

OmniEPDG

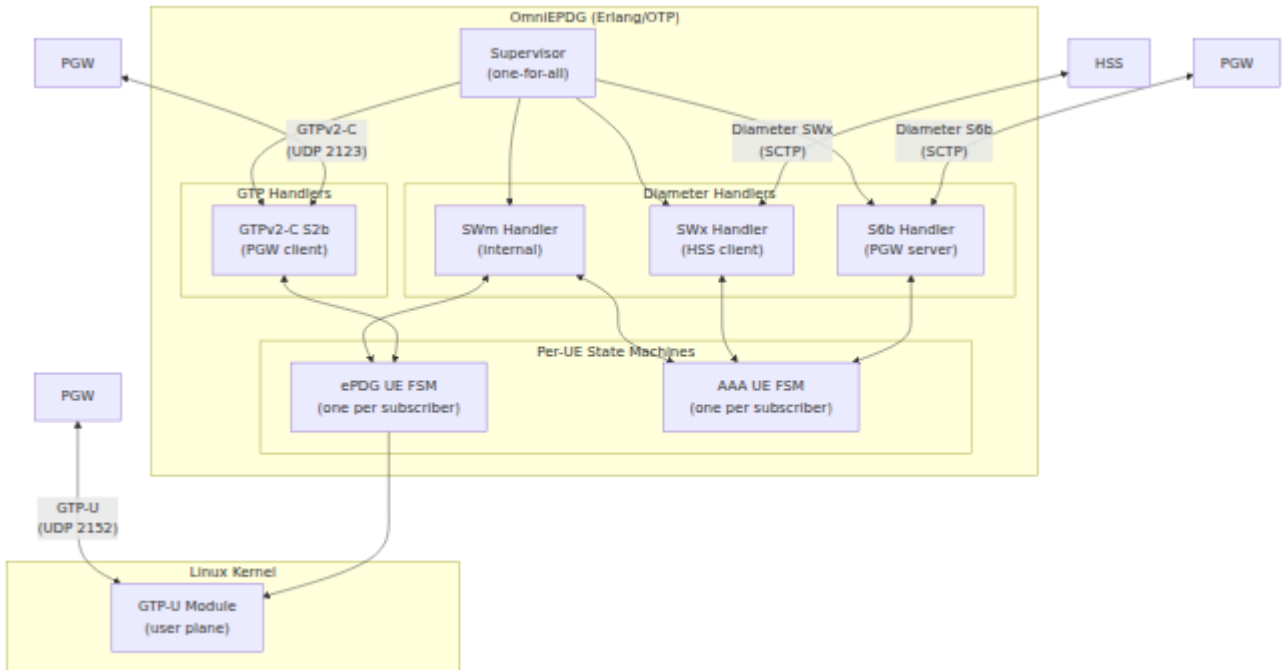
OmniEPDG 3GPP ePDG, WiFi, VoWiFi, VPN, TUN, GTP, PGW, HSS, Diameter S6b, Diameter SWx, GTPv2-C, GTP-U, Linux Kernel, GTP-U Module (user plane)

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 할당 관리
simple_vpn_pool	IP 풀	ETS, CIDR, IPv4 풀
simple_vpn_route	VPN 라우팅	omniepdg@ TUN 모듈

기타 모듈

이 모듈은 IMSI 기반 OmniEPDG 모듈을 구성합니다.

- **ePDG UE FSM** (`epdg_ue_fsm`) - ePDG 프로세스에서 GTP 프로세스와 통신
- **AAA UE FSM** (`aaa_ue_fsm`) - AAA 프로세스에서 HSS와 Diameter SWx 프로세스와 PGW와 S6b 프로세스와 통신

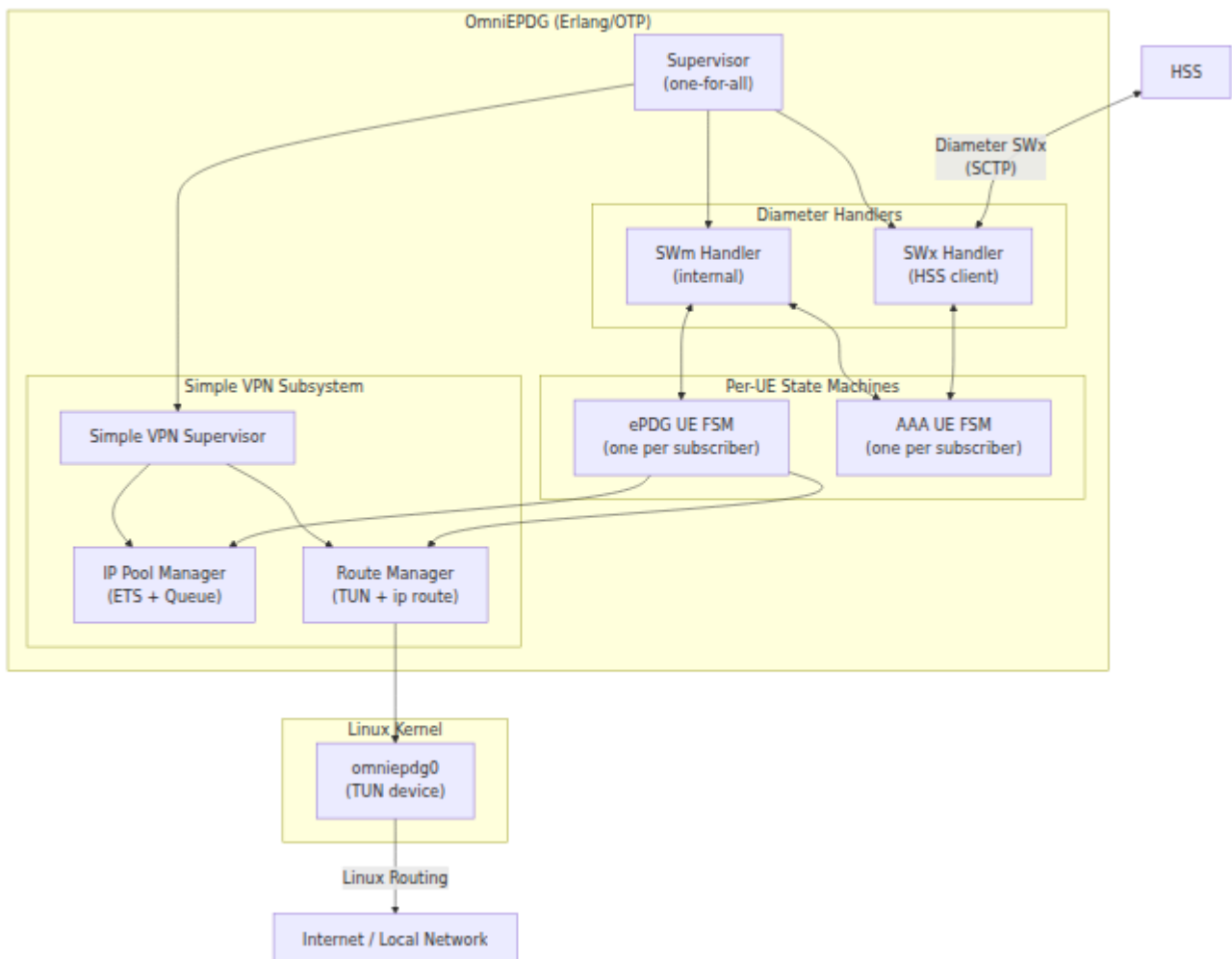
이 FSM은 Erlang `gen_statem` 프레임워크를 사용하여 구현됨

ePDG UE FSM

ePDG UE FSM 프로세스는 `authenticated` 상태를 유지하며

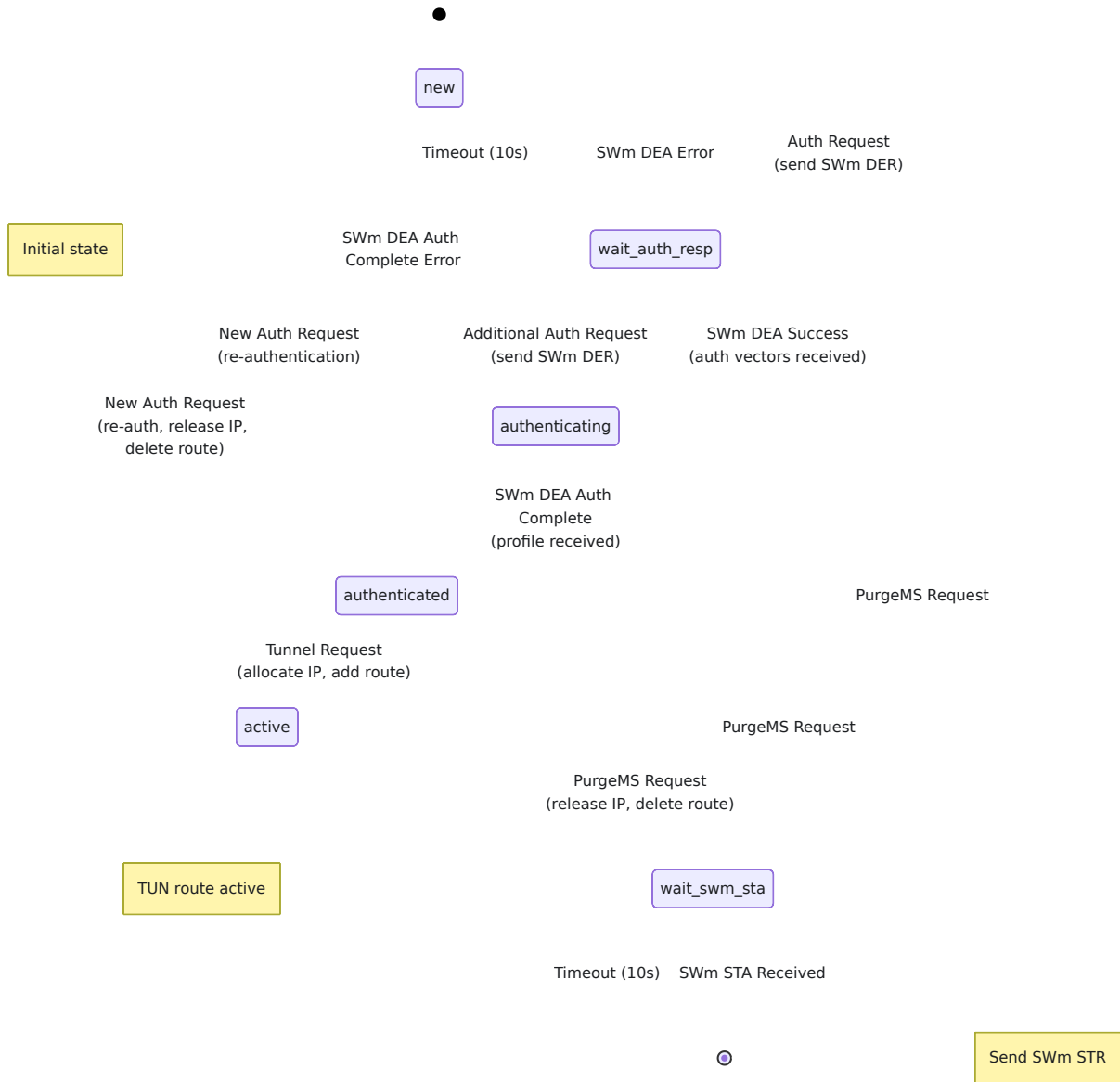
GTP 프로세스 FSM

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



VPN FSM

VPN FSM states: `authenticated`, `active`, `wait_create_session_resp`, `wait_delete_session_resp`, `dereg_pgw_wait_cancel`, `dereg_net_wait_s2b_delete`

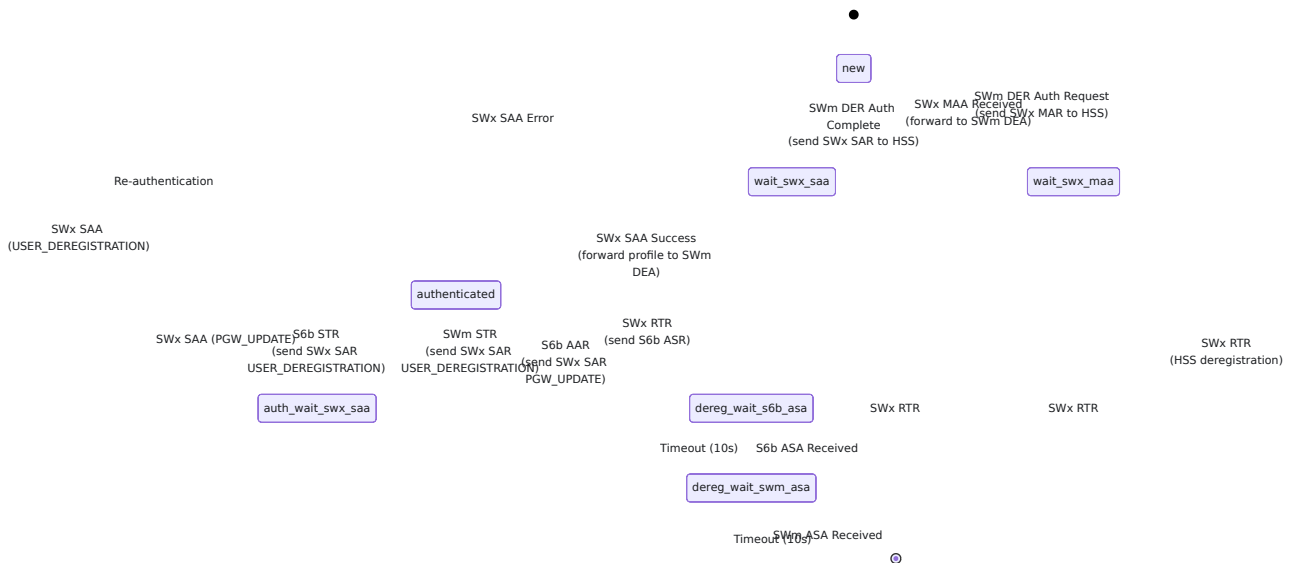


ePDG UE FSM □□□□

□□	□□	□□	□□
new	□□	□□□□□□□□□□□□	□□ UE □□□□ □
wait_auth_resp	□□	□□ SWm DER □□□□□□ □□	SWm DEA □ □□□□□□
authenticating	□□	□□□□□□□EAP □□□□□□	□□□□/□□□□
authenticated	□□	□□□□□□□□□□□□	□□ UE □□□□ □
wait_create_session_resp	GTP	GTPv2-C □□□□□□□□□□ PGW□	PGW □□□□□ □□
active	□□	□□/□□□□□□□□□□□□□□□□	□□□□
wait_delete_session_resp	GTP	GTPv2-C □□□□□□□□□□ PGW□□□□□□□□□□	PGW □□□□□ □□
wait_swm_sta	□□	□□ SWm □□□□□□□	□□ AAA □ SWm STA
dereg_pgw_wait_cancel	GTP	PGW □□□□□□□□□□□□□□ UE□	□□□□□□
dereg_net_wait_cancel	GTP	□□/□□□□ □□□□□□□□□□□□ □□ UE□	□□□□□□
dereg_net_wait_s2b_delete	GTP	□□□□□□□□□□S2b □□□□□□□ □ PGW□	□□□□□□

AAA UE FSM

AAA UE FSM HSS SWx PGW S6b Diameter



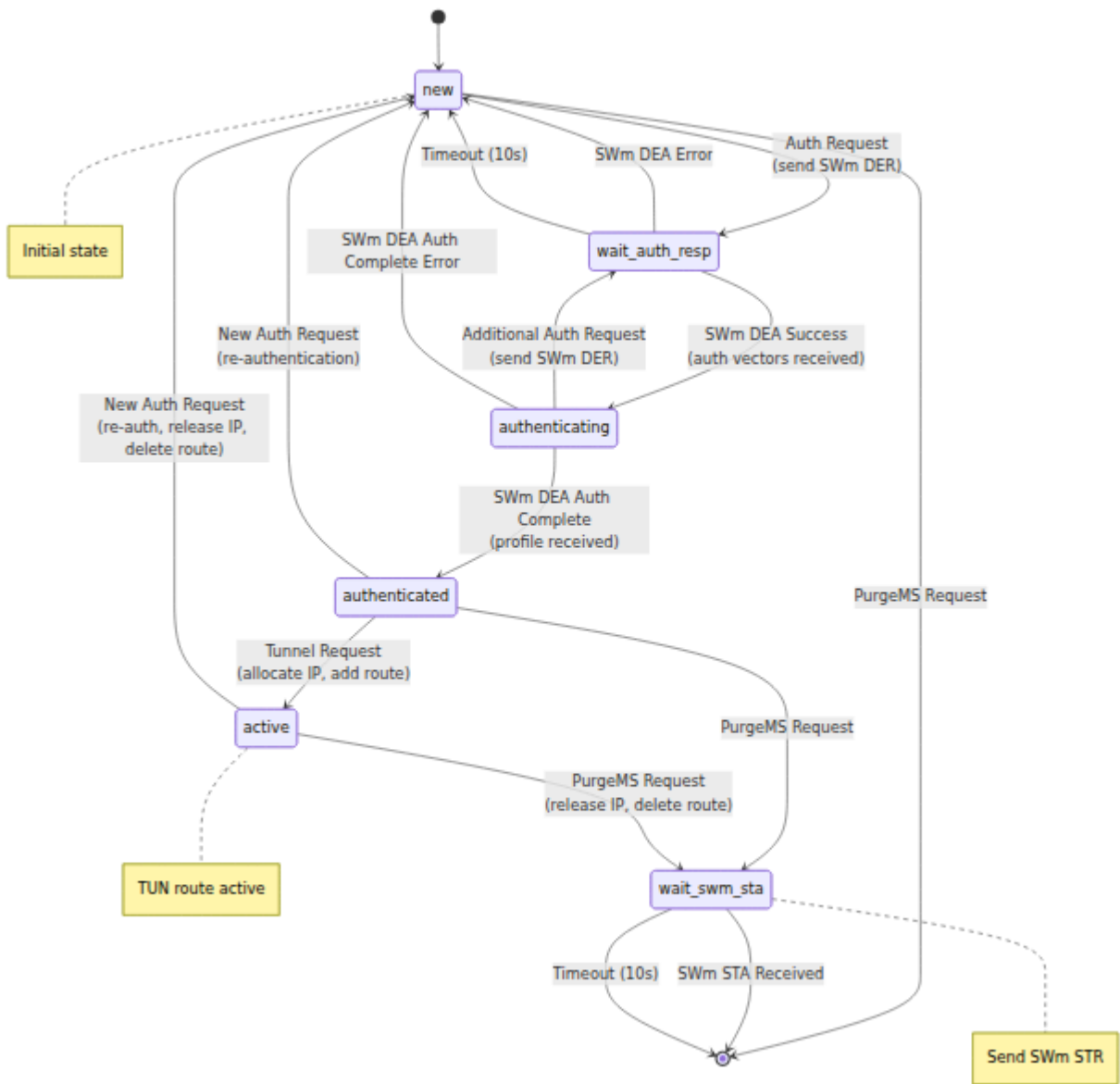
AAA UE FSM □□□□

□□	□□	□□
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	SWx SAR □□□□□ PGW □□□□□□ □□□	□□ HSS □ SWx SAA
dereg_net_wait_s6b_asa	HSS □□□□□□□ S6b ASR □□□ PGW□	PGW □ S6b ASA
dereg_net_wait_swm_asa	S6b □□□□□□ SWm ASR □□□ ePDG□	□□ ePDG □ SWm ASA

□□□□

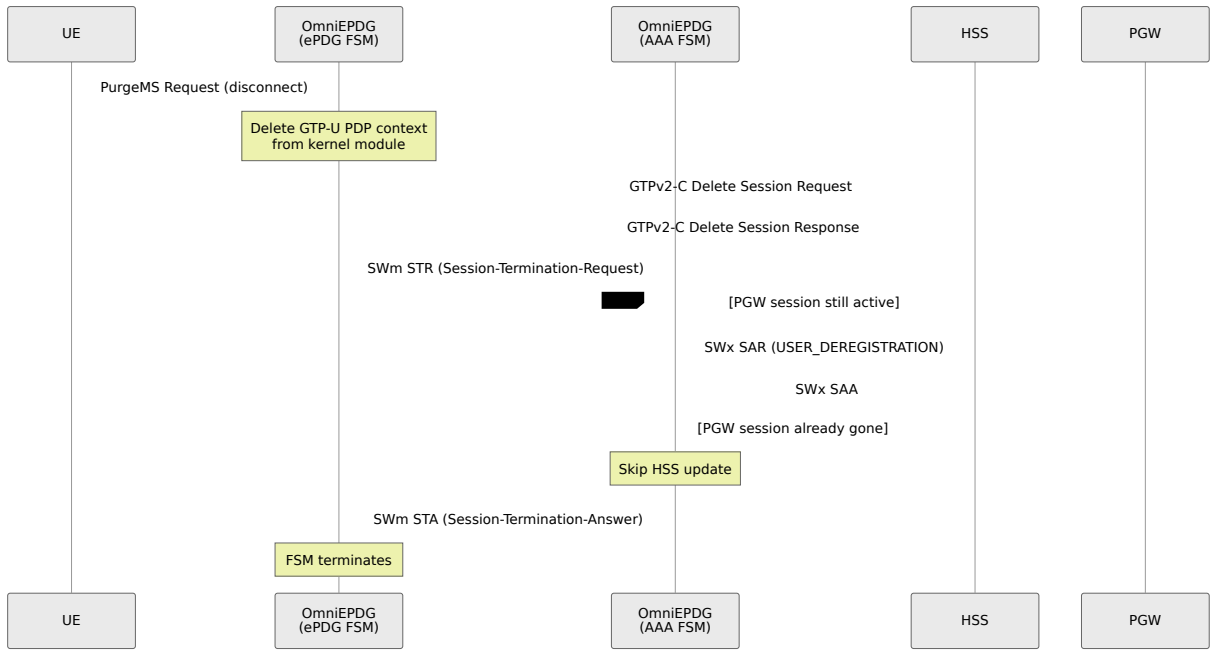
GTP □□□□□□□□□□

□□□□□□□□ EAP-AKA □□□□□ GTP □□□□□□□□□□



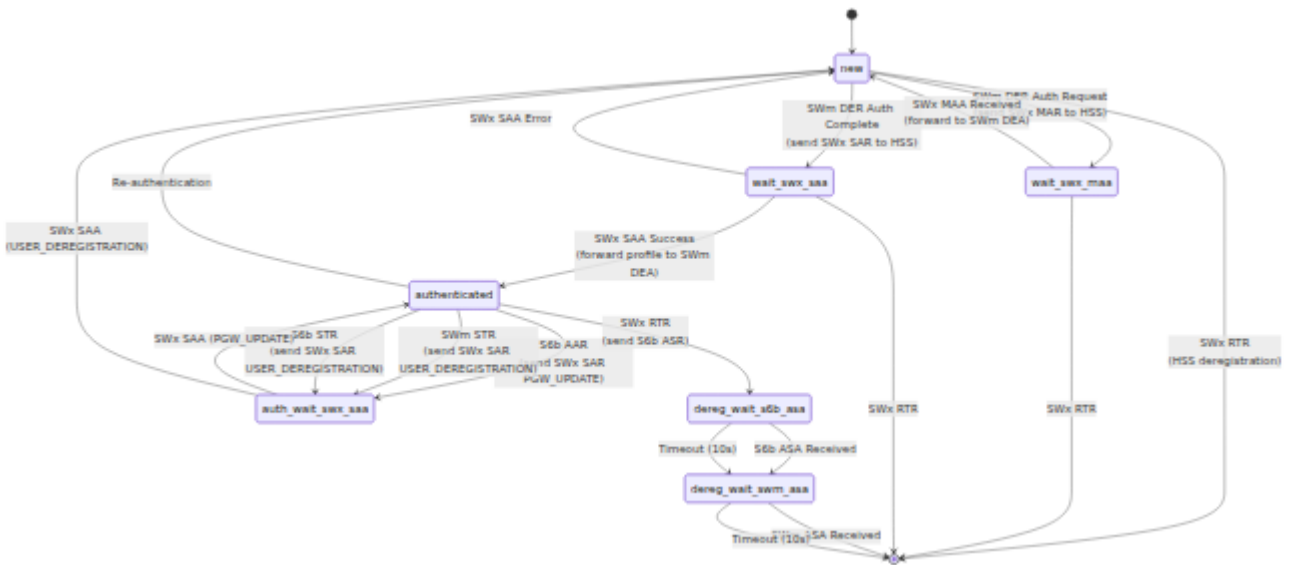
GTP

WiFi



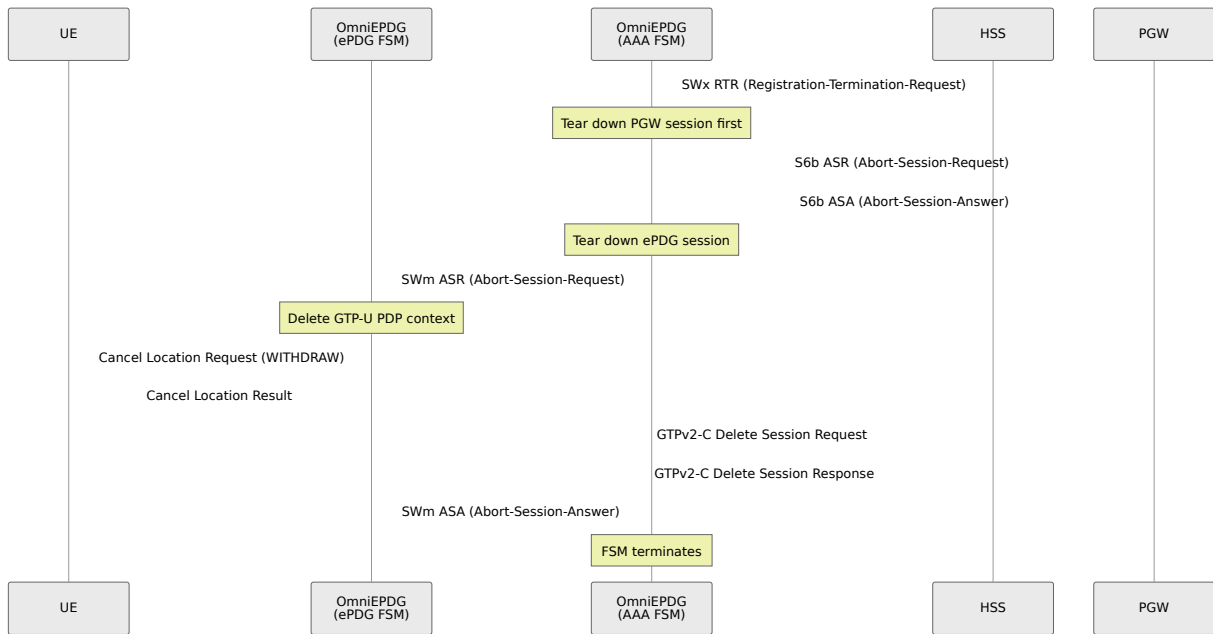
GTP PGW

PGW



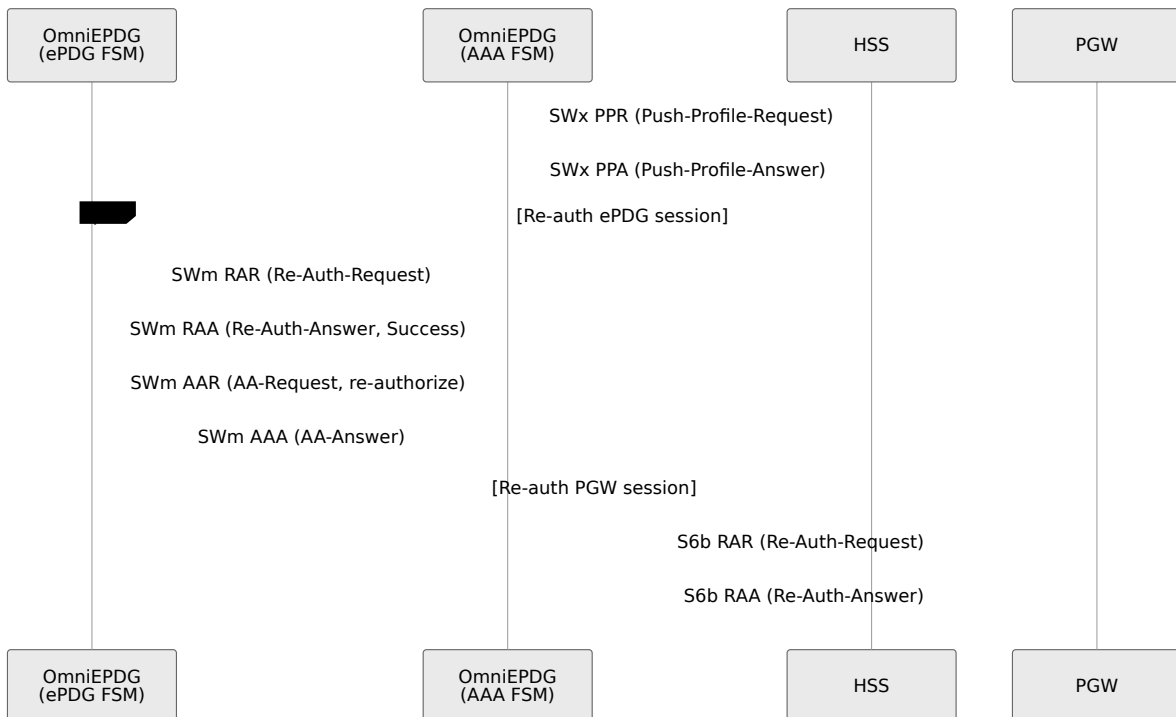
GTP HSS

HSS



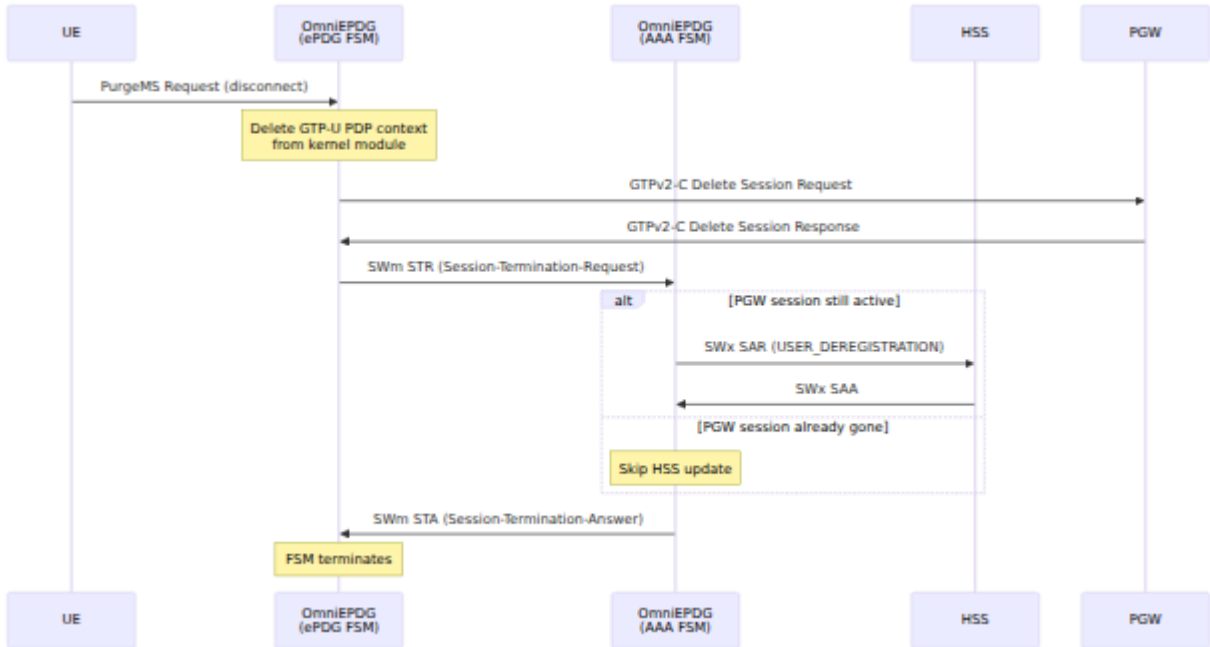
GTP HSS

HSS OmniEPDG ePDG SWm PGW S6b 3GPP TS 29.273 8.1.2.3.3



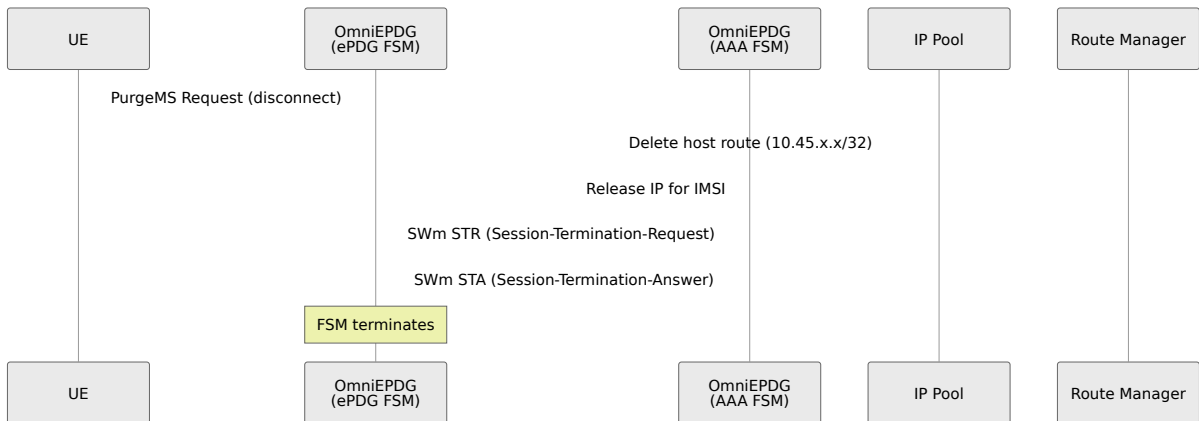
VPN EAP-AKA

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



VPN 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 29.261
5001	DIAMETER_ERROR_USER_UNKNOWN	未知 IMSI 用户 HSS 数据不可用	3GPP TS 29.261
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 29.261
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	漫游不被允许	3GPP TS 29.261
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 29.261
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	接入技术不被允许	3GPP TS 29.261

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

GTPv2-C 프로토콜 GTP 메시지

OmniEPDG 및 PGW 프로토콜/프로시저에서 GTPv2-C 메시지 1-15 및 16-63 메시지
64 프로시저에서 3GPP TS 29.274 8.4 참조

메시지

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

Priority	Protocol	Authentication Method
0	EAP-AKA	AKA over WiFi
6	EAP-AKA'	AKA over IPsec

OmniEPDG Authentication Method 0 EAP-AKA over WiFi

OmniEPDG Authentication Method @ NAI IMSI IMSI

Authentication

OmniEPDG Authentication Method 3GPP TS 33.402 RFC 7296 IKEv2

IKEv2 Authentication

Authentication Method	ID	Key Length	Authentication Method	Reference
AES-CBC	12	128, 192, 256 bits	256 bits	RFC 3602
AES-GCM-16	20	128, 192, 256 bits		RFC 5282
AES-GCM-12	19	128, 192, 256 bits		RFC 5282
AES-GCM-8	18	128, 192, 256 bits		RFC 5282
3DES	3	192 bits		RFC 2451

IKEv2 HMAC

HMAC	ID	Key Length	ICV Length	Key Size	Reference
HMAC-SHA2-256-128	12	256 bits	128 bits	256 bits	RFC 4868
HMAC-SHA2-384-192	13	384 bits	192 bits	256 bits	RFC 4868
HMAC-SHA2-512-256	14	512 bits	256 bits	256 bits	RFC 4868
HMAC-SHA1-96	2	160 bits	96 bits	160 bits	RFC 2404
HMAC-MD5-96	1	128 bits	96 bits	128 bits	RFC 2403

IKEv2 PRF HMAC

PRF-HMAC	ID	Key Length	Key Size	Reference
PRF-HMAC-SHA2-256	5	256 bits	256 bits	RFC 4868
PRF-HMAC-SHA2-384	6	384 bits	256 bits	RFC 4868
PRF-HMAC-SHA2-512	7	512 bits	256 bits	RFC 4868
PRF-HMAC-SHA1	2	160 bits	160 bits	RFC 2104
PRF-HMAC-MD5	1	128 bits	128 bits	RFC 2104

IKEv2 Diffie-Hellman

	ID	bits	group	reference
MODP-2048	14	2048 bits	modp2048	RFC 3526
MODP-1024	2	1024 bits	modp1024	RFC 2409
MODP-1536	5	1536 bits	modp1536	RFC 3526
MODP-3072	15	3072 bits	modp3072	RFC 3526
MODP-4096	16	4096 bits	modp4096	RFC 3526
ECP-256	19	256 bits	secp256r1	RFC 5903
ECP-384	20	384 bits	secp384r1	RFC 5903
ECP-521	21	521 bits	secp521r1	RFC 5903
Curve25519	31	256 bits	curve25519	RFC 8031
Curve448	32	448 bits	curve448	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}
]
}

# 许可证客户端 (runtime.exs)
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

IKEv2 许可证

IKEv2 许可证 UEs 与 OmniEPDG 许可证 SWu 许可证 IPsec 许可证 EAP-AKA 许可证

名前	型	型	値
listen_ip	string	string	{0, 0, 0, 0}
port_500	int	int	500
port_4500	int	int	4500
cert_file	string	string	/etc/omniepdg/certs/epdg.crt

項目	型	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 制限
  auth_rate_limit_per_ip: 10,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 300_000,

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

参数	是否必填	是否可配置	默认值	描述
auth_rate_limit_per_ip	否	否	10	每个IP地址每秒允许的最大认证次数
auth_rate_limit_ip_window_ms	否	否	60000	IP地址认证速率限制的窗口时间，单位为毫秒
auth_rate_limit_ip_block_ms	否	否	300000	IP地址认证速率限制触发后的阻塞时间，单位为毫秒
auth_rate_limit_per_imsi	否	否	5	每个IMSI号码每秒允许的最大认证次数
auth_rate_limit_imsi_window_ms	否	否	60000	IMSI号码认证速率限制的窗口时间，单位为毫秒
auth_rate_limit_imsi_block_ms	否	否	600000	IMSI号码认证速率限制触发后的阻塞时间，单位为毫秒

GeoIP 配置

```

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	備考
<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>	文字列の配列	<code>[]</code>		ISO 3166-1 alpha-2 コード の配列 <code>["AU", "NZ", "US"]</code>
<code>geoup_allow_unknown</code>	ブール値	<code>false</code>		未知のIP アドレスを 許可する かどうか <code>true</code> にする
<code>geoup_fail_open</code>	ブール値	<code>true</code>		GeoIP データベース が読み込 めなかった 場合

VPN 配置

名称	类型	模式	配置	备注
vpn_mode	字符串	simple	EPDG_VPN_MODE	配置为 simple 模式，使用 TUN 接口，IP 地址池使用 gtp 模式，支持 GTPv2-C/GTP-U 隧道，配置 IP 地址池。

配置 VPN 配置

simple_vpn 配置为 VPN 配置，IP 地址池、DNS、OmniEPDG 支持 IPv4 和 IPv6 配置。

```
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	说明
pool_ipv4	IP地址池	IPv4	"10.45.0.0/16"	CIDR 地址池 IPv4 地址池 用于 IPv4 业务
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 用于 IPv4 DNS 业务
dns_servers_ipv6	DNS服务器	IPv6	["2001:4860:4860::8888", "2001:4860:4860::8844"]	PCO 配置 用于 IPv6 DNS 业务
p_cscf_ipv4	IMS P-CSCF	IPv4	[]	VoWiFi 业务 IMS P-CSCF 地址池
p_cscf_ipv6	IMS P-CSCF	IPv6	[]	VoWiFi 业务 IMS P-CSCF 地址池
mtu	MTU		1400	接口 MTU 配置

項目	項目	項目	項目	項目
nat_enabled			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	項目	項目	項目	項目
service_name	項目 項目	項目	:omniepdg	-
listen_ip	項目 項目 項目	項目	"0.0.0.0"	DIA_LIST
listen_port	項目 項目	項目	3868	DIA_LIST
host	項目 項目 項目	項目	"epdg"	DIA_HOST
realm	項目 項目 項目	項目	"epc.mnc001.mcc001.3gppnetwork.org"	DIA_REAL
product_name	項目 項目	項目	"OmniEPDG"	-

項目	種別	単位	値	説明
vendor_id	整数		10415	-

peers

peers Diameter HSS

項目	種別	単位	値	パラメータ	説明
host	文字列		-	HSS_HOST	Diameter Origin-Host
ip	文字列		-	HSS_IP	IP TCP/SCTP
port	整数		3868	HSS_PORT	Diameter
transport	文字列		: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"	ライセンス製品名

Web コンソール

Web コンソールの設定

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

Port	Protocol	Direction	Port	Environment Variable	Access Method
port	HTTP	Outgoing	4000	CONTROL_PANEL_PORT	Web UI HTTP

Prometheus Configuration

OmniEPDG HTTP Prometheus Configuration

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

Port	Protocol	Direction	Port	Environment Variable	Access Method
port	HTTP	Incoming	9568	PROMETHEUS_PORT	Prometheus /metrics HTTP

Configuration

Configuration

- `epdg_ikev2_session_initiated_count` - IKE_SA_INIT
- `epdg_ikev2_session_established_count` - IKE SAs
- `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` - AA

- `epdg_diameter_s6b_str_count` - 会话数
- `epdg_session_created_count` - 会话创建数 `vpn_mode`
- `epdg_session_terminated_count` - 会话终止数
- `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

会话数 5 会话数

- `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

会话持续时间

- `epdg_auth_duration_ms` - 认证持续时间
- `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 会话

- `vm_memory_total` - VM 内存总量
- `vm_memory_processes` - VM 进程数
- `vm_memory_binary` - VM 二进制文件数
- `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 会话

```

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

```

FSM

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 DER/DEA, STR/STA
S6b	10,000 ms	GTP	AAA UE FSM	Diameter S6b ASR/ASA

Configuration

Configuration file: `config/runtime.exe`

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	View active UE sessions
<code>/diameter</code>	Diameter	Diameter interface details
<code>/logs</code>	GET	System logs
<code>/docs</code>	GET	API documentation
<code>/resources</code>	GET	BEAM VM resources
<code>/configuration</code>	GET	System configuration

API

OmniEPDG API endpoints and methods

Table 1

Table 1: UE categories and their characteristics

Category	Characteristics
Category 1	Low power UE
Category (UL)	Low power UEs
Category (DL)	Low power UEs
Diameter	Low power / Low power

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** - Low power Diameter
- Category - Low power
- - Low power

Table 3

Table 3: UE categories and their characteristics

項目	説明
VPN 種別	標準 GTP 型 SIMPLE
IKEv2 種別	標準 500 (IKE), 4500 (NAT-T)
Diameter 種別	標準 Diameter 型
IP 種別 (IPv4)	標準 IP 型 CIDR 型 VPN 型

標準

標準

標準

標準 UE 標準

標準 UE 標準

□□□□

□□□□□□□□

□	□□
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
Connected	
Last Activity	
Duration	

概要

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

注

詳細については、

- "IMS" の
- IMS の UE

参照

関連する情報は、

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	値
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	値
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 Prometheus Grafana 监控系统

□□

□ config/runtime.exs □□❖❖□□□□

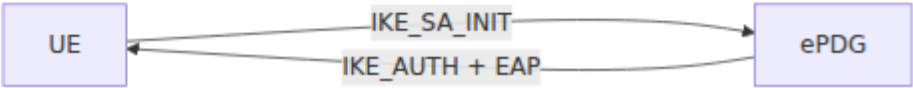
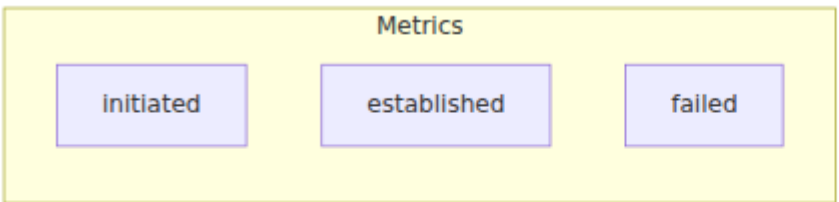
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

□□	□□	□□□	□□□□	□□
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

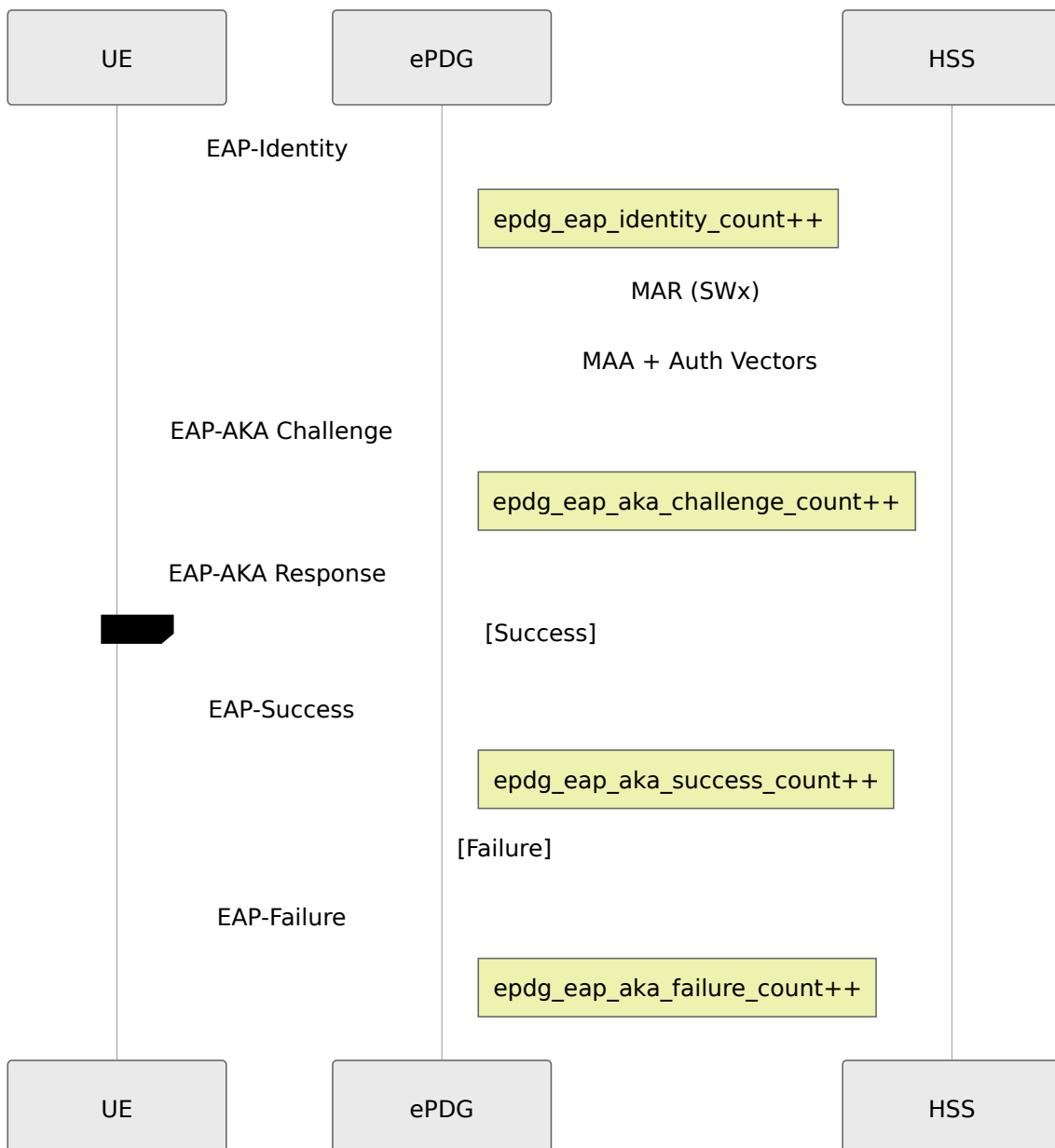
log: IKE SA log

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 EAP-Identity 计数

计数器: epdg_eap_aka_challenge_count

单位: 计数

描述: UE EAP-AKA 挑战计数

计数器: epdg_eap_aka_success_count

单位: 计数

描述: EAP-AKA 成功计数

计数器: epdg_eap_aka_failure_count

单位: 计数

描述: EAP-AKA 失败计数

原因:

- reason - res_mismatch, invalid_identity, authentication_rejected
-

计数器: epdg_eap_aka_sync_failure_count

单位: 计数

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

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 验证失败计数

SQL: `epdg_auth_rate_limited_count`

SQL: `SQL`

SQL: `SQL`

SQL:

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

SQL:

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

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

SQL: `epdg_auth_geoip_blocked_count`

SQL: `SQL`

SQL: `GeoIP`

SQL:

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

SQL:

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

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

SQL: `epdg_esp_replay_detected_count`

SQL: `SQL`

SQL: `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

명: `epdg_sessions_active_count`

명: 명

명: 명명명명명명명명 5 명명명명

명: `epdg_sessions_by_state_count`

명: 명

명: 명 FSM 명명명명명

명:

- `state` - 명명명명명명 `init` `eap_identity` `eap_aka_challenge` `authenticated` `established`
-

명: `epdg_auth_duration_ms`

명: 명

명: 명 IKE_SA_INIT 명명명명명명명명명명명명명명

명: 100, 250, 500, 1000, 2500, 5000, 10000 ms

명: `epdg_session_duration_seconds`

명: 명

명: 명명명명명명명명명명

명: 60, 300, 900, 1800, 3600, 7200, 14400 seconds `1` 명명 4 명

ESP 명명명명

명 RFC 4303 명 ESP 명명명명명

명: `epdg_esp_packets_in_count`

명: 명

명: 명명명명 ESP 명명명명명 UE → 명명명명

명: `epdg_esp_packets_out_count`

명: 명

명: 명명명명 ESP 명명명명명명명명명명 → UE 명명

名称: epdg_esp_bytes_in_total

单位: 字节

描述: ESP 字节数

名称: epdg_esp_bytes_out_total

单位: 字节

描述: ESP 字节数

IP 地址

VPN 地址 IP 地址

名称: epdg_ip_allocated_count

单位: 计数

描述: IP 地址

名称:

- type - 地址类型 ipv4 或 ipv6
-

名称: epdg_ip_released_count

单位: 计数

描述: IP 地址

名称:

- type - 地址类型 ipv4 或 ipv6
-

名称: epdg_ip_pool_allocated_count

单位: 计数

描述: IP 地址

名称: epdg_ip_pool_available_count

单位: 计数

描述: IP 地址

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 或 1.0 以上

VM 内存

用于 Erlang/BEAM 的内存

名称: vm_memory_total

单位: 字节

范围: 0

说明: VM 总内存

名称: vm_memory_processes

单位: 字节

范围: 0

说明: Erlang 进程内存

名称: vm_memory_binary

单位: 字节

范围: 0

说明: 二进制数据内存

名称: vm_memory_ets

单位: 字节

范围: 0

说明: ETS 内存

名称: vm_system_info_process_count

单位: 进程数

说明: 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: "速率过高"
  description: "速率过高"

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

"

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

"

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

# AUTH 速率过高 MITM
- 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"
```


IMS I

参数	单位	默认值	描述
auth_rate_limit_per_imsi	个	5	每 IMSI 允许的认证速率 IP 地址
auth_rate_limit_imsi_window_ms	毫秒	60000	IMS I 认证的窗口时间
auth_rate_limit_imsi_block_ms	毫秒	600000	IMS I 认证的阻塞时间 10 个 IP 地址

配置

配置 IP/IMS I 认证的速率、窗口时间和阻塞时间。

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 IMSI 认证速率 5 个 IP 地址 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

00	0 0	0 0	00	00
<code>geop_enabled</code>	0 0	0	<code>false</code>	00000000 GeoIP 00000000 00 <code>false</code> 000 0 IP 0000000000 0000
<code>geop_database_path</code>	0 0 0	0	<code>"/etc/omniepdg/GeoLite2-Country.mmdb"</code>	MaxMind GeoLite2 0000 000000000000 MMDB0
<code>geop_mode</code>	0 0	0	<code>:whitelist</code>	000000 00 :whitelist 000000000000 :blacklist00 00000000000000 0000
<code>geop_countries</code>	0 0	0	<code>[]</code>	ISO 3166-1 alpha-2 000000 0000000000 <code>geop_mode</code> 0
<code>geop_allow_unknown</code>	0 0	0	<code>000</code>	00000000000000 0 IP 00000000 IP000000000000 00000000 <code>false</code> 00000000 000000 <code>true</code> 0
<code>geop_fail_open</code>	0 0	0	<code>true</code>	GeoIP 00000000 0000000000

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
```

IP 設定 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
```

UE 設定

設定

IP Whitelisting

IP Whitelisting

- 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.

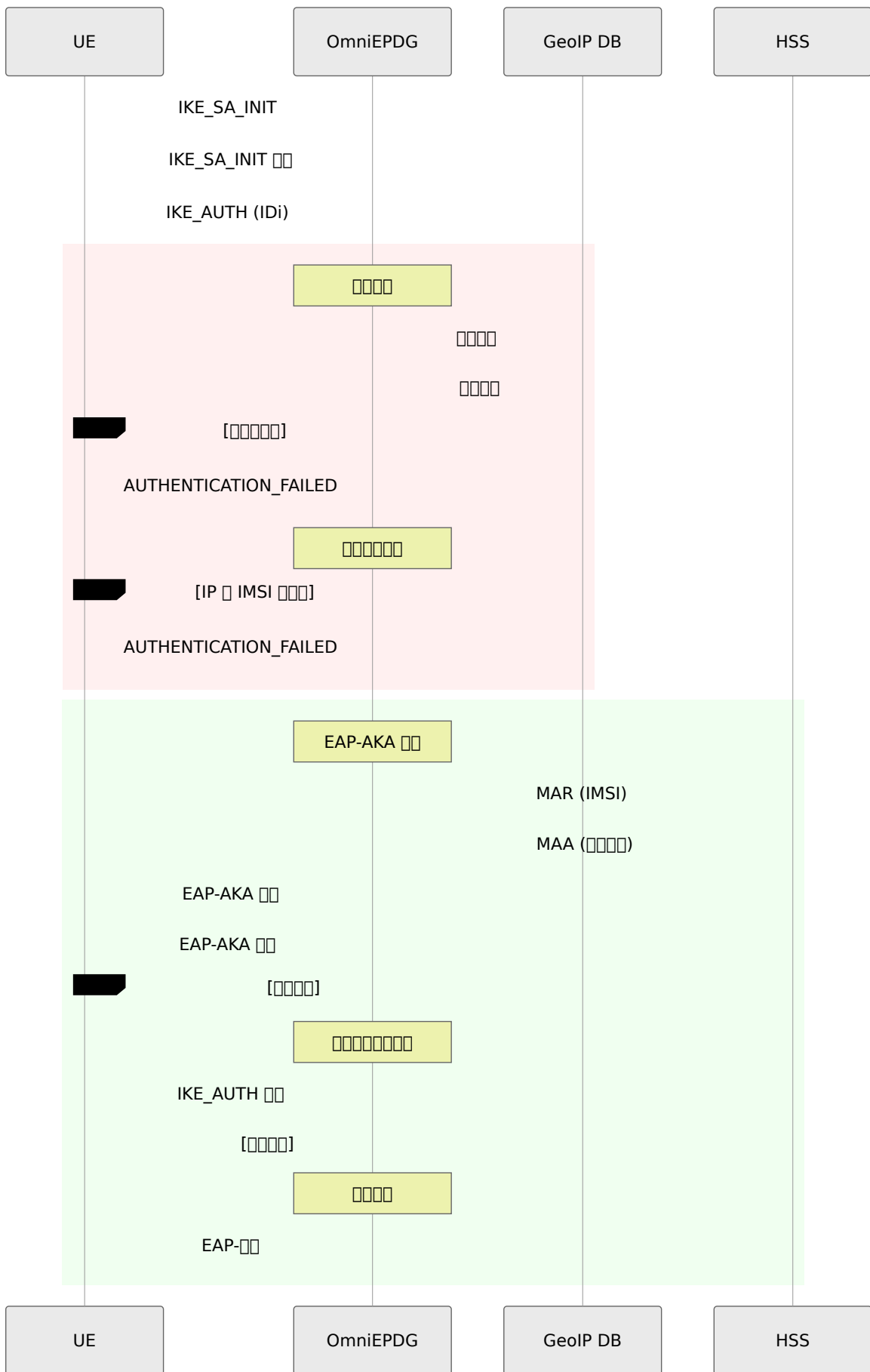
□□□□□□

□□	□□	□□	□□
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

確認事項

前提: GeoIP データ UE あり

設定:

- GeoIP データあり
- GeoIP データあり
- `geop_allow_unknown: false` 不明な IP

手順:

1. GeoIP データあり
2. GeoIP データあり2 確認
3. 設定/確認 `geop_allow_unknown: true`
4. GeoIP データあり

GeoIP 設定

前提: GeoIP データあり

設定:

- GeoIP データあり
- GeoIP データあり
- GeoIP データあり MMDB あり

手順:

1. 確認 `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. 設定 `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. GeoIP MaxMind データあり

確認事項

前提: GeoIP データあり

□□□□:

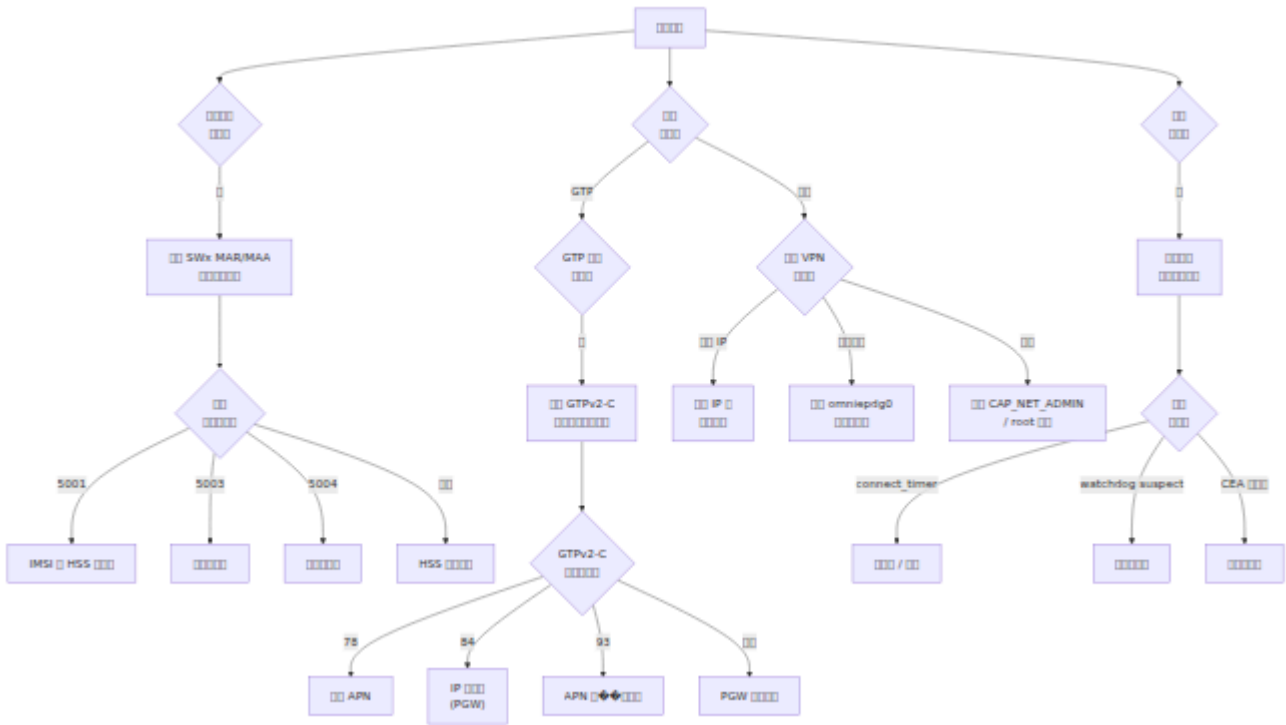
- VPN/□□□ IP □□□□□□□□
- GeolP □□□□□
- □□□□□□□□□□

□□□□:

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

OmniEPDG

OmniEPDG



OmniEPDG log/

파일	내용	설명
log/console.log	콘솔 로그	디버깅용 로그
log/error.log	에러 로그	에러 발생 시 기록되는 로그
log/crash.log	OTP 에러 로그	OTP 런타임 에러 로그
log/erlang.log	Erlang 에러 로그	Erlang/OTP 에러 로그

로그 파일

로그 파일

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

UE FSM 로그

- 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 로그

HSS 로그 (SWx)

SWx 로그는 HSS 로그를 포함합니다.

□□□□

- □□□□ 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 □□□□□□□□ PGW □□□□ S6b AAR□□□□□□□□ S6b peer_up □□□

□□□□

- PGW □□□□□□□□ OmniEPDG □ S6b □□□
- □□□□□□□□ OmniEPDG □ S6b □□□□□□□□ SCTP □□ 3868
- PGW □□□□ `dia_s6b_local_ip`
- 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 EAP-AKA EAP-AKA'
- HSS EAP

3GPP TS 23.003 NAI

- EAP-AKA
- EAP-AKA'

OmniEPDG UE WiFi UE EAP-AKA

1. UE NAI
2. HSS
3. SIM

EAP-AKA RES

"RES" "res_mismatch"

- SIM
- UE
- HSS

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

GTP 隧道 (GTP 隧道)

PGW 隧道

PGW 隧道 GTPv2-C 隧道

隧道

隧道 ID	隧道名称	隧道描述
78	APN 隧道	APN 隧道 PGW 隧道
82	RAT 隧道	PGW 隧道 WiFi 3GPP 隧道
84	隧道	PGW IP 隧道
92	隧道	PGW 隧道 S6b 隧道
93	APN 隧道	隧道 PGW 隧道 APN
96	IMSI/IMEI 隧道	隧道 PGW 隧道 S6b 隧道
113	APN 隧道	APN 隧道 PGW 隧道
120	GTP-C 隧道	PGW 隧道

隧道

隧道 10 隧道 Timeout create_session_timeout 隧道 state_wait_create_session_resp 隧道

VPN (VPN)

TUN

OmniEPDG `omniepdg0` `simple_vpn_route`

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

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

IP

`simple_vpn_pool` IP

- CIDR
- IP
-

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

编译选项

编译选项

编译OmniEPDG 编译选项

编译选项

- 编译选项
- 编译选项 `gen_socket`
- 编译选项

编译选项

1. 编译 `log/crash.log` 编译选项
2. 编译 `gen_socket` 编译选项 `libdir` 编译选项
3. 编译 `config/runtime.exs` 编译选项
4. 编译选项

编译选项

编译Erlang VM 编译选项

编译选项

- UE FSM 编译选项
- 编译选项
- 编译选项

编译选项

1. 编译选项 `epdg_ue_fsm` 编译选项 `aaa_ue_fsm` 编译选项
2. 编译 FSM 编译选项 `terminating` 编译选项
3. 编译选项

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 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 实现

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

实现

- 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 实现 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