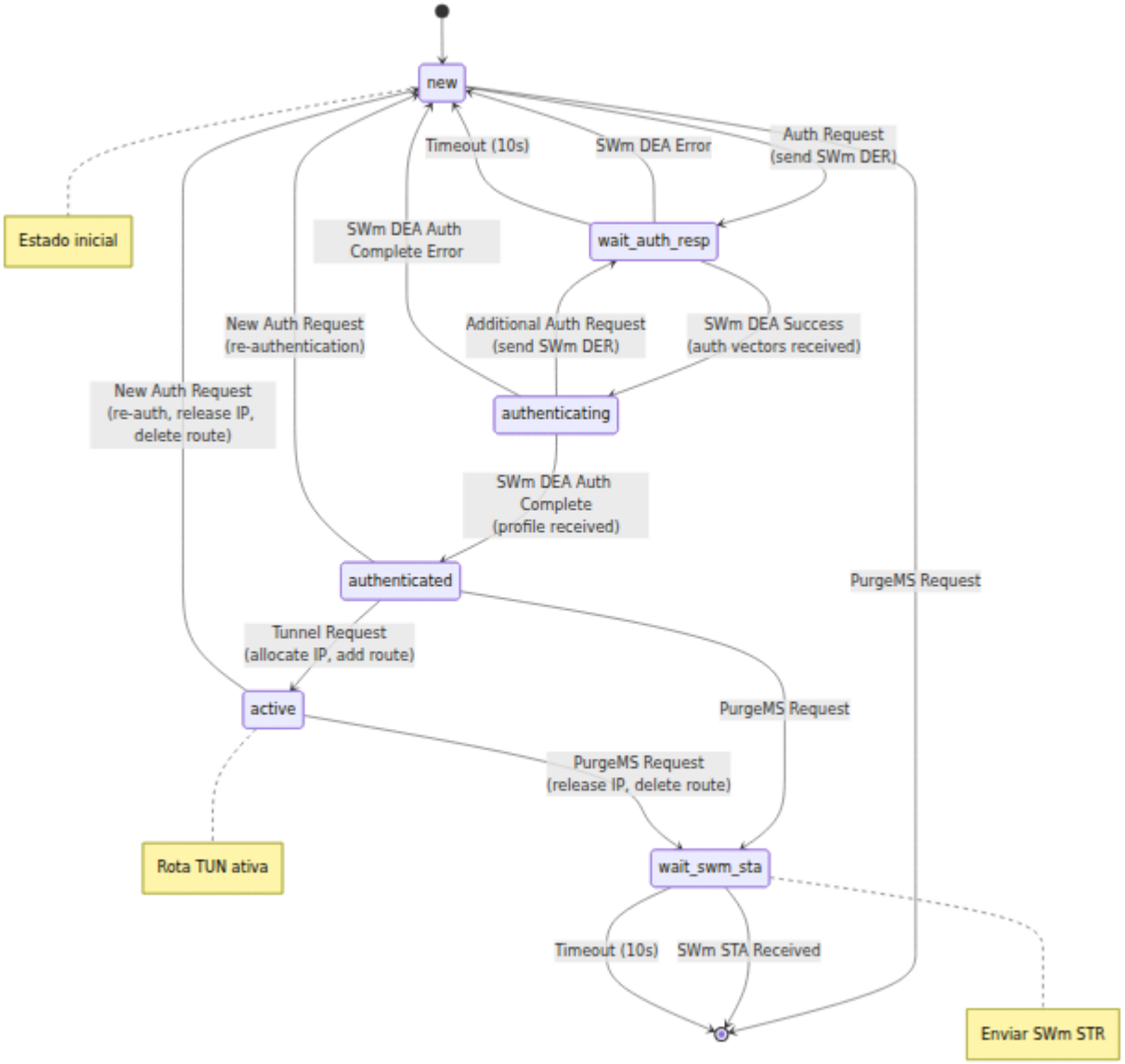
Referência de Estados da FSM UE AAA

Estado	Descrição	Aguardando
`new`	Estado inicial. Nenhuma sessão AAA ativa.	Solicitação de autenticação Diameter
`wait_swx_maa`	SWx MAR enviado ao HSS para vetores EAP-AKA.	SWx MAA do HSS
`wait_swx_saa`	SWx SAR enviado ao HSS para atribuição de servidor.	SWx SAA do HSS
`authenticated`	Ambas as sessões ePDG e PGW podem estar ativas. Rastreia o estado da sessão dupla.	Eventos de sessão
`auth_wait_swx_saa`	SWx SAR enviado para atualização do PGW ou desregistro do usuário.	SWx SAA do HSS
`dereg_net_wait_s6b_asa`	Desregistro iniciado pelo HSS. S6b ASR enviado ao PGW.	S6b ASA do PGW
`dereg_net_wait_swm_asa`	Encerramento do S6b completo. SWm ASR enviado ao ePDG.	SWm ASA do ePDG

Fluxos de Chamadas

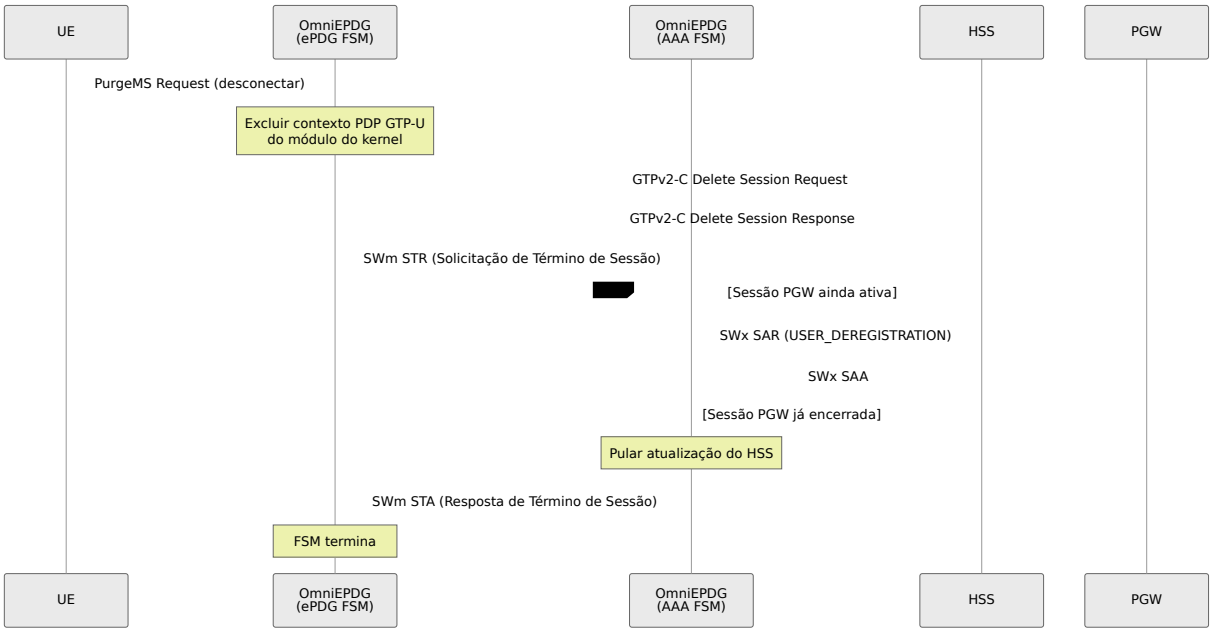
Modo GTP: Estabelecimento de Sessão Bem-Sucedido

Esta sequência mostra uma sessão completa e bem-sucedida desde a autenticação EAP-AKA até um túnel GTP ativo.



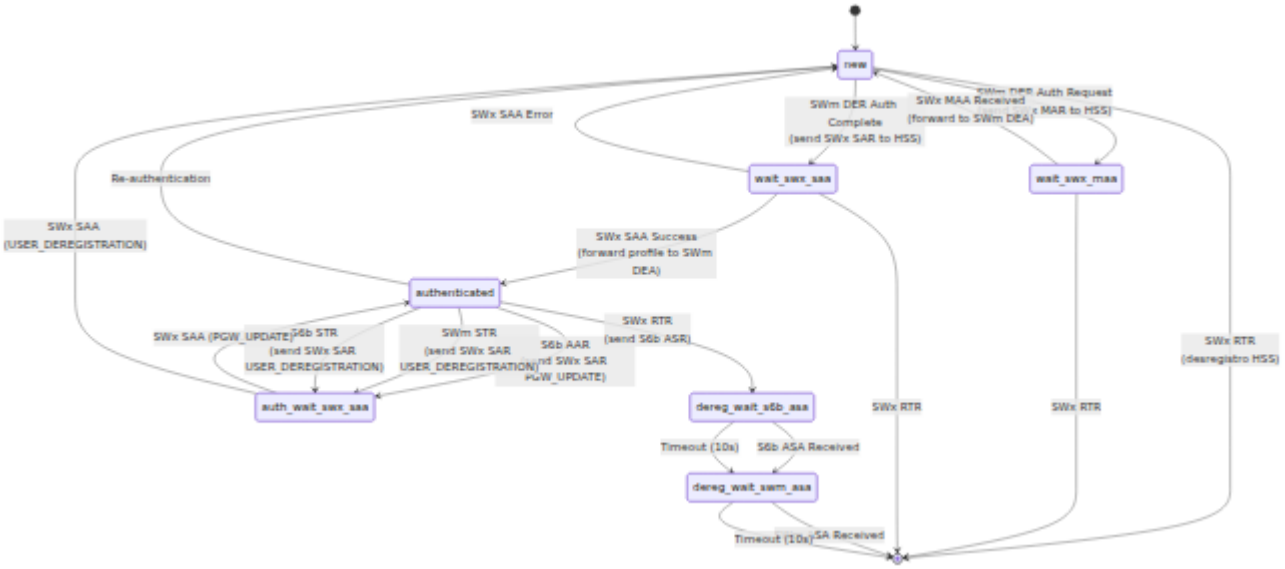
Modo GTP: Encerramento de Sessão Iniciado pelo UE

Quando o UE desconecta (por exemplo, muda de WiFi para celular ou o usuário desliga).



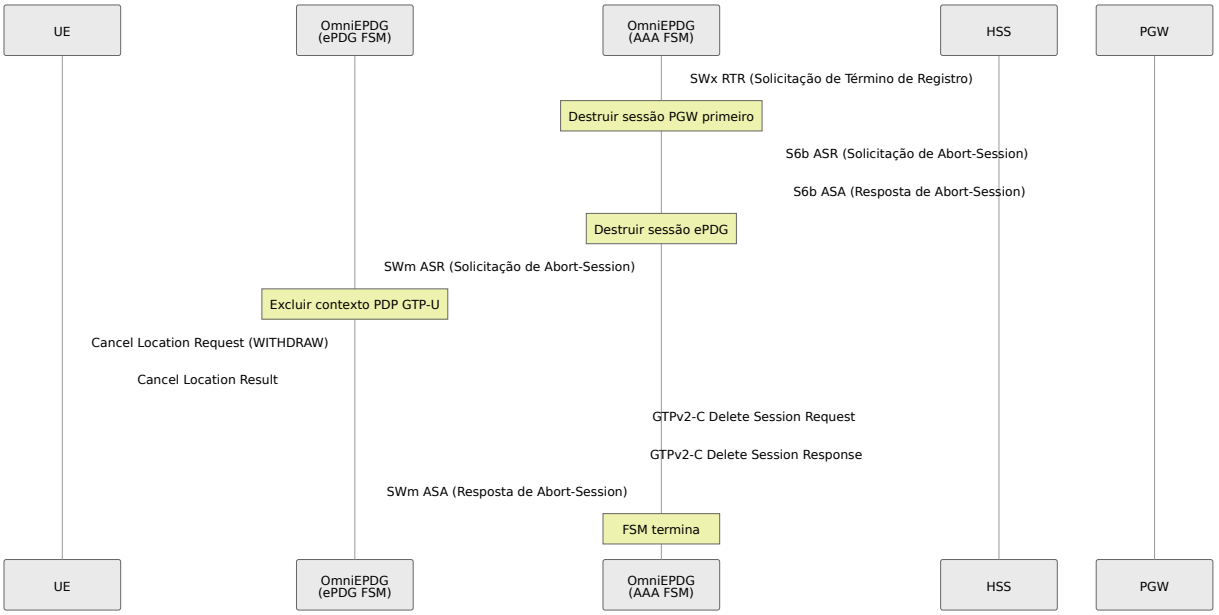
Modo GTP: Encerramento de Sessão Iniciado pelo PGW

Quando o PGW encerra a sessão (por exemplo, violação de política, timeout ou ação administrativa).



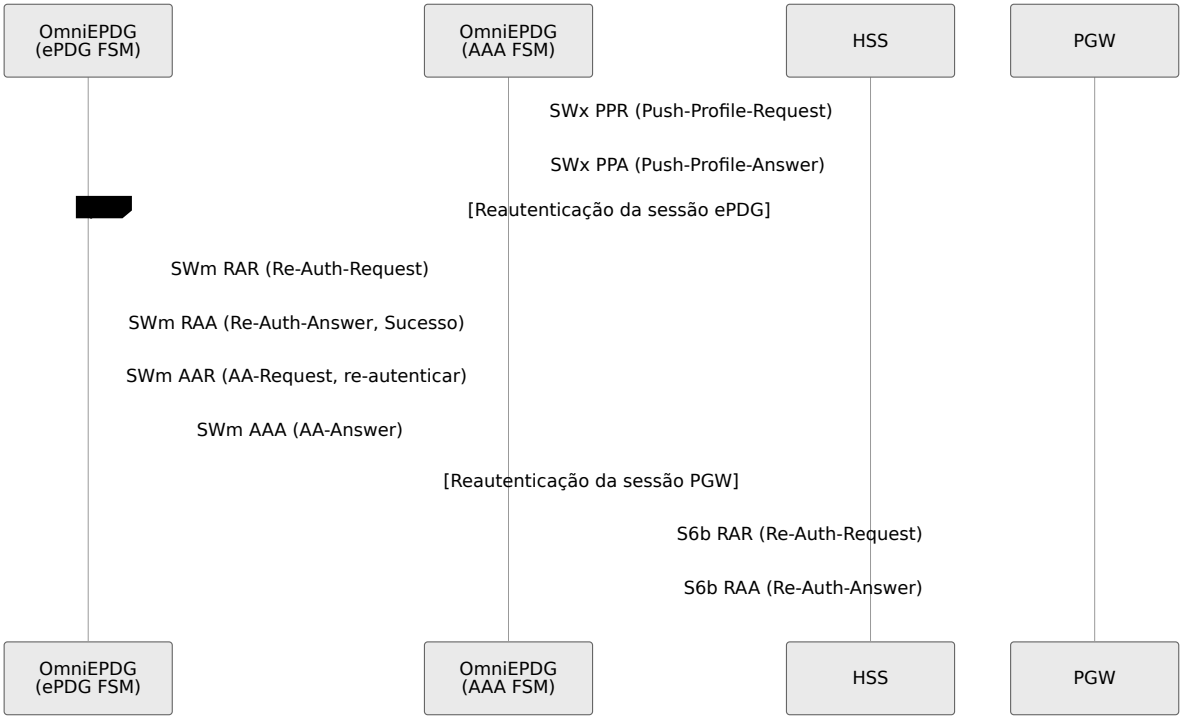
Modo GTP: Desregistro Iniciado pela Rede (HSS)

Quando o HSS revoga o registro de um assinante (por exemplo, mudança de assinatura, detecção de fraude ou ação administrativa).



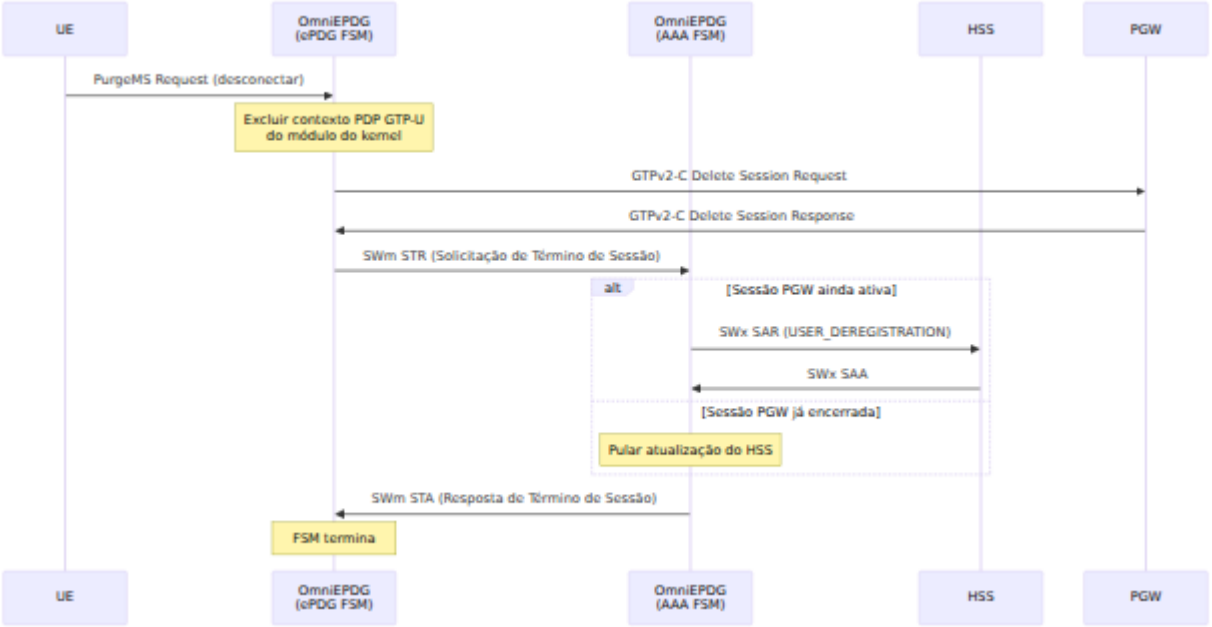
Modo GTP: Push de Perfil HSS e Reautenticação

Quando o HSS envia um perfil de assinante atualizado, o OmniEPDG aciona a reautenticação nas sessões ePDG (SWm) e PGW (S6b) conforme 3GPP TS 29.273 Seção 8.1.2.3.3.



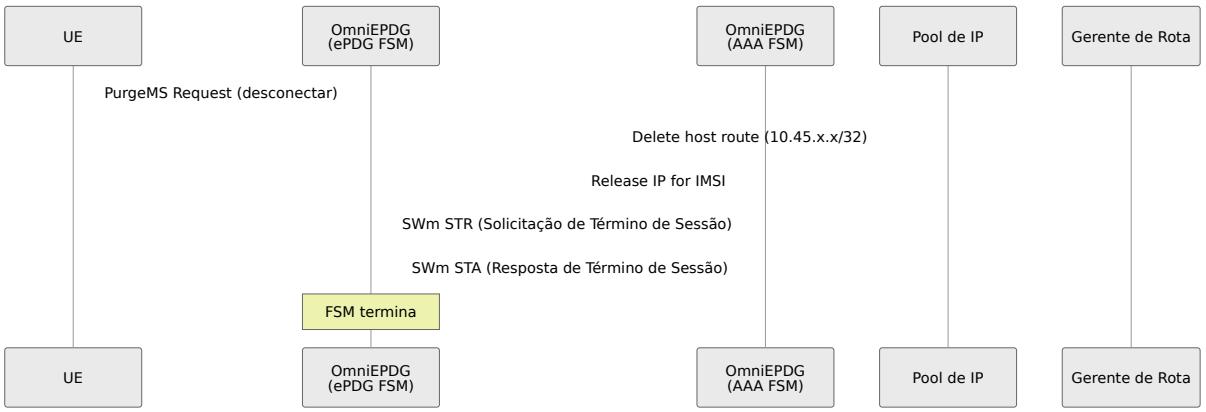
Modo VPN Simples: Estabelecimento de Sessão Bem-Sucedido

No modo VPN Simples, o estabelecimento da sessão é mais curto. Após a autenticação EAP-AKA, a FSM ePDG aloca um IP do pool local e configura uma rota de host na interface TUN, evitando toda interação com o PGW. Se `skip_sar` estiver habilitado, a troca SAR/SAA com o HSS também é pulada.



Modo VPN Simples: Encerramento de Sessão Iniciado pelo UE

Quando o UE desconecta no modo VPN Simples, a FSM libera o endereço IP alocado e remove a rota de host.



IDs de Aplicação Diameter

ID da Aplicação	Interface	ID do Fornecedor	Descrição	Referência
16777265	SWx	10415 (3GPP)	ePDG ↔ HSS autenticação e gerenciamento de assinantes	3GPP TS 29.273
16777272	S6b	10415 (3GPP)	AAA ↔ PGW autorização de sessão	3GPP TS 29.273

Códigos de Resultado Diameter

O OmniEPDG mapeia códigos de resultado Diameter para valores de causa internos para propagação de erros entre protocolos.

Códigos de Resultado Padrão

Código de Resultado	Nome	Significado
2001	DIAMETER_SUCCESS	Operação concluída com sucesso
2002	DIAMETER_LIMITED_SUCCESS	Operação parcialmente bem-sucedida

Códigos de Resultado Experimentais 3GPP

Código de Resultado	Nome	Significa
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	HSS temporaria não pode fornecer da de autenti
5001	DIAMETER_ERROR_USER_UNKNOWN	IMSI do assinante encontrad HSS
5002	DIAMETER_UNKNOWN_SESSION_ID	Sessão não encontrada (usada par STR/AAR obsoletos)
5003	DIAMETER_AUTHORIZATION_REJECTED	Assinante autorizado o serviço
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	Restrições roaming se aplicam
5005	DIAMETER_MISSING_AVP	AVP neces ausente na mensagem
5012	DIAMETER_UNABLE_TO_COMPLY	Falha gené de processam

Código de Resultado	Nome	Significa
5420	DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION	Nenhuma assinatura encontrada
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	Tecnologia acesso não permitida
5422	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	Dispositivo não reconh

Códigos de Causa GTPv2-C (Somente Modo GTP)

O OmniEPDG lida com os seguintes códigos de causa GTPv2-C nas respostas de Criação/Exclusão de Sessão do PGW. Os códigos de 1 a 15 são informativos, de 16 a 63 indicam sucesso e 64+ indicam erros. Consulte 3GPP TS 29.274 Seção 8.4.

Causas de Sucesso

Código	Nome	Descrição
16	Request Accepted	Operação concluída com sucesso
17	Request Accepted Partially	Sucesso parcial
18	New PDN Type (Network Preference)	Tipo de PDN alterado devido à preferência da rede
19	New PDN Type (Single Address Bearer)	Tipo de PDN alterado devido à restrição de bearer de endereço único

Causas de Erro (Selecionadas)

Código	Nome	Descrição
64	Context Not Found	Contexto de sessão não encontrado no PGW
73	No Resources Available	Exaustão de recursos do PGW
78	Missing or Unknown APN	APN solicitado não configurado no PGW
82	Denied in RAT	Tecnologia de acesso não permitida
84	All Dynamic Addresses Occupied	Pool de endereços IP exaurido no PGW
92	User Authentication Failed	Falha de autenticação no PGW
93	APN Access Denied	Assinante não autorizado para APN
96	IMSI/IMEI Not Known	Identidade do assinante não reconhecida
109	Invalid Peer	Validação do par falhou
113	APN Congestion	APN sobrecarregado
120	GTP-C Entity Congestion	Plano de controle do PGW sobrecarregado

Formato NAI

O OmniEPDG identifica assinantes usando o formato de Identificador de Acesso à Rede (NAI) definido na 3GPP TS 23.003 Seção 19:

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

Prefixo de Identidade e Tipo de Autenticação

O prefixo NAI determina o método de autenticação EAP conforme 3GPP TS 23.003:

Prefixo	Tipo de Autenticação	Descrição
`0`	EAP-AKA	Autenticação AKA padrão (mais comum para chamadas WiFi)
`6`	EAP-AKA'	Autenticação AKA aprimorada com vinculação à rede

O OmniEPDG seleciona automaticamente o método de autenticação com base no prefixo de identidade do UE. A maioria dos UEs usa o prefixo `0` (EAP-AKA) para chamadas WiFi.

O OmniEPDG extrai o IMSI do NAI analisando tudo entre o prefixo e o símbolo `@`. O IMSI é então usado como a chave primária para todas as máquinas de estado e operações de sinalização por assinante.

Algoritmos Criptográficos

O OmniEPDG implementa algoritmos criptográficos conforme 3GPP TS 33.402 e RFC 7296 (IKEv2).

Algoritmos de Criptografia IKEv2

Algoritmo	ID	Tamanho da Chave	Status	Referência
AES-CBC	12	128, 192, 256 bits	Suportado (padrão: 256)	RFC 3602
AES-GCM-16	20	128, 192, 256 bits	Suportado	RFC 5282
AES-GCM-12	19	128, 192, 256 bits	Suportado	RFC 5282
AES-GCM-8	18	128, 192, 256 bits	Suportado	RFC 5282
3DES	3	192 bits	Suportado (legado)	RFC 2451

Algoritmos de Integridade IKEv2

Algoritmo	ID	Tamanho da Chave	Tamanho do ICV	Status	Referência
HMAC-SHA2-256-128	12	256 bits	128 bits	Suportado (padrão)	RFC 4868
HMAC-SHA2-384-192	13	384 bits	192 bits	Suportado	RFC 4868
HMAC-SHA2-512-256	14	512 bits	256 bits	Suportado	RFC 4868
AES-XCBC-96	5	128 bits	96 bits	Suportado	RFC 3566
HMAC-SHA1-96	2	160 bits	96 bits	Suportado (legado)	RFC 2404
HMAC-MD5-96	1	128 bits	96 bits	Suportado (legado)	RFC 2403

AES-XCBC-96 (`AUTH_AES_XCBC_96`) é exigido por alguns dispositivos, notavelmente certos clientes Samsung VoWiFi, que o oferecem como seu único transformador de integridade. Ele é implementado conforme RFC 3566 com o manuseio de chave variável e truncamento de nonce SKEYSEED definidos em RFC 4434 e RFC 7296 Seção 2.14.

Algoritmos PRF IKEv2

Algoritmo	ID	Tamanho da Saída	Status	Referência
PRF-HMAC-SHA2-256	5	256 bits	Suportado (padrão)	RFC 4868
PRF-HMAC-SHA2-384	6	384 bits	Suportado	RFC 4868
PRF-HMAC-SHA2-512	7	512 bits	Suportado	RFC 4868
PRF-AES128-XCBC	4	128 bits	Suportado	RFC 4434
PRF-HMAC-SHA1	2	160 bits	Suportado (legado)	RFC 2104
PRF-HMAC-MD5	1	128 bits	Suportado (legado)	RFC 2104

Quando `PRF-AES128-XCBC` é negociado, SKEYSEED é derivado apenas dos primeiros 64 bits de cada um de Ni e Nr (conforme RFC 7296 Seção 2.14), enquanto os full nonces alimentam a expansão da chave prf+.

Grupos Diffie-Hellman IKEv2

Grupo	ID	Tamanho	Status	Referência
MODP-2048	14	2048 bits	Suportado (padrão)	RFC 3526
MODP-1024	2	1024 bits	Suportado (legado)	RFC 2409
MODP-1536	5	1536 bits	Suportado	RFC 3526
MODP-3072	15	3072 bits	Suportado	RFC 3526
MODP-4096	16	4096 bits	Suportado	RFC 3526
ECP-256	19	256 bits	Suportado	RFC 5903
ECP-384	20	384 bits	Suportado	RFC 5903
ECP-521	21	521 bits	Suportado	RFC 5903
Curve25519	31	256 bits	Suportado	RFC 8031
Curve448	32	448 bits	Suportado	RFC 8031

Algoritmos ESP (Child SA)

Os algoritmos do túnel ESP são negociados a partir da proposta de SA que o UE oferece em IKE_AUTH (e em CREATE_CHILD_SA na rekey). O OmniEPDG seleciona um transformador que o UE realmente ofereceu e deriva as chaves Child SA com os tamanhos de chave e ICV correspondentes. Não força um conjunto fixo.

Tipo	Algoritmos	Notas
Criptografia	AES-CBC-128 / 192 / 256	O cifrador segue o comprimento da chave negociada
Integridade	HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256, AES-XCBC-96, HMAC-SHA1-96	O ICV do AES-XCBC-96 é de 12 bytes (vs 16 para HMAC-SHA2-256-128)

Fallback (somente quando a proposta do UE não pode ser analisada):

- Criptografia: AES-CBC-256 (chave de 32 bytes, IV de 16 bytes)
- Integridade: HMAC-SHA2-256-128 (chave de 32 bytes, ICV de 16 bytes)

Funções Criptográficas EAP-AKA

Função	Algoritmo	Referência
Derivação de MK	SHA-1	RFC 4187 Seção 7
Expansão de chave PRF+	PRF FIPS 186-2 (SHA-1)	RFC 4187 Apêndice D
AT_MAC	HMAC-SHA1-128	RFC 4187 Seção 10.15
Milenage (f1-f5)	AES-128	3GPP TS 35.206

Funções Criptográficas EAP-AKA'

Função	Algoritmo	Referência
Derivação de CK'/IK'	HMAC-SHA-256	RFC 5448 Seção 3.3
Derivação de MK	SHA-256	RFC 5448 Seção 3.4
AT_MAC	HMAC-SHA256-128	RFC 5448 Seção 3.1

Conformidade com 3GPP

O OmniEPDG implementa todos os algoritmos criptográficos obrigatórios especificados na 3GPP TS 33.402 Seção 8:

Requisito	Algoritmo	Status
Criptografia IKEv2 (obrigatório)	AES-CBC-128	✓ Suportado
Integridade IKEv2 (obrigatório)	HMAC-SHA2-256-128	✓ Suportado (padrão)
PRF IKEv2 (obrigatório)	PRF-HMAC-SHA-256	✓ Suportado (padrão)
DH IKEv2 (obrigatório)	Grupo 14 (MODP-2048)	✓ Suportado (padrão)
Criptografia ESP (obrigatório)	AES-CBC-128/256	✓ Suportado
Integridade ESP (obrigatório)	HMAC-SHA2-256-128	✓ Suportado (padrão)
EAP-AKA	RFC 4187	✓ Implementado
EAP-AKA'	RFC 5448	✓ Implementado

Além do conjunto obrigatório, o OmniEPDG também suporta os transformadores de integridade e PRF AES-XCBC (RFC 3566 / RFC 4434) para interoperabilidade com dispositivos que os oferecem exclusivamente: por exemplo, certos clientes Samsung VoWiFi, que propõem AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048 e não voltarão para HMAC-SHA2.

Tipos de Endereço PDP (Somente Modo GTP)

O OmniEPDG suporta os seguintes tipos de endereço PDP conforme definido na 3GPP TS 29.274 Seção 8.14. No modo VPN Simples, apenas endereços IPv4 são

alocados do pool local.

Tipo	Descrição	Formato PAA GTPv2-C
IPv4	bearer somente IPv4	endereço IPv4 de 4 bytes
IPv6	bearer somente IPv6	comprimento do prefixo de 1 byte + endereço IPv6 de 16 bytes
IPv4v6	bearer de pilha dupla	comprimento do prefixo de 1 byte + IPv6 de 16 bytes + IPv4 de 4 bytes

Referência de Configuração do OmniEPDG

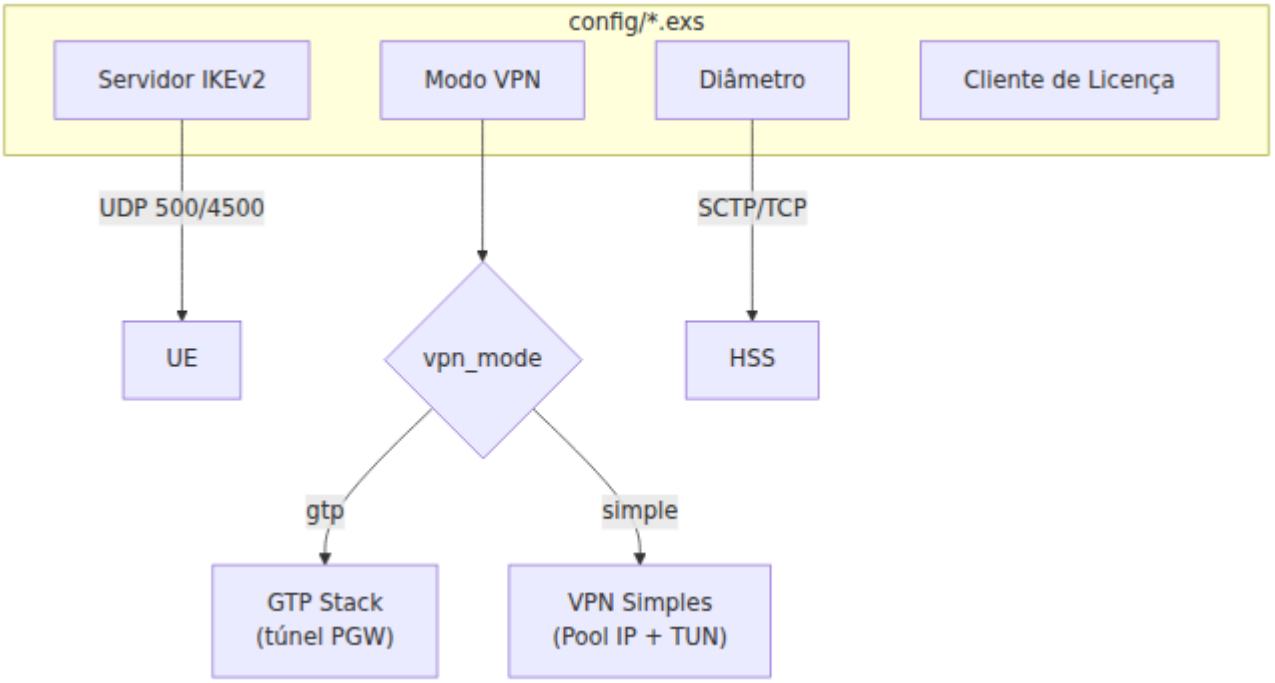
OmniEPDG é configurado via `config/runtime.exs` e variáveis de ambiente. Toda a configuração voltada para o cliente é realizada em tempo de execução - os padrões de tempo de compilação estão embutidos na versão e não são expostos.

Para implantações em contêineres, use variáveis de ambiente conforme documentado na seção Referência de Variáveis de Ambiente.

Índice

- Parâmetros do Servidor IKEv2
- Parâmetros de Segurança de Autenticação
- Seleção do Modo VPN
- Parâmetros de VPN Simples
- Parâmetros de Diâmetro
- Configuração do Cliente de Licença
- Configuração do Painel de Controle
- Configuração de Métricas do Prometheus
- Configuração de Webhooks
- Referência de Variáveis de Ambiente
- Referência de Timeout

Estrutura da Configuração



Arquivo de Configuração

Toda a configuração é feita em `config/runtime.exs`. O OmniEPDG lê este arquivo quando inicia. O arquivo suporta substituição de variáveis de ambiente para implantações em contêineres.

Exemplo de Configuração

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

  # Modo VPN: :simple (quebra local) ou :gtp (PGW via GTP-C)
  vpn_mode: :simple,

  # Configurações do modo VPN Simples
  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"]
  ]

# Configuração do painel de controle
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"}
  ]

# Configuração de Diâmetro (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}
    ]
  }

# Configuração do cliente de licença (runtime.exs)
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

Parâmetros do Servidor IKEv2

O servidor IKEv2 gerencia a interface SWu entre UEs e OmniEPDG. Ele termina túneis IPSec e realiza autenticação EAP-AKA.

Parâmetro	Tipo	Requerido	Padr
`listen_ip`	Tupla	Não	`{0, 0, 0, 0}`
`port_500`	Inteiro	Não	`500`
`port_4500`	Inteiro	Não	`4500`
`cert_file`	String	Sim	`/etc/omniepdg/c`

Parâmetro	Tipo	Requerido	Padr
`key_file`	String	Sim	`/etc/omniepdg/c`
`session_inactivity_timeout_ms`	Inteiro	Não	`300000`

Parâmetros de Segurança de Autenticação

OmniEPDG inclui proteção embutida contra ataques de força bruta e controle de acesso geográfico. Consulte o Guia de Segurança para documentação detalhada.

Parâmetros de Limitação de Taxa

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

  # Limitação de taxa por IMSI
  auth_rate_limit_per_imsi: 5,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 600_000
```

Parâmetro	Tipo	Requerido	Padrão	De
`auth_rate_limit_per_ip`	Inteiro	Não	`10`	Máxir tenta auter falha antes bloqu
`auth_rate_limit_ip_window_ms`	Inteiro	Não	`60000`	Janela desliz conta falhas (milis
`auth_rate_limit_ip_block_ms`	Inteiro	Não	`300000`	Duraç bloqu IPs qu exced limite minut
`auth_rate_limit_per_imsi`	Inteiro	Não	`5`	Máxir tenta auter falha IMSI a bloqu
`auth_rate_limit_imsi_window_ms`	Inteiro	Não	`60000`	Janela desliz conta falhas (milis
`auth_rate_limit_imsi_block_ms`	Inteiro	Não	`600000`	Duraç bloqu

Parâmetro	Tipo	Requerido	Padrão	De
				IMSIs exced limite minut

Parâmetros 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
```

Parâmetro	Tipo	Requerido	Padrão
`geoip_enabled`	Booleano	Não	`false`
`geoip_database_path`	String	Não	`"/etc/omniepdg/GeoLite2 Country.mmdb"`
`geoip_mode`	Átomo	Não	`:whitelist`
`geoip_countries`	Lista	Não	`[]`

Parâmetro	Tipo	Requerido	Padrão
`geoip_allow_unknown`	Booleano	Não	dependente do modo
`geoip_fail_open`	Booleano	Não	`true`

Seleção do Modo VPN

Parâmetro	Tipo	Requerido	Padrão	Var Env	Descriç
`vpn_mode`	Átomo	Não	`:simple`	`EPDG_VPN_MODE`	Modo operacion `:simple` para que de IP loca via interf TUN, `:gt` para tunelame através d um PGW GTPv2-C/GTP-U. Consulte Guia de Operaçõe para uma compara detalhad

Parâmetros de VPN Simples

O bloco de configuração `simple_vpn` controla a alocação de IP e DNS para o modo VPN Simples. O OmniEPDG suporta pools de endereços IPv4 e 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
  ]
```

Parâmetro	Tipo	Requerido	Padrão
`pool_ipv4`	String	Sim	`"10.45.0.0/16"`
`pool_ipv6`	String	Não	`"2001:db8::/32"`
`dns_servers_ipv4`	Lista	Não	`["8.8.8.8", "8.8.4.4"]`
`dns_servers_ipv6`	Lista	Não	`["2001:4860:4860::8888", "2001:4860:4860::8844"]`
`p_cscf_ipv4`	Lista	Não	`[]`

Parâmetro	Tipo	Requerido	Padrão
`p_cscf_ipv6`	Lista	Não	`[]`
`mtu`	Inteiro	Não	`1400`
`nat_enabled`	Booleano	Não	`true`

Parâmetros de Diâmetro

A configuração de Diâmetro controla as interfaces SWx (HSS) e S6b (PGW). Quando `diameter_enabled` é `true`, o OmniEPDG inicia a pilha de Diâmetro e se conecta aos 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}
    ]
  }
```

Parâmetros de Serviço

Parâmetro	Tipo	Requerido	Padrão
`service_name`	Átomo	Não	`:omniepdg`
`listen_ip`	String	Não	`"0.0.0.0"`
`listen_port`	Inteiro	Não	`3868`
`host`	String	Sim	`"epdg"`
`realm`	String	Sim	`"epc.mnc001.mcc001.3gppnetwork.o`

Parâmetro	Tipo	Requerido	Padrão
`product_name`	String	Não	`"OmniEPDG"`
`vendor_id`	Inteiro	Não	`10415`

Parâmetros de Par

Cada entrada na lista `peers` define uma conexão de par de Diâmetro (tipicamente para o HSS).

Parâmetro	Tipo	Requerido	Padrão	Var Env	Descrição
`host`	String	Sim	-	`HSS_HOST`	Identidade de Diâmetro do par (Origin-Host). Deve corresponder à identidade configurada do par.
`ip`	String	Sim	-	`HSS_IP`	Endereço IP do par para conexão TCP/SCTP.
`port`	Inteiro	Não	`3868`	`HSS_PORT`	Porta de Diâmetro do par.
`transport`	Átomo	Não	`:tcp`	-	Protocolo de transporte: `:tcp` ou `:sctp`.

IDs de Aplicação

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

Configuração do Cliente de Licença

O cliente de licença valida o OmniEPDG contra um servidor de licença.

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

Parâmetro	Tipo	Requerido	Padrão	Var Env	
`server_url`	String	Sim	-	`LICENSE_SERVER_URL`	
`product`	String	Não	`"omniepdg"`	-	

Configuração do Painel de Controle

O painel de controle web fornece capacidades de monitoramento e gerenciamento.

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

Parâmetro	Tipo	Requerido	Padrão	Var Env	Des
`port`	Inteiro	Não	`4000`	`CONTROL_PANEL_PORT`	Port para inter web pain cont

Configuração de Métricas do Prometheus

OmniEPDG expõe métricas do Prometheus via HTTP para monitoramento e alerta.

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

Parâmetro	Tipo	Requerido	Padrão	Var Env	Descri
`port`	Inteiro	Não	`9568`	`PROMETHEUS_PORT`	Porta H para o endpoir de métr do Prometh (`/metri`

Métricas Expostas

Métricas de Contador (Baseadas em Eventos):

- `epdg_ikev2_session_initiated_count` - Trocas IKE_SA_INIT iniciadas
- `epdg_ikev2_session_established_count` - SAs IKE estabelecidas com sucesso
- `epdg_ikev2_session_failed_count` - Falhas na criação de SA IKE (por motivo)
- `epdg_eap_identity_count` - Solicitações de identidade EAP
- `epdg_eap_aka_challenge_count` - Desafios EAP-AKA enviados
- `epdg_eap_aka_success_count` - Autenticações EAP-AKA bem-sucedidas
- `epdg_eap_aka_failure_count` - Autenticações EAP-AKA falhadas (por motivo)
- `epdg_eap_aka_sync_failure_count` - Falhas de sincronização SQN EAP-AKA

- `epdg_diameter_swx_mar_count` - Solicitações de Autenticação Multimídia (por resultado)
- `epdg_diameter_swx_sar_count` - Solicitações de Atribuição de Servidor (por resultado)
- `epdg_diameter_s6b_aar_count` - Solicitações AA tratadas (por resultado)
- `epdg_diameter_s6b_str_count` - Solicitações de Término de Sessão
- `epdg_session_created_count` - Sessões criadas (por vpn_mode)
- `epdg_session_terminated_count` - Sessões encerradas (por motivo)
- `epdg_esp_packets_in_count` - Pacotes ESP descriptografados
- `epdg_esp_packets_out_count` - Pacotes ESP criptografados
- `epdg_ip_allocated_count` - Endereços IP alocados (por tipo)
- `epdg_ip_released_count` - Endereços IP liberados (por tipo)

Métricas de Gauge (Consultadas a cada 5s):

- `epdg_sessions_active_count` - Total de sessões ativas
- `epdg_sessions_by_state_count` - Sessões por estado da FSM
- `epdg_ip_pool_allocated_count` - IPs atualmente alocados
- `epdg_ip_pool_available_count` - IPs disponíveis no pool
- `epdg_ip_pool_utilization_ratio` - Utilização do pool (0.0-1.0)
- `epdg_diameter_swx_pending_count` - Solicitações SWx pendentes
- `epdg_diameter_s6b_active_sessions_count` - Sessões S6b ativas

Métricas de Histograma (Rastreamento de Latência):

- `epdg_auth_duration_ms` - Duração total do fluxo de autenticação
- `epdg_diameter_swx_mar_latency_ms` - Tempo de resposta do MAR
- `epdg_diameter_swx_sar_latency_ms` - Tempo de resposta do SAR
- `epdg_session_duration_seconds` - Tempo de vida da sessão

Métricas de VM:

- `vm_memory_total` - Memória total da VM
- `vm_memory_processes` - Memória do processo
- `vm_memory_binary` - Memória binária
- `vm_memory_ets` - Memória da tabela ETS

- `vm_system_info_process_count` - Processos em execução
- `vm_system_info_port_count` - Portas abertas
- `vm_statistics_run_queue` - Fila de execução do escalonador

Configuração de Coleta do Prometheus

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

Configuração de Webhooks

OmniEPDG pode enviar webhooks de saída para eventos do ciclo de vida da sessão do assinante. Quando habilitado, o OmniEPDG envia um `POST` HTTP com um corpo JSON para cada endpoint configurado em um anexo bem-sucedido e em um desanexo. Consulte Webhooks para o modelo de entrega, o esquema de carga útil e exemplos de cargas úteis.

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

Parâmetro	Tipo	Requerido	Padrão
`enabled`	Booleano	Não	`false`
`endpoints`	Lista	Não	`["https://127.0.0.1/webhook"]`
`events`	Lista	Não	`[:session_established, :session_terminated]`

OmniEPDG entrega webhooks com um modelo de fire-and-forget, e não tenta uma entrega falhada. Para o modelo de entrega completo e o esquema de carga útil JSON, consulte Webhooks.

Referência de Timeout

Todos os timeouts internos da FSM são codificados. Estes governam quanto tempo as máquinas de estado esperam por respostas antes de considerá-las falhadas.

Timeout	Valor	Modo	Contexto	Descrição
Resposta GTP	10.000 ms	GTP	FSM UE ePDG	Tempo máximo de espera pela Resposta de Criação/Exclusão de Sessão GTPv2-C do PGW.
Resposta SWm	10.000 ms	Ambos	FSM UE ePDG	Tempo máximo de espera pela resposta interna de Diâmetro SWm (DER/DEA, STR/STA).
Resposta S6b	10.000 ms	GTP	FSM UE AAA	Tempo máximo de espera pela resposta de Diâmetro S6b (ASR/ASA).

Referência de Variáveis de Ambiente

As variáveis de ambiente são lidas em `config/runtime.exs` e substituem os padrões de tempo de compilação.

Servidor IKEv2

Variável	Padrão	Descrição
`EPDG_LISTEN_IP`	`"0.0.0.0"`	Endereço de vinculação do servidor IKEv2 (formato decimal pontuado, por exemplo, `"10.0.0.1"`).
`EPDG_PORT_500`	`"500"`	Porta do protocolo IKE.
`EPDG_PORT_4500`	`"4500"`	Porta do IKE NAT-Traversal.
`EPDG_CERT_FILE`	`"/etc/omniepdg/certs/epdg.crt"`	Caminho para o certificado do servidor IKEv2 (PEM).
`EPDG_KEY_FILE`	`"/etc/omniepdg/certs/epdg.key"`	Caminho para a chave privada do servidor IKEv2 (PEM).
`EPDG_SESSION_TIMEOUT`	`"300000"`	Timeout de inatividade da sessão em milissegundos

Modo VPN

Variável	Padrão	Descrição
`EPDG_VPN_MODE`	`"simple"`	Modo VPN: `"simple"` ou `"gtp"`.

Diâmetro

Variável	Padrão	Descrição
`DIA_LISTEN_IP`	`"0.0.0.0"`	Endereço de vinculação do ouvinte de Diâmetro.
`DIA_LISTEN_PORT`	`"3868"`	Porta do ouvinte de Diâmetro.
`DIA_HOST`	`"epdg"`	Origin-Host de Diâmetro (sem realm).
`DIA_REALM`	`"epc.mnc001.mcc001.3gppnetwork.org"`	Origin-Realm de Diâmetro.

Par HSS

Variável	Padrão	Descrição
`HSS_HOST`	`"hss"`	Identidade de Diâmetro do HSS (Origin-Host).
`HSS_IP`	`"127.0.0.1"`	Endereço IP do HSS.
`HSS_PORT`	`"3868"`	Porta de Diâmetro do HSS.

Licença, Painel de Controle e Métricas

Variável	Padrão	Descrição
`LICENSE_SERVER_URL`	-	URL da API do servidor de licença (obrigatório).
`CONTROL_PANEL_PORT`	`"4000"`	Porta HTTP do painel de controle.
`PROMETHEUS_PORT`	`"9568"`	Porta HTTP das métricas do Prometheus (endpoint `/metrics`).

Exemplo: 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"

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

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

      # Painel de controle
      CONTROL_PANEL_PORT: "4000"

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

Painel de Controle OmniEPDG

O OmniEPDG inclui um painel de controle baseado na web para monitoramento em tempo real de sessões, pares Diameter e logs do sistema. O painel de controle fornece visualizações que se atualizam ao vivo sem atualizações de página.

Índice

- Acessando o Painel de Controle
- Painel
- Visualização de Sessões
- Visualização de Pares Diameter
- Visualização de Logs
- Visualização de Documentos
- Visualização de Recursos
- Visualização de Configuração

Acessando o Painel de Controle

O painel de controle é servido na porta HTTP configurada (padrão 4000):

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

Navegação

O painel de controle fornece uma barra lateral com links para todas as visualizações:

Caminho	Visualização	Descrição
`/dashboard`	Painel	Visão geral do sistema e links rápidos
`/sessions`	Sessões	Lista de sessões UE ativas
`/diameter`	Pares Diameter	Status da conexão de pares Diameter
`/logs`	Logs	Streaming de logs em tempo real
`/docs`	Documentos	Navegador de documentação integrada
`/resources`	Recursos	Informações sobre BEAM VM e aplicações
`/configuration`	Configuração	Visualizador de configuração do sistema

Painel

O Painel fornece uma visão geral de alto nível do status do OmniEPDG com métricas chave e navegação rápida.

Cartões de Estatísticas

O painel exibe quatro estatísticas principais:

Estatística	Descrição
Sessões Ativas	Número atual de sessões UE estabelecidas
Dados Recebidos (UL)	Total de bytes recebidos dos UEs (direção uplink)
Dados Enviados (DL)	Total de bytes enviados para os UEs (direção downlink)
Pares Diameter	Pares conectados / total de pares configurados

Os valores de dados são automaticamente escalonados para as unidades apropriadas (B, KB, MB, GB).

Links Rápidos

Navegação direta para visualizações detalhadas:

- **Ver Sessões** - Navegar para a visualização de Sessões para informações detalhadas sobre UE
- **Pares Diameter** - Navegar para a visualização de Pares Diameter para status de conectividade
- **Logs do Sistema** - Navegar para a visualização de Logs para streaming de logs em tempo real
- **Configuração** - Navegar para a visualização de Configuração para configurações do sistema

Informações do Sistema

Exibe a configuração operacional atual:

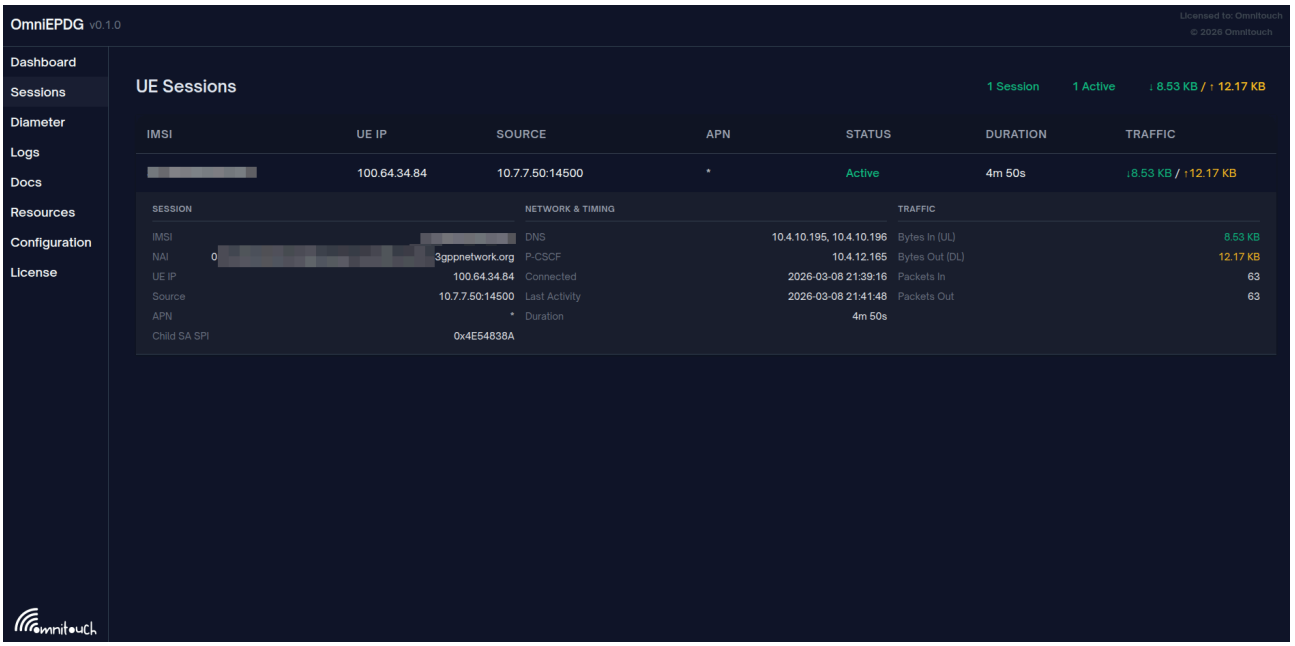
Campo	Descrição
Modo VPN	Modo atual: `GTP` ou `SIMPLE`
Portas IKEv2	Portas padrão: 500 (IKE), 4500 (NAT-T)
Status Diameter	Se o sinalizador Diameter está habilitado
Pool de IP (IPv4)	CIDR do pool de IP configurado (apenas modo VPN Simples)

Atualização Automática

O painel se atualiza automaticamente a cada segundo para exibir estatísticas atuais.

Visualização de Sessões

A visualização de Sessões exibe todas as sessões UE ativas com informações detalhadas para cada assinante.



A visualização de Sessões mostra conexões UE ativas com estatísticas de tráfego em tempo real e duração da sessão.

Lista de Sessões

Cada linha de sessão exibe:

Coluna	Descrição
IMSI	Identidade Internacional do Assinante Móvel do assinante
UE IP	Endereço IPv4/IPv6 atribuído
FONTE	IP externo e porta do UE (endereço NAT)
APN	Nome do Ponto de Acesso para a conexão
STATUS	Estado atual da sessão (Ativa/Inativa)
DURAÇÃO	Tempo desde a estabelecimento da sessão
TRÁFEGO	Bytes recebidos / enviados (UL/DL)

Indicadores de Status

As sessões exibem status com badges codificados por cores:

Status	Cor	Descrição
Ativa	Verde	Sessão totalmente estabelecida e operacional
Conectando	Amarelo	Estabelecimento da sessão em progresso
Inativa	Vermelho	Sessão terminada ou falhou

Detalhes da Sessão

Clique em qualquer linha de sessão para expandir informações detalhadas:

Visualização expandida da sessão mostrando IMSI, NAI, configuração de rede e estatísticas de tráfego.

Seção da Sessão

Campo	Descrição
IMSI	Valor completo do IMSI
NAI	Identificador de Acesso à Rede (formato 3GPP)
UE IP	Endereço IPv4/IPv6 atribuído
Fonte	IP externo e porta do UE (endereço NAT)
APN	Nome do Ponto de Acesso para a conexão PDN
Child SA SPI	Índice de Parâmetro de Segurança do Child SA IPSec

Seção de Rede e Tempo

Campo	Descrição
DNS	Servidores DNS fornecidos ao UE
P-CSCF	Servidores Proxy-CSCF para sinalização IMS
Conectado	Timestamp quando a sessão foi estabelecida
Última Atividade	Timestamp da atividade de pacote mais recente
Duração	Tempo desde a estabelecimento da sessão

Seção de Tráfego

Campo	Descrição
Bytes In (UL)	Total de bytes recebidos do UE (uplink)
Bytes Out (DL)	Total de bytes enviados para o UE (downlink)
Pacotes In	Total de pacotes recebidos do UE
Pacotes Out	Total de pacotes enviados para o UE

Estado Vazio

Quando não há sessões ativas, a visualização exibe:

- Mensagem "Nenhuma sessão ativa"
- Indica se as conexões UE devem ser tentadas

Atualização Automática

A lista de sessões se atualiza automaticamente a cada segundo.

Visualização de Pares Diameter

A visualização de Pares Diameter exibe o status de todos os pares Diameter configurados (HSS para SWx, PGW para S6b).

Lista de Pares

Cada linha de par exibe:

Coluna	Descrição
Par	Identidade Diameter (Origin-Host)
Realm	Realm Diameter (Origin-Realm)
Endereço IP	Endereço de transporte no formato `protocolo://ip:porta`
Status	Status da conexão

Indicadores de Status

Status	Cor	Descrição
Conectado	Verde	Conexão de par Diameter estabelecida
Desconectado	Vermelho	Par não conectado
Desconhecido	Cinza	Status não pode ser determinado

Resumo da Contagem de Pares

O cabeçalho exibe contagens agregadas:

- **X Conectados** - Número de pares com conexões ativas
- **Y Desconectados** - Número de pares sem conexões

Detalhes do Par

Clique em qualquer linha de par para expandir informações detalhadas:

Campo	Descrição
Iniciação da Conexão	Quem inicia: `local` (nós conectamos ao par) ou `remoto` (par se conecta a nós)
Transporte	Protocolo: `tcp` ou `sctp`
Nome do Produto	Nome do produto anunciado do par a partir de CER/CEA
Aplicações Anunciadas	IDs de Aplicação Diameter suportados pelo par

Estado Vazio

Quando nenhum par está configurado, a visualização exibe:

- "Nenhum Par Diameter configurado" se Diameter estiver habilitado
- "Diameter está desabilitado" com dica de configuração se desabilitado

Atualização Automática

A lista de pares se atualiza automaticamente a cada segundo.

Visualização de Logs

A visualização de Logs fornece streaming em tempo real de logs do sistema com capacidades de filtragem e pesquisa.

Exibição de Logs

Os logs aparecem em um contêiner rolável com as entradas mais novas na parte inferior. Cada entrada de log exibe:

Elemento	Descrição
Timestamp	Quando a entrada de log foi gerada
Nível	Nível de severidade com codificação de cores
Mensagem	Conteúdo da mensagem de log

Níveis de Log

Os logs são codificados por cores de acordo com a severidade:

Nível	Cor	Descrição
debug	Cinza	Informações diagnósticas detalhadas
info	Azul	Mensagens informativas gerais
warning	Amarelo	Condições de aviso
error	Vermelho	Condições de erro

Filtragem por Nível

Filtrar logs por nível de severidade mínima usando o dropdown:

Filtro	Mostra
Todos os Níveis	debug, info, warning, error
Info+	info, warning, error
Warning+	warning, error
Apenas Erro	error

Pesquisa

A caixa de pesquisa filtra logs em tempo real:

- Digite qualquer texto para filtrar mensagens de log
- A correspondência não diferencia maiúsculas de minúsculas
- Limpa quando a caixa de pesquisa é esvaziada

Controles

Controle	Descrição
Pausar/Retomar	Alternar streaming de logs on/off
Limpar	Remover todos os logs exibidos
Rolagem Automática	Alternar rolagem automática para as entradas mais novas

Buffer de Logs

- Máximo de 1000 entradas de log são retidas
- Entradas mais antigas são removidas quando o limite é alcançado
- Limpar logs remove todas as entradas da exibição

Estado Vazio

Quando nenhum log corresponde aos filtros atuais:

- Mensagem "Nenhum log para exibir"
- Verifique as configurações de filtro se logs forem esperados

Atualização Automática

Novos logs aparecem automaticamente à medida que são gerados (quando não estão pausados).

Visualização de Documentos

A visualização de Documentos fornece um navegador de documentação integrada, permitindo que os operadores acessem toda a documentação do OmniEPDG diretamente do painel de controle.

Seleção de Documentos

Selecione entre os arquivos de documentação disponíveis usando a barra de botões:

Documento	Descrição
OPERATIONS.md	Guia de operações com início rápido e procedimentos
README.md	Visão geral do projeto e instruções de configuração
architecture.md	Arquitetura do sistema e fluxos de chamadas
configuration.md	Referência completa de configuração
control-panel.md	Este guia do painel de controle
metrics.md	Referência de métricas do Prometheus
troubleshooting.md	Problemas comuns e etapas de resolução

Renderização de Markdown

A documentação é renderizada com suporte completo a Markdown, incluindo:

- Cabeçalhos e formatação de texto
- Blocos de código com destaque de sintaxe
- Tabelas
- Links (internos e externos)
- Listas e citações

Visualização de Recursos

A visualização de Recursos exibe estatísticas da BEAM VM e aplicações OTP em execução.

Métricas do Sistema

Métrica	Descrição
Uso de Memória	Total de memória usada pela BEAM VM
Processos BEAM	Número de processos Erlang/Elixir em execução
Tempo de Atividade	Tempo desde que a aplicação foi iniciada

Aplicações em Execução

Lista todas as aplicações OTP carregadas agrupadas por categoria:

Categoria	Descrição
Principal	A aplicação OmniEPDG
Sistema	Aplicações principais Erlang/OTP e Elixir

Clique em uma aplicação para ver seus detalhes, incluindo versão, descrição e dependências.

Visualização de Configuração

A visualização de Configuração exibe a configuração em tempo de execução e as aplicações carregadas.

Informações do Ambiente

Campo	Descrição
Ambiente	Ambiente Mix atual (Desenvolvimento/Produção)
Versão do Elixir	Versão do Elixir em execução

Lista de Aplicações

Exibe todas as aplicações OTP carregadas com suas versões. Selecione uma aplicação para ver:

- Descrição da aplicação
- Informações da versão
- Dependências
- Parâmetros de configuração

Configuração do Painel de Controle

Porta HTTP

Configure a porta do painel de controle em `config/runtime.exs`:

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

Parâmetro	Tipo	Padrão	Descrição
`port`	Inteiro	4000	Porta HTTP para o painel de controle

Desabilitando o Painel de Controle

O painel de controle pode ser desabilitado não iniciando o endpoint web em produção, se não for necessário. Entre em contato com seu integrador de sistema para configuração específica de implantação.

Referência de Métricas do OmniEPDG

OmniEPDG expõe métricas do Prometheus para monitorar fluxos de autenticação, ciclo de vida de sessão, sinalização Diameter e saúde do sistema. As métricas são servidas via HTTP para raspagem pelo Prometheus.

Índice

- Endpoint de Métricas
- Configuração
- Categorias de Métricas
  - Métricas de Sessão IKEv2
  - Métricas de Autenticação EAP
  - Métricas de Segurança de Autenticação
  - Métricas Diameter SWx
  - Métricas Diameter S6b
  - Métricas de Ciclo de Vida de Sessão
  - Métricas de Plano de Dados ESP
  - Métricas de Pool de IP
  - Métricas de VM
- Integração com Prometheus
- Consultas de Exemplo
- Regras de Alerta

Endpoint de Métricas

OmniEPDG expõe métricas em:

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

O endpoint retorna métricas no formato de exposição do Prometheus, compatível com Prometheus, Grafana e outras ferramentas de monitoramento.

Configuração

Configure o endpoint de métricas em `config/runtime.exs`:

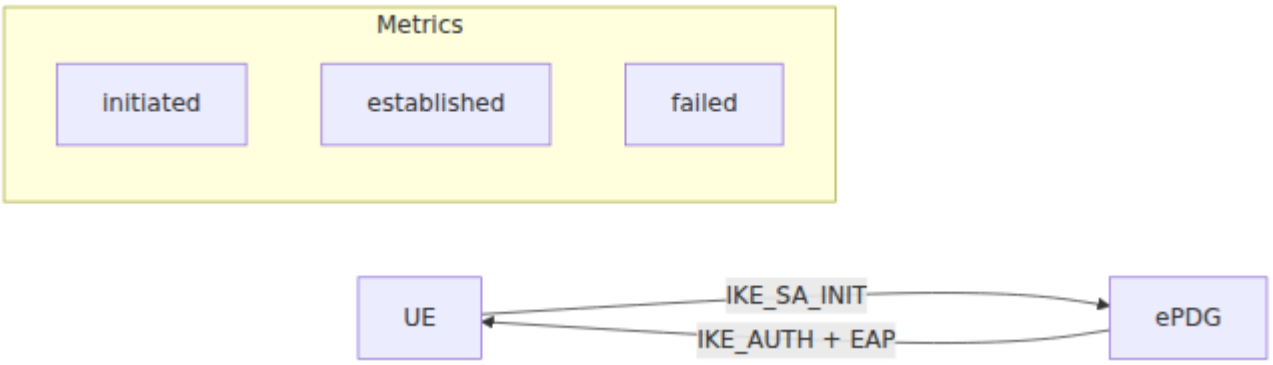
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

Parâmetro	Tipo	Padrão	Var. de Ambiente	Descrição
`port`	Inteiro	`9568`	`PROMETHEUS_PORT`	Porta HTTP para o endpoint `/metrics`

Categorias de Métricas

Métricas de Sessão IKEv2

Métricas que rastreiam o estabelecimento de túneis IKEv2 na interface SWu.



Métrica: `epdg_ikev2_session_initiated_count`
Tipo: Contador

Descrição: Total de trocas IKE_SA_INIT iniciadas. Incrementa quando um UE inicia o estabelecimento do túnel.

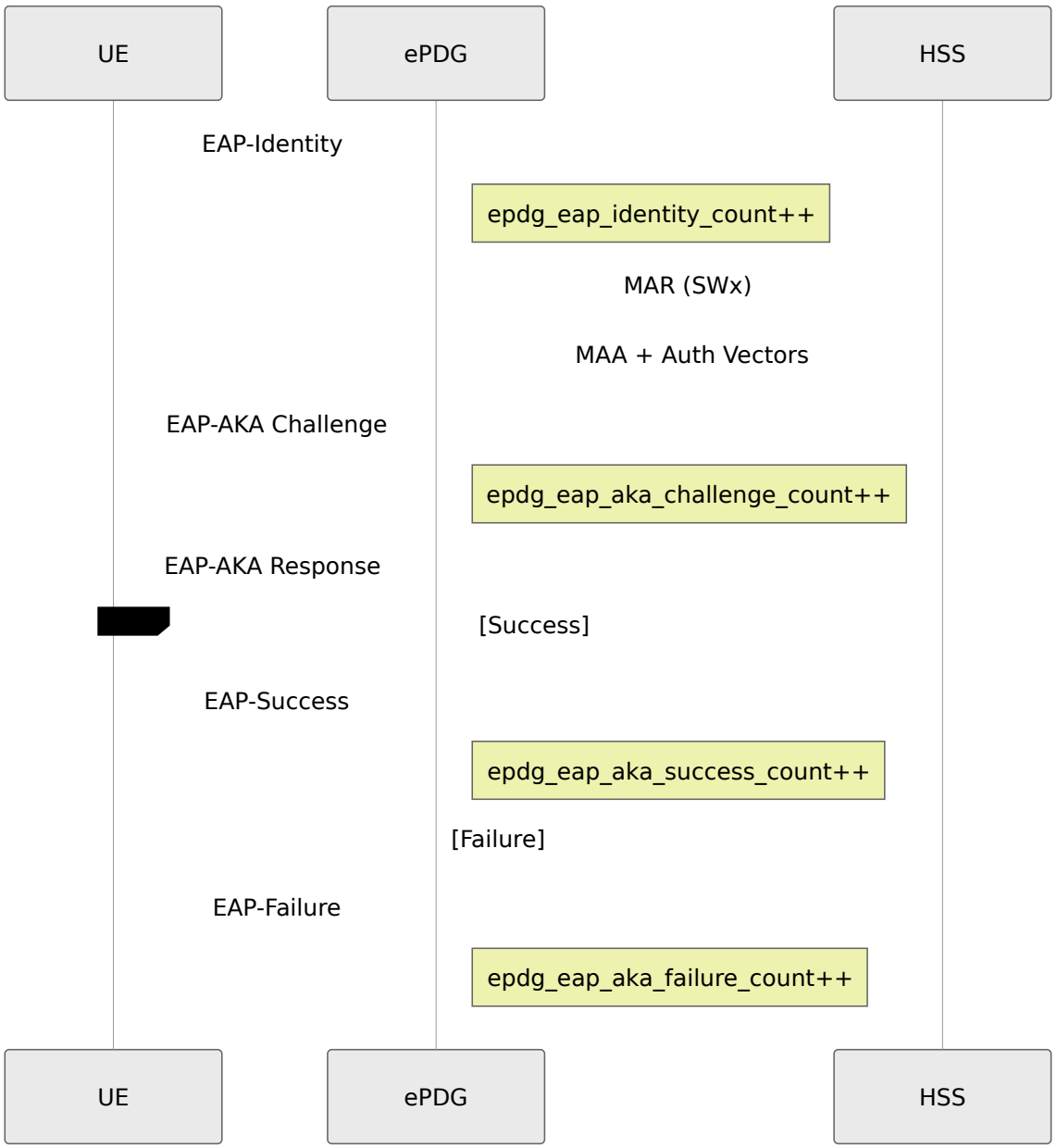
Métrica: `epdg_ikev2_session_established_count`
Tipo: Contador
Descrição: Total de IKE SAs estabelecidos com sucesso. Incrementa após autenticação EAP-AKA bem-sucedida e criação do Child SA.

Métrica: `epdg_ikev2_session_failed_count`
Tipo: Contador
Descrição: Total de falhas no estabelecimento de IKE SA
Rótulos:

- `reason` - Motivo da falha (por exemplo, `auth_failed`, `timeout`, `invalid_proposal`)

Métricas de Autenticação EAP

Métricas que rastreiam fluxos de autenticação EAP-AKA conforme RFC 4187. O OmniEPDG também suporta EAP-AKA' conforme RFC 5448, com o tipo de autenticação selecionado automaticamente com base no prefixo de identidade NAI do UE.



Métrica: `epdg_eap_identity_count`
Tipo: Contador
Descrição: Total de solicitações EAP-Identity recebidas de UEs

---

Métrica: `epdg_eap_aka_challenge_count`
Tipo: Contador
Descrição: Total de desafios EAP-AKA enviados para UEs

Métrica: `epdg_eap_aka_success_count`
Tipo: Contador
Descrição: Total de autenticações EAP-AKA bem-sucedidas

Métrica: `epdg_eap_aka_failure_count`
Tipo: Contador
Descrição: Total de autenticações EAP-AKA falhadas
Rótulos:

- `reason` - Motivo da falha (por exemplo, `res_mismatch`, `invalid_identity`, `authentication_rejected`)

Métrica: `epdg_eap_aka_sync_failure_count`
Tipo: Contador
Descrição: Total de falhas de sincronização do número de sequência (SQN) EAP-AKA. Indica incompatibilidade do número de sequência USIM/HSS que requer re-sincronização.

Métricas de Segurança de Autenticação

Métricas para a camada de segurança de autenticação. Consulte o Guia de Segurança para detalhes de configuração.

Métrica: `epdg_auth_verification_failed_count`
Tipo: Contador
Descrição: Total de falhas na verificação do payload AUTH. Indica potenciais ataques man-in-the-middle ou bugs de implementação.

Métrica: `epdg_auth_rate_limited_count`
Tipo: Contador
Descrição: Total de tentativas de autenticação bloqueadas por limitação de taxa
Rótulos:

- `type` - Motivo do bloqueio: `ip` (limite por IP excedido) ou `imsi` (limite por IMSI excedido)

Consultas de exemplo:

```
# Tentativas limitadas por taxa por minuto
rate(epdg_auth_rate_limited_count[1m])

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

Métrica: `epdg_auth_geoip_blocked_count`
Tipo: Contador
Descrição: Total de tentativas de autenticação bloqueadas por filtragem de país GeoIP
Rótulos:

- `country` - Código do país ISO 3166-1 alpha-2 (por exemplo, `CN`, `RU`), ou `UNKNOWN` para IPs que não puderam ser geolocalizados

Consultas de exemplo:

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

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

Métrica: `epdg_esp_replay_detected_count`
Tipo: Contador
Descrição: Total de pacotes ESP rejeitados devido à detecção de replay (por RFC 4303). Indica potenciais ataques de replay ou problemas de rede que causam reordenação de pacotes.

Métricas Diameter SWx

Métricas para a interface SWx entre ePDG e HSS conforme 3GPP TS 29.273.

Métrica: `epdg_diameter_swx_mar_count`
Tipo: Contador

Descrição: Total de Multimedia-Auth-Requests enviados ao HSS para recuperação de vetores de autenticação
Rótulos:

- `result` - Resultado da solicitação: `success` ou `failure`

Métrica: `epdg_diameter_swx_sar_count`
Tipo: Contador
Descrição: Total de Server-Assignment-Requests enviados ao HSS para registro/deregistro
Rótulos:

- `result` - Resultado da solicitação: `success` ou `failure`

Métrica: `epdg_diameter_swx_mar_latency_ms`
Tipo: Histograma
Descrição: Tempo de resposta MAR em milissegundos
Buckets: 50, 100, 250, 500, 1000, 2500 ms

Métrica: `epdg_diameter_swx_sar_latency_ms`
Tipo: Histograma
Descrição: Tempo de resposta SAR em milissegundos
Buckets: 50, 100, 250, 500, 1000, 2500 ms

Métrica: `epdg_diameter_swx_pending_count`
Tipo: Gauge
Descrição: Número atual de solicitações SWx pendentes aguardando resposta. Valores altos indicam congestionamento do HSS ou problemas de conectividade.

Métricas Diameter S6b

Métricas para a interface S6b entre o servidor AAA e o PGW conforme 3GPP TS 29.273. Apenas aplicável no modo GTP.

Métrica: `epdg_diameter_s6b_aar_count`
Tipo: Contador
Descrição: Total de AA-Requests tratados para autorização de sessão
Rótulos:

- `result` - Resultado da solicitação: `success` ou `failure`

Métrica: `epdg_diameter_s6b_str_count`
Tipo: Contador
Descrição: Total de Session-Termination-Requests processados

Métrica: `epdg_diameter_s6b_active_sessions_count`
Tipo: Gauge
Descrição: Número atual de sessões S6b ativas

Métricas de Ciclo de Vida de Sessão

Métricas que rastreiam a criação e terminação de sessões PDN.

Métrica: `epdg_session_created_count`
Tipo: Contador
Descrição: Total de sessões criadas
Rótulos:

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

Métrica: `epdg_session_terminated_count`
Tipo: Contador
Descrição: Total de sessões terminadas
Rótulos:

- `reason` - Motivo da terminação: `user_request`, `timeout`, `error`, `admin`

Métrica: `epdg_sessions_active_count`
Tipo: Gauge

Descrição: Número atual de sessões ativas. Consultado a cada 5 segundos.

Métrica: `epdg_sessions_by_state_count`
Tipo: Gauge
Descrição: Sessões agrupadas por estado FSM
Rótulos:

- `state` - Estado da sessão (por exemplo, `init`, `eap_identity`, `eap_aka_challenge`, `authenticated`, `established`)

Métrica: `epdg_auth_duration_ms`
Tipo: Histograma
Descrição: Duração total do fluxo de autenticação desde IKE_SA_INIT até a sessão estabelecida
Buckets: 100, 250, 500, 1000, 2500, 5000, 10000 ms

Métrica: `epdg_session_duration_seconds`
Tipo: Histograma
Descrição: Tempo de vida da sessão desde o estabelecimento até a terminação
Buckets: 60, 300, 900, 1800, 3600, 7200, 14400 segundos (1 min a 4 horas)

Métricas de Plano de Dados ESP

Métricas para processamento de pacotes ESP conforme RFC 4303.

Métrica: `epdg_esp_packets_in_count`
Tipo: Contador
Descrição: Total de pacotes ESP decriptados com sucesso (direção UE → rede)

Métrica: `epdg_esp_packets_out_count`
Tipo: Contador
Descrição: Total de pacotes ESP criptografados (direção rede → UE)

Métrica: `epdg_esp_bytes_in_total`
Tipo: Gauge
Descrição: Total de bytes decriptados de pacotes ESP

Métrica: `epdg_esp_bytes_out_total`
Tipo: Gauge
Descrição: Total de bytes criptografados em pacotes ESP

Métricas de Pool de IP

Métricas para gerenciamento de pool de endereços IP no modo VPN Simples.

Métrica: `epdg_ip_allocated_count`
Tipo: Contador
Descrição: Total de endereços IP alocados
Rótulos:

- `type` - Tipo de endereço: `ipv4` ou `ipv6`

Métrica: `epdg_ip_released_count`
Tipo: Contador
Descrição: Total de endereços IP liberados
Rótulos:

- `type` - Tipo de endereço: `ipv4` ou `ipv6`

Métrica: `epdg_ip_pool_allocated_count`
Tipo: Gauge
Descrição: Número atual de endereços IP alocados

Métrica: `epdg_ip_pool_available_count`
Tipo: Gauge
Descrição: Número atual de endereços IP disponíveis no pool

Métrica: `epdg_ip_pool_utilization_ratio`
Tipo: Gauge
Descrição: Utilização do pool de IP como uma razão de 0.0 a 1.0. Valores próximos a 1.0 indicam risco de exaustão do pool.

Métricas de VM

Métricas da máquina virtual Erlang/BEAM para monitoramento da saúde do sistema.

Métrica: `vm_memory_total`
Tipo: Gauge
Unidade: Bytes
Descrição: Total de memória alocada pela VM

Métrica: `vm_memory_processes`
Tipo: Gauge
Unidade: Bytes
Descrição: Memória usada por processos Erlang

Métrica: `vm_memory_binary`
Tipo: Gauge
Unidade: Bytes
Descrição: Memória usada para binários (incluindo buffers de pacotes)

Métrica: `vm_memory_ets`
Tipo: Gauge
Unidade: Bytes
Descrição: Memória usada por tabelas ETS (estado da sessão, registros)

Métrica: `vm_system_info_process_count`
Tipo: Gauge
Descrição: Número de processos Erlang em execução

Métrica: `vm_system_info_port_count`
Tipo: Gauge
Descrição: Número de portas abertas (sockets, identificadores de arquivos)

Métrica: `vm_statistics_run_queue`
Tipo: Gauge
Descrição: Comprimento total das filas de execução do escalonador. Valores altos indicam saturação da CPU.

Integração com Prometheus

Configuração de Raspagem

Adicione o OmniEPDG ao seu `prometheus.yml` do Prometheus:

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

Descoberta de Serviços

Para implantações no Kubernetes, use a descoberta de serviços:

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

Consultas de Exemplo

Taxa de Sucesso de Autenticação

```
# Taxa de sucesso ao longo de 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])))
```

Taxa de Estabelecimento de Sessão

```
# Sessões estabelecidas por segundo
rate(epdg_ikev2_session_established_count[5m])
```

Latência de Autenticação (p95)

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

Latência do HSS (p99)

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

Sessões Ativas

```
epdg_sessions_active_count
```

Utilização do Pool de IP

```
epdg_ip_pool_utilization_ratio * 100
```

Throughput ESP

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

# Pacotes por segundo (ambas as direções)
rate(epdg_esp_packets_in_count[5m]) +
rate(epdg_esp_packets_out_count[5m])
```

Quebra de Falhas por Motivo

```
# Falhas EAP por motivo
sum by (reason) (rate(epdg_eap_aka_failure_count[5m]))

# Terminações de sessão por motivo
sum by (reason) (rate(epdg_session_terminated_count[5m]))
```

Regras de Alerta

Exemplo de regras de alerta do Prometheus para o OmniEPDG:

```yaml
groups:
  - name: omniepdg
    rules:
      # Alta taxa de falhas de autenticação
      - 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 taxa de falhas de autenticação EAP-AKA"
          description: "A taxa de falhas de autenticação é {{
$value | humanizePercentage }} nos últimos 5 minutos"

      # Pool de IP próximo da exaustão
      - alert: OmniEPDGIPPoolLow
        expr: epdg_ip_pool_utilization_ratio > 0.9
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Utilização do pool de IP acima de 90%"
          description: "O pool de IP está {{ $value |
humanizePercentage }} utilizado"

      # Pool de IP exaurido
      - alert: OmniEPDGIPPoolExhausted
        expr: epdg_ip_pool_available_count == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "Pool de IP exaurido"
          description: "Nenhum endereço IP disponível para novas
sessões"

      # Latência alta do HSS
      - alert: OmniEPDGHSSLatencyHigh
```

```yaml
        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 latência do HSS (SWx)"
          description: "O percentil 95 da latência MAR é {{ $value
}}ms"

      # Acúmulo de solicitações SWx pendentes
      - alert: OmniEPDGSWxBacklog
        expr: epdg_diameter_swx_pending_count > 100
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "Acúmulo de solicitações SWx em construção"
          description: "{{ $value }} solicitações SWx pendentes"

      # Memória da VM alta
      - alert: OmniEPDGMemoryHigh
        expr: vm_memory_total > 2147483648
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Uso de memória do OmniEPDG alto"
          description: "O uso de memória da VM é {{ $value |
humanize1024 }}"

      # Sobrecarga do escalonador
      - alert: OmniEPDGSchedulerOverload
        expr: vm_statistics_run_queue > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Fila de execução do escalonador Erlang alta"
          description: "O comprimento da fila de execução é {{
$value }}, indicando saturação da CPU"
```

```yaml
      # Sem sessões (potencial problema de serviço)
      - alert: OmniEPDGNoSessions
        expr: epdg_sessions_active_count == 0 and
epdg_ikev2_session_initiated_count > 0
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Sem sessões ativas apesar das tentativas de
conexão"
          description: "As sessões estão sendo iniciadas, mas
nenhuma está ativa"

      # Alta atividade de limitação de taxa (potencial ataque)
      - alert: OmniEPDGHighRateLimiting
        expr: rate(epdg_auth_rate_limited_count[5m]) > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta taxa de tentativas de autenticação
bloqueadas"
          description: "{{ $value | printf \"%.1f\" }} tentativas
de autenticação bloqueadas por segundo"

      # Pico de bloqueio GeoIP (potencial ataque de região
específica)
      - alert: OmniEPDGGeoIPBlockingSpike
        expr: |
          rate(epdg_auth_geoip_blocked_count[5m]) > 5
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Atividade elevada de bloqueio GeoIP"
          description: "{{ $value | printf \"%.1f\" }} conexões
bloqueadas por segundo por GeoIP"

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

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

      # Falhas de verificação AUTH (potencial MITM)
      - alert: OmniEPDGAuthVerificationFailures
        expr: rate(epdg_auth_verification_failed_count[5m]) > 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Falhas de verificação do payload AUTH
detectadas"
          description: "Potencial ataque man-in-the-middle ou bug
de implementação"
```

Requisitos de Rede

Este documento cobre as portas do firewall e as entradas DNS necessárias para implantar o OmniEPDG para chamadas WiFi.

Portas do Firewall

Portas de Internet (UE ↔ ePDG)

Essas portas devem estar abertas para a internet para que dispositivos móveis estabeleçam conexões de chamadas WiFi.

Porta	Protocolo	Direção	Propósito
500	UDP	Entrada	Troca inicial IKEv2 (IKE_SA_INIT, IKE_AUTH)
4500	UDP	Entrada	NAT-Traversal IKEv2 e encapsulamento ESP-em-UDP

Porta 500/UDP lida com a negociação inicial do IKEv2. Se o NAT for detectado entre o UE e o ePDG (o que é quase sempre o caso para chamadas WiFi), a conexão migra automaticamente para a porta 4500.

Porta 4500/UDP transporta tanto sinalização IKEv2 quanto dados de usuário criptografados em ESP quando o NAT-T está ativo. Este é o caminho de dados principal para todo o tráfego de chamadas WiFi.

Portas de Rede Interna (ePDG ↔ Core)

Essas portas são usadas para comunica►►ão entre o OmniEPDG e a rede central móvel. Elas devem ser acessíveis a partir do ePDG, mas não expostas à internet.

Porta	Protocolo	Direção	Propósito	Par
3868	TCP	Bidirecional	Diameter SWx (autenticação)	HSS / DRA
3868	TCP	Bidirecional	Diameter S6b (autorização de sessão)	PGW / AAA
2123	UDP	Bidirecional	GTPv2-C plano de controle (S2b)	PGW
2152	UDP	Bidirecional	GTP-U plano de usuário (S2b-U)	PGW

Portas de Gerenciamento

Essas portas são para monitoramento operacional e devem ser restritas a redes de gerenciamento.

Porta	Protocolo	Propósito
4000	TCP	Interface web do painel de controle (HTTP)
443	TCP	Interface web do painel de controle (HTTPS, produção)
9568	TCP	Endpoint de métricas do Prometheus

Requisitos de DNS

Registro DNS de Descoberta do ePDG

Dispositivos móveis descobrem o ePDG usando uma convenção de nomenclatura DNS padronizada definida no 3GPP TS 23.003. O formato FQDN

é:

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

Onde:

- `<MCC>` é o Código de País Móvel de 3 dígitos (por exemplo, `505` para Austrália)
- `<MNC>` é o Código de Rede Móvel de 2 ou 3 dígitos, preenchido com zeros até 3 dígitos (por exemplo, `001`)

O registro DNS deve ser um **registro A** (ou AAAA para IPv6) apontando para o endereço IP público do OmniEPDG.

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

Nome Comum do Certificado

O certificado TLS do ePDG deve ter um Nome Alternativo de Assunto (SAN) correspondente ao FQDN do ePDG ao qual os dispositivos se conectarão. Isso é validado pelo UE durante a autenticação IKEv2.

Requisitos do certificado:

- O SAN deve incluir o FQDN de descoberta do ePDG (por exemplo, `epdg.epc.mnc001.mcc001.pub.3gppnetwork.org`)
- O certificado deve ser assinado por uma CA confiável (os dispositivos validam a cadeia)
- Mínimo de RSA 2048 bits ou ECDSA P-256

DNS do Domínio Diameter

Para um roteamento Diameter adequado, o domínio deve ser resolvido via registros DNS NAPTR/SRV conforme o RFC 6408. O formato do domínio é:

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

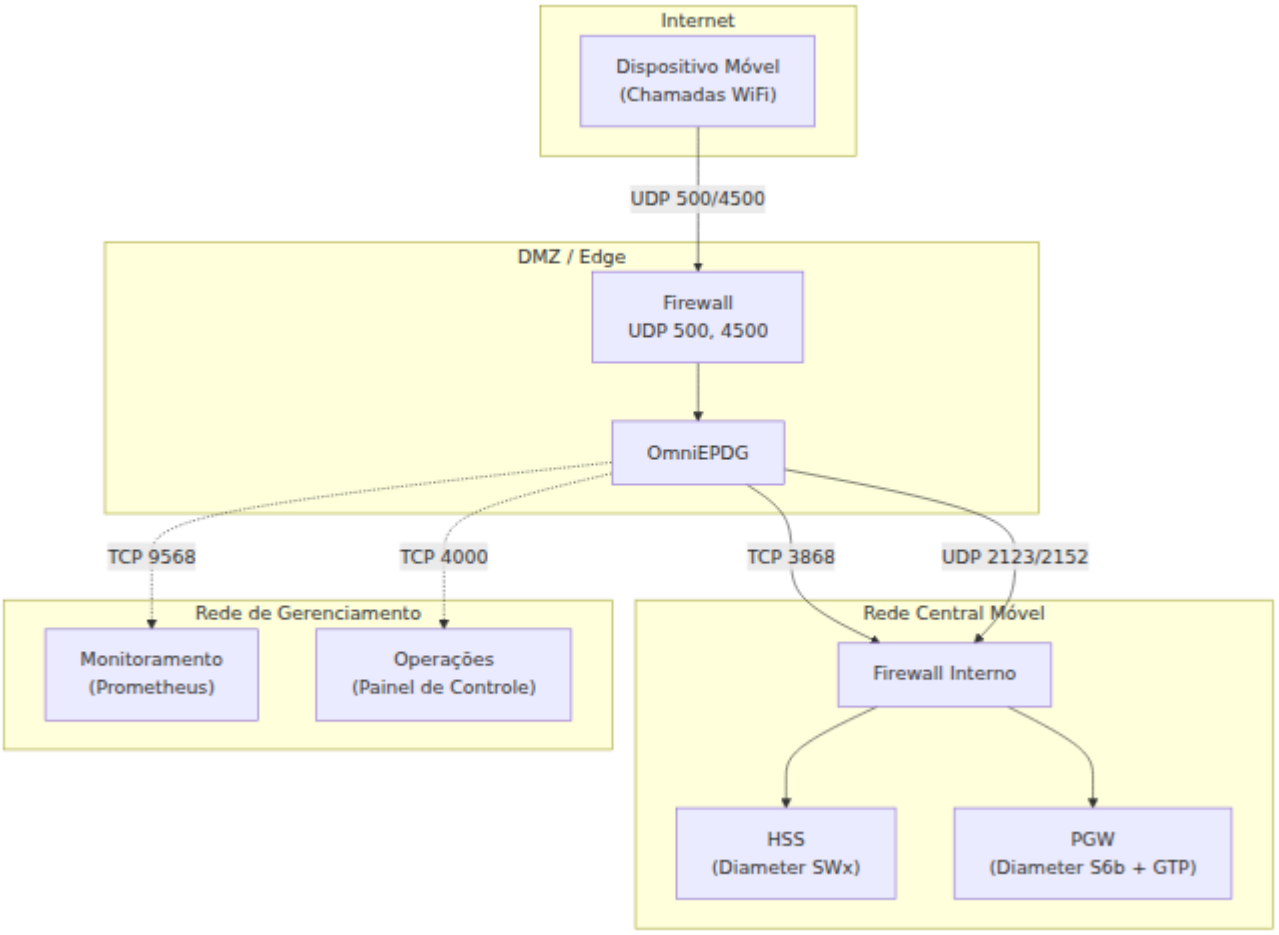
Exemplo:

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

Este domínio é usado em:

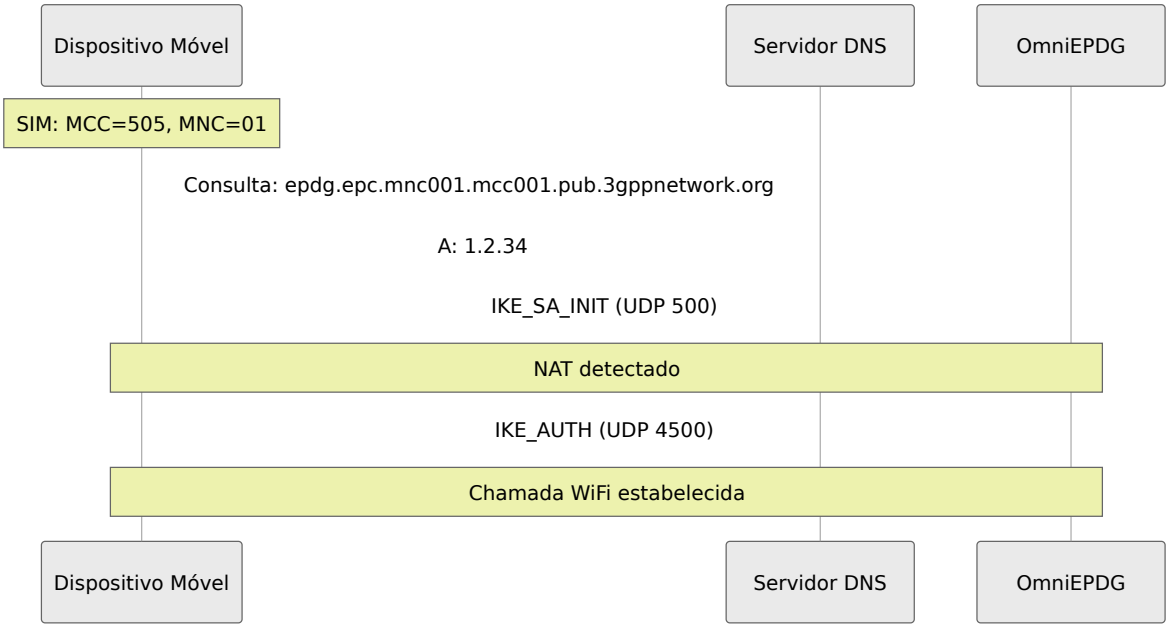
- NAI (Identificador de Acesso à Rede) enviado pelo UE durante a autenticação
- AVPs de Diameter Origin-Realm e Destination-Realm
- Decisões de roteamento Diameter

Topologia da Rede



Fluxo de Consulta DNS

Quando um dispositivo móvel inicia uma chamada WiFi, a seguinte resolução DNS ocorre:



Lista de Verificação

Requisitos de Internet

- [ ] UDP 500 aberto para entrada no OmniEPDG
- [ ] UDP 4500 aberto para entrada no OmniEPDG
- [ ] Registro DNS A: `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` → IP público do ePDG
- [ ] Certificado TLS com SAN correspondente instalado

Requisitos da Rede Central

- [ ] TCP 3868 aberto entre OmniEPDG e HSS/DRA
- [ ] TCP 3868 aberto entre OmniEPDG e PGW/AAA (apenas modo GTP)
- [ ] UDP 2123 aberto entre OmniEPDG e PGW (apenas modo GTP)
- [ ] UDP 2152 aberto entre OmniEPDG e PGW (apenas modo GTP)

Requisitos de Gerenciamento

- [ ] TCP 4000/443 acessível a partir da rede de operações
- [ ] TCP 9568 acessível a partir da infraestrutura de monitoramento

Referências

- 3GPP TS 23.003 - Numeração, endereçamento e identificação (formato FQDN do ePDG)
- 3GPP TS 23.402 - Melhorias de arquitetura para acessos não 3GPP
- RFC 7296 - Protocolo IKEv2
- RFC 3948 - Encapsulamento UDP de Pacotes ESP do IPsec (NAT-T)
- RFC 6733 - Protocolo Base Diameter

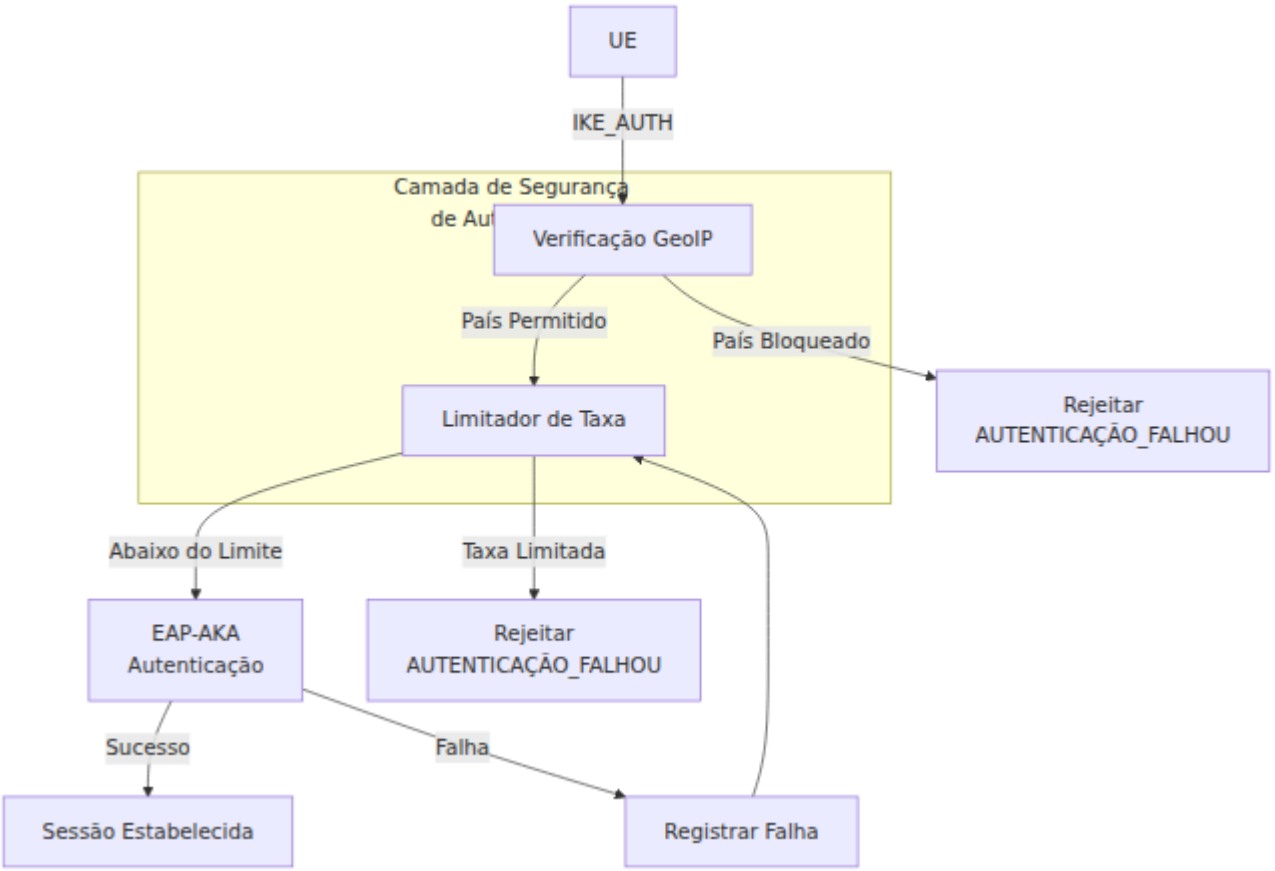
Segurança de Autenticação do OmniEPDG

O OmniEPDG implementa múltiplas camadas de segurança de autenticação para proteger contra ataques de força bruta, preenchimento de credenciais e acesso não autorizado de regiões restritas.

Índice

- Visão Geral
- Limitação de Taxa de Autenticação
- Bloqueio de Países GeoIP
- Fluxo de Segurança
- Métricas
- Solução de Problemas

Visão Geral



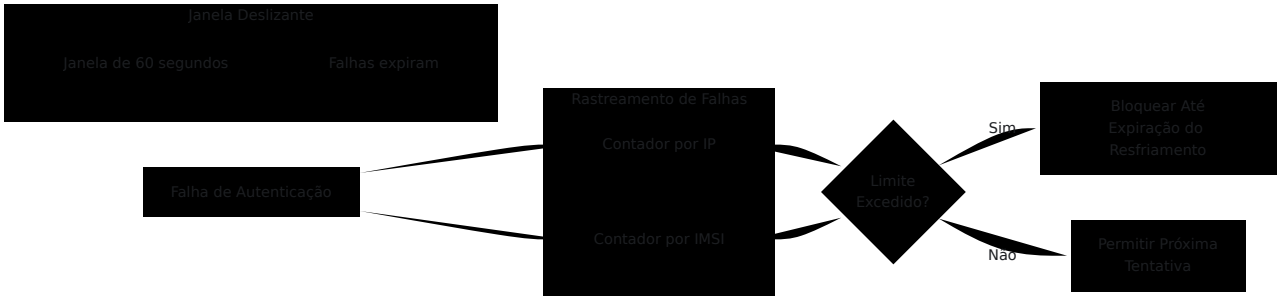
O OmniEPDG realiza verificações de segurança no início da troca IKE_AUTH, antes de operações criptográficas dispendiosas:

1. **Verificação GeoIP** (opcional) - Verifica se o IP de origem é de um país permitido
2. **Verificação de Limite de Taxa** - Garante que o IP/IMSI não excedeu os limites de falha
3. **Autenticação EAP-AKA** - A autenticação padrão 3GPP prossegue se as verificações forem bem-sucedidas

Limitação de Taxa de Autenticação

A limitação de taxa protege contra ataques de força bruta rastreando tentativas de autenticação falhadas por IP de origem e por IMSI. Quando os limites são excedidos, novas tentativas são temporariamente bloqueadas.

Como Funciona



O limitador de taxa usa um **algoritmo de janela deslizante**:

- Cada tentativa falhada é registrada com um timestamp
- Tentativas mais antigas do que a janela configurada são automaticamente expiradas
- Quando as falhas na janela excedem o limite, a fonte é bloqueada
- Bloqueios expiram após o período de resfriamento configurado

Rastreamento Duplo

Dois limites independentes são aplicados simultaneamente:

Tipo de Rastreamento	Propósito	Limite Padrão	Bloqueio Padrão
Por IP	Captura scanners de porta e ataques distribuídos de fontes únicas	10 falhas / minuto	5 minutos
Por IMSI	Captura ataques direcionados a assinantes específicos	5 falhas / minuto	10 minutos

Ambas as verificações devem ser bem-sucedidas para que uma tentativa de autenticação prossiga. Se qualquer limite for excedido, a tentativa é rejeitada.

Configuração

```
config :omniepdg,
  # Limitação de taxa por IP
  auth_rate_limit_per_ip: 10,            # Máx. falhas antes do
bloqueio
  auth_rate_limit_ip_window_ms: 60_000,  # Tamanho da janela (1
minuto)
  auth_rate_limit_ip_block_ms: 300_000,  # Duração do bloqueio (5
minutos)

  # Limitação de taxa por IMSI
  auth_rate_limit_per_imsi: 5,             # Máx. falhas antes do
bloqueio
  auth_rate_limit_imsi_window_ms: 60_000,  # Tamanho da janela (1
minuto)
  auth_rate_limit_imsi_block_ms: 600_000   # Duração do bloqueio
(10 minutos)
```

Parâmetros por IP

Parâmetro	Tipo	Obrigatório	Padrão	Des
`auth_rate_limit_per_ip`	Inteiro	Não	`10`	Máxim tentati autent falhad permit um ún endere dentro períod janela do blo
`auth_rate_limit_ip_window_ms`	Inteiro	Não	`60000`	Taman janela desliza milisse para contag falhas Falhas antiga que iss são co
`auth_rate_limit_ip_block_ms`	Inteiro	Não	`300000`	Duraçã milisse para b um IP exced limite. padrão minuto

Parâmetros por IMSI

Parâmetro	Tipo	Obrigatório	Padrão	De
`auth_rate_limit_per_imsi`	Inteiro	Não	`5`	Máx tent aute falh perr para únic dent perí jane do b Men por capt atac dire
`auth_rate_limit_imsi_window_ms`	Inteiro	Não	`60000`	Tam jane desl milis para cont falh IMSI
`auth_rate_limit_imsi_block_ms`	Inteiro	Não	`600000`	Dura milis para um exce limit padr

Parâmetro	Tipo	Obrigatório	Padrão	De
				min (ma que bloq IP pa prot assi espe

Comportamento em Caso de Sucesso

Quando a autenticação é bem-sucedida, o limitador de taxa limpa todo o histórico de falhas para aquele par IP/IMSI. Isso permite que usuários legítimos que enfrentaram falhas transitórias (por exemplo, problemas de rede) se recuperem sem serem penalizados permanentemente.

Exemplos de Configuração

Ambiente de Alta Segurança

Limites rigorosos para ambientes com baixa tolerância a tentativas falhadas:

```
config :omniepdg,
  auth_rate_limit_per_ip: 5,
  auth_rate_limit_ip_window_ms: 120_000,   # Janela de 2 minutos
  auth_rate_limit_ip_block_ms: 900_000,    # Bloqueio 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  # Bloqueio de 30
minutos
```

Como funciona: Apenas 5 falhas por IP ou 3 falhas por IMSI são permitidas dentro de uma janela de 2 minutos. Os bloqueios duram de 15 a 30 minutos, respectivamente.

Caso de uso: Implantações empresariais, bases de assinantes de alto valor ou redes sob ataque ativo.

Ambiente Relaxado

Limites mais permissivos para desenvolvimento ou testes:

```
config :omniepdg,
  auth_rate_limit_per_ip: 50,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 60_000,     # Bloqueio 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   # Bloqueio de 2 minutos
```

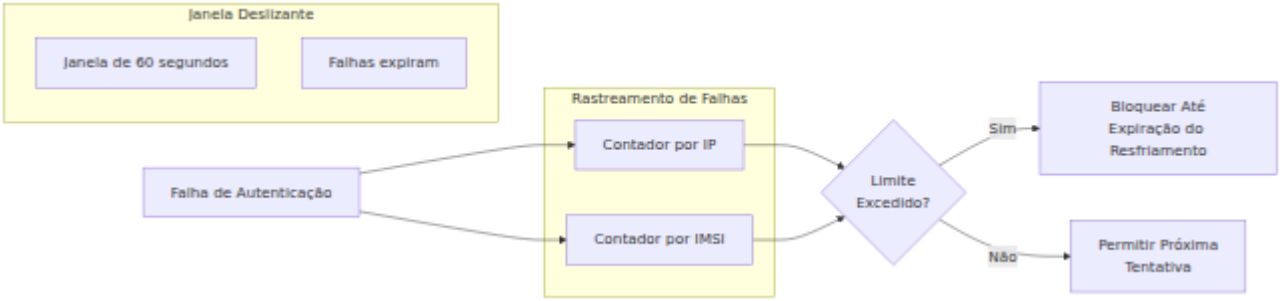
Como funciona: Limites mais altos e bloqueios mais curtos permitem mais flexibilidade de teste.

Caso de uso: Ambientes de desenvolvimento, testes de integração.

Bloqueio de Países GeoIP

O bloqueio GeoIP restringe o acesso a chamadas WiFi com base na localização geográfica do endereço IP de conexão. Isso é útil para operadores que precisam limitar o serviço a países específicos por razões regulatórias ou comerciais.

Visão Geral



Banco de dados de geolocalização de IP

O OmniEPDG usa o banco de dados **DB-IP IP-to-City Lite** (CC BY 4.0. Veja `priv/geoip/ATTRIBUTION.md`). Ele **não** está comprometido com o git (~125 MB). Em vez disso, é **baixado no momento da construção**. O `mix release` executa a tarefa `geoip.fetch` como uma etapa de lançamento, então cada pacote envia um banco de dados atual. (Dev/teste busca sob demanda via o alias `mix test`.) Por causa disso:

- **Cada sessão é anotada automaticamente** com país, cidade e coordenadas aproximadas. A interface web ("Coluna Localização") e a resposta do `/api/sessions` mostram isso: `country_code`, `country_name`, `continent_code`, `geo_city`, `geo_latitude`, `geo_longitude`.
- `geoip_enabled` **apenas** controla se as conexões são *bloqueadas* por país. A anotação acontece independentemente deste sinalizador.

Usando seu próprio banco de dados (opcional). Defina `geoip_database_path` para um MaxMind GeoLite2 (`https://www.maxmind.com/en/geolite2/signup`) ou outro DB-IP/MaxMind MMDB. Se o arquivo configurado estiver ausente, o banco de dados incluído (baixado) é usado. Nota: O EULA do MaxMind GeoLite2 **não** permite redistribuí-lo dentro de um produto, que é o motivo pelo qual o DB-IP Lite (CC BY 4.0) é usado em vez disso.

Para atualizar o banco de dados manualmente (o DB-IP publica mensalmente):

```
mix geoip.fetch
```

Configuração

```
config :omniepdg,
  # Bloquear conexões por país (anotação de geolocalização está
sempre ativada)
  geoip_enabled: true,

  # Opcional: substituir o DB incluído pelo seu próprio MMDB (País
ou Cidade)
  # geoip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",

  # Modo de controle de acesso
  geoip_mode: :whitelist,

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

  # Lidar com IPs desconhecidos
  geoip_allow_unknown: false,

  # Comportamento quando o banco de dados não está disponível
  geoip_fail_open: true
```

Parâmetros

Parâmetro	Tipo	Obrigatório	Padrão	Descri
`geoip_enabled`	Booleano	Não	`false`	Ativar ou desativar controle c acesso ba em GeoIP (bloqueio Quando `f` todos os I permitido as sessõe ainda são anotadas.
`geoip_database_path`	String	Não	banco de dados incluído `dbip-country-lite.mmdb`	Caminho um banco dados no formato M (País ou Cidade). Reverte p banco de DB-IP incl se não es definido c estiver au
`geoip_mode`	Átomo	Não	`:whitelist`	Modo de controle c acesso: `:whiteli` (apenas permitir p listados) c

Parâmetro	Tipo	Obrigatório	Padrão	Descri
				`:blackli` (bloquear países list permitir o
`geoip_countries`	Lista	Não	`[]`	Lista de c de países 3166-1 al A interpre depende `geoip_mo`
`geoip_allow_unknown`	Booleano	Não	Veja abaixo	Permitir conexões que não p ser geolocaliz (IPs priva faixas desconhe O padrão `false` pa modo de branca, `t` para o mo lista negr
`geoip_fail_open`	Booleano	Não	`true`	Comporta quando o de dados falha ao carregar. Quando `t` permite t as conexõ (falha abe

Parâmetro	Tipo	Obrigatório	Padrão	Descri
				Quando `f` bloqueia t as conexõ (falha fec

Modos de Controle de Acesso

Modo de Lista Branca (Recomendado para Chamadas WiFi)

Permitir apenas conexões de países especificados. Todos os outros países são bloqueados.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ", "FJ"]  # Austrália, Nova Zelândia,
Fiji
```

Como funciona: Apenas UEs conectando de endereços IP australianos, neozelandeses ou fijianos podem se autenticar. Todos os outros países são rejeitados.

Caso de uso: Operadores que desejam restringir chamadas WiFi às suas áreas de serviço licenciadas.

Modo de Lista Negra

Bloquear conexões de países especificados. Todos os outros países são permitidos.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :blacklist,
  geoip_countries: ["CN", "RU", "KP", "IR"]  # China, Rússia,
Coreia do Norte, Irã
```

Como funciona: UEs conectando dos países listados são rejeitados. Todos os outros países podem se autenticar.

Caso de uso: Bloqueio de regiões de alto risco enquanto permite roaming global.

Lidar com Países Desconhecidos

Alguns endereços IP não podem ser geolocalizados:

- Faixas de IP privadas (10.x.x.x, 192.168.x.x, etc.)
- Blocos de IP recém-alocados que ainda não estão no banco de dados
- Nós de saída Tor e alguns VPNs

O parâmetro `geoip_allow_unknown` controla o comportamento:

Modo	`geoip_allow_unknown` Padrão	Comportamento
Lista Branca	`false`	Desconhecido = não está na lista branca = bloqueado
Lista Negra	`true`	Desconhecido = não está na lista negra = permitido

Para substituir o padrão:

```
config :omniepdg,
  geoip_mode: :whitelist,
  geoip_allow_unknown: true  # Permitir IPs desconhecidos mesmo no
modo de lista branca
```

Atualizações do Banco de Dados

A MaxMind atualiza o banco de dados GeoLite2 semanalmente. Para atualizar:

1. Baixe o novo arquivo `GeoLite2-Country.mmdb`

2. Substitua o arquivo existente no caminho configurado
3. O banco de dados é recarregado automaticamente na próxima verificação (sem necessidade de reinício)

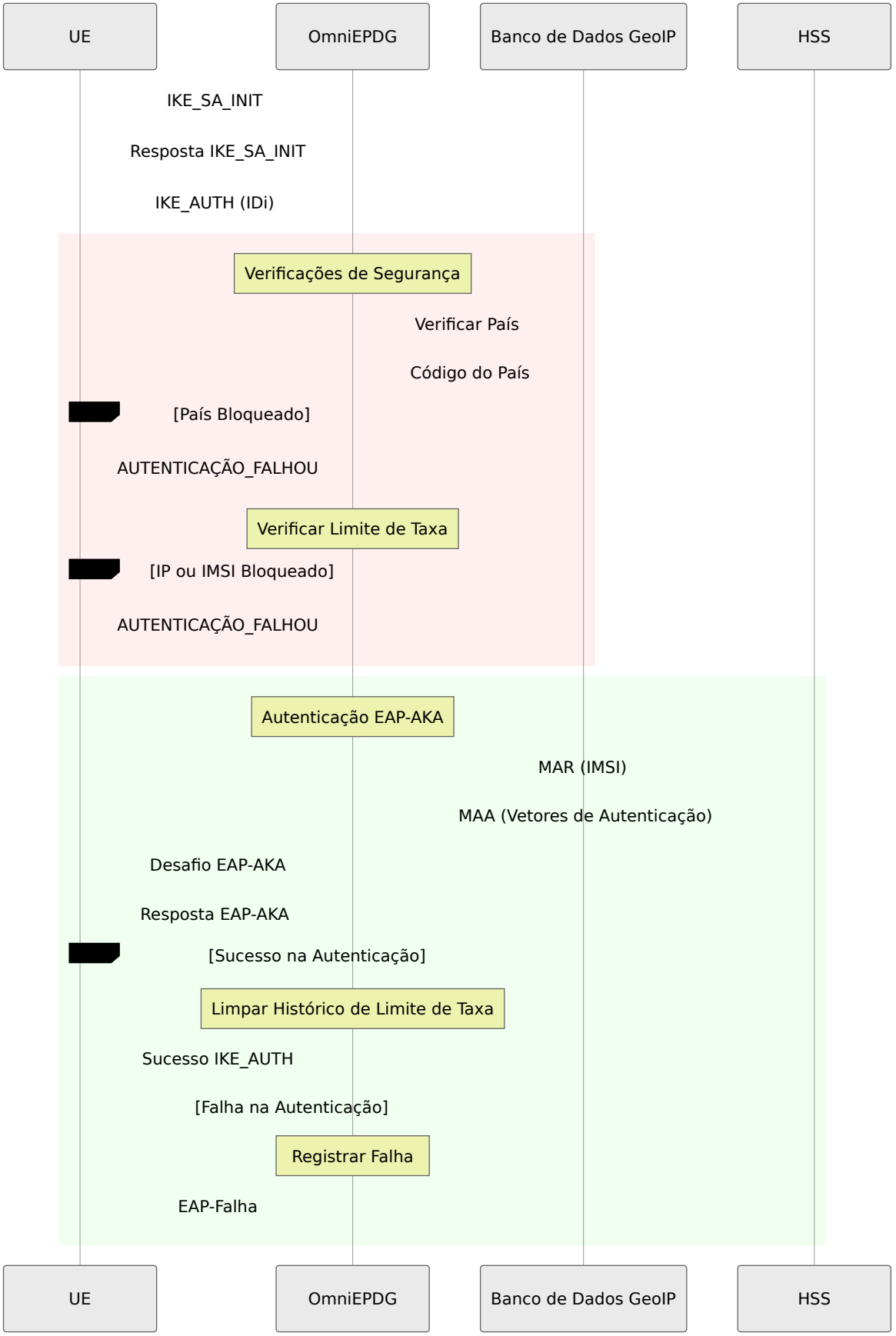
Códigos de País Comuns

Código	País	Código	País
AU	Austrália	US	Estados Unidos
NZ	Nova Zelândia	GB	Reino Unido
CA	Canadá	DE	Alemanha
FR	França	JP	Japão
SG	Cingapura	HK	Hong Kong
IN	Índia	CN	China

Lista completa: ISO 3166-1 alpha-2

Fluxo de Segurança

O fluxo completo de segurança de autenticação:


UE
OmniEPDG
Banco de Dados GeoIP
HSS
IKE_SA_INIT
Resposta IKE_SA_INIT
IKE_AUTH (IDi)
Verificações de Segurança
Verificar País
Código do País
[País Bloqueado]
AUTENTICAÇÃO_FALHOU
Verificar Limite de Taxa
[IP ou IMSI Bloqueado]
AUTENTICAÇÃO_FALHOU
Autenticação EAP-AKA
MAR (IMSI)
MAA (Vetores de Autenticação)
Desafio EAP-AKA
Resposta EAP-AKA
[Sucesso na Autenticação]
Limpar Histórico de Limite de Taxa
Sucesso IKE_AUTH
[Falha na Autenticação]
Registrar Falha
EAP-Falha
UE
OmniEPDG
Banco de Dados GeoIP
HSS

Métricas

Métricas de Limitação de Taxa

Métrica: `epdg_auth_rate_limited_count` **Tipo**: Contador **Descrição**: Número de tentativas de autenticação bloqueadas pela limitação de taxa **Rótulos**:

- `type` - Razão do bloqueio: `ip` (limite de IP excedido) ou `imsi` (limite de IMSI excedido)

Consultas de exemplo:

```
# Tentativas limitadas por taxa por minuto
rate(epdg_auth_rate_limited_count[1m])

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

# Alerta: Alta atividade de limitação de taxa
rate(epdg_auth_rate_limited_count[5m]) > 10
```

Métricas GeoIP

Métrica: `epdg_auth_geoip_blocked_count` **Tipo**: Contador **Descrição**: Número de tentativas de autenticação bloqueadas pelo GeoIP **Rótulos**:

- `country` - Código do país ISO 3166-1 alpha-2, ou `UNKNOWN` para IPs não resolvíveis

Consultas de exemplo:

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

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

# Alerta: País incomum tentando acesso
increase(epdg_auth_geoip_blocked_count{country="XX"}[1h]) > 100
```

Solução de Problemas

Problemas de Limitação de Taxa

Usuários Legítimos Sendo Bloqueados

Sintomas: Usuários relatam que não conseguem se conectar após tentativas falhadas

Possíveis causas:

- Usuário inseriu credenciais erradas várias vezes
- Problemas de rede causaram timeouts de autenticação contados como falhas
- Limites configurados muito baixos para o ambiente

Resolução:

1. Verifique as métricas para o IP/IMSI afetado
2. Considere aumentar os limites se falsos positivos forem comuns
3. Após corrigir a causa raiz, o bloqueio expirará automaticamente

Alta Taxa de Tentativas Bloqueadas

Sintomas: `epdg_auth_rate_limited_count` aumentando rapidamente

Possíveis causas:

- Ataque de força bruta em andamento

- UE mal configurado falhando repetidamente na autenticação
- Ataque de preenchimento de credenciais

Resolução:

1. Revise os IPs de origem nos logs em busca de padrões
2. Considere implementar regras de firewall em nível de IP para atacantes persistentes
3. Verifique a conectividade do HSS se usuários legítimos forem afetados

Problemas GeoIP

Todas as Conexões Sendo Bloqueadas

Sintomas: Nenhum UE consegue se conectar após ativar o GeoIP

Possíveis causas:

- Arquivo do banco de dados não encontrado ou corrompido
- Códigos de país errados na configuração
- `geoip_allow_unknown: false` bloqueando IPs privados em ambiente de laboratório

Resolução:

1. Verifique se o arquivo do banco de dados existe no caminho configurado
2. Verifique se os códigos de país estão corretos (maiúsculas, 2 letras)
3. Para laboratório/desenvolvimento, defina `geoip_allow_unknown: true`
4. Verifique os logs para avisos relacionados ao GeoIP

Banco de Dados GeoIP Não Carregando

Sintomas: Aviso nos logs: "Banco de dados GeoIP não encontrado"

Possíveis causas:

- Caminho do arquivo incorreto
- Permissões de arquivo impedem leitura

- O arquivo não é um formato MMDB válido

Resolução:

1. Verifique se o arquivo existe: `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. Verifique as permissões: `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. Verifique a integridade do arquivo baixando uma cópia nova do MaxMind

Bloqueios de Países Inesperados

Sintomas: Usuários de países permitidos sendo bloqueados

Possíveis causas:

- VPN/proxy fazendo o IP parecer de um país diferente
- Banco de dados GeoIP desatualizado
- Egress de rede corporativa em local inesperado

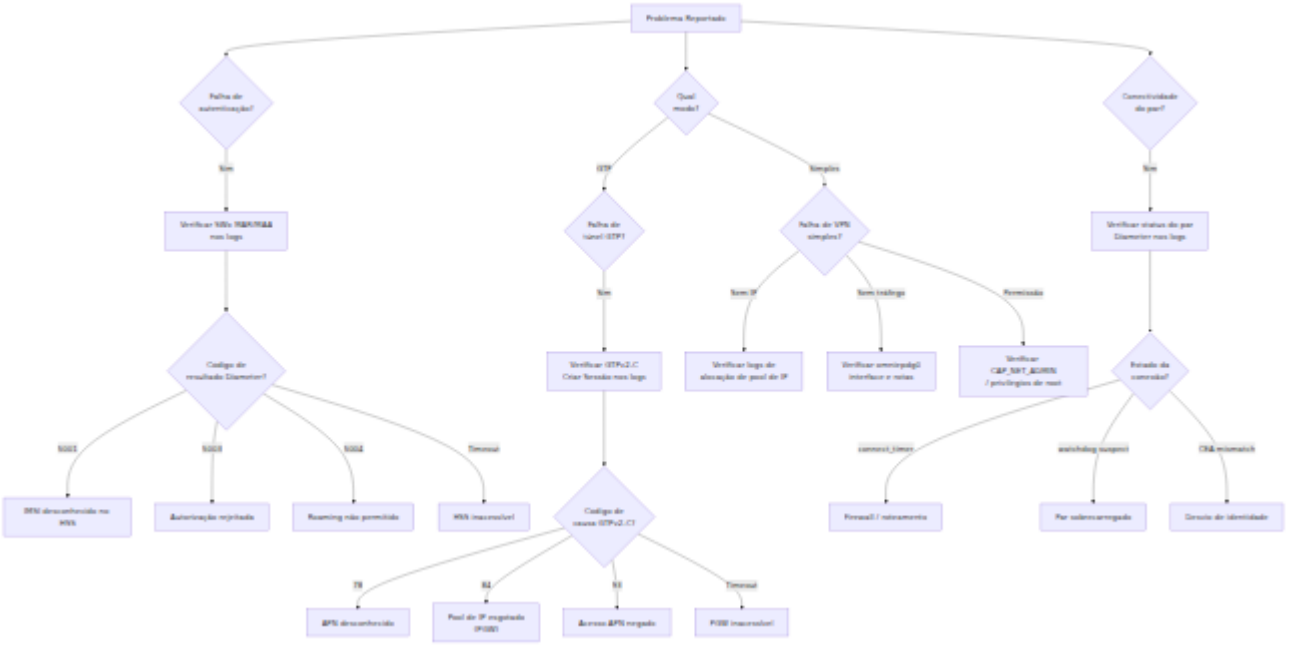
Resolução:

1. Atualize o banco de dados GeoIP para a versão mais recente
2. Verifique o IP de saída real do usuário em comparação com o país esperado
3. Considere adicionar países adicionais se os usuários passarem por redes corporativas

Solução de Problemas do OmniEPDG

Este guia cobre problemas operacionais comuns, procedimentos de diagnóstico e etapas de resolução para o OmniEPDG.

Visão Geral do Diagnóstico



Arquivos de Log

O OmniEPDG grava logs no diretório `log/` relativo ao diretório de trabalho da aplicação. Consulte a Referência de Configuração para detalhes sobre a configuração de logs.

Arquivo	Propósito	Quando Verificar
`log/console.log`	Todas as mensagens da aplicação no nível de depuração	Primeiro ponto de investigação para qualquer problema
`log/error.log`	Somente erros	Verificação rápida para problemas ativos
`log/crash.log`	Falhas de processos OTP	Quando os processos estão reiniciando inesperadamente
`log/erlang.log`	Registrador do núcleo Erlang	Problemas de baixo nível do Erlang/OTP

Padrões de Log Chave

Eventos de conexão de par Diameter:

- `peer_up` - Par Diameter conectado e capacidades trocadas
- `peer_down` - Par Diameter desconectado

Transições de estado do FSM UE:

- `ue_fsm state_<name> event=<event>` - FSM processando um evento em um dado estado
- `ue_fsm init(<IMSI>)` - Nova instância de FSM criada para o assinante
- `terminating epdg_ue_fsm with reason <reason>` - FSM encerrando

Eventos de Timeout:

- `Timeout swm_der_timeout` - Resposta SWm DER expirou
- `Timeout create_session_timeout` - Resposta GTPv2-C Criar Sessão expirou
- `Timeout s2b_delete_session_timeout` - Resposta GTPv2-C Deletar Sessão expirou

- `Timeout cancel_location_timeout` - Resposta Cancelar Localização expirou

Problemas de Conectividade Diameter

Falha de Conexão HSS (SWx)

Sintomas: Nenhum assinante consegue se autenticar. Os logs mostram tentativas de conexão repetidas ao HSS.

Causas possíveis:

- Firewall bloqueando a porta SCTP 3868 entre OmniEPDG e HSS
- `dia_swx_remote_ip` ou `dia_swx_remote_port` incorretos na configuração
- HSS não está em execução ou não aceita conexões Diameter
- SCTP não habilitado no caminho da rede (alguns firewalls bloqueiam SCTP por padrão)
- Desvio de Origin-Host ou Origin-Realm causando rejeição de CEA

Resolução:

1. Verifique a conectividade da rede com o IP e a porta do HSS
2. Confirme que `dia_swx_remote_ip` e `dia_swx_remote_port` correspondem à configuração do HSS
3. Verifique se o tráfego SCTP é permitido através de todos os firewalls. Se SCTP estiver bloqueado, defina `dia_swx_proto` como `tcp` como uma alternativa
4. Verifique se `dia_swx_origin_host` é um FQDN resolvível e corresponde ao que o HSS espera
5. Verifique os logs do HSS para falhas de negociação Diameter CER/CEA

Falha de Conexão PGW (S6b)

Sintomas: A autenticação é bem-sucedida, mas a criação do túnel GTP falha ou o AAR S6b nunca chega do PGW. Os logs não mostram evento S6b peer_up.

Causas possíveis:

- PGW não configurado para conectar ao ouvinte S6b do OmniEPDG
- Firewall bloqueando a porta SCTP 3868 no endereço de ligação S6b do OmniEPDG
- `dia_s6b_local_ip` não acessível a partir do PGW
- Desvio de Origin-Host ou Origin-Realm

Resolução:

1. Confirme que o PGW está configurado para conectar ao OmniEPDG em `dia_s6b_local_ip`:`dia_s6b_local_port`
2. Verifique se o endereço de ligação S6b é acessível a partir da rede do PGW
3. Verifique se as regras do firewall permitem SCTP de entrada na porta 3868 no endereço S6b
4. Verifique se `dia_s6b_origin_host` e `dia_s6b_origin_realm` correspondem ao que o PGW espera

Falhas do Watchdog Diameter

Sintomas: Conexões Diameter estabelecidas caem intermitentemente. Os logs mostram transições do watchdog para o estado SUSPECT ou DOWN.

Causas possíveis:

- Instabilidade do caminho da rede ou perda de pacotes
- Par sobrecarregado e não respondendo ao DWR dentro do `dia_swx_watchdog_timer`
- Configuração agressiva do watchdog (poucas tentativas antes de declarar suspeito)

Resolução:

1. Verifique a qualidade do caminho da rede (perda de pacotes, latência) entre o OmniEPDG e o par
2. Se a perda de pacotes for esperada, aumente os limites de `dia_swx_watchdog_config` / `dia_s6b_watchdog_config` (por exemplo, `[{okay, 5}, {suspect, 3}]`)
3. Verifique a saúde do sistema do par (CPU, memória, contagem de conexões)

Falhas de Negociação IKEv2

Nenhuma Proposta Escolhida

Sintomas: O IKE_SA_INIT do UE é rejeitado com `NO_PROPOSAL_CHOSEN`; os logs mostram `exchange error: :no_proposal_chosen`. O UE nunca avança além do IKE_SA_INIT.

Causas possíveis:

- O UE oferece apenas transformações criptográficas que o OmniEPDG não suporta.
- Um scanner ou cliente mal configurado sondando as portas públicas.

Contexto: O OmniEPDG aceita criptografia AES-CBC e AES-GCM; integridade HMAC-SHA2, HMAC-SHA1 e **AES-XCBC-96**; PRFs HMAC-SHA2, HMAC-SHA1 e **PRF-AES128-XCBC**; e grupos DH MODP/ECP/Curve25519/448. Consulte Algoritmos Criptográficos para a lista completa. Alguns dispositivos (notavelmente certos clientes Samsung VoWiFi) oferecem apenas `AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048`, todos suportados.

Resolução:

1. Ative o registro `:debug` e inspecione o evento `IKEv2 packet` para a carga útil SA do UE. Os campos `payloads[].proposals[]` listam as transformações exatas oferecidas.
2. Confirme que a criptografia / integridade / PRF / DH oferecidas aparecem como Suportadas nas tabelas de algoritmos.

3. Se uma transformação genuinamente não suportada for necessária, eleve a questão com a engenharia.

Conexão Estabelecida e Depois Cai Imediatamente (Child SA Deletada)

Sintomas: O IKE_AUTH é concluído, a sessão é brevemente estabelecida, então o UE envia um `DELETE` INFORMATIVO dentro de ~100 ms. Nenhum fluxo de mídia. Repete em cada tentativa.

Causas possíveis:

- As transformações do Child SA (ESP) na resposta não correspondem ao que o UE ofereceu, então o UE encerra o SA.
- Um algoritmo de integridade/criptografia ESP que o plano de dados não consegue processar.

Contexto: O OmniEPDG negocia o Child SA ESP a partir da proposta oferecida pelo UE (incluindo AES-XCBC-96 e AES-CBC-128/192/256) em vez de forçar um conjunto fixo. Uma resposta que seleciona uma transformação que o UE não ofereceu é rejeitada conforme o RFC 7296.

Resolução:

1. No `:debug`, verifique a linha de log `child SA proposal selected`. Os campos `esp_offered`, `esp_encr` e `esp_integ` mostram o que foi oferecido e escolhido.
2. Verifique se o comprimento da chave de criptografia ESP selecionada corresponde ao cifrador (uma incompatibilidade aparece como `Bad key size` e um pacote descartado).
3. Confirme que a integridade ESP oferecida pelo UE é uma que o OmniEPDG suporta (veja Algoritmos do Child SA ESP).

Falhas de Autenticação

IMSI Desconhecido (Diameter 5001)

Sintomas: Assinantes específicos falham na autenticação EAP-AKA. Os logs mostram SWx MAA com código de resultado 5001 (DIAMETER_ERROR_USER_UNKNOWN).

Causas possíveis:

- Assinante não provisionado no HSS
- Incompatibilidade de IMSI entre o SIM do UE e o banco de dados do HSS
- Formato NAI incorreto, causando falha na extração do IMSI

Resolução:

1. Verifique se o IMSI do assinante existe no banco de dados do HSS
2. Verifique se o formato NAI nos logs corresponde ao padrão esperado: `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`
3. Confirme se o IMSI do cartão SIM corresponde ao valor provisionado no HSS

Autorização Rejeitada (Diameter 5003)

Sintomas: Assinante se autentica, mas é rejeitado durante a atribuição do servidor. Os logs mostram SWx SAA com código de resultado 5003.

Causas possíveis:

- Assinante não autorizado para o serviço de chamadas WiFi
- APN não permitido para este assinante
- Restrições de perfil de assinatura

Resolução:

1. Verifique o perfil de serviço do assinante no HSS
2. Confirme se o acesso a chamadas WiFi / ePDG está habilitado para o assinante

3. Verifique se a APN solicitada está na lista de APNs permitidas do assinante

Roaming Não Permitido (Diameter 5004)

Sintomas: Assinantes em roaming falham na autenticação. Os logs mostram SWx MAA ou SAA com código de resultado 5004.

Causas possíveis:

- A política de roaming do HSS rejeita a localização atual do assinante
- Chamadas WiFi não permitidas para assinantes em roaming

Resolução:

1. Revise as políticas de roaming do HSS para a combinação HPLMN/VPLMN do assinante
2. Verifique se as chamadas WiFi são permitidas sob acordos de roaming

Timeout de Autenticação

Sintomas: A autenticação fica pendente e depois falha após 10 segundos. Os logs mostram `Timeout swm_der_timeout` no `state_wait_auth_resp`.

Causas possíveis:

- HSS não respondendo ao SWx MAR dentro de 10 segundos
- Conexão Diameter SWx interrompida durante a solicitação
- HSS sobrecarregado

Resolução:

1. Verifique a capacidade de resposta e carga do HSS
2. Confirme se o par Diameter SWx está em estado OKAY (não SUSPECT ou DOWN)
3. Verifique se `dia_swx_transmit_timer` é adequado para a latência da rede até o HSS

Incompatibilidade de Tipo EAP-AKA

Sintomas: A autenticação falha com erro "type_mismatch" nos logs. O prefixo de identidade do UE não corresponde ao método EAP utilizado.

Causas possíveis:

- UE envia identidade com prefixo `0` (EAP-AKA), mas a rede espera EAP-AKA', ou vice-versa
- HSS retorna vetores de autenticação para o tipo EAP errado

Contexto: De acordo com o 3GPP TS 23.003, o prefixo de identidade NAI indica o tipo de autenticação esperado:

- Prefixo `0` indica EAP-AKA
- Prefixo `6` indica EAP-AKA'

O OmniEPDG seleciona automaticamente o método de autenticação com base no prefixo de identidade do UE. A maioria dos UEs de chamadas WiFi usa o prefixo `0` (EAP-AKA).

Resolução:

1. Verifique a identidade NAI do UE nos logs para confirmar o prefixo
2. Certifique-se de que o HSS esteja configurado para retornar vetores de autenticação apropriados
3. Verifique se o cartão SIM está provisionado corretamente para o tipo de autenticação esperado

Incompatibilidade de RES EAP-AKA

Sintomas: A autenticação falha após desafio/resposta. Os logs mostram erro "RES mismatch" ou "res_mismatch".

Causas possíveis:

- Falha de autenticação do cartão SIM
- Incompatibilidade na derivação de chave entre o UE e a rede

- Vetores de autenticação corrompidos do HSS

Resolução:

1. Verifique se o cartão SIM é válido e não está danificado
2. Verifique se o HSS retornou vetores de autenticação válidos (RAND, AUTN, XRES, CK, IK)
3. Ative o registro de depuração para comparar o XRES esperado com o RES recebido
4. Se estiver usando SIMs de teste, verifique se os valores Ki e OP/OPc correspondem entre o SIM e o HSS

Falhas de Túnel GTP (Somente Modo GTP)

Criação de Sessão Rejeitada pelo PGW

Sintomas: A autenticação é bem-sucedida, mas a criação do túnel falha. Os logs mostram Resposta de Criação de Sessão GTPv2-C com código de erro.

Códigos de causa comuns e ações:

Código de Causa	Nome	Ação
78	APN Faltando ou Desconhecido	Verifique se a APN está configurada no PGW e corresponde ao perfil do assinante
82	Negado em RAT	Verifique se a política do PGW permite tipo de acesso WiFi (não-3GPP)
84	Todos os Endereços Dinâmicos Ocupados	Pool de IP do PGW esgotado; expanda o pool ou investigue vazamentos
92	Falha na Autenticação do Usuário	Falha de autenticação do lado do PGW; verifique a autorização da sessão S6b
93	Acesso APN Negado	Assinante não autorizado para APN no PGW
96	IMSI/IMEI Não Conhecido	Assinante desconhecido para o PGW; verifique se a sessão S6b foi autorizada
113	Congestionamento de APN	APN sobrecarregado; tente novamente ou investigue a capacidade do PGW
120	Congestionamento da Entidade GTP-C	Plano de controle do PGW sobrecarregado

Timeout de Criação de Sessão

Sintomas: A criação do túnel fica pendente por 10 segundos e depois falha. Os logs mostram `Timeout create_session_timeout` no

`state_wait_create_session_resp`.

Causas possíveis:

- PGW não acessível em `gtpc_remote_ip`:`gtpc_remote_port`
- Firewall bloqueando a porta UDP 2123 entre OmniEPDG e PGW
- PGW sobrecarregado e não respondendo a solicitações GTPv2-C

Resolução:

1. Verifique a conectividade da rede com o PGW na porta UDP 2123
2. Verifique se as regras do firewall permitem UDP 2123 entre OmniEPDG e PGW
3. Verifique a saúde do PGW e a capacidade de processamento GTPv2-C

Túnel GTP-U Não Transmitindo Tráfego

Sintomas: O túnel está estabelecido (Criação de Sessão bem-sucedida), mas o tráfego do assinante não flui.

Causas possíveis:

- Módulo do kernel GTP-U não carregado
- O socket `gtp_u_kmod` IP não corresponde ao endereço do ponto final do túnel GTP-U sinalizado ao PGW
- Roteamento não configurado para o dispositivo do túnel GTP
- Firewall bloqueando a porta UDP 2152 (GTP-U)

Resolução:

1. Verifique se o módulo GTP do kernel Linux está carregado (`lsmod | grep gtp`)
2. Confirme se o dispositivo do túnel GTP existe (`ip link show gtp0`)
3. Verifique se `gtp_u_kmod` `ip` corresponde a `gtpc_local_ip` ou ao endereço sinalizado na Solicitação de Criação de Sessão
4. Verifique se a tabela de roteamento inclui rotas através do dispositivo do túnel GTP

5. Verifique se o firewall permite a porta UDP 2152 entre OmniEPDG e PGW

Falhas de VPN Simples (Somente Modo VPN Simples)

Interface TUN Não Criada

Sintomas: O OmniEPDG inicia, mas nenhuma interface `omniepdg0` aparece. As sessões falham na configuração do túnel. Os logs podem mostrar erros de `simple_vpn_route` durante a inicialização.

Causas possíveis:

- O processo OmniEPDG não possui a capacidade `CAP_NET_ADMIN` ou não está sendo executado como root
- Módulo do kernel TUN/TAP não carregado
- Outro processo já criou uma interface chamada `omniepdg0`

Resolução:

1. Verifique se o módulo do kernel TUN está disponível (`lsmod | grep tun`)
2. Confirme que o OmniEPDG está sendo executado com privilégios suficientes para criar interfaces TUN
3. Verifique se `omniepdg0` já existe de uma instância anterior (`ip link show omniepdg0`)
4. Verifique `log/crash.log` para erros do processo do gerenciador de rotas

Pool de IP Esgotado

Sintomas: A autenticação é bem-sucedida, mas a configuração do túnel falha. Os logs mostram falha de alocação de IP de `simple_vpn_pool`.

Causas possíveis:

- Todos os endereços no pool CIDR configurado estão alocados para sessões ativas

- Endereços IP não estão sendo liberados após a finalização da sessão (vazamento)
- Tamanho do pool muito pequeno para o número de assinantes concorrentes

Resolução:

1. Verifique o número de processos `epdg_ue_fsm` ativos em relação ao tamanho do pool
2. Verifique se as sessões estão sendo encerradas corretamente (verifique mensagens de log `terminating`)
3. Se o pool estiver realmente cheio, expanda-o usando um prefixo CIDR maior em `simple_vpn_pool_ipv4` (requer reinício)
4. Verifique se há falhas no FSM durante a finalização em `log/crash.log` que podem ter impedido a liberação de IP

Tráfego do Assinante Não Fluindo

Sintomas: A sessão está estabelecida e o UE recebe um endereço IP, mas o tráfego não flui pela interface TUN.

Causas possíveis:

- Rota host não adicionada para o IP do assinante em `omniepdg0`
- Encaminhamento de IP não habilitado no host OmniEPDG
- Regras de firewall bloqueando tráfego na interface `omniepdg0`
- Regras NAT/mascaramento ausentes para tráfego de saída do intervalo de IP do assinante

Resolução:

1. Verifique se a rota host existe (`ip route show` e procure a rota /32 do assinante via `omniepdg0`)
2. Confirme se o encaminhamento de IP está habilitado (`sysctl net.ipv4.ip_forward`)
3. Verifique as regras do iptables/nftables permitem o encaminhamento através de `omniepdg0`

4. Se os assinantes precisarem de acesso à internet, verifique se o NAT/mascaramento está configurado para o intervalo de IP do assinante (por exemplo, `iptables -t nat -A POSTROUTING -s 10.45.0.0/16 -o <wan-interface> -j MASQUERADE`)

Rotas Obsoletas Após Falha

Sintomas: Rotas host para IPs de assinantes permanecem na tabela de roteamento após o OmniEPDG reiniciar ou após sessões terminarem anormalmente.

Causas possíveis:

- FSM falhou antes que a rota pudesse ser removida
- Processo OmniEPDG foi encerrado sem desligamento gracioso

Resolução:

1. Verifique `log/crash.log` para falhas de processo durante a finalização
2. Remova manualmente rotas obsoletas (`ip route del <subscriber-ip>/32 dev omniepdg0`)
3. Reiniciar o OmniEPDG recriará a interface `omniepdg0`, o que remove todas as rotas associadas

Problemas de Finalização de Sessão

Finalização Pendendo Durante a Desregistracão

Sintomas: A finalização da sessão não é concluída. FSM do UE preso em um estado `dereg_*` ou `wait_*`.

Causas possíveis:

- PGW não respondendo à Solicitação de Deletar Sessão

- Par Diameter não respondendo ao STR ou ASR
- Timeout em cascata não completando devido a múltiplos timeouts empilhados

Resolução:

1. Verifique os logs para mensagens de timeout no estado relevante
2. Verifique a conectividade do PGW e HSS
3. Após 10 segundos, o FSM deve expirar e prosseguir para a próxima etapa de finalização ou encerrar. Se não o fizer, verifique eventos inesperados registrados como `Unexpected call event`

Contextos PDP GTP-U Orfãos

Sintomas: Entradas de túnel GTP-U permanecem no kernel após as sessões terminarem. `ip link show gtp0` mostra que o dispositivo ainda tem contextos PDP ativos.

Causas possíveis:

- FSM terminou anormalmente antes de deletar o contexto PDP
- Falha durante a sequência de finalização

Resolução:

1. Verifique `log/crash.log` para falhas de processo durante a finalização
2. O callback `terminate/3` do FSM tenta limpar o contexto PDP. Se o FSM foi encerrado (por exemplo, reinício do supervisor), a limpeza pode ter sido pulada
3. Reiniciar o OmniEPDG recriará o socket GTP-U e limpará contextos obsoletos

Problemas de Processo e Sistema

Loops de Reinício do Supervisor

Sintomas: Processos do OmniEPDG reiniciam repetidamente. Os logs mostram mensagens de reinício do supervisor e relatórios de falha.

Causas possíveis:

- Erro de configuração persistente causando uma falha de manipulador na inicialização
- Dependência externa indisponível (por exemplo, biblioteca gen_socket não encontrada)
- Par Diameter enviando mensagens malformadas causando falhas de manipulador

Resolução:

1. Verifique `log/crash.log` para a causa raiz da falha
2. Verifique se o caminho `libdir` do `gen_socket` está correto e se os arquivos da biblioteca existem
3. Verifique se todos os parâmetros de configuração necessários estão presentes em `config/runtime.exs`
4. Procure mensagens Diameter malformadas no relatório de falha

Alto Uso de Memória

Sintomas: O consumo de memória da VM Erlang cresce ao longo do tempo.

Causas possíveis:

- Processos FSM do UE não sendo limpos após a finalização da sessão
- Acúmulo de mensagens de log nas caixas de correio
- Grande número de sessões concorrentes

Resolução:

1. Verifique o número de processos `epdg_ue_fsm` e `aaa_ue_fsm` em execução (esses devem corresponder à contagem de assinantes ativos)
2. Verifique se os FSMs estão terminando corretamente após a finalização da sessão (verifique mensagens de log `terminating`)
3. Revise as configurações de rotação de logs para garantir que os arquivos de log estejam sendo rotacionados

Webhooks do OmniEPDG

OmniEPDG pode enviar webhooks de saída para eventos do ciclo de vida da sessão do assinante. Quando um assinante se conecta ou desconecta, o OmniEPDG envia um `POST` HTTP com um corpo JSON para cada endpoint configurado. Use webhooks para alimentar um sistema de cobrança, um serviço de presença ou um pipeline de análise em tempo quase real.

Webhooks estão desativados por padrão. Consulte Configuração de Webhooks para os parâmetros de configuração.

Índice

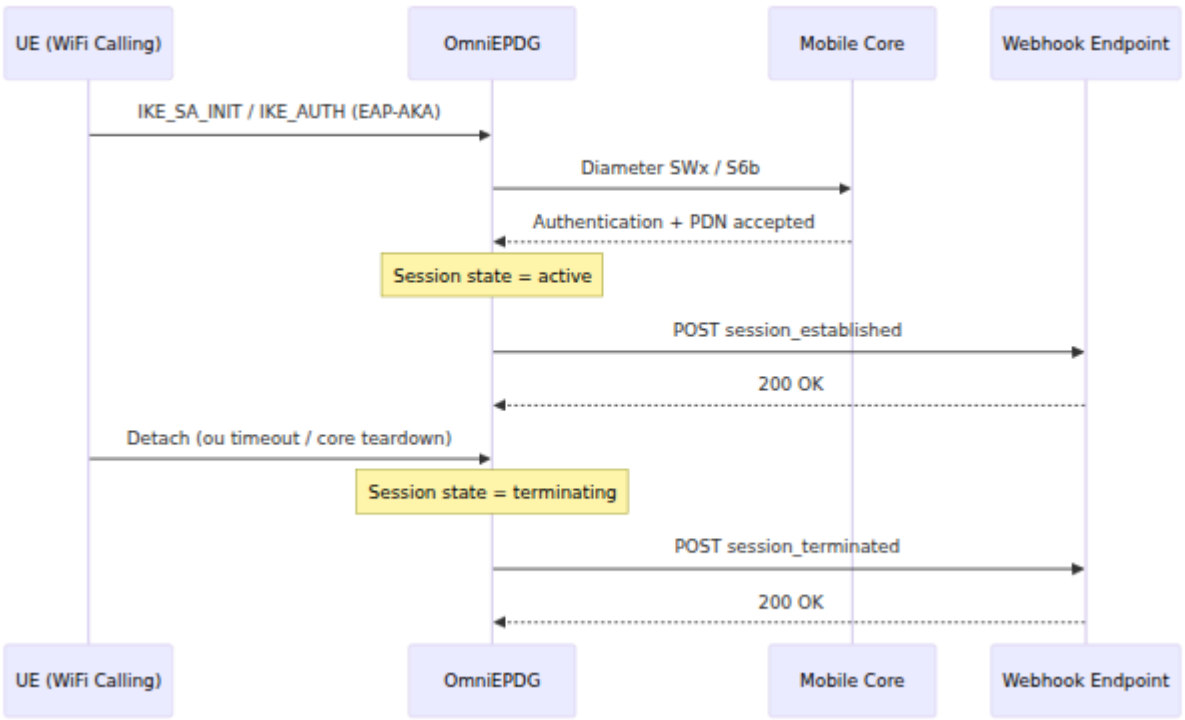
- Visão Geral
- Eventos
- Modelo de Entrega
- Esquema de Payload
- Exemplos de Payloads
- Requisitos do Receptor
- Solução de Problemas

Visão Geral

OmniEPDG rastreia cada sessão de assinante com uma máquina de estados. Duas transições produzem um webhook:

- A sessão atinge o estado `active` após uma conexão bem-sucedida.
- A sessão atinge o estado `terminating` após uma desconexão.

O diagrama a seguir mostra onde cada webhook é enviado no ciclo de vida da sessão.



Eventos

Evento	Gatilho	Descrição
`session_established`	Conexão bem-sucedida	OmniEPDG envia este evento quando o assinante se autentica e a conexão PDN está ativa. A sessão está pronta para transportar tráfego.
`session_terminated`	Desconexão	OmniEPDG envia este evento quando uma sessão estabelecida é encerrada. A causa é uma desconexão do UE, um timeout de inatividade ou um encerramento iniciado pelo núcleo.

OmniEPDG envia `session_terminated` apenas para sessões que atingiram o estado `active`. Uma conexão que falha antes que a conexão PDN seja estabelecida não produz um webhook.

Defina o parâmetro de configuração `events` para controlar quais eventos o OmniEPDG envia. Consulte Configuração de Webhooks.

Modelo de Entrega

OmniEPDG entrega webhooks com um modelo de fire-and-forget. Cada entrega é executada em uma tarefa de fundo supervisionada. A entrega nunca bloqueia ou atrasa a máquina de estados da sessão, e um endpoint lento ou indisponível não afeta o processamento da chamada.

Observe as seguintes propriedades de entrega:

- OmniEPDG envia um `POST` por endpoint configurado, por evento.
- OmniEPDG não tenta novamente uma entrega falhada. Uma entrega falhada é registrada e descartada.
- OmniEPDG não garante a ordem dos eventos entre os dois eventos. Projete o receptor para lidar com eventos pelo campo `timestamp`.
- OmniEPDG aceita qualquer resposta HTTP `2x` como sucesso. Ele registra um aviso para um erro de conexão ou uma resposta não `2xx`.
- OmniEPDG não valida o certificado TLS de um endpoint `https`. Use um caminho de rede confiável para o receptor.

Esquema de Payload

Cada corpo de webhook é um objeto JSON com os seguintes campos.

Campo	Tipo	Descrição
`event`	String	O nome do evento: `session_established` ou `session_terminated`.
`timestamp`	String	O horário do evento no formato ISO 8601 (UTC).
`session_id`	String	O identificador interno da sessão do OmniEPDG.
`imsi`	String	O IMSI do assinante.
`apn`	String ou null	O Nome do Ponto de Acesso para a conexão PDN.
`pdn_type`	String	O tipo de PDN: `ipv4`, `ipv6` ou `ipv4v6`.
`ue_ipv4`	String ou null	O endereço IPv4 alocado para o UE.
`ue_ipv6`	String ou null	O endereço IPv6 alocado para o UE.
`peer_ip`	String ou null	O endereço IP público do UE (o ponto de acesso WiFi).
`geoip`	Object ou null	A geolocalização de `peer_ip`. Consulte Objeto GeoIP. É `null` quando o endereço não pode ser localizado.
`handover`	Boolean	`true` se a sessão foi criada como uma transferência de LTE para WiFi.
`bytes_in`	Integer	A contagem de bytes de uplink para a sessão no momento do evento.
`bytes_out`	Integer	A contagem de bytes de downlink para a sessão no momento do evento.

Campo	Tipo	Descrição
`metadata`	Object	Um objeto com contexto adicional do evento. Está vazio para a maioria dos eventos.

Os campos `bytes_in` e `bytes_out` são `0` para um evento `session_established`, porque nenhum tráfego foi transmitido ainda.

Objeto GeoIP

OmniEPDG anota cada sessão com a geolocalização do IP público do UE no momento da conexão. A anotação usa o banco de dados DB-IP incluído, e isso acontece independentemente de o controle de acesso GeoIP estar habilitado. O campo `geoip` carrega essa anotação. Os campos `city`, `latitude` e `longitude` estão presentes apenas com um banco de dados de nível de cidade.

Campo	Tipo	Descrição
`country_code`	String ou null	O código do país ISO 3166-1 alpha-2 (por exemplo, `AU`).
`country_name`	String ou null	O nome do país.
`continent_code`	String ou null	O código do continente de duas letras (por exemplo, `OC`).
`city`	String ou null	O nome da cidade. Presente apenas com um banco de dados de nível de cidade.
`latitude`	Number ou null	A latitude aproximada. Presente apenas com um banco de dados de nível de cidade.
`longitude`	Number ou null	A longitude aproximada. Presente apenas com um banco de dados de nível de cidade.

Exemplos de Payloads

session_established

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

session_terminated

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

Requisitos do Receptor

Construa o receptor de webhook para atender a estes requisitos:

- Aceitar um `POST` HTTP com um corpo `Content-Type: application/json`.
- Retornar uma resposta `2xx` assim que você aceitar o evento. Não mantenha a conexão aberta para processamento posterior.
- Combinar eventos com sessões pelo campo `session_id`.
- Lidar com um evento duplicado. Uma condição de rede pode fazer com que o OmniEPDG envie o mesmo evento mais de uma vez.
- Ordenar eventos pelo campo `timestamp`, não pela ordem de chegada.

Solução de Problemas

Nenhum webhook chega

Sintomas: O receptor não recebe solicitações após uma conexão ou desconexão.

Causas possíveis:

- Webhooks estão desativados (`enabled: false`).
- O evento não está na lista de `events`.
- A URL do endpoint está errada ou não é acessível a partir do host OmniEPDG.
- Um firewall bloqueia a conexão de saída para o endpoint.

Resolução:

1. Confirme `enabled: true` na configuração do webhook.
2. Confirme que o nome do evento está na lista de `events`.
3. Confirme que a URL do endpoint está correta e acessível a partir do host OmniEPDG.
4. Verifique os logs do OmniEPDG para um aviso de entrega de webhook.

Apenas session_established chega, não session_terminated

Sintomas: O receptor recebe eventos de conexão, mas não eventos de desconexão.

Causas possíveis:

- `session_terminated` não está na lista de `events`.
- As sessões nunca atingiram o estado `active`, então nenhum evento de desconexão foi gerado.

Resolução:

1. Adicione `:session_terminated` à lista de `events`.
2. Confirme que as sessões completam uma conexão bem-sucedida antes de terminarem.

Entregas são registradas como falhadas

Sintomas: Os logs do OmniEPDG mostram um aviso de entrega de webhook.

Causas possíveis:

- O receptor retorna uma resposta não `2xx`.
- O receptor está lento ou indisponível.
- A URL do endpoint usa um host que não se resolve.

Resolução:

1. Confirme que o receptor retorna uma resposta `2xx`.
2. Confirme que o receptor responde rapidamente, pois o OmniEPDG não tenta novamente.
3. Confirme que o host do endpoint se resolve a partir do host OmniEPDG.