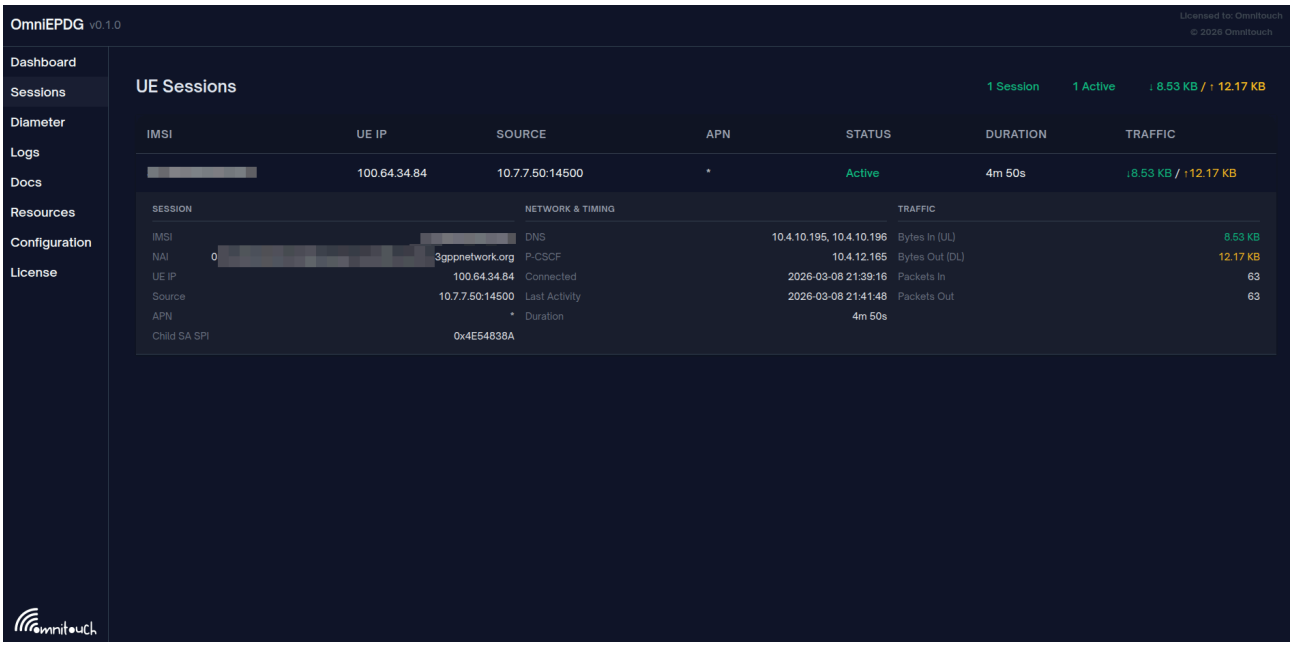
دليل عمليات OmniEPDG

OmniEPDG هو بوابة بيانات الحزمة المتطورة (ePDG) عبر WiFi التي تمكن مكالمات الصوت عبر WiFi غير الموثوقة باستخدام EAP-AKA، يقوم بمصادقة المشتركين المحمولين عبر شبكات (VoWiFi). وأنفاق GTP إلى HSS إلى Diameter ويربطهم بشبكة النواة المحمولة من خلال إشارات بوابة الحزمة (PGW).



تظهر جلسة مشترك نشطة مع إحصائيات حركة المرور في الوقت OmniEPDG لوحة التحكم في الحقيقي.

يدعم OmniEPDG وضعين تشغيليين:

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

يمكن أيضًا أن يعمل OmniEPDG كـ **N3IWF** 5G على نفس مستمع IKEv2. انظر وضع N3IWF.

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
- **وضع N3IWF** - 5 غير الموثوق غير الوصولIG 3 غيرGPP: EAP-5G عبر NWu، NGAP إلى AMF، و GTP-U إلى UPF

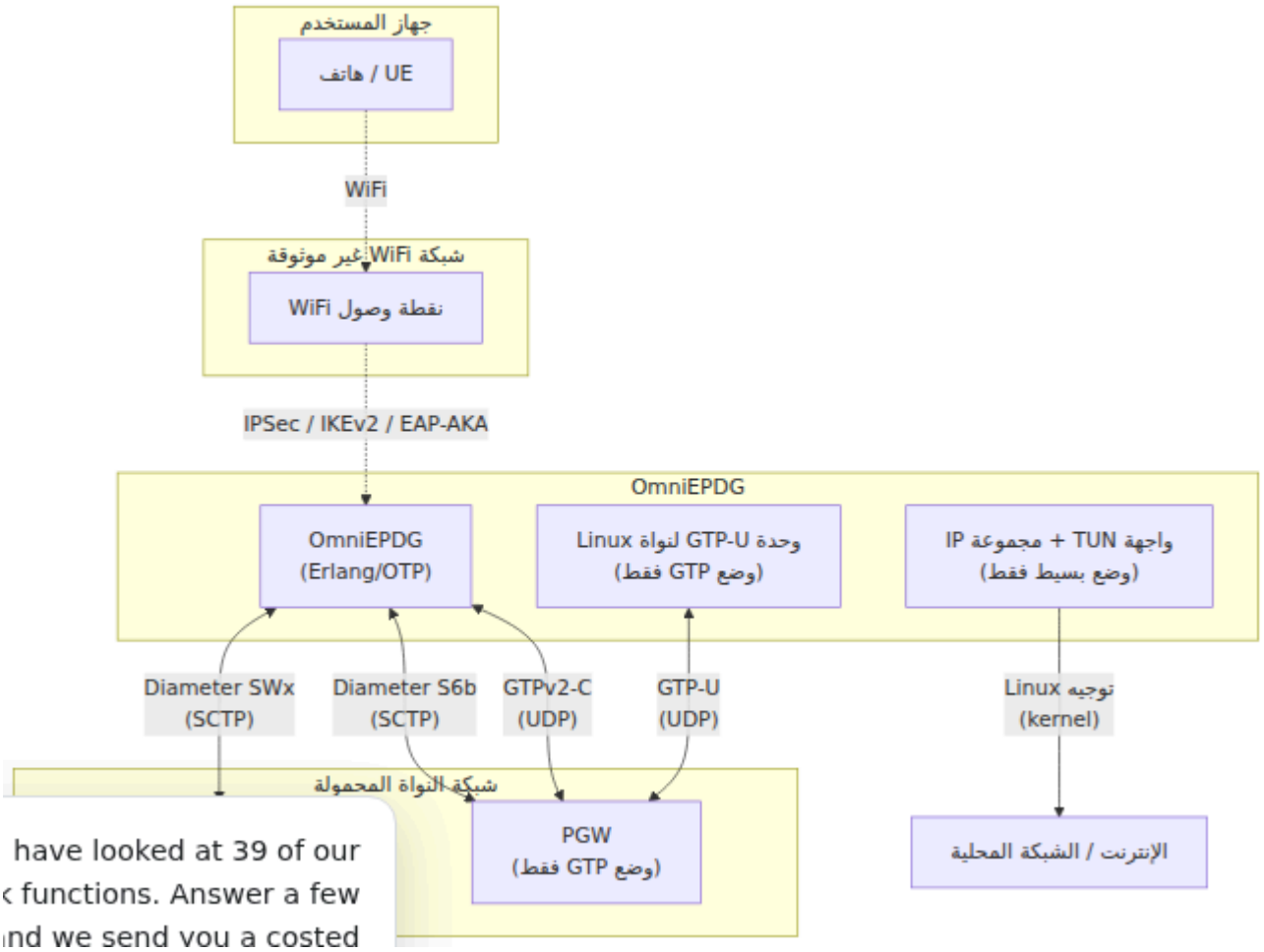
الأمان

- **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** - المشكلات الشائعة، وإجراءات التشخيص، وخطوات الحل

الأوضاع التشغيلية



وضع GTP

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

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

البنية التحتية المطلوبة: HSS، PGW

وضع VPN بسيط

يقوم OmniEPDG بتخصيص عناوين IP مباشرة من مجموعة محلية ويوجه حركة مرور المشتركين عبر واجهة TUN لنظام Linux (`tun_epdg`) لا حاجة لبنية نواة قياسي. باستخدام توجيه PGW أو

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: يقوم علم `skip_sar` بتجاوز HSS Server-Assignment-Request/Answer، مما يقلل من وقت إعداد الاتصال. هذا يعني أن ePDG لن تتعقب أي HSS مناسب. HSS يخدم المشترك، وإجراءات المبدوءة (إلغاء التسجيل، دفع الملف الشخصي) لن تعمل. للنشر الخاص بدون متطلبات تجوال.

مقارنة الأوضاع

القدرة	وضع GTP	وضع VPN بسيط
متوافق مع 3GPP	نعم	لا (مع `skip_sar`)، جزئي (بدون)
PGW مطلوب	نعم	لا
HSS مطلوب	نعم	نعم (للمصادقة فقط)
تخصيص IP	من PGW	مجموعة محلية (CIDR)
الطائرة المستخدمة	وحدة GTP-U لنواة Linux	توجيه Linux + TUN لنظام
دفع الملف الشخصي لـ HSS	نعم (PPR/PPA)	لا
إلغاء تسجيل HSS	نعم (RTR/RTA)	لا (مع `skip_sar`)
إنهاء بدء 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 ونفق الطائرة المستخدمة	3GPP TS 29.274

الميزات

الوظائف الأساسية

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

ميزات وضع GTP

- **إنشاء نفق GTP** - إنشاء جلسة GTPv2-C و GTP-U للطائرة المستخدمة عبر وحدة نواة Linux

- **إنهاء بدء PGW** - يرسل PGW طلب حذف الناقل، و ePDG يقوم بإنهاء الجلسة إلى UE
- **إنهاء بدء الشبكة** - يقوم HSS بتحفيز إلغاء التسجيل عبر SWx RTR، و 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 IP مجموعة** - تخصيص عنوان IPv4 يعتمد على CIDR مع تتبع لكل IMSI
- **توجيه واجهة TUN** - جهاز TUN قياسي لنظام Linux (`tun_epdg`) مع مسارات مضيف لكل UE
- **تكوين DNS** - خوادم DNS قابلة للتكوين مقدمة إلى UEs عبر PCO
- **تخطي SAR اختياري** - تجاوز تسجيل HSS لتسريع إعداد الاتصال

ميزات الأمان

- **تحديد معدل المصادقة** - حماية من هجمات القوة الغاشمة لكل IMSI و لكل IP مع عتبات قابلة للتكوين
- **حظر الدول باستخدام GeoIP** - التحكم في الوصول بناءً على الدول باستخدام MaxMind GeoLite2
- **كشف الأقران الميتة** - مراقبة نشاط نشط مع اختبارات قابلة للتكوين
- **حماية ضد إعادة تشغيل ESP** - نافذة منزلقة 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 المشترك وتكوين APN (يمكن تخطيه في الوضع البسيط)
- **طلب/إجابة دفع الملف الشخصي (PPR/PPA)** - استلام ملفات 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)

S6b Diameter:

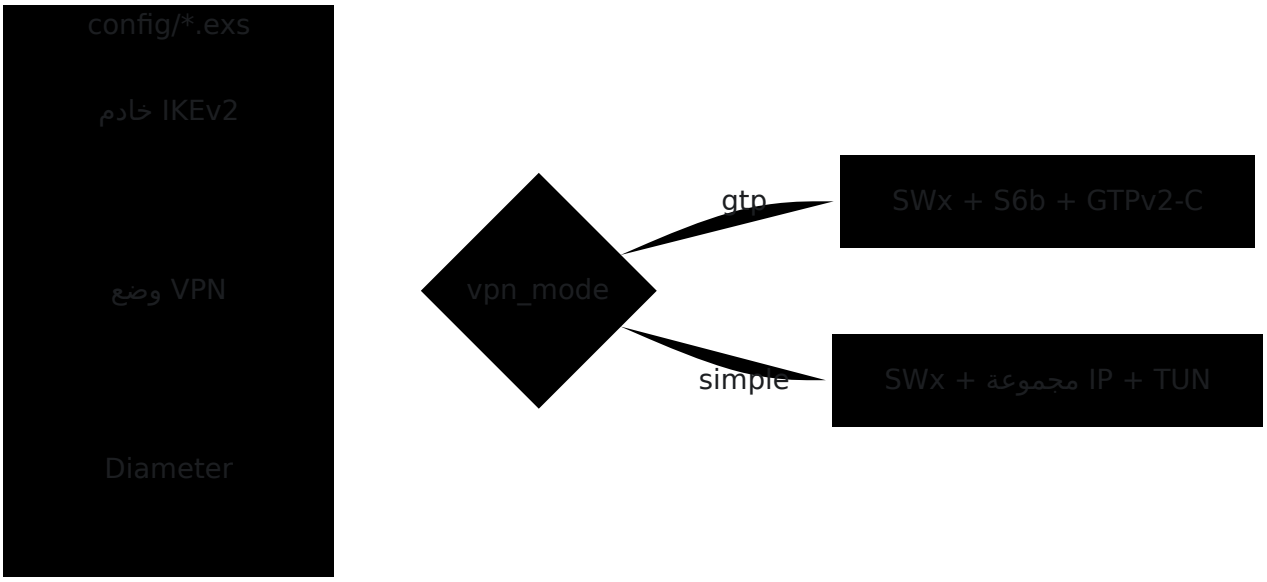
- **طلب/إجابة AA (AAR/AAA)** - تفويض جلسات PGW
- **طلب/إجابة إنهاء الجلسة (STR/STA)** - إنهاء جلسات PGW
- **طلب/إجابة إعادة التفويض (RAR/RAA)** - إعادة تفويض الجلسات النشطة
- **طلب/إجابة إنهاء الجلسة بالقوة (ASR/ASA)** - إنهاء الجلسات بالقوة

S2b GTPv2-C:

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

البدء السريع

هيكل التكوين



يتم التكوين 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 والطائرة المستخدمة (وضع GTP)
TS 33.402	الأمان للوصول غير 3GPP	مصادقة EAP-AKA لشبكة WiFi غير الموثوقة
TS 23.402	تحسينات العمارة للوصول غير 3GPP	العمارة والإجراءات العامة لـ ePDG
TS 23.003	الترقيم والعناوين والتعريف	تنسيق NAI، هيكل IMSI
TS 29.229	Cx/Dx Diameter (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 بـ العمارة وتدفقات المكالمات لفهم النظام وكلا الوضعين التشغيليين
2. راجع مرجع التكوين لمعلمات النشر
3. راجع GeoIP دليل الأمان لتكوين تحديد معدل المصادقة وحظر
4. قم بإعداد المراقبة باستخدام Prometheus مرجع المقاييس لتكامل
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 GPP للبروتوكول الامتثال لضمان أعلاه 3

دليل عمليات OmniEPDG

OmniEPDG هو بوابة بيانات حزمة مطورة (ePDG) 3GPP متوافقة مع مكالمات WiFi من خلال ربط الوصول غير الموثوق لشبكة WiFi بشبكة الجوال الأساسية. يدعم وضعين تشغيليين: **بسيط** لكسر IP المحلي و **وضع VPN** لنفق PGW **وضع GTP**.

روابط سريعة

التكوين والنشر

- **متطلبات الشبكة** - منافذ جدار الحماية ومدخلات DNS المطلوبة للنشر
- **مرجع التكوين** - وثائق كاملة للمعلمات لـ VPN وجميع أوضاع Diameter وIKEv2 إعدادات وقت التشغيل
- **نظرة عامة على الهندسة المعمارية** - هيكل النظام، تدفقات المكالمات، آلات الحالة، ومراجع البروتوكول

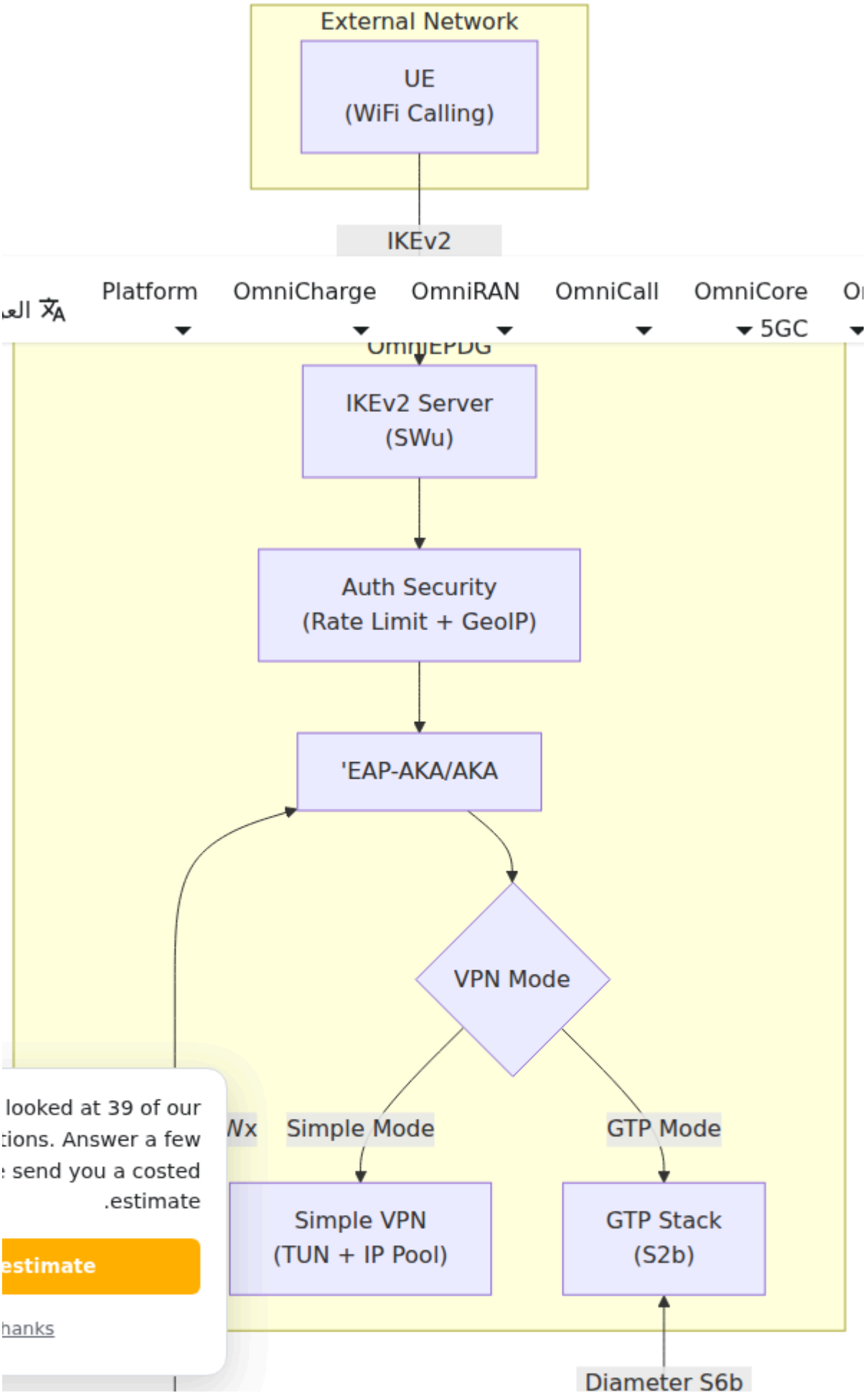
العمليات والمراقبة

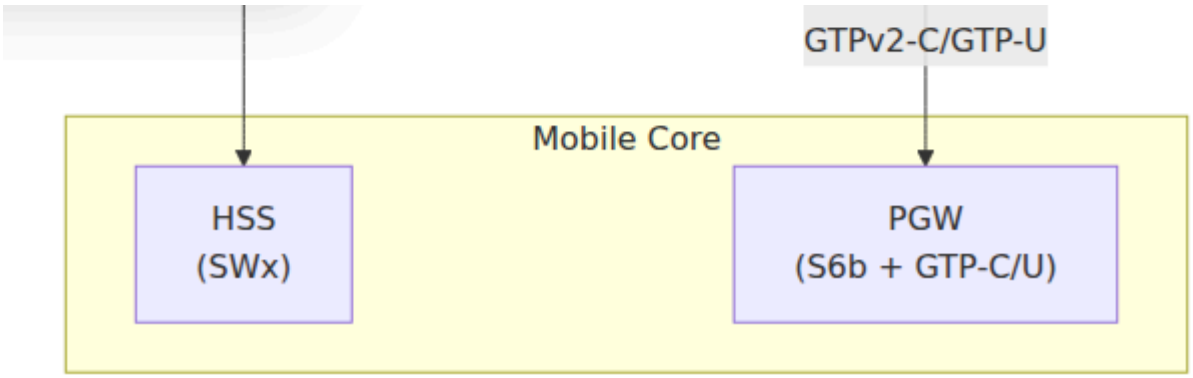
- **لوحة التحكم** - واجهة مراقبة قائمة على الويب للجلسات، أقران Diameter، والسجلات
- **مرجع المقاييس** - مقاييس Prometheus، استعلامات نموذجية، وقواعد التنبيه
- **Webhooks** - إشعارات دورة حياة الجلسة الصادرة عند الاتصال والفصل
- **استكشاف الأخطاء** - المشكلات الشائعة، إجراءات التشخيص، وخطوات الحل

الأمان

- **أمان المصادقة** - تحديد المعدل وحظر البلدان باستخدام GeoIP

نظرة عامة على الهندسة المعمارية


External Network
UE
(WiFi Calling)
IKEv2
Platform
OmniCharge
OmniRAN
OmniCall
OmniCore
5GC
IKEv2 Server
(SWu)
Auth Security
(Rate Limit + GeoIP)
'EAP-AKA/AKA
VPN Mode
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 من خلال PGW. نفق كامل متوافق مع 3GPP وتوجيهها عبر الشبكة الأساسية للجوال.

استخدم عندما:

- التكامل مع بنية الشبكة الأساسية للجوال الحالية
- السياسة والفوترة من خلال PCRF/PCEF
- مطلوب التجوال وتسليم بين المشغلين

المكونات:

- Diameter S6b لتفويض جلسة PGW
- GTPv2-C (إنشاء/حذف/تعديل الجلسة) لإدارة الجلسات
- وحدة GTP-U لنواة Linux لطائرة المستخدم

وضع VPN بسيط

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

استخدم عندما:

- نشر مستقل بدون PGW
- الاختبار والتطوير

- سيناريوهات كسر محلي

المكونات:

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

أمان المصادقة

يتضمن OmniEPDG ميزات أمان مدمجة لحماية ضد هجمات القوة الغاشمة وتقييد الوصول حسب الموقع الجغرافي. راجع دليل أمان المصادقة لمزيد من التفاصيل.

تحديد المعدل

يحمي من هجمات القوة الغاشمة من خلال تتبع محاولات المصادقة الفاشلة:

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

حظر البلدان باستخدام GeoIP

تحكم اختياري في الوصول الجغرافي باستخدام قاعدة بيانات MaxMind GeoLite2:

- **وضع القائمة البيضاء** - السماح فقط بالاتصالات من البلدان المحددة
- **وضع القائمة السوداء** - حظر الاتصالات من البلدان المحددة
- معالجة قابلة للتكوين لـ IPs غير المعروفة/الخاصة
- سلوك الفشل المفتوح أو الفشل 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 وثائق المعلمات الكاملة.

المراقبة

لوحة التحكم

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

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

راجع دليل لوحة التحكم لمزيد من التفاصيل.

مقاييس Prometheus

قم بجمع المقاييس 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 المقاييس للاستعلامات وقواعد التنبيه.

استكشاف الأخطاء

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 بسيط	تحقق من واجهة TUN والمسارات	مشكلات VPN بسيطة
مشكلات تحديد المعدل	ضبط العتبات	إيجابيات كاذبة في تحديد المعدل
مشكلات GeoIP	تحقق من قاعدة البيانات ورموز البلدان	مشكلات حظر GeoIP

راجع دليل استكشاف الأخطاء للحصول على إجراءات تشخيصية مفصلة.

فهرس الوثائق

الوثيقة	الوصف
الهندسة المعمارية	تصميم النظام، آلات الحالة، تدفقات المكالمات، مراجع البروتوكول
التكوين	مرجع تكوين كامل مع أمثلة
لوحة التحكم	دليل واجهة الويب مع لقطات شاشة
المقاييس	مقاييس Prometheus، وتنبيهات، استعلامات
متطلبات الشبكة	منافذ جدار الحماية ومدخلات DNS للنشر
الأمان	تحديد المعدل وحظر البلدان باستخدام GeoIP
استكشاف الأخطاء	المشكلات الشائعة وإجراءات التشخيص

بنية OmniEPDG وتدفقات المكالمات

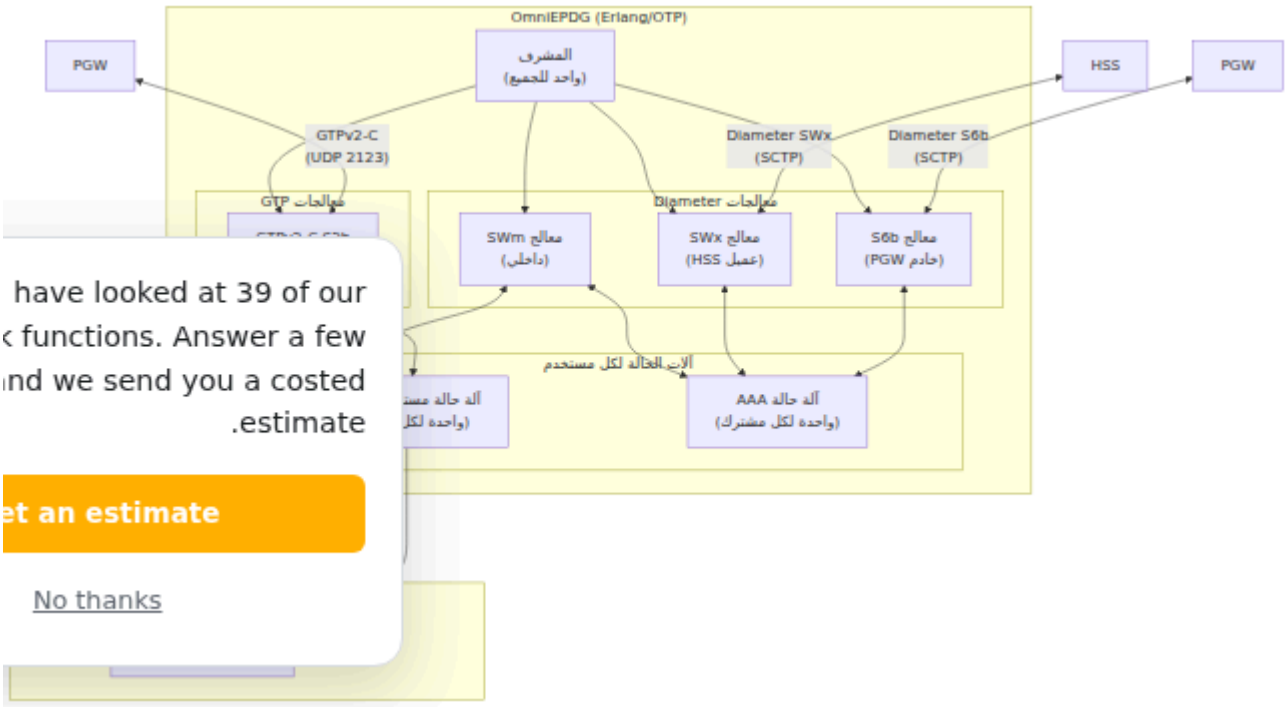
تصف هذه الوثيقة البنية الداخلية لـ OmniEPDG، وآلات الحالة وواجهات البروتوكول الخاصة به، ومخططات تسلسل الرسائل التفصيلية للإجراءات الرئيسية. يدعم OmniEPDG وضعين تشغيليين: **وضع GTP** (3 نفق كامل GPP عبر PGW) و**وضع VPN بسيط** (انفصال محلي مع واجهة TUN). لمقارنة عالية المستوى راجع دليل العمليات.

بنية النظام

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

بنية وضع GTP

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



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 لإجراء عمليات المصادقة وإدارة ملف المشترك
`aaa_diameter_swm`	Diameter SWm (داخلي)	يوجه رسائل EAP وsession Diameter بين ePDG وآلات حالة AAA
`epdg_diameter_swm`	معالج SWm ePDG	يتعامل مع إشارات ePDG من جانب Diameter الداخلية SWm

العمليات الإضافية 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 الجلسة إلى PGW عبر S2b
`gtp_u_kmod`	معالج Kernel GTP-U	يدير سياقات PDP GTP-U في وحدة نواة Linux

العمليات الإضافية 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 ويحرر عناوين IPv4 من مجموعة المكونة باستخدام CIDR ETS
`simple_vpn_route`	مدير المسار	ينشئ واجهة TUN `omniepdg0` ويدير مسارات المضيف لكل مشترك

آلات الحالة لكل مستخدم

لكل مشترك نشط (يتم التعرف عليه بواسطة IMSI)، ينشئ OmniEPDG حالتين لآلة الحالة:

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

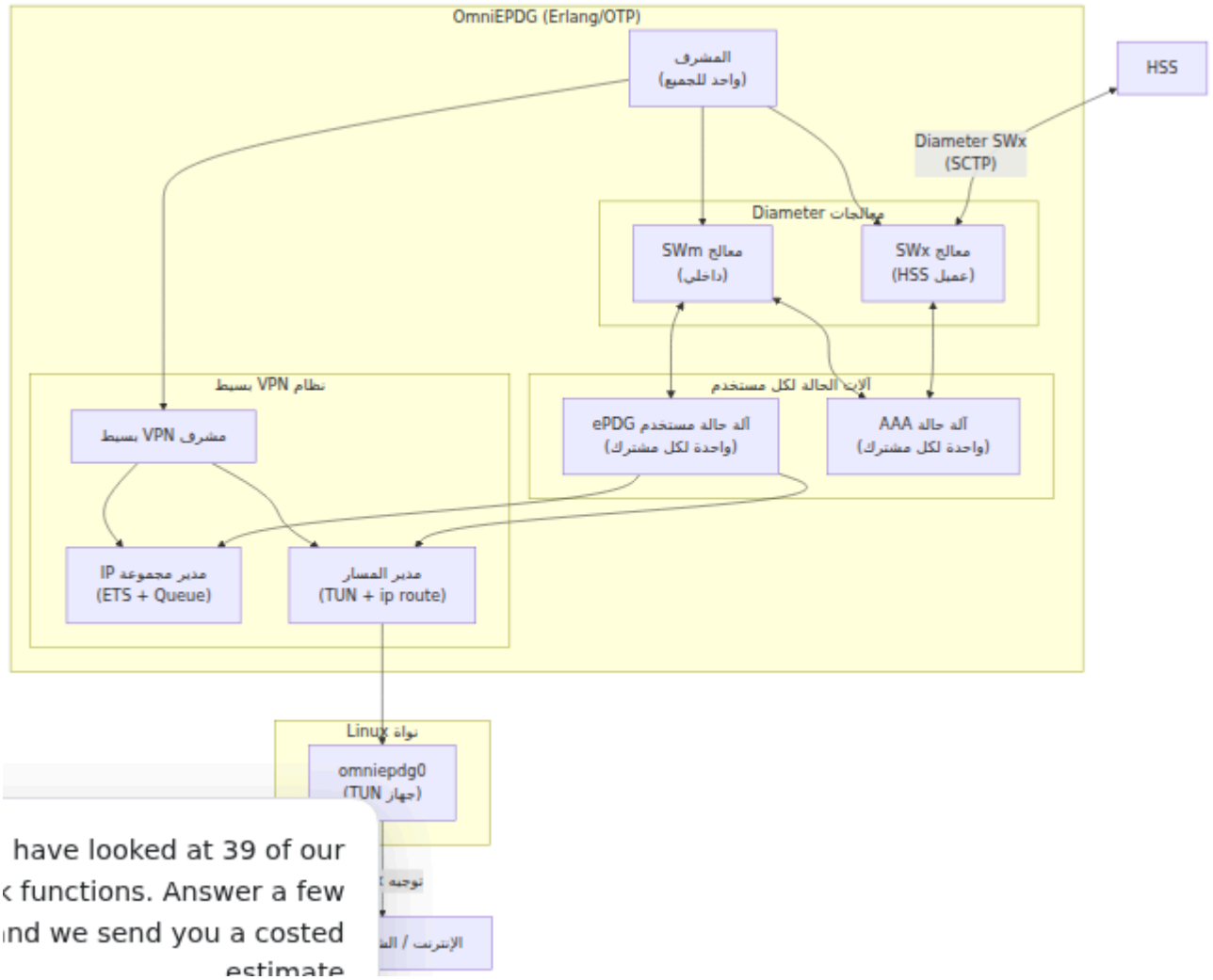
كلا الآلتين يتم تنفيذهما كعمليات Erlang `gen_statem` مع وضع رد نداء وظيفة الحالة.

حالات آلة حالة مستخدم ePDG

تتبع آلة حالة مستخدم ePDG جلسة المشترك من طلب المصادقة الأولي إلى حالة النفق النشط `authenticated` بناءً على الوضع التشغيلي. يتباين سلوك الآلة عند حالة حتى الإنهاء.

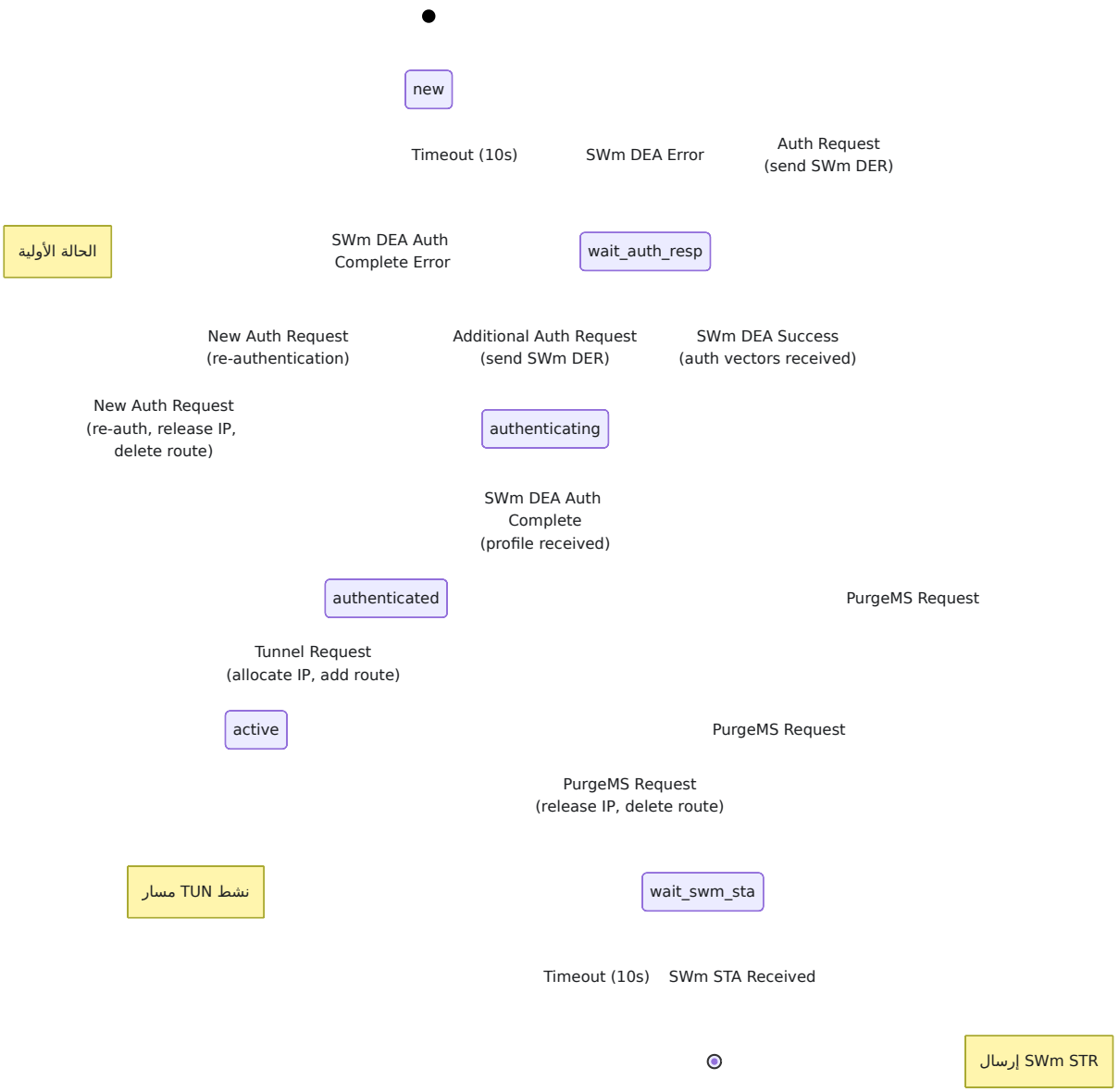
آلة حالة GTP

في وضع GTP، يتم إنشاء النفق عبر GTPv2-C Create Session إلى PGW، ويتضمن الإنهاء deregistration التي وتدفقات PGW، وحذف الناقل الذي يبدأه GTPv2-C Delete Session، يبدأها HSS.



آلة حالة VPN بسيطة

في وضع VPN بسيط، تأخذ الآلة اختصارًا عند الحالة `authenticated`. بدلاً من إرسال طلب GTPv2-C Create Session، تقوم الآلة بتخصيص عنوان IP وإنشاء مسار من المجموعة المحلية، والانتقال مباشرة إلى `active`. لا تُستخدم حالات الإنهاء الخاصة بـ GTP مضيف على واجهة TUN، (`wait_create_session_resp`، `wait_delete_session_resp`، `dereg_pgw_wait_cancel`، `dereg_net_wait_s2b_delete`).


new
Timeout (10s)
SWm DEA Error
Auth Request
(send SWm DER)
الحالة الأولية
SWm DEA Auth
Complete Error
wait_auth_resp
New Auth Request
(re-authentication)
Additional Auth Request
(send SWm DER)
SWm DEA Success
(auth vectors received)
New Auth Request
(re-auth, release IP,
delete route)
authenticating
SWm DEA Auth
Complete
(profile received)
authenticated
PurgeMS Request
Tunnel Request
(allocate IP, add route)
active
PurgeMS Request
PurgeMS Request
(release IP, delete route)
مسار TUN نشط
wait_swm_sta
Timeout (10s)
SWm STA Received
إرسال SWm STR

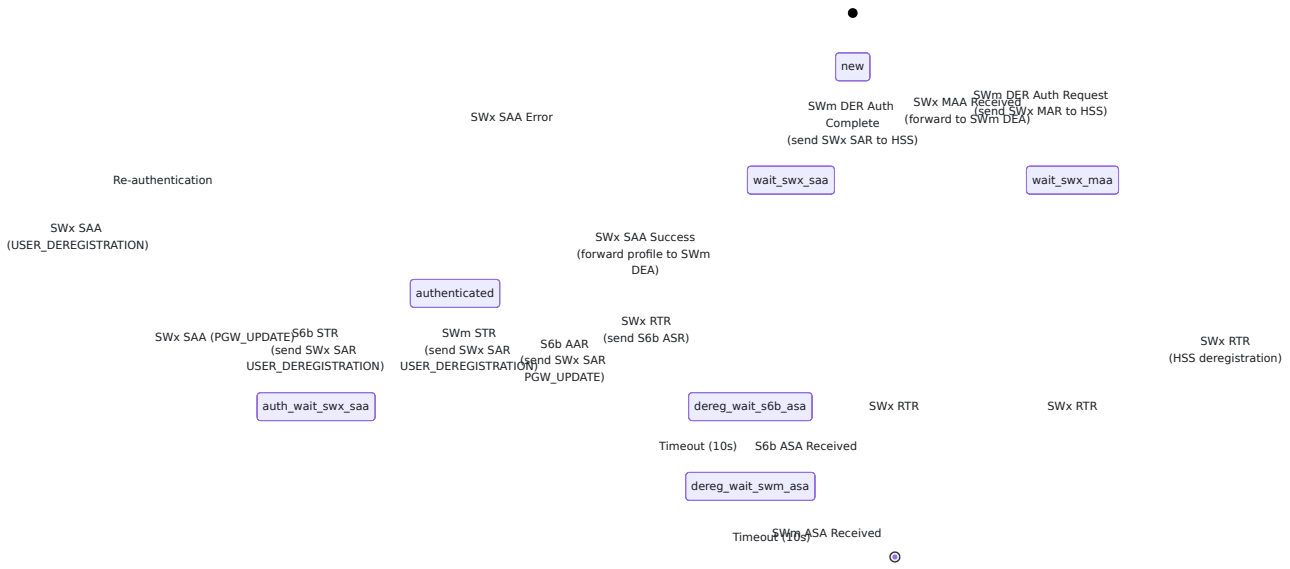
مرجع حالات آلة حالة مستخدم ePDG

الحالة	الوضع	الوصف	الانتظار لـ
`new`	كلاهما	الحالة الأولية. لا توجد جلسة نشطة.	طلب مصادقة 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 / إكمال المصادقة
`authenticated`	كلاهما	اكتملت المصادقة، تم تنزيل ملف المشترك.	طلب نفق من UE
`wait_create_session_resp`	GTP	تم إرسال طلب GTPv2-C Create Session إلى PGW.	استجابة Create Session 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 بدأه UE).	استجابة Delete Session من PGW
`wait_swm_sta`	كلاهما	تم إرسال طلب إنهاء جلسة SWm.	SWm STA من AAA

الحالة	الوضع	الوصف	الانتظار لـ
`dereg_pgw_wait_cancel`	GTP	deregistration بدأه PGW. تم إرسال Cancel Location إلى UE.	نتيجة Cancel Location
`dereg_net_wait_cancel`	GTP	deregistration بدأه الشبكة/HSS. ت إرسال Cancel Location إلى UE.	نتيجة Cancel Location
`dereg_net_wait_s2b_delete`	GTP	deregistration بدأه الشبكة. تم إرسال S2b Delete Session إلى PGW.	استجابة Delete Session

حالات آلة حالة AAA UE

تدير آلة حالة AAA UE الإشارات Diameter نحو HSS (SWx) وPGW (S6b) نيابة عن كل مشترك.



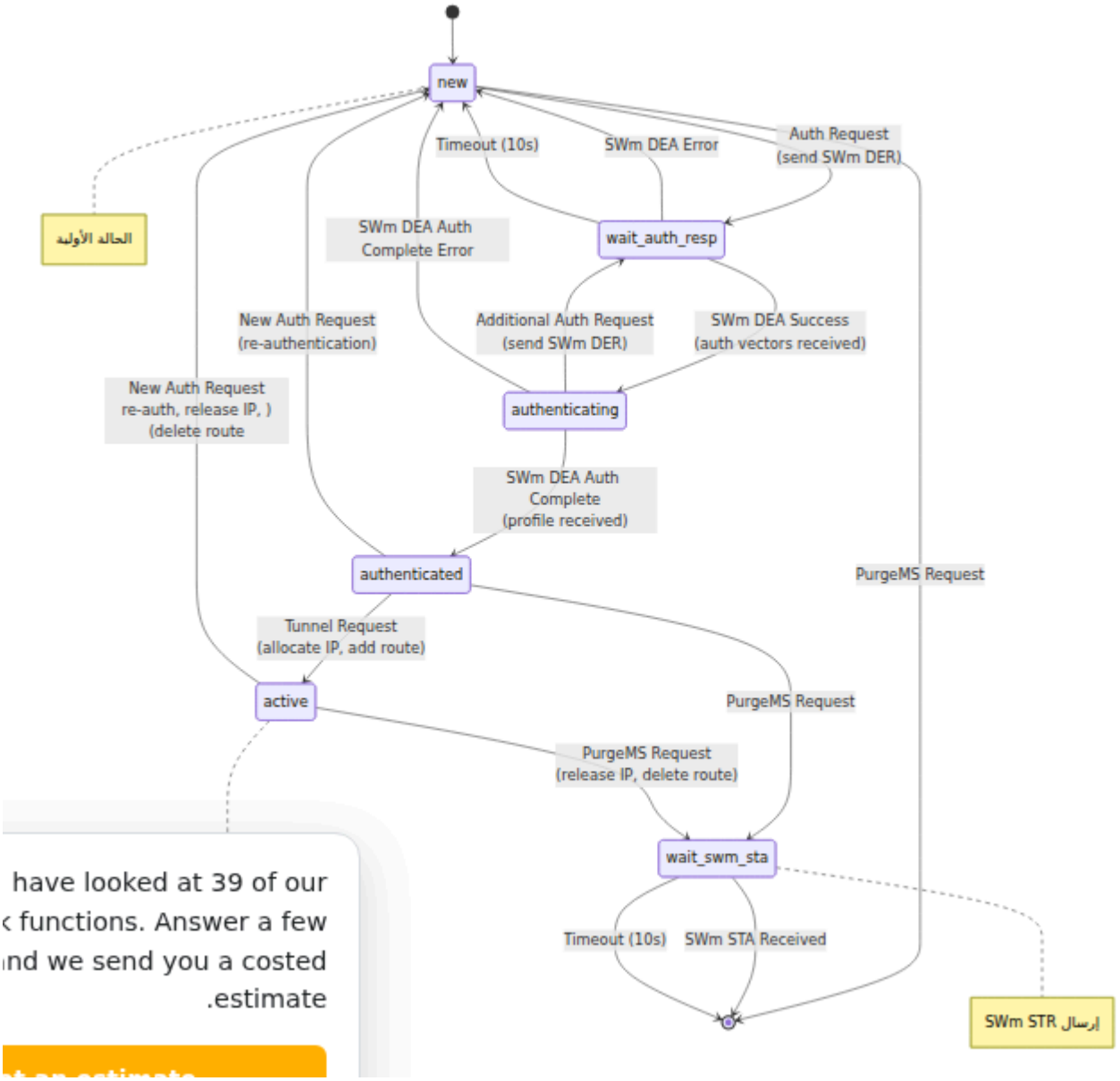
مرجع حالات آلة حالة AAA UE

الحالة	الوصف	الانتظار لـ
`new`	الحالة الأولية لـ AAA. لا توجد جلسة نشطة.	طلب مصادقة 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`	قد تكون جلسات ePDG وPGW نشطة. تتبع حالة الجلسة المزدوجة.	أحداث الجلسة
`auth_wait_swx_saa`	تم إرسال SWx SAR لتحديث PGW المستخدم أو deregistration.	SWx SAA من HSS
`dereg_net_wait_s6b_asa`	تم بدأه HSS. deregistration 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

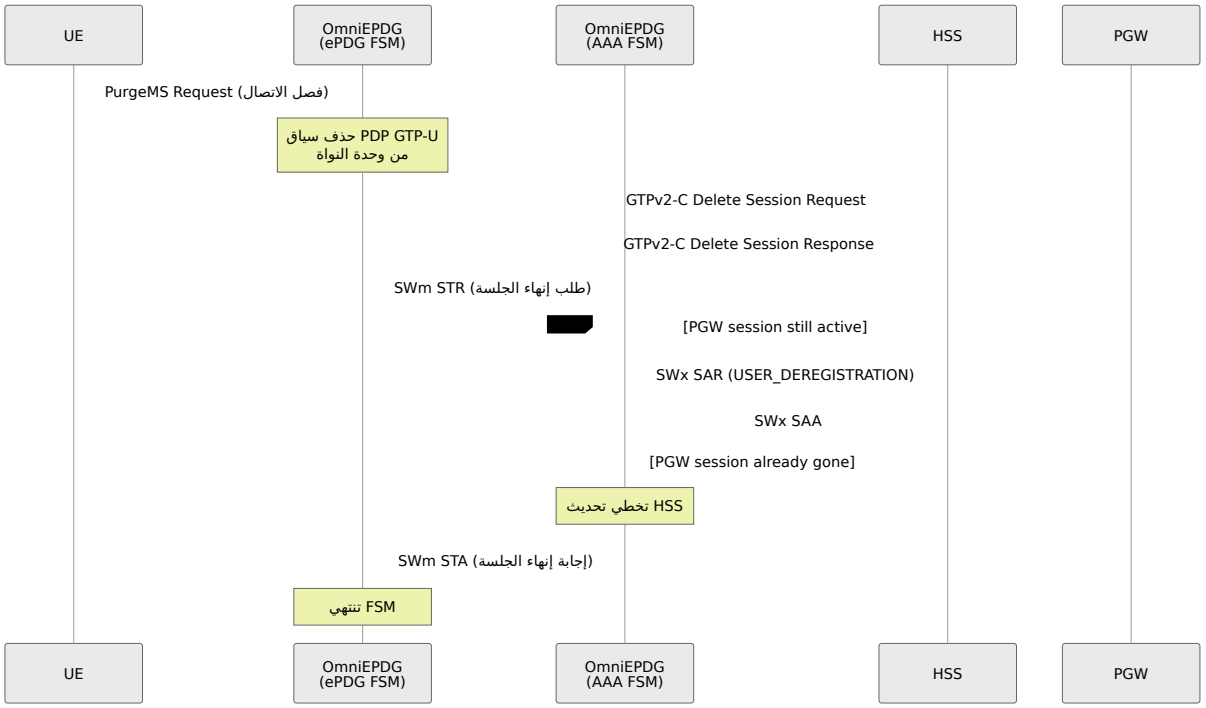
إنشاء جلسة ناجحة: GTP وضع

تظهر هذه ال��لسلة جلسة ناجحة كاملة من مصادقة EAP-AKA حتى نفق GTP نشط.



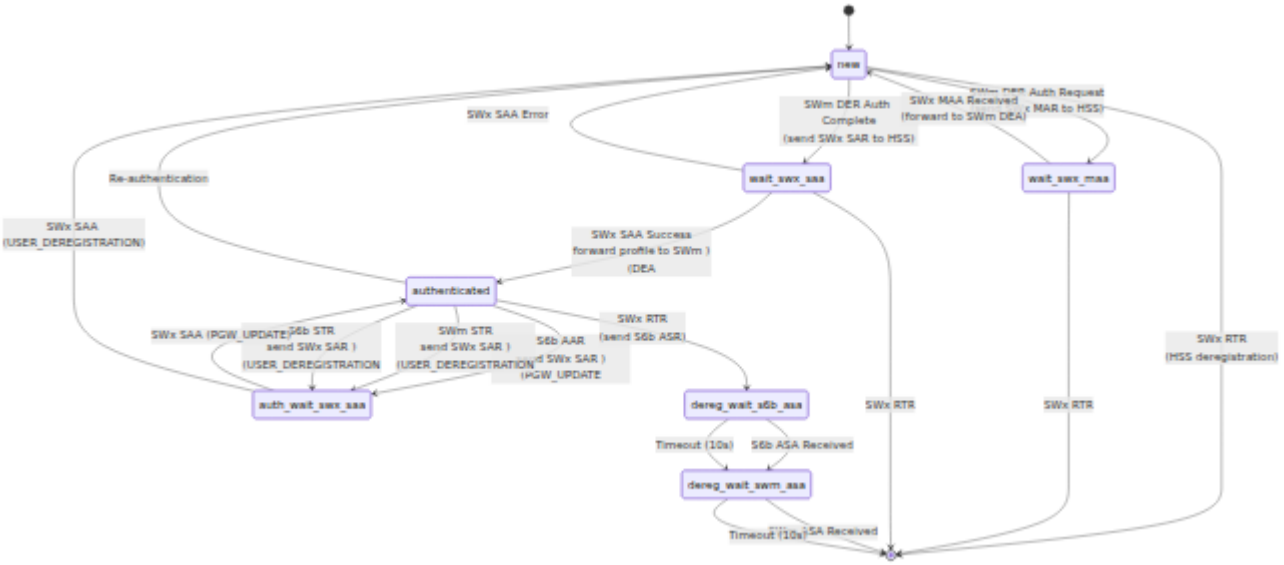
وضع GTP: إنهاء الجلسة التي بدأها UE

إلى الخلوية أو يقوم WiFi على سبيل المثال، الانتقال من) بفصل الاتصال UE عندما يقوم المستخدم بإنهاء المكالمة).



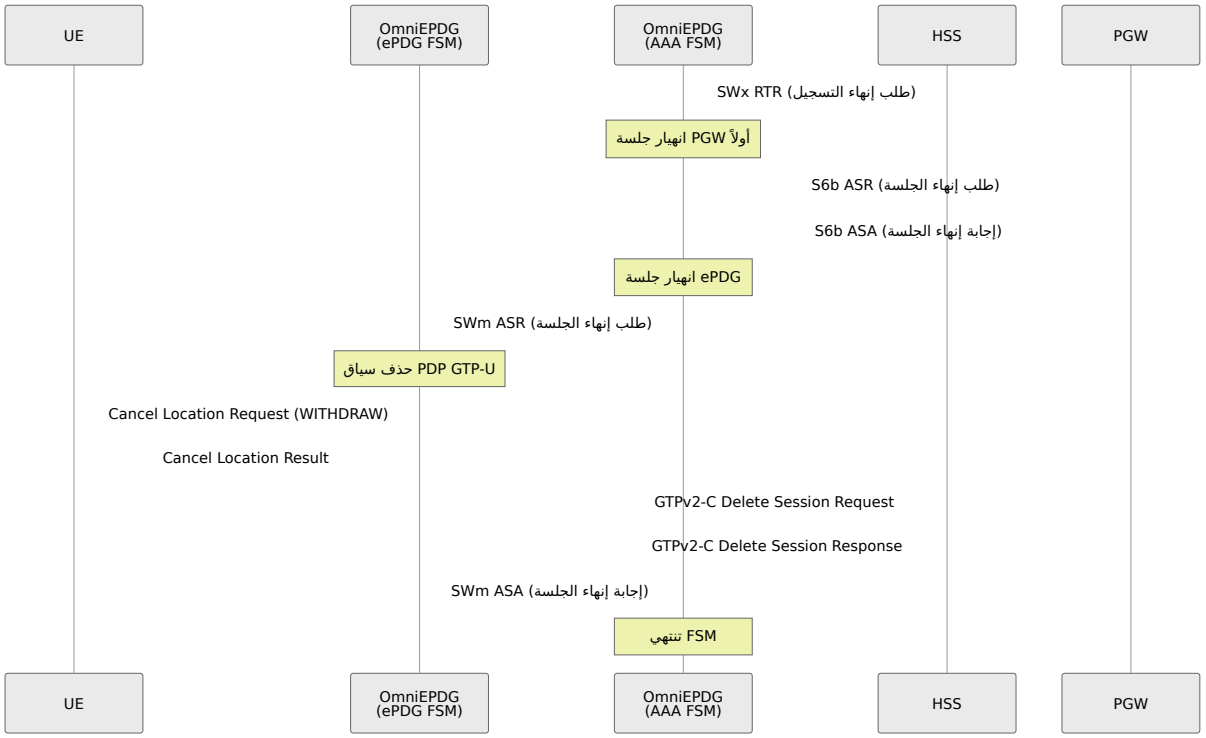
وضع GTP: إنهاء الجلسة التي بدأها PGW

عندما ينهي PGW (على سبيل المثال، انتهاك السياسة، انتهاء الوقت، أو إجراء إداري) الجلسة.



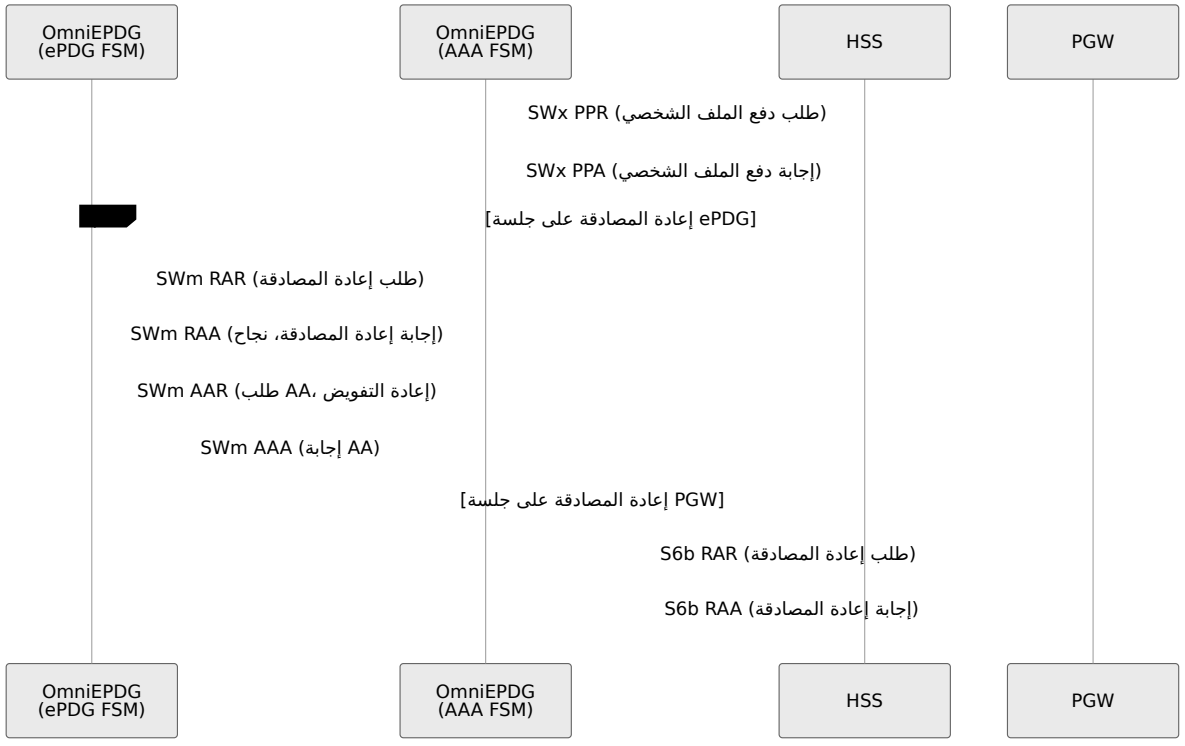
وضع GTP: deregistration التي بدأت بها الشبكة (HSS)

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



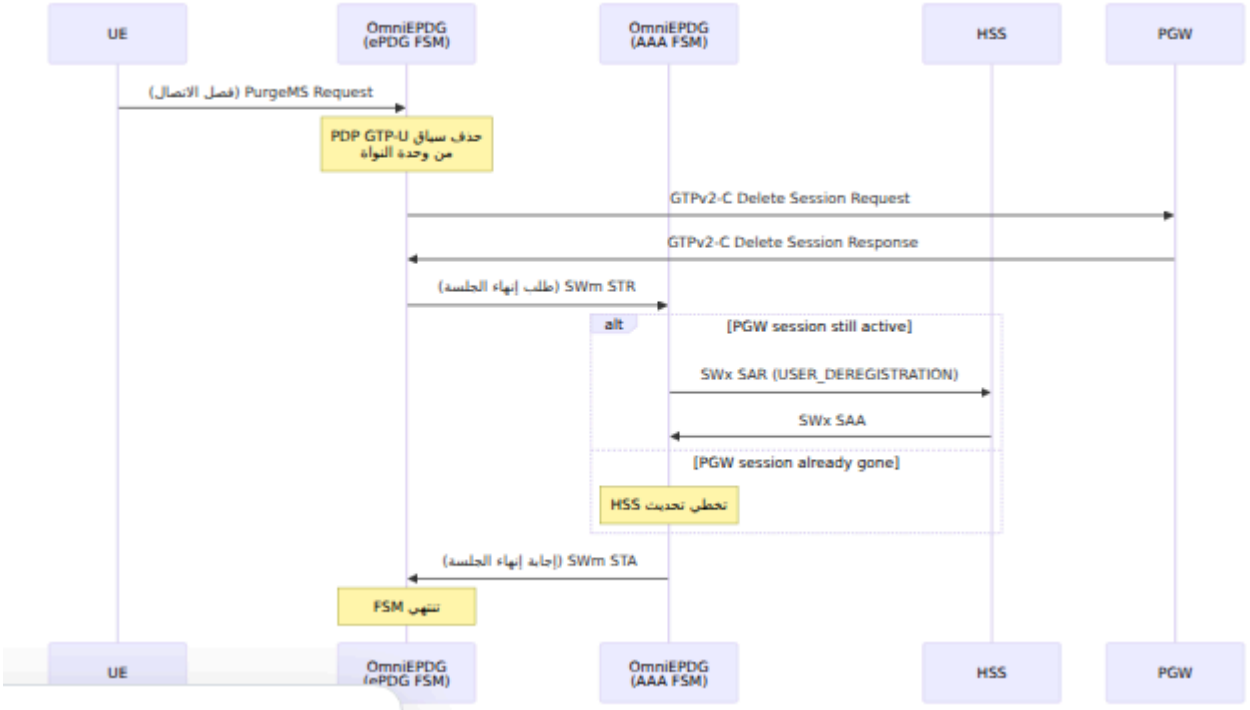
وإعادة المصادقة HSS دفع ملف تعريف :GTP وضع

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



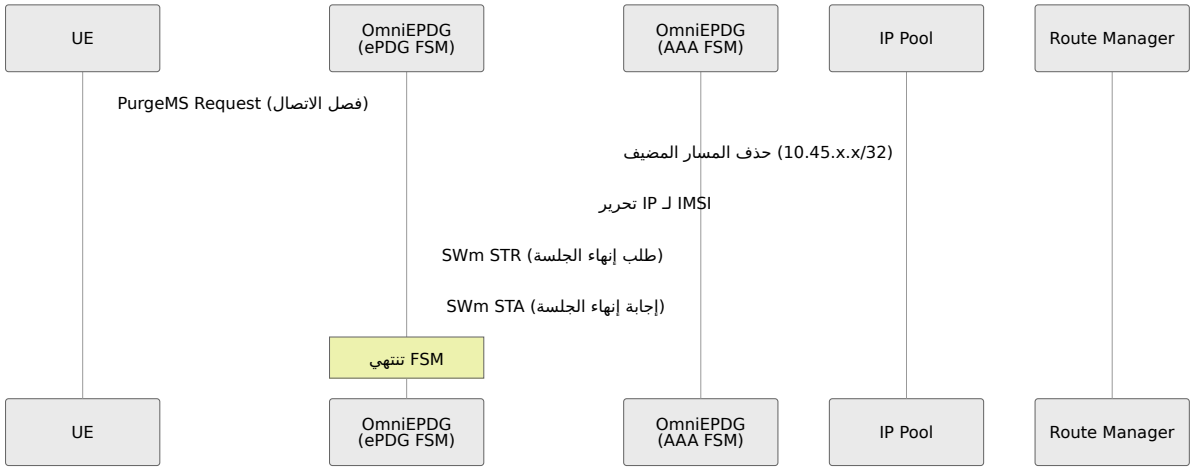
بسيط: إنشاء جلسة ناجحة VPN وضع

في وضع VPN بسيط، يكون إنشاء الجلسة أقصر. بعد مصادقة EAP-AKA، تقوم آلة حالة ePDG بتخصيص IP متجاوزة كل تفاعل مع TUN، من المجموعة المحلية وإعداد مسار مضيف على واجهة PGW. إذا تم تمكين `skip_sar`، يتم أيضًا تخطي تبادل SAR/SAA مع HSS.



بسيط: إنهاء الجلسة التي بدأها UE وضع VPN

عندما يقوم UE بفصل الاتصال في وضع VPN، تقوم الآلة بتحرير عنوان IP المخصص وإزالة المسار المضيف.



معرفات تطبيق Diameter

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

رموز نتائج Diameter

يتم ربط رموز نتائج Diameter لـ اب الداخلية إلى قيم الأس��لنقل الأخطاء عبر OmniEPDG البروتوكولات.

رموز النتائج القياسية

رمز النتيجة	الاسم	المعنى
2001	DIAMETER_SUCCESS	تمت العملية بنجاح
2002	DIAMETER_LIMITED_SUCCESS	تمت العملية جزئيًا بنجاح

3GPP رموز النتائج التجريبية

رمز النتيجة	الاسم	المعنى	رجع
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	لا HSS يمكنه توفير بيانات المصادقة مؤقتًا	3GP TS 29.
5001	DIAMETER_ERROR_USER_UNKNOWN	لم يتم العثور على IMSI المشترك في HSS	3GP TS 29.
5002	DIAMETER_UNKNOWN_SESSION_ID	لم يتم العثور على الجلسة (يستخدم لطلب STR/AAR القديم)	RFC 673
5003	DIAMETER_AUTHORIZATION_REJECTED	المشترك غير مخول للخدمة	3GP TS 29.
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	تنطبق قيود التجوال	3GP TS 29.
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 سبب GTPv2-C (وضع GTP فقط)

يتعامل OmniEPDG مع رموز سبب 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.راجع 3GPP TS 29.274 Section 8.4.

أسباب النجاح

الرمز	الاسم	الوصف
16	Request Accepted	تمت العملية بنجاح
17	Request Accepted Partially	نجاح جز��ي
18	New PDN Type (Network Preference)	تغير نوع PDN بسبب تفضيل الشبكة
19	New PDN Type (Single Address Bearer)	تغير نوع PDN بسبب قيود الناقل ذو العنوان الواحد

أسباب الخطأ (محدد)

الرمز	الاسم	الوصف
64	Context Not Found	لم يتم العثور على سياق الجلسة على PGW
73	No Resources Available	استنفاد موارد PGW
78	Missing or Unknown APN	APN المطلوب غير مكون على PGW
82	Denied in RAT	تقنية الوصول غير مسموح بها
84	All Dynamic Addresses Occupied	استنفاد مجموعة عناوين IP على PGW
92	User Authentication Failed	فشل المصادقة في PGW
93	APN Access Denied	APN المشترك غير مخول لـ
96	IMSI/IMEI Not Known	لم يتم التعرف على هوية المشترك
109	Invalid Peer	فشل التحقق من النظير
113	APN Congestion	APN مزدحم
120	GTP-C Entity Congestion	تحميل زائد في مستوى التحكم PGW

تنسيق NAI

يتعرف OmniEPDG على المشتركين باستخدام تنسيق معرف الوصول الشبكي (NAI) المحدد في 3GPP TS 23.003 Section 19:

```
<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 المحسنة مع ربط الشبكة

يختار OmniEPDG تلقائيًا طريقة المصادقة بناءً على بادئة هوية UE. يستخدم 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 لكل مشترك.

الخوارزميات التشفيرية

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

خوارزميات تشفير 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
AES-XCBC-96	5	128 بت	96 بت	مدعوم	RFC 3566
HMAC-SHA1-96	2	160 بت	96 بت	مدعوم (قديم)	RFC 2404
HMAC-MD5-96	1	128 بت	96 بت	مدعوم (قديم)	RFC 2403

مطلوب من بعض الهواتف، وخاصة بعض عملاء (`AUTH_AES_XCBC_96`) AES-XCBC-96 الذين يقدمونه كتحويل سلامة الوحيد لديهم. يتم تنفيذه وفقًا لـ RFC 3566، Samsung VoWiFi المحدد في RFC 4434 وRFC 7296 مع معالجة المفتاح المتغير وتقليص nonce SKEYSEED Section 2.14.

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-AES128-XCBC	4	128 بت	مدعوم	RFC 4434
PRF-HMAC-SHA1	2	160 بت	مدعوم (قديم)	RFC 2104
PRF-HMAC-MD5	1	128 بت	مدعوم (قديم)	RFC 2104

عند التفاوض على `PRF-AES128-XCBC`، يتم اشتقاق SKEYSEED من أول 64 بت فقط من كل prf+. بينما تغذي النونسات الكاملة توسيع مفتاح، (RFC 7296 Section 2.14 وفقًا لـ) Nr و Ni من

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 (Child SA)

تتم المفاوضات على خوارزميات نفق ESP من اقتراح SA الذي يقدمه UE في IKE_AUTH (وفي CREATE_CHILD_SA عند إعادة التشفير). يختار OmniEPDG تحويلًا قدمه UE بالفعل ويشتق مفاتيح Child SA و أحجام المفاتيح وICV ثابتة. لا يفرض مجموعة المطابقة.

النوع	الخوارزميات	الملاحظات
التشفير	AES-CBC-128 / 192 / 256	يتبع الشيفرة طول المفتاح المتفاوض عليه
السلامة	HMAC-SHA2-256-128، HMAC-SHA2-384-192، HMAC-SHA2-512-256، AES-XCBC-96، HMAC-SHA1-96	هو 12 ICV لـ AES-XCBC-96 بايت (مقابل 16 لـ HMAC-SHA2-256-128)

الاحتياطي (اقتراح فقط عندما لا يمكن تحليل UE):

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

وظائف EAP-AKA التشفيرية

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

وظائف EAP-AKA' التشفيرية

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

الامتثال لـ 3GPP

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

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

بجانب المجموعة الإلزامية، يدعم OmniEPDG أيضًا تحويلات سلامة AES-XCBC وPRF (RFC 3566 / RFC 4434) للتوافق مع الهواتف التي تقدمها حصريًا: على سبيل المثال، بعض عملاء Samsung VoWiFi، الذين يقترحون AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048 ولن يتراجعوا إلى HMAC-SHA2.

أنواع عنوان PDP (وضع GTP فقط)

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

النوع	الوصف	تنسيق PAA GTPv2-C
IPv4	ناقل IPv4 فقط	مكون من 4 بايت IPv4 عنوان
IPv6	ناقل IPv6 فقط	مكون من 16 IPv6 طول بادئة مكون من بايت واحد + عنوان بايت
IPv4v6	ناقل مزدوج	مكون من 16 IPv6 طول بادئة مكون من بايت واحد + عنوان مكون من 4 بايت IPv4 بايت + عنوان

مرجع تكوين OmniEPDG

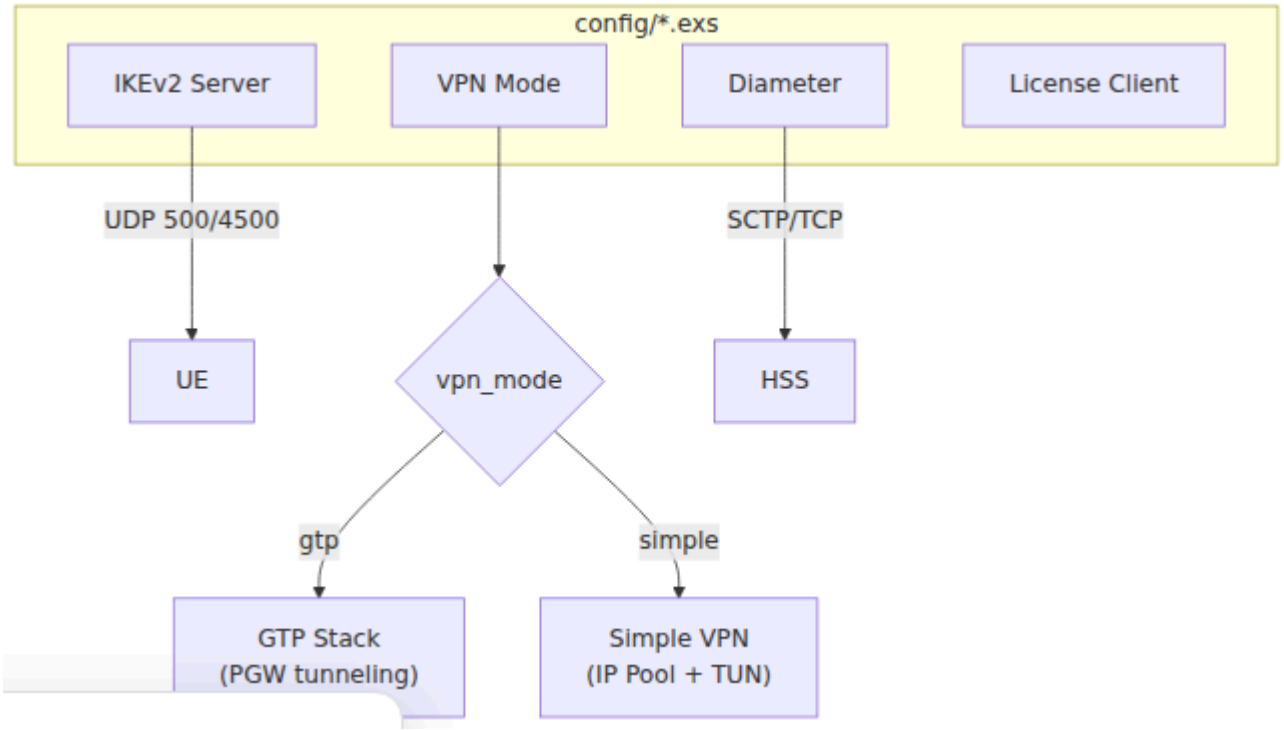
يتم تكوين OmniEPDG عبر `config/runtime.exs`. يتم إجراء جميع التكوينات ومتغيرات البيئة. القيم الافتراضية في وقت الترجمة مضمنة في الإصدار وليست مكشوفة للعملاء في وقت التشغيل - الموجهة.

للنشر في الحاويات، استخدم متغيرات البيئة كما هو موثق في قسم مرجع متغيرات البيئة.

جدول المحتويات

- معلمات خادم IKEv2
- معلمات أمان المصادقة
- اختيار وضع VPN
- معلمات VPN بسيطة
- معلمات Diameter
- تكوين عميل الترخيص
- تكوين لوحة التحكم
- تكوين مقاييس Prometheus
- تكوين Webhooks
- مرجع المهلات

هيكل التكوين



ملف التكوين

يتم إجراء جميع التكوينات في `config/runtime.exs`. يقوم OmniEPDG بقراءة هذا الملف عند بدء التشغيل. يدعم الملف استبدال متغيرات البيئة للنشر في الحاويات.

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 بسيط
  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. ينهي أنفاق IPSec ويقوم بإجراء مصادقة EAP-AKA.

المعلمة	النوع	مطلوب	الافتراضي
`listen_ip`	Tuple	لا	`{0, 0, 0, 0}`
`port_500`	Integer	لا	`500`
`port_4500`	Integer	لا	`4500`

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

معلمات أمان المصادقة

يتضمن OmniEPDG حماية مدمجة ضد هجمات القوة الغاشمة والتحكم في الوصول الجغرافي. 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 لعدد محاولات لمصادقة الفاشلة IP لكل قبل الحظر.
`auth_rate_limit_ip_window_ms`	Integer	لا	`60000`	نافذة متحركة لعد الفشل في IP بالملي) ثانية).
`auth_rate_limit_ip_block_ms`	Integer	لا	`300000`	مدة لحظر لـ التي IPs تتجاوز عتبة 5) دقائق).
`auth_rate_limit_per_imsi`	Integer	لا	`5`	الحد الأقصى لعدد محاولات لمصادقة الفاشلة IMS لكل قبل الحظر.

المعلمة	النوع	مطلوب	الافتراضي	لوصف
`auth_rate_limit_imsi_window_ms`	Integer	لا	`60000`	نافذة متحركة لعد الفشل في IMS (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`	ر ءً ة ن M C
`geoip_database_path`	String	لا	`"/etc/omniepdg/GeoLite2-Country.mmdb"`	ة ن M C C (M
`geoip_mode`	Atom	لا	`:whitelist`	(ة (ة
`geoip_countries`	List	لا	`[]`	ن I a ("
`geoip_allow_unknown`	Boolean	لا	يعتمد على الوضع	ـ ن L .

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

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 لمقارنة مفصلة.

معلمات VPN بسيطة

يتحكم كتلة التكوين `simple_vpn` في تخصيص IP وDNS لوضع VPN بسيط. يدعم OmniEPDG IPv4 وIPv6 كلاً من تجمعات عناوين.

```
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"`	ناوين IPv4 سيق CIDR صيص لكل شترك
`pool_ipv6`	String	لا	`"2001:db8::/32"`	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 CSC Prox IPv4

المعلمة	النوع	مطلوب	الافتراضي	ف
				VoW مها لـ UEs سجيل IMS.
`p_cscf_ipv6`	List	لا	`[]`	ناوين CSC Prox IPv6 VoW
`mtu`	Integer	لا	`1400`	قيمة اجهة القيم تقلل جزئة
`nat_enabled`	Boolean	لا	`true`	مكين مرور ركين. كين، طبيق قواعد تمويه حركة مرور سادرة

معلمات Diameter

يتحكم تكوين Diameter في واجهات SWx (HSS) وS6b (PGW). عندما تكون `diameter_enabled` هي `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"`

المعلمة	النوع	مطلوب	الافتراضي
`realm`	String	نعم	`"epc.mnc001.mcc001.3gppnetwork.org"`
`product_name`	String	لا	`"OmniEPDG"`
`vendor_id`	Integer	لا	`10415`

معلمات الأقران

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

المعلمة	النوع	مطلوب	الافتراضي	متغير البيئة	الوصف
`host`	String	نعم	-	`HSS_HOST`	هوية Diameter للنظير (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 OmniEPDG ضد خادم الترخيص.

```
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` - تبادل 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 المصادقة متعددة الوسائط (حسب النتيجة)
- `epdg_diameter_swx_sar_count` - طلبات تعيين الخادم (حسب النتيجة)
- `epdg_diameter_s6b_aar_count` - طلبات AA (حسب النتيجة) المعالجة
- `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 المفرج عنها (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 التجمع
- `epdg_ip_pool_utilization_ratio` - نسبة استخدام التجمع (0.0-1.0)
- `epdg_diameter_swx_pending_count` - طلبات SWx المعلقة
- `epdg_diameter_s6b_active_sessions_count` - الجلسات النشطة S6b

مقاييس المدرج التكراري (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 الثنائي
- `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 سحب Prometheus

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

تكوين Webhooks

يمكن لـ OmniEPDG إرسال webhooks عند الصادرة لأحداث دورة حياة جلسة المشترك. التمكين، يرسل OmniEPDG `POST` HTTP مع جسم JSON إلى كل نقطة نهاية مكونة عند الارتباط الناجح وعند الفصل. راجع Webhooks لنموذج التسليم، ومخطط الحمولة، وأمثلة الحمولة.

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

المعلمة	النوع	مطلوب	الافتراضي	
`enabled`	Boolean	لا	`false`	و تعطيل webhc `false` OmniE webhc
`endpoints`	List	لا	`["https://127.0.0.1/webhook"]`	عناوين . يرسل `POST` ل حدث
`events`	List	لا	`[:session_established, :session_terminated]`	ي يجب لحة هي `:sess` ط ناجح) `:sess` فصل).

بنموذج "إطلاق النار والنسيان"، ولا يعيد محاولة التسليم الفاشل. يوصل OmniEPDG webhooks للحصول على نموذج التسليم الكامل ومخطط الحمولة JSON، راجع Webhooks.

مرجع المهلات

جميع مهلات FSM الداخلية مشفرة بشكل ثابت. تتحكم هذه في المدة التي تنتظرها آلات الحالة للحصول على ردود قبل اعتبارها فاشلة.

المهلة	القيمة	الوضع	السياق	الوصف
إجابة GTP	10,000 ms	GTP	ePDG UE FSM	الحد الأقصى للانتظار لاستجابة GTPv2-C لإنشاء/حذف الجلسة 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` وتجاوز القيم الافتراضية في وقت الترجمة.

خادم IKEv2

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

وضع VPN

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

Diameter

المتغير	الافتراضي	الوصف
`DIA_LISTEN_IP`	`"0.0.0.0"`	عنوان الربط لمستمع Diameter.
`DIA_LISTEN_PORT`	`"3868"`	منفذ مستمع Diameter.
`DIA_HOST`	`"epdg"`	Diameter Origin-Host (بدون مجال).
`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 الخاص بلوحة 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 والأقران Diameter وسجلات النظام في الوقت الحقيقي. توفر لوحة التحكم عرضًا يتم تحديثه مباشرة دون الحاجة إلى تحديث الصفحة.

جدول المحتويات

- الوصول إلى لوحة التحكم
- لوحة المعلومات
- عرض الجلسات
- عرض الأقران Diameter
- عرض السجلات
- عرض الوثائق
- عرض الموارد
- عرض التكوين

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`	الأقران Diameter	حالة اتصال الأقران 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 التي تم إنشاؤها UE
البيانات المستلمة (UL)	إجمالي البايتات المستلمة من UEs (اتجاه الرفع)
البيانات المرسلة (DL)	إجمالي البايتات المرسلة إلى UEs (اتجاه التنزيل)
الأقران Diameter	الأقران المتصلة / الأقران المكونة الكلية

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

الروابط السريعة

التنقل المباشر إلى العروض التفصيلية:

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

معلومات النظام

يعرض التكوين التشغيلي الحالي:

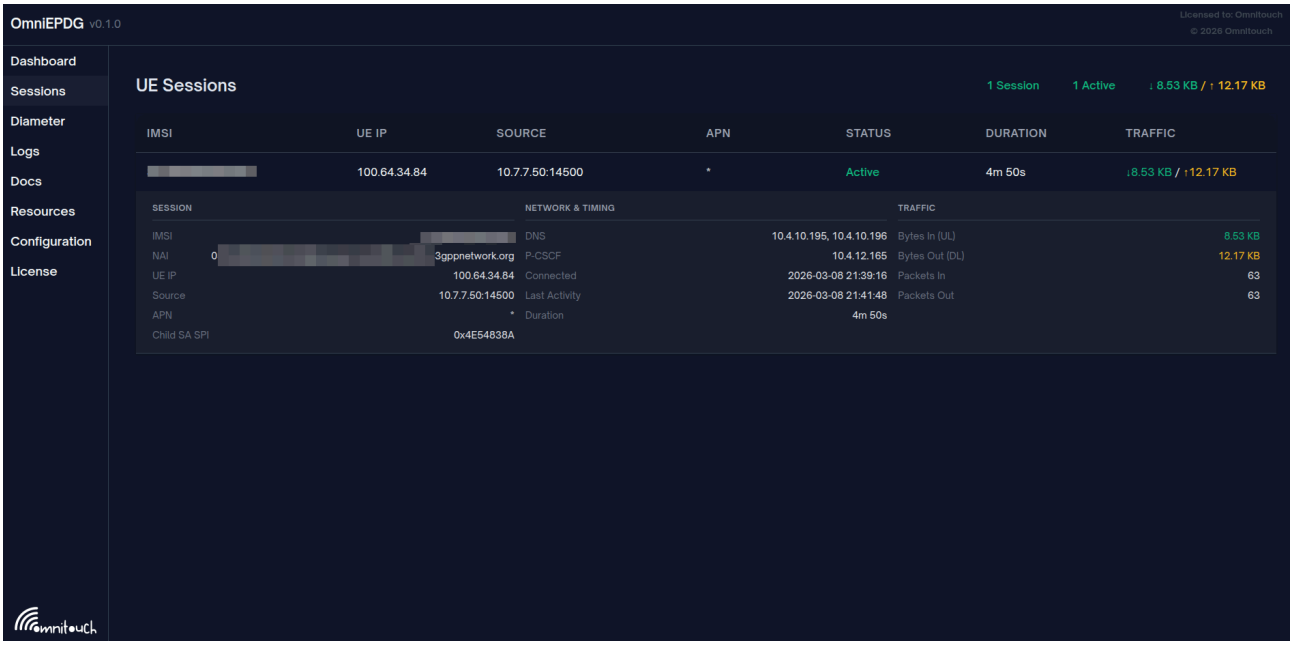
الحقل	الوصف
وضع VPN	الوضع الحالي: `GTP` أو `SIMPLE`
منافذ IKEv2	المنافذ القياسية: 500 (IKE)، 4500 (NAT-T)
حالة Diameter	ما إذا كان إشارات Diameter مفعلة
مجموعة IP (IPv4)	CIDR لمجموعة IP المكونة (وضع VPN بسيط فقط)

التحديث التلقائي

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

عرض الجلسات

يعرض عرض الجلسات جميع جلسات UE النشطة مع معلومات تفصيلية 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 للهاتف المحمول
UE IP	عنوان IPv4/IPv6 المعين
SOURCE	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 تم إنشاؤها بالكامل وتعمل
جارٍ الاتصال	أصفر	جاري إنشاء الجلسة
غير نشطة	أحمر	تم إنهاء الجلسة أو فشلت

تفاصيل الجلسة

انقر على أي صف من الجلسات لتوسيع المعلومات التفصيلية:

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

قسم الجلسة

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

قسم الشبكة والتوقيت

الحقل	الوصف
DNS	خوادم DNS المقدمة للـ UE
P-CSCF	خوادم Proxy-CSCF لإشارات IMS
Connected	الطابع الزمني عند 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 الأقران Diameter

يعرض عرض الأقران Diameter حالة جميع الأقران Diameter المكونة (HSS لـ SWx، PGW لـ S6b).

قائمة الأقران

تعرض كل صف من الأقران:

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

مؤشرات الحالة

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

ملخص عدد الأقران

يعرض الرأس الأعداد الإجمالية:

- **متصل** - عدد الأقران مع اتصالات نشطة **X**
- **غير متصل** - عدد الأقران بدون اتصالات **Y**

تفاصيل النظير

انقر على أي صف من الأقران لتوسيع المعلومات التفصيلية:

الحقل	الوصف
Initiation Connection	من يقوم بالبدء: `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 تكون هناك أقران مكونة، يعرض العرض:

- "لا توجد أقران Diameter مكونة" إذا كان Diameter مفعلًا
- "Diameter معطل" مع تلميح التكوين إذا كان معطلًا

التحديث التلقائي

تقوم قائمة الأقران بتحديث نفسها تلقائيًا كل ثانية.

عرض السجلات

يوفر عرض السجلات بثًا في الوقت الحقيقي لسجلات النظام مع إمكانيات التصفية والبحث.

عرض السجلات

تظهر السجلات في حاوية قابلة للتمرير مع أحدث الإدخالات في الأسفل. تعرض كل إدخال سجل:

العنصر	الوصف
Timestamp	متى تم إنشاء إدخال السجل
Level	مستوى الخطورة مع ترميز الألوان
Message	محتوى رسالة السجل

مستويات السجلات

تُرمز السجلات بالألوان حسب الخطورة:

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

تصفية المستوى

يمكن تصفية السجلات حسب الحد الأدنى لمستوى الخطورة باستخدام القائمة المنسدلة:

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

البحث

تقوم مربع البحث بتصفية السجلات في الوقت الحقيقي:

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

التحكم

التحكم	الوصف
إيقاف/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 إدخال سجل
- تتم إزالة أقدم الإدخالات عند الوصول إلى الحد
- يؤدي مسح السجل��ت إلى إزالة جميع الإدخالات من العرض

الحالة الفارغة

عندما لا تتطابق أي سجلات مع الفلاتر الحالية:

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

التحديث التلقائي

تظهر سجلات جديدة تلقائيًا عند إنشائها (عند عدم الإيقاف).

عرض الوثائق

يوفر عرض الوثائق متصفح وثائق مدمج، مما يسمح للمشغلين بالوصول 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	هندسة النظام وتدفقات المكالمات
configuration.md	مرجع تكوين كامل
control-panel.md	دليل لوحة التحكم هذه
metrics.md	مرجع مقاييس Prometheus
troubleshooting.md	القضايا الشائعة وخطوات الحل

عرض Markdown

تُعرض الوثائق بدعم كامل من Markdown بما في ذلك:

- العناوين وتنسيق النص
- كتل التعليمات البرمجية مع تمييز الصيغة
- 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 التي تعمل

تدرج جميع تطبيقات OTP المحملة مقسمة حسب الفئة:

الفئة	الوصف
الرئيسية	تطبيق OmniEPDG
النظام	تطبيقات Erlang/OTP وElixir الأساسية

انقر على تطبيق لعرض تفاصيله بما في ذلك الإصدار والوصف 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

يعرض 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

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

جدول المحتويات

- نقطة نهاية المقاييس
- التكوين
- فئات المقاييس
  - مقاييس جلسة IKEv2
  - مقاييس مصادقة EAP
  - مقاييس أمان المصادقة
  - مقاييس Diameter SWx
  - مقاييس Diameter S6b
  - مقاييس دورة حياة الجلسة
  - مقاييس بيانات ESP
  - مقاييس مجموعة IP
  - مقاييس VM
- تكامل Prometheus
- استعلامات نموذجية
- قواعد التنبيه

نقطة نهاية المقاييس

يقدم OmniEPDG المقاييس في:

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

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

التكوين

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

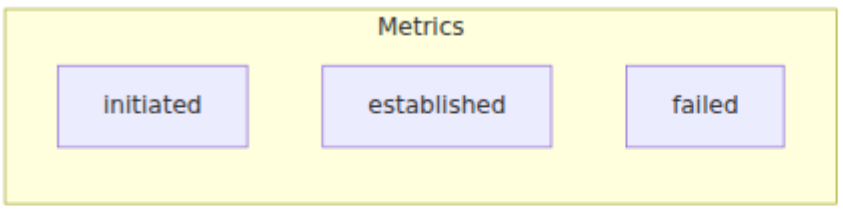
```
config :omniepdg,
  prometheus: %{
    port: 9568
  }
```

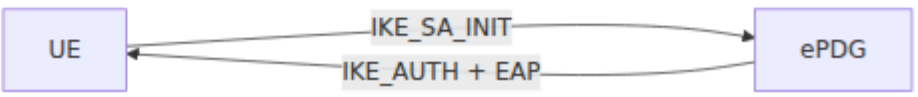
المعامل	النوع	الافتراضي	متغير البيئة	الوصف
`port`	عدد صحيح	`9568`	`PROMETHEUS_PORT`	منفذ HTTP لنقطة نهاية `/metrics`

فئات المقاييس

مقاييس جلسة IKEv2

مقاييس تتبع إنشاء نفق IKEv2 على واجهة SWu.





المقياس: `epdg_ikev2_session_initiated_count`
النوع: عداد
الوصف: إجمالي تبادلات IKE_SA_INIT التي تم بدءها. يزيد عندما يقوم UE ببدء إنشاء النفق.

المقياس: `epdg_ikev2_session_established_count`
النوع: عداد

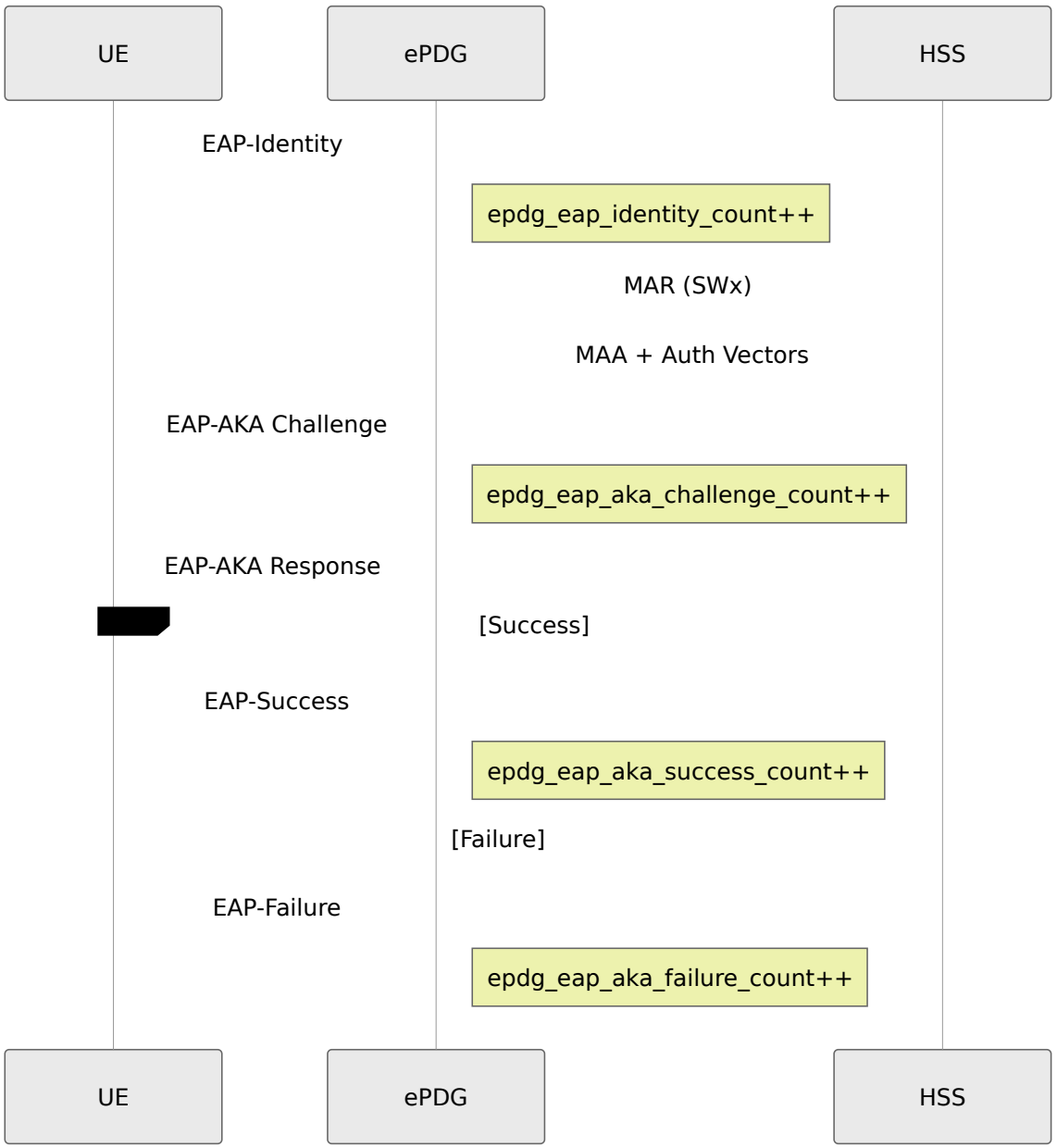
الوصف: إجمالي IKE SAs التي تم إنشاؤها بنجاح. يزيد بعد المصادقة الناجحة باستخدام EAP-AKA وإنشاء Child SA.

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

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

مقاييس مصادقة EAP

مقاييس تتبع تدفقات مصادقة EAP-AKA وفقًا لـ RFC 4187. يدعم OmniEPDG أيضًا EAP-AKA' مع تحديد 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 إعادة 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 فش�� التحقق من الحمولة AUTH. يشير 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). يشير إلى هجمات محتملة من نوع إعادة التشغيل أو مشاكل 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-Requests 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-Requests 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 بالميلي ثانية
الأ��سام: 50، 100، 250، 500، 1000، 2500 مللي ثانية

المقياس: `epdg_diameter_swx_sar_latency_ms`
النوع: هيستوجرام
الوصف: زمن استجابة SAR بالميلي 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 مشاكل في الاتصال HSS.

مقاييس Diameter S6b

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

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

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

المقياس: `epdg_diameter_s6b_str_count`
النوع: عداد
الوصف: إجمالي طلبات Session-Termination-Requests المعالجة

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

مقاييس دورة حياة الجلسة

مقاييس تتبع إنشاء الجلسة PDN وإنهائها.

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 مللي 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 (اتجاه UE → الشبكة)

المقياس: `epdg_esp_packets_out_count`
النوع: عداد
الوصف: إجمالي حزم ESP التي تم تشفيرها (اتجاه الشبكة → UE)

المقياس: `epdg_esp_bytes_in_total`
النوع: مقياس
الوصف: إجمالي البايتات المفككة من حزم ESP

المقياس: `epdg_esp_bytes_out_total`
النوع: مقياس
الوصف: إجمالي البايتات المشفرة في حزم ESP

مقاييس مجموعة IP

مقاي��س لإدارة مجموعة 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 التي تم تحريرها
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 المجموعة

المقياس: `epdg_ip_pool_utilization_ratio`
النوع: مقياس
الوصف: استخدام مجموعة IP كنسبة من 0.0 إلى 1.0. تشير القيم القريبة من 1.0 إلى خطر استنفاد المجموعة.

مقاييس VM

مقاييس آلة افتراضية Erlang/BEAM لمراقبة صحة النظام.

المقياس: `vm_memory_total`
النوع: مقياس
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، مقبضات الملفات)

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

تكامل Prometheus

تكوين السحب

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

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

اكتشاف الخدمة

لعمليات نشر 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 استجابة 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 مجموعة 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]))

# إنهاءات 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 المصادقة باستخدام"
          description: "معدل فشل المصادقة هو {{ $value |
humanizePercentage }} خلال آخر 5 دقائق"

      # قريبة من الاستنفاد IP مجموعة
      - alert: OmniEPDGIPPoolLow
        expr: epdg_ip_pool_utilization_ratio > 0.9
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "استخدام مجموعة IP 90 فوق%"
          description: "مجموعة IP مستخدمة بنسبة {{ $value |
humanizePercentage }}"

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

      # 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: "زمن استجابة HSS (SWx) مرتفع"
          description: "زمن استجابة MAR هو 95 في النسبة المئوية {{
$value }}ms"

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

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

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

      # لا توجد جلسات (مشكلة محتملة في الخدمة)
```

```
      - 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 العالي (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: "نشاط حجب GeoIP مرتفع"
          description: "{{ $value | printf \"%.1f\" }} اتصالات
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"
```

```
      # حالات فشل التحقق من AUTH (هجوم محتمل من نوع MITM)
      - 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"
```

وضع N3IWF (الوصول غير GPP) غير 3 G الموثوق 5

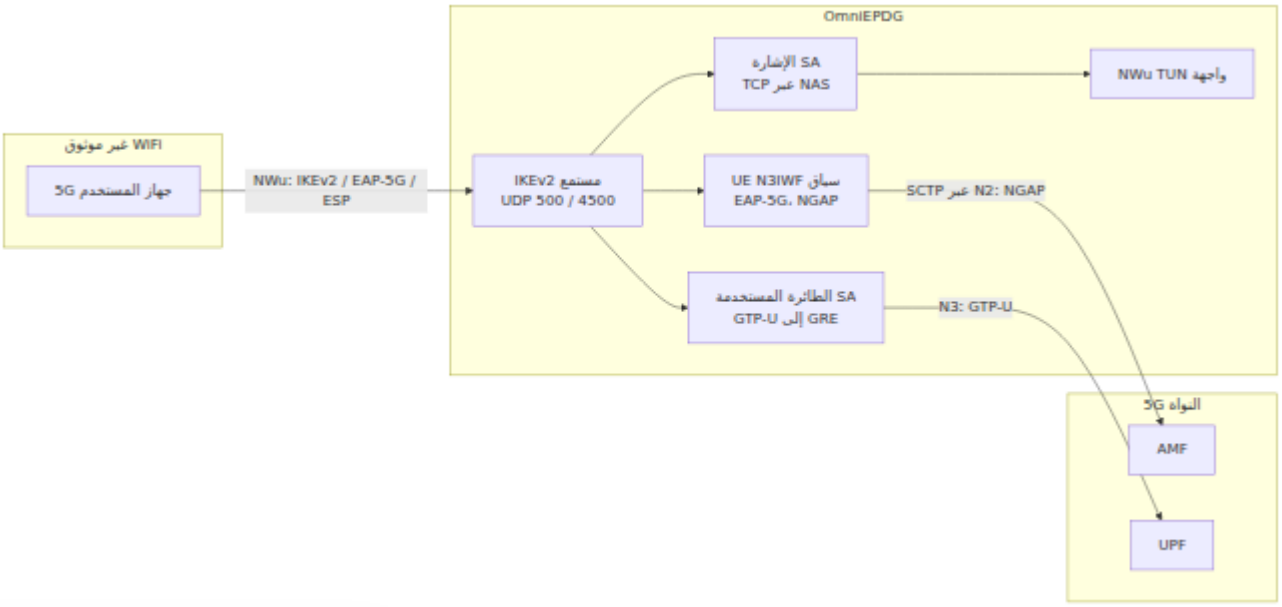
يمكن أن تعمل OmniEPDG **3 غير وظيفة التداخل** كـ**GPP (N3IWF)**. في هذا الوضع، يتصل OmniEPDG. تستخدم OmniEPDG من خلال G (5GC) غير موثوقة بالنواة WiFi 5 بشبكة G جهاز المستخدم 5 N3IWF و ePDG نفس مستمع IKEv2، ونفس مسار بيانات ESP ونفس مقبس GTP-U.

العودة إلى دليل العمليات.

جدول المحتويات

- نظرة عامة على المعمارية
- كيفية اختيار OmniEPDG لوضع N3IWF
- الواجهات
- اختيار AMF
- تدفق التسجيل
- تدفق جلسة PDU
- تدفق الإنهاء
- العنوان الداخلي NWu
- التكوين
- متطلبات المضيف
- المقاييس
- القيود
- استكشاف الأخطاء وإصلاحها
- مواصفات 3GPP

نظرة عامة على المعمارية



تقوم N3IWF بنقل رسائل NAS بين UE و AMF. لا تقرأ N3IWF محتوى NAS. تنتقل بيانات المستخدم في حزم GRE داخل SA فرعية IPsec. تقوم N3IWF بتحويل كل حزمة GRE إلى حزمة GTP-U لـ UPF، والعكس بالنسبة للبيانات الهابطة.

كيفية اختيار OmniEPDG لوضع N3IWF

تفحص OmniEPDG أول طلب IKE_AUTH لكل SA IKE.

يرسل UE	سلوك OmniEPDG
IDi من النوع `ID_KEY_ID` ولا يوجد حمولة AUTH	تعمل الجلسة كجلسة N3IWF (جهاز المستخدم 5GIG).
IDi من النوع `ID_RFC822_ADDR` (NAI)	تعمل الجلسة كجلسة ePDG (EAP-AKA، SWx، S2b).

يجب على جهاز المستخدم 5G إرسال `ID_KEY_ID` في IDi، كما تحدد 3GPP TS 33.501 §7.2.1 3 و3GPP TS 24.502 §7.3.2.1. لا تتغير جلسات ePDG عند تمكين وضع N3IWF.

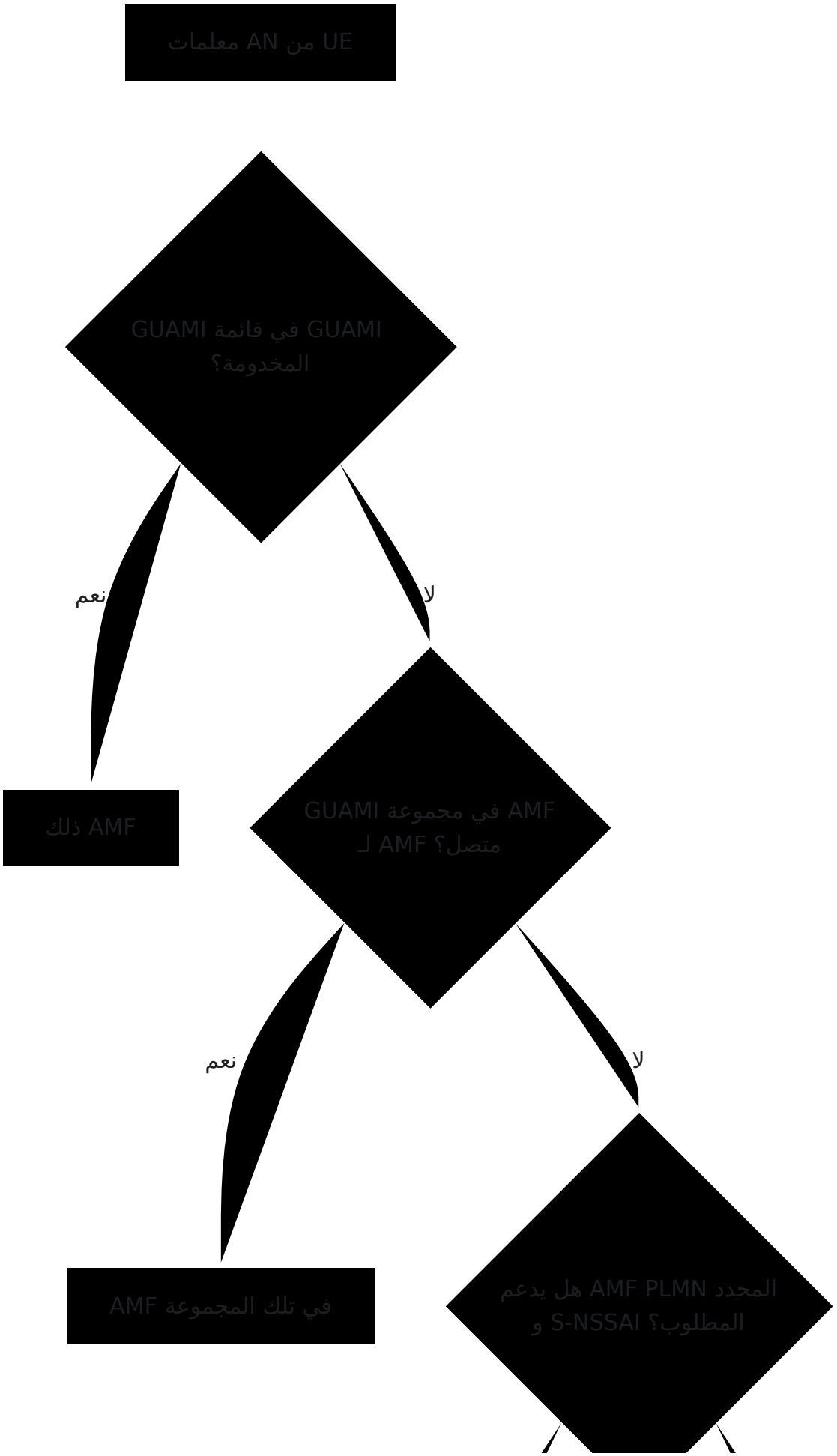
الواجهات

الواجهة	النظير	النقل	البروتوكول	المرجع
NWu	جهاز المستخدم 5G	UDP 500 / 4500	IKEv2، EAP-5G، ESP (NAT-T)	TS 24.502، RFC 7296
NWu (داخلي)	جهاز المستخدم 5G	TCP داخل SA الإشارة	غلاف رسالة NAS	TS 24.502 §8.2
NWu (داخلي)	جهاز المستخدم 5G	GRE داخل SA الطائرة المستخدمة	GRE مع QFI في المفتاح	TS 24.502 §8.3
N2	AMF	SCTP، PPID 60	NGAP	TS 38.412، TS 38.413
N3	UPF	UDP 2152	GTP-U مع حاوية جلسة PDU	TS 29.281، TS 38.415

عند بدء التشغيل، تتصل OmniEPDG بكل AMF في `amfs` إعداد NG وترسل لكل منها طلب 5G أجهزة المستخدم OmniEPDG تقبل. `GlobalN3IWF-ID` عندما يكون قد أرسل AMF واحد على الأقل استجابة إعداد NG. إذا فشل ارتباط SCTP، تحاول OmniEPDG ذلك AMF مرة أخرى بإلغاء فقط جلسات OmniEPDG كل 5 ثوانٍ. إذا انقطع ارتباط، تقوم N3IWF على ذلك AMF.

اختيار AMF

تختار N3IWF AMF واحد لكل UE عند وصول أول رسالة NAS EAP-5G. تستخدم N3IWF معلمات AN من UE (TS 24.502 §9.3.2.2.2) والبيانات التي أرسلها كل AMF في استجابته لإعداد NG. يبقى UE على ذلك AMF حتى الإنهاء. انظر TS 23.501 §6.3.5.


معلمات AN من UE
GUAMI في قائمة GUAMI المخدومة؟
نعم
لا
AMF ذلك
AMF في مجموعة GUAMI متصل؟ AMF لـ
نعم
لا
في تلك المجموعة AMF
AMF PLMN المحدد هل يدعم S-NSSAI و المطلوب؟



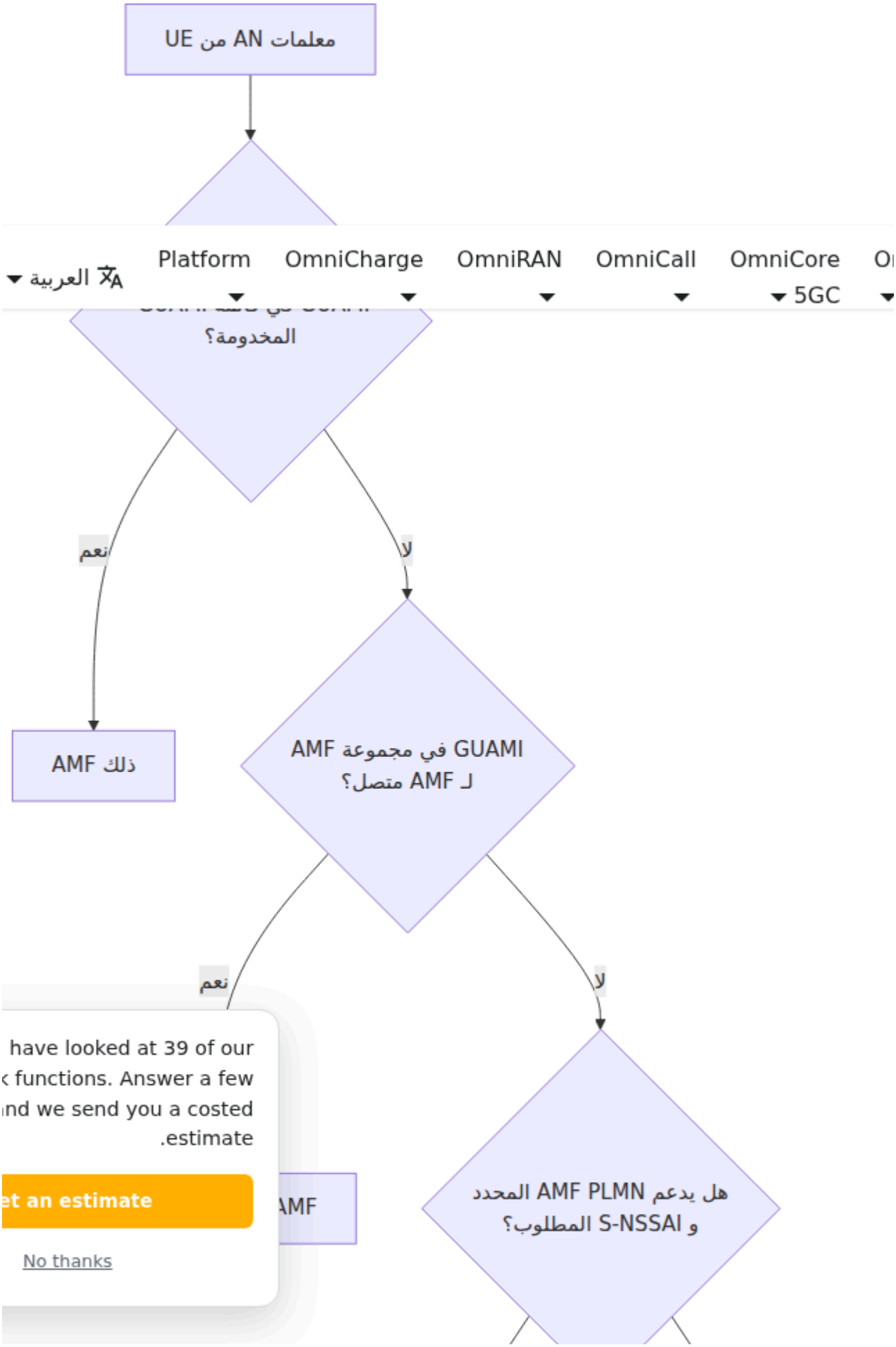
الخطوة	معلمة AN	بيانات AMF من استجابة إعداد NG	النتيجة
1	GUAMI	قائمة GUAMI المخدومة	GUAMI الذي يخدم هذا AMF بالضبط. يعود UE المسجل إلى AMF الخاص به.
2	GUAMI	قائمة GUAMI المخدومة	AMF بنفس PLMN، معرف منطقة AMF ومعرف مجموعة AMF.
3	معرف PLMN المحدد، NSSAI المطلوب	قائمة دعم PLMN	AMF الذي يدعم PLMN المحدد و S-NSSAI المطلوب على الأقل. إذا لم يرسل UE PLMN أو NSSAI، فإن هذا التحقق لا ينطبق.

واحدًا عشوائيًا. يتم وزن الاختيار بواسطة N3IWF مع خطوة، تختار AMF عندما يتطابق أكثر من سعة AMF النسبية لكل AMF. يحصل AMF بسعة 0 على UE فقط عندما يتطابق GUAMI الدقيق المتطابق بسعة 0 AMF معه، أو عندما يكون كل UE للـ.

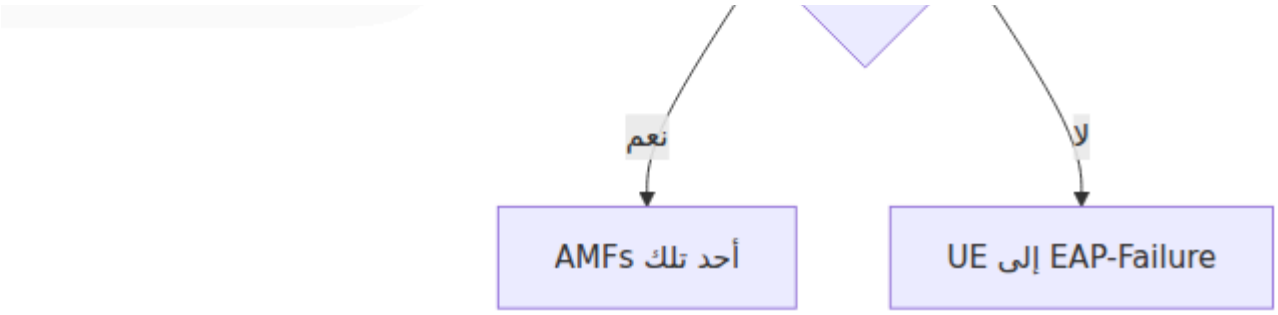
إذا لم يتطابق أي AMF متصل، ترسل N3IWF EAP-Failure إلى UE `لا` وتقوم بتسجيل `AMF يخدم GUAMI، PLMN أو شرائح UE`.

حالة الاستخدام: استخدم N3IWF 5 واحدة للمشتركين على نوى G لكل نواة AMF مختلفة. ضع GUAMI الخاص بها بواسطة AMF التي تم تسجيلها مسب`amfs`ا إلى UEs تعود في . تذهب UEs الجديدة إلى AMF الذي يخدم PLMN وشرائحها.

تدفق التسجيل



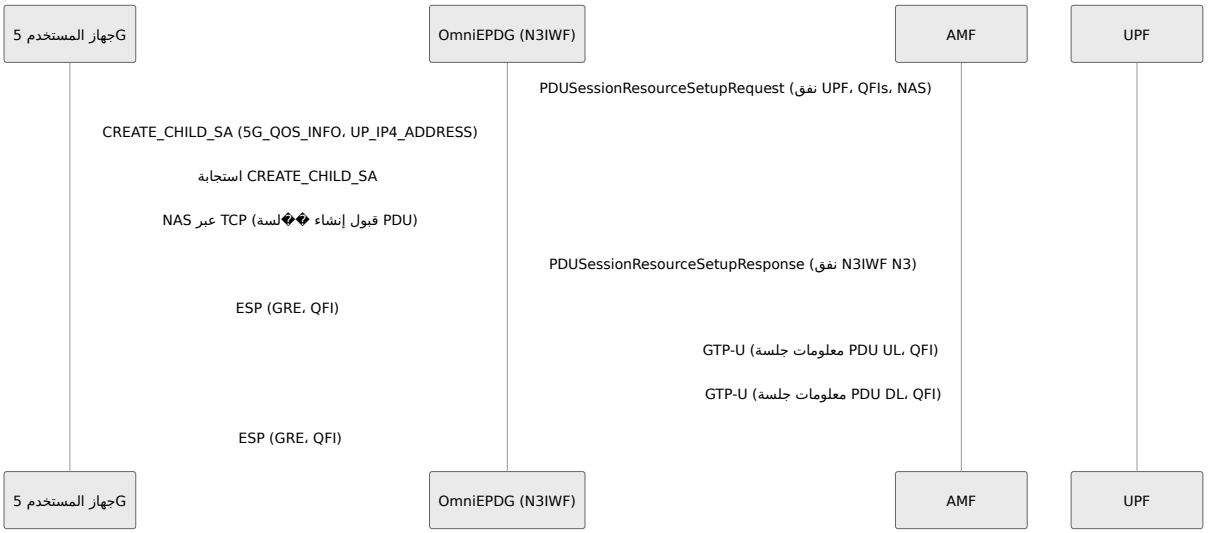
have looked at 39 of our
k functions. Answer a few
nd we send you a costed
.estimate
et an estimate
No thanks



تنطبق هذه النقاط على التدفق:

- تقوم N3IWF بتوقيع أول استجابة IKE_AUTH لها باستخدام المفتاح في `key_file`. تتضمن N3IWF شهادتها فقط إذا أرسل UE CERTREQ.
- لا تجيب N3IWF على طلب EAP-5G من UE حتى يرسل AMF رسالة NAS أو هابطة مفتاح N3IWF.
- يستخدم UE و N3IWF **Kn3iwf** من InitialContextSetupRequest كـ EAP MSK. يقوم كلا الطرفين بحساب حمولة AUTH النهائية الخاصة بهم من هذا المفتاح.
- إذا أرسل AMF NAS هابطة قبل أن يفتح UE اتصال TCP، تحتفظ N3IWF برسالة NAS وترسلها عند فتح الاتصال.
- إذا أرسل UE EAP-Response/5G-Stop، ترسل N3IWF EAP-Failure وتزيل SA IKE.

تدفق جلسة PDU



تقوم N3IWF بإنشاء SA فرعية واحدة للطائرة المستخدمة لكل جلسة PDU. هذه SA هي الفرعية الافتراضية وتحمل جميع تدفقات QoS لجلسة PDU. تخبر حمولة الإخطار SA بمعرف جلسة PDU و QFIs. 5G_QOS_INFO UE

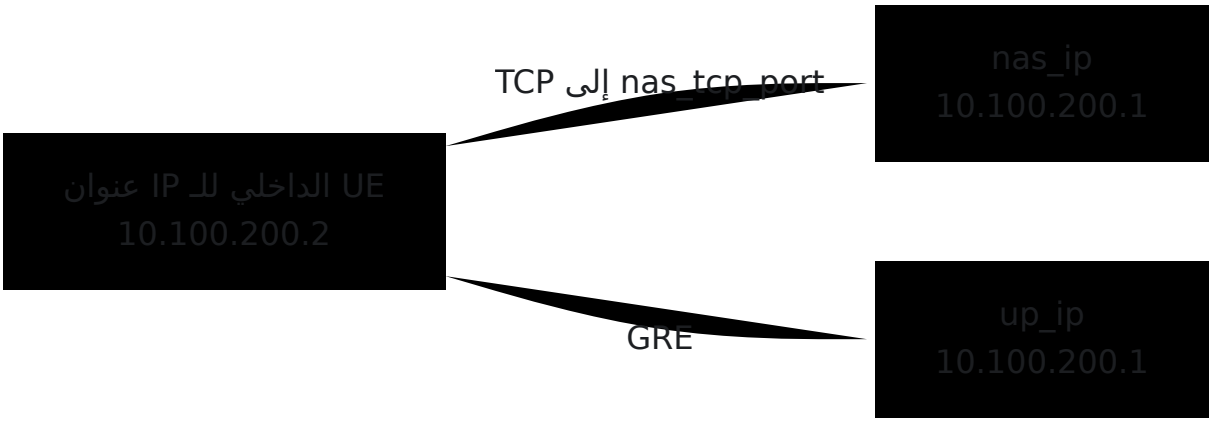
إذا رفض UE SA بالإبلاغ عن جلسة N3IWF فرعية، أو لم يرد بعد 5 عمليات إرسال، تقوم PDU على أنها فاشلة في PDUSessionResourceSetupResponse.

تدفق الإنهاء

إجراء N3IWF	الزناد
تقوم N3IWF بحذف SA IKE، وإغلاق اتصال NAS وإرسال UEContextReleaseComplete.	UEContextReleaseCommand من AMF
ترسل N3IWF UEContextReleaseRequest إلى AMF.	يقوم UE بحذف SA IKE
تقوم N3IWF بحذف SA الفرعية لكل جلسة PDU وترسل PDUSessionResourceReleaseRespons	PDUSessionResourceReleaseCommand من AMF
تقوم N3IWF بإلغاء UEs المسماة (أو جميع UEs) وترسل NGResetAcknowledge.	NG Reset من AMF
تقوم N3IWF بإلغاء جميع جلسات N3IWF.	فقدان ارتباط N2
تقوم N3IWF بإلغاء الجلسة بعد `session_inactivity_timeout_ms` ون حركة مرور IKE أو ESP. انظر مرجع التكوين.	عدم النشاط في الجلسة

العنوان الداخلي NWu

تمنح N3IWF كل UE **عنوان IP داخلي** من `ue_ip_pool`. يستخدم UE هذا العنوان داخل أنفاق IPsec الخاصة به.



- **الإشارة:** يفتح SA اتصال UE إلى TCP إلى `nas_ip` و `nas_tcp_port`. تكتب N3IWF هذه الحزم إلى واجهة NWu TUN، بحيث ينهي مكدس TCP في Linux الاتصال.
- **الطائرة المستخدمة:** يرسل SA حزم GRE إلى UE `up_ip`. تقوم OmniEPDG بفك تغليف GRE في مساحة المستخدم. لا ترى النواة هذه الحزم.

`up_ip` نفس `nas_ip` و يمكن أن يكون UE. إلى `up_ip` أو `nas_ip` لا تعطي المجموعة العنوان.

التكوين

وضع N3IWF في مغلق بشكل افتراضي. ��م بتعيين المعلما�ت `runtime.exs`.

```
config :omniepdg, :n3iwf,
  enabled: true,
  # GlobalN3IWF-ID و TA المخدومة لإعداد NG
  n3iwf_id: 1,
  name: "OmniN3IWF",
  plmn: {"001", "01"},
  tac: 1,
  slices: [%{sst: 1, sd: nil}],
  # N2 (SCTP) إلى كل AMF
  amfs: [
    %{name: "amf1", ip: {10, 74, 0, 40}, port: 38412},
    %{name: "amf2", ip: {10, 74, 0, 41}, port: 38412}
  ],
  ngap_local_ip: {10, 74, 0, 13},
  # IDr المرسل إلى UEs والشهادة/المفتاح الذي يوقع IKE_AUTH
  identity: "n3iwf.5gc.mnc001.mcc001.3gppnetwork.org",
  cert_file: "/etc/omniepdg/certs/n3iwf.crt",
  key_file: "/etc/omniepdg/certs/n3iwf.key",
  # عنوان GTP-U N3 المعلن لـ UPF
  n3_ip: {10, 74, 0, 13},
  # العنوان الداخلي NWu
  ue_ip_pool: "10.100.200.0/24",
  nas_ip: {10, 100, 200, 1},
  up_ip: {10, 100, 200, 1},
  nas_tcp_port: 20000,
  tun_name: "omnin3iwf0"
```

إذا كانت معلمة مفقودة أو غير صالحة، `enabled` هي `true`. جميع المعلمات مطلوبة عندما تكون `enabled`. يذكر خطأ بدء التشغيل اسم المعلمة. لا تبدأ OmniEPDG.

المعلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	نعم	`false`	يشغل أو يغلق وضع N3IWF. عندما تكون `false`، تتجاهل جميع OmniEPDG المعلمات الأخرى لـ N3IWF.
`n3iwf_id`	Integer	نعم	-	معرف N3IWF في `GlobalN3IWF-ID` لطلب إعداد NG. النطاق من 0 إلى 65535 (16 بت). انظر TS 38.413 §9.3.1.57.
`name`	String	نعم	-	اسم عقدة RAN في طلب إعداد NG. يظهر هذا AMF الاسم لـ N3IWF.
`plmn`	Tuple	نعم	-	PLMN لـ N3IWF كـ `{mcc, mnc}` سلاسل رقمية. يجب أن يخدم هذا AMF PLMN.
`tac`	Integer	نعم	-	رمز منطقة التتبع (24 بت) في قائمة TA المدعومة لطلب إعداد NG. يجب أن يخدم هذا AMF TAC.
`slices`	List	نعم	-	S-NSSAIs التي تدعمها N3IWF. كل إدخال هو `%{sst: 0..255, sd: nil}` أو `%{sst: 0..255, sd: <<b1, b2, b3>>}`.
`amfs`	List	نعم	-	AMFs للاتصال بها عبر N2. كل إدخال هو `%{name:`

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				`string, ip: IPv4 tuple, port: integer}`. `name` هو تسمية فريدة للسجلات. `port` هو منفذ SCTP المنفذ. N2 لواجهة AMF القياسي هو 38412 (TS 38.412). انظر اختيار AMF.
`ngap_local_ip`	Tuple	نعم	-	عنوان IPv4 محلي لارتباطات SCTP إلى AMFs.
`identity`	String	نعم	-	هوية N3IWF (FQDN) في حمولة IDr. يقارن UE هذه القيمة مع N3IWF التي اختارها. استخدم FQDN في الشهادة.
`cert_file`	String	نعم	-	مسار شهادة N3IWF (PEM). ترسل N3IWF هذه الشهادة عندما يرسل UE CERTREQ.
`key_file`	String	نعم	-	مسار المفتاح الخاص (PEM، غير مشفر) لـ `cert_file`. تقوم مفاتيح RSA بالتوقيع باستخدام طريقة AUTH 1. تقوم مفاتيح ECDSA P-256 بالتوقيع باستخدام طريقة AUTH 9.
`n3_ip`	Tuple	نعم	-	عنوان IPv4 على N3 الذي تعطيه N3IWF لـ AMF للبيانات الهابطة GTP-U. يرسل UPF البيانات الهابطة

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				إلى هذا العنوان عبر UDP 2152.
`ue_ip_pool`	String	نعم	-	CIDR IPv4 لعناوين UE الداخلية. يجب أن يكون طول البادئة من 8 إلى 30.
`nas_ip`	Tuple	نعم	-	عنوان IPv4 الداخلي لـ NAS هذا N3IWF. ترسل عبر TCP في حمولة الإخطار NAS_IP4_ADDRESS وتعينه لواجهة NWu TUN. استخدم عنوانًا داخل `ue_ip_pool`.
`up_ip`	Tuple	نعم	-	عنوان IPv4 الداخلي لبيانات المستخدم GRE. ترسل هذا في حمولة N3IWF الإخطار UP_IP4_ADDRESS.
`nas_tcp_port`	Integer	نعم	-	منفذ TCP لنقل NAS. ترسل هذا في حمولة N3IWF الإخطار NAS_TCP_PORT.
`tun_name`	String	نعم	-	اسم واجهة NWu TUN. استخدم اسمًا لا تستخدمه أي عملية أخرى.

إعدادات مستمع N3IWF تستخدم IKEv2 (`listen_ip`، `port_500`، `port_4500`) و `session_inactivity_timeout_ms` من التكوين الرئيسي. انظر مرجع التكوين.

مثال على التكوين: ePDG و N3IWF على مضيف واحد

```
config :omniepdg,
  listen_ip: {0, 0, 0, 0},
  port_500: 500,
  port_4500: 4500,
  vpn_mode: :gtp

config :omniepdg, :n3iwf,
  enabled: true,
  n3iwf_id: 1,
  name: "OmniN3IWF",
  plmn: {"001", "01"},
  tac: 1,
  slices: [%{sst: 1, sd: nil}],
  amfs: [%{name: "amf1", ip: {10, 74, 0, 40}, port: 38412}],
  ngap_local_ip: {10, 74, 0, 13},
  identity: "n3iwf.5gc.mnc001.mcc001.3gppnetwork.org",
  cert_file: "/etc/omniepdg/certs/n3iwf.crt",
  key_file: "/etc/omniepdg/certs/n3iwf.key",
  n3_ip: {10, 74, 0, 13},
  ue_ip_pool: "10.100.200.0/24",
  nas_ip: {10, 100, 200, 1},
  up_ip: {10, 100, 200, 1},
  nas_tcp_port: 20000,
  tun_name: "omnin3iwf0"
```

كيف يعمل: تستخدم UEs 4G (هوية NAI) تدفق ePDG و PGW عبر S2b. تستخدم UEs 5G (هوية `ID_KEY_ID`) تدفق N3IWF و AMF عبر N2. يتشارك كلا التدفقين UDP 500 و UDP 4500 ومقبس GTP-U على UDP 2152.

حالة الاستخدام: بوابة اتصال WiFi 4 واحدة لمشتركي 5G و G.

المعلمات في الكتلة الأولى موجودة في مرجع التكوين. المعلمات في الكتلة الثانية موجودة في المعلمات.

متطلبات المضيف

- يجب أن يكون لدى OmniEPDG إذن لإنشاء واجهة NWu TUN ولتشغيل `ip addr` و `ip link` لها (`CAP_NET_ADMIN`). إذا لم تتمكن OmniEPDG من إنشاء الواجهة، فإنها لا تبدأ.
- يجب أن يدعم النواة SCTP (`sctp` module).
- السماح لـ SCTP من `ngap_local_ip` إلى كل AMF في `amfs` على `port` الخاص به.
- السماح لـ UDP 2152 بين `n3_ip` و UPF.
- يجب أن يقوم UPF بتوجيه حركة المرور الهابطة إلى `n3_ip`.

المقاييس

تستخدم جلسات N3IWF نفس مقاييس الجلسة مثل جلسات ePDG. انظر مرجع المقاييس.

النوع: عداد **الوصف**: إجمالي الجلسات التي تم إنشاؤها. تحتوي جلسات N3IWF على قيمة تسمية `vpn_mode="n3iwf"`. **التسميات**:

المقياس: `epdg_session_created_count`

- `vpn_mode` - `simple`، `gtp` أو `n3iwf`

استعلامات المثال:

```
# تسجيلات N3IWF في الثانية
rate(epdg_session_created_count{vpn_mode="n3iwf"}[5m])
```

تظهر صفحة الجلسات في لوحة التحكم جلسات N3IWF مع التسمية `n3iwf-<RAN-UE-NGAP-ID>`. لا تعرف N3IWF SUPI، لأن رسائل NAS مشفرة بين UE و AMF.

القيود

- IPv4 فقط للعناوين الداخلية، نقل NAS و N3.
- ترسل N3IWF نفس `plmn` و `tac` و `slices` في طلب إعداد NG إلى كل AMF. يجب أن يخدم كل AMF في `amfs` هذا PLMN و TAC.
- تقرأ N3IWF قائمة GUAMI المخدومة، قائمة دعم PLMN وسعة AMF النسبية من استجابة إعداد NG فقط. لا تطبق تحديث تكوين AMF.

- SA فرعية واحدة للطائرة المستخدمة لكل جلسة PDU. لا تقوم N3IWF بإنشاء SA فرعية إضافية لتدفقات QoS منفصلة.
- لا تقبل N3IWF طلبات CREATE_CHILD_SA من UE. تجيب بـ NO_ADDITIONAL_SAS، لذا فإن إعادة التشفير التي يبدأها UE غير متاحة.
- تقوم N3IWF بتسجيل PDUSessionResourceModifyRequest ولا تتصرف بناءً عليه.

استكشاف الأخطاء وإصلاحها

لا تتصل UEs 5G

الأعراض: يرسل UE IKE_AUTH ويتلقى AUTHENTICATION_FAILED. يظهر السجل `n2_not_ready`.

الأسباب المحتملة:

- لا يوجد ارتباط SCTP مع AMF نشط.
- رفضت AMFs طلب إعداد NG.

الحل:

1. ابحث عن `فشل الاتصال` بـ `AMF SCTP N2` أو `رفض إعداد` في `AMF بواسطة NG` السجل. يحدد حقل السجل `amf` الإدخال في `amfs`.
2. تأكد من أن `ip` و `port` لكل إدخال في `amfs` صحيحة.
3. تأكد من أن كل AMF يخدم قيم `plmn` و `tac`.

يتلقى UE EAP-Failure بعد أول رسالة EAP-5G

الأعراض: يتلقى UE EAP-Failure `لا` بعد أن يرسل طلب التسجيل. يظهر السجل `AMF يخدم UE أو شرائح PLMN أو GUAMI`.

الأسباب المحتملة:

- لا يخدم أي AMF متصل GUAMI، PLMN المحدد أو S-NSSAI المطلوب لـ UE.

الحل:

1. قارن حقول السجل `guami` و `selected_plmn` و `requested_nssai` مع قائمة دعم PLMN لكل AMF.
2. تأكد من أن AMF موجود في ��النوا لتلك `amfs` وأن ارتباطه نشط.

N3IWF يرفض شهادة UE

الأعراض: يتوقف UE بعد أول استجابة IKE_AUTH.

الأسباب المحتملة:

- لا يثق UE بالشهادة في `cert_file`.
- FQDN للشهادة ليس هو نفسه `identity`.

الحل:

1. قم بتثبيت CA الجذر لـ `cert_file` على UE.
2. تأكد من أن `identity` هو FQDN في الشهادة.

EAP-Success بعد UE لكن AUTH للـ التحقق من فشل

الأعراض: يظهر السجل `N3IWF: فشل التحقق من AUTH للـ UE`.

الأسباب المحتملة:

- استمد AMF Kn3iwf باستخدام مميز نوع الوصول الخاطئ. بالنسبة للوصول غير 3GPP، يكون المميز هو `0x02` (TS 33.501 الملحق A.9).
- استخدم AMF عد NAS الهابطة COUNT الذي يختلف عن قيمة UE.

الحل:

1. تأكد من أن AMF 3 يستخدم مميز الوصول غير 3GPP لـ Kn3iwf.
2. تأكد من أن AMF يستخدم COUNT NAS للاتصال NAS 3 غير 3GPP.

UE لا يصل قبول التسجيل إلى

الأعراض: SA IPsec نشطة. يرسل AMF DownlinkNASTransport، لكن UE لا يسجل.

الأسباب المحتملة:

- لا يمكن لـ UE تصال فتح TCP إلى `nas_ip` و `nas_tcp_port`.
- واجهة NWu TUN غير نشطة.

الحل:

1. تأكد من أن واجهة TUN `tun_name` نشطة ولديها `nas_ip`.
2. تأكد من أن لا قاعدة جدار ناري تمنع TCP إلى `nas_tcp_port` على واجهة TUN.

لا توجد بيانات مستخدم بعد إعداد جلسة PDU

الأعراض: جلسة PDU نشطة، لكن UE لا توجد لديه بيانات.

الأسباب المحتملة:

- لا يمكن لـ UPF الوصول إلى `n3_ip` عبر UDP 2152.
- يمنع جدار ناري GTP-U بين N3IWF و UPF.

الحل:

1. تأكد من أن UPF يرسل GTP-U هابط إلى `n3_ip`.
2. تأكد من أن UDP 2152 مفتوح في كلا الاتجاهين.

مواصفات 3GPP

المواصفة	العنوان
TS 23.501	معمارية النظام لنظام 5G
TS 23.502	الإجراءات لنظام 5G (§4.12: الوصول غير الموثوق غير 3GPP)
TS 24.502	الوصول إلى 3GPP 5GC عبر الشبكات غير 3GPP (EAP-5G، NWu، GRE)
TS 33.501	معمارية الأمان والإجراءات لنظام 5G (§7.2.1، الملحق A.9)
TS 38.412	نقل الإشارات NG (SCTP)
TS 38.413	بروتوكول التطبيق NG (NGAP)
TS 38.415	بروتوكول الطائرة المستخدمة لجلسة PDU
TS 29.281	GTP-U
RFC 7296	IKEv2

متطلبات الشبكة

تتناول هذه الوثيقة منافذ جدار الحماية وإدخالات DNS المطلوبة لنشر OmniEPDG لمكالمات WiFi.

منافذ جدار الحماية

المنافذ المواجهة للإنترنت (UE ↔ ePDG)

يجب أن تكون هذه المنافذ مفتوحة على الإنترنت حتى 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	IKEv2 NAT-Traversal و ESP-in-UDP encapsulation

المنفذ 500/UDP يتعامل مع التفاوض الأولي لـ IKEv2. إذا تم اكتشاف NAT بين UE و ePDG، فإن الاتصال ينتقل تلقائيًا إلى المنفذ 4500، وهو الأمر الذي يحدث تقريبًا دائمًا في مكالمات WiFi.

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

منافذ الشبكة الداخلية (ePDG ↔ Core)

تستخدم 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 التحكم (S2b)	PGW
2152	UDP	ثنائي الاتجاه	GTP-U بيانات المستخدم (S2b-U)	PGW

منافذ الإدارة

تستخدم هذه المنافذ للمراقبة التشغيلية ويجب تقييدها على الشبكات الإدارية.

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

متطلبات DNS

سجل DNS لاكتشاف ePDG

تكتشف الأجهزة المحمولة ePDG باستخدام نظام 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، مضافًا بالصفر إلى 3 أرقام (مثل `001`)

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

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

الاسم الشائع للشهادة

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

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 موثوق (تتحقق الأجهزة من السلسلة)
- الحد الأدنى هو RSA 2048-bit أو ECDSA P-256

مجال Diameter DNS

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

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

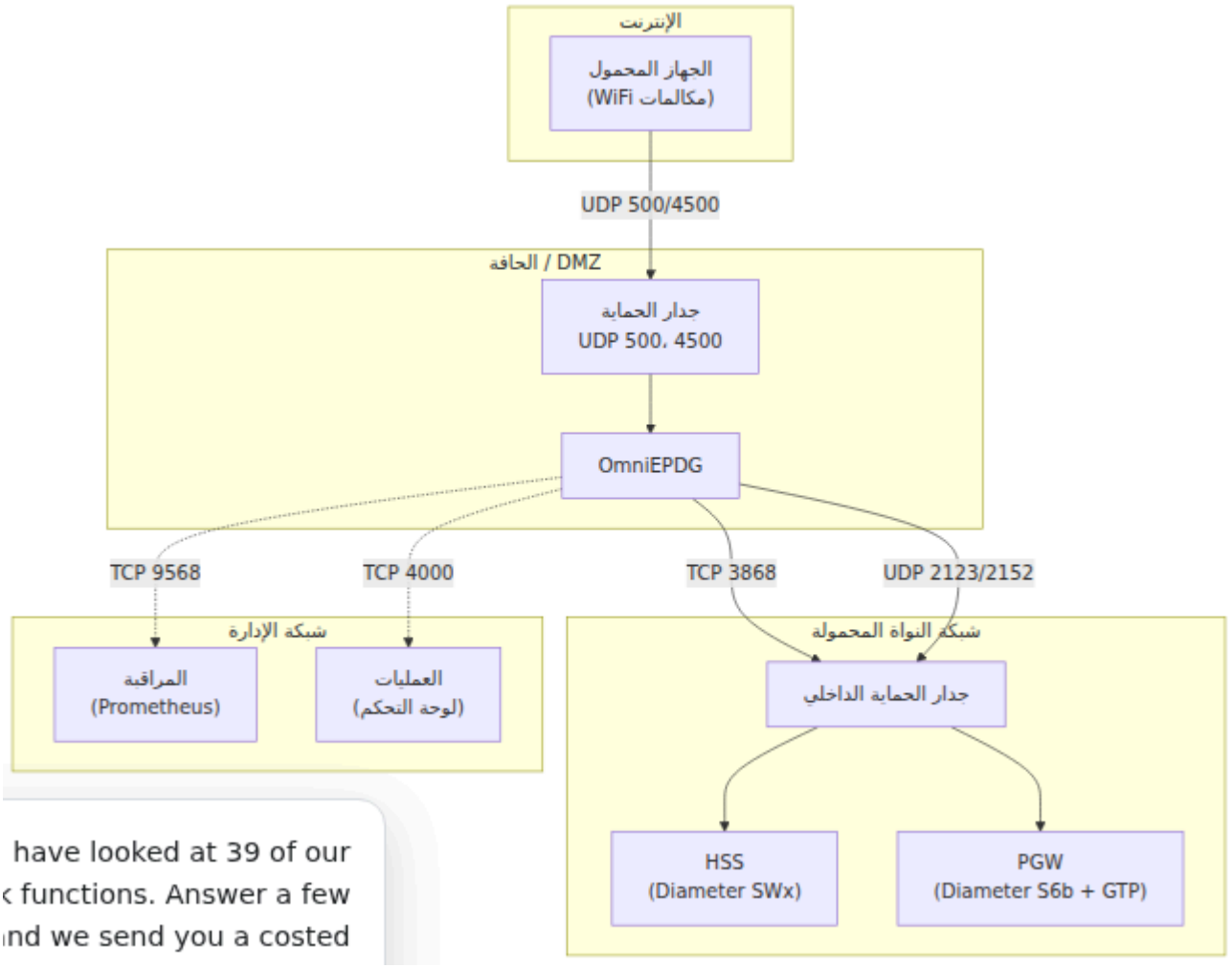
مثال:

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

يستخدم هذا المجال في:

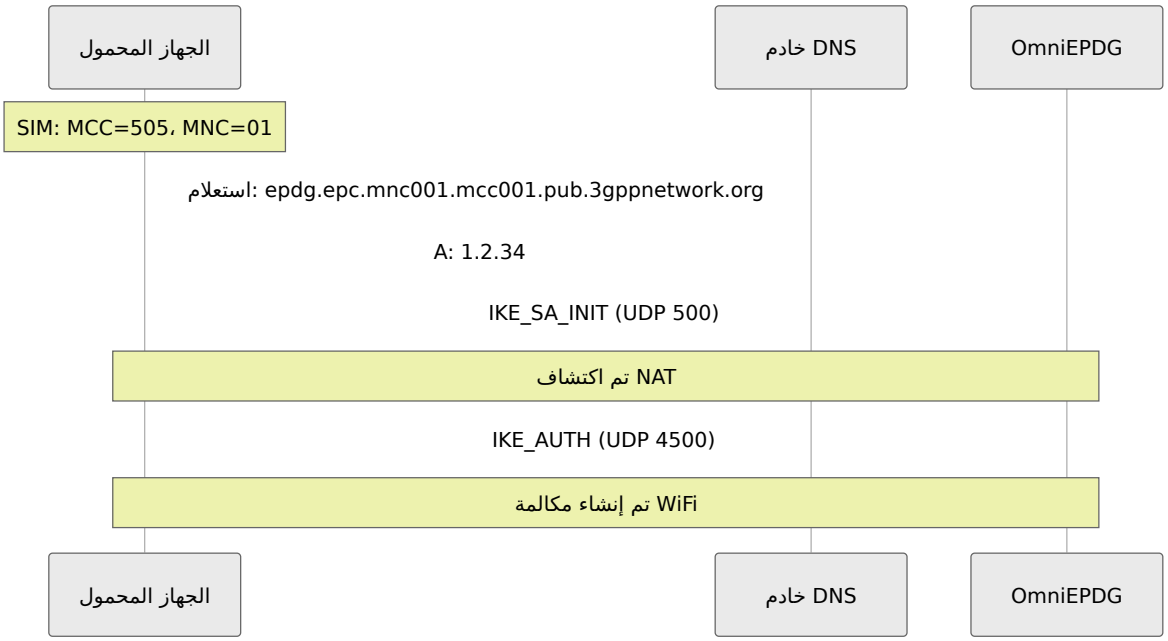
- NAI (معرف الوصول إلى الشبكة) المرسل بواسطة UE خلال المصادقة
- AVPs Diameter Origin-Realm و Destination-Realm
- قرارات توجيه Diameter

هندسة الشبكة



تدفق بحث DNS

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



قائمة التحقق

متطلبات المواجهة للإنترنت

- [ ] 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
- [ ] شهادة TLS مع SAN مطابق مثبتة

متطلبات ش��كة النواة

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

متطلبات الإدارة

- [ ] الوصول إلى TCP 4000/443 من شبكة العمليات
- [ ] الوصول إلى TCP 9568 من بنية المراقبة

المراجع

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

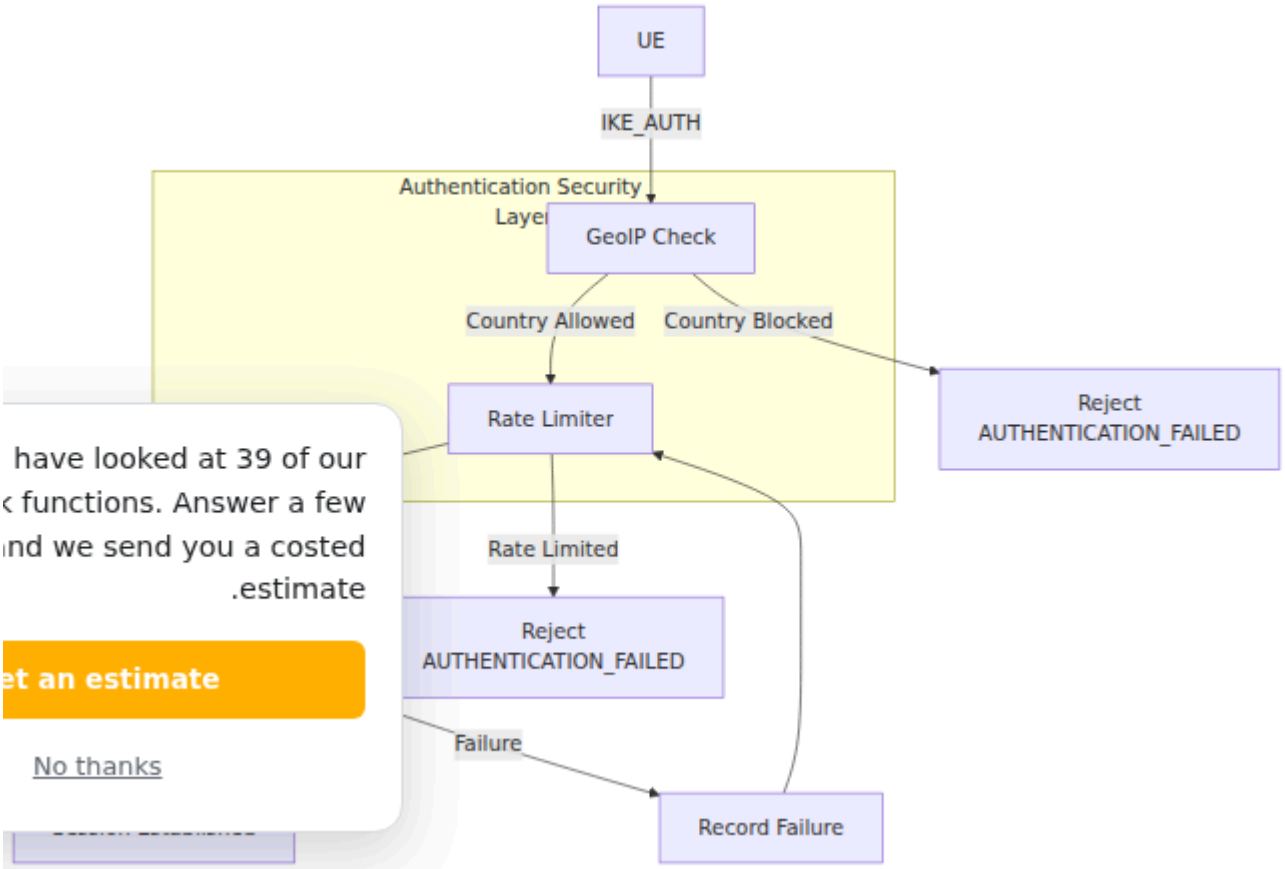
أمان المصادقة في OmniEPDG

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
- تحديد معدل المصادقة
- حظر الدول باستخدام GeoIP
- تدفق الأمان
- المقاييس
- استكشاف الأخطاء وإصلاحها

نظرة عامة



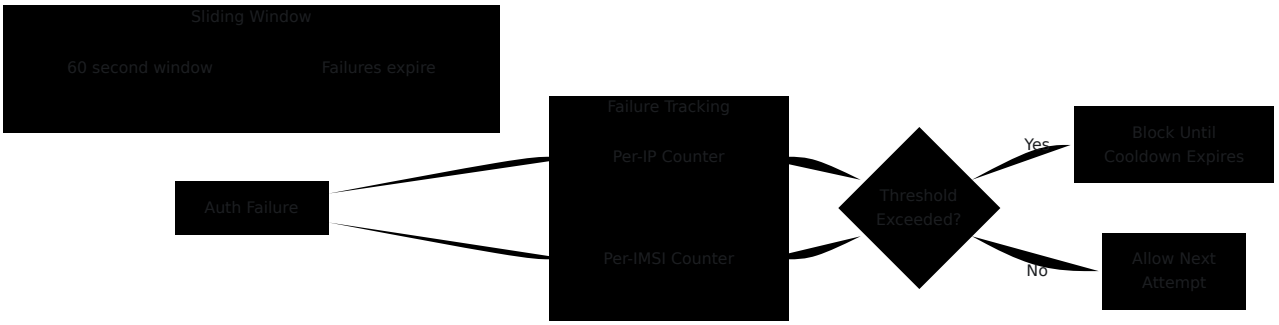
تقوم OmniEPDG بإجراء فحوصات الأمان في بداية تبادل IKE_AUTH، قبل العمليات التشفيرية المكلفة:

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

تحديد معدل المصادقة

يعمل تحديد المعدل على حماية 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 المنزلقة**:

- يتم تسجيل كل محاولة فاشلة مع طابع زمني
- يتم انتهاء صلاحية المحاولات الأقدم من النافذة المحددة تلقائيًا
- عندما تتجاوز الفشل في النافذة العتبة، يتم حظر المصدر
- تنتهي الحظر بعد فترة التهدئة المحددة

تتبع مزدوج

يتم فرض حدين مستقلين في وقت واحد:

نوع التتبع	الغرض	العتبة الافتراضية	الحظر الافتراضي
Per-IP	يلتقط ماسحات المنافذ والهجمات الموزعة من مصادر فردية	10 / فشل دقيقة	5 دقائق
Per-IMSI	يلتقط الهجمات المستهدفة على المشتركين المحددين	5 / فشل دقيقة	10 دقائق

يجب أن تمر كلت�ا الفحوصات حتى تستمر محاولة المصادقة. إذا تم تجاوز أي من العتبات، يتم رفض المحاولة.

التكوين

```
config :omniepdg,
  # تحديد معدل لكل IP
  auth_rate_limit_per_ip: 10,           # الحد الأقصى للفشل 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 معدل لكل IMSI
  auth_rate_limit_per_imsi: 5,            # الحد الأقصى للفشل 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 Per-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 الحظر.
`auth_rate_limit_ip_window_ms`	عدد صحيح	لا	`60000`	حجم النافذة المنزلقة بالمللي ثانية لعد الفشل في الفشل. IP الأقدم من ذلك لا يتم احتسابه.
`auth_rate_limit_ip_block_ms`	عدد صحيح	لا	`300000`	مدة الحظر بالمللي ثانية لعنوان IP بعد تجاوز العتبة. الافتراضي

الوصف	الافتراضي	مطلوب	النوع	المعلمة
هو 5 دقائق.				

معلمات Per-IMSI

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`auth_rate_limit_per_imsi`	عدد صحيح	لا	`5`	الحد الأقصى لمحاولات المصادقة الفاشلة المسموح بها لمعدل واحد IMSI خلال فترة النافذة قبل الحظر. أقل من Per-IP لالتقاط الهجمات المستهدفة.
`auth_rate_limit_imsi_window_ms`	عدد صحيح	لا	`60000`	حجم النافذة المنزلقة بالمللي ثانية لعد الفشل في IMSI.
`auth_rate_limit_imsi_block_ms`	عدد صحيح	لا	`600000`	مدة الحظر بالمللي ثانية لمعدل IMSI بعد تجاوز العتبة. الافتراضي هو 10

الوصف	الافتراضي	مطلوب	النوع	المعلمة
دقائق أطول من) IP حظر لحماية المشتركين المحددين).				

السلوك عند النجاح

عند نجاح المصادقة، يقوم محدد المعدل بمسح جميع سجلات الفشل لذلك الزوج من IP/IMSI. وهذا يسمح للمستخد��ين الشرعيين الذين واجهوا فشلاً عابراً (مثل مشكلات الشبكة) بالتعافي دون أن يتم معاقبتهم بشكل دائم.

أمثلة على التكوينات

بيئة عالية الأمان

حدود صارمة للبيئات التي لديها تحمل منخفض لمحاولات الفشل:

```
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 فشل لكل IP أو 3 فشل لكل IMSI. خلال نافذة مدتها دقيقتان. تستمر الحظورات لمدة 15-30 دقيقة على التوالي.

حالة الاستخدام: نشرات المؤسسات، 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
```

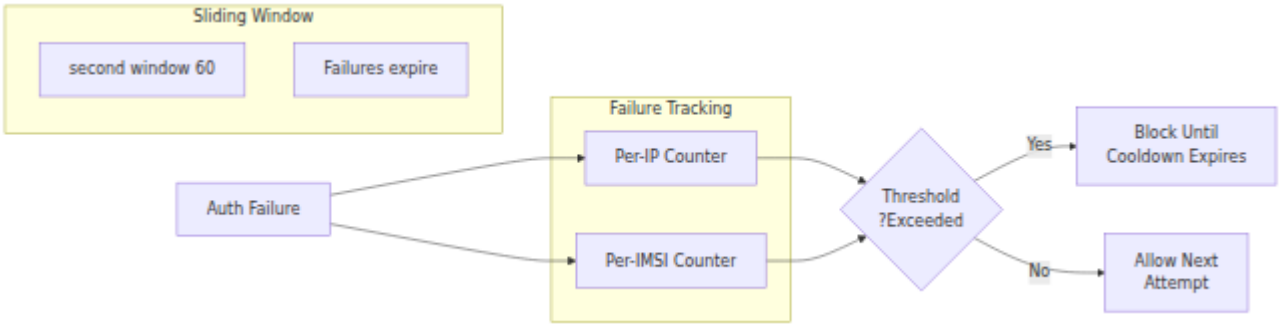
كيف يعمل: عتبات أعلى وحظورات أقصر تسمح بمزيد من المرونة في الاختبار.

حالة الاستخدام: بيئات التطوير، اختبار التكامل.

حظر الدول باستخدام GeoIP

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

نظرة عامة



قاعدة بيانات تحديد موقع IP

تستخدم OmniEPDG قاعدة بيانات **DB-IP IP-to-City Lite** (CC BY 4.0. انظر `priv/geoip/ATTRIBUTION.md`). إنها **غير** مرفوعة إلى git (~125 ميغابايت). بدلاً من ذلك، يتم `mix release` بتشغيل مهمة `geoip.fetch` كخطوة **تنزيلها في وقت البناء**. يقوم

يتم تنزيلها عند الطلب عبر اختصار) `mix test`.) بسبب ذلك:

- **يتم وضع علامة على كل جلسة تلقائيًا** مع الدولة، المدينة والإحداثيات التقريبية. هذه `/api/sessions` تعرض واجهة الويب ("عمود الموقع") واستجابة: `country_code`, `country_name`, `continent_code`, `geo_city`, `geo_latitude`, `geo_longitude`.
- يتحكم `geoip_enabled` فيما إذا كانت الاتصالات *محظورة* حسب الدولة. يتم **فقط** وضع العلامات بغض النظر عن هذه العلامة.

إلى `geoip_database_path` **استخدام قاعدة البيانات الخاصة بك (اختياري).** قم بتعيين أو قاعدة MaxMind GeoLite2 (`https://www.maxmind.com/en/geolite2/signup`) بيانات أخرى من DB-IP/MaxMind MMDB. إذا كانت الملف المحدد مفقودًا، يتم استخدام قا��دة البيانات المدمجة (المحمّلة). ملاحظة: لا تسمح اتفاقية استخدام MaxMind GeoLite2 بإعادة توزيعها داخل منتج، ولهذا السبب يتم استخدام DB-IP Lite (CC BY 4.0) بدلاً من ذلك.

لتحديث قاعدة البيانات يدويًا (تحديثات شهرية تنشر DB-IP):

```
mix geoip.fetch
```

التكوين

```
config :omniepdg,
  # حظر الاتصالات حسب الدولة (تحديد الموقع الجغرافي دائمًا مفعل)
  geoip_enabled: true,

  # اختياري: تجاوز قاعدة البيانات المدمجة بقاعدة بيانات MMDB
(دولة أو مدينة) الخاصة بك
  # 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	الوصف
`geoip_enabled`	Boolean	لا	`false`	تمكين أو تعطيل التحكم في الوصول القائم على GeoIP * (الحظر). عندما تكون `false`، يتم السماح بجميع عناوين IP، ولكن تظل الجلسات محددة جغرافيًا.
`geoip_database_path`	String	لا	قاعدة البيانات المدمجة `dbip-country-lite.mmdb`	مسار لقاعدة بيانات بتنسيق MMDB (دولة أو مدينة). يتراجع إلى قاعدة بيانات DB-IP المدمجة إذا لم يتم تعيينها أو كانت مفقودة.
`geoip_mode`	Atom	لا	`:whitelist`	وضع التحكم في الوصول: `:whitelist` (يسمح فقط بالدول المدرجة) أو `:blacklist` (يمنع الدول المدرجة، ويسمح بالباقي).
`geoip_countries`	List	لا	`[]`	قائمة رموز الدول ISO 3166-1

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				alpha-2. يعتمد التفسير على `geoip_mode`.
`geoip_allow_unknown`	Boolean	لا	انظر أدناه	السماح بالاتصالات من IPs التي لا يمكن تحديد موقعها (عناوين IP الخاصة، النطاقات غير المعروفة). الافتراضي هو `false` لوضع القائمة البيضاء، و`true` لوضع القائمة السوداء.
`geoip_fail_open`	Boolean	لا	`true`	السلوك ع��د فشل تحميل قاعدة بيانات GeoIP. عندما تكون `true`، يتم السماح بجميع الاتصالات (فشل مفتوح). عندما تكون `false`، يتم حظر جميع الاتصالات (فشل مغلق).

أوضاع التحكم في الوصول

WiFi) موصى به لمكالمات) وضع القائمة البيضاء

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 لمناطق الخدمة المرخصة لديهم.

وضع القائمة السوداء

يمنع الاتصالات من الدول المحددة. يتم السماح 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:

- نطاقات IP الخاصة (10.x.x.x، 192.168.x.x، إلخ.)
- كتل IP المخصصة حديثًا التي لم يتم إدراجها بعد في قاعدة البيانات
- نقاط خروج Tor وبعض خدمات VPN

تتحكم معلمة `geoip_allow_unknown` في السلوك:

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

لتجاوز الافتراضي:

```
config :omniepdg,
  geoip_mode: :whitelist,
  geoip_allow_unknown: true  # ال��ماح بالـ IPs غير المعروفة حتى في وضع القائمة البيضاء
```

تحديثات قاعدة البيانات

تقوم MaxMind بتحديث قاعدة بيانات GeoLite2 للتحديث. أسبوعيًا:

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

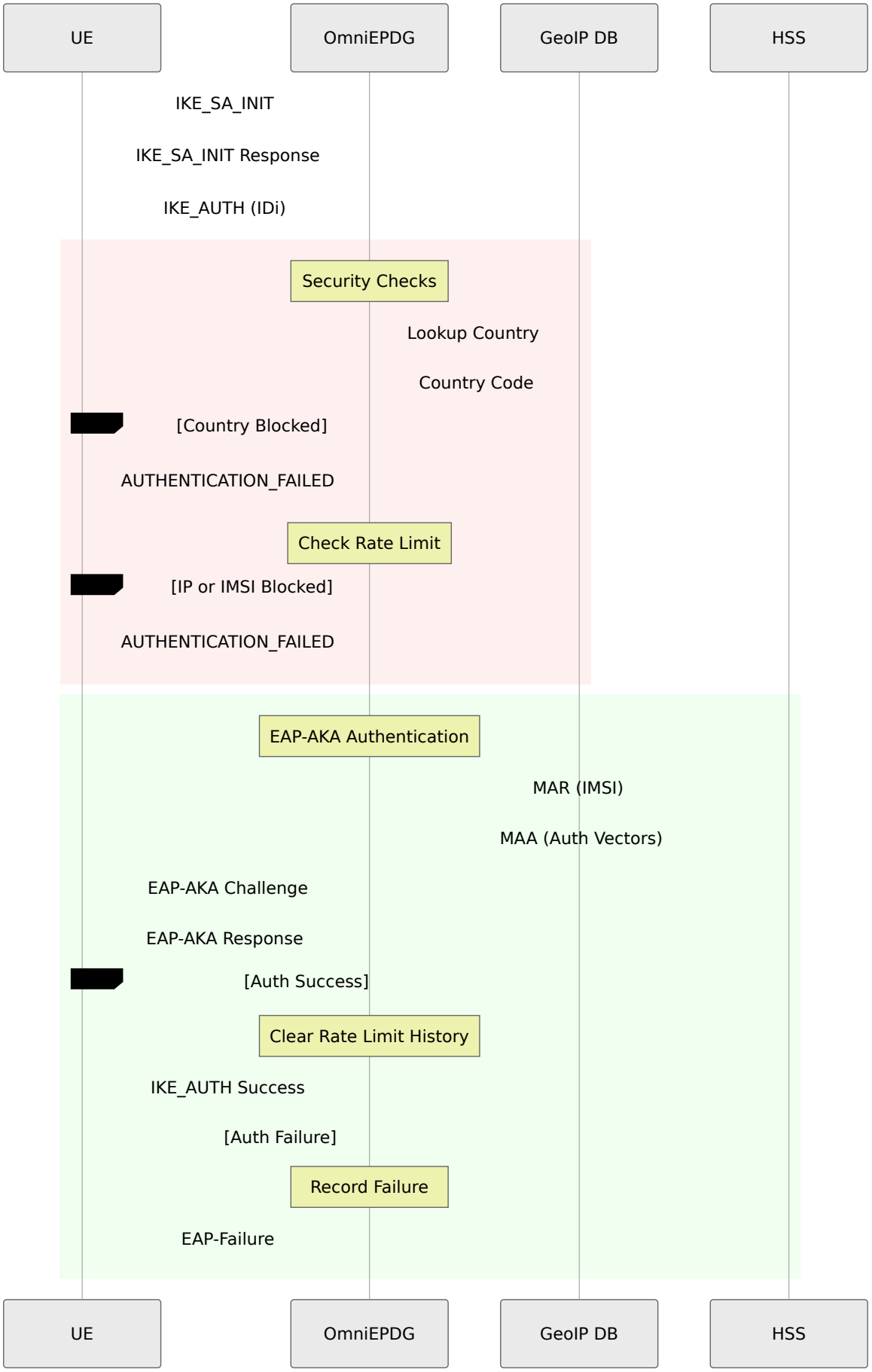
رموز الدول الشائعة

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
IKE_SA_INIT Response
IKE_AUTH (IDi)
Security Checks
Lookup Country
Country Code
[Country Blocked]
AUTHENTICATION_FAILED
Check Rate Limit
[IP or IMSI Blocked]
AUTHENTICATION_FAILED
EAP-AKA Authentication
MAR (IMSI)
MAA (Auth Vectors)
EAP-AKA Challenge
EAP-AKA Response
[Auth Success]
Clear Rate Limit History
IKE_AUTH Success
[Auth Failure]
Record Failure
EAP-Failure
UE
OmniEPDG
GeoIP DB
HSS

المقاييس

مقاييس تحديد المعدل

النوع: عداد **الوصف**: عدد محاولات `epdg_auth_rate_limited_count` **المقياس**: المصادقة المحظورة بسبب 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 معدل مرتفع
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:

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

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

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

استكشاف الأخطاء وإصلاحها

مشكلات تحديد المعدل

حظر المستخدمين الشرعيين

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

الأسباب المحتملة:

- أدخل المستخ��م بيانات اعتماد خاطئة عدة مرات
- تسببت مشكلات الشبكة في انتهاء وقت المصادقة التي تم احتسابها كفشل
- تم تعيين العتبات منخفضة جدًا للبيئة

الحل:

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

ارتفاع معدل 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. راجع عناوين IP المصدر في السجلات للأنماط
2. اعتبر تنفيذ قواعد جدار حماية على مستوى IP للمهاجمين المستمرين
3. تحقق من اتصال HSS إذا تأثر المستخدمون الشرعيون

مشكلات GeoIP

حظر جميع الاتصالات

الأعراض: لا يمكن لأي UE الاتصال بعد تمكين GeoIP

الأسباب ا��محتملة:

- لم يتم العثور على ملف قاعدة البيانات أو تالف
- رموز الدول غير صحيحة في التكوين
- `geoip_allow_unknown: false` يحظر عناوين IP الخاصة في بيئة المختبر

الحل:

1. تحقق من وجود ملف قاعدة البيانات في المسار المحدد
2. تحقق من أن رموز الدول صحيحة (حروف كبيرة، 2 حرف)
3. بالنسبة للمختبر/التطوير، قم بتعيين `geoip_allow_unknown: true`
4. تحقق من السجلات بحثًا عن تحذيرات تتعلق بـ GeoIP

لا يتم تحميلها GeoIP قاعدة بيانات

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

الأسباب المحتملة:

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

الحل:

1. تحقق 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

حظر 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

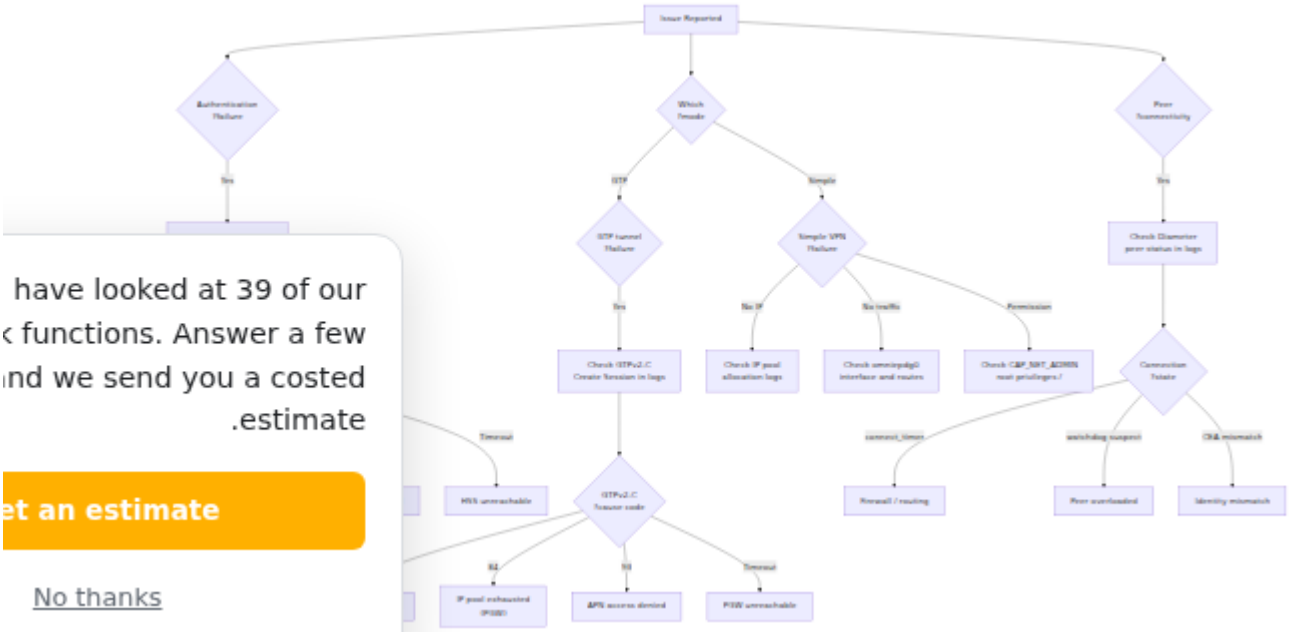
الحل:

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

استكشاف أخطاء وإصلاحها OmniEPDG

تغطي هذه الدليل المشكلات التشغيلية الشائعة وإجراءات التشخيص وخطوات الحل لـ OmniEPDG.

نظرة عامة على التشخيص



ملفات السجل

تكتب OmniEPDG السجلات إلى الدليل `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`	الأخطاء فقط	مسح سريع للمشكلات النشطة
`log/crash.log`	أعطال عملية OTP	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 قطع الاتصال بنظير Diameter

انتقالات حالة FSM UE:

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

أحداث انتهاء الوقت:

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

مشكلات الاتصال Diameter

فشل الاتصال بـ HSS (SWx)

الأعراض: لا يمكن لأي مشتركين ��لمصادقة. تظهر السجلات محاولات اتصال متكررة بـ HSS.

الأسباب المحتملة:

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

الحل:

1. تحقق من الاتصال الشبكي بعنوان IP و منفذ HSS
2. تأكد من أن `dia_swx_remote_ip` و `dia_swx_remote_port` يتطابقان 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 نطاق مؤهل يمكن حله ويتطابق مع ما يتوقعه HSS
5. تحقق من سجلات Diameter CER/CEA لعمليات التفاوض الفاشلة لـ HSS

فشل الاتصال بـ PGW (S6b)

الأعراض: تنجح المصادقة ولكن فشل إنشاء نفق GTP ص��ل أو لا تظهر AAR من PGW. السجلات عدم وجود حدث peer_up لـ S6b.

الأسباب المحتملة:

- OmniEPDG's S6b listener غير مكون للاتصال بـ PGW
- جدار ناري يمنع منفذ SCTP 3868 على عنوان الربط S6b الخاص بـ OmniEPDG
- `dia_s6b_local_ip` غير قابلة للوصول من PGW
- عدم تطابق Origin-Host أو Origin-Realm

الحل:

1. تأكد من أن PGW مكون للاتصال بـ OmniEPDG على `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 على المنفذ 3868 الواردة على عنوان S6b
4. تحقق من أن `dia_s6b_origin_host` و `dia_s6b_origin_realm` يتطابقان مع ما يتوقعه PGW

فشل مراقبة Diameter

الأعراض: تنقطع اتصالات Diameter التي تم إنشاؤها بشكل متقطع. تظهر السجلات انتقالات مراقبة إلى حالة SUSPECT أو DOWN.

الأسباب المحتملة:

- عدم استقرار مسار الشبكة أو فقدان الحزم
- نظير محمل بشكل زائد ولا يستجيب لـ DWR ضمن `dia_swx_watchdog_timer`
- تكوين مراقبة ع��واني (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 مفاوضة IKEv2

لا اقتراح مختار

الأعراض: يتم رفض IKE_SA_INIT الخاص بـ UE مع `NO_PROPOSAL_CHOSEN`؛ تظهر السجلات `exchange error: :no_proposal_chosen`. لا يتجاوز UE IKE_SA_INIT.

الأسباب المحتملة:

- يقدم UE فقط تحويلات تشفير لا تدعمها OmniEPDG.
- ماسح أو عميل غير مكون بشكل صحيح يستكشف المنافذ العامة.

الخلفية: تقبل OmniEPDG تشفير AES-GCM؛ AES-CBC و HMAC-SHA1، HMAC-SHA2 للنزاهة؛ **PRF-AES128-XCBC** PRFs؛ **AES-XCBC-96** و HMAC-SHA1، HMAC-SHA2 ومجموعات DH MODP/ECP/Curve25519/448. راجع الخوارزميات التشفيرية للحصول على القائمة الكاملة. تقدم بعض الهواتف (لا سيما بعض عملاء Samsung VoWiFi) فقط `AES-CBC-256 / AUTH_AES_XCBC_96 / PRF_AES128_XCBC / MODP-2048`، جميعها مدعومة.

الحل:

1. قم بتمكين تسجيل `:debug` وتفقد حدث `IKEv2 packet` لتحميل SA الخاص بـ UE. تسرد حقول `payloads[].proposals[]` التحويلات المعروضة بالضبط.
2. تأكد من أن التشفير / PRF / DH / النزاهة المعروضة تظهر كمدعومة في جداول الخوارزمية.
3. إذا كان هناك تحويل غير مدعوم حقًا مطلوب، قم برفع الأمر مع الهندسة.

تم حذف) الاتصال يتم إنشاؤه ثم ينقطع على الفور Child SA)

الأعراض: يكتمل IKE_AUTH، يتم إنشاء الجلسة لفترة وجيزة، ثم يرسل UE معلومات `DELETE` خلال ~100 مللي ثانية. لا تتدفق الوسائط. يتكرر في كل محاولة.

الأسباب المحتملة:

- لا تتطابق تحويلات Child SA (ESP) في الاستجابة مع ما قدمه UE، لذلك يقوم UE بإسقاط SA.
- لا يمكن معالجة البيانات من خلالها ESP خوارزمية نزاهة/تشفير.

الخلفية: تت��اوض OmniEPDG على Child SA ESP من الاقتراح المقدم من UE (بما في ذلك AES-CBC-128/192/256 و AES-XCBC-96) بدلاً من فرض مجموعة ثابتة. يتم رفض الاستجابة التي تختار تحويلًا لم يقدمه UE وفقًا لـ RFC 7296.

الحل:

1. في `:debug`، تحقق من سطر السجل `child SA proposal selected`. تظهر حقول `esp_offered` و `esp_encr` و `esp_integ` ما تم تقديمه وما تم اختياره.

2. تحقق من أن طول مفتاح تشفير ESP المختار يتطابق مع الشيفرة (يظهر عدم التطابق كـ `Bad key size` وحزمة تم إسقاطها).
3. تأكد من أن نزاهة ESP المعروضة من UE هي واحدة تدعمها OmniEPDG (راجع خوارزميات Child SA ESP).

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 مصادقة المشترك ولكن يتم رفضه أثناء تعيين الخادم. تظهر السجلات SWx SAA مع رمز النتيجة 5003.

الأسباب المحتملة:

- المشترك غير مصرح له بخدمة الاتصال عبر WiFi
- APN غير مسموح به لهذا المشترك
- قيود على ملف الاشتراك

الحل:

1. تحقق من ملف خدمة المشترك في HSS
2. تحقق 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 ��وقع 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. تحقق مما إذا كان الاتصال عبر WiFi مسموحًا بموجب اتفاقيات التجوال

انتهاء وقت 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 SWx أثناء الطلب
- HSS محمل بشكل زائد

الحل:

1. تحقق من استجابة HSS والحمولة
2. تحقق من أن نظير Diameter SWx في حالة OKAY (ليس SUSPECT أو DOWN)
3. تحقق من أن `dia_swx_transmit_timer` كافية لزمن الانتقال 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:

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

الخلفية: وفقًا لـ 3GPP TS 23.003، تشير بادئة هوية NAI إلى نوع المصادقة المتوقع:

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

تختار OmniEPDG تلقائيًا طريقة المصادقة بناءً على بادئة هوية UE. تستخدم معظم UEs للاتصال عبر WiFi `0` بادئة (EAP-AKA).

الحل:

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

عدم تطابق EAP-AKA RES

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 الفاسدة من HSS

الحل:

1. تحقق من أن بطاقة SIM صالحة وليست تالفة

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

فشل نفق GTP (وضع GTP فقط)

تم رفض إنشاء الجلسة بواسطة PGW

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

رموز الأسباب الشائعة والإجراءات:

رمز السبب	الاسم	الإجراء
78	APN مفقود أو غير معروف	تحقق من تكوين APN على PGW ويتطابق مع ملف تعريف المشترك
82	RAT مرفوض في	تحقق من أن سياسة PGW تسمح بنوع الوصول (3GPP غير) عبر WiFi
84	جميع العناوين الديناميكية مشغولة	قم بتوسيع PGW الخاصة بـ IP نفاد 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 مصرح له بـ
96	IMSI/IMEI غير معروف	تحقق من أن PGW المشترك غير معروف لـ ؛ S6b تم تفويضها جلسة
113	APN ازدحام	محمل؛ حاول مرة أخرى أو تحقق من سعة APN PGW
120	GTP-C ازدحام كيان	PGW محمل التحكم في

انتهاء وقت 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 على `gtpc_remote_ip`:`gtpc_remote_port`
- جدار ناري يمنع منفذ UDP 2123 بين OmniEPDG و PGW
- PGW محمل 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 OmniEPDG و PGW
3. تحقق من صحة GTPv2-C وسعة معالجة PGW

لا ينقل الحركة GTP-U نفق

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

الأسباب المحتملة:

- لم يتم تحميل وحدة نواة GTP-U
- عنوان IP لمقبس `gtp_u_kmod` لا يتطابق مع عنوان نقطة نهاية نفق GTP-U المعلن لـ PGW
- لم يتم تكوين التوجيه لجهاز نفق GTP
- جدار ناري يمنع منفذ UDP 2152 (GTP-U)

الحل:

1. تحقق من تحميل وحدة GTP في نواة Linux (`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 طرق عبر جهاز نفق GTP
5. تحقق من أن الجدار الناري يسمح بمنفذ UDP 2152 بين OmniEPDG و PGW

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:

- أو لا تعمل كجذر `CAP_NET_ADMIN` إلى قدرة OmniEPDG تفتقر عملية
- لم يتم تحميل وحدة نوا TUN/TAP
- تم إنشاء واجهة أخرى بالفعل باسم `omniepdg0`

الحل:

1. تحقق من أن وحدة نواة 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` بحثًا عن 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
- لا 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 أنه يتم إنهاء الجلسات بشكل صحيح `terminating`)
3. إذا كانت المجموعة ممتلئة حقًا، قم بتوسيعها باستخدام بادئة CIDR أكبر في `simple_vpn_pool_ipv4` (يتطلب إعادة تشغيل)
4. تحقق من وجود أعطال 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 لا تتدفق الحركة عبر واجهة TUN.

الأسباب المحتملة:

- لم يتم إضافة مسار المضيف لعنوان IP الخاص بالمشترك على `omniepdg0`
- لم يتم تمكين إعادة توجيه IP على مضيف OmniEPDG
- قواعد الجدار الناري تمنع الحركة على واجهة `omniepdg0`
- قواعد NAT/masquerade المفقودة لحركة المرور الصادرة من نطاق IP الخاص بالمشترك

الحل:

1. تحقق من وجود المسار المضيف (`ip route show` وابحث عن المسار /32 الخاص بالمشترك 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 المشتركين بحاجة إلى الوصول إلى الإنترنت، تحقق من تكوين NAT/masquerade لنطاق IP الخاص بالمشتركين (على سبيل المثال، `iptables -t nat -A POSTROUTING -s 10.45.0.0/16 -o <wan-interface> -j MASQUERADE`)

طرق قديمة بعد العطل

الأعراض: تبقى طرق المضيف لعنوان IP الخاص بالمشتركين 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 بدون إيقاف تشغيل سلس

الحل:

1. تحقق من `log/crash.log` بحثًا عن أعطال العمليات أثناء إنهاء الجلسة
2. قم بإزالة الطرق القديمة يدويًا (`ip route del <subscriber-ip>/32 dev omniepdg0`)
3. ستعيد إعادة تشغيل OmniEPDG 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:

- PGW لا يستجيب لطلب حذف الجلسة
- نظير Diameter لا يستجيب لـ STR أو ASR
- عدم اكتمال انتهاء الوقت المتسلسل بسبب تراكم عدة انتهاء وقت

الحل:

1. تحقق من السجلات بحثًا عن رسائل انتهاء الوقت في الحالة ذات الصلة
2. تحقق من الاتصال بـ HSS و PGW
3. ويواصل الخطوة التالية لإنهاء الجلسة أو ينهيها. إذا لم FSM بعد 10 ثوانٍ، يجب أن ينتهي يحدث ذلك، تحقق من الأحداث غير المتوقعة المسجلة كـ `Unexpected call event`

سياقات PDP GTP-U اليتيمة

الأعراض: تبقى إدخالات نفق GTP-U في النواة بعد إنهاء الجلسات. يظهر `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` بحثًا عن أعطال العمليات أثناء إنهاء الجلسة
2. تحاول وظيفة `terminate/3` الخاصة بـ FSM تنظيف سياق PDP. إذا تم قتل FSM قد يكون قد تم تخطي التنظيف، (على سبيل المثال، إعادة تشغيل المشرف)
3. ستعيد إعادة تشغيل OmniEPDG إنشاء مقبس GTP-U وت□□ السياقات القديمة

OmniEPDG ويب هوكس

يمكن لـ OmniEPDG إرسال ويب هوكس صادرة لأحداث دورة حياة جلسات المشتركين. عندما يقوم مشترك بالاتصال أو الفصل، يرسل OmniEPDG طلب HTTP `POST` مع جسم JSON إلى كل نقطة نهاية تم تكوينها. استخدم ويب هوكس لتغذية نظام الفوترة، أو خدمة الحضور، أو خط أنابيب التحليلات في الوقت الحقيقي تقريبًا.

الويب هوكس معطلة بشكل افتراضي. راجع تكوين الويب هوكس لمعلمات التكوين.

جدول المحتويات

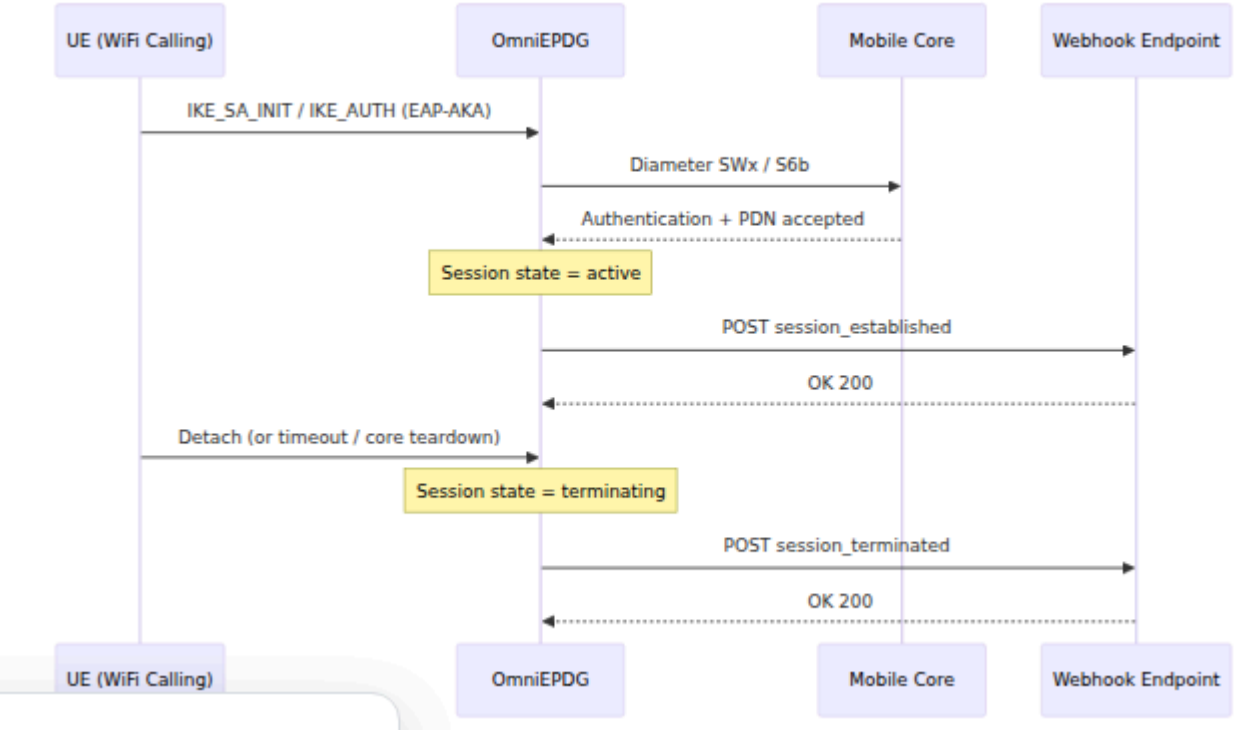
- نظرة عامة
- الأحداث
- نموذج التسليم
- مخطط الحمولة
- أمثلة على الحمولة
- متطلبات المستلم
- استكشاف الأخطاء وإصلاحها

نظرة عامة

يتتبع OmniEPDG كل جلسة مشترك باستخدام آلة حالة. ينتج عن انتقالين ويب هوك:

- تصل الجلسة إلى حالة `active` بعد اتصال ناجح.
- تصل الجلسة إلى حالة `terminating` بعد الفصل.

يوضح المخطط التالي مكان إرسال كل ويب هوك في دورة حياة الجلسة.



الأحداث

الحدث	الزناد	الوصف
`session_established`	اتصال ناجح	هذا الحدث عندما يتم مصادقة OmniEPDG يرسل جاهزًا. الجلسة جاهزة PDN المشترك وتكون اتصال لنقل البيانات.
`session_terminated`	فصل	هذا الحدث عندما يتم إنهاء OmniEPDG يرسل أو انتهاء مهلة، UE جلسة قائمة. السبب هو فصل عدم النشاط، أو إنهاء بدأه النواة.

يرسل OmniEPDG `session_terminated` فقط للجلسات التي وصلت إلى حالة `active`. لا جاهزًا ويب هوك PDN ينتج عن اتصال يفشل قبل أن يصبح اتصال.

راجع تكوين OmniEPDG. للتحكم في الأحداث التي يرسلها `events` قم بتعيين معلمة التكوين الويب هوكس.

نموذج التسليم

يوصل OmniEPDG الويب هوكس بنموذج "إطلاق وانسَ". يتم تشغيل كل تسليم على مهمة خلفية تحت الإشراف. لا تعيق عملية التسليم أو تؤخر آلة حالة الجلسة، ولا تؤثر نقطة نهاية بطيئة أو غير متاحة على معالجة المكالمات.

لاحظ الخصائص التالية للتسليم:

- يرسل OmniEPDG طلب `POST` واحد لكل نقطة نهاية تم تكوينها، لكل حدث.
- لا يعيد OmniEPDG محاولة تسليم فاشل. يتم تسجيل التسليم الفاشل وإسقاطه.
- لا يضمن OmniEPDG تر��يب الأحداث بين الحدثين. صمم المستلم للتعامل مع الأحداث حسب حقل `timestamp`.
- يقبل OmniEPDG أي استجابة HTTP `2x` كنجاح. يسجل تحذيرًا لخطأ الاتصال أو استجابة غير `2xx`.
- لا يتحقق OmniEPDG من شهادة TLS لنقطة نهاية `https`. استخدم مسار شبكة موثوق به إلى المستلم.

مخطط الحمولة

يحتوي على الحقول التالية JSON كل جسم ويب هوك هو كائن.

الحقل	النوع	الوصف
`event`	String	اسم الحدث: `session_established` أو `session_terminated`.
`timestamp`	String	وقت الحدث بتنسيق ISO 8601 (UTC).
`session_id`	String	معرف الجلسة الداخلي لـ OmniEPDG.
`imsi`	String	IMSI المشترك.
`apn`	String أو null	اسم نقطة الوصول لاتصال PDN.
`pdn_type`	String	نوع PDN: `ipv4`، `ipv6`، أو `ipv4v6`.
`ue_ipv4`	String أو null	عنوان IPv4 المخصص لـ UE.
`ue_ipv6`	String أو null	عنوان IPv6 المخصص لـ UE.
`peer_ip`	String أو null	عنوان IP العام لـ UE (نقطة وصول WiFi).
`geoip`	Object أو null	الموقع الجغراف❓❓ لـ `peer_ip`. راجع كائن GeoIP. يكون `null` عندما لا يمكن تحديد الموقع.
`handover`	Boolean	`true` إذا تم إنشاء الجلسة كتحويل من LTE إلى WiFi.
`bytes_in`	Integer	عدد البايتات في الاتجاه الصاعد للجلسة في وقت الحدث.
`bytes_out`	Integer	عدد البايتات في الاتجاه النازل للجلسة في وقت الحدث.
`metadata`	Object	كائن يحتوي على سياق الحدث الإضافي. يكون فارغًا لمعظم الأحداث.

لأنه لم يتم، `session_established` تساوي `0` لحدث `bytes_out` و `bytes_in` تكون حقول نقل أي بيانات بعد.

كائن GeoIP

يعلق OmniEPDG في وقت الاتصال. يتم استخدام قاعدة UE العام لـ IP على كل جلسة بموقع GeoIP المجمعة، ويحدث ذلك بغض النظر عما إذا كان التحكم في الوصول إلى DB-IP بيانات `longitude` و `latitude` و `city` هذا التعليق. تكون الحقول `geoip` مفعلًا. يحمل حقل موجودة فقط مع قاعدة بيانات على مستوى المدينة.

الحقل	النوع	الوصف
`country_code`	String أو null	رمز الدولة ISO 3166-1 alpha-2 (على سبيل المثال `AU`).
`country_name`	String أو null	اسم الدولة.
`continent_code`	String أو null	رمز القارة المكون من حرفين (على سبيل المثال `OC`).
`city`	String أو null	اسم المدينة. موجود فقط مع قاعدة بيانات على مستوى المدينة.
`latitude`	Number أو null	خط العرض التقريبي. موجود فقط مع قاعدة بيانات على مستوى المدينة.
`longitude`	Number أو null	خط الطول التقريبي. موجود فقط مع قاعدة بيانات على مستوى المدينة.

أمثلة على الحمولة

session_established


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

session_terminated

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

متطلبات المستلم

قم ببناء مستلم الويب هوك لتلبية هذه المتطلبات:

- قبول طلب HTTP `POST` مع جسم `Content-Type: application/json`.
- إرجاع استجابة `2xx` بمجرد قبول الحدث. لا تحتفظ بالاتصال مفتوحًا للمعالجة اللاحقة.
- مطابقة الأحداث مع الجلسات باستخدام حقل `session_id`.
- التعامل مع حدث مكرر. يمكن أن تتسبب حالة الشبكة في إرسال OmniEPDG لنفس الحدث أكثر من مرة.
- ترتيب الأحداث حسب حقل `timestamp`، وليس حسب ترتيب الوصول.

استكشاف الأخطاء وإصلاحها

لا تصل الويب هوكس

الأعراض: لا يتلقى المستلم أي طلبات بعد الاتصال أو الفصل.

الأسباب المحتملة:

- الويب هوكس معطلة (`enabled: false`).
- الحدث ليس في قائمة `events`.
- عنوان URL لنقطة النهاية خاطئ أو غير قابل للوصول من مضيف OmniEPDG.
- يمنع جدار ناري الاتصال الصادر إلى نقطة النهاية.

الحل:

1. تأكد من `enabled: true` في تكوين الويب هوكس.
2. تأكد من أن اسم الحدث موجود في قائمة `events`.
3. تأكد من أن عنوان URL لنقطة النهاية صحيح وقابل للوصول من مضيف OmniEPDG.
4. تحقق من سجلات OmniEPDG للحصول على تحذير تسليم ويب هوك.

تصل فقط session_established، وليس session_terminated

الأعراض: يتلقى المستلم أحداث الاتصال ولكن لا يتلقى أحداث الفصل.

الأسباب المحتملة:

- `session_terminated` ليس في قائمة `events`.
- لذا لم يكن هناك حدث ف��ل ، `active` لم تصل الجلسات أبدًا إلى حالة.

الحل:

1. أضف `:session_terminated` إلى قائمة `events`.
2. تأكد من أن الجلسات تكمل اتصالًا ناجحًا قبل أن تنتهي.

يتم تسجيل التسليمات على أنها فاشلة

الأعراض: تظهر سجلات OmniEPDG تحذير تسليم ويب هوك.

الأسباب المحتملة:

- يعيد المستلم استجابة غير `2xx`.
- المستلم بطيء أو غير متاح.
- يستخدم عنوان URL لنقطة النهاية مضيفًا لا يتم حله.

الحل:

1. تأكد من أن المستلم يعيد استجابة `2xx`.
2. تأكد من أن المستلم يستجيب بسرعة، لأن OmniEPDG لا يعيد المحاولة.
3. تأكد من أن مضيف نقطة النهاية يتم حله من مضيف OmniEPDG.