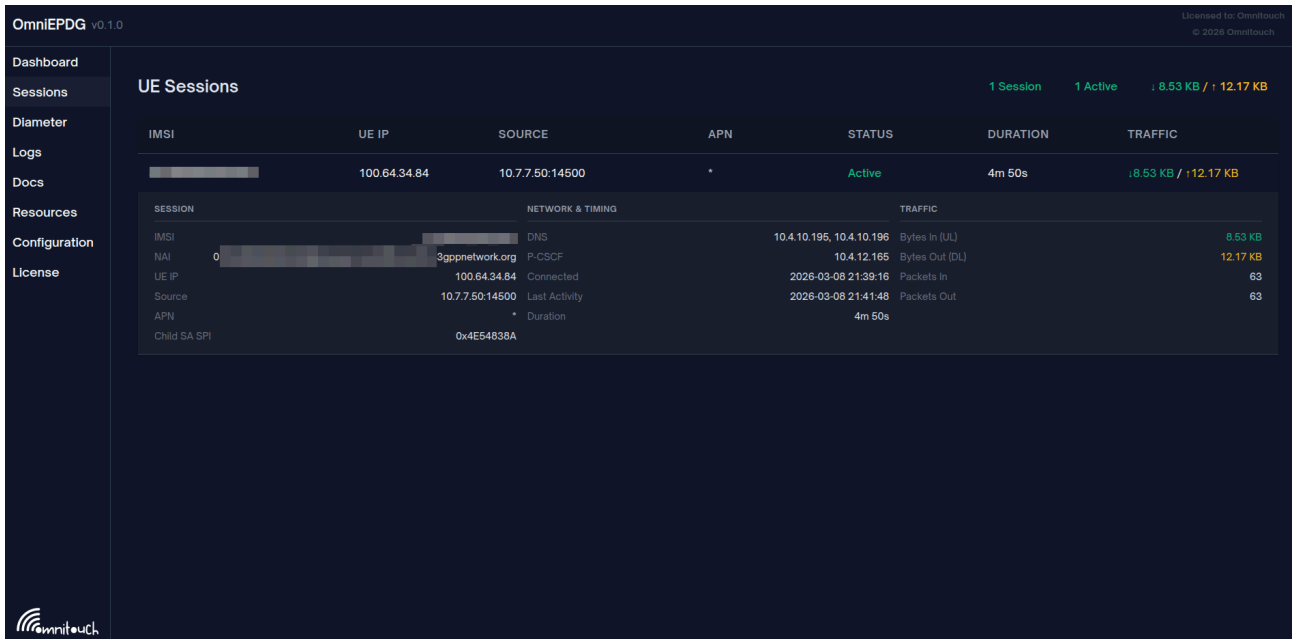


OmniEPDG

OmniEPDG (ePDG) WiFi (VoWiFi) EAP-AKA WiFi Diameter HSS GTP (PGW)



OmniEPDG

OmniEPDG

- **GTP** - GTPv2-C GTP-U PGW 3GPP
- **VPN** - IP Linux TUN PGW



- - UE
- - Diameter GTPv2-C GTP-U VPN
- - Diameter Web UI

GTP

OmniEPDG PGW GTPv2-C GTP-U Linux 3GPP EPC

UE → IPsec → OmniEPDG → GTPv2-C → GTP-U → PGW

HSS PGW

VPN

OmniEPDG IP Linux TUN tun_epdg PGW GTP Diameter SWx HSS

UE → IPsec → OmniEPDG → IP → TUN → Linux →

HSS PGW

skip_sar HSS HSS ePDG HSS

□□□□

□□	GTP □□	□□ VPN □□
3GPP □□	□	□□□□ skip_sar □□□□□□□□□□
□□ PGW	□	□
□□ HSS	□	□□□□□□□□
IP □□	□□ PGW	□□□□CIDR□
□□□□	GTP-U □□□□	Linux TUN + □□
HSS □□□□□□	□□PPR/PPA□	□
HSS □□	□□RTR/RTA□	□□□□ skip_sar□
PGW □□□□□□	□	□□□
□□□□	□	□
IPv6 / □□	□	□ IPv4

VPN

- **IP** - CIDR IPv4 IMSI
- **TUN** - Linux TUN tun_epdg UE
- **DNS** - PCO UE DNS
- **SAR** - HSS

- IP IMSI
- **GeoIP** - MaxMind GeoLite2
-
- **ESP** - RFC 4303 64

HSS (SWx Diameter)

- **(MAR/MAA)** - EAP-AKA
- **(SAR/SAA)** - APN
- **(PPR/PPA)** - HSS GTP
- **(RTR/RTA)** - HSS GTP

PGW GTP

S6b Diameter:

- **AA** (AAR/AAA) - PGW
- **(STR/STA)** - PGW
- **(RAR/RAA)** -
- **(ASR/ASA)** -

S2b GTPv2-C:

- TEID GTP
- GTP
- PGW

VPN

Component	IP	Details
OmniEPDG (TUN)	10.44.0.1	tun_epdg IP
UE IP	10.45.0.0/16	CIDR IP
HSS	10.74.0.21:3868	SWx Diameter

3GPP

Reference	Protocol/Component	Details
TS 29.273	EPS AAA (SWx, S6b, SWm)	ePDG Diameter
TS 29.274	GTPv2-C & GTP-U	S2b GTP
TS 33.402	3GPP	WiFi & EAP-AKA
TS 23.402	3GPP	ePDG
TS 23.003		NAI & IMSI
TS 29.229	Cx/Dx Diameter	SWx
RFC 6733	Diameter	Diameter
RFC 4187	EAP-AKA	IKEv2

1. [Python 3 入門](#) 入門から実践まで
2. [Python 3 入門](#) 入門から実践まで
3. [Python 3 入門](#) 入門から実践まで GeolIP 編
4. [Python 3 入門](#) 入門から実践まで Prometheus 編
5. [Python 3 入門](#) 入門から実践まで









おわりに

1. [Python 3 入門](#) 入門から実践まで
2. [Python 3 入門](#) 入門から実践まで
3. [Python 3 入門](#) 入門から実践まで
4. [Python 3 入門](#) 3GPP 入門から実践まで

OmniEPDG

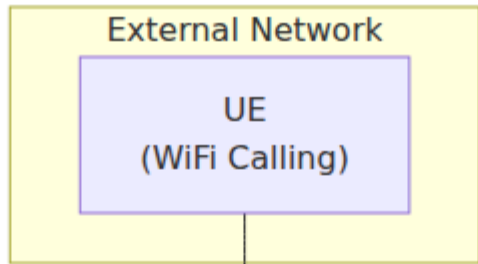
OmniEPDG  3GPP  ePDG WiFi 
WiFi  **GTP**  PGW  **VPN**  IP 

-  -  DNS 
-  - IKEv2DiameterVPN 
-  - 

-  - Diameter  Web 
-  - Prometheus 
-  - 

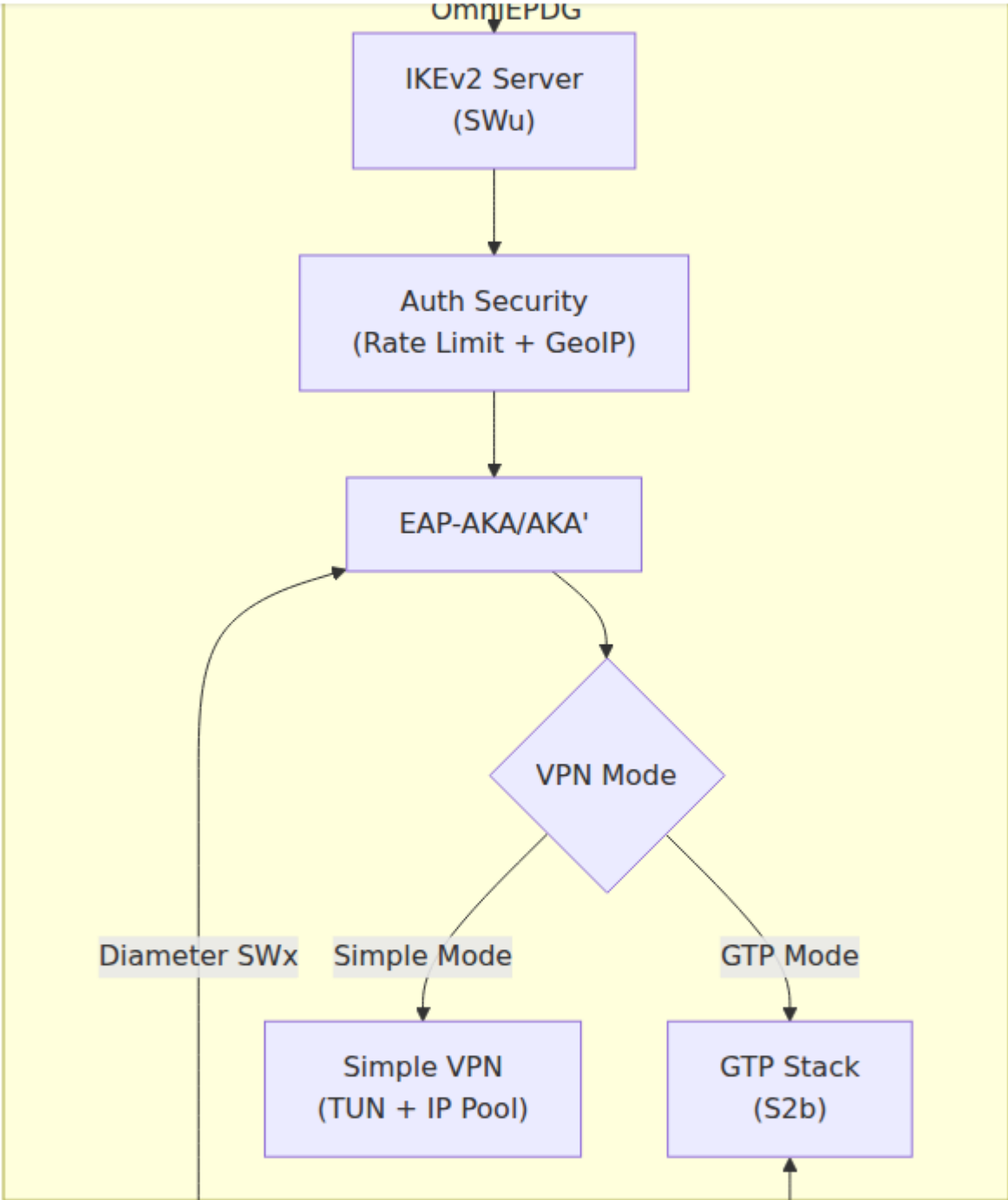
-  -  GeoIP 





IKEv2

ore OmniCore OmniCall OmniRAN OmniCharge Platform 5GC

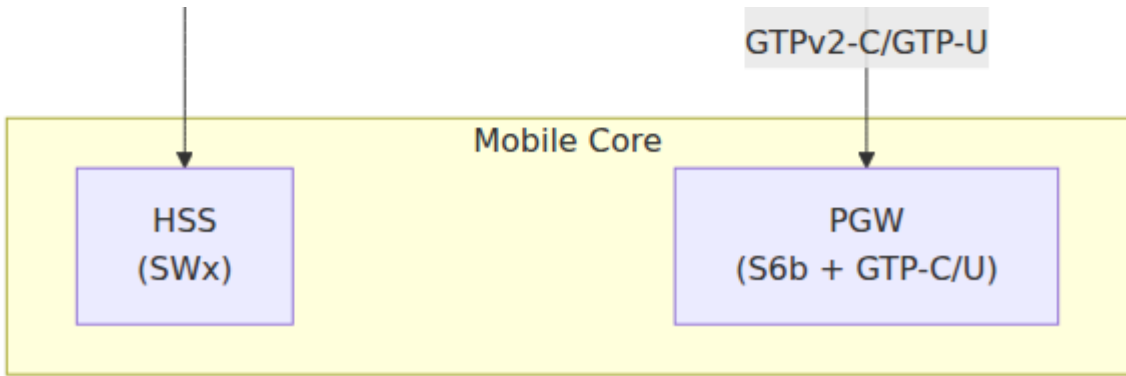


Diameter SWx

Simple Mode

GTP Mode

Diameter S6b



□□□□

OmniEPDG □□□□ vpn_mode □□□□□□□□□□□□□□

GTP □□

□□ PGW □□□□□ 3GPP □□□□□□□□□□□ GTP-U □□□□□□□□□□□□

□□□□□

- □□□□□□□□□□□□□□
- □□ PCRF/PCEF □□□□□□□□
- □□□□□□□□□□□□

□□□□

- □□ PGW □□□□□ Diameter S6b
- □□□□□□□□□□/□□/□□□□□□□ GTPv2-C
- □□□□□□□□□□ Linux □□ GTP-U □□

□□ VPN □□

□□ TUN □□□□□□□ IP □□□□□□□□□□□□□ OmniEPDG □□□□□□□□ PGW □□□□

□□□□□

- □ PGW □□□□□□
- □□□□□□
- □□□□□□□□

□□□□

□□□□□□ **VPN** □□□

```
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}  
    ]  
  }  
}
```

□□□□□□□□

```
config :omniepdg,  
  # □□□□□□□□□□□□□□□□  
  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,  
  
  # GeoIP □□□□□□□□  
  geoup_enabled: true,  
  geoup_mode: :whitelist,  
  geoup_countries: ["AU", "NZ"]
```

□□□□□□□□□□ □□□□

□□

□□□□

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

- □□□□□□
- Diameter □□□□□
- □□□□□
- □□□□

□□□□□□□□□□ □□□□ □□□

Prometheus □□

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

- □□□□□□/□□□
- □□□□□□□□
- Diameter □□□□
- □□□□□□□□□□ GeolIP □□□
- IP □□□□
- ESP □□□□□□

□□□□□□□□□□□□ □□□□

□□□□

□□□□□□□□□□

項目	説明	備考
ネットワーク	ネットワーク SWx MAR/MAA	ネットワーク
Diameter 認証	認証サーバー	Diameter 認証
GTP 認証	ネットワーク GTPv2-C 認証	GTP 認証
VPN 接続	VPN TUN 接続	VPN 接続
IPsec	IPsec	IPsec
GeoIP 認証	GeoIP 認証	GeoIP 認証

ネットワーク 認証

ネットワーク

項目	説明
ネットワーク	ネットワーク
ネットワーク	ネットワーク
ネットワーク	ネットワーク Web 接続
ネットワーク	Prometheus 監視
ネットワーク	ネットワーク DNS 接続
ネットワーク	ネットワーク GeoIP 認証
ネットワーク	ネットワーク

OmniEPDG

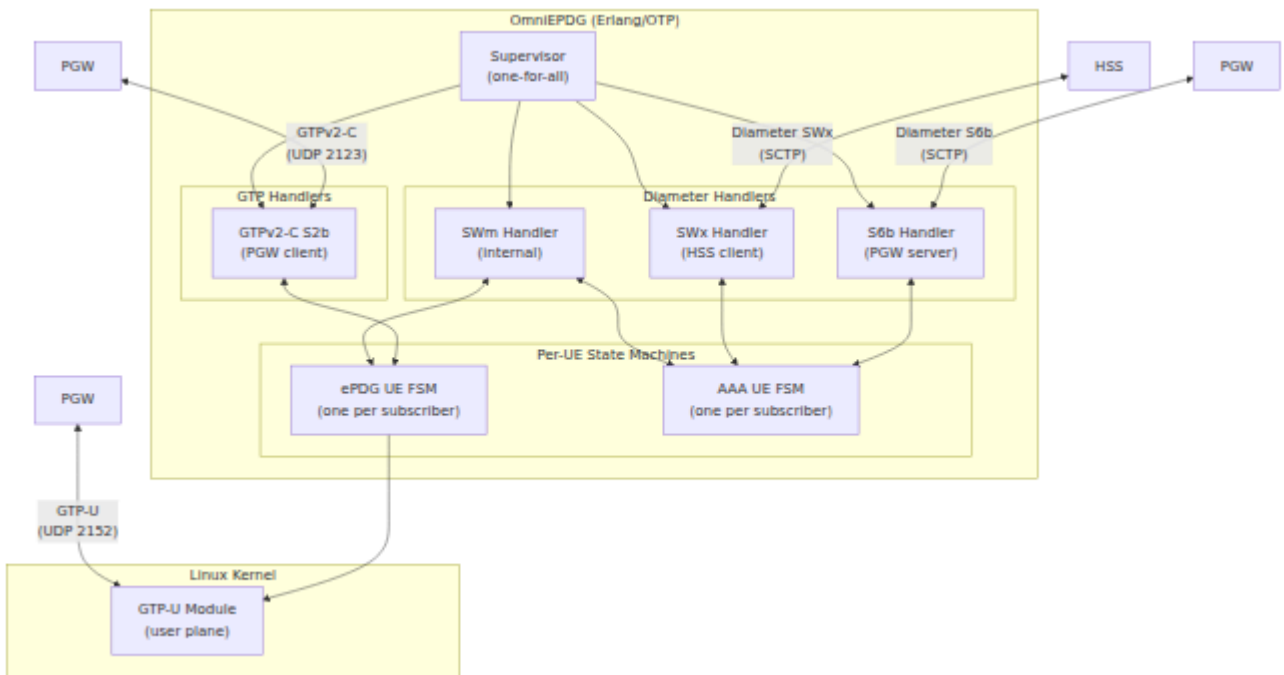
OmniEPDG 3GPP ePDG, VoWiFi, GTP, PGW, VPN, TUN

Architecture

OmniEPDG Erlang/OTP, 3GPP ePDG, WiFi, VoWiFi

GTP

GTP PGW GTPv2-C Linux GTP-U



VPN

VPN Linux TUN PGW GTP Diameter S6b GTPv2-C GTP-U VPN

이름	기능	설명
aaa_diameter_swx	Diameter SWx 모듈	HSS와 연결되는 Diameter SWx 모듈
aaa_diameter_swm	Diameter SWm 모듈	ePDG, AAA FSM, Diameter EAP 모듈
epdg_diameter_swm	SWm ePDG 모듈	ePDG 모듈과 SWm Diameter 모듈

GTP 모듈

이름	기능	설명
aaa_diameter_s6b	Diameter S6b 모듈	PGW와 연결되는 Diameter S6b 모듈
epdg_gtpc_s2b	GTPv2-C 모듈	PGW와 연결되는 GTPv2-C 모듈
gtp_u_kmod	GTP-U 모듈	Linux에서 실행되는 GTP-U PDP 모듈

VPN 모듈

이름	기능	설명
simple_vpn_supervisor	VPN 모듈	IP 주소 관리 모듈
simple_vpn_pool	IP 풀	ETS, CIDR, IPv4 풀
simple_vpn_route	루트	omniepdg@ TUN 모듈

이벤트

이벤트: IMSI, OmniEPDG

- **ePDG UE FSM** (`epdg_ue_fsm`) - ePDG 프로세스에서 프로세스별 GTP 프로세스 관리
- **AAA UE FSM** (`aaa_ue_fsm`) - AAA 프로세스와 HSS 및 Diameter SWx 프로세스와 PGW 및 S6b 프로세스

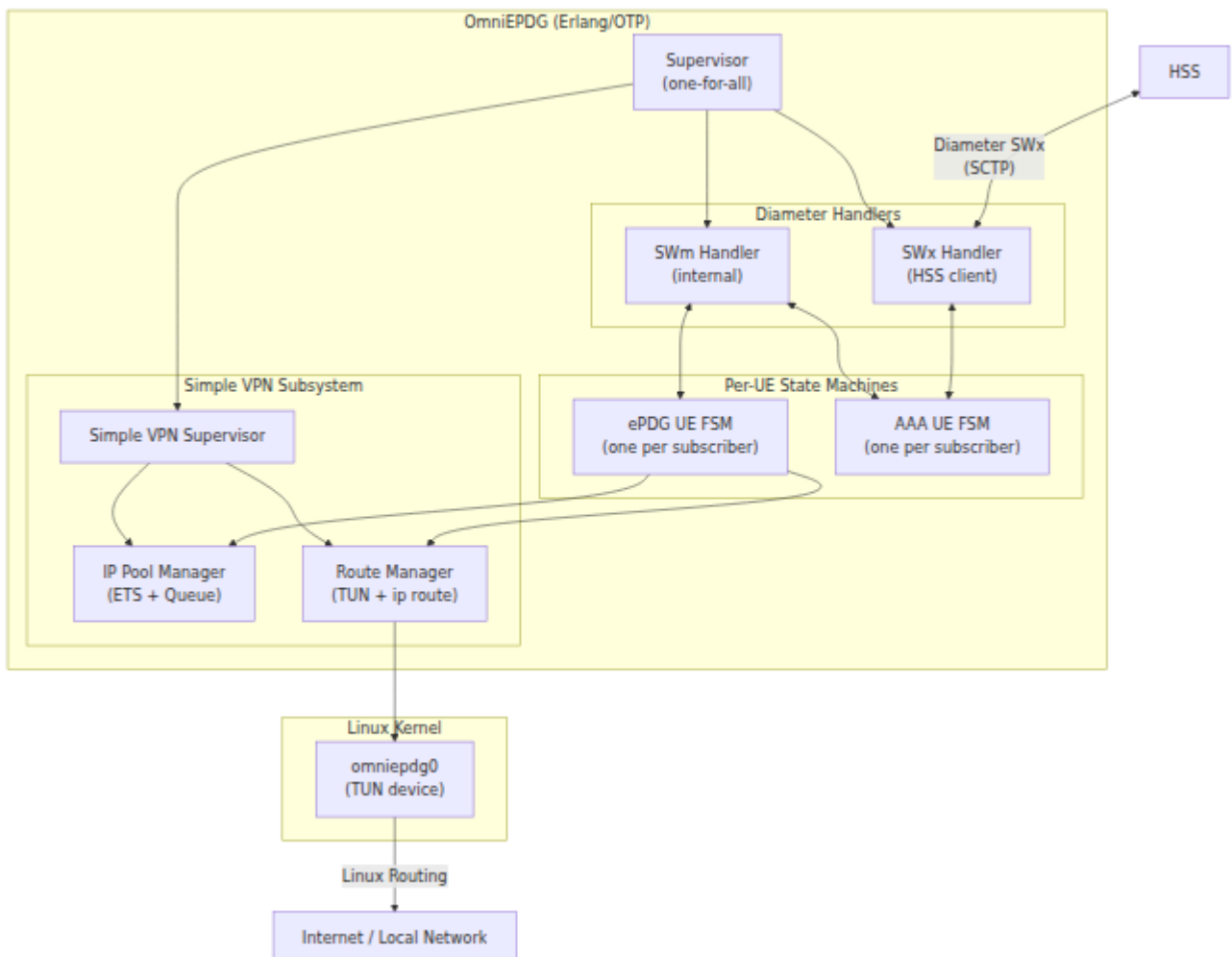
이러한 FSM 프로세스는 Erlang `gen_statem` 프로세스를 사용하여 구현됩니다.

ePDG UE FSM 프로세스

ePDG UE FSM 프로세스는 프로세스별 FSM 프로세스인 `authenticated` 프로세스를 포함하고 있습니다.

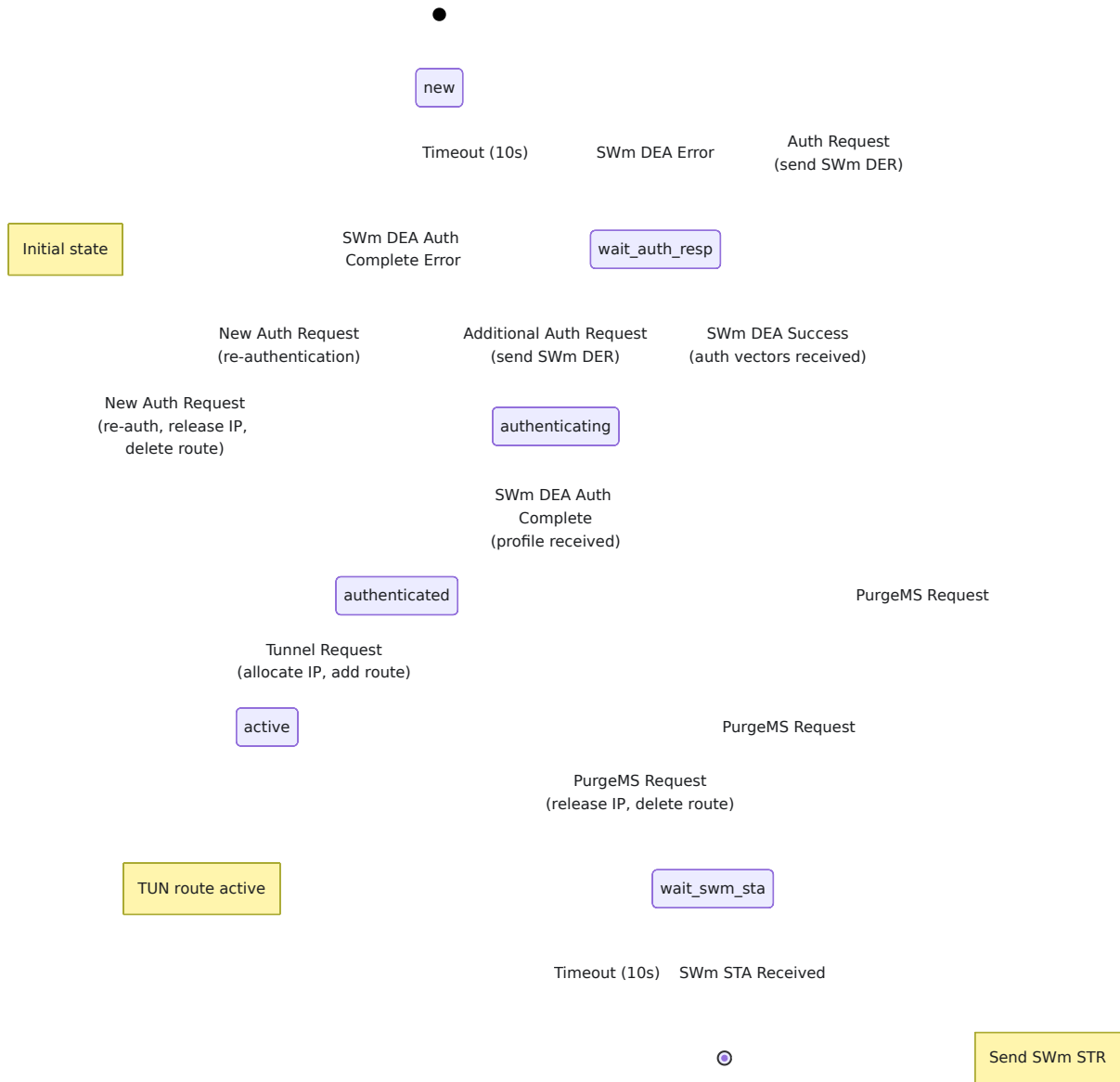
GTP 프로세스 FSM

이 GTP 프로세스는 GTPv2-C 프로세스와 PGW 프로세스와 GTPv2-C 프로세스와 PGW 프로세스와 HSS 프로세스와



VPN FSM

VPN FSM authenticated FSM GTPv2-C IP TUN active GTP
 wait_create_session_resp wait_delete_session_resp
 dereg_pgw_wait_cancel dereg_net_wait_s2b_delete

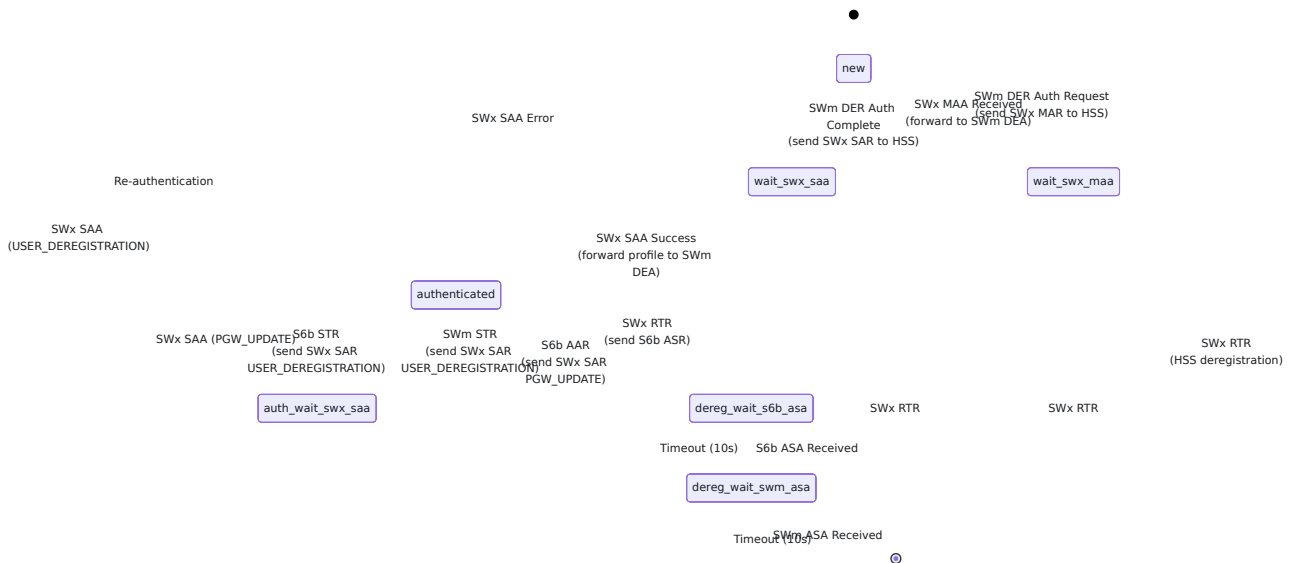


ePDG UE FSM

State	Event	Action	Result
new		Initial state	Initial state
wait_auth_resp		SWm DER received	SWm DEA received
authenticating		EAP exchange	EAP exchange
authenticated		Authentication successful	Authentication successful
wait_create_session_resp	GTP	PGW GTPv2-C create request	PGW GTPv2-C create response
active		Normal operation	Normal operation
wait_delete_session_resp	GTP	PGW GTPv2-C delete request	PGW GTPv2-C delete response
wait_swm_sta		SWm STA received	AAA SWm STA
dereg_pgw_wait_cancel	GTP	PGW deregistration request	PGW deregistration response
dereg_net_wait_cancel	GTP	HSS deregistration request	HSS deregistration response
dereg_net_wait_s2b_delete	GTP	PGW S2b delete request	PGW S2b delete response

AAA UE FSM

AAA UE FSM HSS SWx PGW S6b Diameter

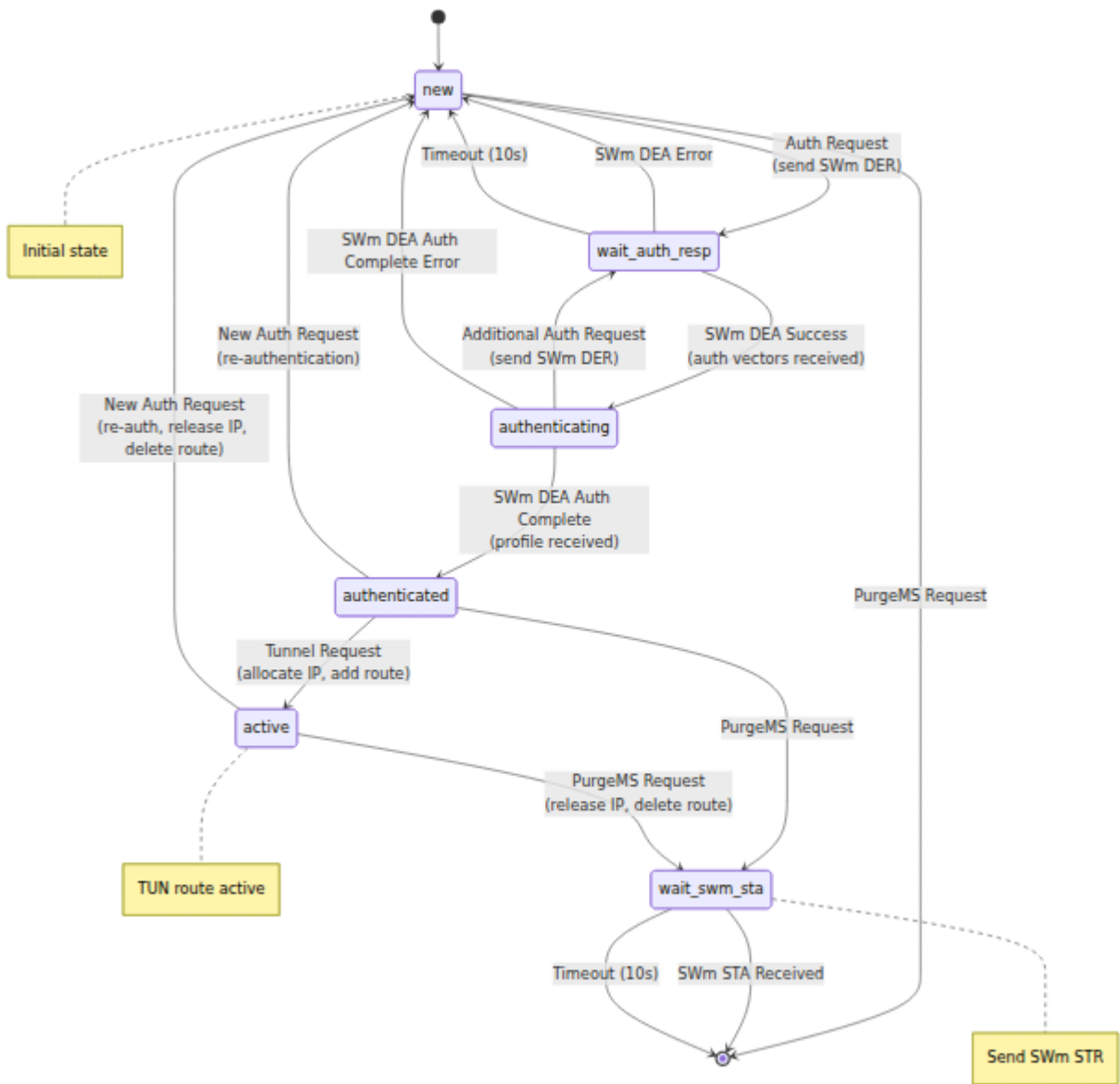


AAA UE FSM

State	Transitions	Network Elements
new	AAA	Diameter
wait_swx_maa	SWx MAR, HSS, EAP-AKA	HSS, SWx, MAA
wait_swx_saa	SWx SAR, HSS	HSS, SWx, SAA
authenticated	ePDG, PGW	
auth_wait_swx_saa	PGW, SWx SAR	HSS, SWx, SAA
dereg_net_wait_s6b_asa	HSS, PGW, S6b, ASR	PGW, S6b, ASA
dereg_net_wait_swm_asa	S6b, SWm, ASR, ePDG	ePDG, SWm, ASA

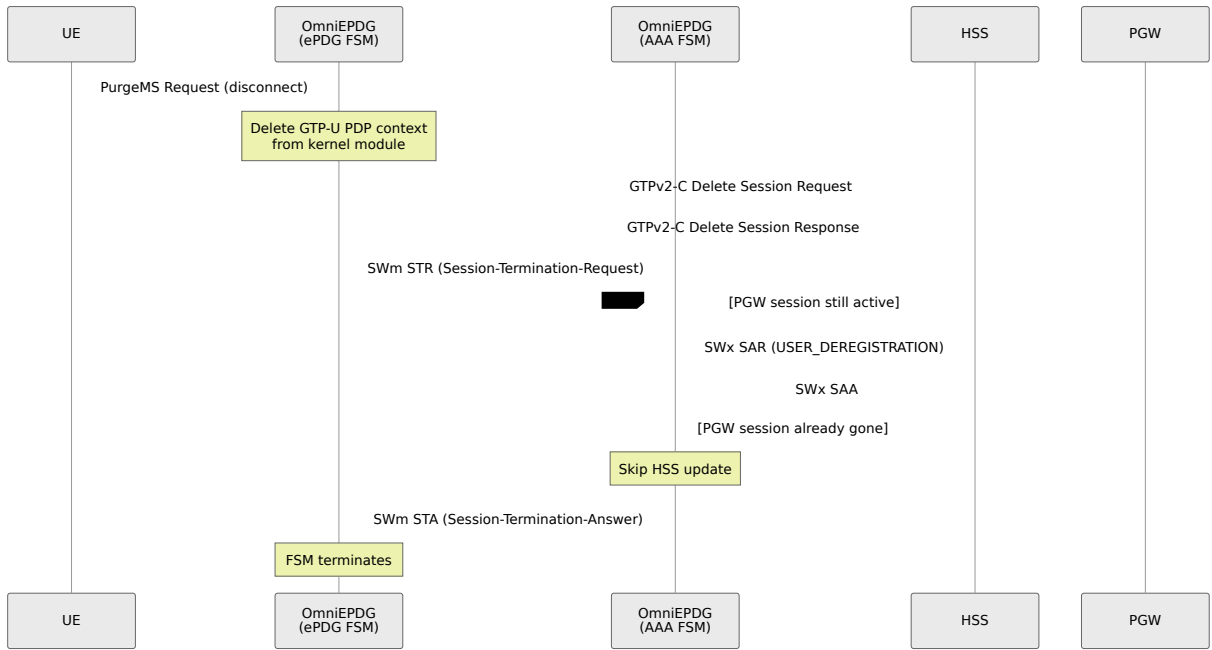
GTP

EAP-AKA GTP



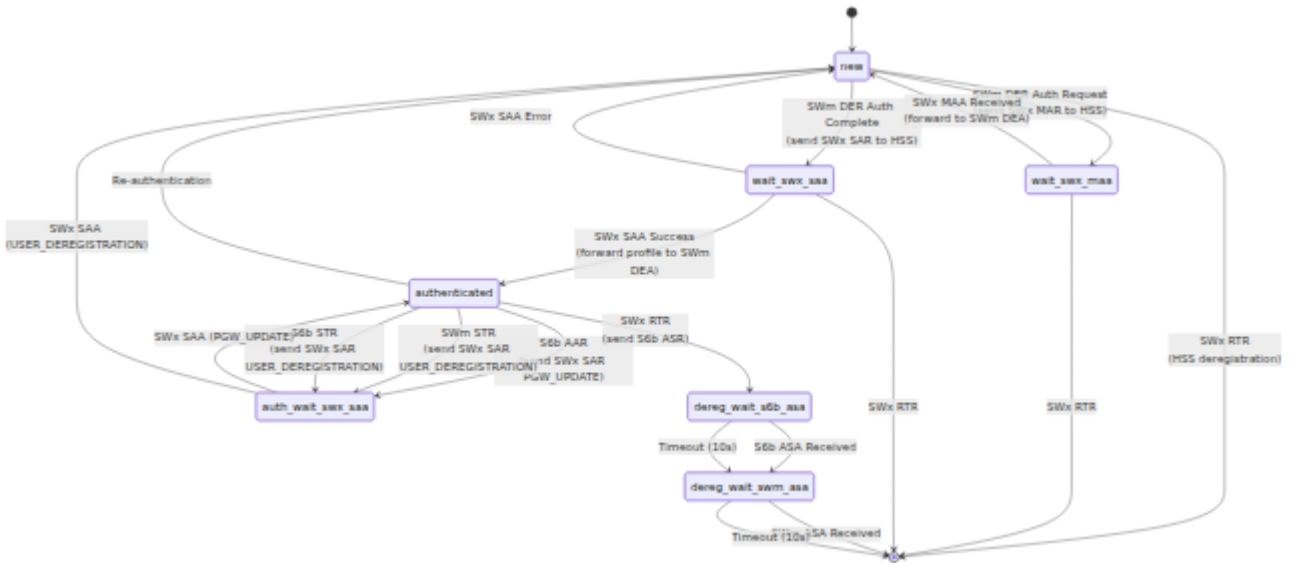
GTP 认证鉴权流程

认证鉴权流程 WiFi 认证鉴权流程



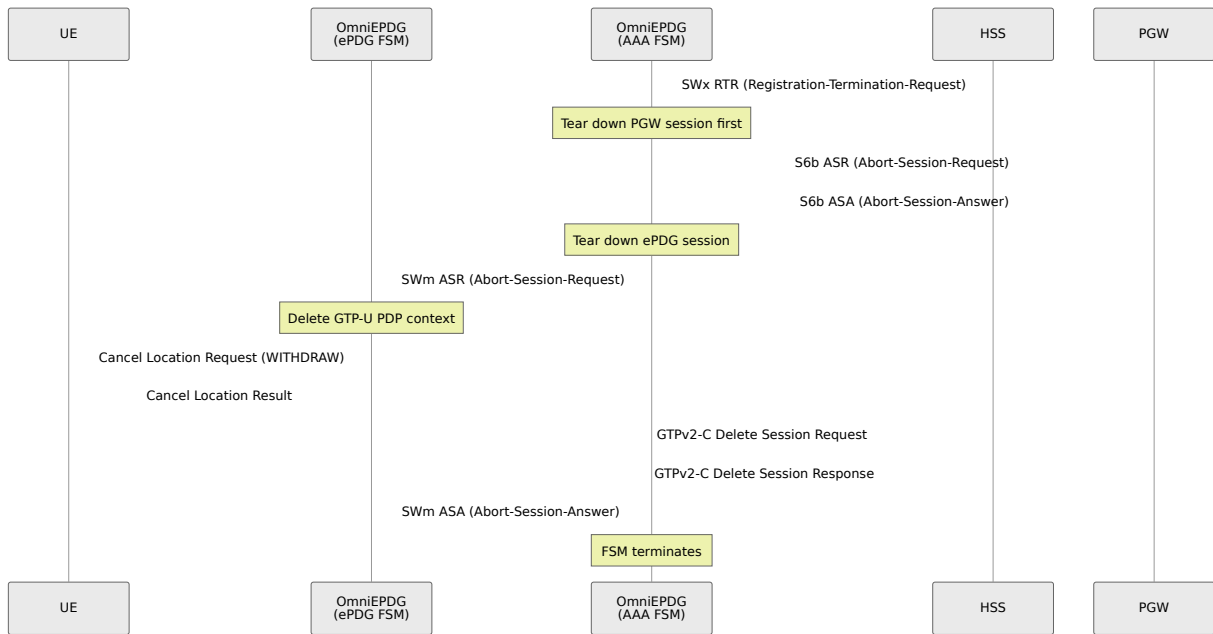
GTP PGW

PGW



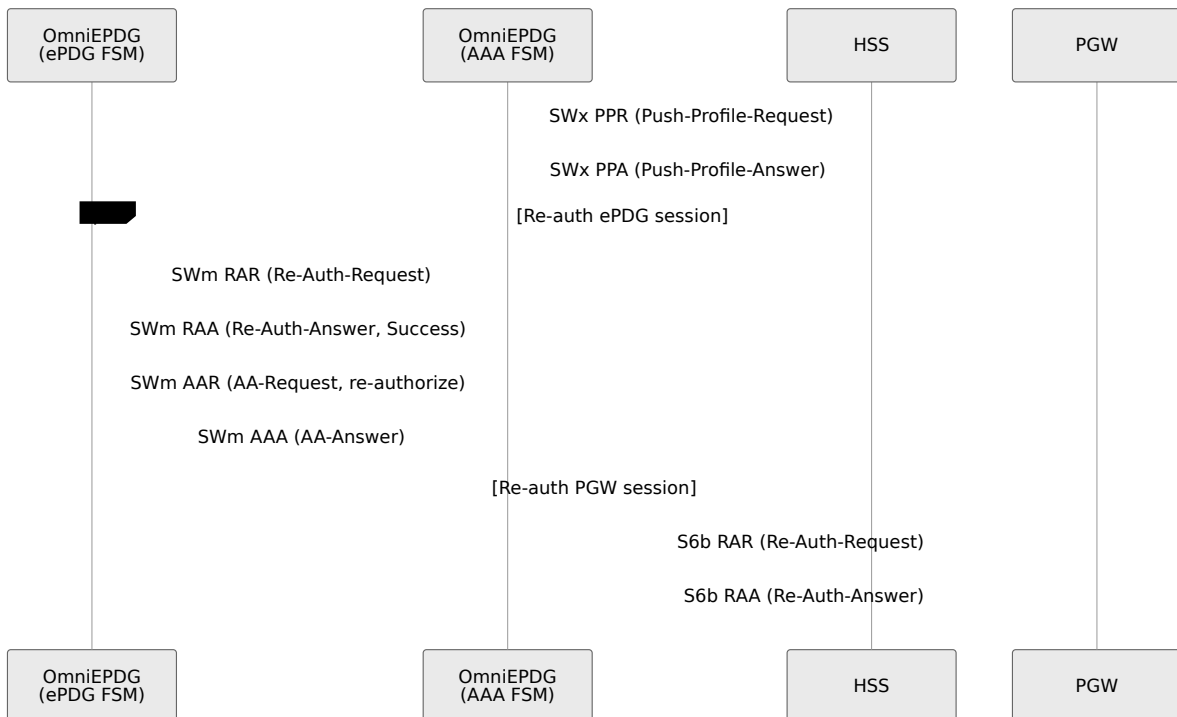
GTP HSS

HSS



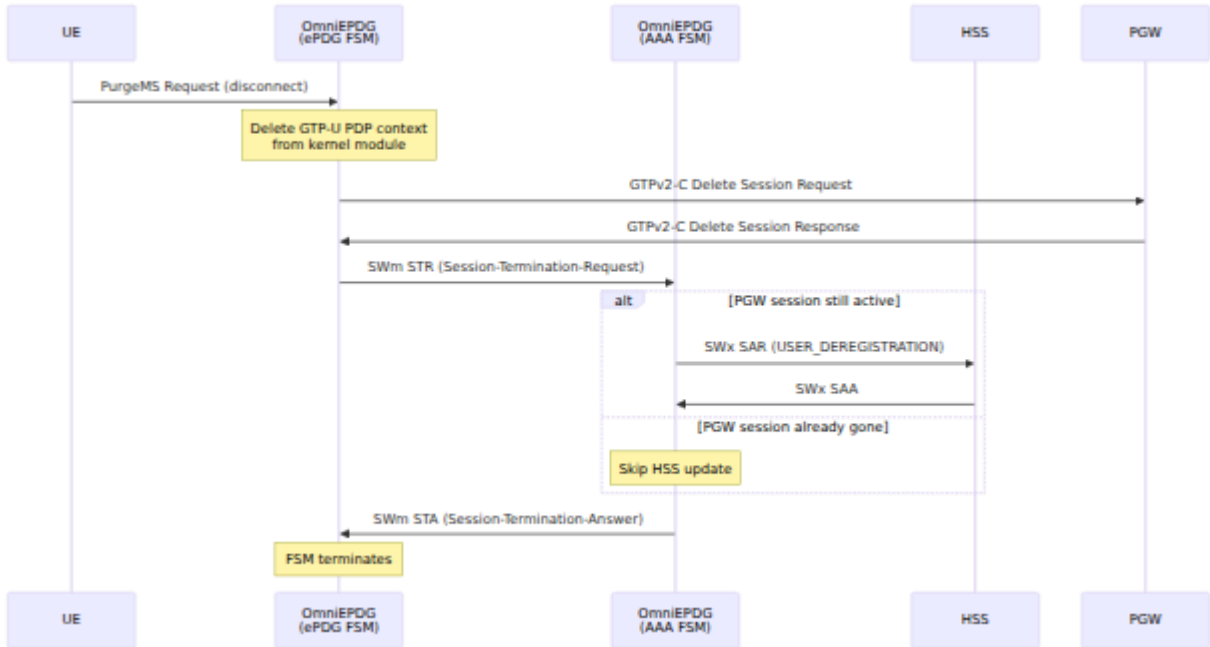
GTP HSS

HSS OmniEPDG 3GPP TS 29.273 8.1.2.3.3 ePDG
 SWm PGW S6b



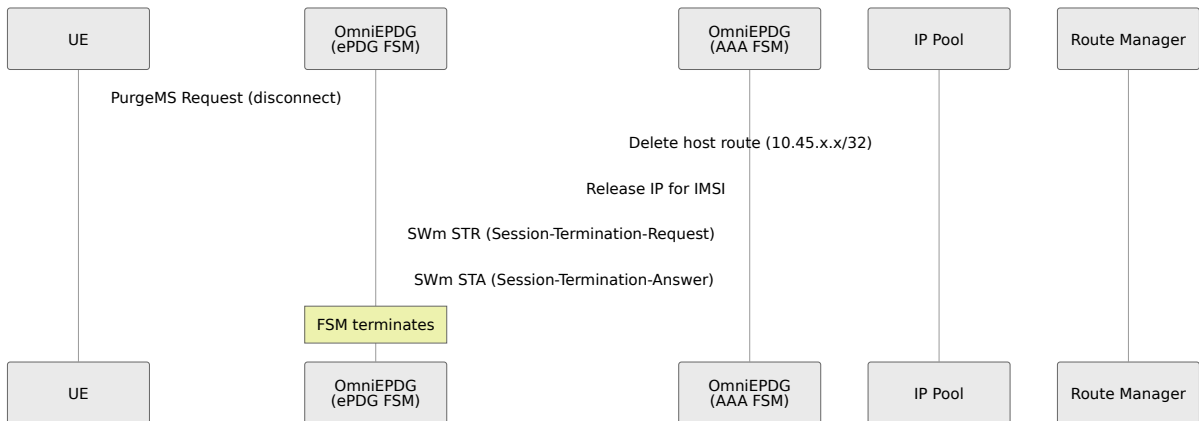
VPN EAP-AKA

VPN EAP-AKA ePDG FSM IP TUN PGW skip_sar HSS SAR/SAA



VPN FSM IP

VPN FSM IP



3GPP 错误码列表

错误码	描述	来源	版本
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	HSS 数据不可用	3GPP TS 29.273
5001	DIAMETER_ERROR_USER_UNKNOWN	未知 IMSI 用户 HSS 数据不可用	3GPP TS 29.273
5002	DIAMETER_UNKNOWN_SESSION_ID	未知会话 ID STR/AAR	RFC 673
5003	DIAMETER_AUTHORIZATION_REJECTED	授权被拒绝	3GPP TS 29.273
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	漫游不被允许	3GPP TS 29.273
5005	DIAMETER_MISSING_AVP	缺少 AVP	RFC 673
5012	DIAMETER_UNABLE_TO_COMPLY	无法遵守	RFC 673
5420	DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION	未知 EPS 订阅	3GPP TS 29.273
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	RAT 不被允许	3GPP TS 29.273

코드	이름	설명	참고
5422	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	IMEI 값이 없음	3GPP TS 29.274

GTPv2-C 메시지 목록 GTP 메시지

OmniEPDG 및 PGW-CP/CP-IPsec 터널을 위한 GTPv2-C 메시지 목록은 1-15 및 16-63 메시지와 64 메시지인 3GPP TS 29.274 8.4에 나열되어 있습니다.

메시지

번호	이름	설명
16	Request Accepted	수용됨
17	Request Accepted Partially	부분적으로 수용됨
18	New PDN Type (Network Preference)	네트워크 선호 PDN 유형
19	New PDN Type (Single Address Bearer)	단일 주소 Bearer PDN 유형

エラーコード

エラーコード	エラーメッセージ	原因
64	Context Not Found	PGW コンテキストが見つからない
73	No Resources Available	PGW リソース不足
78	Missing or Unknown APN	APN が PGW に登録されていない
82	Denied in RAT	ネットワークアクセスが拒否された
84	All Dynamic Addresses Occupied	PGW の動的 IP アドレスがすべて占有されている
92	User Authentication Failed	PGW のユーザー認証が失敗した
93	APN Access Denied	APN にアクセスが拒否された
96	IMSI/IMEI Not Known	IMSI/IMEI が不明である
109	Invalid Peer	不正なピアである
113	APN Congestion	APN が混雑している
120	GTP-C Entity Congestion	PGW の GTP-C エンティティが混雑している

NAI

OmniEPDG は 3GPP TS 23.003 19 に定義されている NAI を使用する。

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

設定

NAI は 3GPP TS 23.003 に定義された EAP を使用する。

Priority	Protocol	Authentication Method
0	EAP-AKA	AKA with WiFi authentication
6	EAP-AKA'	AKA without WiFi authentication

OmniEPDG authentication method is set to 0 EAP-AKA with WiFi authentication

OmniEPDG authentication method is set to @ IMSI over IMSI authentication

Priority

OmniEPDG uses 3GPP TS 33.402 and RFC 7296 IKEv2 authentication

IKEv2 Authentication

Algorithm	ID	Key Length	Support Status	Reference
AES-CBC	12	128, 192, 256 bits	Supported (default: 256)	RFC 3602
AES-GCM-16	20	128, 192, 256 bits	Supported	RFC 5282
AES-GCM-12	19	128, 192, 256 bits	Supported	RFC 5282
AES-GCM-8	18	128, 192, 256 bits	Supported	RFC 5282
3DES	3	192 bits	Supported (legacy)	RFC 2451

IKEv2 HMAC

HMAC	ID	Key Length	ICV Length	Support	Reference
HMAC-SHA2-256-128	12	256 bits	128 bits	Supported (default)	RFC 4868
HMAC-SHA2-384-192	13	384 bits	192 bits	Supported	RFC 4868
HMAC-SHA2-512-256	14	512 bits	256 bits	Supported	RFC 4868
HMAC-SHA1-96	2	160 bits	96 bits	Supported (legacy)	RFC 2404
HMAC-MD5-96	1	128 bits	96 bits	Supported (legacy)	RFC 2403

IKEv2 PRF HMAC

PRF-HMAC	ID	Key Length	Support	Reference
PRF-HMAC-SHA2-256	5	256 bits	Supported (default)	RFC 4868
PRF-HMAC-SHA2-384	6	384 bits	Supported	RFC 4868
PRF-HMAC-SHA2-512	7	512 bits	Supported	RFC 4868
PRF-HMAC-SHA1	2	160 bits	Supported (legacy)	RFC 2104
PRF-HMAC-MD5	1	128 bits	Supported (legacy)	RFC 2104

IKEv2 Diffie-Hellman

	ID			
MODP-2048	14	2048 bits	Supported (default)	RFC 3526
MODP-1024	2	1024 bits	Supported (legacy)	RFC 2409
MODP-1536	5	1536 bits	Supported	RFC 3526
MODP-3072	15	3072 bits	Supported	RFC 3526
MODP-4096	16	4096 bits	Supported	RFC 3526
ECP-256	19	256 bits	Supported	RFC 5903
ECP-384	20	384 bits	Supported	RFC 5903
ECP-521	21	521 bits	Supported	RFC 5903
Curve25519	31	256 bits	Supported	RFC 8031
Curve448	32	448 bits	Supported	RFC 8031

ESP SA

ESP IKEv2 CREATE_CHILD_SA

ESP

- AES-CBC-256 32 16 IV
- HMAC-SHA2-256-128 32 16 ICV

EAP-AKA □□□□

□□	□□	□□
MK □□	SHA-1	RFC 4187 □ 7 □
PRF+ □□□□	FIPS 186-2 PRF□SHA-1□	RFC 4187 □□ D
AT_MAC	HMAC-SHA1-128	RFC 4187 □ 10.15 □
Milenage□f1-f5□	AES-128	3GPP TS 35.206

EAP-AKA' □□□□

□□	□□	□□
CK'/IK' □□	HMAC-SHA-256	RFC 5448 □ 3.3 □
MK □□	SHA-256	RFC 5448 □ 3.4 □
AT_MAC	HMAC-SHA256-128	RFC 5448 □ 3.1 □

3GPP □□□

OmniEPDG □□□ 3GPP TS 33.402 □ 8 □□□□□□□□□□□□□□

項目	仕様	対応状況
IKEv2 暗号化	AES-CBC-128	✓ 対応
IKEv2 認証	HMAC-SHA2-256-128	✓ 対応
IKEv2 PRF	PRF-HMAC-SHA-256	✓ 対応
IKEv2 DH	14 MODP-2048	✓ 対応
ESP 暗号化	AES-CBC-128/256	✓ 対応
ESP 認証	HMAC-SHA2-256-128	✓ 対応
EAP-AKA	RFC 4187	✓ 対応
EAP-AKA'	RFC 5448	✓ 対応

PDP 設定 GTP 設定

OmniEPDG 3GPP TS 29.274 8.14 PDP 設定 VPN 設定
IPv4 設定

項目	仕様	GTPv2-C PAA 設定
IPv4	IPv4	4 IPv4
IPv6	IPv6	1 + 16 IPv6
IPv4v6		1 + 16 IPv6 + 4 IPv4

OmniEPDG 部署

OmniEPDG 通过 `config/runtime.exe` 部署 - 部署

部署

部署

- IKEv2 部署
- 部署
- VPN 部署
- VPN 部署
- Diameter 部署
- 部署
- 部署
- Prometheus 部署
- 部署
- 部署

□□□□

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

  # VPN □□: :simple (□□□□) □ :gtp (□□ GTP-C □ PGW)
  vpn_mode: :simple,

  # □□ VPN □□□□
  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"]
  ]

# □□□□□□
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"}
  ]

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

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

# ██████████ (runtime.exs)
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

IKEv2 ████████

IKEv2 ████████ UEs █ OmniEPDG █████ SWu ████████ IPsec ████████ EAP-AKA █████

Name	Type	Value	Default
listen_ip	string		{0, 0, 0, 0}
port_500	int		500
port_4500	int		4500
cert_file	string		/etc/omniepdg/certs/epdg.crt

項目	種別	単位	値
key_file	文字列		/etc/omniepdg/certs/epdg.key
session_inactivity_timeout_ms	整数	ms	300000

設定例

OmniEPDG の設定例を示します。

設定例

```

config :omniepdg,
  # IP アドレス
  auth_rate_limit_per_ip: 10,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 300_000,

  # IMSI
  auth_rate_limit_per_imsi: 5,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 600_000

```

項目	単位	範囲	初期値	説明
auth_rate_limit_per_ip	件/分	0-255	10	IPアドレスごとに認証リクエストの最大数を制限する
auth_rate_limit_ip_window_ms	ms	0-65535	60000	IPアドレスごとの認証リクエスト制限のウィンドウ時間
auth_rate_limit_ip_block_ms	ms	0-65535	300000	IPアドレスごとの認証リクエスト制限を超過した場合のブロック時間 (5分)
auth_rate_limit_per_imsi	件/分	0-255	5	IMSIごとに認証リクエストの最大数を制限する
auth_rate_limit_imsi_window_ms	ms	0-65535	60000	IMSIごとの認証リクエスト制限のウィンドウ時間
auth_rate_limit_imsi_block_ms	ms	0-65535	600000	IMSIごとの認証リクエスト制限を超過した場合のブロック時間 (10分)

GeoIP 設定

```

config :omniepdg,
  geoup_enabled: false,
  geoup_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",
  geoup_mode: :whitelist,
  geoup_countries: ["AU", "NZ"],
  geoup_allow_unknown: false,
  geoup_fail_open: true

```

項目	型	デフォルト	説明
<code>geoup_enabled</code>	ブール値	<code>false</code>	GeoIP MaxMind GeoLite2 を有効にするかどうか
<code>geoup_database_path</code>	文字列	<code>"/etc/omniepdg/GeoLite2-Country.mmdb"</code>	MaxMind GeoLite2 データベースの MMDB ファイルのパス
<code>geoup_mode</code>	文字列	<code>:whitelist</code>	<code>:whitelist</code> モード <code>:blacklist</code> モード
<code>geoup_countries</code>	文字列	<code>[]</code>	ISO 3166-1 alpha-2 コードの リスト <code>["AU", "NZ", "US"]</code>
<code>geoup_allow_unknown</code>	ブール値	未知	未知の IP に対して <code>false</code> または <code>true</code>
<code>geoup_fail_open</code>	ブール値	<code>true</code>	GeoIP データベース が利用 できない

VPN 配置

名称	类型	模式	配置	备注
vpn_mode	简单	简单	EPDG_VPN_MODE	配置为 simple 模式，TUN 隧道 IP 地址为 gtp 模式，支持 GTPv2-C/GTP-U 协议，PGW 接口支持 IPv4 和 IPv6 地址。

配置 VPN 配置

simple_vpn 配置用于配置 VPN 隧道 IP 地址、DNS、OmniEPDG 隧道 IPv4 和 IPv6 地址。

```

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
  ]

```

名称	类型	范围	配置值	描述
pool_ipv4	IP地址池	IPv4	"10.45.0.0/16"	CIDR 地址池 IPv4 地址池 用于 IPv4
pool_ipv6	IP地址池	IPv6	"2001:db8::/32"	CIDR 地址池 IPv6 地址池
dns_servers_ipv4	DNS服务器	IPv4	["8.8.8.8", "8.8.4.4"]	PCO 配置 UEs 使用 IPv4 DNS 服务器
dns_servers_ipv6	DNS服务器	IPv6	["2001:4860:4860::8888", "2001:4860:4860::8844"]	PCO 配置 UEs 使用 IPv6 DNS 服务器
p_cscf_ipv4	IMS P-CSCF	IPv4	[]	VoWiFi 配置 IPv4 P-CSCF/IMS UEs 使用 IMS
p_cscf_ipv6	IMS P-CSCF	IPv6	[]	VoWiFi 配置 IPv6 P-CSCF/IMS
mtu	MTU		1400	MTU 配置 用于 VoWiFi

項目	項目	項目	項目	項目
nat_enabled	項目	項目	true	項目 NAT項目 true 項目 項目

Diameter 項目

Diameter 項目 SWx項目HSS項目 S6b項目PGW項目項目 diameter_enabled 項目 true 項目
OmniEPDG 項目 Diameter 項目項目項目項目項目

```

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}
    ]
  }

```

項目

項目	型	値	説明	参照
service_name	文字列	:omniepdg		-
listen_ip	文字列	"0.0.0.0"		DIA_LISTEN_IP
listen_port	整数	3868		DIA_LISTEN_PORT
host	文字列	"epdg"		DIA_HOSTNAME
realm	文字列	"epc.mnc001.mcc001.3gppnetwork.org"		DIA_REALM

Field	Value	Unit	Description	Default
product_name	"OmniEPDG"			-
vendor_id	10415			-

Peers

peers Diameter HSS

Field	Value	Unit	Default	Parameter	Description
host			-	HSS_HOST	Diameter Origin-Host
ip			-	HSS_IP	IP TCP/SCTP
port			3868	HSS_PORT	Diameter
transport			:tcp	-	:tcp :sctp

ID

名前	ID	グループ ID	接続	規格
SWx	16777265	10415	ePDG ↔ HSS	3GPP TS 29.273
S6b	16777272	10415	AAA ↔ PGW	3GPP TS 29.273

ライセンスクライアント

ライセンスクライアント OmniEPDG の設定

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

名前	タイプ	値	説明
server_url	文字列	-	LICENSE_SERVER_URL API の URL
product	文字列	"omniepdg"	製品名

Web コンソール

Web コンソールの設定

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

Port	Protocol	Direction	Port	Parameter	Notes
port	HTTP	Out	4000	CONTROL_PANEL_PORT	Web UI HTTP

Prometheus

OmniEPDG HTTP Prometheus

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

Port	Protocol	Direction	Port	Parameter	Notes
port	HTTP	Out	9568	PROMETHEUS_PORT	Prometheus /metrics HTTP

Metrics

Available Metrics

- epdg_ikev2_session_initiated_count - IKE_SA_INIT
- epdg_ikev2_session_established_count - IKE SA
- epdg_ikev2_session_failed_count - IKE SA
- epdg_eap_identity_count - EAP
- epdg_eap_aka_challenge_count - EAP-AKA
- epdg_eap_aka_success_count - EAP-AKA
- epdg_eap_aka_failure_count - EAP-AKA
- epdg_eap_aka_sync_failure_count - EAP-AKA SQN
- epdg_diameter_swx_mar_count - Diameter
- epdg_diameter_swx_sar_count - Diameter
- epdg_diameter_s6b_aar_count - Diameter AA

- `epdg_diameter_s6b_str_count` - 字符串
- `epdg_session_created_count` - 创建会话数 `vpn_mode`
- `epdg_session_terminated_count` - 终止会话数
- `epdg_esp_packets_in_count` - ESP 包入
- `epdg_esp_packets_out_count` - ESP 包出
- `epdg_ip_allocated_count` - IP 地址分配数
- `epdg_ip_released_count` - IP 地址释放数

计数器 5

- `epdg_sessions_active_count` - 活跃会话数
- `epdg_sessions_by_state_count` - FSM 状态数
- `epdg_ip_pool_allocated_count` - IP 池分配数
- `epdg_ip_pool_available_count` - IP 池可用数
- `epdg_ip_pool_utilization_ratio` - IP 池利用率 0.0-1.0
- `epdg_diameter_swx_pending_count` - SWx 待处理数
- `epdg_diameter_s6b_active_sessions_count` - S6b 活跃会话数

性能计数器

- `epdg_auth_duration_ms` - 认证耗时
- `epdg_diameter_swx_mar_latency_ms` - MAR 延迟
- `epdg_diameter_swx_sar_latency_ms` - SAR 延迟
- `epdg_session_duration_seconds` - 会话持续时间

VM 性能

- `vm_memory_total` - VM 内存总量
- `vm_memory_processes` - VM 内存进程数
- `vm_memory_binary` - VM 内存二进制数
- `vm_memory_ets` - ETS 内存数
- `vm_system_info_process_count` - VM 系统信息进程数
- `vm_system_info_port_count` - VM 系统信息端口数
- `vm_statistics_run_queue` - VM 统计运行队列

Prometheus 配置

```

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

```

Table

Table FSM configuration table

Protocol	Interval	Protocol	FSM	Target
GTP	10,000 ms	GTP	ePDG UE FSM	PGW GTPv2-C
SWm	10,000 ms		ePDG UE FSM	Diameter SWm
S6b	10,000 ms	GTP	AAA UE FSM	Diameter S6b

File

File `config/runtime.exe` configuration

IKEv2 配置

項目	値	説明
EPDG_LISTEN_IP	"0.0.0.0"	IKEv2 接続を 受け付ける IP "10.0.0.1"
EPDG_PORT_500	"500"	IKE 接続ポート
EPDG_PORT_4500	"4500"	IKE NAT- Traversal ポート
EPDG_CERT_FILE	"/etc/omniepdg/certs/epdg.crt"	IKEv2 接続に 使用する PEM形式の 証明書
EPDG_KEY_FILE	"/etc/omniepdg/certs/epdg.key"	IKEv2 接続に 使用する PEM形式の 秘密鍵
EPDG_SESSION_TIMEOUT	"300000"	セッション タイムアウト 時間

VPN 設定

項目	値	説明
EPDG_VPN_MODE	"simple"	VPN モード "simple" または "gtp"

Diameter

변수명	값	설명
DIA_LISTEN_IP	"0.0.0.0"	Diameter 서버 수신 IP 주소
DIA_LISTEN_PORT	"3868"	Diameter 서버 수신 포트
DIA_HOST	"epdg"	Diameter Origin-Host 이름
DIA_REALM	"epc.mnc001.mcc001.3gppnetwork.org"	Diameter Origin-Realm 이름

HSS 구성

변수명	값	설명
HSS_HOST	"hss"	HSS Diameter 서버 Origin-Host 이름
HSS_IP	"127.0.0.1"	HSS IP 주소
HSS_PORT	"3868"	HSS Diameter 서버 포트

□□□□□□□□□□

□□	□□	□□
LICENSE_SERVER_URL	-	□□□□□□ API URL□□□□□
CONTROL_PANEL_PORT	"4000"	□□□□ HTTP □□□
PROMETHEUS_PORT	"9568"	Prometheus □□ HTTP □□□ /metrics □□□□

📄📄📄 Docker Compose

```
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"

      # VPN 📄📄
      EPDG_VPN_MODE: "simple"

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

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

      # 📄📄📄📄
      CONTROL_PANEL_PORT: "4000"

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


URI	Method	Description
<code>/dashboard</code>	GET	Dashboard overview
<code>/sessions</code>	GET	Active UE sessions
<code>/diameter</code>	Diameter	Diameter interface
<code>/logs</code>	GET	System logs
<code>/docs</code>	GET	Documentation
<code>/resources</code>	GET	BEAM VM resources
<code>/configuration</code>	GET	System configuration

API

OmniEPDG API endpoints

Table 1

Table 1: UE categories and their characteristics

Category	Characteristics
Category 1	Low power UE
Category 2 (UL)	Low power UE with uplink only
Category 3 (DL)	Low power UE with downlink only
Diameter 1000	1000 / 1000

Table 1: UE categories and their characteristics (B, KB, MB, GB)

Table 2

Table 2: UE categories and their characteristics

- Category 1 - Low power UE
- Diameter 1000** - 1000 Diameter
- Category 2 - Low power UE
- Category 3 - Low power UE

Table 3

Table 3: UE categories and their characteristics

VPN	GTP SIMPLE
IKEv2	500 (IKE), 4500 (NAT-T)
Diameter	Diameter
IP (IPv4)	IP CIDR VPN

 UE

OmniEPDG v0.1.0 Licensed to: Omnitouch
© 2020 Omnitouch

Dashboard

Sessions

Diameter

Logs

Docs

Resources

Configuration

License

UE Sessions

1 Session
1 Active
↓ 8.53 KB / ↑ 12.17 KB

IMSI	UE IP	SOURCE	APN	STATUS	DURATION	TRAFFIC
	100.64.34.84	10.7.7.50:14500	*	Active	4m 50s	↓ 8.53 KB / ↑ 12.17 KB

SESSION	NETWORK & TIMING	TRAFFIC
IMSI	DNS	10.4.10.195, 10.4.10.196 Bytes In (UL) 8.53 KB
NAI	3gppnetwork.org P-CSCF	10.4.12.165 Bytes Out (DL) 12.17 KB
UE IP	100.64.34.84 Connected	2026-03-08 21:39:16 Packets In 63
Source	10.7.7.50:14500 Last Activity	2026-03-08 21:41:48 Packets Out 63
APN	* Duration	4m 50s
Child SA SPI	0x4E54838A	

UE

□□□□

□□□□□□□□

□	□□
IMSI	□□□□□□□□□□□□
UE IP	□□□ IPv4/IPv6 □□
SOURCE	UE □□□ IP □□□□NAT □□□
APN	□□□□□□□□
STATUS	□□□□□□□□□□/□□□□
DURATION	□□□□□□□□□□
TRAFFIC	□□/□□□□□□□□UL/DL□

□□□□□□

□□□□□□□□□□□□□□□□





□□	□□	□□
□□	□□	□□□□□□□□□□□□
□□□	□□	□□□□□□
□□□	□□	□□□□□□□□

□□□□

□□□□□□□□□□□□□□□□

□□□□□□□□ IMSI□NAI□□□□□□□□□□

□□□□

□□	□□
IMSI	□□□ IMSI □
NAI	□□□□□□□□3GPP □□□
UE IP	□□□ IPv4/IPv6 □□
Source	UE □□□ IP □□□□NAT □     □
APN	PDN □□□□□□□□
Child SA SPI	IPSec □ SA □□□□□□

□□□□□□□

項目	説明
DNS	UE が DNS を
P-CSCF	IMS の P-CSCF を
Connected	接続状態
Last Activity	最後のアクティビティ
Duration	持続時間

項目

項目	説明
Bytes In (UL)	UE が送信したバイト数
Bytes Out (DL)	UE が受信したバイト数
Packets In	UE が送信したパケット数
Packets Out	UE が受信したパケット数

項目

項目

- "項目" 項目
- 項目 UE 項目

項目

項目

Diameter 配置

Diameter 設定は Diameter 設定 HSS 設定 SWx PGW 設定 S6b 設定

設定

設定

項目	設定
Peer	Diameter 設定 Origin-Host
Realm	Diameter 設定 Origin-Realm
IP 設定	設定 protocol://ip:port
設定	設定

設定

項目	項目	設定
設定	設定	Diameter 設定
設定	設定	設定
設定	設定	設定

設定

設定

- X 設定 - 設定
- Y 設定 - 設定

□□	□□
□□□	□□□□□□□□□□
□□	□□□□□□□□□□□□□□
□□	□□□□□□□

□□□□

□□□□□□□□□□□□□□

□□	□□	□□
debug	□□	□□□□□□□□
info	□□	□□□□□□□□
warning	□□	□□□□
error	□□	□□□□

□□□□

□□□□□□□□□□□□□□□□□□

□□□	□□
□□□□	debug, info, warning, error
□□+	info, warning, error
□□+	warning, error
□□□	error

□□

□□□□□□□□□□

- □□□□□□□□□□□□
- □□□□□□□□
- □□□□□□□□□□

□□

□□	□□
□□/□□	□□□□□□□□/□
□□	□□□□□□□□□□
□□□□	□□□□□□□□□□□□

□□□□

- □□□□ 1000 □□□□□□
- □□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□

□□□

□□□□□□□□□□□□□□

- "□□□□□□□□" □□
- □□□□□□□□□□□□□□□□

□□□□

□□□□□□□□□□□□□□□□□□

Markdown 00

000000 Markdown 000000000000

- 00000000
- 000000000000
- 00
- 000000000000
- 00000000

000000

000000 BEAM VM 000000000000 OTP 000000

□□□□

□□	□□
□□	□□ Mix □□□□/□□□
Elixir □□	□□□□ Elixir □□

□□□□□□

□□□□□□ OTP □□□□□□□□□□□□□□□□□□

- □□□□□□
- □□□□
- □□□□
- □□□□

OmniEPDG 部署

OmniEPDG 通过 Prometheus 监控系统，支持 Diameter 接口，通过 HTTP 接口提供 Prometheus 数据。

目录

- 部署
- 配置
- 接口
 - IKEv2 接口
 - EAP 接口
 - 接口
 - Diameter SWx 接口
 - Diameter S6b 接口
 - 接口
 - ESP 接口
 - IP 接口
 - VM 接口
- Prometheus 配置
- 部署
- 部署

部署

OmniEPDG 部署

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

部署 Prometheus 监控系统，通过 Prometheus 和 Grafana 监控系统。

□□

□ config/runtime.exs □□❖❖□□□□

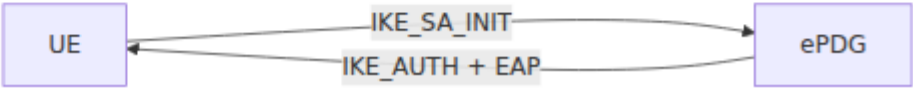
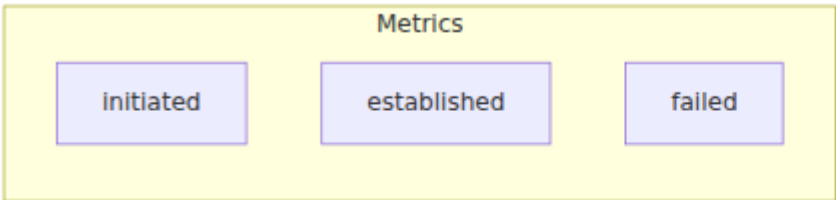
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

□□	□□	□□□	□□□□	□□
port	□□	9568	PROMETHEUS_PORT	/metrics □□□ HTTP □□

□□□□

IKEv2 □□□□

□□ SWu □□□ IKEv2 □□□□□□□□



□□: epdg_ikev2_session_initiated_count

□□: □□□

□□: □□□ IKE_SA_INIT □□□□□□ UE □□□□□□□□□□

□□: epdg_ikev2_session_established_count

□□: □□□

□□: □□□□□ IKE SA □□□□□□□□ EAP-AKA □□□□□□ SA □□□□□□

log: epdg_ikev2_session_failed_count

log: log

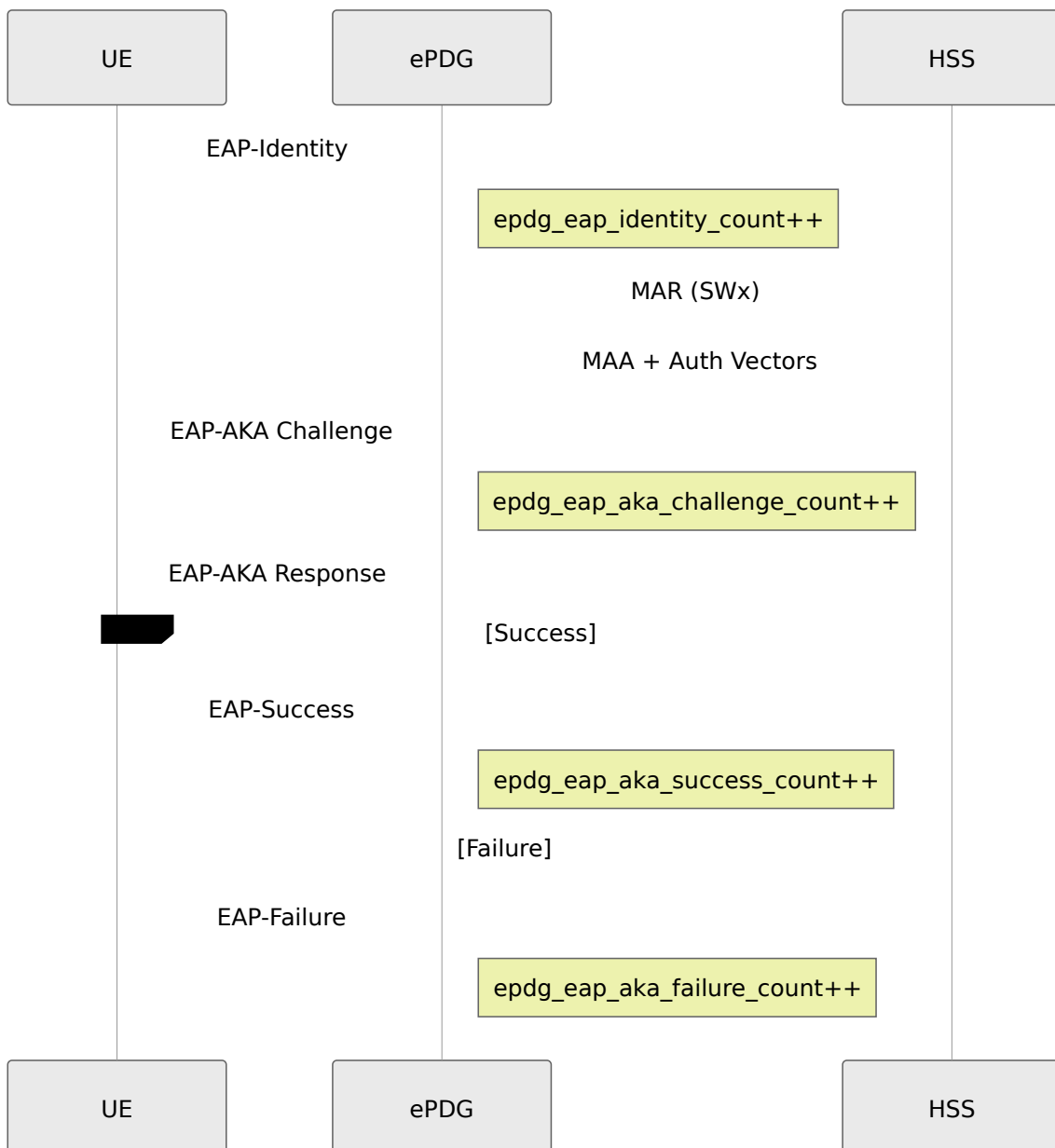
log: IKE SA log

log:

- reason - log auth_failed log timeout log invalid_proposal log

EAP log

log RFC 4187 log EAP-AKA log OmniEPDG log RFC 5448 log EAP-AKA' log
log UE log NAI log



计数器: epdg_eap_identity_count

单位: 计数

描述: UE 发起 EAP-Identity 请求的总次数

计数器: epdg_eap_aka_challenge_count

单位: 计数

描述: UE 发起 EAP-AKA 挑战请求的总次数

计数器: epdg_eap_aka_success_count

单位: 计数

描述: EAP-AKA 认证成功次数

计数器: epdg_eap_aka_failure_count

单位: 计数

描述: EAP-AKA 认证失败次数

原因:

- reason - 认证失败原因: res_mismatch, invalid_identity, authentication_rejected
-

计数器: epdg_eap_aka_sync_failure_count

单位: 计数

描述: EAP-AKA 同步失败 (SQN) 次数 (USIM/HSS 同步失败)

计数器: epdg_auth_verification_failed_count

单位: 计数

计数器: epdg_auth_verification_failed_count

单位: 计数

描述: AUTH 验证失败次数

🔍: `epdg_auth_rate_limited_count`

🔍: 📄

🔍: 📄📄📄📄📄📄📄📄📄📄📄📄📄📄📄📄

🔍:

- `type` - 📄📄📄📄 `ip` 📄📄 IP 📄📄📄📄📄 `imsi` 📄📄 IMSI 📄📄📄📄

📄📄📄📄:

```
# 📄📄📄📄📄📄  
rate(epdg_auth_rate_limited_count[1m])  
  
# 📄📄📄📄  
sum by (type) (rate(epdg_auth_rate_limited_count[5m]))
```

🔍: `epdg_auth_geoip_blocked_count`

🔍: 📄

🔍: 📄 GeoIP 📄📄📄📄📄📄📄📄📄📄📄📄📄📄

🔍:

- `country` - ISO 3166-1 alpha-2 📄📄📄📄📄📄 `CN` 📄 `RU` 📄📄 `UNKNOWN` 📄📄📄📄📄📄📄
IP

📄📄📄📄:

```
# 📄📄📄📄 GeoIP 📄  
rate(epdg_auth_geoip_blocked_count[1m])  
  
# 📄📄📄📄📄📄  
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))
```

🔍: `epdg_esp_replay_detected_count`

🔍: 📄

🔍: 📄📄📄📄📄📄📄📄 ESP 📄📄📄📄📄📄 RFC 4303📄📄📄📄📄📄📄📄📄📄📄📄📄📄📄📄📄📄

Diameter SWx

3GPP TS 29.273 ePDG HSS SWx

epdg_diameter_swx_mar_count

Count

Count HSS

Count

- result - success failure
-

epdg_diameter_swx_sar_count

Count

Count HSS

Count

- result - success failure
-

epdg_diameter_swx_mar_latency_ms

Count

MAR

50, 100, 250, 500, 1000, 2500 ms

epdg_diameter_swx_sar_latency_ms

Count

SAR

50, 100, 250, 500, 1000, 2500 ms

epdg_diameter_swx_pending_count

Count

Count SWx HSS

Diameter S6b

3GPP TS 29.273 AAA PGW S6b GTP

epdg_diameter_s6b_aar_count

:

: AA

:

- result - success failure
-

epdg_diameter_s6b_str_count

:

:

epdg_diameter_s6b_active_sessions_count

:

: S6b

PDN

epdg_session_created_count

:

:

:

- vpn_mode - VPN simple gtp
-

epdg_session_terminated_count

:

:

:

- reason - user_request timeout error admin

计数器: `epdg_sessions_active_count`

计数器: 计数器

计数器: 计数器计数器计数器 5 计数器

计数器: `epdg_sessions_by_state_count`

计数器: 计数器

计数器: 计数器 FSM 计数器

计数器:

- `state` - 计数器计数器 `init` 计数器 `eap_identity` 计数器 `eap_aka_challenge` 计数器 `authenticated` 计数器 `established` 计数器
-

计数器: `epdg_auth_duration_ms`

计数器: 计数器

计数器: 计数器 IKE_SA_INIT 计数器计数器计数器计数器计数器

计数器: 100, 250, 500, 1000, 2500, 5000, 10000 ms

计数器: `epdg_session_duration_seconds`

计数器: 计数器

计数器: 计数器计数器计数器计数器

计数器: 60, 300, 900, 1800, 3600, 7200, 14400 seconds 计数器 1 计数器 4 计数器

ESP 计数器

计数器 RFC 4303 计数器 ESP 计数器

计数器: `epdg_esp_packets_in_count`

计数器: 计数器

计数器: 计数器 ESP 计数器 UE → 计数器

计数器: `epdg_esp_packets_out_count`

计数器: 计数器

计数器: 计数器 ESP 计数器 → UE 计数器

命令: `epdg_esp_bytes_in_total`

命令: 显示


命令: 显示 ESP 流量统计

命令: `epdg_esp_bytes_out_total`

命令: 显示

命令: 显示 ESP 流量统计

IP 统计

显示 VPN 流量 IP 统计 

命令: `epdg_ip_allocated_count`

命令: 显示

命令: 显示 IP 统计

命令:

- `type` - 指定 IP 类型 `ipv4` 或 `ipv6`
-

命令: `epdg_ip_released_count`

命令: 显示

命令: 显示 IP 统计

命令:

- `type` - 指定 IP 类型 `ipv4` 或 `ipv6`
-

命令: `epdg_ip_pool_allocated_count`

命令: 显示

命令: 显示 IP 池统计

命令: `epdg_ip_pool_available_count`

命令: 显示

命令: 显示 IP 池统计

名称: epdg_ip_pool_utilization_ratio
单位: 百分比
范围: IP 地址池利用率 0.0 到 1.0 的浮点数值

VM 内存

用于 Erlang/BEAM 的内存

名称: vm_memory_total
单位: 字节
范围: 0
描述: VM 总内存

名称: vm_memory_processes
单位: 字节
范围: 0
描述: Erlang 进程内存

名称: vm_memory_binary
单位: 字节
范围: 0
描述: 二进制数据内存

名称: vm_memory_ets
单位: 字节
范围: 0
描述: ETS 表内存

名称: vm_system_info_process_count
单位: 计数
范围: 0
描述: Erlang 进程数

[[[vm_system_info_port_count

[[[]]

[[[]]

[[[vm_statistics_run_queue

[[[]]

[[[]]

Prometheus [[[]]

[[[]]

[[[]]

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

[[[]]

[[[]]

```

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

```

□□□□

□□□□□□□□

```

# 5 □□□□□□□□
sum(rate(epdg_eap_aka_success_count[5m]))
/
(sum(rate(epdg_eap_aka_success_count[5m])) +
sum(rate(epdg_eap_aka_failure_count[5m])))

```

□□□□□□

```

# □□□□□□□□
rate(epdg_ikev2_session_established_count[5m])

```

□□□□□□ (p95)

```

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

```

HSS 指标 (p99)

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

指标名称

```
epdg_sessions_active_count
```

IP 指标

```
epdg_ip_pool_utilization_ratio * 100
```

ESP 指标

```
# 总流量  
rate(epdg_esp_bytes_in_total[5m])  
  
# 总包数  
rate(epdg_esp_packets_in_count[5m]) +  
rate(epdg_esp_packets_out_count[5m])
```

指标名称

```
# EAP 失败原因  
sum by (reason) (rate(epdg_eap_aka_failure_count[5m]))  
  
# 会话终止原因  
sum by (reason) (rate(epdg_session_terminated_count[5m]))
```



OmniEPDG Prometheus

```

groups:
- name: omniepdg
  rules:
    # EAP-AKA
    - 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: "EAP-AKA "
        description: "5  {{{ $value |
humanizePercentage }}"

    # IP
    - alert: OmniEPDGIPPoolLow
      expr: epdg_ip_pool_utilization_ratio > 0.9
      for: 5m
      labels:
        severity: warning
      annotations:
        summary: "IP 90%"
        description: "IP {{{ $value | humanizePercentage
}}"

    # IP
    - alert: OmniEPDGIPPoolExhausted
      expr: epdg_ip_pool_available_count == 0
      for: 1m
      labels:
        severity: critical
      annotations:
        summary: "IP "
        description: "IP "

    # HSS
    - alert: OmniEPDGHSSLatencyHigh
      expr: |

```

```

        histogram_quantile(0.95,
sum(rate(epdg_diameter_swx_mar_latency_ms_bucket[5m])) by (le))
    > 1000
    for: 5m
    labels:
      severity: warning
    annotations:
      summary: "HSS (SWx) 🚨"
      description: "95 🚨 MAR 🚨 {{ $value }}ms"

# 🚨 SWx 🚨🚨
- alert: OmniEPDGSWxBacklog
  expr: epdg_diameter_swx_pending_count > 100
  for: 2m
  labels:
    severity: warning
  annotations:
    summary: "SWx 🚨🚨"
    description: "{{ $value }} 🚨🚨 SWx 🚨"

# VM 🚨🚨
- alert: OmniEPDGMemoryHigh
  expr: vm_memory_total > 2147483648
  for: 10m
  labels:
    severity: warning
  annotations:
    summary: "OmniEPDG 🚨🚨🚨"
    description: "VM 🚨🚨🚨 {{ $value | humanize1024 }}"

# 🚨🚨🚨🚨
- alert: OmniEPDGSchedulerOverload
  expr: vm_statistics_run_queue > 10
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Erlang 🚨🚨🚨🚨🚨"
    description: "🚨🚨🚨🚨 {{ $value }}🚨🚨 CPU 🚨"

# 🚨🚨🚨🚨🚨🚨🚨
- alert: OmniEPDGNoSessions
  expr: epdg_sessions_active_count == 0 and
epdg_ikev2_session_initiated_count > 0

```

```

for: 10m
labels:
  severity: warning
annotations:
  summary: "High rate of authentication failures"
  description: "High rate of authentication failures"

# High rate of authentication failures
- alert: OmniEPDGHighRateLimiting
  expr: rate(epdg_auth_rate_limited_count[5m]) > 10
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "High rate of authentication failures"
    description: "{{ $value | printf \"%.1f\" }} High rate of authentication failures"

# GeoIP blocking spike
- alert: OmniEPDGGeoIPBlockingSpike
  expr: |
    rate(epdg_auth_geoip_blocked_count[5m]) > 5
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "GeoIP blocking spike"
    description: "{{ $value | printf \"%.1f\" }} GeoIP blocking spike"

# ESP replay attack
- alert: OmniEPDGReplayAttack
  expr: rate(epdg_esp_replay_detected_count[5m]) > 0
  for: 2m
  labels:
    severity: warning
  annotations:
    summary: "ESP replay attack"
    description: "{{ $value | printf \"%.1f\" }} ESP replay attack"

# AUTH verification failures
- alert: OmniEPDGAuthVerificationFailures
  expr: rate(epdg_auth_verification_failed_count[5m]) > 0
  for: 2m

```

```
labels:  
  severity: critical  
annotations:  
  summary: "AUTH AUTH AUTH AUTH"  
  description: "AUTH AUTH AUTH AUTH"
```



OmniEPDG WiFi DNS



(UE ↔ ePDG)

WiFi

500	UDP		IKEv2 (IKE_SA_INIT, IKE_AUTH)
4500	UDP		IKEv2 NAT ESP-in-UDP

500/UDP IKEv2 UE ePDG NAT WiFi 4500

4500/UDP NAT-T IKEv2 ESP WiFi

(ePDG ↔)

OmniEPDG ePDG

3868	TCP		Diameter SWx ()	HSS / DRA
3868	TCP		Diameter S6b ()	PGW / AAA
2123	UDP		GTPv2-C (S2b)	PGW
2152	UDP		GTP-U (S2b-U)	PGW

□□□□

□□□□□□□□□□□□□□□□□□□□

□□	□□	□□
4000	TCP	□□□□□□□□ (HTTP)
443	TCP	□□□□□□□□ (HTTPS, □□)
9568	TCP	Prometheus □□□□

DNS □□

ePDG □□ DNS □□

□□□□□□ 3GPP TS 23.003 □□□□□□□□ DNS □□□□□□ ePDG□FQDN □□□□

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

□□□

- <MCC> □ 3 □□□□□□□□□□□□□□□□□□□□ 505□
- <MNC> □ 2 □ 3 □□□□□□□□□□□□□□□□□□□□ 3 □□□□□□ 001□

DNS □□□□□□ OmniEPDG □□ IP □□□ **A** □□□□ IPv6 □ AAAA □□□□

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

□□□□□□□

ePDG □ TLS □□□□□□□□□□□□□□□□□□□□ ePDG FQDN □□□□□□□□□□ (SAN)□□ IKEv2 □□□□□□□□□□ □□□□□□□□□□

□□□□

- SAN □□□□ ePDG □□ FQDN□□□□
`epdg.epc.mnc001.mcc001.pub.3gppnetwork.org` □
- □□□□□□□□ CA □□□□□□□□
- □□ RSA 2048 □□ ECDSA P-256

Diameter □ DNS

□□□□ Diameter □□□□□□ DNS NAPTR/SRV □□□□□□ RFC 6408□□□□□□

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

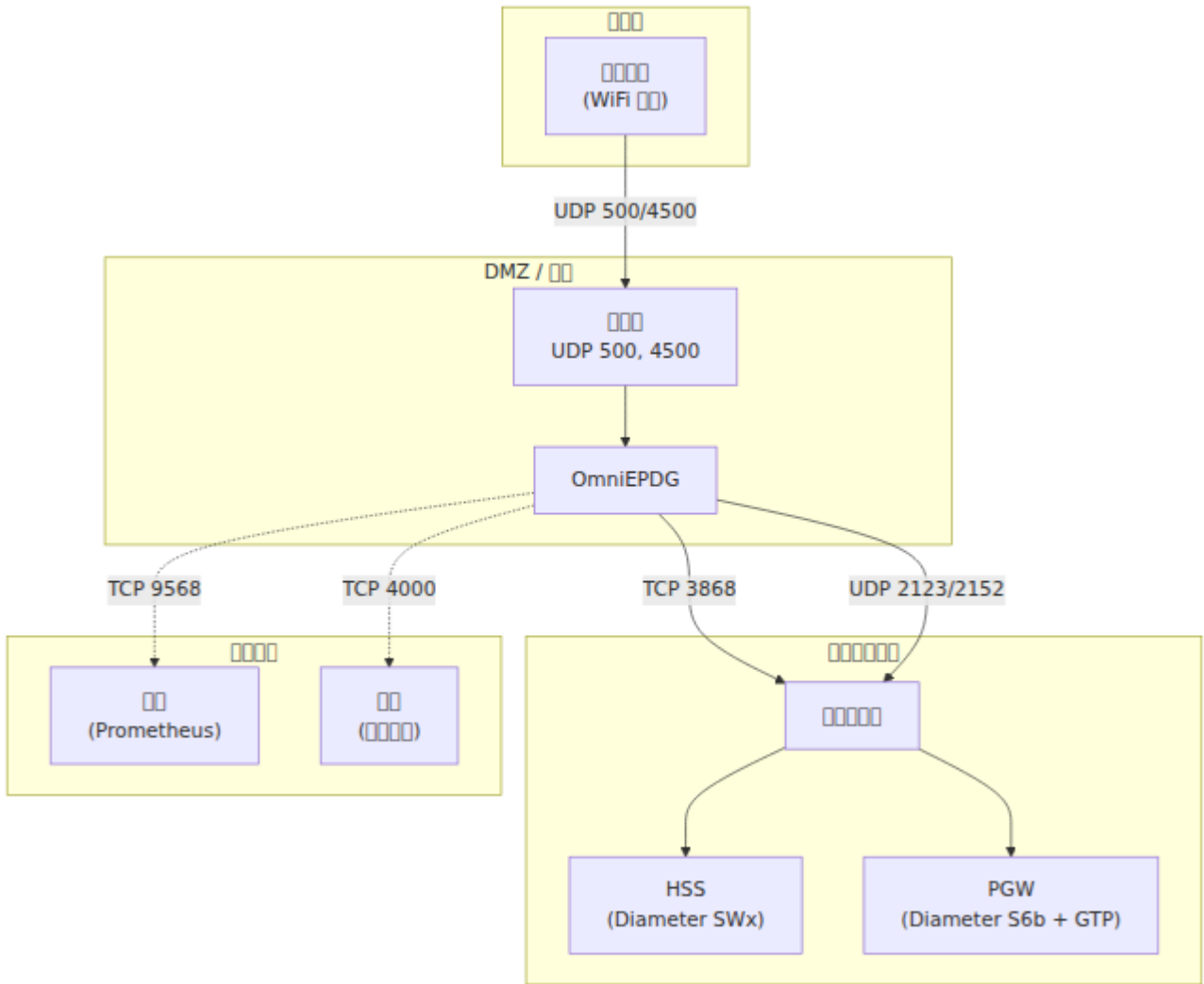
□□□

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

□□□□

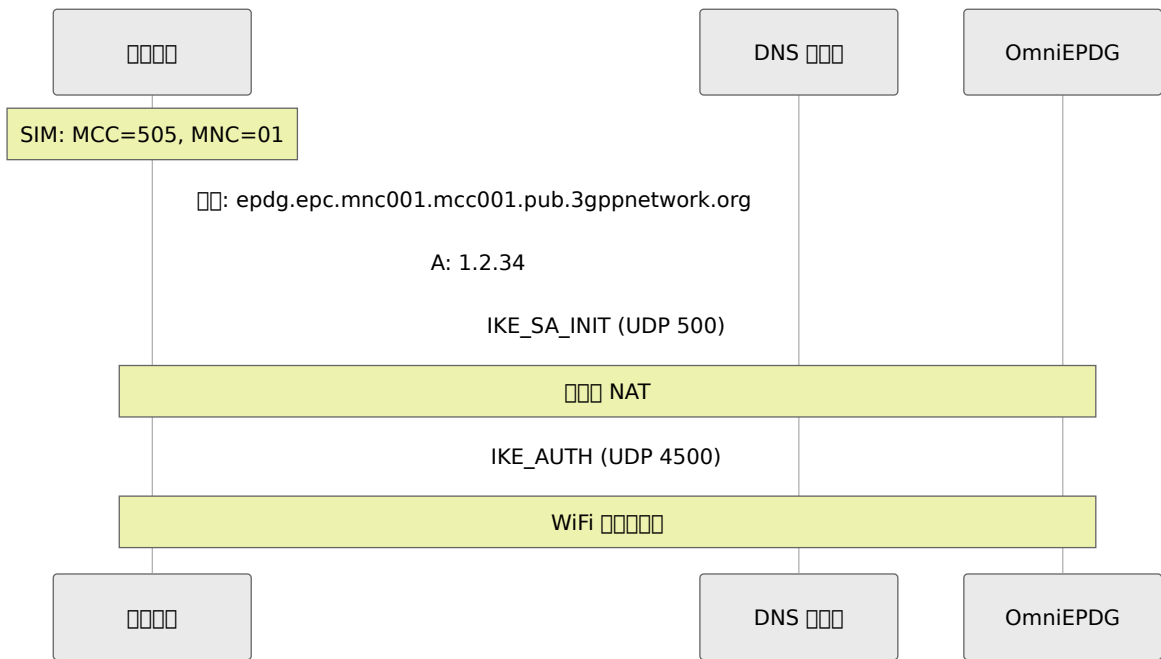
- UE □□□□□□□□ NAI□□□□□□□□□□
- Diameter Origin-Realm □ Destination-Realm AVP
- Diameter □□□□

□□□□



DNS □□□□

□□□□□□ WiFi □□□□□□□□ DNS □□□



IP

IP

- UDP 500 → OmniEPDG
- UDP 4500 → OmniEPDG
- DNS A: `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` → ePDG IP
- SAN → TLS

IP

- TCP 3868 → OmniEPDG → HSS/DRA
- TCP 3868 → OmniEPDG → PGW/AAA → GTP
- UDP 2123 → OmniEPDG → PGW → GTP
- UDP 2152 → OmniEPDG → PGW → GTP

IP

- TCP 4000/443

TCP 9568 0000000000

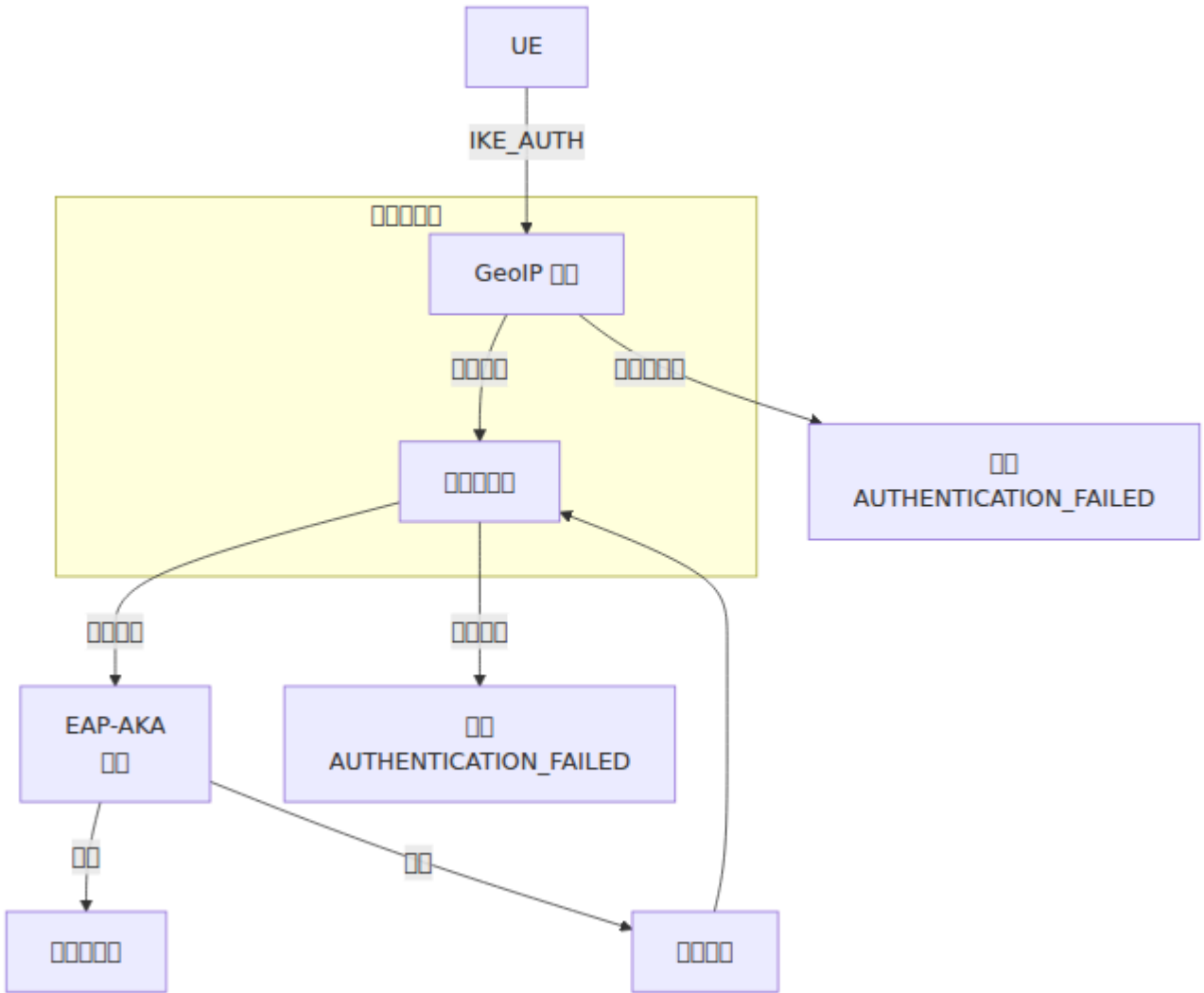
0000

- [3GPP TS 23.003](#) - 00000000 (ePDG FQDN 00)
- [3GPP TS 23.402](#) - 0 3GPP 00000000
- [RFC 7296](#) - IKEv2 00
- [RFC 3948](#) - IPsec ESP 0000 UDP 00 (NAT-T)
- [RFC 6733](#) - Diameter 0000

OmniEPDG

OmniEPDG 

- 
- 
- **GeoIP** 
- 
- 
- 



OmniEPDG IKE_AUTH

1. **GeolP** - IP
2. - IP/IMSI
3. **EAP-AKA** - 3GPP



IP IMSI

IMSI

参数	单位	默认值	描述
auth_rate_limit_per_imsi	每秒	5	每个 IMSI 每秒允许的认证请求数
auth_rate_limit_imsi_window_ms	毫秒	60000	每个 IMSI 的认证速率限制窗口
auth_rate_limit_imsi_block_ms	毫秒	600000	每个 IMSI 认证失败后的阻塞时间，最多 10 个 IP 地址

配置

配置 IP/IMSI 认证速率限制和阻塞时间

配置

配置

配置

```
config :omniepdg,
  auth_rate_limit_per_ip: 5,
  auth_rate_limit_ip_window_ms: 120_000, # 2 分钟
  auth_rate_limit_ip_block_ms: 900_000, # 15 分钟

  auth_rate_limit_per_imsi: 3,
  auth_rate_limit_imsi_window_ms: 120_000,
  auth_rate_limit_imsi_block_ms: 1_800_000 # 30 分钟
```

配置 2 个 IP 地址，每个 IMSI 每秒 5 个认证请求，阻塞时间 15-30 分钟

MaxMind GeoLite2 安裝

GeoIP 安裝 MaxMind GeoLite2 資料庫 IP 地址

安裝 GeoIP

1. 安裝 MaxMind GeoLite2 資料庫
2. 安裝 GeoLite2-Country.mmdb 資料庫
3. 將資料庫複製到 /etc/omniepdg/GeoLite2-Country.mmdb
4. 安裝 GeoIP

配置

```
config :omniepdg,  
  # 安裝 GeoIP  
  geip_enabled: true,  
  
  # MaxMind 資料庫  
  geip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",  
  
  # 安裝模式  
  geip_mode: :whitelist,  
  
  # 安裝 ISO 3166-1 alpha-2 代碼  
  geip_countries: ["AU", "NZ"],  
  
  # 安裝 IP  
  geip_allow_unknown: false,  
  
  # 安裝 fail-open  
  geip_fail_open: true
```

00

名前	型	デフォルト値	説明
<code>geoiP_enabled</code>	boolean	<code>false</code>	GeoiP を有効にするかどうか。 true: 有効 false: 無効 IP アドレスを地理的に位置付ける かどうか
<code>geoiP_database_path</code>	string	<code>"/etc/omniepdg/GeoLite2-Country.mmdb"</code>	MaxMind GeoLite2 Country データベースのパス MMDB形式
<code>geoiP_mode</code>	string	<code>:whitelist</code>	GeoiP モード。 :whitelist: 許可リスト :blacklist: 拒否リスト :geoip: GeoiP データベース を使用
<code>geoiP_countries</code>	list	<code>[]</code>	ISO 3166-1 alpha-2 形式の 許可リスト geoiP_mode が :whitelist の場合
<code>geoiP_allow_unknown</code>	boolean	<code>true</code>	未知の IP アドレスを 許可するかどうか。 true: 許可 false: 拒否
<code>geoiP_fail_open</code>	boolean	<code>true</code>	GeoiP データベース が読み込めない場合

項目	項目	項目	項目
			<input type="checkbox"/> true 有効 <input type="checkbox"/> false 無効

設定

WiFi 設定

設定

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ", "FJ"] # 有効
```

設定 IP UE 設定

WiFi 設定

設定

設定

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :blacklist,
  geoip_countries: ["CN", "RU", "KP", "IR"] # 有効
```

設定 UE 設定

設定

IP Whitelist

IP Whitelist

- IP 10.x.x.x 192.168.x.x
- IP
- Tor VPN

`geip_allow_unknown`

	<code>geip_allow_unknown</code>	
	<code>false</code>	= =
	<code>true</code>	= =

```
config :omniepdg,  
  geip_mode: :whitelist,  
  geip_allow_unknown: true # IP
```

GeoIP

MaxMind GeoLite2

1. `GeoLite2-Country.mmdb`
- 2.
- 3.

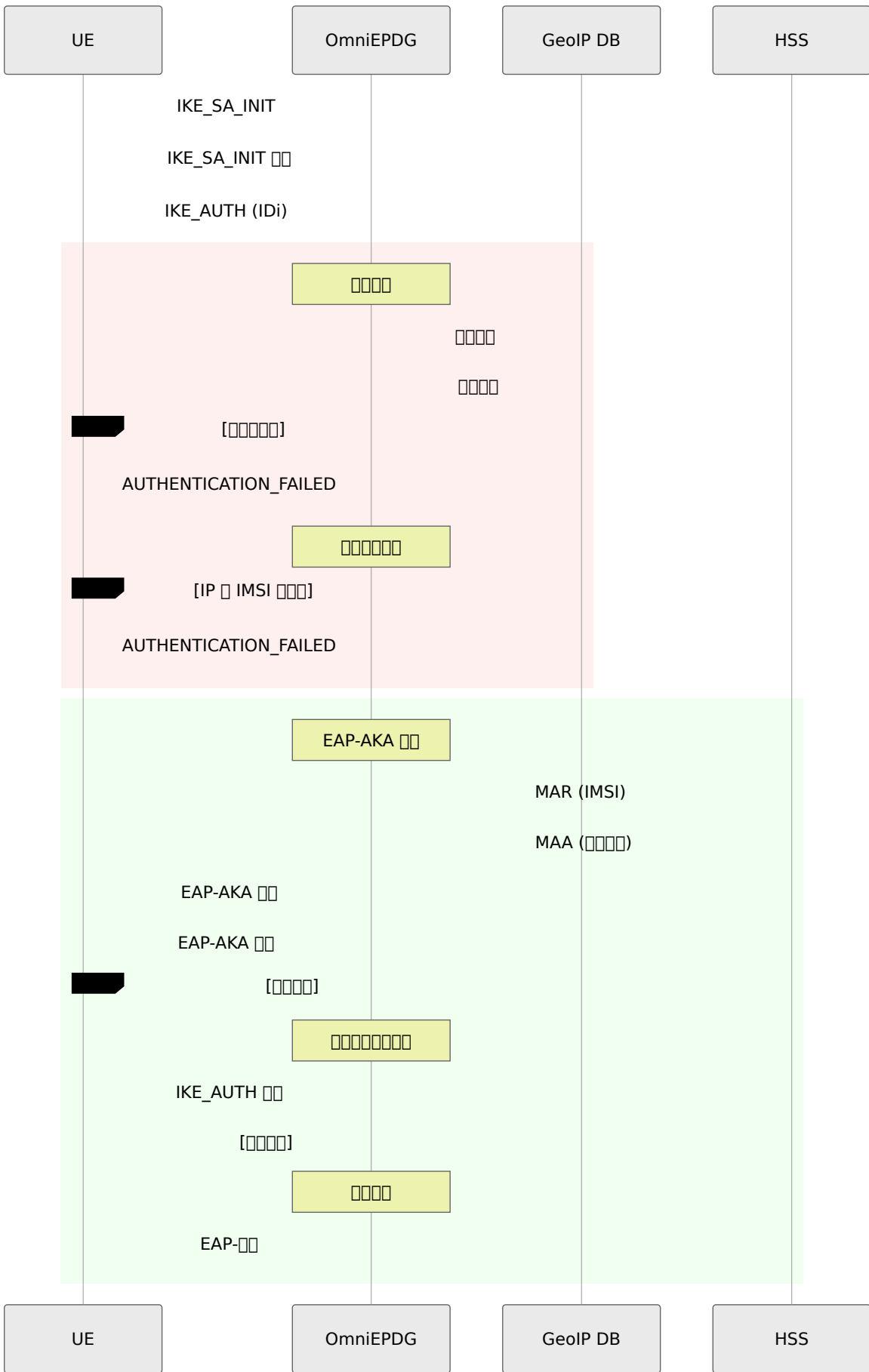
□□□□□□

□□	□□	□□	□□
AU	□□□□	US	□□
NZ	□□□	GB	□□
CA	□□□	DE	□□
FR	□□	JP	□□
SG	□□□	HK	□□
IN	□□	CN	□□

□□□□□ [ISO 3166-1 alpha-2](#)

□□□□

□□□□□□□□□□



□□

□□□□□□

□□: `epdg_auth_rate_limited_count` □□: □□□ □□: □□□□□□□□□□□□□□ □□:

- `type` - □□□□□ `ip` □IP □□□□□□ `imsi` □IMSI □□□□□

□□□□□

```
# □□□□□□□□□□
rate(epdg_auth_rate_limited_count[1m])

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

# □□□□□□□□□□□□
rate(epdg_auth_rate_limited_count[5m]) > 10
```

GeoIP □□

□□: `epdg_auth_geoip_blocked_count` □□: □□□ □□: □ GeoIP □□□□□□□□□□ □□:

- `country` - ISO 3166-1 alpha-2 □□□□□□ □□□□□□ □□□□□□□□ IP

□□□□□

```
# □□□□□ GeoIP □□
rate(epdg_auth_geoip_blocked_count[1m])

# □□□□□□□□□□
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))

# □□□□□□□□□□□□□□
increase(epdg_auth_geoip_blocked_count{country="XX"}[1h]) > 100
```


□□□□

□□□□□□

□□□□□□

□□: □□□□□□□□□□□□

□□□□:

- □□□□□□□□□□
- □□□□□□□□□□□□□□□
- □□□□□□□□□□

□□□□:

1. □□□□□□ IP/IMSI □□□□
2. □□□□□□□□□□□□□□
3. □□□□□□□□□□□□□□

□□□□□□□□□□

□□: `epdg_auth_rate_limited_count` □□□□

□□□□:

- □□□□□□□□□□
- □□□□□ UE □□□□□□
- □□□□□□

□□□□:

1. □□□□□□□ IP □□□□□□
2. □□□□□□□□□□ IP □□□□□□
3. □□□□□□□□□□□□□□ HSS □□

GeoIP 設定

インストール

コマンド: `sudo apt-get install geoip-bin`

確認:

- `geoiplookup`
- `geoiplookup -i`
- `geoiplookup -i $(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 16 | xargs echo | sha1sum | cut -d ' ' -f 1)` IP

設定:

1. `geoiplookup`
2. `geoiplookup -i`
3. `geoiplookup -i $(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 16 | xargs echo | sha1sum | cut -d ' ' -f 1)` `geoip_allow_unknown: true`
4. `geoiplookup` GeoIP 設定

GeoIP 設定

コマンド: `sudo apt-get install geoip-bin`

確認:

- `geoiplookup`
- `geoiplookup -i`
- `geoiplookup -i $(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 16 | xargs echo | sha1sum | cut -d ' ' -f 1)` MMDB 設定

設定:

1. `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. `MaxMind` 設定

インストール

コマンド: `sudo apt-get install geoip-bin`

□□□□:

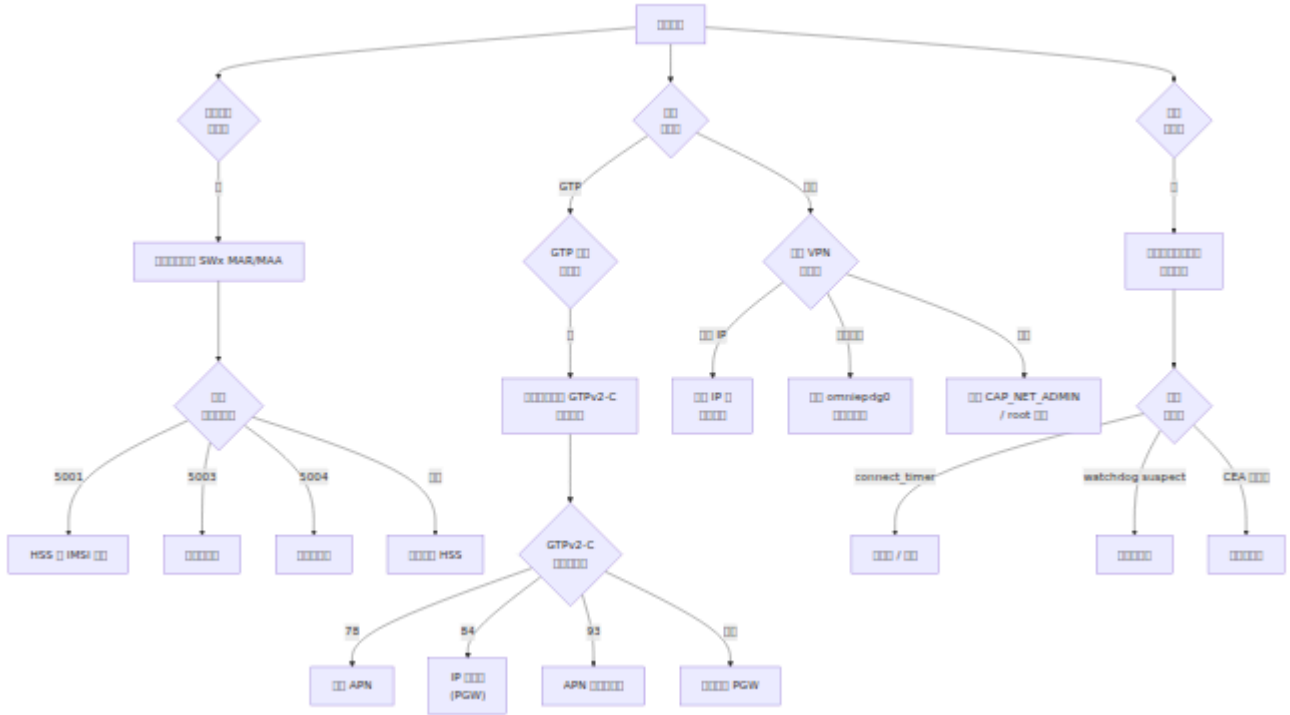
- VPN/□□□ IP □□□□□□□□
- GeolP □□□□□
- □□□□□□□□□□

□□□□:

1. □□ GeolP □□□□□□□□
2. □□□□□□□□ IP □□□□□
3. □□□□□□□□□□□□□□□□□□

OmniEPDG

OmniEPDG



OmniEPDG [log/](#)

파일	내용	설명
log/console.log	콘솔 로그	디버깅용 로그
log/error.log	오류 로그	오류 발생 시 기록되는 로그
log/crash.log	OTP 실패 로그	OTP 실패 시 기록되는 로그
log/erlang.log	Erlang 실행 로그	Erlang/OTP 실행 로그

로그 파일

로그 파일

- peer_up - 연결 성공 로그
- peer_down - 연결 실패 로그

UE FSM

- ue_fsm state_<name> event=<event> - FSM 상태 변경 로그
- ue_fsm init(<IMSI>) - FSM 초기화 로그
- terminating epdg_ue_fsm with reason <reason> - FSM 종료 로그

타이머

- Timeout swm_der_timeout - SWm DER 타이머
- Timeout create_session_timeout - GTPv2-C 세션 생성 타이머
- Timeout s2b_delete_session_timeout - GTPv2-C 세션 삭제 타이머
- Timeout cancel_location_timeout - 위치 취소 타이머

SWx

HSS (SWx)

SWx와 HSS 간의 상호작용

□□□□

- □□□□ OmniEPDG □ HSS □□□ SCTP □□ 3868
- □□□□ `dia_swx_remote_ip` □ `dia_swx_remote_port` □□□
- HSS □□□□□□□□□□
- □□□□□□□□ SCTP□□□□□□□□□□ SCTP□
- Origin-Host □ Origin-Realm □□□□□ CEA □□

□□□□

1. □□□ HSS IP □□□□□□□□□□
2. □□ `dia_swx_remote_ip` □ `dia_swx_remote_port` □ HSS □□□□
3. □□□□□□□□□□ SCTP □□□□□ SCTP □□□□□ `dia_swx_proto` □□□ `tcp` □□□□
4. □□ `dia_swx_origin_host` □□□□□ FQDN□□□□ HSS □□□□□
5. □□ HSS □□□□□□□□ CER/CEA □□□□□□□□

PGW □□□□ (S6b)

□□□□□□□□□□ GTP □□□□□□□□ S6b AAR □ PGW □□□□□□□□□□□□ S6b peer_up □□□

□□□□

- PGW □□□□□□□□ OmniEPDG □ S6b □□□
- □□□□□□□□ OmniEPDG □ S6b □□□□□□□□ SCTP □□ 3868
- `dia_s6b_local_ip` □ PGW □□□□
- Origin-Host □ Origin-Realm □□□

□□□□

1. □□ PGW □□□□□□□□□□ OmniEPDG □ `dia_s6b_local_ip:dia_s6b_local_port`
2. □□ S6b □□□□□□□□□□ PGW □□□□
3. □□□□□□□□□□□□□□ S6b □□□□□□□□ 3868 □□□□□ SCTP
4. □□ `dia_s6b_origin_host` □ `dia_s6b_origin_realm` □ PGW □□□□□

□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□□□□□□ SUSPECT □ DOWN □□□

□□□□

- □□□□ WiFi □□□□□□
- APN □□□□□□□□
- □□□□□□□□

□□□□

1. □□ HSS □□□□□□□□□□
2. □□ WiFi □□ / ePDG □□□□□□□□□□
3. □□□□ APN □□□□□□□□ APN □□□

□□□□ (□□ 5004)

□□□□□□□□□□□□□□□□□□ SWx MAA □ SAA □□□ 5004□

□□□□

- HSS □□□□□□□□□□□□
- □□□□□□□□□□ WiFi □□

□□□□

1. □□ HSS □□□□□□□□□□ HPLMN/VPLMN □□
2. □□□□□□□□□□□□ WiFi □□

□□□□□□

□□□□□□□□□□□□ 10 □□□□□□□□□□ Timeout swm_der_timeout □
state_wait_auth_resp □□

□□□□

- HSS □ 10 □□□□□□ SWx MAR
- SWx □□□□□□□□□□□□
- HSS □□

□□□□

1. HSS
2. SWx OKAY SUSPECT DOWN
3. `dia_swx_transmit_timer` HSS

EAP-AKA

"type_mismatch" UE EAP

- UE 0 EAP-AKA EAP-AKA'
- HSS EAP

3GPP TS 23.003 NAI

- 0 EAP-AKA
- 6 EAP-AKA'

OmniEPDG UE WiFi UE 0 EAP-AKA

1. UE NAI
2. HSS
3. SIM

EAP-AKA RES

"RES mismatch" "res_mismatch"

- SIM
- UE
- HSS

1. SIM 注册
2. HSS 鉴权 RAND, AUTN, XRES, CK, IK
3. XRES 鉴权 RES
4. SIM 注册 SIM 鉴权 HSS 鉴权 Ki 鉴权 OP/OPc 鉴权

GTP 注册 GTP 鉴权

PGW 注册

注册 GTPv2-C 注册

注册

注册	鉴权	注册
78	注册 APN	注册 APN 注册 PGW 注册
82	注册 RAT 注册	注册 PGW 注册 WiFi 注册 3GPP 注册
84	注册	PGW IP 注册 注册
92	注册	PGW 注册 S6b 注册
93	APN 注册	注册 PGW 注册 APN 注册
96	IMSI/IMEI 注册	注册 PGW 注册 S6b 注册
113	APN 注册	APN 注册 PGW 注册
120	GTP-C 注册	PGW 注册

注册

注册 10 注册 Timeout create_session_timeout 注册 state_wait_create_session_resp 注册

VPN 配置 VPN 配置

TUN 配置

OmniEPDG 配置 `omniepdg0` 配置 `simple_vpn_route` 配置

配置

- OmniEPDG 配置 `CAP_NET_ADMIN` 配置 `root` 配置
- TUN/TAP 配置
- 配置 `omniepdg0` 配置

配置

1. 配置 TUN 配置 `lsmod | grep tun`
2. 配置 OmniEPDG 配置 TUN 配置
3. 配置 `omniepdg0` 配置 `ip link show omniepdg0`
4. 配置 `log/crash.log` 配置

IP 配置

配置 `simple_vpn_pool` 配置 IP 配置

配置

- 配置 CIDR 配置
- 配置 IP 配置
- 配置

配置

1. 配置 `epdg_ue_fsm` 配置
2. 配置 `terminating` 配置
3. 配置 `simple_vpn_pool_ipv4` 配置 CIDR 配置
4. 配置 `log/crash.log` 配置 FSM 配置 IP 配置

