بنية OmniEPDG وتدفقات المكالمات

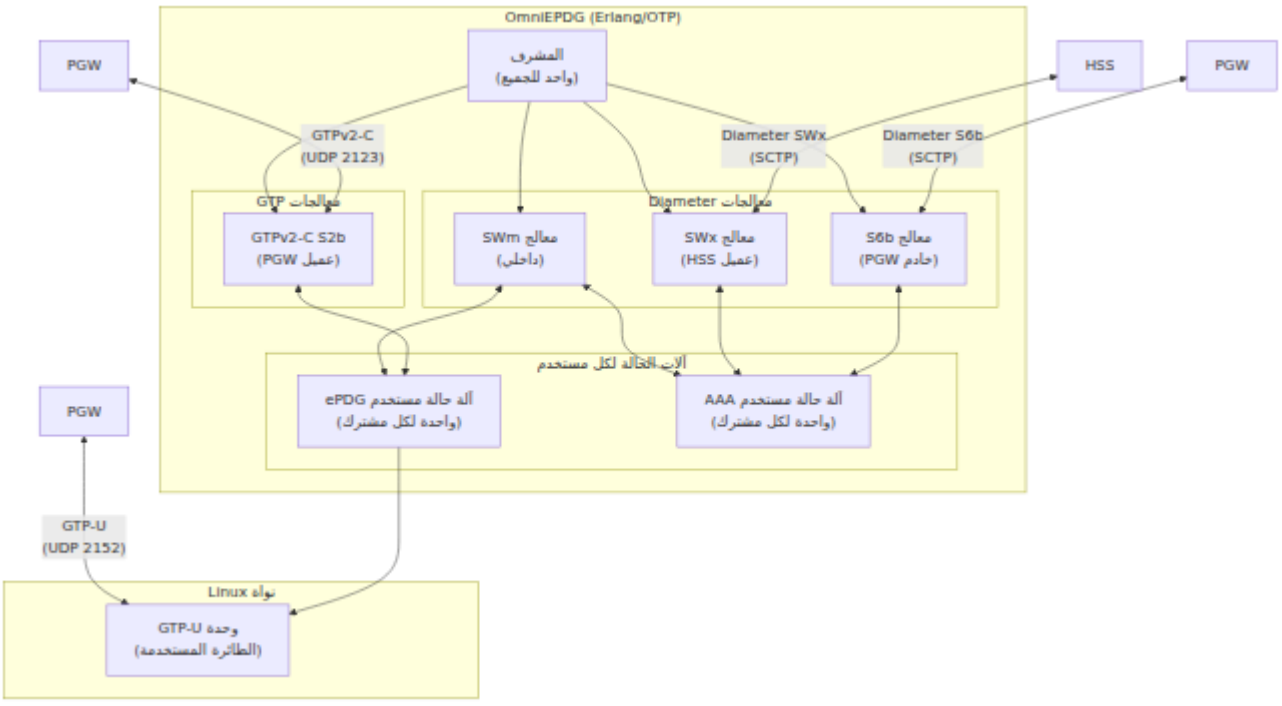
تصف هذه الوثيقة البنية الداخلية لـ OmniEPDG، وآلات الحالة الخاصة، وواجهات البروتوكول، ومخططات تسلسل الرسائل التفصيلية للإجراءات الرئيسية. يدعم OmniEPDG بالمستخدم، ومخططات تسلسل الرسائل التفصيلية للإجراءات الرئيسية. يدعم اختراق محلي مع (**بسيط VPN** و **وضع** PGW) نفق كامل عبر (**GTP** وضعين تشغيليين: **وضع** واجهة TUN). انظر إلى دليل العمليات لمقارنة عالية المستوى.

بنية النظام

تم بناء OmniEPDG على Erlang/OTP 3 ويطبق وظيفة الشبكة GPP ePDG (بوابة بيانات الحزمة) إلى الشبكة الأساسية المحمولة، مما يسمح WiFi إنه يربط الوصول غير الموثوق لشبكة (المتطورة. للمستخدمين بإجراء واستقبال مكالمات VoWiFi.

بنية وضع GTP

في وضع GTP، يتم نفق حركة مرور المشتركين عبر PGW باستخدام GTPv2-C للتحكم في الجلسة ووحدة GTP-U في نواة Linux للطائرة المستخدمة.



بسيط VPN بنية وضع

في وضع VPN بسيط، يتم توجيه حركة مرور المشتركين محليًا عبر واجهة TUN في Linux. لا يتطلب الأمر بنية GTP-U وGTPv2-C وDiameter S6b أو PGW GTP. يتم استبدال مكونات بسيط VPN بنظام.

شجرة المشرف

يستخدم OmniEPDG استراتيجية مشرف **واحد للجميع**، مما يعني أنه إذا تعطل أي عملية فرعية، يتم إعادة تشغيل جميع العمليات الفرعية. يبدأ المشرف بشكل مشروط عمليات فرعية مختلفة اعتمادًا على الوضع التشغيلي.

العمليات التي تبدأ في كلا الوضعين:

العملية	الدور	الوصف
`aaa_diameter_swx`	عميل Diameter SWx	يتصل بـ HSS وعمليات لأغراض المصادقة وملف المشترك
`aaa_diameter_swm`	SWm Diameter (داخلي)	يوجه رسائل EAP وsession Diameter بين ePDG وآلات حالة AAA
`epdg_diameter_swm`	معالج SWm ePDG	يتعامل مع جانب ePDG من إشارات SWm الداخلية Diameter

عمليات إضافية في وضع GTP:

العملية	الدور	الوصف
`aaa_diameter_s6b`	خادم Diameter S6b	يقبل الاتصالات من PGW لتفويض الجلسة
`epdg_gtpc_s2b`	عميل GTPv2-C	يرسل طلبات إنشاء/حذف جلسة إلى PGW عبر S2b
`gtp_u_kmod`	معالج نواة GTP-U	يدير سياقات PDP GTP-U في وحدة نواة Linux

عمليات إضافية في وضع VPN بسيط:

العملية	الدور	الوصف
`simple_vpn_supervisor`	مشرف نظام VPN	يشرف على عمليات مدير مجموعة IP ومدير المسار
`simple_vpn_pool`	مدير مجموعة IP	يخصص ويفرج عن عناوين IPv4 من مجموعة CIDR المكونة باستخدام ETS
`simple_vpn_route`	مدير المسار	ينشئ واجهة TUN `omniepdg0` ويدير مسارات المضيف لكل مشترك

آلات الحالة لكل مستخدم

لكل مشترك نشط (معرف بواسطة IMSI)، ينشئ OmniEPDG آلات الحالة حالتين من:

- **آلة حالة مستخدم ePDG** (`epdg_ue_fsm`) - تدير دورة حياة جلسة المشترك من منظور ePDG: إنشاء نفق GTP، المصادقة، وتنسيق الإنهاء
- **آلة حالة مستخدم AAA** (`aaa_ue_fsm`) - تدير الإشارات من جانب AAA: تبادلات Diameter SWx مع HSS وتبادلات S6b مع PGW

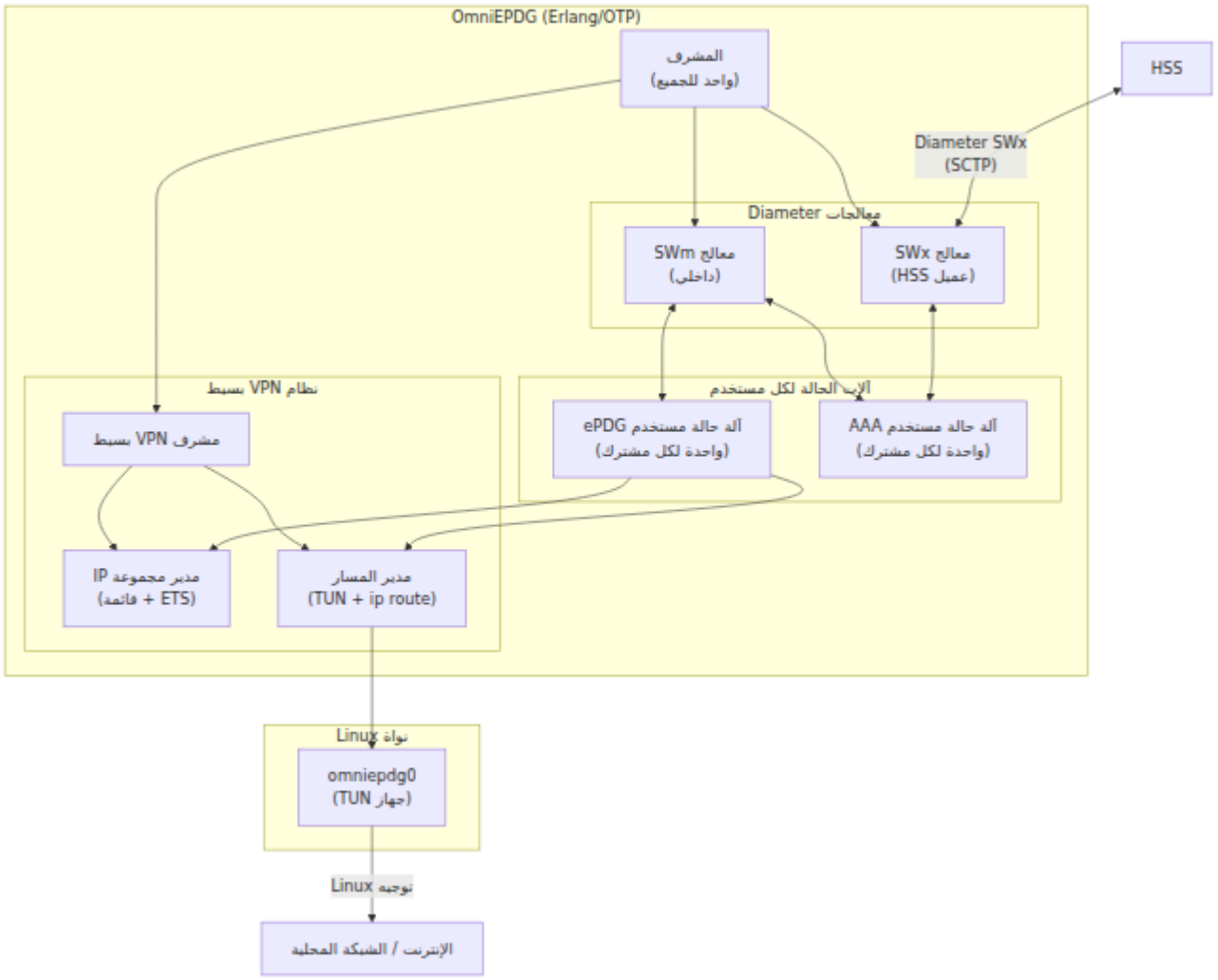
تتم تنفيذ كلا الآلتين كعمليات `gen_statem` في Erlang مع وضع رد نداء وظيفة الحالة.

حالات آلة حالة مستخدم ePDG

تتبع آلة حالة مستخدم ePDG جلسة المشترك من طلب المصادقة الأولي إلى حالة النفق النشط بناءً على الوضع التشغيلي `authenticated`. في حالة FSM سلوك diverge إلى الإنهاء. يت.

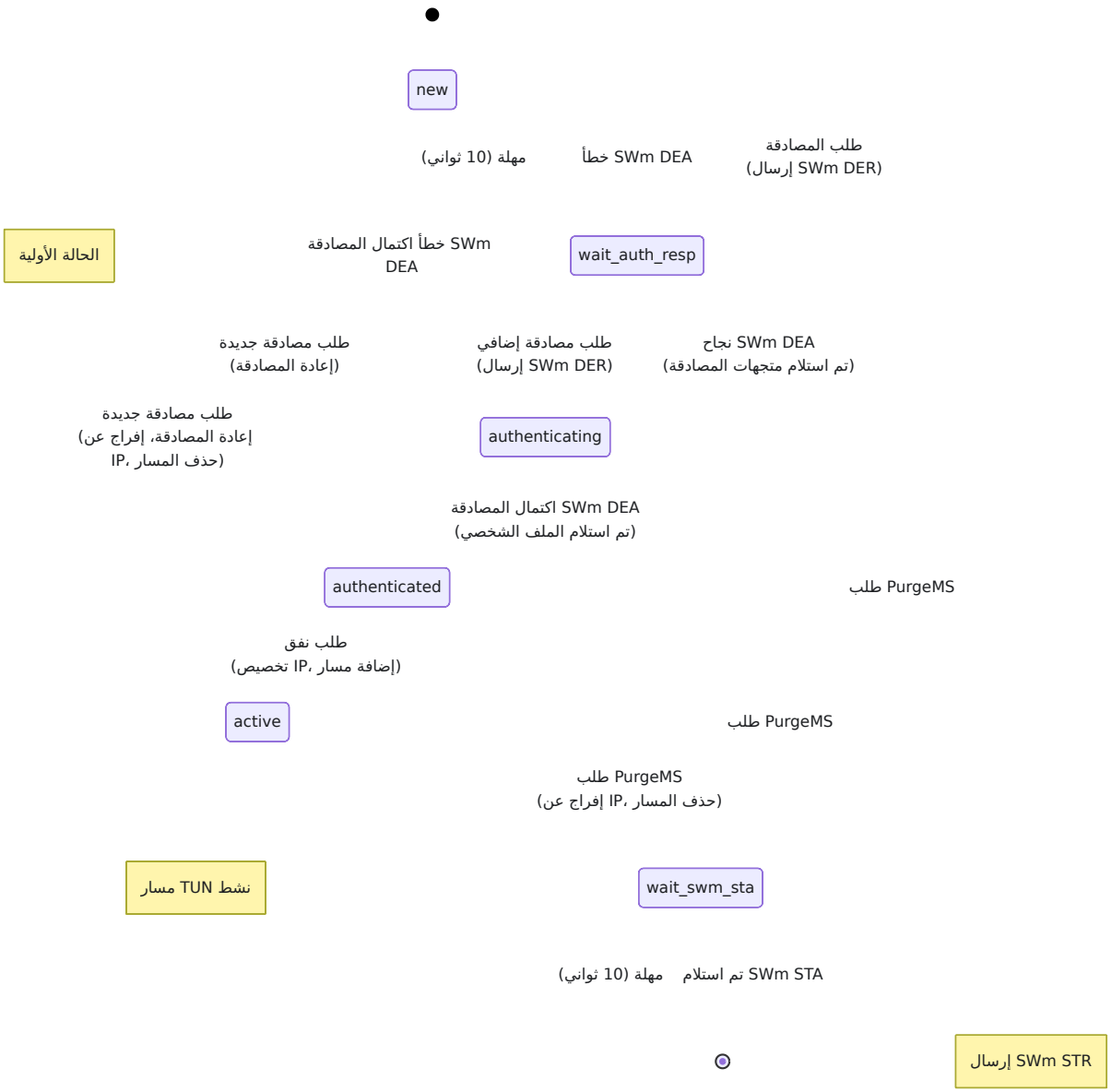
وضع GTP FSM

يمر إنشاء النفق عبر GTPv2-C Create Session إلى PGW، في وضع GTP، ويتضمن الإنهاء وتدفقات إلغاء التسجيل التي تبدأ من PGW، وحذف حامل بدء GTPv2-C Delete Session، HSS.



وضع FSM بسيط VPN

في وضع VPN بسيط، تأخذ FSM في حالة `authenticated` اختصارًا بدلاً من إرسال طلب إنشاء جلسة GTPv2-C، تقوم FSM بتخصيص عنوان IP من المجموعة المحلية، وإنشاء مسار مضيف على واجهة TUN، وتنتقل مباشرة إلى `active`. لا يتم استخدام حالات الإنهاء الخاصة بـ GTP (`wait_create_session_resp`، `wait_delete_session_resp`، `dereg_pgw_wait_cancel`، `dereg_net_wait_s2b_delete`).


new
طلب المصادقة
(إرسال SWm DER)
خطأ SWm DEA
مهلة (10 ثواني)
wait_auth_resp
نجاح SWm DEA
(تم استلام متجهات المصادقة)
طلب مصادقة إضافي
(إرسال SWm DER)
طلب مصادقة جديدة
(إعادة المصادقة)
authenticating
اكتمال المصادقة SWm DEA
(تم استلام الملف الشخصي)
طلب مصادقة جديدة
(إعادة المصادقة، إفراج عن IP، حذف المسار)
خطأ اكتمال المصادقة SWm DEA
الحالة الأولية
authenticated
طلب PurgeMS
طلب نفق
(إضافة مسار IP، تخصيص)
active
طلب PurgeMS
طلب PurgeMS
(إفراج عن IP، حذف المسار)
wait_swm_sta
تم استلام SWm STA
مهلة (10 ثواني)
إرسال SWm STR
نشط TUN مسار

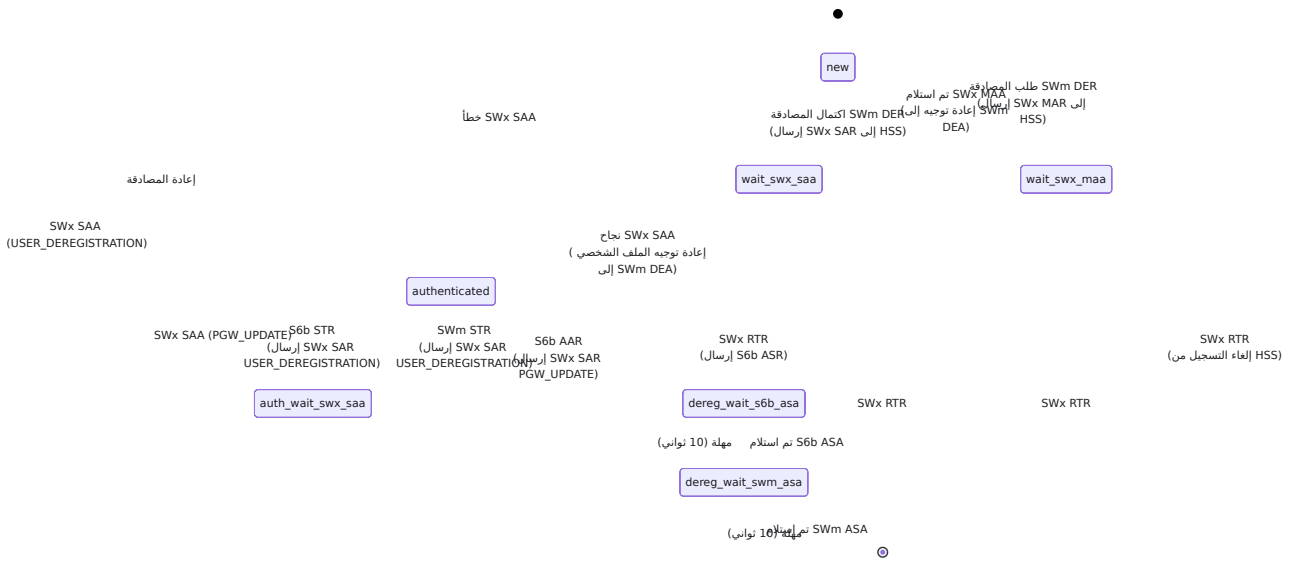
مرجع حالة آلة حالة مستخدم ePDG

الحالة	الوضع	الوصف	الانتظار لـ
`new`	كلاهما	الحالة الأولية. لا توجد جلسة نشطة.	طلب المصادقة من UE
`wait_auth_resp`	كلاهما	تم إرسال طلب المصادقة عبر SWm DER.	SWm DEA مع متجهات المصادقة أو خطأ
`authenticating`	كلاهما	تم استلام متجهات المصادقة، تبادل EAP جارٍ.	تحديث الموقع / اكتمال المصادقة
`authenticated`	كلاهما	اكتمال المصادقة، تم تنزيل ملف المشترك.	طلب النفق من UE
`wait_create_session_resp`	GTP	تم إرسال طلب GTPv2-C Create Session إلى PGW.	استجابة إنشاء الجلسة من PGW
`active`	كلاهما	النفق/المسار نشط. تتدفق حركة مرور المشترك.	مشغل الإنهاء
`wait_delete_session_resp`	GTP	تم إرسال طلب GTPv2-C Delete Session إلى PGW (إنهاء بدء UE).	استجابة حذف الجلسة من PGW
`wait_swm_sta`	كلاهما	تم إرسال طلب إنهاء جلسة SWm.	SWm STA من AAA
`dereg_pgw_wait_cancel`	GTP	إلغاء التسجيل الذي يبدأ تم إرسال .PGW من	نتيجة إلغاء الموقع

الحالة	الوضع	الوصف	الانتظار لـ
		إلغاء الموقع إلى UE.	
`dereg_net_wait_cancel`	GTP	إلغاء التسجيل الذي يبدأ من الشبكة/HSS. تم إرسال إلغاء الموقع إلى UE.	نتيجة إلغاء الموقع
`dereg_net_wait_s2b_delete`	GTP	إلغاء التسجيل الذي يبدأ من الشبكة. تم إرسال S2b Delete Session إلى PGW.	استجابة حذف الجلسة

حالات آلة حالة مستخدم AAA

نيابة عن كل PGW (S6b)و HSS (SWx) نحو Diameter الإشارات AAA تدير آلة حالة مستخدم مشترك.



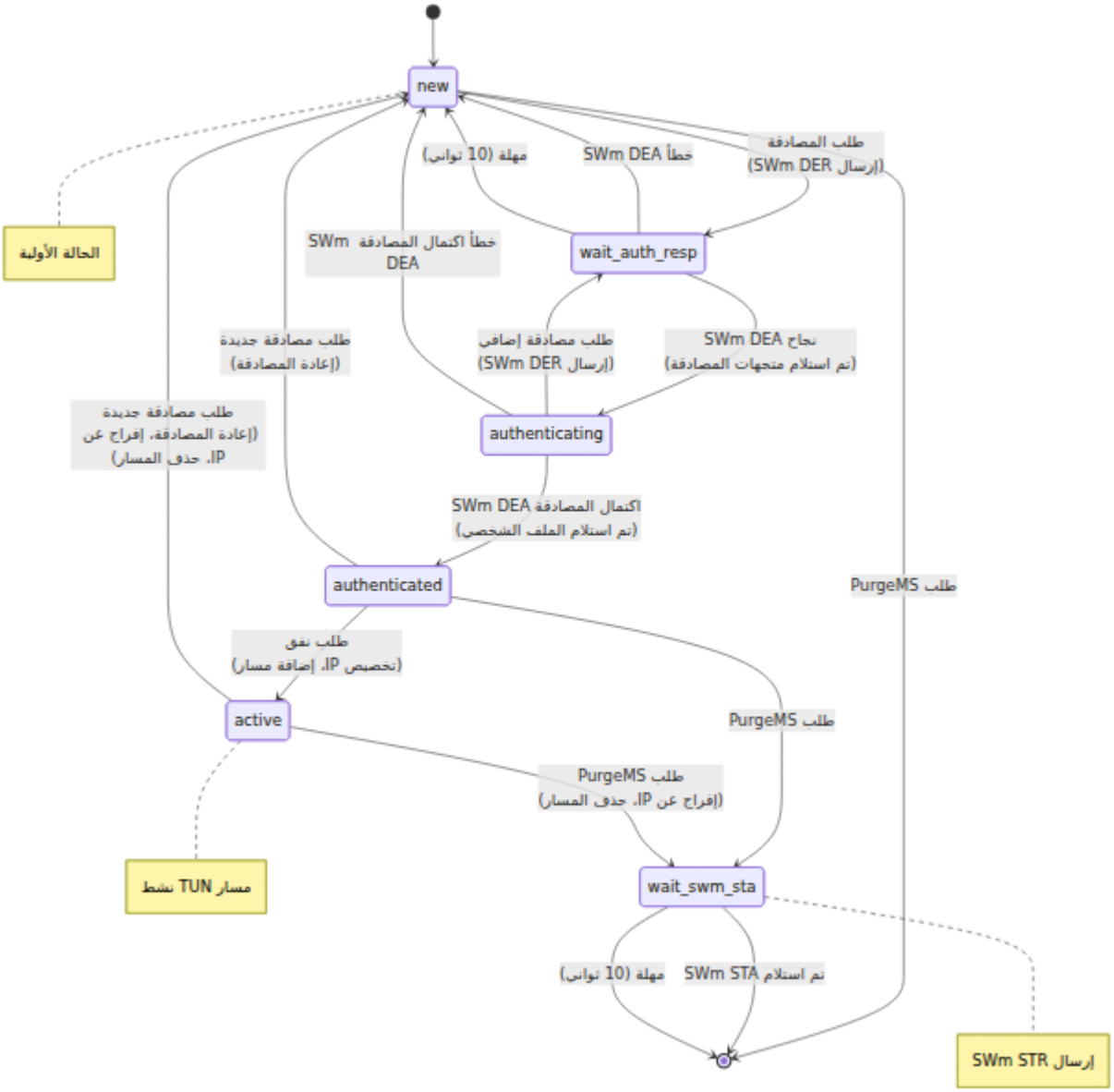
مرجع حالة آلة حالة مستخدم AAA

الحالة	الوصف	الانتظار لـ
`new`	الحالة الأولية AAA. لا توجد جلسة نشطة.	طلب المصادقة Diameter
`wait_swx_maa`	تم إرسال SWx MAR إلى HSS للحصول على متجهات EAP-AKA.	SWx MAA من HSS
`wait_swx_saa`	تم إرسال SWx SAR إلى HSS لتعيين الخادم.	SWx SAA من HSS
`authenticated`	د تكون جلسات ePDG وPGW نشطة. تتبع حالة الجلسة المزدوجة.	أحداث الجلسة
`auth_wait_swx_saa`	تم إرسال SWx SAR لتحديث PGW أو إلغاء تسجيل المستخدم.	SWx SAA من HSS
`dereg_net_wait_s6b_asa`	إلغاء التسجيل الذي يبدأ من HSS. تم إرسال S6b ASR إلى PGW.	S6b ASA من PGW
`dereg_net_wait_swm_asa`	اكتمل إنهاء S6b. تم إرسال SWm ASR إلى ePDG.	SWm ASA من ePDG

تدفقات المكالمات

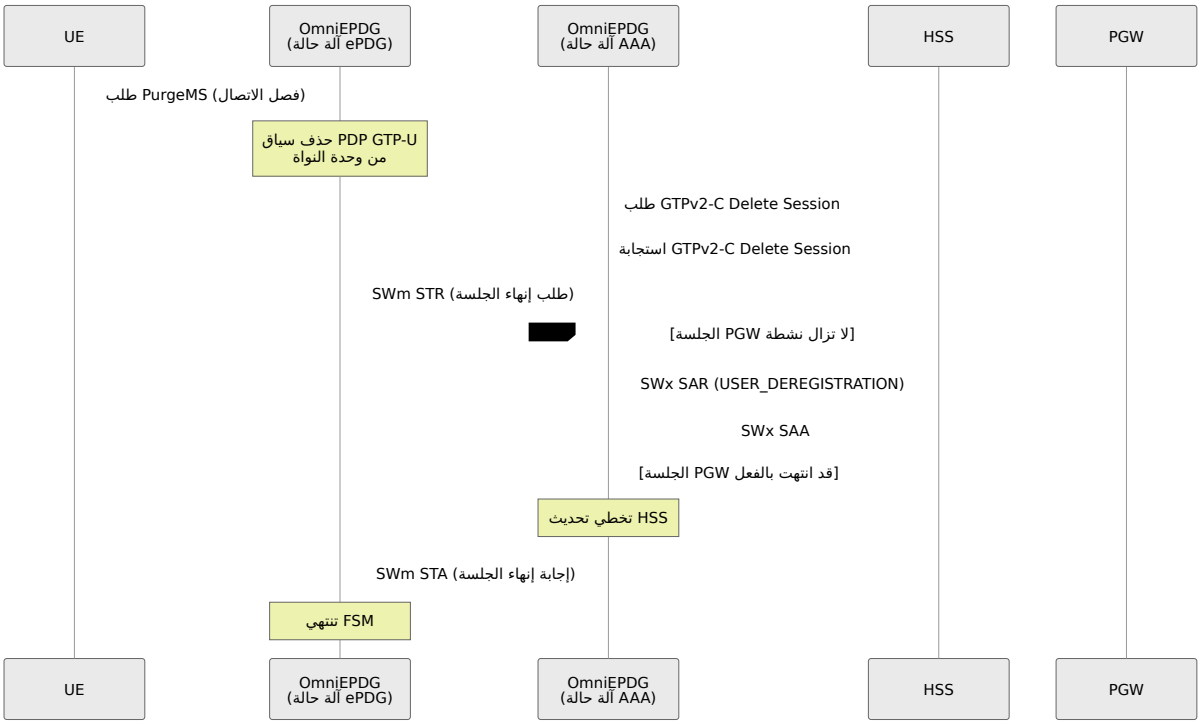
إنشاء جلسة ناجحة: GTP وضع

تظهر هذه السلسلة جلسة كاملة ناجحة من المصادقة EAP-AKA إلى نفق GTP النشط.



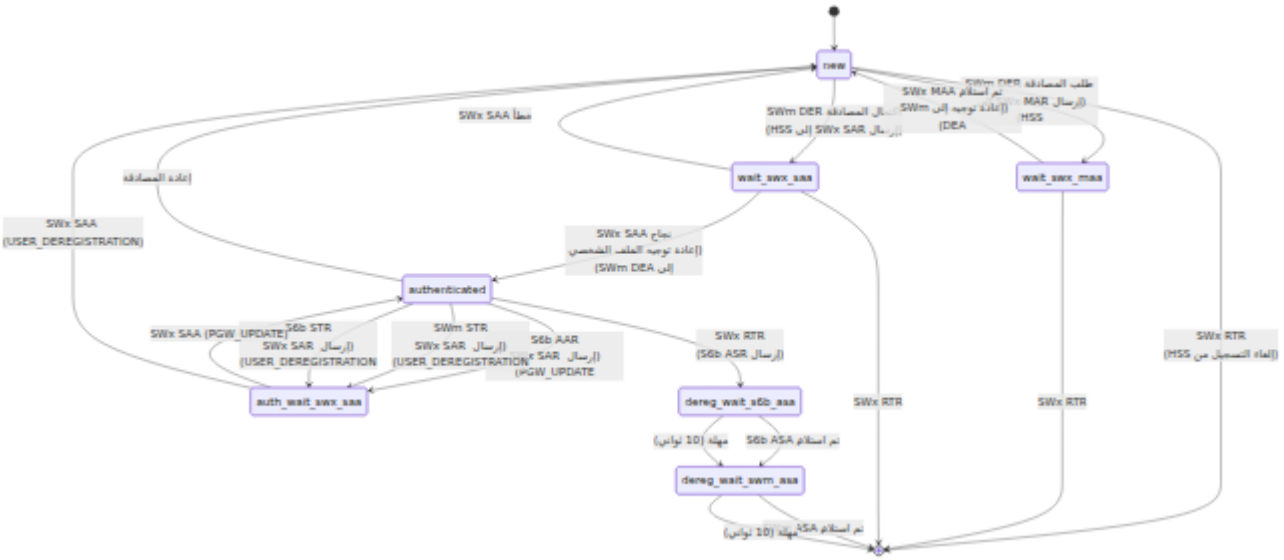
وضع GTP: إنهاء الجلسة التي يبدأها UE

إلى الشبكة الخ��وية أو WiFi على سبيل المثال، الانتقال من) بفصل الاتصال UE عندما يقوم إنهاء المستخدم).



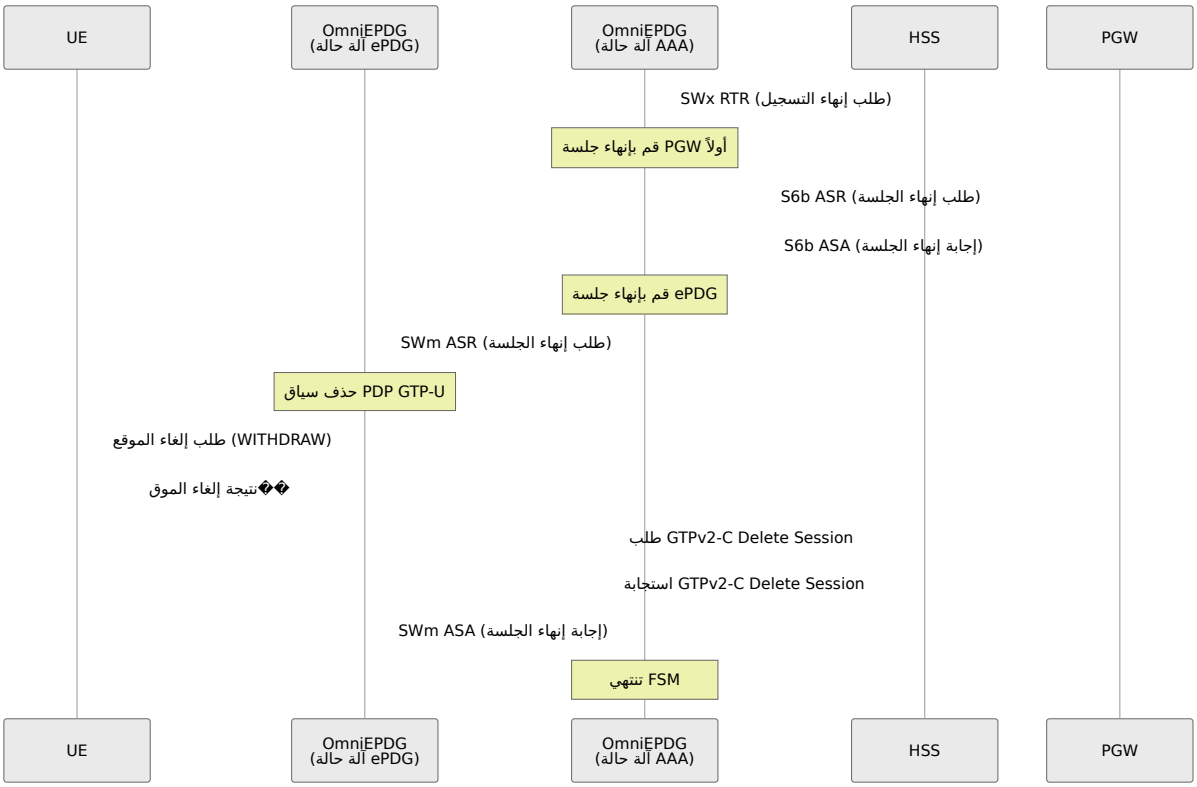
PGW إنهاء الجلسة التي يبدأها :GTP وضع

عندما يقوم PGW (على سبيل المثال، انتهاك السياسة، المهلة، أو إجراء إداري) بإنهاء الجلسة.



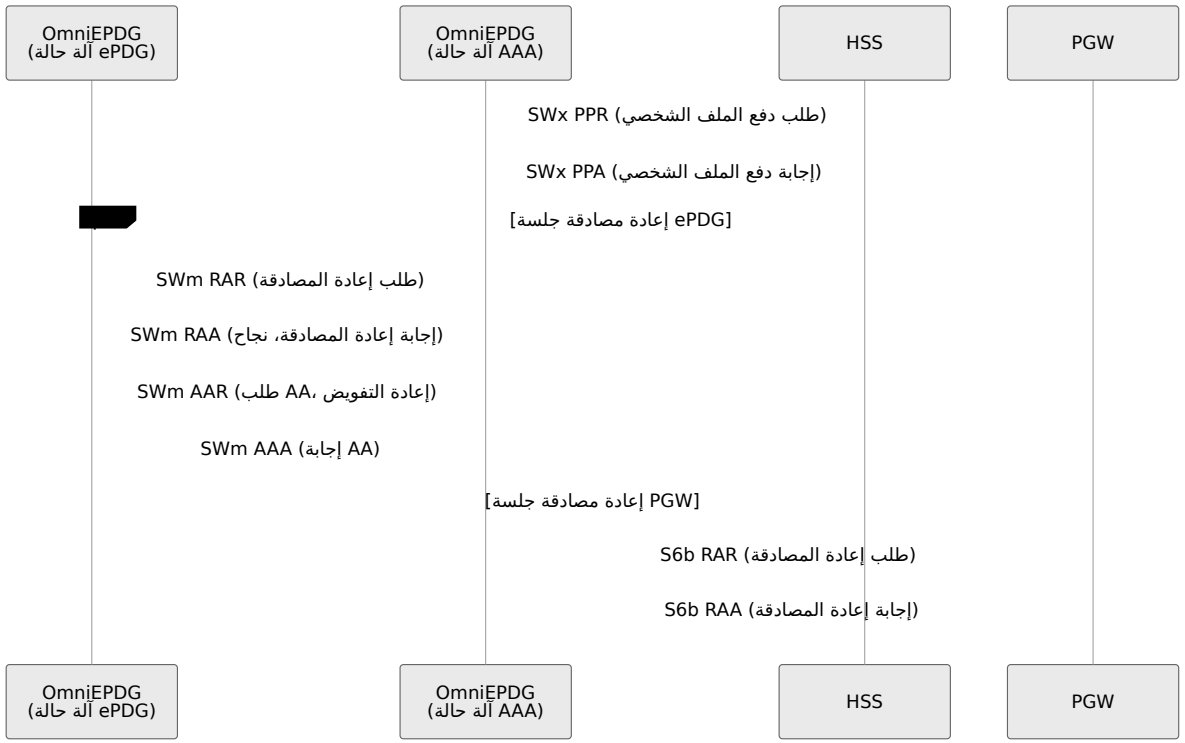
إلغاء التسجيل الذي يبدأه الشبكة (HSS) :GTP وضع

عندما يقوم HSS بإلغاء تسجيل مشترك (على سبيل المثال، تغيير الاشتراك، اكتشاف الاحتيال، أو إجراء إداري).



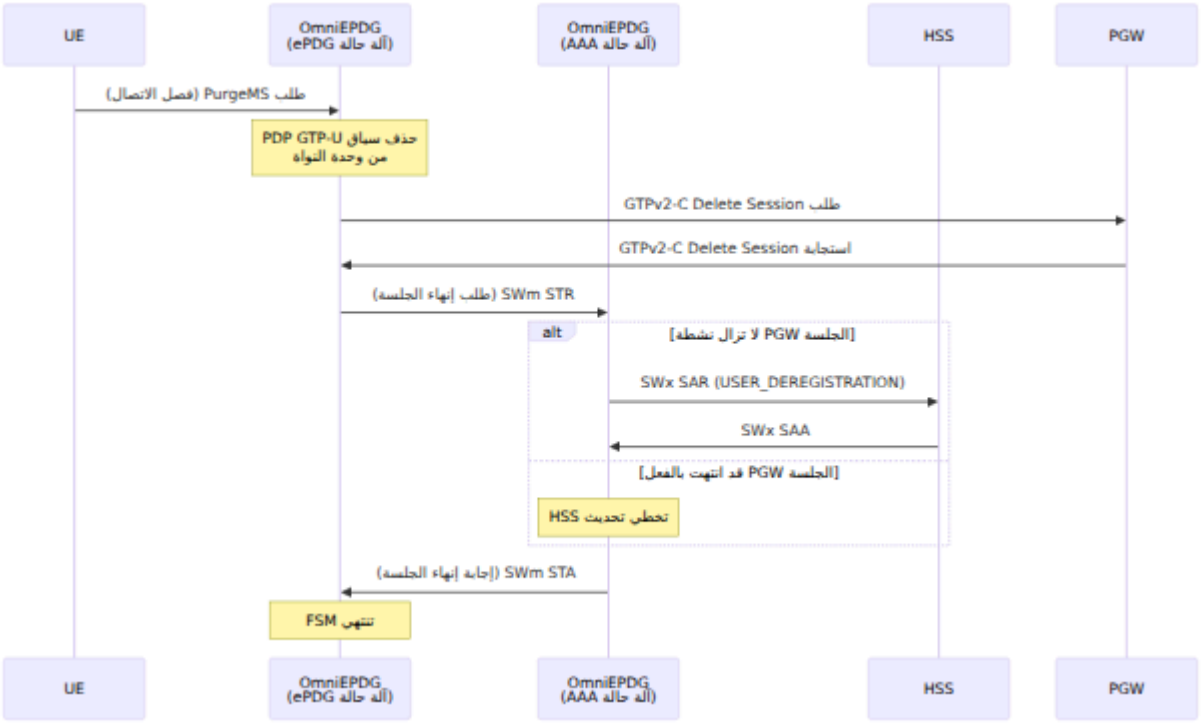
وإعادة المصادقة HSS دفع ملف تعريف :GTP وضع

بتحفيز إعادة المصادقة OmniEPDG بدفع ملف تعريف مشترك محدث، يقوم HSS عندما يقوم القسم 3 GPP TS 29.273وفقًا لـ 3 PGW (S6b)و ePDG (SWm) على كل من جلسات 8.1.2.3.3.



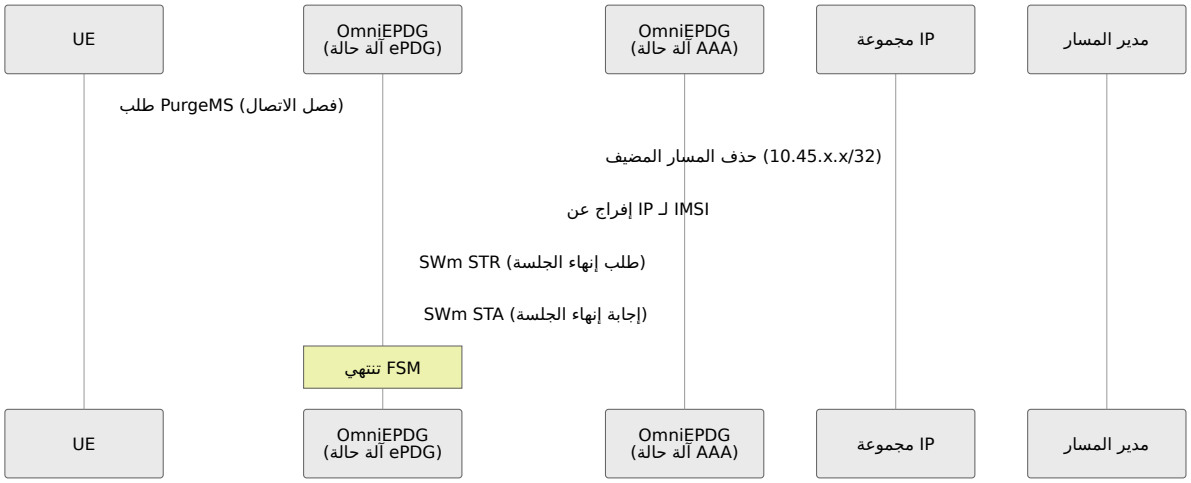
بسيط: إنشاء جلسة ناجحة VPN وضع

في وضع VPN تقوم آلة حالة EAP-AKA، بسيط، يكون إنشاء الجلسة أقصر. بعد المصادقة ePDG متجاوزة جميع TUN، من المجموعة المحلية وتعيين مسار مضيف على واجهة IP بتخصيص التفاعلات مع PGW. إذا كانت `skip_sar` مفعلة، يتم أيضًا تخطي تبادل SAR/SAA مع HSS.



بسيط: إنهاء الجلسة التي يبدأها UE وضع VPN

عندما يفصل UE في وضع VPN الاتصال بسيط، تقوم FSM بإفراج عنوان IP وإزالة ال��خصص المسار المضيف.



معرفات تطبيق Diameter

معرف التطبيق	الواجهة	معرف البائع	الوصف	المرجع
16777265	SWx	10415 (3GPP)	المصادقة وإدارة المشتركين بين ePDG وHSS	3GPP TS 29.273
16777272	S6b	10415 (3GPP)	تفويض جلسة AAA ↔ PGW	3GPP TS 29.273

رموز نتائج Diameter

يقوم OmniEPDG بربط رموز نتائج Diameter عبر بقيم الأسباب الداخلية لنقل الأخطاء البروتوكولات.

رموز النت��ئج القياسية

رمز النتيجة	الاسم	المعنى
2001	DIAMETER_SUCCESS	تم إكمال العملية بنجاح
2002	DIAMETER_LIMITED_SUCCESS	كانت العملية ناجحة جزئيًا

رموز النتائج التجريبية 3GPP

رمز النتيجة	الاسم	المعنى	رجع
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	لا يمكن لـ HSS توفير بيانات المصادقة مؤقتًا	3GP TS 29.2
5001	DIAMETER_ERROR_USER_UNKNOWN	لم يتم العثور على IMSI المشترك في HSS	3GP TS 29.2
5002	DIAMETER_UNKNOWN_SESSION_ID	لم يتم العثور على الجلسة (يستخدم لـ STR/AAR القديمة)	RFC 673
5003	DIAMETER_AUTHORIZATION_REJECTED	المشترك غير مصرح له بالخدمة	3GP TS 29.2
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	تنطبق قيود التجوال	3GP TS 29.2
5005	DIAMETER_MISSING_AVP	AVP المطلوب	RFC 673

رمز النتيجة	الاسم	المعنى	رجع
		مفقود من الرسالة	
5012	DIAMETER_UNABLE_TO_COMPLY	فشل معالجة عام	RFC 673
5420	DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION	لم يتم العثور على اشتراك EPS	3GP TS 29.
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	تقنية الوصول غير مسموح بها	3GP TS 29.
5422	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	جهاز IMEI غير معترف به	3GP TS 29.

رموز أسباب GTPv2-C (وضع GTP فقط)

يتعامل OmniEPDG مع رموز أسباب GTPv2-C التالية في استجابات Create/Delete Session. الرموز من 1-15 هي معلوماتية، 16-63 تشير إلى النجاح، و64+ تشير إلى الأخطاء. من PGW.

انظر إلى 3GPP TS 29.274 القسم 8.4.

أسباب النجاح

الرمز	الاسم	الوصف
16	الطلب مقبول	تم إكمال العملية بنجاح
17	الطلب مقبول جزئيًا	نجاح جزئي
18	نوع PDN (تفضيل الشبكة) جديد	تغير نوع PDN بسبب تفضيل الشبكة
19	نوع PDN (حامل عنوان واحد) جديد	تغير نوع PDN بسبب قيود حامل عنوان واحد

أسباب الخطأ (مختارة)

الرمز	الاسم	الوصف
64	السياق غير موجود	PGW لم يتم العثور على سياق الجلسة على
73	لا توجد موارد متاحة	PGW استنفاد موارد
78	APN مفقود أو غير معروف	APN المطلوب غير مكون على PGW
82	RAT مرفوض في	تقنية الوصول غير مسموح بها
84	جميع العناوين الديناميكية مشغولة	PGW على IP استنفاد مجموعة عناوين
92	فشل مصادقة المستخدم	PGW فشل المصادقة في
93	APN تم رفض الوصول إلى	APN المشترك غير مصرح له بـ
96	IMSI/IMEI غير معروف	الهوية المشتركة غير معترف بها
109	نظير غير صالح	فشل التحقق من النظير
113	APN ازدحام	APN محمل
120	GTP-C ازدحام كيان	PGW تحميل زائد في خطة التحكم

تنسيق NAI

يحدد OmniEPDG الوصول الشبكي م��رف المشتركين باستخدام تنسيق (NAI) المحدد في القسم 19 3GPP TS 23.003:

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

بادئة الهوية ونوع المصادقة

تحدد بادئة NAI طريقة المصادقة EAP 3وفقًا لـ GPP TS 23.003:

البادئة	نوع المصادقة	الوصف
`0`	EAP-AKA	مصادقة AKA القياسية (الأكثر شيوعًا لمكالمات WiFi)
`6`	EAP-AKA'	مصادقة AKA المحسّنة مع ربط الشبكة

يختار OmniEPDG تلقائيًا طريقة المصادقة بناءً على بادئة هوية UE. تستخدم معظم UE البادئة `0` لمكالمات WiFi (EAP-AKA).

يستخرج OmniEPDG IMSI من NAI عن طريق تحليل كل شيء بين البادئة ورمز `@`. ثم يتم استخدام IMSI كمفتاح أساسي لجميع آلات الحالة والإشارات الخاصة بالمشترك.

الخوارزميات التشفيرية

يطبق OmniEPDG 3الخوارزميات التشفيرية وفقًا لـ GPP TS 33.402و RFC 7296 (IKEv2).

خوارزميات ت��فير IKEv2

الخوارزمية	المعرف	حجم المفتاح	الحالة	المرجع
AES-CBC	12	128، 192، 256 بت	مدعوم (افتراضي: 256)	RFC 3602
AES-GCM-16	20	128، 192، 256 بت	مدعوم	RFC 5282
AES-GCM-12	19	128، 192، 256 بت	مدعوم	RFC 5282
AES-GCM-8	18	128، 192، 256 بت	مدعوم	RFC 5282
3DES	3	192 بت	مدعوم (قديم)	RFC 2451

خوارزميات سلامة IKEv2

الخوارزمية	المعرف	حجم المفتاح	حجم ICV	الحالة	المرجع
HMAC-SHA2-256-128	12	256 بت	128 بت	مدعوم (افتراضي)	RFC 4868
HMAC-SHA2-384-192	13	384 بت	192 بت	مدعوم	RFC 4868
HMAC-SHA2-512-256	14	512 بت	256 بت	مدعوم	RFC 4868
HMAC-SHA1-96	2	160 بت	96 بت	مدعوم (قديم)	RFC 2404
HMAC-MD5-96	1	128 بت	96 بت	مدعوم (قديم)	RFC 2403

خوارزميات PRF IKEv2

الخوارزمية	المعرف	حجم الإخراج	الحالة	المرجع
PRF-HMAC-SHA2-256	5	256 بت	مدعوم (افتراضي)	RFC 4868
PRF-HMAC-SHA2-384	6	384 بت	مدعوم	RFC 4868
PRF-HMAC-SHA2-512	7	512 بت	مدعوم	RFC 4868
PRF-HMAC-SHA1	2	160 بت	مدعوم (قديم)	RFC 2104
PRF-HMAC-MD5	1	128 بت	مدعوم (قديم)	RFC 2104

مجموعات Diffie-Hellman IKEv2

المجموعة	المعرف	الحجم	الحالة	المرجع
MODP-2048	14	2048 بت	مدعوم (افتراضي)	RFC 3526
MODP-1024	2	1024 بت	مدعوم (قديم)	RFC 2409
MODP-1536	5	1536 بت	مدعوم	RFC 3526
MODP-3072	15	3072 بت	مدعوم	RFC 3526
MODP-4096	16	4096 بت	مدعوم	RFC 3526
ECP-256	19	256 بت	مدعوم	RFC 5903
ECP-384	20	384 بت	مدعوم	RFC 5903
ECP-521	21	521 بت	مدعوم	RFC 5903
Curve25519	31	256 بت	مدعوم	RFC 8031
Curve448	32	448 بت	مدعوم	RFC 8031

خوارزميات ESP (SA الطفل)

يستخدم نفق ESP نفس خوارزميات التشفير والسلامة التي تم التفاوض عليها خلال IKEv2 CREATE_CHILD_SA.

تكوين ESP الافتراضي:

- التشفير: AES-CBC-256 (مفتاح 32 بايت، IV 16 بايت)
- السلامة: HMAC-SHA2-256-128 (مفتاح 32 بايت، ICV 16 بايت)

وظائف التشفير EAP-AKA

الوظيفة	الخو��رزمية	المرجع
اشتقاق MK	SHA-1	RFC 4187 القسم 7
توسيع مفتاح PRF+	FIPS 186-2 PRF (SHA-1)	RFC 4187 الملحق D
AT_MAC	HMAC-SHA1-128	RFC 4187 القسم 10.15
Milenage (f1-f5)	AES-128	3GPP TS 35.206

وظائف التشفير EAP-AKA'

الوظيفة	الخوارزمية	المرجع
اشتقاق CK'/IK'	HMAC-SHA-256	RFC 5448 القسم 3.3
اشتقاق MK	SHA-256	RFC 5448 القسم 3.4
AT_MAC	HMAC-SHA256-128	RFC 5448 القسم 3.1

الامتثال لـ 3GPP

يطبق OmniEPDG 3 جميع خوارزميات التشفير الإلزامية المحددة في 3GPP TS 33.402 القسم 8:

المتطلب	الخوارزمية	الحالة
تشفير IKEv2 (إلزامي)	AES-CBC-128	✓ مدعوم
سلامة IKEv2 (إلزامي)	HMAC-SHA2-256-128	✓ مدعوم (افتراضي)
PRF IKEv2 (إلزامي)	PRF-HMAC-SHA-256	✓ مدعوم (افتراضي)
DH IKEv2 (إلزامي)	المجموعة 14 (MODP-2048)	✓ مدعوم (افتراضي)
تشفير ESP (إلزامي)	AES-CBC-128/256	✓ مدعوم
سلامة ESP (إلزامي)	HMAC-SHA2-256-128	✓ مدعوم (افتراضي)
EAP-AKA	RFC 4187	✓ تم التنفيذ
EAP-AKA'	RFC 5448	✓ تم التنفيذ

أنواع عنوان PDP (وضع GTP فقط)

يدعم OmniEPDG أنواع عنوان PDP التالية كما هو محدد في 3GPP TS 29.274 القسم 8.14. فقط من المجموعة المحلية IPv4 بسيط، يتم تخصيص عناوين VPN في وضع.

النوع	الوصف	تنسيق PAA GTPv2-C
IPv4	حامل IPv4 فقط	عنوان IPv4 4 بايت
IPv6	حامل IPv6 فقط	عنوان + 1 بايت طول بادئة IPv6 16 بايت
IPv4v6	حامل مزدوج	عنوان + 1 بايت طول بادئة IPv6 16 بايت + عنوان IPv4 4 بايت

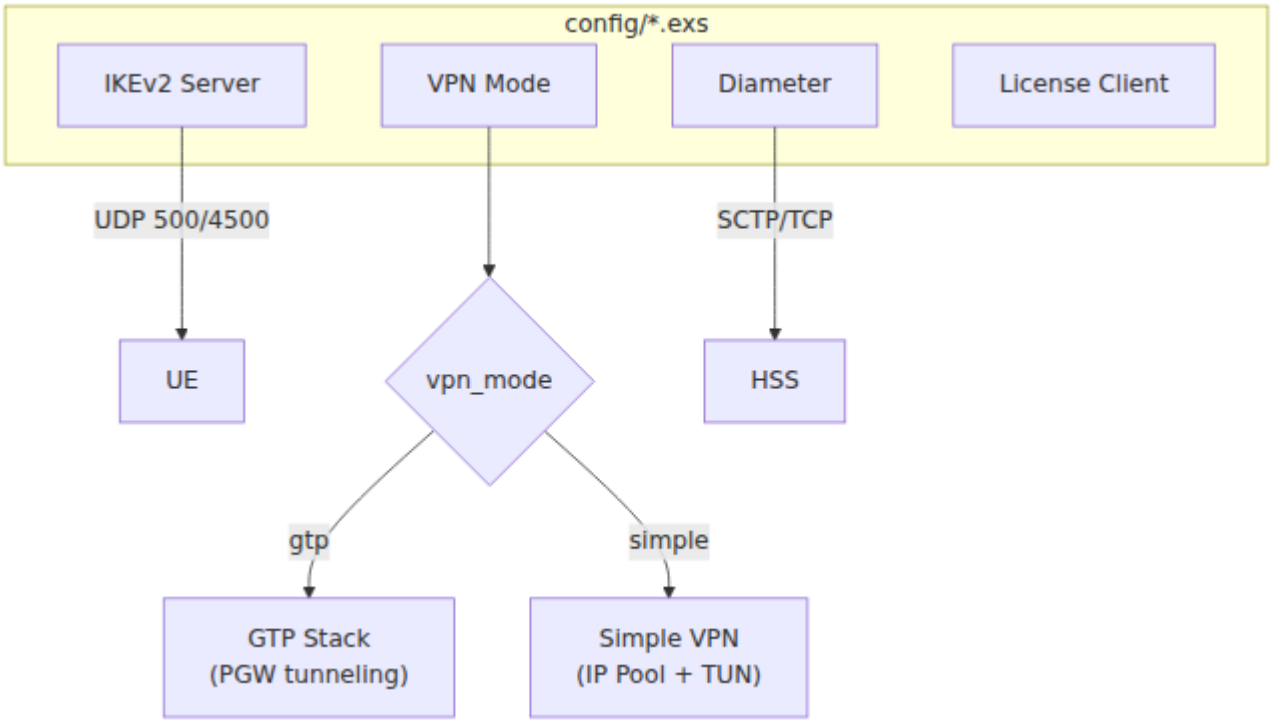
مرجع تكوين OmniEPDG

يتم تكوين OmniEPDG عبر `config/runtime.exs` ومتغيرات البيئة. يتم إجراء جميع التكوينات التي تواجه العملاء في وقت التشغيل - القيم الافتراضية في وقت الترجمة مضمنة في الإصدار وليست مكشوفة.

بالنسبة للتوزيعات المعبأة في حاويات، استخدم متغيرات البيئة كما هو موثق في قسم مرجع متغيرات البيئة.

جدول المحتويات

هيكل التكوين



ملف التكوين

يتم قراءة هذا الملف عند بدء `config/runtime.exs`. يتم إجراء جميع التكوينات في OmniEPDG ويدعم استبدال متغيرات البيئة للتوزيعات المعبأة في حاويات.

مثال على التكوين

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

  # وضع VPN: :simple (اختراق محلي) أو :gtp (PGW عبر GTP-C)
  vpn_mode: :simple,

  # إعدادات وضع VPN البسيط
  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"]
  ]

# تكوين لوحة التحكم
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"}
  ]

# تكوين 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}
    ]
  }

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

معلمات خادم IKEv2

يتعامل خادم IKEv2 مع واجهة SWu بين UEs و OmniEPDG. يقوم بإنهاء أنفاق IPSec ويقوم بمصادقة EAP-AKA.

المعلمة	النوع	مطلوب	الافتراضي
`listen_ip`	Tuple	لا	`{0, 0, 0, 0}`
`port_500`	Integer	لا	`500`
`port_4500`	Integer	لا	`4500`
`cert_file`	String	نعم	`/etc/omniepdg/cert`

المعلمة	النوع	مطلوب	الافتراضي
`key_file`	String	نعم	`/etc/omniepdg/certs`
`session_inactivity_timeout_ms`	Integer	لا	`300000`

معلمات أمان المصادقة

حماية مدمجة ضد هجمات القوة الغاشمة والتحكم في الوصول الجغرافي. OmniEPDG يتضمن
راجع دليل الأمان للحصول على وثائق مفصلة.

معلمات تحديد المعدل

```
config :omniepdg,
  # تحديد المعدل لكل IP
  auth_rate_limit_per_ip: 10,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 300_000,

  # تحديد المعدل لكل IMSI
  auth_rate_limit_per_imsi: 5,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 600_000
```

المعلمة	النوع	مطلوب	الافتراضي	لوصف
`auth_rate_limit_per_ip`	Integer	لا	`10`	الحد الأقصى محاولات لمصادقة الفاشلة لكل IP قبل الحظر.
`auth_rate_limit_ip_window_ms`	Integer	لا	`60000`	نافذة متحركة لحساب فشل IP (بالملي ثانية).
`auth_rate_limit_ip_block_ms`	Integer	لا	`300000`	مدة لحظر لـ التي IPs تتجاوز لعتبة (5 دقائق).
`auth_rate_limit_per_imsi`	Integer	لا	`5`	الحد الأقصى محاولات لمصادقة الفاشلة لكل IMSI قبل الحظر.
`auth_rate_limit_imsi_window_ms`	Integer	لا	`60000`	نافذة متحركة

المعلمة	النوع	مطلوب	الافتراضي	لوصف
				لحساب فشل IMSI (بالملي ثانية).
`auth_rate_limit_imsi_block_ms`	Integer	لا	`600000`	مدة لحظر لـ IMSIs التي تتجاوز العتبة (10 دقائق).

معلمات 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
```

المعلمة	النوع	مطلوب	الافتراضي	
`geoip_enabled`	Boolean	لا	`false`	
`geoip_database_path`	String	لا	`"/etc/omniepdg/GeoLite2-Country.mmdb"`	
`geoip_mode`	Atom	لا	`:whitelist`	
`geoip_countries`	List	لا	`[]`	
`geoip_allow_unknown`	Boolean	لا	mode-dependent	

المعلمة	النوع	مطلوب	الافتراضي	
				ي ة ء ء
`geoip_fail_open`	Boolean	لا	`true`	ع I ة ك ك

اختيار وضع VPN

المعلمة	النوع	مطلوب	الافتراضي	متغير البيئة	الوصف
`vpn_mode`	Atom	لا	`:simple`	`EPDG_VPN_MODE`	وضع التشغيل: `:simple` للاختراق المحلي عبر واجهة TUN، `:gtp` للتنقل عبر PGW عبر GTPv2-C/GTP-U. راجع دليل العمليات للحصول على مقارنة مفصلة.

معلمات VPN بسيطة

يدعم VPN البسيط OmniEPDG. تتحكم كتلة تكوين `simple_vpn` في تخصيص IP وDNS لوضع VPN. كل من مجموعات عناوين IPv4 وIPv6.

```
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
  ]
```

المعلمة	النوع	مطلوب	الافتراضي	ف
`pool_ipv4`	String	نعم	`"10.45.0.0/16"`	موعة ناوين IPv4 سيق CIDR صيص د لكل شترك
`pool_ipv6`	String	لا	`"2001:db8::/32"`	موعة ناوين IPv6 سيق CIDR ركين تائيي كدس
`dns_servers_ipv4`	List	لا	`["8.8.8.8", "8.8.4.4"]`	خوادم IPv4 مة لـ UEs PCO رات) كوين وكول
`dns_servers_ipv6`	List	لا	`["2001:4860:4860::8888", "2001:4860:4860::8844"]`	خوادم IPv6 مة لـ UEs PCO
`p_cscf_ipv4`	List	لا	`[]`	ناوين IPv4

المعلمة	النوع	مطلوب	الافتراضي	ف
				CSC Prox VoW مة لـ UEs سجيل IMS.
`p_cscf_ipv6`	List	لا	`[]`	ناوين IPv6 CSC Prox VoW
				قيمة واجهة القيم تقلل جزئة
`nat_enabled`	Boolean	لا	`true`	مكين مرور ركين. كين، طبيق قواعد تمويه حركة مرور صادرة

معلمات Diameter

يتحكم تكوين Diameter في واجهات SWx (HSS) وS6b (PGW). عندما تكون `diameter_enabled` `true`، يبدأ OmniEPDG كومة Diameter ويتصل بالأقران المكونة.

```
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}
    ]
  }
```

معلمات الخدمة

المعلمة	النوع	مطلوب	الافتراضي
`service_name`	Atom	لا	`:omniepdg`
`listen_ip`	String	لا	`"0.0.0.0"`
`listen_port`	Integer	لا	`3868`
`host`	String	نعم	`"epdg"`
`realm`	String	نعم	`"epc.mnc001.mcc001.3gppnetwork.org"`

المعلمة	النوع	مطلوب	الافتراضي
`product_name`	String	لا	`"OmniEPDG"`
`vendor_id`	Integer	لا	`10415`

معلمات الأقران

`peers` كل إدخال في قائمة يحدد اتصال نظير Diameter (عادةً إلى HSS).

المعلمة	النوع	مطلوب	الافتراضي	متغير البيئة	الوصف
`host`	String	نعم	-	`HSS_HOST`	هوية نظير Diameter (Origin-Host). يجب أن تتطابق مع الهوية المكونة للنظير.
`ip`	String	نعم	-	`HSS_IP`	عنوان IP للنظير لاتصال TCP/SCTP.
`port`	Integer	لا	`3868`	`HSS_PORT`	منفذ Diameter للنظير.
`transport`	Atom	لا	`:tcp`	-	بروتوكول النقل: `:tcp` أو `:sctp`.

معرفات التطبيقات

التطبيق	المعرف	معرف البائع	الواجهة	المرجع
SWx	16777265	10415	ePDG ↔ HSS	3GPP TS 29.273
S6b	16777272	10415	AAA ↔ PGW	3GPP TS 29.273

تكوين عميل الترخيص

يحقق عميل الترخيص من صحة مقابل خادم الترخيص OmniEPDG.

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

المعلمة	النوع	مطلوب	الافتراضي	متغير البيئة	صف
`server_url`	String	نعم	-	`LICENSE_SERVER_URL`	عنوان URL نقطة نهاية واجهة رمجة بيقات خادم رخيص
`product`	String	لا	`"omniepdg"`	-	عرف المنتج تحقق من رخيص

تكوين لوحة التحكم

توفر لوحة التحكم على الويب قدرات المراقبة والإدارة.

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

المعلمة	النوع	مطلوب	الافتراضي	متغير البيئة	الوصف
`port`	Integer	لا	`4000`	`CONTROL_PANEL_PORT`	منفذ HTTP لواجهة الويب الخاصة بلوحة التحكم.

تكوين مقاييس Prometheus

يعرض OmniEPDG مقاييس Prometheus عبر HTTP للمراقبة والتنبيه.

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

الوصف	متغير البيئة	الافتراضي	مطلوب	النوع	المعلمة
منفذ HTTP لنقطة نهاية مقاييس Prometheus (`/metrics`).	`PROMETHEUS_PORT`	`9568`	لا	Integer	`port`

المقاييس المعروضة

مقاييس العد (مدفوعة بالأحداث):

- `epdg_ikev2_session_initiated_count` - تبادلات IKE_SA_INIT التي بدأت
- `epdg_ikev2_session_established_count` - تم إنشاء IKE SAs بنجاح
- `epdg_ikev2_session_failed_count` - فشل إنشاء IKE SA (حسب السبب)
- `epdg_eap_identity_count` - طلبات هوية EAP
- `epdg_eap_aka_challenge_count` - تحديات EAP-AKA المرسلة
- `epdg_eap_aka_success_count` - نجاح مصادقات EAP-AKA
- `epdg_eap_aka_failure_count` - فشل مصادقات EAP-AKA (حسب السبب)
- `epdg_eap_aka_sync_failure_count` - فشل مزامنة SQN لـ EAP-AKA
- `epdg_diameter_swx_mar_count` - طلبات Multimedia-Auth (حسب النتيجة)
- `epdg_diameter_swx_sar_count` - طلبات Server-Assignment (حسب النتيجة)
- `epdg_diameter_s6b_aar_count` - الطلبات AA (حسب النتيجة) التي تم التعامل معها
- `epdg_diameter_s6b_str_count` - طلبات إنهاء الجلسة

- `epdg_session_created_count` - الجلسات التي تم إنشاؤها (حسب vpn_mode)
- `epdg_session_terminated_count` - الجلسات التي تم إنهاؤها (حسب السبب)
- `epdg_esp_packets_in_count` - حزم ESP التي تم فك تشفيرها
- `epdg_esp_packets_out_count` - حزم ESP التي تم تشفيرها
- `epdg_ip_allocated_count` - عناوين IP المخصصة (حسب النوع)
- `epdg_ip_released_count` - عناوين IP التي تم تحريرها (حسب النوع)

مقاييس القياس (يتم استقصاؤها كل 5 ثواني):

- `epdg_sessions_active_count` - إجمالي الجلسات النشطة
- `epdg_sessions_by_state_count` - الجلسات حسب حالة FSM
- `epdg_ip_pool_allocated_count` - IPs المخصصة حاليًا
- `epdg_ip_pool_available_count` - IPs المتاحة في المجموعة
- `epdg_ip_pool_utilization_ratio` - نسبة استخدام المجموعة (0.0-1.0)
- `epdg_diameter_swx_pending_count` - طلبات SWx المعلقة
- `epdg_diameter_s6b_active_sessions_count` - الجلسات النشطة لـ S6b

مقاييس الهستوغرام (تتبع الكمون):

- `epdg_auth_duration_ms` - مدة تدفق المصادقة الكاملة
- `epdg_diameter_swx_mar_latency_ms` - زمن استجابة MAR
- `epdg_diameter_swx_sar_latency_ms` - زمن استجابة SAR
- `epdg_session_duration_seconds` - عمر الجلسة

مقاييس VM:

- `vm_memory_total` - إجمالي ذاكرة VM
- `vm_memory_processes` - ذاكرة العمليات
- `vm_memory_binary` - ذاكرة الثنائيات
- `vm_memory_ets` - ذاكرة جدول ETS
- `vm_system_info_process_count` - العمليات الجارية
- `vm_system_info_port_count` - المنافذ المفتوحة
- `vm_statistics_run_queue` - قائمة تشغيل المجدول

تكوين استقصاء Prometheus

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

مرجع المهلة

جميع مهلات FSM الداخلية مشفرة. تتحكم هذه في المدة التي تنتظر فيها آلات الحالة للحصول على استجابات قبل اعتبارها فاشلة.

المهلة	القيمة	الوضع	السياق	الوصف
إجابة GTP	10,000 ms	GTP	ePDG UE FSM	الحد الأقصى للانتظار لاستجابة GTPv2-C Create/Delete Session من PGW.
إجابة SWm	10,000 ms	كلاهما	ePDG UE FSM	الحد الأقصى للانتظار لاستجابة Diameter SWm الداخلية (DER/DEA، STR/STA).
إجابة S6b	10,000 ms	GTP	AAA UE FSM	الحد الأقصى للانتظار لاستجابة Diameter S6b (ASR/ASA).

مرجع متغيرات البيئة

يتم قراءة متغيرات البيئة في `config/runtime.exs` وقت الترجمة وتجاوز القيم الافتراضية في.

خادم IKEv2

المتغير	الافتراضي	الوصف
`EPDG_LISTEN_IP`	`"0.0.0.0"`	عنوان ربط خادم IKEv2 (بتنسيق عشري منقوط، مثل `10.0.0.1""`).
`EPDG_PORT_500`	`"500"`	منفذ بروتوكول IKE.
`EPDG_PORT_4500`	`"4500"`	منفذ IKE NAT-Traversal.
`EPDG_CERT_FILE`	`"/etc/omniepdg/certs/epdg.crt"`	المسار إلى شهادة خادم IKEv2 (PEM).
`EPDG_KEY_FILE`	`"/etc/omniepdg/certs/epdg.key"`	المسار إلى المفتاح الخاص لخادم IKEv2 (PEM).
`EPDG_SESSION_TIMEOUT`	`"300000"`	مهلة عدم النشاط للجلسة بالميلي ثانية.

وضع VPN

المتغير	الافتراضي	الوصف
`EPDG_VPN_MODE`	`"simple"`	وضع VPN: `"simple"` أو `"gtp"`.

Diameter

المتغير	الافتراضي	الوصف
`DIA_LISTEN_IP`	`"0.0.0.0"`	عنوان ربط المستمع Diameter.
`DIA_LISTEN_PORT`	`"3868"`	منفذ المستمع Diameter.
`DIA_HOST`	`"epdg"`	Diameter Origin-Host (بدون نطاق).
`DIA_REALM`	`"epc.mnc001.mcc001.3gppnetwork.org"`	Diameter Origin-Realm.

نظير HSS

المتغير	الافتراضي	الوصف
`HSS_HOST`	`"hss"`	هوية Diameter لـ HSS (Origin-Host).
`HSS_IP`	`"127.0.0.1"`	عنوان IP لـ HSS.
`HSS_PORT`	`"3868"`	منفذ Diameter لـ HSS.

الترخيص، لوحة التحكم، والمقاييس

المتغير	الافتراضي	الوصف
`LICENSE_SERVER_URL`	-	عنوان URL لواجهة برمجة تطبيقات خادم الترخيص (مطلوب).
`CONTROL_PANEL_PORT`	`"4000"`	منفذ HTTP لواجهة لوحة التحكم.
`PROMETHEUS_PORT`	`"9568"`	منفذ HTTP لمقاييس Prometheus (نقطة نهاية `/metrics`).

مثال: 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"

      # وضع 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"

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

      # لوحة التحكم
      CONTROL_PANEL_PORT: "4000"

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

لوحة التحكم OmniEPDG

تتضمن OmniEPDG لوحة تحكم قائمة على الويب لمراقبة الجلسات، ونظراء Diameter، وسجلات النظام في الوقت الحقيقي. توفر لوحة التحكم عرضًا يتم تحديثه مباشرة دون الحاجة إلى تحديث الصفحة.

جدول المحتويات

الوصول إلى لوحة التحكم

تُقدم لوحة التحكم على منفذ HTTP (الافتراضي 4000) المكون:

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

التنقل

توفر لوحة التحكم شريط جانبي يحتوي على روابط لجميع العروض:

المسار	العرض	الوصف
`/dashboard`	لوحة المعلومات	نظرة عامة على النظام وروابط سريعة
`/sessions`	الجلسات	قائمة بجلسات UE النشطة
`/diameter`	نظراء Diameter	حالة اتصال نظراء Diameter
`/logs`	السجلات	بث السجلات في الوقت الحقيقي
`/docs`	الوثائق	متصفح الوثائق المدمج
`/resources`	الموارد	معلومات عن BEAM VM والتطبيقات
`/configuration`	التكوين	عارض تكوين النظام

لوحة المعلومات

توفر لوحة المعلومات نظرة عامة عالية المستوى عن حالة OmniEPDG مع مقاييس رئيسية وتنقل سريع.

بطاقات الإحصائيات

تظهر لوحة المعلومات أربع إحصائيات رئيسية:

الإحصائية	الوصف
الجلسات النشطة	العدد الحالي للجلسات UE المكونة
البيانات المستلمة (UL)	إجمالي البايتات المستلمة من UEs (اتجاه الرفع)
البيانات المرسلة (DL)	إجمالي البايتات المرسلة إلى UEs (اتجاه التنزيل)
نظراء Diameter	نظراء متصلين / إجمالي نظراء مكونين

تتوسع قيم البيانات تلقائيًا إلى الوحدات المناسبة (B، KB، MB، GB).

روابط سريعة

تنقل مباشر إلى العروض التفصيلية:

- **عرض الجلسات** - الانتقال إلى عرض الجلسات للحصول على معلومات مفصلة عن UE
- **نظراء Diameter** - الانتقال إلى عرض نظراء Diameter لحالة الاتصال
- **سجلات النظام** - الانتقال إلى عرض السجلات لبث السجلات في الوقت الحقيقي
- **التكوين** - الانتقال إلى عرض التكوين لإعدادات النظام

معلومات النظام

يعرض التكوين التشغيلي الحالي:

الحقل	الوصف
وضع VPN	الوضع الحالي: `GTP` أو `SIMPLE`
منافذ IKEv2	المنافذ القياسية: 500 (IKE)، 4500 (NAT-T)
حالة Diameter	ما إذا كان الإشارة Diameter مفعلة
مجموعة IP (IPv4)	CIDR لمجموعة IP المكونة (وضع VPN بسيط فقط)ا

التحديث التلقائي

تقوم لوحة المعلومات بتحديث نفسها تلقائيًا كل ثانية لعرض الإحصائيات الحالية.

عرض الجلسات

يعرض عرض الجلسات جميع جلسات UE النشطة مع معلومات مفصلة لكل مشترك.

يعرض عرض الجلسات اتصالات UE النشطة مع إحصائيات حركة المرور في الوقت الحقيقي ومدة الجلسة.

قائمة الجلسات

تعرض كل صف من الجلسات:

العمود	الوصف
IMSI	هوية المشترك الدولية للمحمول
UE IP	عنوان IPv4/IPv6 المعين
SOURCE	عنوان IP الخارجي للـ UE والمنفذ (عنوان NAT)
APN	اسم نقطة الوصول للاتصال
STATUS	حالة الجلسة الحالية (نشطة/غير نشطة)
DURATION	الوقت منذ إنشاء الجلسة
TRAFFIC	البايتات المستلمة / المرسلة (UL/DL)

مؤشرات الحالة

تعرض الجلسات الحالة مع شارات ملونة:

الحالة	اللون	الوصف
نشطة	أخضر	الجلسة مكونة بالكامل وتعمل
جار الاتصال	أصفر	جاري إنشاء الجلسة
غير نشطة	أحمر	الجلسة تم إنهاؤها أو فشلت

تفاصيل الجلسة

انقر على أي صف من الجلسات لتوسيع المعلومات التفصيلية:

عرض الجلسة الموسعة يظهر IMSI، NAI، وإحصائيات حركة المرور، تكوين الشبكة.

قسم الجلسة

الحقل	الوصف
IMSI	القيمة الكاملة لـ IMSI
NAI	معرف الوصول إلى الشبكة (بتنسيق 3GPP)
UE IP	عنوان IPv4/IPv6 المعين
Source	عنوان IP الخارجي للـ UE والمنفذ (عنوان NAT)
APN	اسم نقطة الوصول لاتصال PDN
Child SA SPI	مؤشر معلمات الأمان لـ SA الفرعية IPSec

قسم الشبكة والتوقيت

الحقل	الوصف
DNS	خوادم DNS المقدمة للـ UE
P-CSCF	خوادم Proxy-CSCF لإشارات IMS
Connected	الطابع الزمني عن إنشاء الجلسة
Last Activity	الطابع الزمني لأحدث نشاط حزمة
Duration	الوقت منذ إنشاء الجلسة

قسم الحركة

الحقل	الوصف
Bytes In (UL)	إجمالي البايتات المستلمة من UE (اتجاه الرفع)
Bytes Out (DL)	إجمالي البايتات المرسلة إلى UE (اتجاه التنزيل)
Packets In	إجمالي الحزم المستلمة من UE
Packets Out	إجمالي الحزم المرسلة إلى UE

الحالة الفارغة

عندما لا تكون هناك جلسات نشطة، يعرض العرض:

- رسالة "لا توجد جلسات نشطة"
- يشير إلى ما إذا كان يجب محاولة اتصالات UE

التحديث التلقائي

تقوم قائمة الجلسات بتحديث نفسها تلقائيًا كل ثانية.

عرض نظراء Diameter

يعرض عرض نظراء Diameter حالة جميع نظراء Diameter المكونين (HSS لـ SWx، PGW لـ S6b).

قائمة النظراء

تعرض كل صف من النظراء:

العمود	الوصف
Peer	هوية Diameter (Origin-Host)
Realm	نطاق Diameter (Origin-Realm)
IP Address	عنوان النقل بتنسيق `protocol://ip:port`
Status	حالة الاتصال

مؤشرات الحالة

الحالة	اللون	الوصف
متصل	أخضر	تم إنشاء اتصال نظراء Diameter
غير متصل	أحمر	غير متصل
غير معروف	رمادي	لا يمكن تحديد الحالة

ملخص عدد النظراء

يعرض العنوان إجمالي الأعداد:

- **متصل** - عدد النظراء الذين لديهم اتصالات نشطة **X**
- **غير متصل** - عدد النظراء بدون اتصالات **Y**

تفاصيل النظراء

انقر على أي صف من النظراء لتوسيع المعلومات التفصيلية:

الحقل	الوصف
Initiation Connection	من يقوم بالاتصال: `محلي` (نحن نتصل بالنظير) أو `بعيد` (النظير يتصل بنا)
Transport	البروتوكول: `tcp` أو `sctp`
Product Name	اسم المنتج المعلن للنظير من CER/CEA
Advertised Applications	معرفات تطبيق Diameter المدعومة من النظير

الحالة الفارغة

عندما لا يتم تكوين أي نظراء، يعرض العرض:

- "لا توجد نظراء" إذا كانت Diameter مكونين
- "Diameter معطلة" مع تلميح التكوين إذا كانت معطلة

التحديث التلقائي

تقوم قائمة النظراء بتحديث نفسها تلقائيًا كل ثانية.

عرض السجلات

يوفر عرض السجلات بثًا في الوقت الحقيقي لسجلات النظام مع قدرات تصفية وبحث.

عرض السجلات

تظهر السجلات في حاوية تمرير مع أحدث الإدخالات في الأسفل. تعرض كل إدخالة سجل:

العنصر	الوصف
Timestamp	متى تم إنشاء إدخالة السجل
Level	مستوى الشدة مع ترميز الألوان
Message	محتوى رسالة السجل

مستويات السجلات

تُرمز السجلات بالألوان حسب الشدة:

المستوى	اللون	الوصف
debug	رمادي	معلومات تشخيصية مفصلة
info	أزرق	رسائل معلوماتية عامة
warning	أصفر	حالات تحذيرية
error	أحمر	حالات خطأ

تص��ية المستوى

قم بتصفية السجلات حسب الحد الأدنى لمستوى الشدة باستخدام القائمة المنسدلة:

الفلتر	يظهر
جميع المستويات	debug، info، warning، error
Info+	info، warning، error
Warning+	warning، error
Error Only	error

البحث

تصفية السجلات في الوقت الحقيقي باستخدام مربع البحث:

- أدخل أي نص لتصفية رسائل السجل
- المطابقة غير حساسة لحالة الأحرف
- يتم مسحها عند إفراغ مربع البحث

التحكم

التحكم	الوصف
توقف/استئناف	تبديل بث السجلات تشغيل/إيقاف
مسح	إزالة جميع السجلات المعروضة
التمرير التلقائي	تبديل التمرير التلقائي إلى أحدث الإدخالات

مخزن السجلات

- يتم الاحتفاظ بحد أقصى 1000 إدخالة سجل
- تتم إزالة أقدم الإدخالات عند الوصول إلى الحد
- يؤدي مسح السجلات إلى إزالة جميع الإدخالات من العرض

الحالة الفارغة

عندما لا تتطابق أي سجلات مع الفلاتر الحالية:

- رسالة "لا توجد سجلات لعرضها"
- تحقق من إعدادات الفلتر إذا كانت السجلات متوقعة

التحديث التلقائي

تظهر سجلات جديدة تلقائيًا عند إنشائها (عندما لا تكون متوقفة).

عرض الوثائق

يوفر عرض الوثائق متصفح وثائق مدمج، مما يتيح للمشغلين الوصول إلى جميع وثائق OmniEPDG مباشرة من لوحة التحكم.

اختيار الوثيقة

اختر من ملفات الوثائق المتاحة باستخدام شريط الأزرار:

الوثيقة	الوصف
OPERATIONS.md	دليل العمليات مع بدء سريع وإجراءات
README.md	نظرة عامة على المشروع وتعليمات الإعداد
architecture.md	بنية النظام وتدفقات المكالمات
configuration.md	مرجع تكوين كامل
control-panel.md	دليل لوحة التحكم هذه
metrics.md	مرجع مقاييس Prometheus
troubleshooting.md	المشكلات الشائعة وخطوات الحل

عرض Markdown

تُعرض الوثائق بدعم كامل لـ Markdown بما في ذلك:

- العناوين وتنسيق النص
- كتل التعليمات البرمجية مع تمييز الصياغة
- الجداول
- الروابط (داخلية وخارجية)
- القوائم واقتباسات الكتل

عرض الموارد

يعرض عرض الموارد إحصائيات BEAM VM والتطبيقات التي تعمل على OTP.

مقاييس النظام

المقياس	الوصف
استخدام الذاكرة	إجمالي الذاكرة المستخدمة بواسطة BEAM VM
عمليات BEAM	عدد عمليات Erlang/Elixir التي تعمل
مدة التشغيل	الوقت منذ بدء التطبيق

التطبيقات قيد التشغيل

تظهر جميع تطبيقات OTP المحملة مقسمة حسب الفئة:

الفئة	الوصف
الرئيسية	تطبيق OmniEPDG
النظام	تطبيقات Erlang/OTP و Elixirالأساسية

انقر على تطبيق لعرض تفاصيله بما في ذلك الإصدار، الوصف، والاعتمادات.

عرض التكوين

يعرض عرض التكوين تكوين وقت التشغيل والتطبيقات المحملة.

معلومات البيئة

الحقل	الوصف
البيئة	البيئة الحالية لـ Mix (تطوير/إنتاج)
إصدار Elixir	إصدار Elixir الجاري

قائمة التطبيقات

تعرض جميع تطبيقات OTP المحملة مع إصداراتها. اختر تطبيقًا لعرض:

- وصف التطبيق
- معلومات الإصدار
- الاعتمادات
- معلمات التكوين

تكوين لوحة التحكم

منفذ HTTP

قم بتكوين منفذ لوحة التحكم في `config/runtime.exs`:

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

المعلمة	النوع	الافتراضي	الوصف
`port`	عدد صحيح	4000	منفذ HTTP لواجهة التحكم

تعطيل لوحة التحكم

يمكن تعطيل لوحة التحكم بعدم بدء نقطة الويب في الإنتاج إذا لم تكن مطلوبة. اتصل بمزود النظام الخاص بك للحصول على تكوين محدد للنشر.

OmniEPDG مرجع مقاييس

تقوم OmniEPDG بتوفير مقاييس Prometheus، ودورة حياة الجلسة، لمراقبة تدفقات المصادقة، وإشارات Diameter، عبر HTTP وصحة النظام. يتم تقديم المقاييس لتمكين عملية السحب بواسطة Prometheus.

جدول المحتويات

نقطة نهاية المقاييس

تقوم OmniEPDG بتوفير المقاييس عند:

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

تُرجع نقطة النهاية المقاييس بتنسيق عرض Prometheus المتوافق مع Prometheus، وأدوات المراقبة الأخرى وGrafana.

التكوين

قم بتكوين نقطة نهاية المقاييس في `config/runtime.exs`:

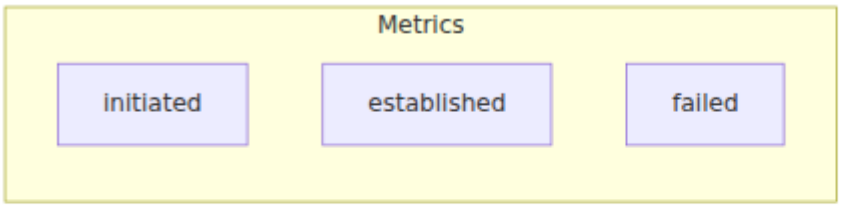
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

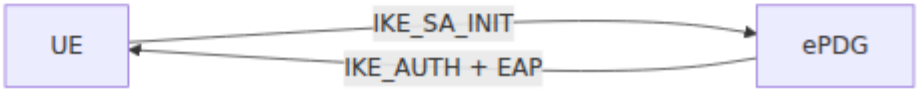
الوصف	متغير البيئة	القيمة الافتراضية	النوع	المعامل
منفذ HTTP لنقطة نهاية `/metrics`	`PROMETHEUS_PORT`	`9568`	عدد صحيح	`port`

فئات المقاييس

مقاييس جلسة IKEv2

مقاييس تتبع إنشاء نفق IKEv2 على واجهة SWu.





المقياس: `epdg_ikev2_session_initiated_count`
النوع: عداد
الوصف: إجمالي تبادل IKE_SA_INIT التي تم البدء بها. يزيد عندما يبدأ UE إنشاء النفق.

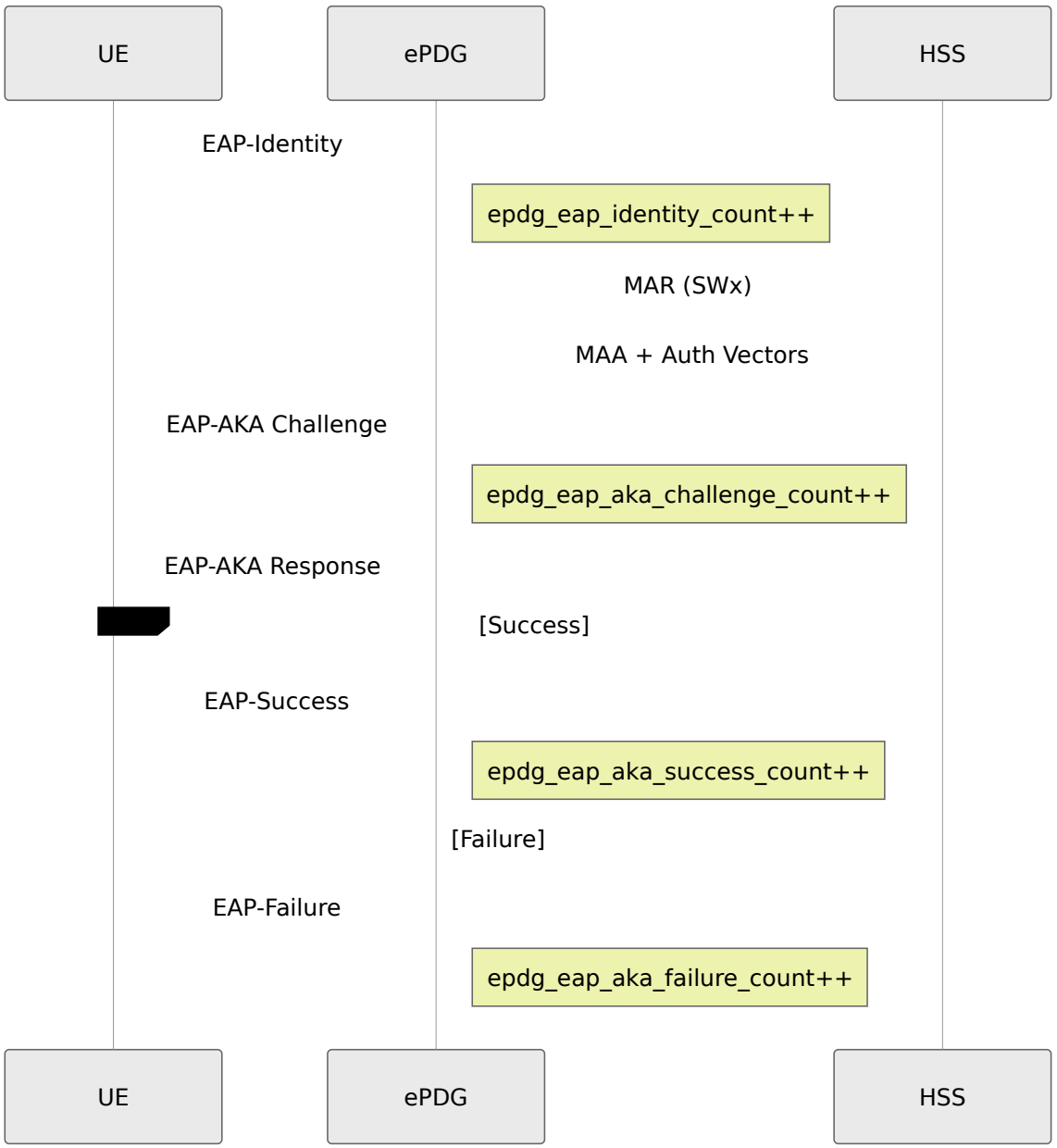
المقياس: `epdg_ikev2_session_established_count`
النوع: عداد
الوصف: إجمالي SAs IKE التي تم إنشاؤها بنجاح. يزيد بعد المصادقة الناجحة باستخدام EAP-AKA وإنشاء SA الفرعي.

المقياس: `epdg_ikev2_session_failed_count`
النوع: عداد
الوصف: إجمالي حالات فشل إنشاء SA IKE
التسميات:

- `reason` - سبب الفشل (مثل `auth_failed`, `timeout`, `invalid_proposal`)

مقاييس مصادقة EAP

مقاييس تتبع تدفقات مصادقة EAP-AKA وفقًا لـ RFC 4187. تدعم OmniEPDG أيضًا EAP-AKA' مع اختيار نوع المصادقة تلقائيًا بناءً على بادئة هوية NAI الخاصة بـ UE، وفقًا لـ RFC 5448.



المقياس: `epdg_eap_identity_count`
النوع: عداد
الوصف: إجمالي طلبات EAP-Identity المستلمة من UEs

المقياس: `epdg_eap_aka_challenge_count`
النوع: عداد
الوصف: إجمالي تحديات EAP-AKA المرسلة إلى UEs

المقياس: `epdg_eap_aka_success_count`
النوع: عداد
الوصف: إجمالي المصادقات الناجحة باستخدام EAP-AKA

المقياس: `epdg_eap_aka_failure_count`
النوع: عداد
الوصف: إجمالي المصادقات الفاشلة باستخدام EAP-AKA
التسميات:

- `reason` - سبب الفشل (مثل `res_mismatch`, `invalid_identity`, `authentication_rejected`)

المقياس: `epdg_eap_aka_sync_failure_count`
النوع: عداد
الوصف: إجمالي حالات فشل مزامنة رقم تسلسل EAP-AKA (SQN). يشير إلى عدم تطابق رقم تسلسل USIM/HSS مما يتطلب إع��دة المزامنة.

مقاييس أمان المصادقة

مقاييس لطبقة أمان المصادقة. راجع دليل الأمان للحصول على تفاصيل التكوين.

المقياس: `epdg_auth_verification_failed_count`
النوع: عداد
الوصف: إجمالي حالات فشل التحقق من الحمولة AUTH. تشير إلى هجمات محتملة من نوع man-in-the-middle أو أخطاء في التنفيذ.

المقياس: `epdg_auth_rate_limited_count`
النوع: عداد
الوصف: إجمالي محاولات المصادقة المحجوبة بواسطة تحديد المعدل
التسميات:

- `type` - سبب الحجب: `ip` (تجاوز الحد لكل IP) أو `imsi` (تجاوز الحد لكل IMSI)

استعلامات نموذجية:

```
# محاولات محجوبة لكل دقيقة
rate(epdg_auth_rate_limited_count[1m])

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

المقياس: `epdg_auth_geoip_blocked_count`
النوع: عداد
الوصف: إجمالي محاولات المصادقة المحجوبة بواسطة تصفية GeoIP حسب الدولة
التسميات:

- `country` - رمز الدولة ISO 3166-1 alpha-2 (مثل `CN`, `RU`)، أو `UNKNOWN` لعناوين IP التي لم يمكن تحديد موقعها جغرافيًا

استعلامات نموذجية:

```
# حجب GeoIP لكل دقيقة
rate(epdg_auth_geoip_blocked_count[1m])

# أعلى الدول المحجوبة
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))
```

المقياس: `epdg_esp_replay_detected_count`
النوع: عداد
الوصف: إجمالي حزم ESP المرفوضة بسبب اكتشاف إعادة التشغيل (وفقًا لـ RFC 4303). تشير إلى هجمات محتملة من نوع إعادة التشغيل أو مشكلات في الشبكة تسبب إعادة ترتيب الحزم.

مقاييس Diameter SWx

مقاييس لواجهة SWx بين ePDG وHSS وفقًا لـ 3GPP TS 29.273.

المقياس: `epdg_diameter_swx_mar_count`
النوع: عداد
الوصف: إجمالي طلبات Multimedia-Auth المرسلة إلى HSS لاسترجاع متجهات المصادقة
التسميات:

- `result` - نتيجة الطلب: `success` أو `failure`

المقياس: `epdg_diameter_swx_sar_count`
النوع: عداد
الوصف: إجمالي طلبات Server-Assignment المرسلة إلى HSS للتسجيل/إلغاء التسجيل
التسميات:

- `result` - نتيجة الطلب: `success` أو `failure`

المقياس: `epdg_diameter_swx_mar_latency_ms`
النوع: هيستوجرام
الوصف: زمن استجابة MAR بالمللي ثانية
الأقسام: 50, 100, 250, 500, 1000, 2500 مللي ثانية

المقياس: `epdg_diameter_swx_sar_latency_ms`
النوع: هيستوجرام
الوصف: زمن استجابة SAR بالمللي ثانية
الأقسام: 50, 100, 250, 500, 1000, 2500 مللي ثانية

المقياس: `epdg_diameter_swx_pending_count`
النوع: مقياس
الوصف: العدد الحالي لطلبات SWx المعلقة في انتظار الاستجابة. تشير القيم العالية إلى ازدحام أو مشكلات في الاتصال HSS.

مقاييس Diameter S6b

مقاييس لواجهة S6b بين خادم PGW و AAA وفقًا لـ 3GPP TS 29.273. تنطبق فقط في وضع GTP.

المقياس: `epdg_diameter_s6b_aar_count`
النوع: عداد
الوصف: إجمالي طلبات AA المعالجة لتفويض الجلسة
التسميات:

- `result` - نتيجة الطلب: `success` أو `failure`

المقياس: `epdg_diameter_s6b_str_count`
النوع: عداد
الوصف: إجمالي طلبات إنهاء الجلسة المعالجة

المقياس: `epdg_diameter_s6b_active_sessions_count`
النوع: مقياس
الوصف: العدد الحالي للجلسات النشطة S6b

مقاييس دورة حياة الجلسة

مقاييس تتبع إنشاء وإنهاء جلسات PDN.

المقياس: `epdg_session_created_count`
النوع: عداد
الوصف: إجمالي الجلسات التي تم إنشاؤها
التسميات:

- `vpn_mode` - وضع VPN: `simple` أو `gtp`

المقياس: `epdg_session_terminated_count`
النوع: عداد
الوصف: إجمالي الجلسات التي تم إنهاؤها
التسميات:

- `reason` - سبب الإنهاء: `user_request`, `timeout`, `error`, `admin`

المقياس: `epdg_sessions_active_count`
النوع: مقياس
الوصف: العدد الحالي للجلسات النشطة. يتم الاستطلاع كل 5 ثوانٍ.

المقياس: `epdg_sessions_by_state_count`
النوع: مقياس
الوصف: الجلسات مجمعة حسب حالة FSM
التسميات:

- `state` - حالة الجلسة (مثل `init`, `eap_identity`, `eap_aka_challenge`, `authenticated`, `established`)

المقياس: `epdg_auth_duration_ms`
النوع: هيستوجرام
الوصف: مدة تدفق المصادقة الكاملة من IKE_SA_INIT إلى الجلسة المنشأة
الأقسام: 100, 250, 500, 1000, 2500, 5000, 10000 ملي ثانية

المقياس: `epdg_session_duration_seconds`
النوع: هيستوجرام
الوصف: عمر الجلسة من الإنشاء إلى الإنهاء
الأقسام: 60, 300, 900, 1800, 3600, 7200, 14400 ثانية (من 1 دقيقة إلى 4 ساعات)

مقاييس بيانات ESP

مقاييس لمعالجة حزم ESP وفقًا لـ RFC 4303.

المقياس: `epdg_esp_packets_in_count`
النوع: عداد
الوصف: إجمالي حزم ESP التي تم فك تشفيرها بنجاح (من الاتجاه UE إلى الشبكة)

المقياس: `epdg_esp_packets_out_count`
النوع: عداد
الوصف: إجمالي حزم ESP التي تم تشفيرها (من الاتجاه UE إلى الشبكة)

المقياس: `epdg_esp_bytes_in_total`
النوع: مقياس
الوصف: إجمالي البايتات التي تم فك تشفيرها من حزم ESP

المقياس: `epdg_esp_bytes_out_total`
النوع: مقياس
الوصف: إجمالي البايتات التي تم تشفيرها في حزم ESP

مقاييس تجمع IP

مقاييس لإدارة تجمع عناوين IP في وضع VPN البسيط.

المقياس: `epdg_ip_allocated_count`
النوع: عداد
الوصف: إجمالي عناوين IP المخصصة
التسميات:

- `type` - نوع العنوان: `ipv4` أو `ipv6`

المقياس: `epdg_ip_released_count`
النوع: عداد
الوصف: إجمالي عناوين IP المفرج عنها
التسميات:

- `type` - نوع العنوان: `ipv4` أو `ipv6`

المقياس: `epdg_ip_pool_allocated_count`
النوع: مقياس
الوصف: العدد الحالي لعناوين IP المخصصة

المقياس: `epdg_ip_pool_available_count`
النوع: مقياس
الوصف: العدد الحالي لعناوين IP المتاحة في التجمع

المقياس: `epdg_ip_pool_utilization_ratio`
النوع: مقياس
الوصف: استخدام تجمع IP كنسبة من 0.0 إلى 1.0. تشير القيم التي تقترب من 1.0 إلى خطر نفاد التجمع.

مقاييس VM

مقاييس آلة Erlang/BEAM الافتراضية لمراقبة صحة النظام.

المقياس: `vm_memory_total`
النوع: مق��اس
الوحدة: بايت
الوصف: إجمالي الذاكرة المخصصة بواسطة VM

المقياس: `vm_memory_processes`
النوع: مقياس
الوحدة: بايت
الوصف: الذاكرة المستخدمة بواسطة عمليات Erlang

المقياس: `vm_memory_binary`
النوع: مقياس
الوحدة: بايت
الوصف: الذاكرة المستخدمة للثنائيات (بما في ذلك مخازن الحزم)

المقياس: `vm_memory_ets`
النوع: مقياس
الوحدة: بايت
الوصف: الذاكرة المستخدمة بواسطة جداول ETS (حالة الجلسة، السجلات)

المقياس: `vm_system_info_process_count`
النوع: مقياس
الوصف: عدد عمليات Erlang النشطة

المقياس: `vm_system_info_port_count`
النوع: مقياس
الوصف: عدد المنافذ المفتوحة (المآخذ، مقبض الملفات)

المقياس: `vm_statistics_run_queue`
النوع: مقياس
الوصف: الطول الإجمالي لقوائم تشغيل المجدول. تشير القيم العالية إلى تشبع وحدة المعالجة المركزية.

تكامل Prometheus

تكوين السحب

أضف OmniEPDG إلى ملف `prometheus.yml` الخاص بك:

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

اكتشاف الخدمة

لعمليات النشر في Kubernetes، استخدم اكتشاف الخدمة:

```
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
```

استعلامات نموذجية

معدل نجاح المصادقة

```
# معدل النجاح على مدى 5 دقائق
sum(rate(epdg_eap_aka_success_count[5m]))
/
(sum(rate(epdg_eap_aka_success_count[5m])) +
sum(rate(epdg_eap_aka_failure_count[5m])))
```

معدل إنشاء الجلسات

```
# الجلسات المنشأة في الثانية
rate(epdg_ikev2_session_established_count[5m])
```

زمن اس��جابة المصادقة (p95)

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

زمن استجابة HSS (p99)

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

الجلسات النشطة

```
epdg_sessions_active_count
```

استخدام تجمع IP

```
epdg_ip_pool_utilization_ratio * 100
```

معدل نقل ESP

```
# بايت في الثانية (الوارد)
rate(epdg_esp_bytes_in_total[5m])

# حزم في الثانية (في كلا الاتجاهين)
rate(epdg_esp_packets_in_count[5m]) +
rate(epdg_esp_packets_out_count[5m])
```

تحليل الفشل حسب السبب

```
# فشل EAP حسب السبب
sum by (reason) (rate(epdg_eap_aka_failure_count[5m]))

# إنهاء الجلسات حسب السبب
sum by (reason) (rate(epdg_session_terminated_count[5m]))
```

قواعد التنبيه

قواعد تنبيه نموذجية لـ Prometheus لـ OmniEPDG:

```yaml
groups:
  - name: omniepdg
    rules:
      # معدل فشل المصادقة العالي
      - 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: "مرتفع EAP-AKA معدل فشل مصادقة"
          description: "معدل فشل المصادقة هو {{ $value |
humanizePercentage }} خلال آخر 5 دقائق"

      # قريب من النفاد IP تجمع
      - alert: OmniEPDGIPPoolLow
        expr: epdg_ip_pool_utilization_ratio > 0.9
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "استخدام تجمع IP 90 فوق%"
          description: "تجمع IP هو {{ $value | humanizePercentage
}} مستخدم"

      # نفاد تجمع IP
      - alert: OmniEPDGIPPoolExhausted
        expr: epdg_ip_pool_available_count == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "نفد تجمع IP"
          description: "لا توجد عناوين IP متاحة لجلسات جديدة"

      # مرتفع HSS زمن استجابة
      - 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: "مرتفع HSS (SWx) زمن استجابة"
          description: "الزمن المئوي 95 لاستجابة MAR هو {{ $value
}}ms"

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

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

      # تحميل المجدول مرتفع
      - alert: OmniEPDGSchedulerOverload
        expr: vm_statistics_run_queue > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "مرتفع Erlang طول قائمة تشغيل مجدول"
          description: "طول قائمة التشغيل هو {{ $value }}، مما
يشير إلى تشبع وحدة المعالجة المركزية"

      # (مشكلة محتملة في الخدمة) لا توجد ج??سات
```

```
      - alert: OmniEPDGNoSessions
        expr: epdg_sessions_active_count == 0 and
epdg_ikev2_session_initiated_count > 0
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "لا توجد جلسات نشطة على الرغم من محاولات الاتصال"
          description: "يتم بدء الجلسات ولكن لا توجد جلسات نشطة"

      # نشاط تحديد المعدل المرتفع (هجوم محتمل)
      - alert: OmniEPDGHighRateLimiting
        expr: rate(epdg_auth_rate_limited_count[5m]) > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "معدل مرتفع من محاولات المصادقة المحجوبة"
          description: "{{ $value | printf \"%.1f\" }} محاولات
مصادقة محجوبة في الثانية"

      # ارتفاع حجب GeoIP (هجوم محتمل من منطقة معينة)
      - alert: OmniEPDGGeoIPBlockingSpike
        expr: |
          rate(epdg_auth_geoip_blocked_count[5m]) > 5
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "مرتفع GeoIP نشاط حجب"
          description: "{{ $value | printf \"%.1f\" }} ا��صالات
محجوبة في الثانية بواسطة GeoIP"

      # اكتشاف هجمات إعادة تشغيل ESP
      - alert: OmniEPDGReplayAttack
        expr: rate(epdg_esp_replay_detected_count[5m]) > 0
        for: 2m
        labels:
          severity: warning
        annotations:
          summary: "اكتشاف هجمات إعادة تشغيل ESP"
          description: "{{ $value | printf \"%.1f\" }} محاولات
إعادة تشغيل في الثانية"
```

```
      # هجوم محتمل من نوع (MITM) حالات فشل التحقق من AUTH
      - alert: OmniEPDGAuthVerificationFailures
        expr: rate(epdg_auth_verification_failed_count[5m]) > 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "اكتشاف حالات فشل التحقق من الحمولة AUTH"
          description: "هجوم محتمل من نوع man-in-the-middle أو خطأ
في التنفيذ"
```

متطلبات الشبكة

يغطي هذا المستند منافذ جدار الحماية وإدخالات DNS المطلوبة لنشر OmniEPDG لمكالمات WiFi.

منافذ جدار الحماية

المنافذ الموجهة للإنترنت (UE ↔ ePDG)

يجب أن تكون هذه المنافذ مفتوحة على الإنترنت لكي تتمكن الأجهزة المحمولة من إنشاء اتصالات مكالمات WiFi.

المنفذ	البروتوكول	الاتجاه	الغرض
500	UDP	وارد	تبادل IKEv2 الأولي (IKE_SA_INIT، IKE_AUTH)
4500	UDP	وارد	UDP في ESP وتغليف IKEv2 NAT-Traversal

المنفذ 500/UDP يتعامل مع مفاوضة IKEv2 الأولية. إذا تم اكتشاف NAT بين UE و ePDG، فإن الاتصال ينتقل تلقائيًا إلى المنفذ 4500 (وهو الحال تقريبًا دائمًا لمكالمات WiFi).

المنفذ 4500/UDP يحمل كل من إشارات IKEv2 وبيانات المستخدم المشفرة بواسطة ESP. هذا هو المسار الرئيسي لجميع حركة مرور مكالمات WiFi عندما يكون NAT-T نشطًا.

منافذ الشبكة الداخلية (ePDG ↔ Core)

تُستخدم هذه المنافذ للتواصل بين OmniEPDG وشبكة النواة المحمولة. يجب أن تكون متاحة من ePDG ولكن لا ينبغي أن تكون مكشوفة على الإنترنت.

المنفذ	البروتوكول	الاتجاه	الغرض	النظير
3868	TCP	ثنائي الاتجاه	Diameter SWx (المصادقة)	HSS / DRA
3868	TCP	ثنائي الاتجاه	Diameter S6b (تفويض الجلسة)	PGW / AAA
2123	UDP	ثنائي الاتجاه	GTPv2-C مستوى التحكم (S2b)	PGW
2152	UDP	ثنائي الاتجاه	GTP-U مستوى المستخدم (S2b-U)	PGW

منافذ الإدارة

تُستخدم هذه المنافذ للمراقبة التشغيلية ويجب تقييدها لشبكات الإدارة.

المنفذ	البروتوكول	الغرض
4000	TCP	واجهة الويب الخاصة بلوحة التحكم (HTTP)
443	TCP	واجهة الويب الخاصة بلوحة التحكم (HTTPS، الإنتاج)
9568	TCP	نقطة نهاية مقاييس Prometheus

متطلب��ت DNS

سجل DNS لاكتشاف ePDG

تكتشف الأجهزة المحمولة ePDG باستخدام معيار تسمية DNS 3 موحد محدد في 3GPP TS 23.003. تنسيق FQDN هو:

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

حيث:

- `<MCC>` هو رمز الدولة المحمولة المكون من 3 أرقام (مثل `505` لأستراليا)
- `<MNC>` هو رمز الشبكة المحمولة المكون من 2 أو 3 أرقام، مع إضافة أصفار إلى 3 أرقام (مثل `001`)

يجب أن يكون سجل DNS **سجل A** (أو AAAA لـ IPv6) يشير إلى عنوان IP العام لـ OmniEPDG.

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

اسم الشهادة الشائعة

يجب أن تحتوي شهادة TLS الخاصة بـ ePDG على اسم بديل للموضوع (SAN) يتطابق مع FQDN الذي ستتصل به الأجهزة. يتم التحقق من ذلك بواسطة UE أثناء مصادقة IKEv2 الخاص بـ ePDG.

متطلبات الشهادة:

- يجب أن يتضمن SAN FQDN اكتشاف ePDG (مثل `epdg.epc.mnc001.mcc001.pub.3gppnetwork.org`)
- يجب أن تكون الشهادة موقعة من قبل CA (تتحقق الأجهزة من السلسلة) موثوق به
- الحد الأدنى هو RSA 2048 بت أو ECDSA P-256

مجال Diameter DNS

وفقًا لـ DNS NAPTR/SRV، يجب أن يتم حل المجال عبر سجلات Diameter للتوجيه الصحيح لـ RFC 6408. تنسيق المجال هو:

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

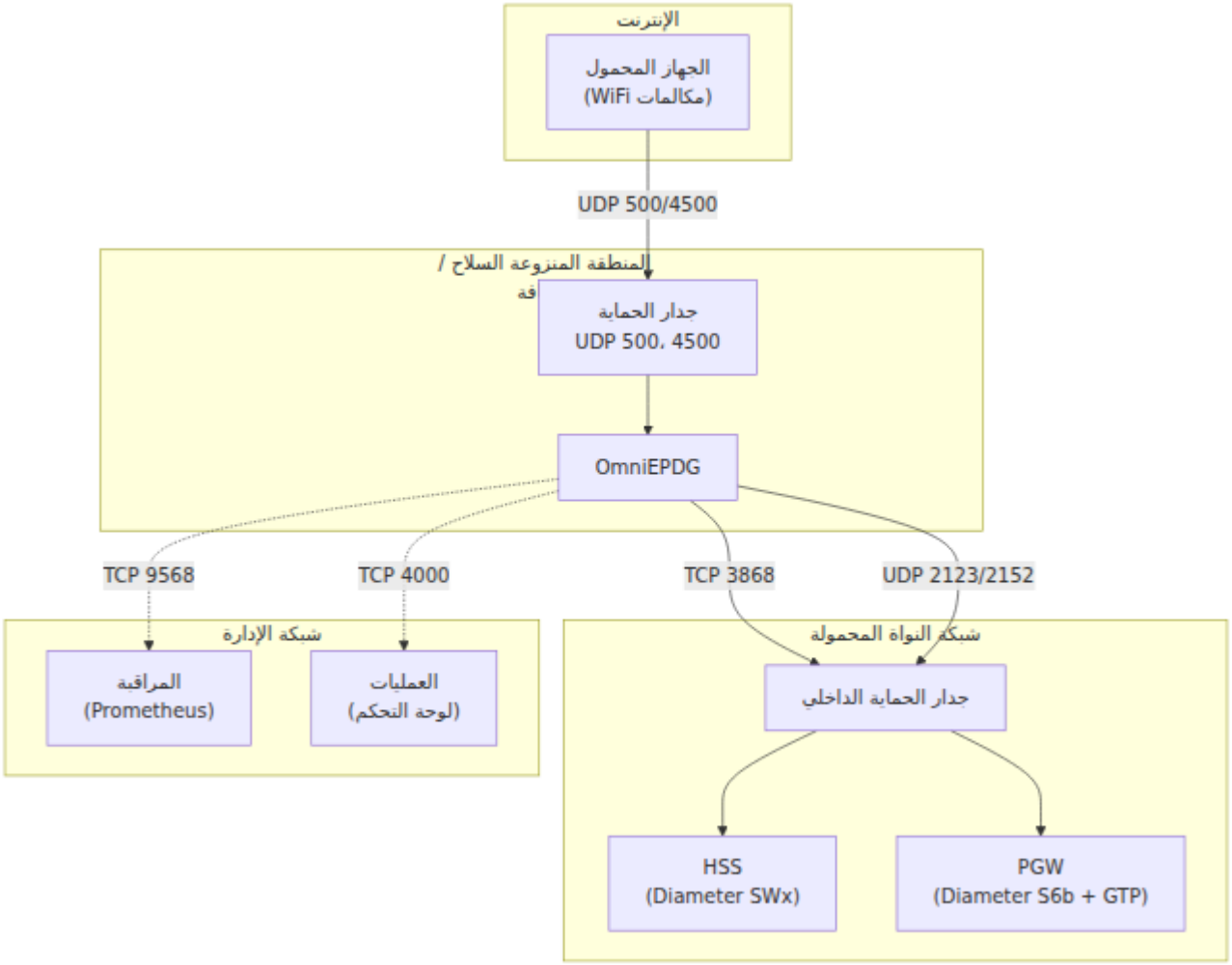
مثال:

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

يتم استخدام هذا المجال في:

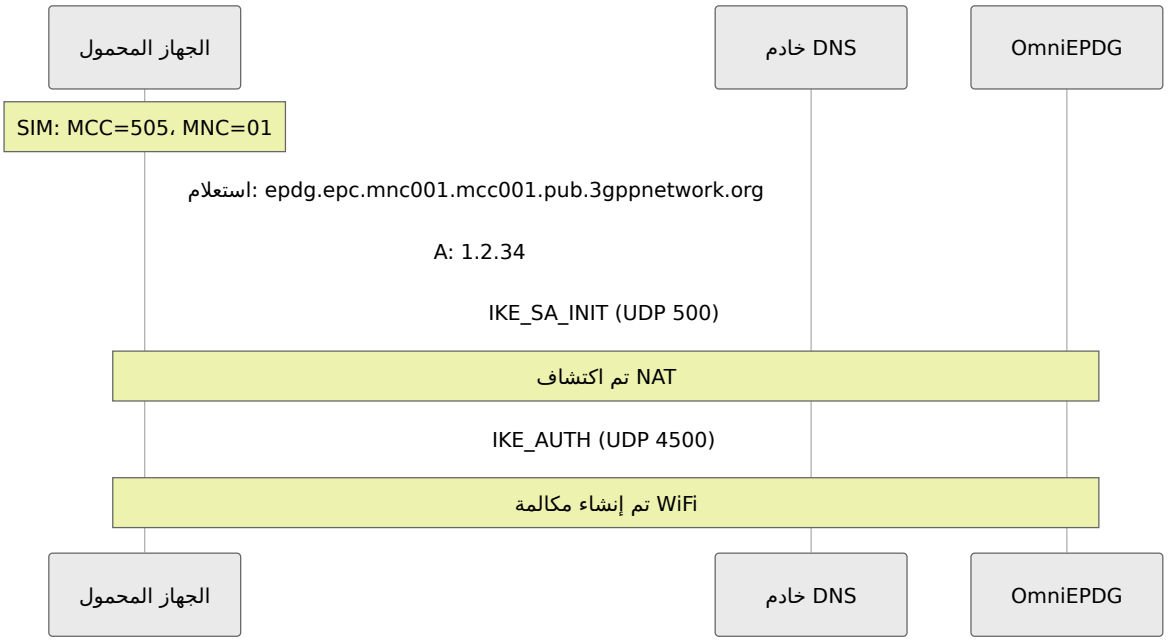
- أثناء المصادقة UE المرسل من (معرف الوصول إلى الشبكة) NAI
- لمجال الأصل ومجال الوجهة لـ Diameter AVPs
- قرارات توجيه Diameter

هيكل الشبكة



تدفق بحث DNS

يحدث حل DNS التالي، عندما يبدأ جهاز محمول مكالمة WiFi:



قائمة التحقق

متطلبات مواجهة الإنترنت

- [ ] فتح UDP 500 وارد إلى OmniEPDG
- [ ] فتح UDP 4500 وارد إلى OmniEPDG
- [ ] سجل DNS A: `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` → عنوان IP العام لـ ePDG
- [ ] تثبيت شهادة TLS مع SAN مطابق

متطلبات شبكة النواة

- [ ] فتح TCP 3868 بين OmniEPDG و HSS/DRA
- [ ] فتح TCP 3868 بين OmniEPDG و PGW/AAA (فقط وضع GTP)
- [ ] فتح UDP 2123 بين OmniEPDG و PGW (فقط وضع GTP)
- [ ] فتح UDP 2152 بين OmniEPDG و PGW (فقط وضع GTP)

متطلبات الإدارة

- [ ] الوصول إلى TCP 4000/443 من شبكة العمليات

- [ ] من بنية المراقبة TCP 9568 الوصول إلى

المراجع

- 3GPP TS 23.003 - الترقيم والعناوين والتعريف (تنسيق ePDG FQDN)
- 3GPP TS 23.402 - تحسينات المعمارية للوصولات غير 3GPP
- RFC 7296 - بروتوكول IKEv2
- RFC 3948 - تغليف UDP لحزم IPsec ESP (NAT-T)
- RFC 6733 - بروتوكول Diameter الأساسي

OmniEPDG دليل عمليات

OmniEPDG هو بوابة بيانات متطورة (ePDG) 3 متوافقة مع 3GPP تمكّن من إجراء المكالمات عبر شبكة WiFi بالشبكة الأساسية المحمولة. يدعم وضعين من خلال ربط الوصول غير الموثوق لشبكة WiFi المحلي IP. تشغيليين: **وضع بسيط** لتفريغ **VPN** و **وضع** PGW لنفق **GTP**.

روابط سريعة

التكوين والنشر

- **متطلبات الشبكة** - منافذ جدار الحماية وإدخالات DNS المطلوبة للنشر
- **مرجع التكوين** - توثيق كامل للمعلمات لـ VPN وجميع أوضاع Diameter و IKEv2 إعدادات وقت التشغيل
- **نظرة عامة على المعمارية** - هيكل النظام، تدفقات المكالمات، آلات الحالة، ومراجع البروتوكول

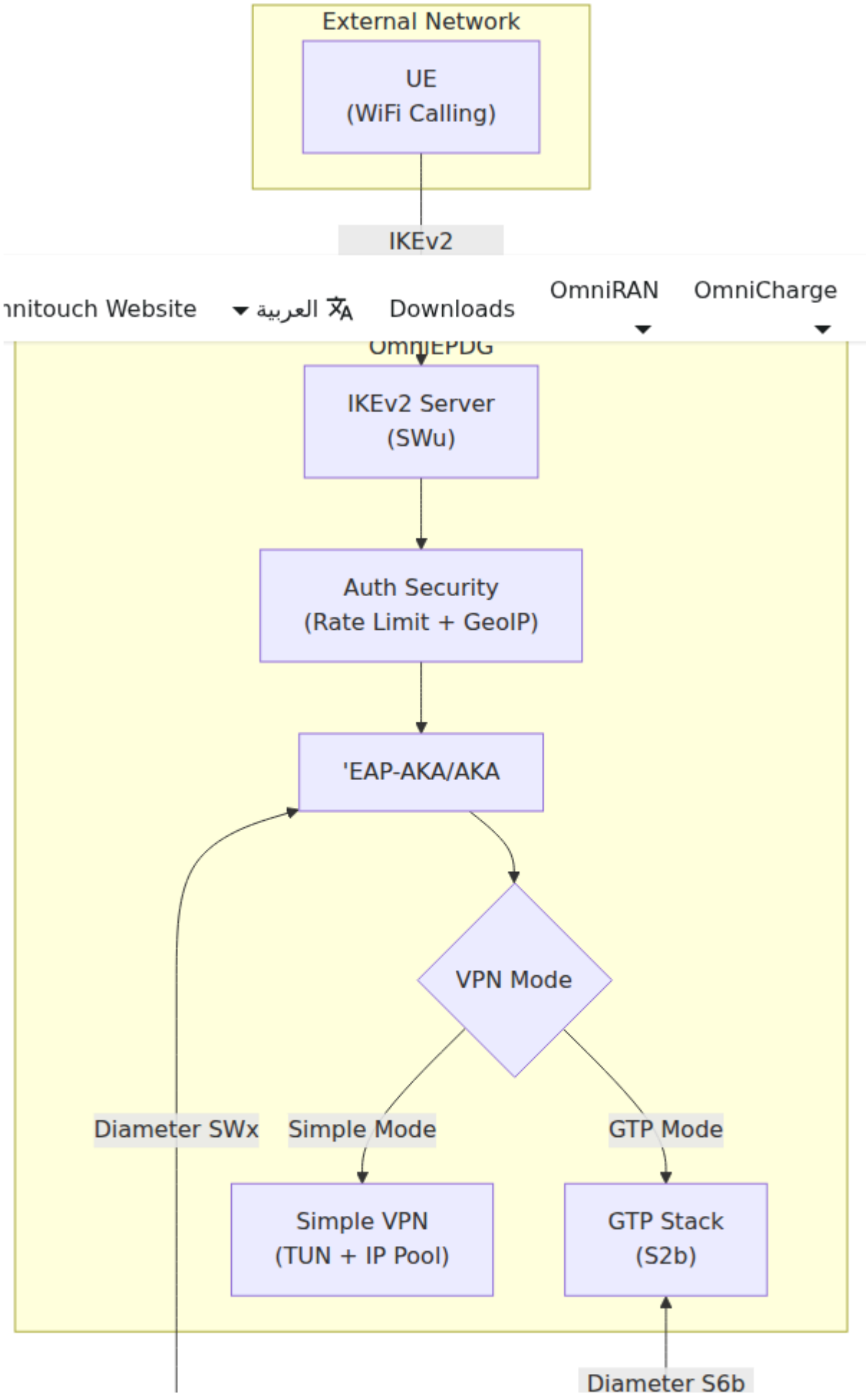
العمليات والمراقبة

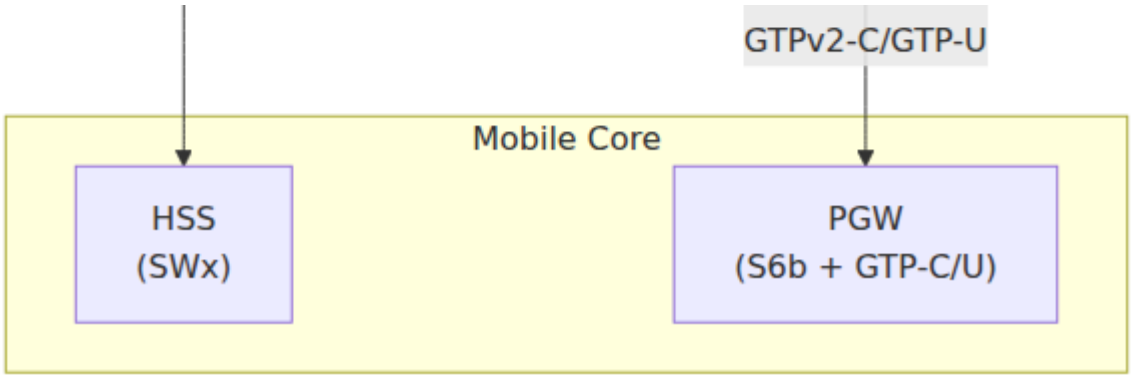
- **لوحة التحكم** - واجهة مراقبة قائمة على الويب للجلسات، أقران Diameter، والسجلات
- **مرجع القياسات** - قياسات Prometheus، استعلامات نموذجية، وقواعد التنبيه
- **استكشاف الأخطاء وإصلاحها** - المشكلات الشائعة، إجراءات التشخيص، وخطوات الحل

الأمان

- **أمان المصادقة** - تحديد المعدل وحظر الدول عبر GeoIP

نظرة عامة على المعمارية


External Network
UE
(WiFi Calling)
IKEv2
nitouch Website
العربية
Downloads
OmniRAN
OmniCharge
OmniEPDG
IKEv2 Server
(SWu)
Auth Security
(Rate Limit + GeoIP)
'EAP-AKA/AKA
VPN Mode
Diameter SWx
Simple Mode
GTP Mode
Simple VPN
(TUN + IP Pool)
GTP Stack
(S2b)
Diameter S6b



الأوضاع التشغيلية

يدعم OmniEPDG وضعين تشغيليين يتم اختيارهما عبر معلمة التكوين `vpn_mode`.

وضع GTP

يتم تغليف حركة مرور المشتركين في GTP-U عبر PGW. نفق GPP امل متوافق مع 3 وتوجيهها عبر الشبكة الأساسية المحمولة.

استخدم عندما:

- التكامل مع بنية الشبكة الأساسية المحمولة الحالية
- السياسة والفوترة عبر PCRF/PCEF
- مطلوب التجوال والتسليم بين المشغلين

المكونات:

- Diameter S6b لتفويض جلسة PGW
- GTPv2-C (إنشاء/حذف/تعديل الجلسة) لإدارة الجلسات
- وحدة GTP-U في نواة Linux للطائرة المستخدمة

وضع VPN بسيط

يتم توجيه حركة مرور المشتركين مباشرة عبر مضيف TUN. المحلي عبر واجهة IP تفريغ OmniEPDG دون تدخل PGW.

استخدم عندما:

- نشر مستقل دون PGW
- الاختبار والتطوير

- سيناريوهات التفريغ المحلي

المكونات:

- إدارة مجموعة IP المحلية (IPv4/IPv6)
- واجهة TUN (`omniepdg0`) مع مسارات مضيف لكل مشترك
- تخفي اختياري للوصول إلى الإنترنت/NAT

أمان المصادقة

يتضمن OmniEPDG ميزات أمان مدمجة لحماية ضد هجمات القوة الغاشمة و��قييد الوصول حسب الموقع الجغرافي. راجع دليل أمان المصادقة للحصول على التفاصيل.

تحديد المعدل

يحمي من هجمات القوة الغاشمة عن طريق تتبع محاولات المصادقة الفاشلة:

- **تحديد لكل IP** - يحظر IPs (حظر لمدة 5 دقائق) بعد 10 فشل في دقيقة واحدة
- **تحديد لكل IMSI** - يحظر IMSIs (حظر لمدة 10 دقائق) بعد 5 فشل في دقيقة واحدة
- خوارزمية نافذة منزلقة مع انتهاء تلقائي
- المصادقة الناجحة تمسح تاريخ الفشل

حظر الدول عبر GeoIP

تحكم جغرافي اختياري باستخدام قاعدة بيانات MaxMind GeoLite2:

- **وضع القائمة البيضاء** - السماح فقط بالاتصالات من الدول المحددة
- **وضع القائمة السوداء** - حظر الاتصالات من الدول المحددة
- معالجة قابلة للتكوين لعنوان IP غير المعروف/الخاص
- سلوك الفشل المفتوح أو المغلق عند عدم توفر قاعدة البيانات

التكوين الرئيسي

التكوين الأدنى (وضع VPN بسيط)

```
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}
    ]
  }
```

تمكين أمان المصادقة

```
config :omniepdg,
  # تحديد المعدل (مفعل بشكل افتراضي مع هذه القيم)
  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,

  # حظر GeoIP (معطل بشكل افتراضي)
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ"]
```

راجع مرجع التكوين للحصول على توثيق كامل للمعلمات.

المراقبة

لوحة التحكم

يمكن الوصول إلى لوحة التحكم على الويب في `http://<host>:4000/dashboard` لـ:

- مراقبة الجلسات في الوقت الحقيقي
- حالة أقران Diameter
- تدفق السجلات المباشرة
- تكوين النظام

راجع دليل لوحة التحكم للحصول على التفاصيل.

قياسات Prometheus

استخرج القياسات من `http://<host>:9568/metrics` لـ:

- معدلات نجاح/فشل المصادقة
- أحداث دورة حياة الجلسة
- زمن إشارة Diameter
- أحداث الأمان (حظر، تحديد المعدل GeoIP)
- استخدام مجموعة IP
- إحصائيات بيانات ESP

راجع مرجع القياسات للحصول على استعلامات وقواعد التنبيه.

استكشاف الأخطاء وإصلاحها

المشكلات الشائعة وخطوات الحل:

قسم الدليل	فحص سريع	المشكلة
فشل المصادقة	تحقق من SWx MAR/MAA في السجلات	فشل المصادقة
اتصال Diameter	تحقق من حالة الأقران في لوحة التحكم	مشكلات اتصال Diameter
فشل نفق GTP	تحقق من رموز سبب GTPv2-C	فشل نفق GTP
فشل VPN البسيطة	تحقق من واجهة TUN والمسارات	مشكلات VPN بسيطة
مشكلات تحديد المعدل	ضبط العتبات	إيجابيا�� كاذبة في تحديد المعدل
مشكلات GeoIP	تحقق من قاعدة البيانات ورموز الدول	مشكلات حظر GeoIP

راجع دليل استكشاف الأخطاء وإصلاحها للحصول على إجراءات تشخيصية مفصلة.

فهرس الوثائق

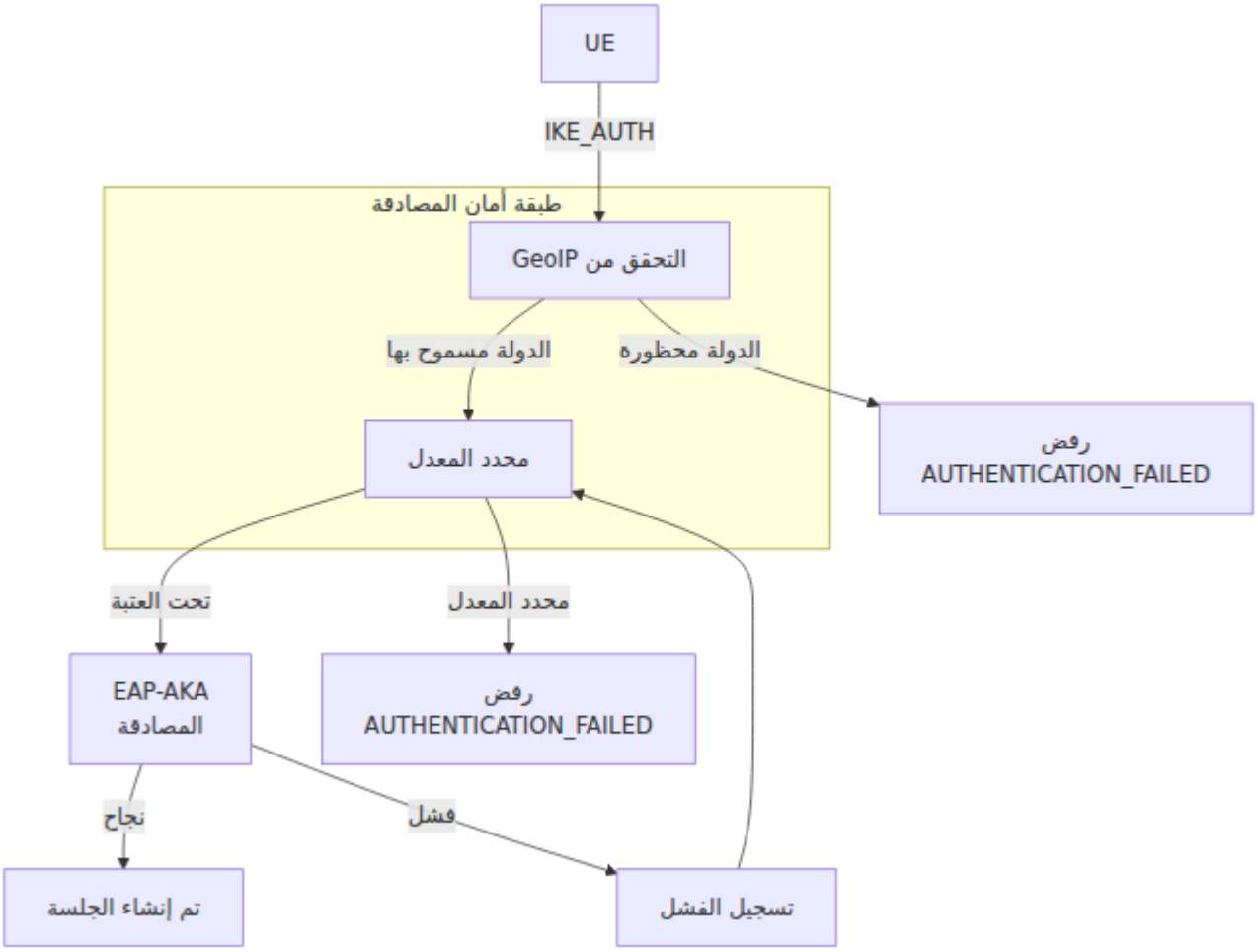
الوثيقة	الوصف
العمارة	تصميم النظام، آلات الحالة، تدفقات المكالمات، مراجع البروتوكول
التكوين	مرجع تكوين كامل مع أمثلة
لوحة التحكم	دليل واجهة الويب مع لقطات شاشة
القياسات	قياسات Prometheus، وتنبيهات، استعلامات
متطلبات الشبكة	منافذ جدار الحماية وإدخالات DNS للنشر
الأمان	تحديد المعدل وحظر الدول عبر GeoIP
استكشاف الأخطاء وإصلاحها	المشكلات الشائعة وإجراءات التشخيص

أمان المصادقة في OmniEPDG

تقوم OmniEPDG، بتنفيذ عدة طبقات من أمان المصادقة لحماية ضد هجمات القوة الغاشمة، وتعبئة بيانات الاعتماد، والوصول غير المصرح به من المناطق المحظورة.

جدول المحتويات

نظرة عامة



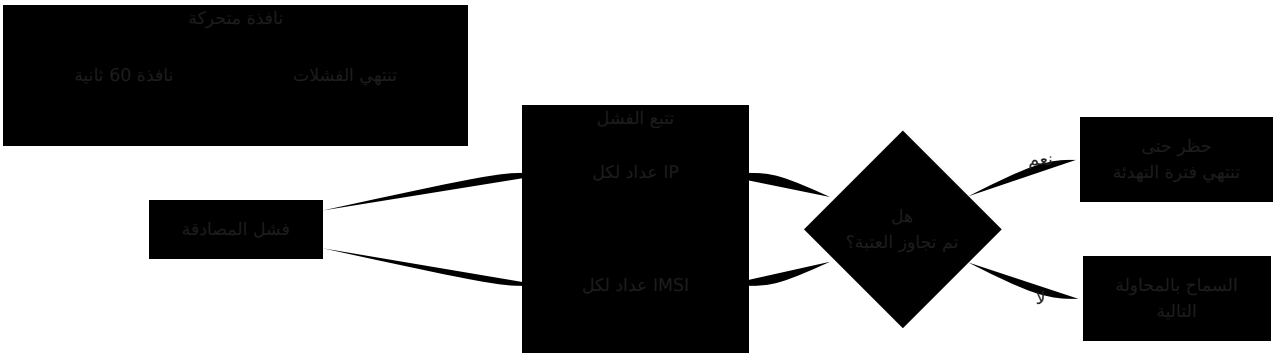
تقوم OmniEPDG بإجراء فحوصات الأمان في بداية تبادل IKE_AUTH، قبل العمليات التشفيرية المكلفة:

1. **التحقق من GeoIP** (اختياري) - يتحقق من أن عنوان IP المصدر من دولة مسموح بها
2. **التحقق من تحديد المعدل** - يضمن أن IP/IMSI لم يتجاوز عتبات الفشل
3. **المصادقة EAP-AKA** - إذا تم اجتياز الفحوصات 3GPP تستمر المصادقة القياسية

تحديد معدل المصادقة

يحمي تحديد المعدل ضد هجمات القوة الغاشمة من خلال تتبع محاولات المصادقة الفاشلة لكل عنوان IP ومعدل IMSI. عندما يتم تجاوز العتبات، يتم حظر المحاولات الإضافية مؤقتًا.

كيف يعمل



يستخدم محدد المعدل **خوارزمية النافذة المتحركة**:

- يتم تسجيل كل محاولة فاشلة مع طابع زمني
- يتم انتهاء المحاولات الأقدم من النافذة المكونة تلقائيًا
- عندما تتجاوز الفشلات في النافذة العتبة، يتم حظر المصدر
- تنتهي الحظرات بعد فترة التهدئة المكونة

تتبع مزدوج

يتم فرض حدين مستقلين في نفس الوقت:

نوع التتبع	الغرض	العتبة الافتراضية	مدة الحظر الافتراضية
لكل IP	يلتقط ماسحات المنافذ والهجمات الموزعة من مصادر واحدة	10 / فشلات دقيقة	5 دقائق
لكل IMSI	يلتقط الهجمات المستهدفة على مشتركين محددين	5 / فشلات دقيقة	10 دقائق

يجب أن يتم اجتياز كلا الفحصين لكي تستمر محاولة المصادقة. إذا تم تجاوز أي من العتبات، يتم رفض المحاولة.

التكوين

```
config :omniepdg,
  # تحديد المعدل لكل IP
  auth_rate_limit_per_ip: 10,           # الحد الأقصى للفشلات قبل الحظر
  auth_rate_limit_ip_window_ms: 60_000,  # حجم النافذة (1 دقيقة)
  auth_rate_limit_ip_block_ms: 300_000,  # مدة الحظر (5 دقائق)

  # تحديد المعدل لكل IMSI
  auth_rate_limit_per_imsi: 5,            # الحد الأقصى للفشلات قبل الحظر
  auth_rate_limit_imsi_window_ms: 60_000,  # حجم النافذة (1 دقيقة)
  auth_rate_limit_imsi_block_ms: 600_000   # مدة الحظر (10 دقائق)
```

معلمات لكل IP

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`auth_rate_limit_per_ip`	عدد صحيح	لا	`10`	الحد الأقصى لمحاولات المصادقة الفاشلة المسموح بها من عنوان IP واحد خلال فترة النافذة قبل ال��ظر.
`auth_rate_limit_ip_window_ms`	عدد صحيح	لا	`60000`	حجم النافذة المتحركة بالمللي ثانية لتعداد فشلات IP. الفشلات الأقدم من ذلك لا تُحتسب.
`auth_rate_limit_ip_block_ms`	عدد صحيح	لا	`300000`	مدة الحظر بالمللي ثانية لعنوان IP بعد تجاوز العتبة. الافتراضي هو 5 دقائق.

معلمات لكل IMSI

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`auth_rate_limit_per_imsi`	عدد صحيح	لا	`5`	الحد الأقصى لمحاولات المصادقة الفاشلة المسموح بها لـ IMSI واحد خلال فترة النافذة قبل الحظر. أقل من المعدل لكل IP لالتقاط الهجمات المستهدفة.
`auth_rate_limit_imsi_window_ms`	عدد صحيح	لا	`60000`	حجم النافذة المتحركة بالمللي ثانية لتعداد فشلات IMSI.
`auth_rate_limit_imsi_block_ms`	عدد صحيح	لا	`600000`	مدة الحظر بالمللي ثانية لـ IMSI بعد تجاوز العتبة. الافتراضي

الوصف	الافتراضي	مطلوب	النوع	المعلمة
هو 10 دقائق أطول من) IP حظرات لحماية المشتركين المحددين).				

السلوك عند النجاح

عندما تنجح المصادقة، يقوم محدد المعدل بمسح كل تاريخ الفشل لذلك الزوج من IP/IMSI. وهذا يسمح للمستخدمين الشرعيين الذين واجهوا فشلات عابرة (مثل مشاكل الشبكة) بالتعافي دون أن يتم معاقبتهم بشكل دائم.

أمثلة على التكوينات

بيئة عالية الأمان

حدود صارمة للبيئات ذات التسامح المنخفض مع الفشلات:

```
config :omniepdg,
  auth_rate_limit_per_ip: 5,
  auth_rate_limit_ip_window_ms: 120_000,   # نافذة 2 دقيقة
  auth_rate_limit_ip_block_ms: 900_000,    # حظر 15 دقيقة

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

كيف يعمل: يُسمح فقط بـ 5 فشلات لكل IP أو 3 فشلات لكل IMSI. خلال نافذة مدتها دقيقتان. تستمر الحظرات لمدة 15-30 دقيقة على التوالي.

حالة الاستخدام: نشرات الشركات، قواعد مشتركي عالية القيمة، أو الشبكات تحت هجوم نشط.

بيئة مريحة

حدود أكثر تساهلاً للتطوير أو الاختبار:

```
config :omniepdg,
  auth_rate_limit_per_ip: 50,
  auth_rate_limit_ip_window_ms: 60_000,
  auth_rate_limit_ip_block_ms: 60_000,     # حظر 1 دقيقة

  auth_rate_limit_per_imsi: 20,
  auth_rate_limit_imsi_window_ms: 60_000,
  auth_rate_limit_imsi_block_ms: 120_000   # حظر 2 دقيقة
```

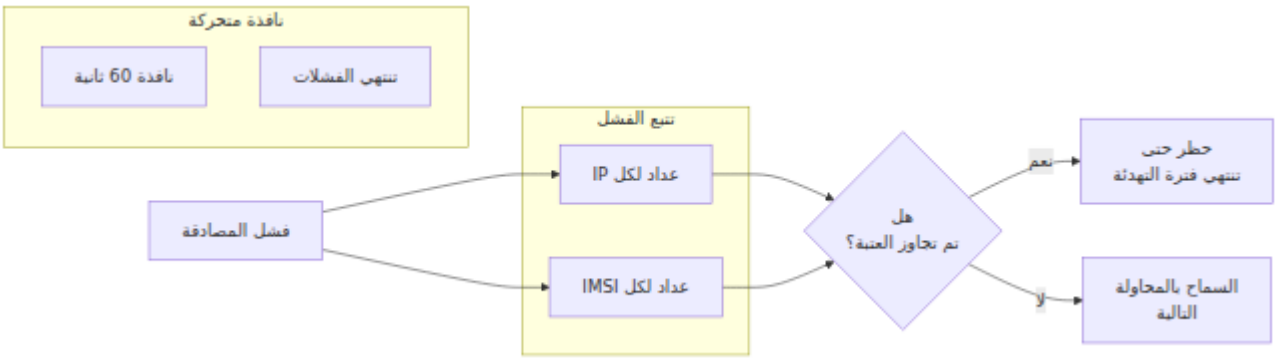
كيف يعمل: تتيح العتبات الأعلى والحظرات الأقصر مزيدًا من المرونة في الاختبار.

حالة الاستخدام: بيئات التطوير، اختبار التكامل.

حظر الدول باستخدام GeoIP

يقيّد حظر GeoIP الوصول إلى مكالمات WiFi بناءً على الموقع الجغرافي لعنوان IP هذا المتصل. مفيد للمشغلين الذين يحتاجون إلى تقييد الخدمة لدول معينة لأسباب تنظيمية أو تجارية.

نظرة عامة



قاعدة بيانات MaxMind GeoLite2

تستخدم عمليات بحث GeoIP قاعدة بيانات MaxMind GeoLite2 Country، وهي قاعدة بيانات مجانية لتحديد الموقع الجغرافي لعنوان IP مع تحديثات أسبوعية.

لتفعيل حظر GeoIP:

1. قم بالتسجيل للحصول على حساب مجاني في MaxMind GeoLite2 Signup
2. قم بتنزيل ملف قاعدة البيانات `GeoLite2-Country.mmdb`
3. ضع الملف في المسار المكون (الافتراضي: `/etc/omniepdg/GeoLite2-Country.mmdb`)
4. قم بتمكين GeoIP في التكوين

التكوين

```
config :omniepdg,
  # تفعيل حظر GeoIP
  geoip_enabled: true,

  # المسار إلى قاعدة بيانات MaxMind
  geoip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",

  # وضع التحكم في الوصول
  geoip_mode: :whitelist,

  # قائمة الدول (رموز ISO 3166-1 alpha-2)
  geoip_countries: ["AU", "NZ"],

  # التعامل مع IPs غير المعروفة
  geoip_allow_unknown: false,

  # السلوك عند عدم توفر قاعدة البيانات
  geoip_fail_open: true
```

المعلمات

المعلمة	النوع	مطلوب	الافتراضي	
`geoip_enabled`	Boolean	لا	`false`	و م ت ت C ن ع ن ن ة
`geoip_database_path`	String	لا	`"/etc/omniepdg/GeoLite2-Country.mmdb"`	ت ة ت M C C ت M
`geoip_mode`	Atom	لا	`:whitelist`	م ت (ت ة (، ج ة

المعلمة	النوع	مطلوب	الافتراضي	
`geoip_countries`	List	لا	`[]`	ز ب 3 a ر ب g
`geoip_allow_unknown`	Boolean	لا	انظر أدناه	ح ن ا د ل ا ر ة و ا ، و ة ء
`geoip_fail_open`	Boolean	لا	`true`	د ب C ن ع ب . ن ا ع

المعلمة	النوع	مطلوب	الافتراضي	
				ك)

أوضاع التحكم في الوصول

وضع القائمة البيضاء (موصى به لمكالمات WiFi)

يسمح فقط بالاتصالات من الدول المحددة. يتم حظر جميع الدول الأخرى.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :whitelist,
  geoip_countries: ["AU", "NZ", "FJ"]  # أستراليا، نيوزيلندا، فيجي
```

كيف يعمل: يمكن فقط للأجهزة المتصلة من عناوين IP الأسترالية أو النيوزيلندية أو الفيجية المصادقة. يتم رفض جميع الدول الأخرى.

حالة الاستخدام: المشغلون الذين يرغبون في تقييد مكالمات WiFi إلى مناطق خدمتهم المرخصة.

وضع القائمة السوداء

يتم حظر الاتصالات من ال��ول المحددة. يُسمح بجميع الدول الأخرى.

```
config :omniepdg,
  geoip_enabled: true,
  geoip_mode: :blacklist,
  geoip_countries: ["CN", "RU", "KP", "IR"]  # الصين، روسيا، كوريا الشمالية، إيران
```

كيف يعمل: يتم رفض الأجهزة المتصلة من الدول المدرجة. يمكن لجميع الدول الأخرى المصادقة.

حالة الاستخدام: حظر المناطق عالية المخاطر مع السماح بالتجوال العالمي.

التعامل مع الدول غير المعروفة

بعض عناوين IP لا يمكن تحديد موقعها:

- النطاقات الخاصة (10.x.x.x، 192.168.x.x، إلخ)
- كتل IP المخصصة حديثًا التي لم تُدرج بعد في قاعدة البيانات
- نقاط خروج Tor وبعض الشبكات الافتراضية الخاصة

تتحكم معلمة `geoip_allow_unknown` في السلوك:

الوضع	القيمة الافتراضية لـ `geoip_allow_unknown`	السلوك
القائمة البيضاء	`false`	غير معروف = غير موجود في القائمة البيضاء = محظور
القائمة السوداء	`true`	غي�� معروف = غير موجود في القائمة السوداء = مسموح

لتجاوز الافتراضي:

```
config :omniepdg,
  geoip_mode: :whitelist,
  geoip_allow_unknown: true  # السماح بـ IPs غير معروفة حتى في وضع القائمة البيضاء
```

تحديثات قاعدة البيانات

تقوم MaxMind بتحديث قاعدة بيانات GeoLite2 أسبوعيًا. للتحديث:

1. قم بتنزيل ملف `GeoLite2-Country.mmdb` الجديد
2. استبدل الملف الموجود في المسار المكون
3. يتم إعادة تحميل قاعدة البيانات تلقائيًا في البحث التالي (لا حاجة لإعادة التشغيل)

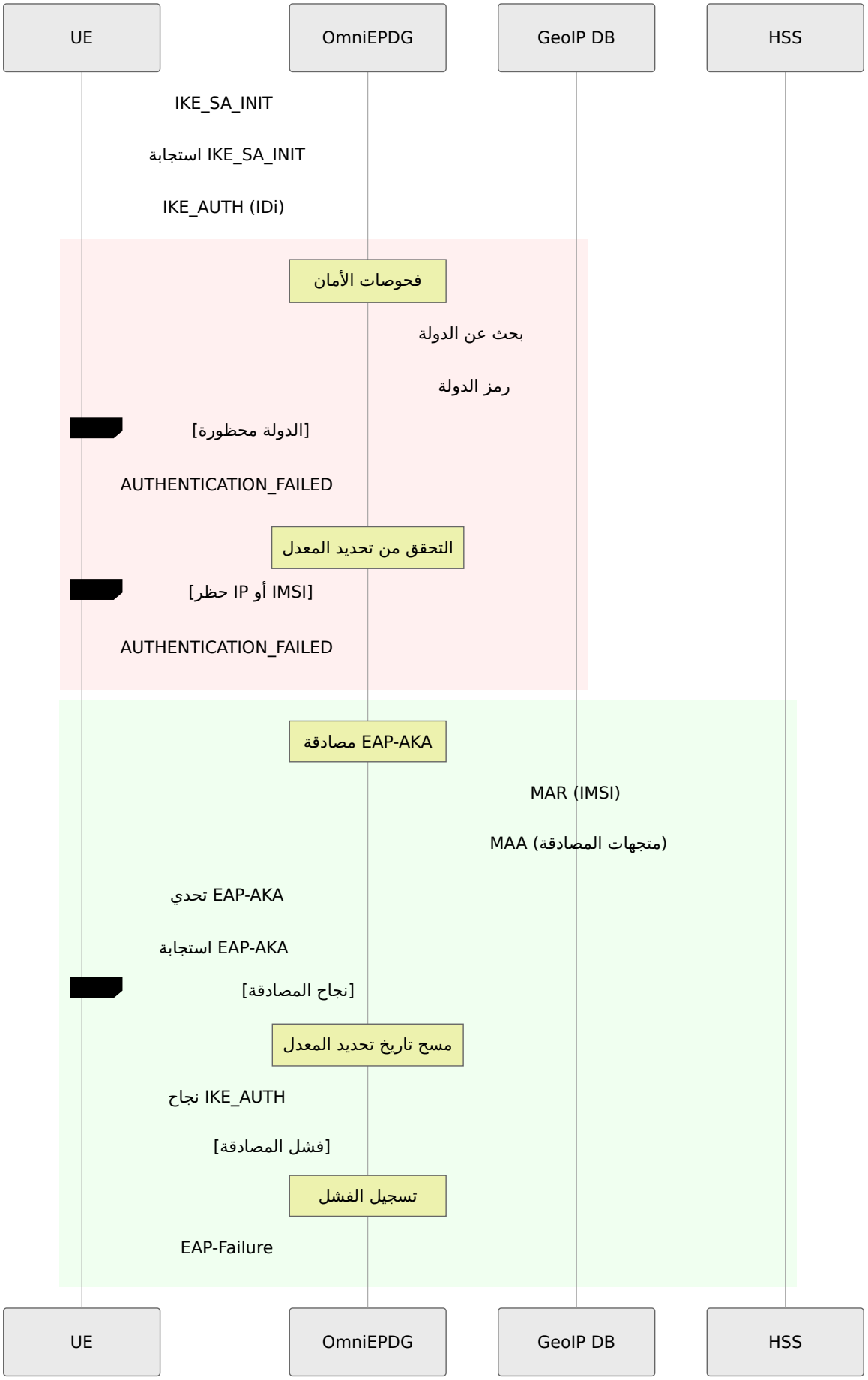
رموز الدول الشائعة

الدولة	الرمز	الدولة	الرمز
الولايات المتحدة	US	أستراليا	AU
المملكة المتحدة	GB	نيوزيلندا	NZ
ألمانيا	DE	كندا	CA
اليابان	JP	فرنسا	FR
هونغ كونغ	HK	سنغافورة	SG
الصين	CN	الهند	IN

القائمة الكاملة: ISO 3166-1 alpha-2

تدفق الأمان

تدفق أمان المصادقة الكامل:


UE
OmniEPDG
GeoIP DB
HSS
IKE_SA_INIT
استجابة IKE_SA_INIT
IKE_AUTH (IDi)
فحوصات الأمان
بحث عن الدولة
رمز الدولة
[الدولة محظورة]
AUTHENTICATION_FAILED
التحقق من تحديد المعدل
[IMSI أو IP حظر]
AUTHENTICATION_FAILED
مصادقة EAP-AKA
MAR (IMSI)
MAA (متجهات المصادقة)
تحدي EAP-AKA
استجابة EAP-AKA
[نجاح المصادقة]
مسح تاريخ تحديد المعدل
نجاح IKE_AUTH
[فشل المصادقة]
تسجيل الفشل
EAP-Failure
UE
OmniEPDG
GeoIP DB
HSS

المقاييس

مقاييس تحديد المعدل

النوع: عداد **الوصف**: عدد محاولات `epdg_auth_rate_limited_count` **المقياس**: المصادقة المحظورة بواسطة تحديد المعدل **التسميات**:

- `type` - سبب الحظر: `ip` (تم تجاوز عتبة IP) أو `imsi` (تم تجاوز عتبة IMSI)

استعلامات المثال:

```
# محاولات محددة بالمعدل في الدقيقة
rate(epdg_auth_rate_limited_count[1m])

# محدد بالمعدل حسب النوع
sum by (type) (rate(epdg_auth_rate_limited_count[5m]))

# تنبيه: نشاط تحديد المعدل العالي
rate(epdg_auth_rate_limited_count[5m]) > 10
```

مقاييس GeoIP

النوع: عداد **الوصف**: عدد محاولات `epdg_auth_geoip_blocked_count` **المقياس**: المصادقة المحظورة بواسطة GeoIP **التسميات**:

- `country` - رمز الدولة ISO 3166-1 alpha-2، أو `UNKNOWN` لعناوين IP التي لا يمكن حلها

استعلامات المثال:

```
# حظرات GeoIP في الدقيقة
rate(epdg_auth_geoip_blocked_count[1m])

# أعلى الدول المحظورة
topk(10, sum by (country) (epdg_auth_geoip_blocked_count))

# تنبيه: دولة غير عادية تحاول الوصول
increase(epdg_auth_geoip_blocked_count{country="XX"}[1h]) > 100
```

استكشاف الأخطاء وإصلاحها

مشاكل تحديد المعدل

حظر المستخدمين الشرعيين

الأعراض: المستخدمون يبلغون عن عدم قدرتهم على الاتصال بعد محاولات فاشلة

الأسباب المحتملة:

- أدخل المستخدم بيانات اعتماد خاطئة عدة مرات
- تسببت مشاكل الشبكة في انتهاء مهلة المصادقة التي تم احتسابها كفشلات
- تم ضبط العتبات منخفضة جدًا للبيئة

الحل:

1. تحقق من المقاييس لعنوان IP/IMSI المتأثر
2. اعتبر زيادة العتبات إذا كانت النتائج الإيجابية الكاذبة شائعة
3. بعد إصلاح السبب الجذري، ستنتهي الحظرة تلقائيًا

معدل مرتفع من المحاولات المحظورة

الأعراض: `epdg_auth_rate_limited_count` تزداد بسرعة

الأسباب المحتملة:

- هجوم قوة غاشمة جارٍ
- غير مكون بشكل صحيح تفشل في المصادقة بشكل متكرر UE
- هجوم تعبئة بيانات الاعتماد

الحل:

1. مراجعة عناوين IP المصدر في السجلات للأنماط
2. تنفيذ قواعد جدار حماية على مستوى IP اعت��ر للمهاجمين المستمرين
3. إذا تأثر المستخدمون الشرعيون تحقق من الاتصال بـ HSS

مشاكل GeoIP

حظر جميع الاتصالات

الأعراض: لا يمكن لأي UE الاتصال بعد تفعيل GeoIP

الأسباب المحتملة:

- لم يتم العثور على ملف قاعدة البيانات أو أنه تالف
- رموز الدول خاطئة في التكوين
- `geoip_allow_unknown: false` تحظر عناوين IP الخاصة في بيئة المختبر

الحل:

1. تحقق من وجود ملف قاعدة البيانات في المسار المكون
2. تحقق من صحة رموز الدول (حروف كبيرة، 2 حرف)
3. في بيئة المختبر/التطوير، اضبط `geoip_allow_unknown: true`
4. تحقق من السجلات للتحذيرات المتعلقة بـ GeoIP

لا تُحمّل GeoIP قاعدة بيانات

الأعراض: تحذير في السجلات: "لم يتم العثور على قاعدة بيانات GeoIP"

الأسباب المحتملة:

- المسار غير صحيح
- أذونات الملف تمنع القراءة
- الملف ليس بتنسيق MMDB صالح

الحل:

1. تحق��: من وجود الملف `ls -la /etc/omniepdg/GeoLite2-Country.mmdb`
2. تحقق من الأذونات: `chmod 644 /etc/omniepdg/GeoLite2-Country.mmdb`
3. تحقق من سلامة الملف عن طريق تنزيل نسخة جديدة من MaxMind

حظرات دول غير متوقعة

الأعراض: يتم حظر المستخدمين من الدول المسموح بها

الأسباب المحتملة:

- VPN/وكيل يجعل IP يظهر من دولة مختلفة
- قاعدة بيانات GeoIP قديمة
- مخرج الشبكة المؤسسية في موقع غير متوقع

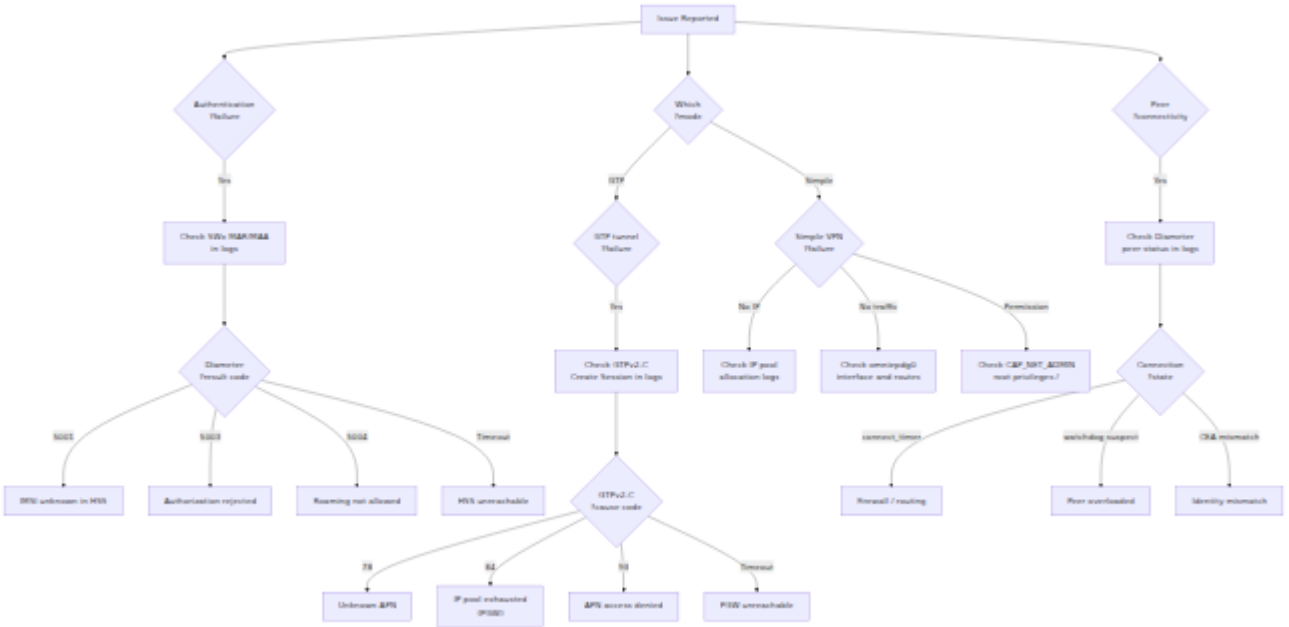
الحل:

1. تحديث قاعدة بيانات GeoIP إلى أحدث إصدار
2. تحقق من عنوان IP الفعلي للمستخدم مقابل الدولة المتوقعة
3. اعتبر إضافة دول إضافية إذا كان المستخدمون يتجولون عبر الشبكات المؤسسية

استكشاف OmniEPDG وإصلاحها الأخطاء

يغطي هذا الدليل القضايا التشغيلية الشائعة، وإجراءات التشخيص، وخطوات الحل لـ OmniEPDG.

نظرة عامة على التشخيص



ملفات السجل

يكتب OmniEPDG السجلات إلى دليل `log/` بالنسبة لدليل العمل الخاص بالتطبيق. راجع مرجع التكوين للحصول على تفاصيل تكوين السجل.

الملف	الغرض	متى يتم التحقق
`log/console.log`	جميع رسائل التطبيق على مستوى التصحيح	النقطة الأولى للتحقيق في أي مشكلة
`log/error.log`	ا��أخطاء فقط	مسح سريع للمشاكل النشطة
`log/crash.log`	عمليات OTP المعطلة	عندما يتم إعادة تشغيل العمليات بشكل غير متوقع
`log/erlang.log`	مسجل نواة Erlang	مشكلات Erlang/OTP على مستوى منخفض

أنماط السجل الرئيسية

أحداث اتصال نظير Diameter:

- `peer_up` - تم الاتصال بنظير Diameter وتبادل القدرات
- `peer_down` - تم فصل نظير Diameter

انتقالات حالة FSM UE:

- `ue_fsm state_<name> event=<event>` - تعالج FSM حدثًا في حالة معينة
- `ue_fsm init(&lt;IMSI>)` - تم إنشاء مثيل جديد من FSM للاشتراك
- `terminating epdg_ue_fsm with reason <reason>` - إيقاف تشغيل FSM

أحداث المهلة:

- `Timeout swm_der_timeout` - تجاوزت المهلة SWm DER استجابة
- `Timeout create_session_timeout` - استجابة GTPv2-C Create Session تجاوزت المهلة
- `Timeout s2b_delete_session_timeout` - استجابة GTPv2-C Delete Session تجاوزت المهلة
- `Timeout cancel_location_timeout` - تجاوزت Cancel Location استجابة المهلة

مشكلات الاتصال Diameter

فشل الاتصال بـ HSS (SWx)

الأعراض: لا ��مكن لأي مشتركين المصادقة. تظهر السجلات محاولات اتصال متكررة بـ HSS.

الأسباب المحتملة:

- جدار ناري يحظر منفذ SCTP 3868 بين OmniEPDG و HSS
- عنوان `dia_swx_remote_ip` أو `dia_swx_remote_port` غير صحيح في التكوين
- Diameter غير قيد التشغيل أو لا يقبل اتصالات HSS
- SCTP غير مفعل على مسار الشبكة (بعض الجدران النارية تحظر SCTP بشكل افتراضي)
- عدم تطابق Origin-Host أو Origin-Realm مما يتسبب في رفض CEA

الحل:

1. تحقق من الاتصال الشبكي بعنوان HSS والمنفذ
2. تأكد من أن `dia_swx_remote_ip` و `dia_swx_remote_port` تتطابق مع تكوين HSS
3. تحقق من أن حركة مرور SCTP مسموح بها عبر جميع الجدران النارية. إذا تم حظر SCTP، قم بتعيين `dia_swx_proto` إلى `tcp` كخيار احتياطي
4. تحقق من أن `dia_swx_origin_host` هو اسم مجال مؤهل قابل للحل ويتطابق مع ما يتوقعه HSS
5. تحقق من سجلات HSS للحصول على فشل في التفاوض على Diameter CER/CEA

فشل الاتصال بـ PGW (S6b)

الأعراض: تنجح المصادقة ولك�� فشل إنشاء نفق GTP أو لم تصل AAR من PGW. تظهر السجلات عدم وجود حدث peer_up لـ S6b.

الأسباب المحتملة:

- غير مكون للاتصال بمستمع PGW الخاص بـ S6b OmniEPDG
- جدار ناري يحظر منفذ SCTP 3868 على عنوان الربط S6b الخاص بـ OmniEPDG
- `dia_s6b_local_ip` غير قابل للوصول من PGW

- عدم تطابق Origin-Host أو Origin-Realm

الحل:

1. تأكد من أن PGW مكون للاتصال بـ OmniEPDG عند `dia_s6b_local_ip`:`dia_s6b_local_port`
2. تحقق من أن عنوان الربط S6b قابل للوصول من شبكة PGW
3. تحقق من أن قواعد الجدار الناري تسمح بحركة SCTP الواردة على المنفذ 3868 عند عنوان S6b
4. تحقق من أن `dia_s6b_origin_host` و `dia_s6b_origin_realm` تتطابق مع ما يتوقعه PGW

فشل مراقبة Diameter

الأعراض: تتقطع اتصالات Diameter القائمة بشكل متقطع. تظهر السجلات انتقالات المراقبة إلى حالة SUSPECT أو DOWN.

الأسباب المحتملة:

- عدم استقرار مسار الشبكة أو فقدان الحزم
- نظير محمّل بشكل زائد ولا يستجيب لـ DWR ضمن `dia_swx_watchdog_timer`
- تكوين مراقبة عدواني (عدد قليل جدًا من المحاولات قبل إعلان الشك)

الحل:

1. تحقق من جودة مسار الشبكة (فقدان الحزم، الكمون) بين OmniEPDG والنظير
2. إذا كان من المتوقع فقدان الحزم، قم بزيادة عتبات `dia_swx_watchdog_config` / `dia_s6b_watchdog_config` (على سبيل المثال، `[{okay, 5}, {suspect, 3}]`)
3. تحقق من صحة نظام النظير (CPU، عدد الاتصالات، الذاكرة)

فشل المصادقة

IMSI غير معروف (Diameter 5001)

الأعراض: يفشل مشتركون محددون في مصادقة EAP-AKA. تظهر السجلات SWx MAA مع رمز النتيجة 5001 (DIAMETER_ERROR_USER_UNKNOWN).

الأسباب المحتملة:

- المشترك غير مكون في HSS
- عدم تطابق IMSI بين بطاقة SIM الخاصة بـ UE وقاعدة بيانات HSS
- تنسيق NAI غير صحيح، مما يتسبب في فشل استخراج IMSI

الحل:

1. تحقق من وجود IMSI المشترك في قاعدة بيانات HSS
2. تحقق من أن تنسيق NAI في السجلات يتطابق مع النمط المتوقع: `0<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org`
3. تأكد من أن IMSI بطاقة SIM تتطابق مع القيمة المكونة في HSS

تم رفض التفويض (Diameter 5003)

الأعراض: يتم المصادقة على المشترك ولكن يتم رفضه أثناء تعيين الخادم. تظهر السجلات SWx SAA مع رمز النتيجة 5003.

الأسباب المحتملة:

- المشترك غير مخول لخدمة الاتصال عبر WiFi
- APN غير مسموح به لهذا المشترك
- قيود على ملف تعريف الاشتراك

الحل:

1. تحقق من ملف تعريف خدمة المشترك في HSS
2. تأكد من تمكين الوصول إلى WiFi / ePDG للمشترك
3. تأكد من أن APN المطلوب موجود في قائمة APN المسموح بها للمشترك

التجوال غير مسموح (Diameter 5004)

الأعراض: يفشل المشتركون المتجولون في المصادقة. تظهر السجلات SWx MAA أو SAA مع رمز النتيجة 5004.

الأسباب المحتملة:

- ترفض موقع المشترك الحالي HSS سياسة التجوال في
- غير مسموح به للمشتركين المتجولين WiFi الاتصال عبر

الحل:

1. راجع سياسات التجوال في HSS لمجموعة HPLMN/VPLMN الخاصة بالمشترك
2. مسموحًا به بموجب اتفاقيات التجوال WiFi تحقق مما إذا كان الاتصال عبر

انتهاء مهلة المصادقة

الأعراض: تتعطل المصادقة ثم تفشل بعد 10 ثوانٍ. تظهر السجلات `Timeout swm_der_timeout` في `state_wait_auth_resp`.

الأسباب المحتملة:

- HSS لا يستجيب لـ SWx MAR خلال 10 ثوانٍ
- تم قطع اتصال Diameter لـ SWx أثناء الطلب
- HSS محمّل بشكل زائد

الحل:

1. تحقق من استجابة HSS والحمولة
2. تحقق من أن نظير Diameter لـ SWx في حالة OKAY (ليس SUSPECT أو DOWN)
3. تحقق من أن `dia_swx_transmit_timer` كافٍ للكمون الشبكي إلى HSS

عدم تطابق نوع EAP-AKA

الأعراض: تفشل المصادقة مع خطأ "type_mismatch" في السجلات. لا يتطابق بادئة هوية UE مع طريقة EAP المستخدمة.

الأسباب المحتملة:

- UE `0` يرسل الهوية مع بادئة (EAP-AKA) ولكن الشبكة تتوقع EAP-AKA'، أو العكس
- HSS يعيد متجهات المصادقة لنوع EAP خاطئ

3 **الخلفية**: وفقًا لمعيار 3GPP TS 23.003، تشير بادئة هوية NAI المتوقع المصادقة ع��ى ن إلى:

- EAP-AKA تشير بادئة `0` إلى
- EAP-AKA' تشير بادئة `6` إلى

يختار OmniEPDG تلقائيًا طريقة المصادقة بناءً على بادئة هوية UE. تستخدم معظم أجهزة الاتصال عبر WiFi بادئة `0` (EAP-AKA).

الحل:

1. تحقق من هوية NAI الخاصة بـ UE في السجلات للتحقق من البادئة
2. تأكد من أن HSS مكون لإعادة متجهات المصادقة المناسبة
3. تحقق من أن بطاقة SIM مكونة بشكل صحيح لنوع المصادقة المتوقع

EAP-AKA RES عدم تطابق

الأعراض: تفشل المصادقة بعد التحدي/الاستجابة. تظهر السجلات "RES mismatch" أو "res_mismatch" خطأ.

الأسباب المحتملة:

- فشل مصادقة بطاقة SIM
- عدم تطابق اشتقاق المفتاح بين UE والشبكة
- متجهات المصادقة التالفة من HSS

الحل:

1. تحقق من أن بطاقة SIM صالحة وليست تالفة
2. تحقق من أن HSS أعاد متجهات المصادقة الصحيحة (RAND، AUTN، XRES، CK، IK)
3. قم بتمكين تسجيل الأخطاء لمقارنة RES المستلم مع XRES المتوقع
4. إذا كنت تستخدم بطاقات SIM تجريبية، تحقق من أن قيم Ki و OP/OPc تتطابق بين HSS و SIM

فشل نفق GTP (وضع GTP فقط)

تم رفض إنشاء جلسة من قبل PGW

الأعراض: تنجح المصادقة ولكن فشل إنشاء النفق. تظهر السجلات استجابة GTPv2-C Create Session مع سبب الخطأ.

أكواد الأسباب الشائعة والإجراءات:

رمز السبب	الاسم	الإجراء
78	APN مفقود أو غير معروف	تحقق من تكوين APN على PGW وتطابقه مع ملف تعريف المشترك
82	RAT مرفوض في	تحقق من أن سياسة PGW تسمح بنوع الوصول عبر WiFi (3 غيرGPP)
84	جميع العناوين الديناميكية مشغولة	قم بتوسيع PGW الخاصة بـ IP نفدت مجموعة ؛ المجموعة أو تحقق من التسريبات
92	فشل مصادقة المستخدم	تحقق من PGW فشل المصادقة على جانب ؛ S6b تفويض جلسة
93	تم رفض الوصول إلى APN	PGW على APN المشترك غير مخول لـ
96	IMSI/IMEI غير معروف	تحقق من تفويض PGW المشترك غير معروف لـ ؛ S6b جلسة
113	APN ازدحام	PGW محمّل؛ أعد المحاولة أو تحقق من سعة APN
120	GTP-C ازدحام كيان	PGW محمّل في مستوى التحكم

انتهاء مهلة إنشاء الجلسة

الأعراض: يتعطل إنشاء النفق لمدة 10 ثوانٍ ثم يفشل. تظهر السجلات `Timeout create_session_timeout` في `state_wait_create_session_resp`.

الأسباب المحتملة:

- PGW غير قابل للوصول عند `gtpc_remote_ip`:`gtpc_remote_port`
- جدار ناري يحظر منفذ UDP 2123 بين PGW و OmniEPDG
- PGW محمّل بشكل زائد ولا يستجيب لطلبات GTPv2-C

الحل:

1. تحقق من الاتصال الشبكي بـ PGW على منفذ UDP 2123
2. تحقق من أن قواعد الجدار الناري تسمح بـ UDP 2123 بين PGW و OmniEPDG
3. تحقق من صحة GTPv2-C وسعة معالجة PGW

لا يمرر حركة المرور GTP-U نفق

الأعراض: تم إنشاء النفق (نجح إنشاء الجلسة) ولكن حركة مرور المشترك لا تتدفق.

الأسباب المحتملة:

- وحدة نواة GTP-U غير محملة
- عنوان مقبس `gtp_u_kmod` لا يتطابق مع عنوان نقطة نهاية نفق GTP-U المعلن إلى PGW
- لم يتم تكوين التوجيه لجهاز نفق GTP
- جدار ناري يحظر منفذ UDP 2152 (GTP-U)

الحل:

1. تحقق من أن وحدة GTP الخاصة بنواة Linux محملة (`lsmod | grep gtp`)
2. تأكد من وجود جهاز نفق GTP (`ip link show gtp0`)
3. تحقق من أن `gtp_u_kmod` `ip` يتطابق مع `gtpc_local_ip` أو العنوان المعلن في طلب إنشاء الجلسة
4. تحقق من أن جدول التوجيه يتضمن طرقًا عبر جهاز نفق GTP
5. تحقق من أن الجدار الناري يسمح بـ UDP المنفذ 2152 بين PGW و OmniEPDG

فشل VPN البسيط (وضع VPN البسيط فقط)

لم يتم إنشاء واجهة TUN

الأعراض: يبدأ OmniEPDG ولكن لا تظهر واجهة `omniepdg0`. تفشل الجلسات عند إعداد النفق. قد تظهر السجلات أخطاء من `simple_vpn_route` أثناء بدء التشغيل.

الأسباب المحتملة:

- عملية OmniEPDG تفتقر إلى قدرة `CAP_NET_ADMIN` أو لا تعمل كجذر
- وحدة نواة TUN/TAP غير محملة
- تم إنشاء واجهة أخرى بالفعل باسم `omniepdg0`

الحل:

1. تحقق من أن وحدة النواة TUN متاحة (`lsmod | grep tun`)
2. تأكد من أن OmniEPDG يعمل بامتيازات كافية لإنشاء واجهات TUN
3. تحقق مما إذا كانت `omniepdg0` موجودة بالفعل من مثيل سابق (`ip link show omniepdg0`)
4. تحقق من `log/crash.log` للحصول على أخطاء من عملية إدارة المسار

نفاد مجموعة IP

الأعراض: تنجح المصادقة ولكن فشل إعداد النفق. تظهر السجلات فشل تخصيص IP من `simple_vpn_pool`.

الأسباب المحتملة:

- تم تخصيص جميع العناوين في مجموعة CIDR المكونة للجلسات النشطة
- لم يتم تحرير عناوين IP (تسرب) بعد إنهاء الجلسة
- حجم المجموعة صغير جدًا لعدد المشتركين المتزامنين

الحل:

1. تحقق من عدد عمليات `epdg_ue_fsm` النشطة مقارنة بحجم المجموعة

2. تحقق من رسائل السجل (تحقق من أن الجلسات يتم إنهاؤها بشكل صحيح "terminating")
3. إذا كانت المجموعة ممتلئة حقًا، قم بتوسيعها باستخدام بادئة CIDR أكبر في `simple_vpn_pool_ipv4` (يتطلب إعادة التشغيل)
4. تحقق من وجود أعطال في FSM أثناء إنهاء الجلسة في `log/crash.log` التي قد تكون منعت تحرير IP

حركة مرور المشترك لا تتدفق

الأعراض: تم إنشاء الجلسة ويتلقى UE عنوان IP، ولكن حركة المرور لا تتدفق عبر واجهة TUN.

الأسباب المحتملة:

- تم إضافة مسار مضيف لعنوان IP للمشترك على `omniepdg0` لم ��
- لم يتم تمكين إعادة توجيه IP على مضيف OmniEPDG
- قواعد الجدار الناري تحظر حركة المرور على واجهة `omniepdg0`
- قواعد NAT/تخفي مفقودة لحركة المرور الصادرة من نطاق IP للمشترك

الحل:

1. تحقق من وجود المسار المضيف (`ip route show` وابحث عن مسار /32 للمشترك عبر `omniepdg0`)
2. تأكد من تمكين إعادة توجيه IP (`sysctl net.ipv4.ip_forward`)
3. تحقق من قواعد iptables/nftables تسمح بإعادة التوجيه عبر `omniepdg0`
4. إذا كان المشتركون بحاجة إلى الوصول إلى الإنترنت، تحقق من تكوين NAT/تخفي لنطاق IP للمشترك (على سبيل المثال، `iptables -t nat -A POSTROUTING -s 10.45.0.0/16 -o <wan-interface> -j MASQUERADE`)

طرق قديمة بعد التعطل

الأعراض: تبقى طرق المضيف لعنوان IP للمشتركين في جدول التوجيه بعد إعادة تشغيل OmniEPDG أو بعد إنهاء الجلسات بشكل غير طبيعي.

الأسباب المحتملة:

- تعطل FSM قبل أن يتم إزالة المسار
- تم قتل عملية OmniEPDG دون إيقاف تشغيل سلس

الحل:

1. تحقق من `log/crash.log` للحصول على أعطال العمليات أثناء إنهاء الجلسة
2. قم بإزالة الطرق القديمة يدويًا (`ip route del <subscriber-ip>/32 dev omniepdg0`)
3. سيؤدي إعادة تشغيل OmniEPDG إلى إعادة إنشاء واجهة `omniepdg0`، مما يزيل جميع الطرق المرتبطة بها

مشكلات إنهاء الجلسة

يتعطل إنهاء الجلسة أثناء إلغاء التسجيل

الأعراض: لا يكتمل إنهاء الجلسة. عالق FSM UE في حالة `dereg_*` أو `wait_*`.

الأسباب المحتملة:

- لا يستجيب PGW لطلب حذف الجلسة
- لا يستجيب لـ STR أو ASR نظير Diameter
- عدم اكتمال تصعيد المهلة بسبب تراكم مهلات متعددة

الحل:

1. تحقق من السجلات للحصول على رسائل المهلة في الحالة ذات الصلة
2. تحقق من الاتصال بـ HSS و PGW
3. بعد 10 ثوانٍ، يجب أن تتجاوز FSM المهلة وتنتقل إلى الخطوة التالية لإنهاء الجلسة أو إنهاءها. إذا لم يحدث ذلك، تحقق من الأحداث غير المتوقعة ��لمسجلة كـ `Unexpected call event`

اليتيمة PDP GTP-U سياقات

الأعراض: تبقى إدخالات نفق GTP-U في النواة بعد إنهاء الجلسات. تظهر `ip link show gtp0` أن الجهاز لا يزال لديه سياقات PDP نشطة.

الأسباب المحتملة:

- تم إنهاء FSM بشكل غير طبيعي قبل حذف سياق PDP
- تعطل أثناء تسلسل الإنهاء

الحل:

1. تحقق من `log/crash.log` للحصول على أعطال العمليات أثناء إنهاء الجلسة
2. تحقق من أن FSM (على PDP. إذا تم قتل FSM يحاول رد الاتصال `terminate/3` لـ FSM تنظيف سياق فقد يتم تخطي التنظيف، (سبيل المثال، إعادة تشغيل المشرف
3. سيؤدي إعادة تشغيل OmniEPDG إلى إعادة إنشاء مقبس GTP-U ومسح السياقات القديمة

مشكلات العملية والنظام

حلقات إعادة تشغيل المشرف

الأعراض: تعيد عمليات OmniEPDG التشغيل بشكل متكرر. تظهر السجلات رسائل إعادة تشغيل المشرف وتقارير الأعطال.

الأسباب المحتملة:

- خطأ تكوين مستمر يتسبب في تعطل معالج عند بدء التشغيل
- الاعتماد الخارجي غير متاح (مكتبة، على سبيل المثال gen_socket غير موجودة)
- يرسل رسائل مشوهة تسبب أعطال المعالج Diameter نظير

الحل:

1. تحقق من `log/crash.log` لمعرفة السبب الجذري للتعطل
2. تحقق من أن مسار `libdir` لـ `gen_socket` صحيح وأن ملفات المكتبة موجودة
3. تحقق من وجود جميع معلمات التكوين المطلوبة في `config/runtime.exs`
4. ابحث عن رسائل Diameter المشوهة في تقرير التعطل

استخدام الذاكرة المرتفع

الأعراض: تزداد استهلاك الذاكرة في آلة Erlang الافتراضية بمرور الوقت.

الأسباب المحتملة:

- عدم تنظيف عمليات FSM UE بعد إنهاء الجلسة
- تراكم رسائل السجل في صناديق البريد

- عدد كبير من الجلسات المتزامنة

الحل:

1. تحقق من عدد عمليات `epdg_ue_fsm` و `aaa_ue_fsm` النشطة (يجب أن تتطابق هذه مع عدد المشتركين النشطين)
2. تحقق من رسائل السجل) تنتهي بشكل صحيح بعد إنهاء الجلسة FSMs تحقق من أن "terminating")
3. راجع إعدادات تدوير السجل لضمان تدوير ملفات السجل

OmniEPDG دليل تشغيل

OmniEPDG هو بوابة بيانات حزم متطورة (ePDG) تمكّن من إجراء مكالمات صوتية عبر WiFi (VoWiFi). يقوم بمصادقة المشتركين عبر الشبكات اللاسلكية غير الموثوقة باستخدام EAP-AKA، وأنفاق GTP إلى بوابة البيانات المحمولة عبر إشارات Diameter إلى HSS ويربطهم بشبكة النواة (PGW).

تعرض جلسة مشترك نشطة مع إحصائيات حركة المرور في OmniEPDG لوحة التحكم الخاصة بـ الوقت الحقيقي.

يدعم OmniEPDG وضعين تشغيليين:

- **وضع GTP** (افتراضي) - نفق كامل متوافق مع 3GPP عبر PGW عبر GTPv2-C و GTP-U
- **وضع VPN** **بسيط** - انقطاع محلي مع مجموعة IP مدمجة وواجهة Linux TUN، لا حاجة لـ PGW

الوثائق

التكوين والعمليات

- **العمارة وتدفقات المكالمات** - عمارة النظام، واجهات البروتوكول، آلات حالة UE، ومخططات تسلسل الرسائل لكلا الوضعين
- **مرجع التكوين** - وثائق كاملة للمعلمات لـ VPN و GTP-U و GTPv2-C و Diameter البسيط والتسجيل
- **لوحة التحكم** - واجهة مراقبة قائمة على الويب للجلسات، ونظراء Diameter، والسجلات

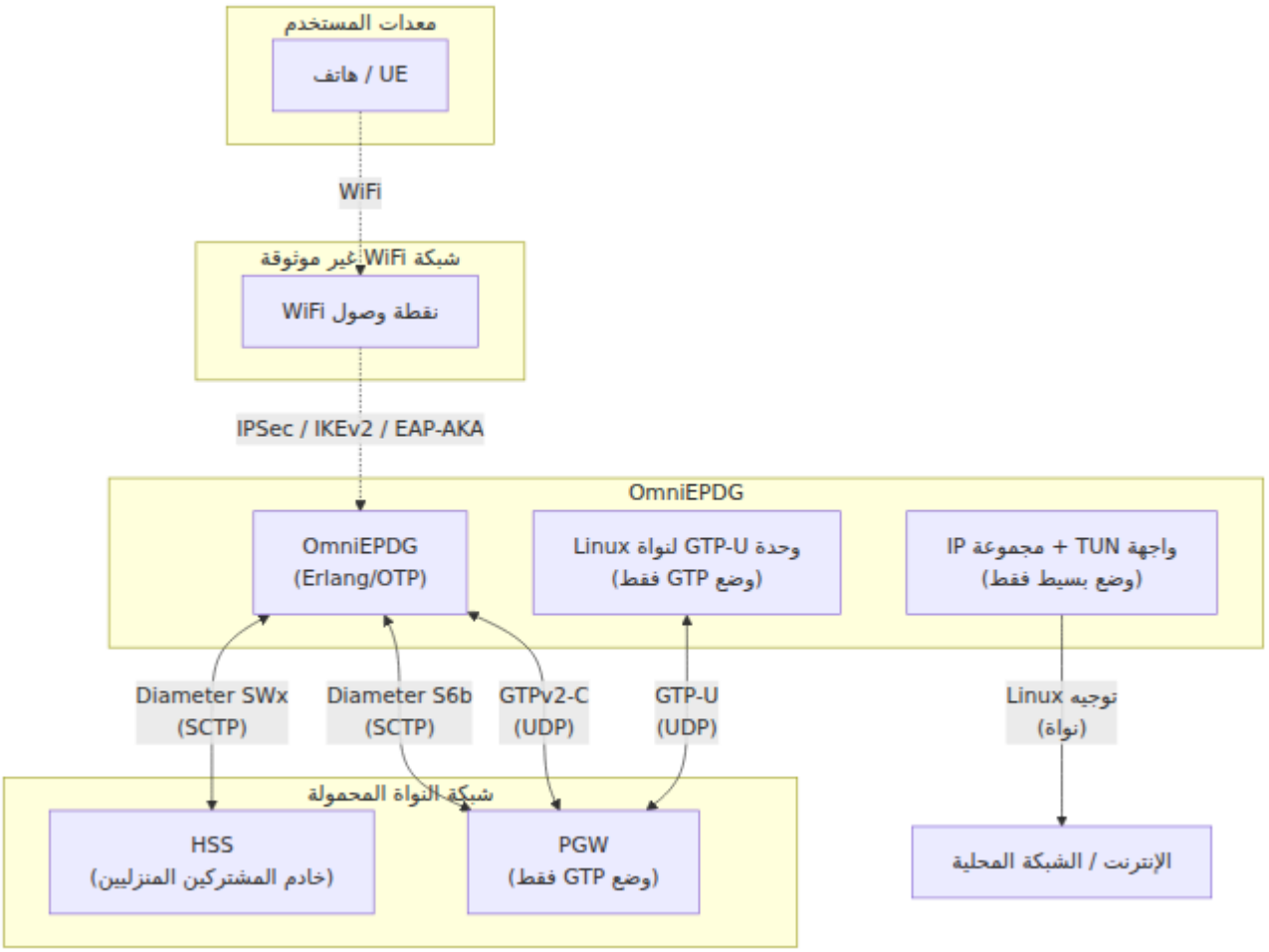
الأمان

- **دليل الأمان** - تحديد معدل المصادقة وحظر الدول باستخدام GeoIP

المراقبة واستكشاف الأخطاء وإصلاحها

- **مرجع المقاييس** - مقاييس Prometheus لمراقبة المصادقة، والجلسات، وإشارات Diameter، وصحة النظام
- **استكشاف الأخطاء** - مشكلات شائعة، وإجراءات تشخيصية، وخطوات الحل

الأوضاع التشغيلية



وضع GTP

الوضع الافتراضي. يقوم OmniEPDG بنفق جميع حركة مرور المشتركين عبر PGW باستخدام GTP-U (عبر وحدة نواة Linux) للتحكم في الجلسات و GTPv2-C لطبقة المستخدم. هذا متوافق تمامًا مع 3GPP ومناسب لنشر شركات الاتصالات مع بنية EPC الحالية.

مسار الحركة: UE → IPSec → OmniEPDG → GTPv2-C نفق → إنشاء جلسة GTP-U → PGW → الإنترنت

بنية التحتية المطلوبة: HSS، PGW

وضع VPN بسيط

يقوم OmniEPDG بتخصيص عناوين IP مباشرة من مجموعة محلية ويوجه حركة مرور المشتركين عبر واجهة Linux TUN (`tun_epdg`) باستخدام توجيه النواة القياسي. لا حاجة لـ PGW أو بنية

GTP. لا تزال المصادقة تحدث عبر Diameter SWx إلى HSS.

مسار الحركة: UE → IPSec → OmniEPDG → تخصيص IP واجهة → محلي TUN → توجيه Linux → الإنترنت

البنية التحتية المطلوبة: HSS فقط (لا حاجة لـ PGW)

تحسين اختياري: `skip_sar` يتجاوز طلب/إجابة تعيين الخادم HSS، مما يقلل من وقت علم المبدوءة HSS تخدم المشترك، وإجراءات ePDG لن تتعقب أي HSS إعداد الاتصال. وهذا يعني أن (إلغاء التسجيل، دفع الملف الشخصي) لن تعمل. مناسب للنشر الخاص دون متطلبات التجوال.

مقارنة الأوضاع

القدرة	وضع GTP	وضع VPN بسيط
متوافق مع 3GPP	نعم	جزئي، لا (مع `skip_sar`) (بدون)
PGW مطلوب	نعم	لا
HSS مطلوب	نعم	نعم (للمصادقة فقط)
تخصيص IP	من PGW	مجموعة محلية (CIDR)
طبقة المستخدم	وحدة GTP-U لنواة Linux	Linux TUN + توجيه
دفع الملف الشخصي HSS	نعم (PPR/PPA)	لا
إلغاء تسجيل HSS	نعم (RTR/RTA)	لا (مع `skip_sar`)
إنهاء مبدوء من PGW	نعم	غير متاح
دعم التجوال	نعم	لا
دعم مزدوج IPv6 /	نعم	فقط IPv4

واجهات البروتوكول

الواجهة	البروتوكول	النقل	الوضع	النظير	الغرض	المرجع
SWu	IKEv2 / IPSec	UDP	كلاهما	UE	نفق آمن ومصادقة EAP-AKA	3GPP TS 33.402
SWx	Diameter	SCTP	كلاهما	HSS	متجهات المصادقة وتعيين الخادم	3GPP TS 29.273 القسم 8
S6b	Diameter	SCTP	GTP فقط	PGW	تفويض الجلسة والسياسة	3GPP TS 29.273 القسم 9
S2b	GTPv2-C / GTP-U	UDP	GTP فقط	PGW	التحكم في النفق وطبقة المستخدم	3GPP TS 29.274

الميزات

الوظائف الأساسية

- **مصادقة EAP-AKA** - 3GPP مصادقة كاملة لمشتركي عبر HSS
- **إدارة نفق IPSec** - نفق آمن قائم على IKEv2 بين UE و ePDG
- **وضعين تشغيليين مزدوجين** - نفق GTP إلى PGW مع VPN بسيط أو انقطاع محلي
- **آلات حالة لكل UE** - FSM Erlang مستقلة لكل مشترك لإدارة دورة حياة الجلسة
- **دعم مزدوج للطبقات** - IPv4 و IPv6 وأنواع عناوين PDP IPv4v6 (وضع GTP)

ميزات وضع GTP

- **إنشاء نفق GTP** - إنشاء جلسة GTPv2-C وطبقة مستخدم GTP-U عبر وحدة نواة Linux

- **إنهاء مبدوء من PGW** - يرسل PGW طلب حذف الحامل، ePDG يقوم بإنهاء الجلسة إلى UE
- **إنهاء مبدوء من الشبكة** - يقوم HSS بتحفيز إلغاء التسجيل عبر SWx RTR، ePDG يقوم بإنهاء جميع الجلسات
- **إعادة المصادقة** - دفع الملف الشخصي المبدوء من HSS 3GPP وإعادة التفويض لكل القسم 7.1.2.5.1 TS 29.273

ميزات وضع VPN بسيط

- **محلية** - تخصي IPv4 قائم على CIDR مع تتبع لكل IMSI
- **مجموعة IP** - تخصي عنوان
- **توجيه واجهة TUN** - جهاز TUN قياسي لـ Linux (`tun_epdg`) مع طرق مضيف لكل UE
- **تكوين DNS** - خوادم DNS قابلة للتكوين مقدمة إلى UEs عبر PCO
- **تجاوز SAR** - تجاوز تسجيل HSS **اختياري** لإعداد اتصال أسرع

ميزات الأمان

- **تحديد معدل المصادقة** - حماية من هجمات القوة الغاشمة لكل IMSI و IP مع عتبات قابلة للتكوين
- **حظر الدول باستخدام GeoIP** - التحكم في الوصول القائم على الدول باستخدام MaxMind GeoLite2
- **كشف الأقران الميتة** - مراقبة حيوية نشطة مع استقصاءات قابلة للتكوين
- **حماية ضد إعادة التشغيل ESP** - نافذة انزلاق 64 بت متوافقة مع RFC 4303

تكامل HSS (SWx Diameter)

- **طلب/إجابة المصادقة متعددة الوسائط (MAR/MAA)** - استرجاع متجهات المصادقة EAP-AKA (كلا الوضعين)
- **طلب/إجابة تعيين الخادم (SAR/SAA)** - تنزيل ملف تعريف المشترك وتكوين APN (يمكن تخطيه في الوضع البسيط)
- **طلب/إجابة دفع الملف الشخصي (PPR/PPA)** - استلام ملفات تعريف المشتركين المحدثة من HSS (وضع GTP)
- **طلب/إجابة إنهاء التسجيل (RTR/RTA)** - إلغاء تسجيل المشترك المبدوء من HSS (وضع GTP)

تكامل PGW (وضع GTP فقط)

Diameter S6b:

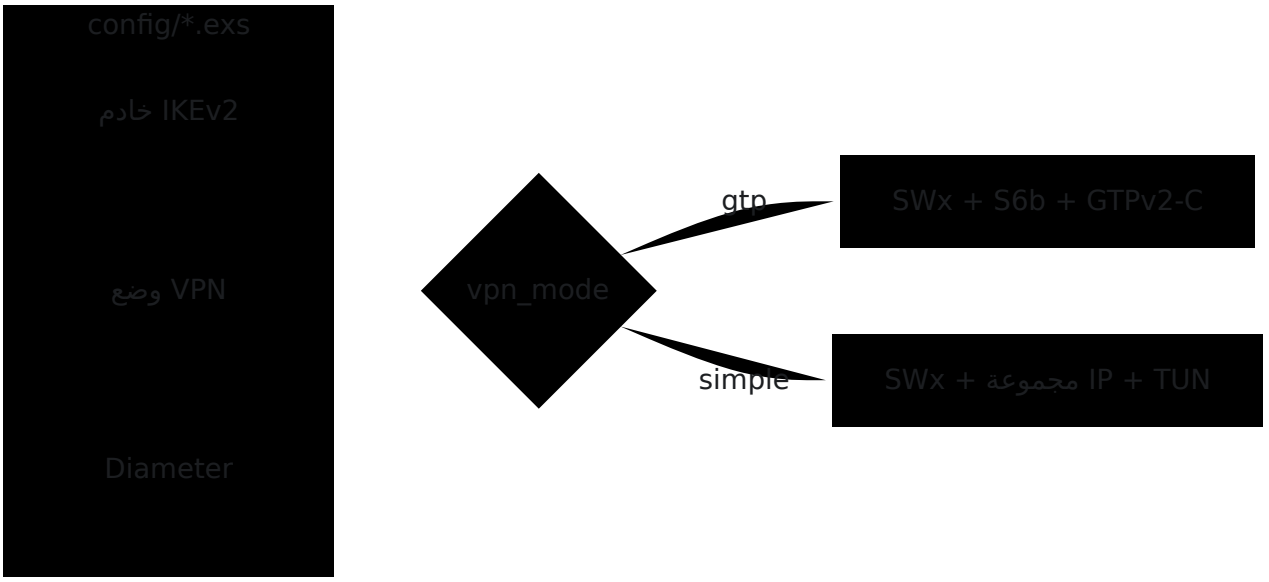
- **طلب/إجابة AA (AAR/AAA)** - تفويض جلسات PGW
- **طلب/إجابة إنهاء الجلسة (STR/STA)** - إنهاء جلسات PGW
- **طلب/إجابة إعادة التفويض (RAR/RAA)** - إعادة تفويض الجلسات النشطة
- **طلب/إجابة إنهاء الجلسة (ASR/ASA)** - إنهاء الجلسات بالقوة

GTPv2-C S2b:

- **طلب/استجابة إنشاء جلسة** GTP مع تخصيص TEID - إنشاء أنفاق
- **طلب/استجابة حذف الجلسة** GTP - إنهاء أنفاق
- **طلب/استجابة حذف الحامل** PGW - إدارة الحامل المبدوء من

البدء السريع

هيكل التكوين



يتم التكو��ن في `config/runtime.exs` أو عبر متغيرات البيئة. يحدد معلمة `vpn_mode` بين أوضاع GTP و VPN البسيط. انظر مرجع التكوين لوثائق المعلمات الكاملة.

العناوين الشبكية النموذجية (وضع GTP)

المكون	عنوان IP	المنفذ	الملاحظات
OmniEPDG (GTP-U)	10.74.0.11	-	نقطة نهاية نفق GTP-U
OmniEPDG (Diameter S6b)	10.74.0.12	3868	مستمع Diameter S6b
HSS	10.74.0.21	3868	نظير Diameter SWx
PGW	10.74.0.23	2123	نظير S6b و GTPv2-C

العناوين الشبكية النموذجية (وضع VPN بسيط)

المكون	عنوان IP	الملاحظات
OmniEPDG (بوابة TUN)	10.44.0.1	عنوان البوابة على واجهة `tun_epdg`
مجموعة IP لـ UE	10.45.0.0/16	مجموعة CIDR قابلة للتكوين لعناوين المشتركين
HSS	10.74.0.21:3868	نظير Diameter SWx (للمصادقة فقط)

مواصفات 3GPP

المواصفة	العنوان	الأهمية
TS 29.273	واجهات EPS AAA (SWx، S6b، SWm)	المواصفة الأساسية لواجهات Diameter ePDG
TS 29.274	GTPv2-C و GTP-U	التحكم في نفق S2b وطبقة المستخدم (وضع GTP)
TS 33.402	الأمان للوصول غير 3GPP	مصادقة EAP-AKA لشبكات WiFi غير الموثوقة
TS 23.402	تحسينات العمارة للوصول غير 3GPP	العمارة العامة ePDG والإجراءات
TS 23.003	الترقيم والعناوين والتعريف	تنسيق NAI، هيكل IMSI
TS 29.229	Diameter Cx/Dx (تعريفات شائعة)	قيم نوع تعيين الخادم المستخدمة من قبل SWx
RFC 6733	بروتوكول Diameter الأساسي	نقل Diameter، مراقبة، إدارة النظير
RFC 4187	EAP-AKA	طريقة المصادقة المستخدمة عبر IKEv2

الوثائق حسب الدور

مشغلو الشبكة:

1. ابدأ مع العمارة وتدفقات المكالمات لفهم النظام وكلا الوضعين التشغيليين
2. راجع مرجع التكوين لمعلمات النشر
3. راجع دليل الأمان لتكوين تحديد المعدل وحظر GeoIP
4. قم بإعداد المراقبة باستخدام Prometheus لتكامل مرجع المقاييس
5. احتفظ بدليل استكشاف الأخطاء متاحًا للعمليات

مُدمجو الأنظمة:

1. راجع العمارة وتدفقات المكالمات لتفاصيل الواجهة وآلات الحالة
2. استخدم مرجع التكوين لإعداد الاتصال بالنظراء
3. قم بتكوين التنبيهات باستخدام مرجع المقاييس
4. ارجع إلى جدول مواصفات 3GPP البروتوكولات أعلاه للتوافق