

OmniEPDG دليل تشغيل

WiFi التي تتيح مكالمات الصوت عبر (ePDG) هي بوابة بيانات الحزمة المتطورة OmniEPDG غير الموثوقة باستخدام WiFi تقوم بالتحقق من هوية المشتركين المتنقلين عبر شبكات (VoWiFi). إلى GTP وأنفاق HSS إلى Diameter وتربطهم بشبكة النواة المتنقلة من خلال إشارة EAP-AKA، (PGW) بوابة الحزمة.

OmniEPDG v0.1.0	Licensed to: Omnitouch © 2020 Omnitouch
Dashboard	UE Sessions 1 Session 1 Active 8.53 KB / 12.17 KB
Sessions	
Diameter	
Logs	
Docs	
Resources	
Configuration	
License	
IMSI	UE IP 100.64.34.84 SOURCE 10.7.7.50:14500 APN * STATUS Active DURATION 4m 50s TRAFFIC 8.53 KB / 12.17 KB
SESSION	NETWORK & TIMING TRAFFIC
IMSI	DNS 10.4.10.195, 10.4.10.196 Bytes In (UL) 8.53 KB
NAI	P-CSCF 10.4.12.165 Bytes Out (DL) 12.17 KB
UE IP	100.64.34.84 Connected 2026-03-08 21:39:16 Packets In 63
Source	10.7.7.50:14500 Last Activity 2026-03-08 21:41:48 Packets Out 63
APN	* Duration 4m 50s
Child SA SPI	0x4E54838A

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

وضعين تشغيليين OmniEPDG يدعم

- GTPv2-C عبر PGW عبر GPP نفق كامل متوافق مع 3 - (افتراضي) **GTP** و **GTP-U**
- Linux، لنظام TUN مدمجة وواجهة IP بسيط - خروج محلي مع مجموعة **VPN** وضع PGW بدون الحاجة إلى

الوثائق

التكوين والعمليات

- **الهندسة المعمارية وتدفقات المكالمات** - هندسة النظام، واجهات البروتوكول، ومخططات تسلسل الرسائل لكلا الوضعين، UE آلات الحالة
- Diameter وGTPv2-C وGTP-U وVPN **مرجع التكوين** - وثائق كاملة للمعلمات لـ البسيط والتسجيل
- Diameter، **لوحة التحكم** - واجهة مراقبة قائمة على الويب للجلسات، ونظراء والسجلات

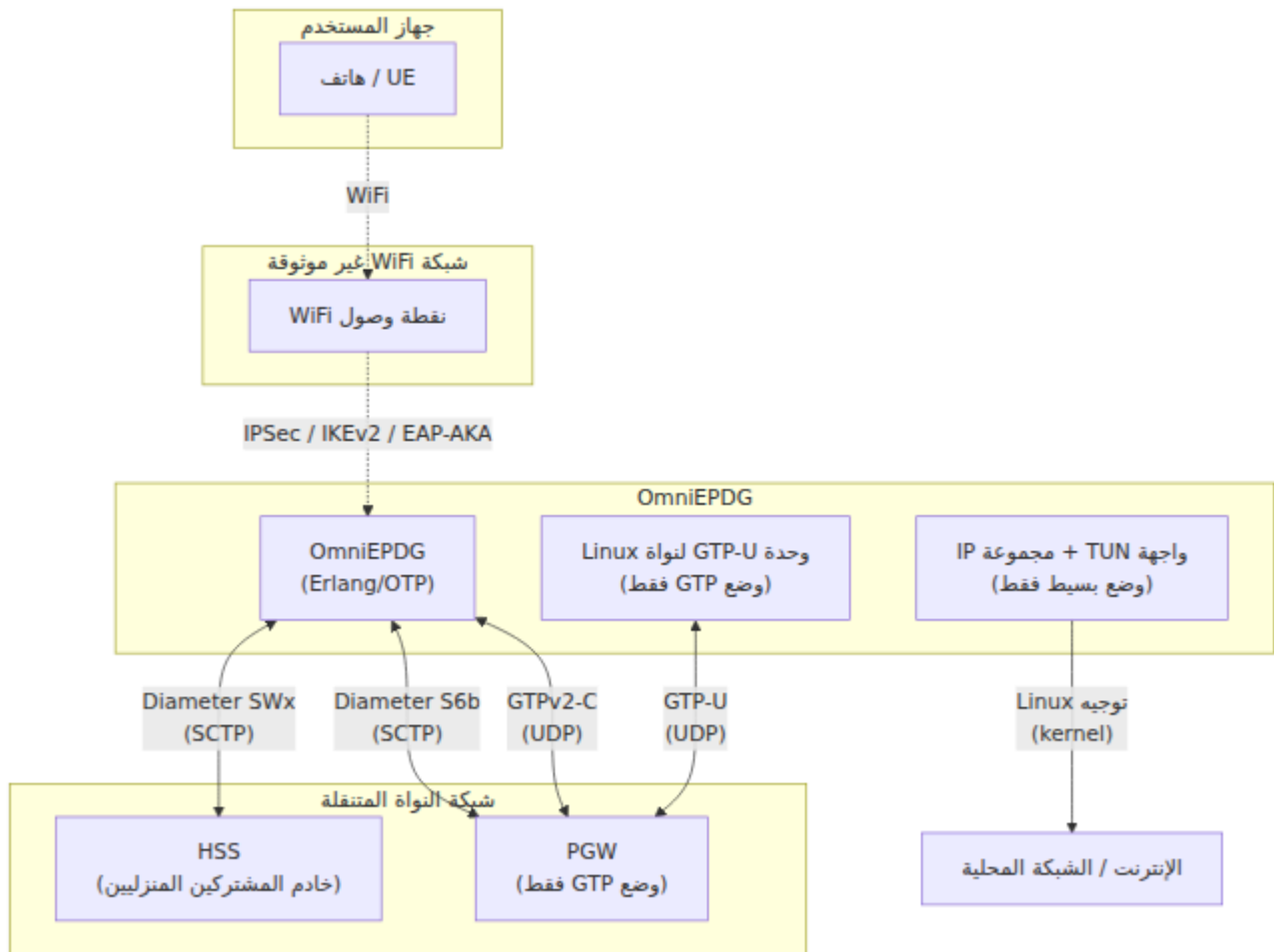
الأمان

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

المراقبة واستكشاف الأخطاء وإصلاحها

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

الأوضاع التشغيلية



GTP وضع

باستخدام PGW بنفق جميع حركة مرور المشتركين عبر OmniEPDG الوضع الافتراضي. يقوم للطائرة المستخدمة. هذا (Linux عبر وحدة نواة) GTP-U لل♦♦حكم في الجلسة و GTPv2-C الحالية EPC ومناسب لنشر شركات الاتصالات مع بنية GPP متوافق تمامًا مع 3.

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

البنية التحتية المطلوبة: HSS, PGW

بسيط VPN وضع

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

HSS إلى Diameter SWx لا تزال المصادقة تحدث عبر GTP.

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

(PGW لا حاجة إلى) فقط HSS : **البنية التحتية المطلوبة**

مما يقلل من HSS، بتجاوز طلب/إجابة تعيين الخادم skip_sar **تحسين اختياري**: يقوم العلم المبدوءة HSS تخدم المشترك وإجراءات ePDG لن تتبع أي HSS وقت إعداد الاتصال. هذا يعني أن (إلغاء التسجيل، دفع الملف الشخصي) لن تعمل. مناسب للنشر الخاص بدون متطلبات تجوال

مقارنة الأوضاع

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

واجهات البروتوكول

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

الميزات

الوظائف الأساسية

- HSS عبر EAP-AKA مصادقة كاملة للمشاركين باستخدام - EAP-AKA مصادقة
- ePDG و UE بين IKEv2 نفق آمن يعتمد على - IPSec إدارة نفق
- بسيط VPN أو خروج محلي مع PGW إلى GTP وضعين تشغيلين مزدوجين - نفق
- مستقلة لكل مشترك لإدارة دورة حياة الجلسة FSM Erlang - UE آلات حالة لكل
- (GTP وضع) IPv4v6 و IPv6 و IPv4 من نوع PDP دعم مزدوج للأنظمة - عناوين

GTP ميزات وضع

- Linux عبر وحدة نواة GTP-U ونفق GTPv2-C إنشاء جلسة - GTP إنشاء نفق

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

بسيط VPN ميزات وضع

- IMSI مع تتبع لكل CIDR بناءً على IPv4 محلية - تخصيص عنوان IP مجموعة
- مع طرق مضيف (tun_epdg) قياسي Linux لنظام TUN جهاز - **TUN توجيه واجهة** لكل UE
- PCO عبر UEs قابلة للتكوين مقدمة إلى DNS خوادم - **DNS تكوين**
- لتسريع إعداد الاتصال HSS **اختياري** - تجاوز تسجيل **SAR تخطي**

ميزات الأمان

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

❖❖ HSS (SWx Diameter) كامل

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

(فقط GTP وضع) PGW تكامل

Diameter S6b:

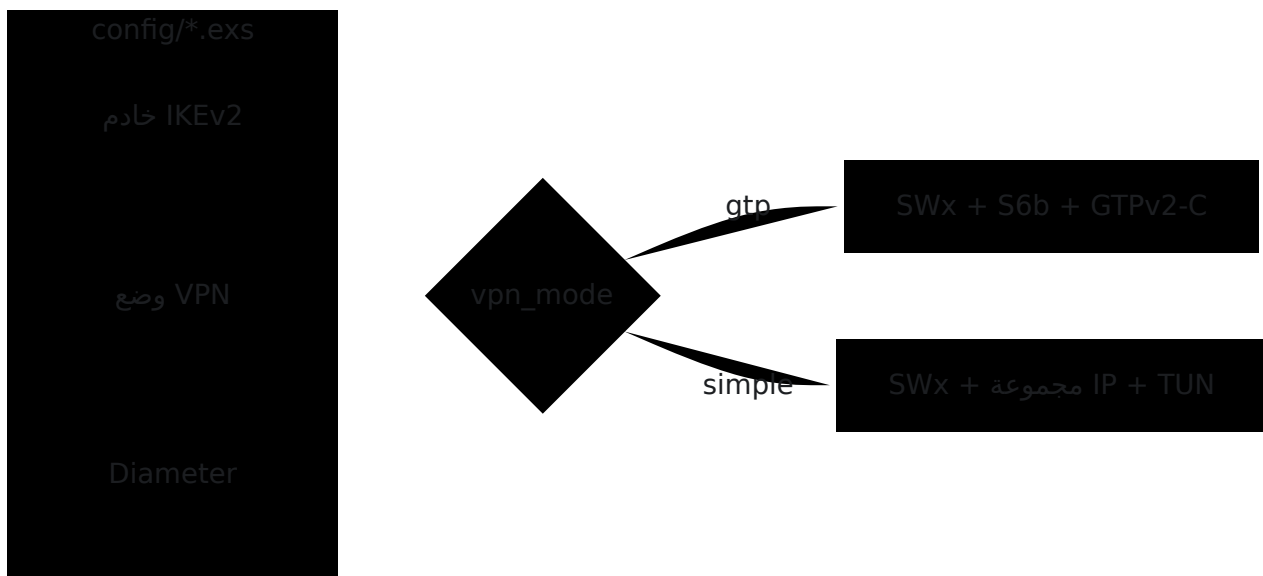
- PGW تفويض جلسات - AA (AAR/AAA) طلب/إجابة
- PGW إنهاء جلسات - (STR/STA) طلب/إجابة إنهاء الجلسة
- إعادة تفويض الجلسات النشطة - (RAR/RAA) طلب/إجابة إعادة التفويض
- إنهاء الجلسات بالقوة - (ASR/ASA) طلب/إجابة إنهاء الجلسة

GTPv2-C S2b:

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

ال??دء السريع

هيكل التكوين



بين `vpn_mode` أو عبر متغيرات البيئة. يحدد معلمة `config/runtime.exs` يتم التكوين في البسيط. راجع مرجع التكوين للحصول على وثائق كاملة للمعاملات VPN و GTP أوضاع.

GTP وضع) العناوين الشبكية النموذجية

المكون	IP عنوان	المنفذ	الملاحظات
OmniEPDG (GTP-U)	10.74.0.11	-	GTP-U نقطة نهاية نفق
OmniEPDG (Diameter S6b)	10.74.0.12	3868	Diameter S6b مستمع
HSS	10.74.0.21	3868	Diameter SWx نظير
PGW	10.74.0.23	2123	GTPv2-C وS6b نظير

بسيط VPN وضع) العناوين الشبكية النموذجية

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

GPP مواصفات 3

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

الوثائق حسب الدور

مشغلو الشبكات:

- ابدأ ب **الهندسة المعمارية وتدفقات المكالمات** لفهم النظام وكلا الوضعين التشغيليين
- راجع **مرجع التكوين** للحصول على معلومات النشر
- GeolP راجع **دليل الأمان** لتكوين تحديد المعدل وحظر

4. Prometheus قم بإعداد المراقبة باستخدام **مرجع القياسات** لتكامل
5. احتفظ بدليل **استكشاف الأخطاء** متاحًا للعمليات

:مُدمجو الأنظمة

1. راجع **الهندسة المعمارية وتدفقات المكالمات** للحصول على تفاصيل الواجهة وآلات الحالة
2. استخدم **مرجع التكوين** لإعداد الاتصال بالنظراء
3. قم بتكوين التنبيهات باستخدام **مرجع القياسات**
4. أعلاه للامتنال للبروتوكول GPP ارجع إلى جدول مواصفات 3

OmniEPDG دليل عمليات

تمكّن من إجراء (ePDG) GPP هو بوابة بيانات حزمة مطورة متوافقة مع 3 OmniEPDG بشبكة الجوال الأساسية. WiFi من خلال ربط الوصول غير الموثوق لشبكة WiFi المكالمات عبر IP. بسيط للاختراق المحلي لعنوان **VPN** ووضع PGW لنفق **GTP** يدعم وضعين تشغيلين: **وضع**

روابط سريعة

التكوين والنشر

- المطلوبة للنشر DNS **متطلبات الشبكة** - منافذ جدار الحماية وإدخالات
- وجميع VPN ووضع Diameter و IKEv2 **مرجع التكوين** - وثائق كاملة للمعلومات ل إعدادات وقت التشغيل
- نظرة عامة على العمارة** - هيكل النظام، تدفقات المكالمات، آلات الحالة، ومراجع البروتوكول

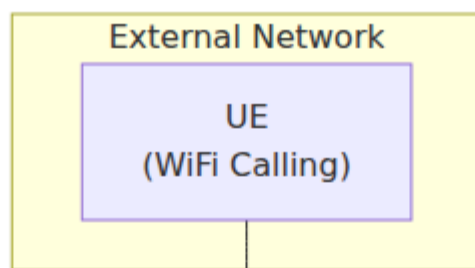
العمليات والمراقبة

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

الأمان

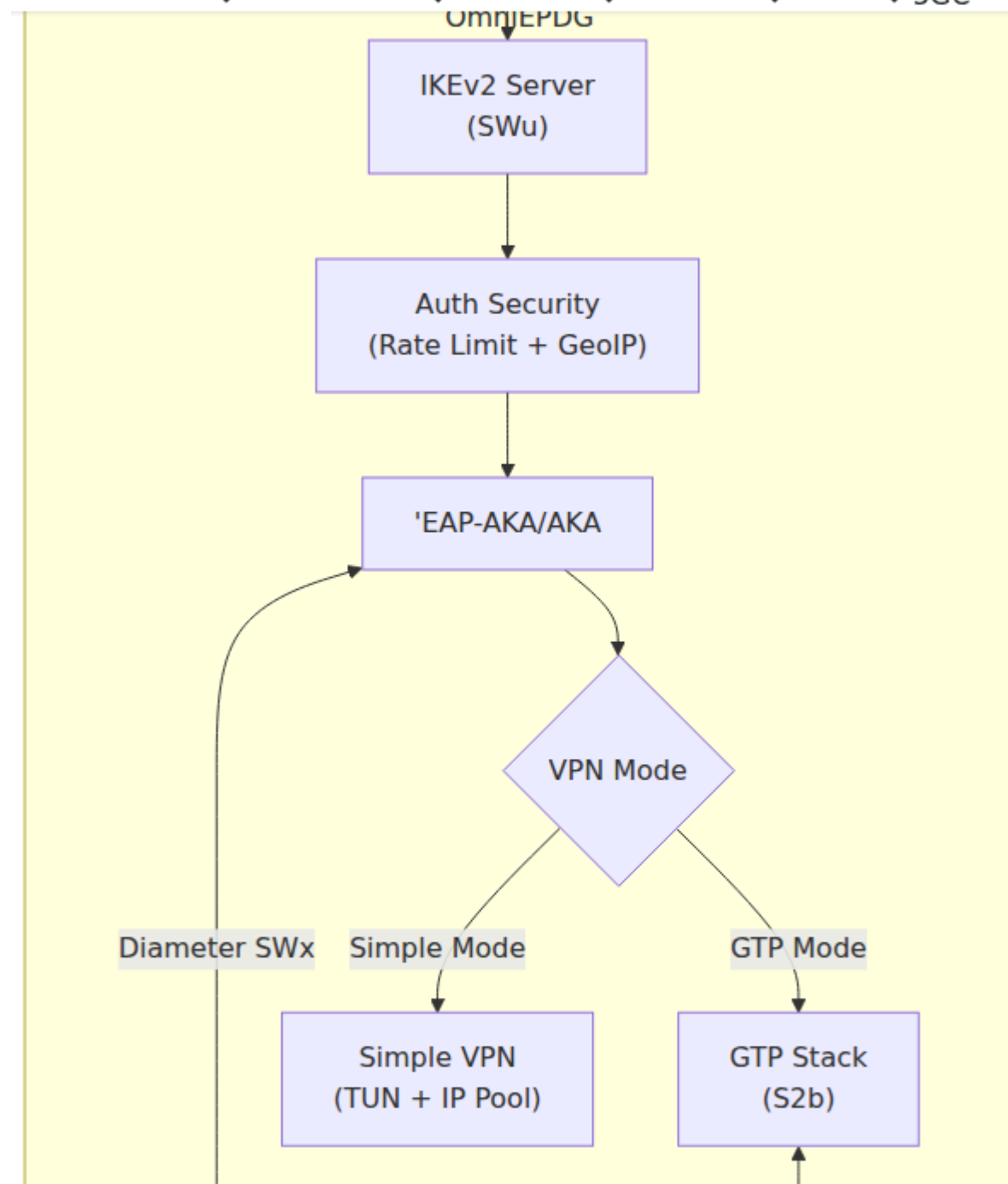
- GeoIP **أمان المصادقة** - تحديد المعدل وحظر البلدان باستخدام

نظرة عامة على العمارة



IKEv2

Platform OmniCharge OmniRAN OmniCall OmniCore Omni

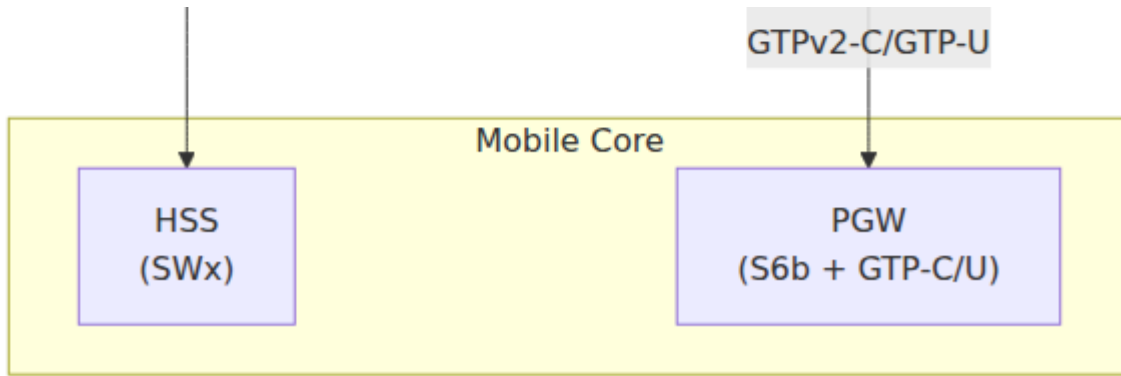


Diameter SWx

Simple Mode

GTP Mode

Diameter S6b



الأوضاع التشغيلية

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

GTP وضع

وتوجيهها عبر الشبكة GTP-U يتم تغليف حركة مرور المشتركين في PGW. عبر GPP نفق كامل 3 الأساسية للجوال.

استخدم عندما:

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

المكونات:

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

بسيط VPN وضع

يتم توجيه حركة مرور المشتركين مباشرة عبر مضيف TUN. عبر واجهة IP اختراق محلي لعنوان PGW. دون تدخل OmniEPDG.

استخدم عندما:

- PGW نشر مستقل بدون
- الاختبار والتطوير

- سيناريوهات الاختراق المحلي

المكونات:

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

أمان المصادقة

مميزات أمان مدمجة لحماية ضد هجمات القوة الغاشمة وتقييد الوصول حسب OmniEPDG يتضمن الموقع الجغرافي. راجع دليل **أمان المصادقة** للحصول على التفاصيل.

تحديد المعدل

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

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

GeoIP حظر البلدان باستخدام

MaxMind GeoLite2 تحكم اختياري في الوصول الجغرافي باستخدام قاعدة بيانات

- **وضع القائمة البيضاء** - السماح فقط بالاتصالات من البلدان المحددة
- **وضع القائمة السوداء** - حظر الاتصالات من البلدان المحددة
- غير المعروفة/الخاصة IP معالجة قابلة للتكوين لعناوين
- سلوك الفشل المفتوح أو الفشل المغلق عند عدم توفر قاعدة البيانات

التكوين الرئيسي

(بسيط VPN وضع) التكوين الأدنى

```
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 (مفعّل 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,

  # معطل بشكل افتراضي (حظر GeoIP)
  geoup_enabled: true,
  geoup_mode: :whitelist,
  geoup_countries: ["AU", "NZ"]
```

راجع مرجع التكوين للحصول على وثائق المعلومات الكاملة.

المراقبة

لوحة التحكم

ل: <http://<host>:4000/dashboard> الوصول إلى لوحة التحكم على الويب عبر

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

راجع دليل [لوحة التحكم](#) للحصول على التفاصيل.

Prometheus قياسات

ل: <http://<host>:9568/metrics> جمع القياسات من

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

راجع [مرجع القياسات](#) للحصول على استعلامات وقواعد التنبيه.

استكشاف الأخطاء

المشكلات الشائعة وخطوات الحل:

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

.راجع دليل **استكشاف الأخطاء** للحصول على إجراءات تشخيص مفصلة

فهرس الوثائق

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

وتدفقات OmniEPDG بنية المكالمات

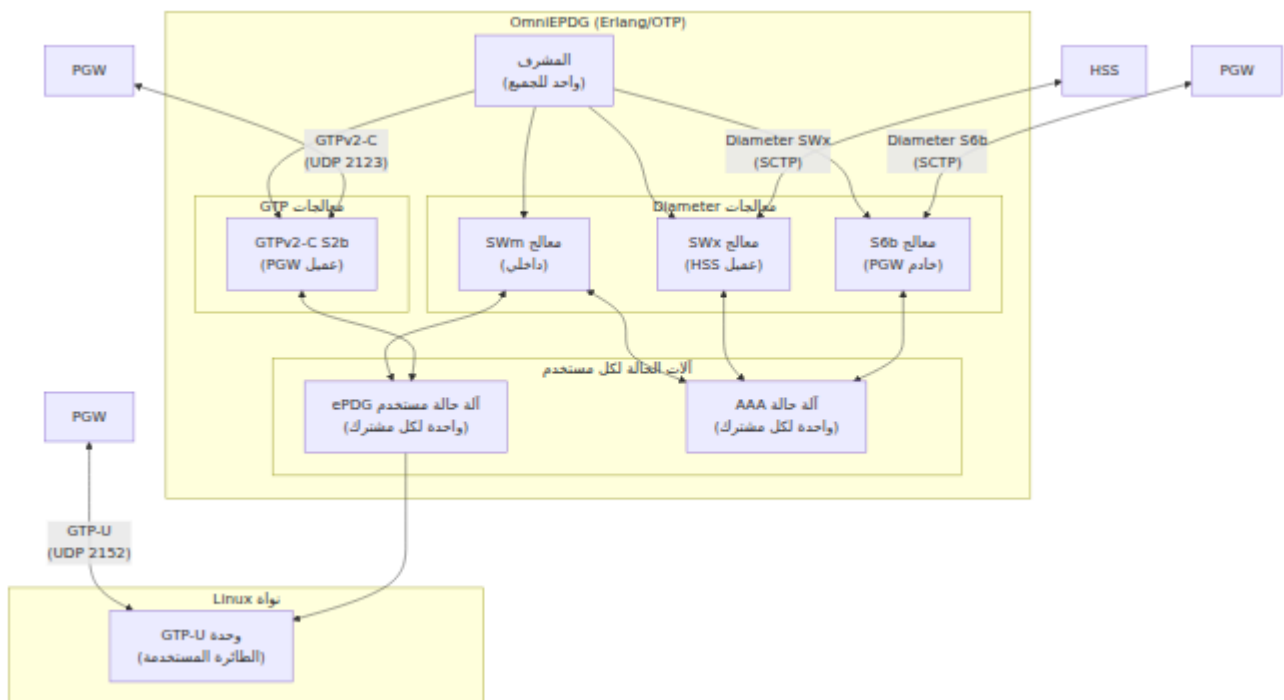
وواجهات البروتوكول الخاصة به، وآلات الحالة، OmniEPDG تصف هذه الوثيقة البنية الداخلية لـ الخاصة بالمستخدمين، ومخططات تسلسل الرسائل التفصيلية للإجراءات الرئيسية. يدعم بسيط VPN ووضع (PGW عبر GPP نفق كامل 3) GTP وضعين تشغيلين: وضع OmniEPDG. راجع دليل العمليات لمقارنة عالية المستوى. (TUN انفصال محلي مع واجهة)

بنية النظام

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

GTP بنية وضع

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



بسيط VPN بنية وضع

لا Linux في TUN بسيط، يتم توجيه حركة مرور المشتركين محليًا عبر واجهة VPN في وضع GTP-U و GTPv2-C و Diameter S6b يتم استبدال مكونات GTP أو PGW يتطلب الأمر بنية بسيط VPN بنظام.



شجرة المشرف

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

العمليات التي تبدأ في كلا الوضعين

الوصف	الدور	العملية
لإجراء عمليات المصادقة HSS يتصل بـ وإدارة ملف المشترك	Diameter عميل SWx	aaa_diameter_swx
session Diameter و EAP يوجه رسائل AAA وآلات حالة ePDG بين	Diameter SWm (داخلي)	aaa_diameter_swm
من إشارات ePDG يتعامل مع جانب Diameter الداخلية SWm	SWm معالج ePDG	epdg_diameter_swm

GTP: العمليات الإضافية في وضع

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

VPN بسيط: العمليات الإضافية في وضع

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

آلات الحالة لكل مستخدم

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

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

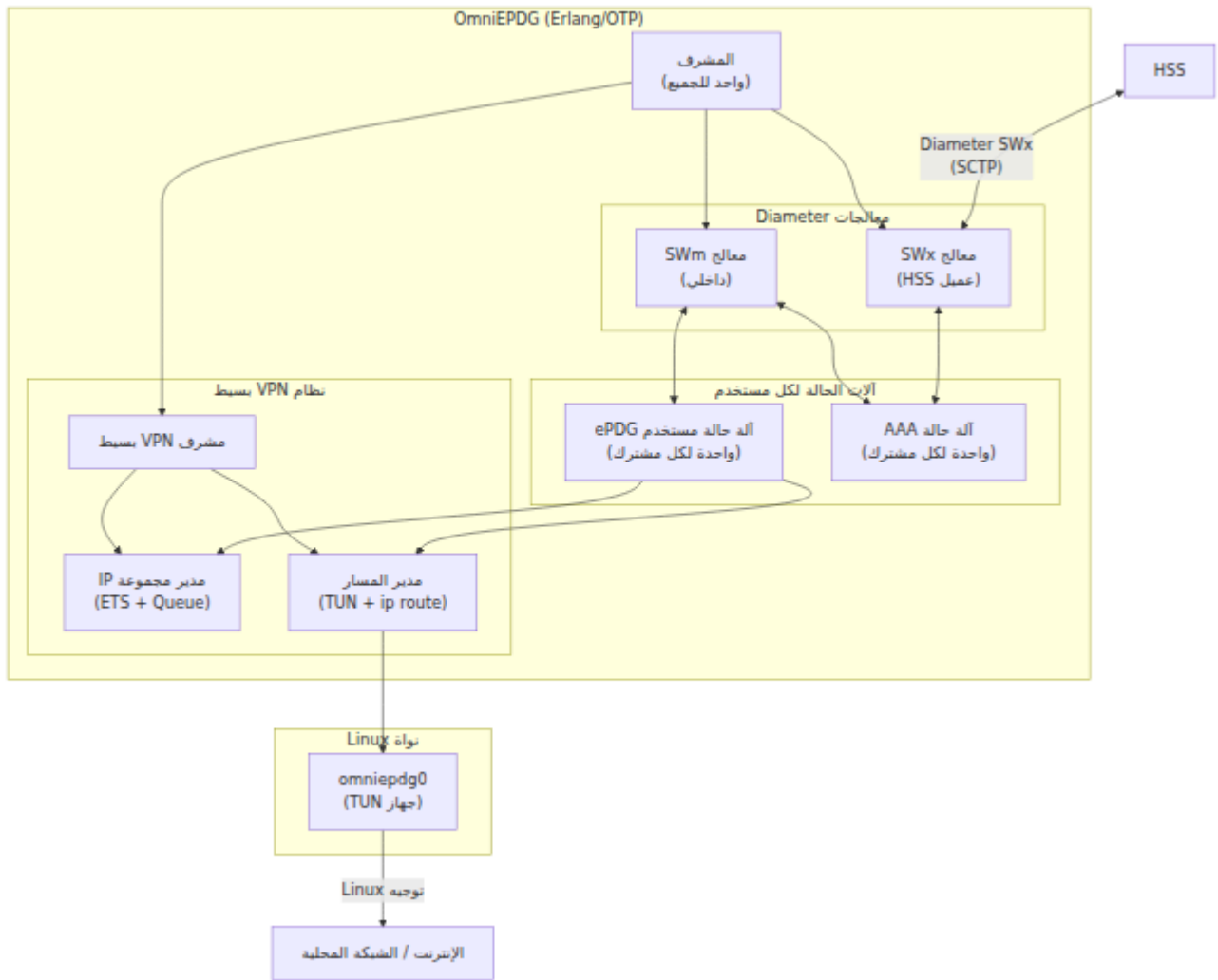
مع وضع رد نداء وظيفة الحالة Erlang gen_statem كلا الآتين يتم تنفيذهما كعمليات

ePDG حالات آلة حالة مستخدم

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

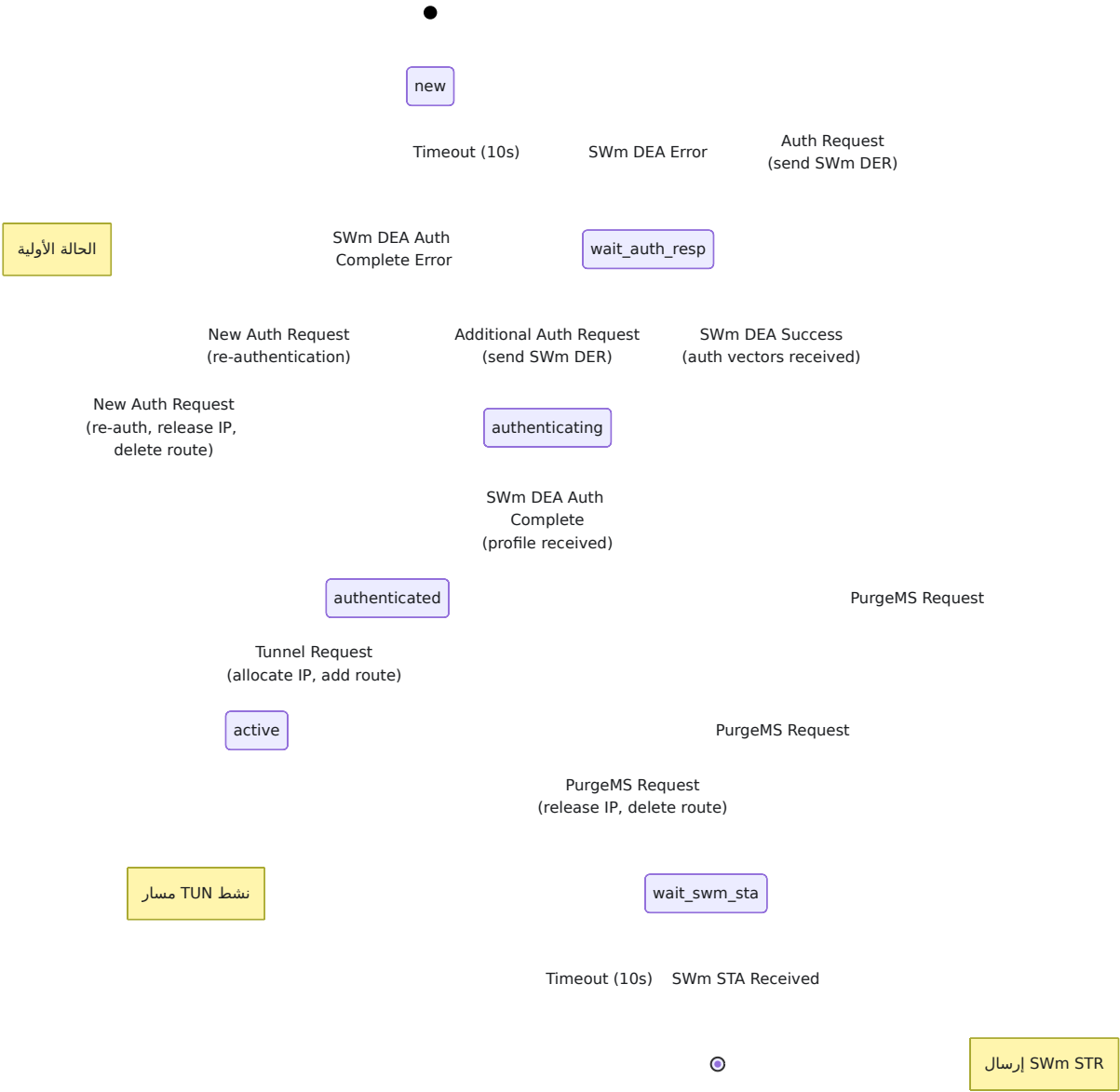
GTP آلة حالة

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



بسيطة VPN آلة حالة

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



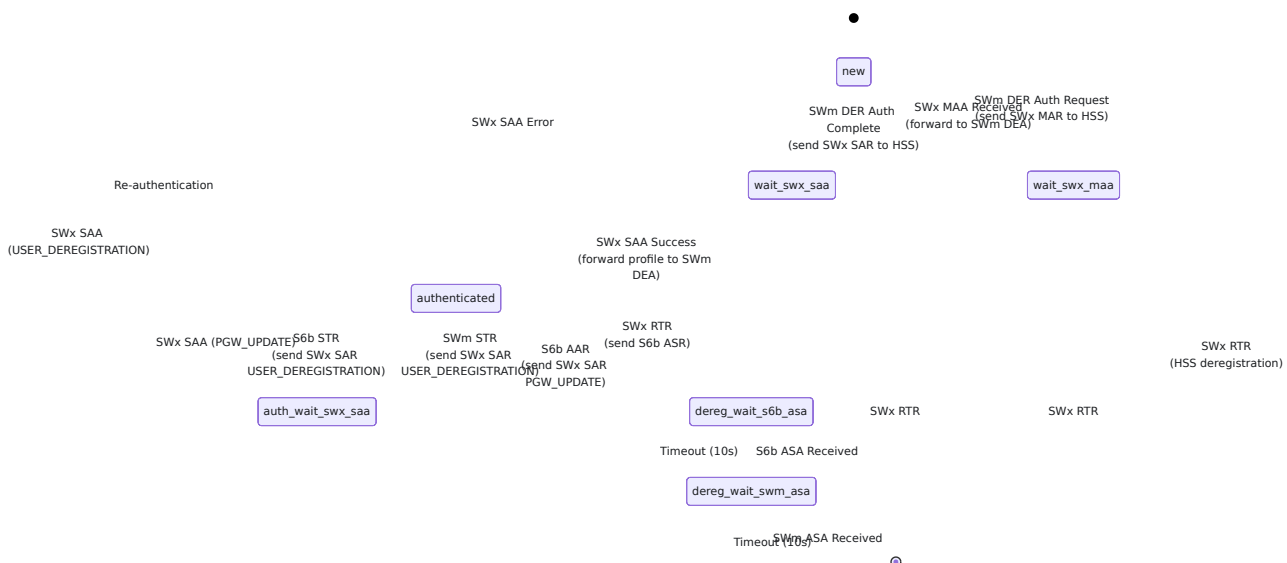
ePDG مرجع حالات آلة حالة مستخدم

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

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

AAA UE حالات آلة حالة

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



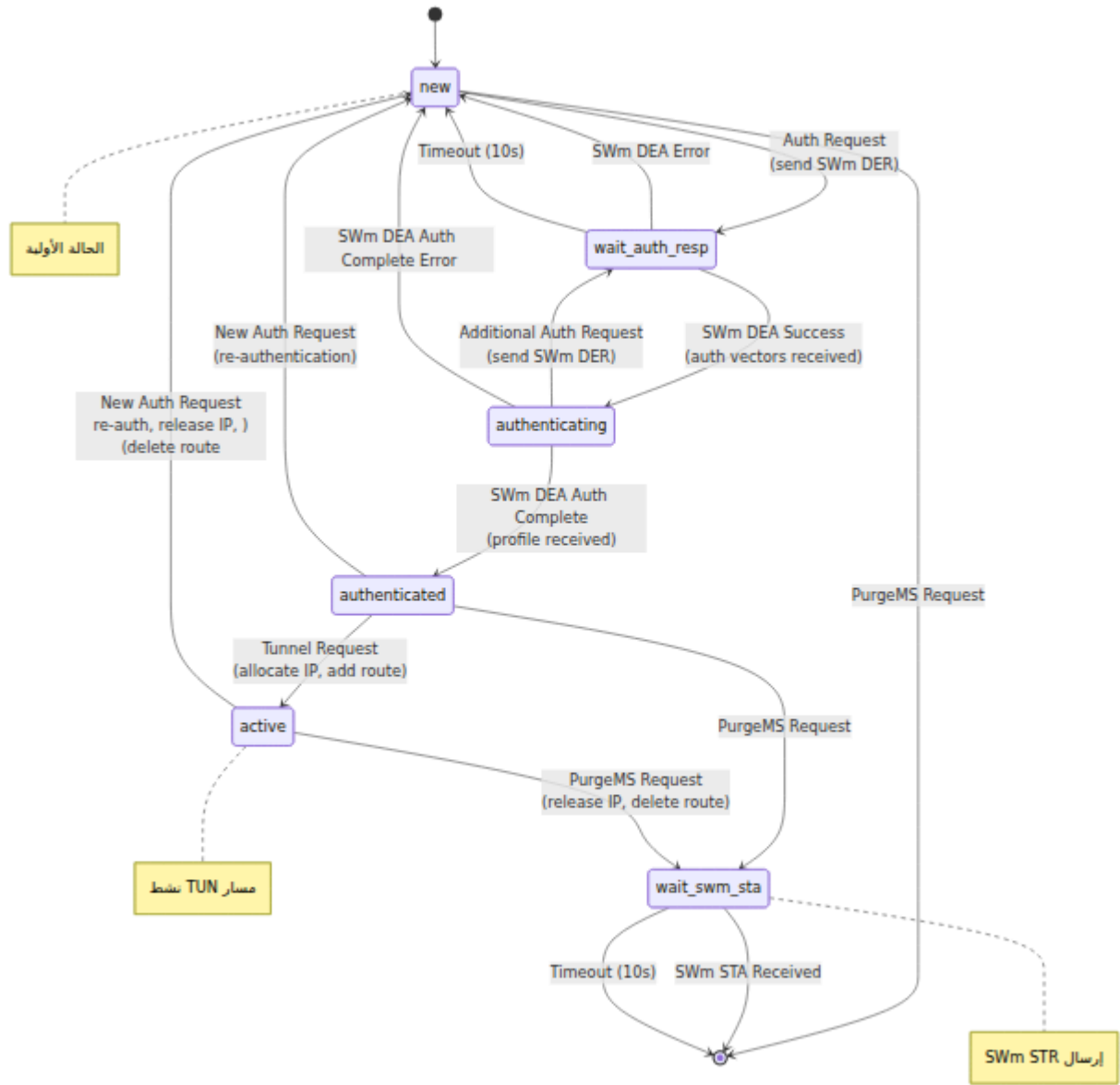
AAA UE مرجع حالات آلة حالة

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

تدفقات المكالمات

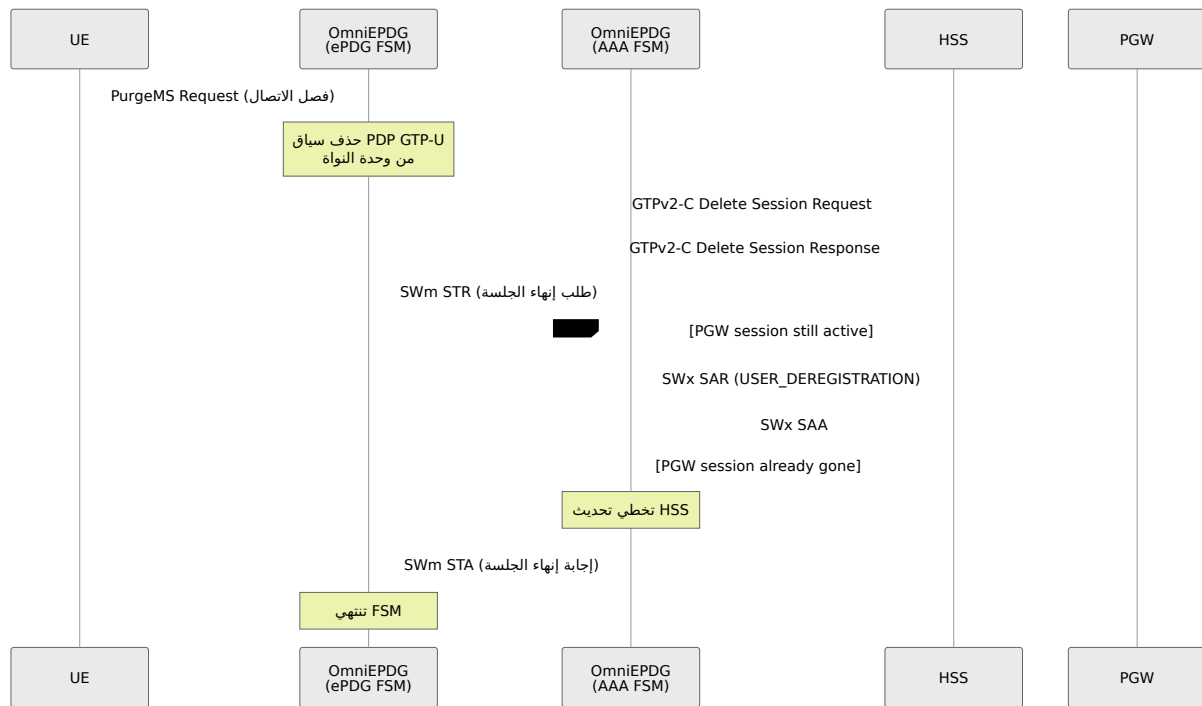
إنشاء جلسة ناجحة: GTP وضع

نشط GTP حتى نفق EAP-AKA تظهر هذه ال❖❖ لسلسلة جلسة ناجحة كاملة من مصادقة



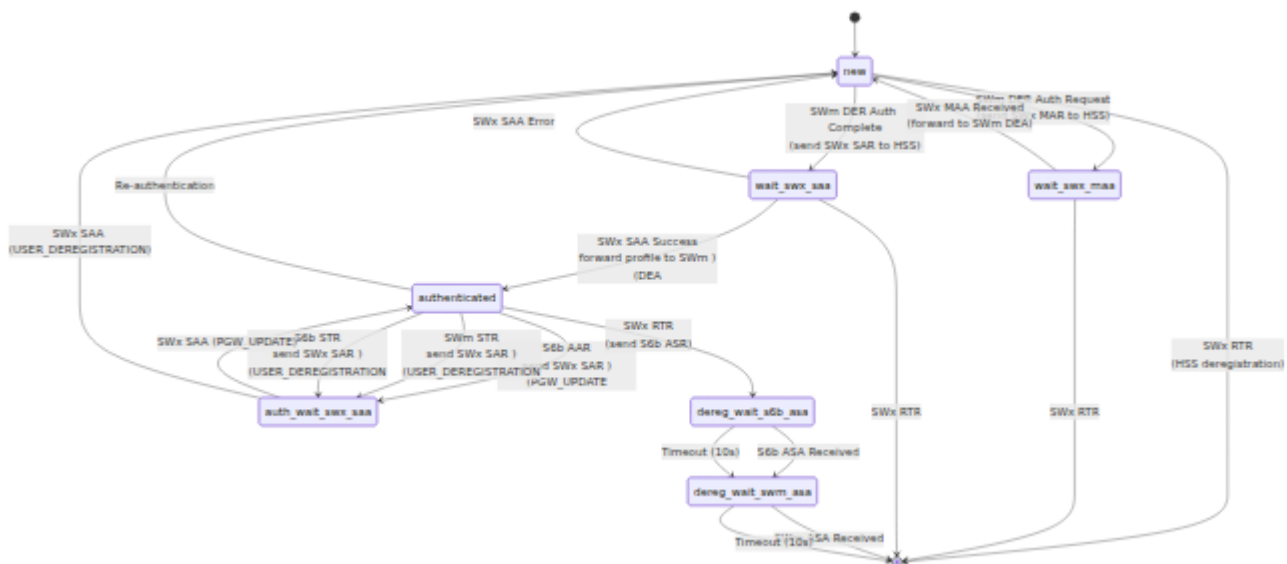
UE إنهاء الجلسة التي بدأها GTP: وضع

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



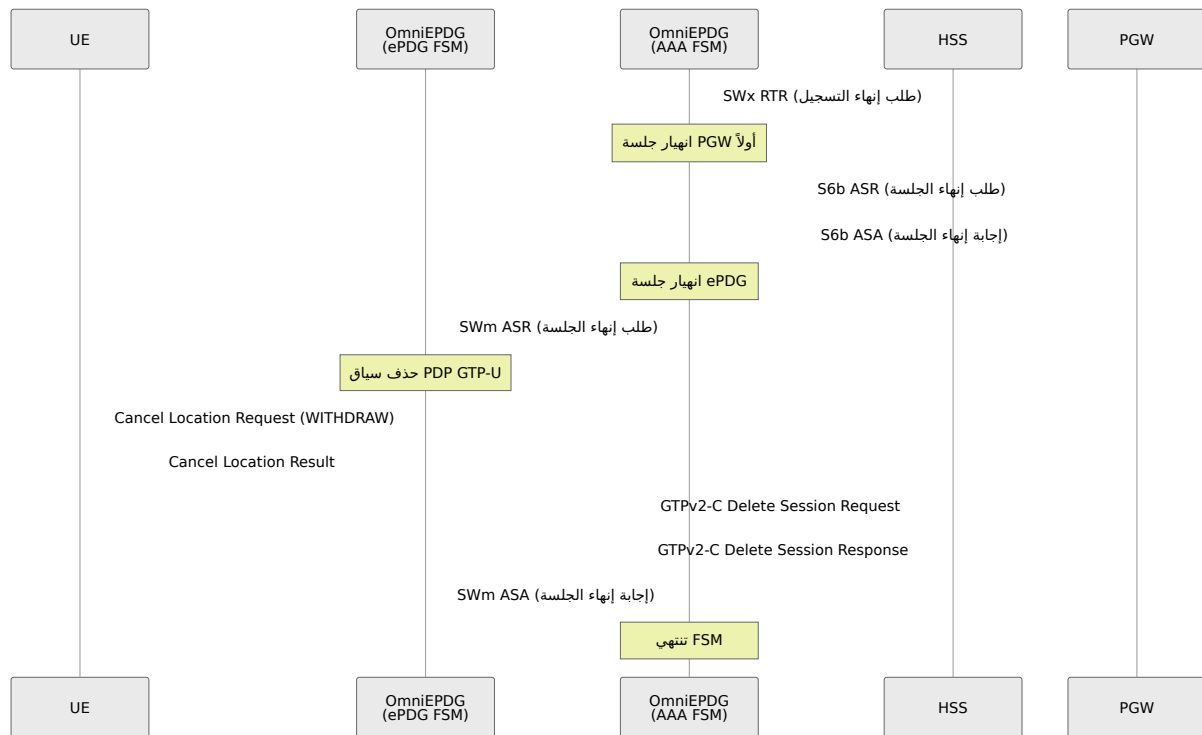
PGW إنهاء الجلسة التي بدأها GTP: وضع

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



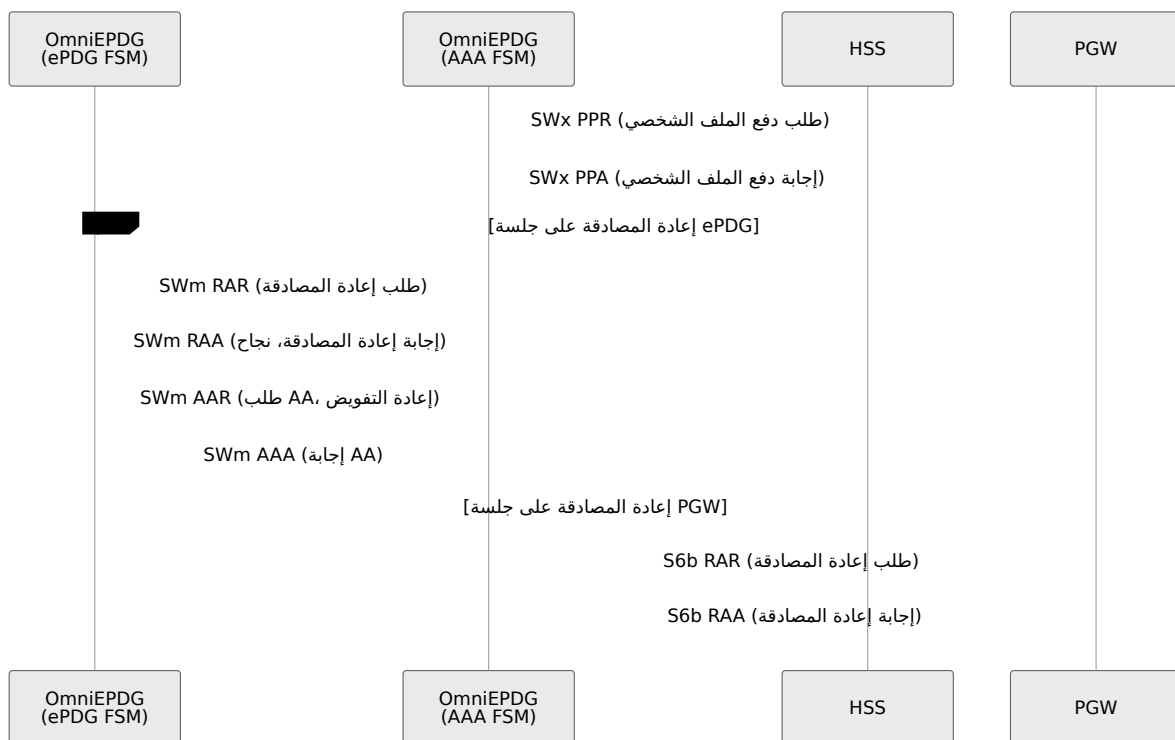
التي بدأت بها الشبكة GTP: deregistration وضع (HSS)

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



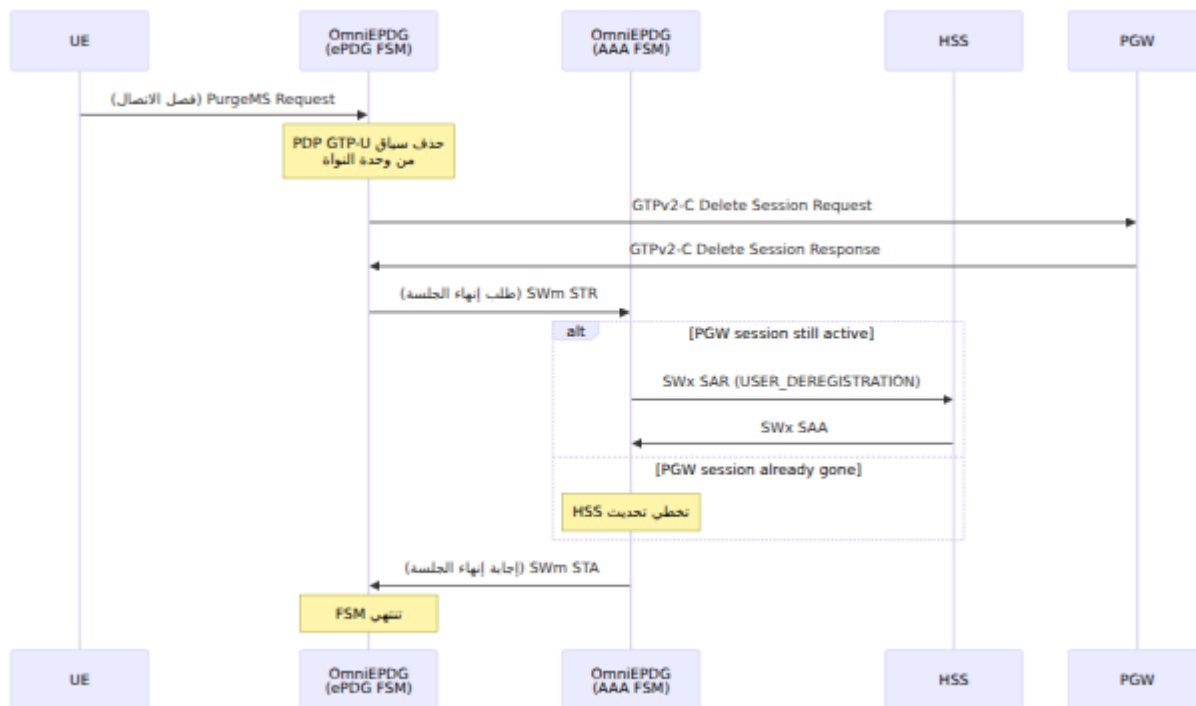
وإعادة المصادقة HSS دفع ملف تعريف GTP: وضع

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



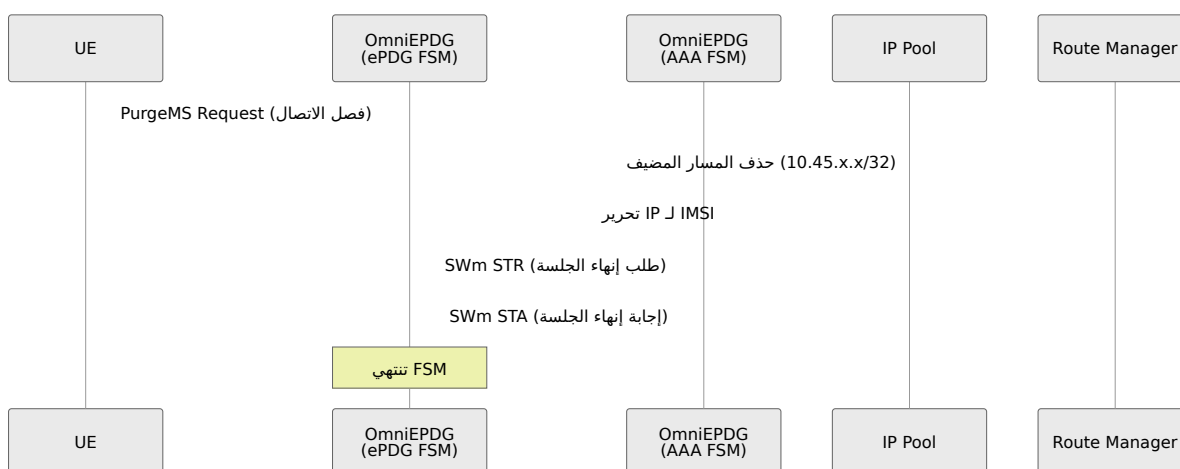
بسيط: إنشاء جلسة ناجحة VPN وضع

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



UE بسيط: إنهاء الجلسة التي بدأها VPN وضع

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



Diameter معرفات تطبيق

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

Diameter رموز نتائج

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

رموز النتائج القياسية

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

GPP رموز النتائج التجريبية 3

رمز النتيجة	الاسم	المعنى	رجع
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	لا HSS يمكنه توفير بيانات المصادقة مؤقتًا	3GPP TS 29.271
5001	DIAMETER_ERROR_USER_UNKNOWN	لم يتم العثور على IMSI المشترك في HSS	3GPP TS 29.271
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	3GPP TS 29.271
5004	DIAMETER_ERROR_ROAMING_NOT_ALLOWED	تنطبق قيود التجوال	3GPP TS 29.271
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	3GPP TS 29.274
5421	DIAMETER_ERROR_RAT_NOT_ALLOWED	تقنية الوصول غير مسموح بها	3GPP TS 29.274
5422	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	IMEI جهاز غير معترف به	3GPP TS 29.274

(فقط GTP وضع) GTPv2-C رموز سبب

Create/Delete Session التالية في استجابات GTPv2-C مع رموز سبب OmniEPDG يتعامل الرموز من 1-15 هي معلوماتية، 16-63 تشير إلى النجاح، و64+ تشير إلى الأخطاء. PGW. من GPP TS 29.274 Section 8.4. راجع 3

أسباب النجاح

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

أسباب الخطأ (محدد)

الرمز	الاسم	الوصف
64	Context Not Found	لم يتم العثور على سياق الجلسة على PGW
73	No Resources Available	PGW استنفاد موارد
78	Missing or Unknown APN	PGW المطلوب غير مكون على APN
82	Denied in RAT	تقنية الوصول غير مسموح بها
84	All Dynamic Addresses Occupied	PGW على IP استنفاد مجموعة عناوين
92	User Authentication Failed	PGW فشل المصادقة في
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	مزدحم APN
120	GTP-C Entity Congestion	PGW تحميل زائد في مستوى التحكم

NAI تنسيق

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

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

بادئة الهوية ونوع المصادقة

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

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

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

عن طريق تحليل كل شيء بين البادئة ورمز @. ثم يتم NAI من IMSI OmniEPDG يستخرج كـ مفتاح أساسي لجميع آلات الحالة والإشارات لكل مشترك IMSI استخدام.

الخوارزميات التشفيرية

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

IKEv2 خوارزميات تشفير

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

IKEv2 خوارزميات سلامة

الخوارزمية	المعرف	حجم المفتاح	حجم ICV	الحالة	المرجع
HMAC-SHA2-256-128	12	بت 256	128 بت	مدعوم (افتراضي)	RFC 4868
HMAC-SHA2-384-192	13	بت 384	192 بت	مدعوم	RFC 4868
HMAC-SHA2-512-256	14	بت 512	256 بت	مدعوم	RFC 4868
AES-XCBC-96	5	بت 128	بت 96	مدعوم	RFC 3566
HMAC-SHA1-96	2	بت 160	بت 96	مدعوم (قديم)	RFC 2404
HMAC-MD5-96	1	بت 128	بت 96	مدعوم (قديم)	RFC 2403

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

خوارزميات PRF IKEv2

المرجع	الحالة	حجم الإخراج	المعرف	الخوارزمية
RFC 4868	مدعوم (افتراضي)	بت 256	5	PRF-HMAC-SHA2-256
RFC 4868	مدعوم	بت 384	6	PRF-HMAC-SHA2-384
RFC 4868	مدعوم	بت 512	7	PRF-HMAC-SHA2-512
RFC 4434	مدعوم	بت 128	4	PRF-AES128-XCBC
RFC 2104	مدعوم (قديم)	بت 160	2	PRF-HMAC-SHA1
RFC 2104	مدعوم (قديم)	بت 128	1	PRF-HMAC-MD5

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

Diffie-Hellman IKEv2 مجموعات

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

خوارزميات ESP (Child SA)

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

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 AES-XCBC-96 J ICV HMAC- مقابل 16 J) بايت (SHA2-256-128)

(UE فقط عندما لا يمكن تحليل اقتراح) الاحتياطي:

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

التشفيرية EAP-AKA وظائف

الوظيفة	الخوارزمية	المرجع
MK اشتقاق	SHA-1	RFC 4187 Section 7
PRF+ توسيع مفتاح	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

التشفيرية EAP-AKA' وظائف

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

3 الـ GPP الامتثال لـ 3

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

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

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

(فقط GTP وضع) PDP أنواع عنوان

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

النوع	الوصف	PAA GTPv2-C تنسيق
IPv4	IPv4 ناقل فقط	مكون من 4 بايت IPv4 عنوان
IPv6	IPv6 ناقل 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

OmniEPDG مرجع تكوين

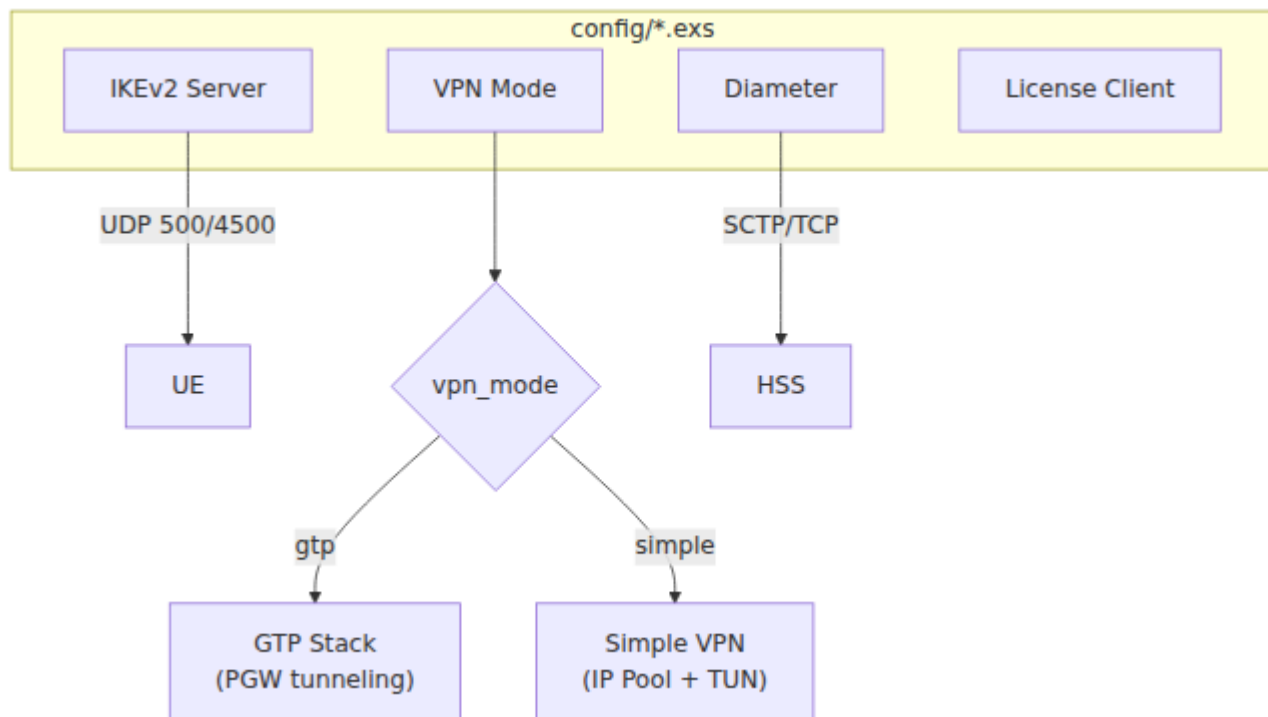
ومتغيرات البيئة. يتم إجراء جميع التكوينات `config/runtime.exs` عبر OmniEPDG يتم تكوين التي تواجه العملاء في وقت التشغيل - القيم الافتراضية في وقت الترجمة مدمجة في الإصدار. وليست مكشوفة.

بالنسبة للتوزيعات المعبأة، استخدم متغيرات البيئة كما هو موضح في قسم **مرجع متغيرات البيئة**.

جدول المحتويات

- IKEv2 معلومات خادم
- معلومات أمان المصادقة
- VPN اختيار وضع
- البسيطة VPN معلومات
- Diameter معلومات
- تكوين عميل الترخيص
- تكوين لوحة التحكم
- Prometheus تكوين مقاييس
- مرجع متغيرات البيئة
- مرجع المهلة

هيكل التكوين



ملف التكوين

هذا الملف عند بدء OmniEPDG يقرأ `config/runtime.exs` يتم إجراء جميع التكوينات في التشغيل. يدعم الملف استبدال متغيرات البيئة للتوزيعات المعبأة.

مثال على التكوين

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

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

  # البسيطة VPN إعدادات وضع
  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 الترخيص (runtime.exs)
config :license_client,
  server_url: "https://license.example.com/api",
  product: "omniepdg"
```

IKEv2 معلومات خادم

IPSec يقوم بإنهاء أن   اق OmniEPDG و UEs بين SWu مع واجهة IKEv2 يتعامل خادم EAP-AKA. ويؤدي مصادقة

المعلمة	النوع	مطلوب	الافتراضي
<code>listen_ip</code>	Tuple	لا	<code>{0, 0, 0, 0}</code>
<code>port_500</code>	Integer	لا	<code>500</code>
<code>port_4500</code>	Integer	لا	<code>4500</code>

المعلمة	النوع	مطلوب	الافتراضي
cert_file	String	نعم	/etc/omniepdg/cert:
key_file	String	نعم	/etc/omniepdg/cert:
session_inactivity_timeout_ms	Integer	لا	300000

معلومات أمان المصادقة

حماية مدمجة ضد هجمات القوة الغاشمة والتحكم في الوصول الجغرافي. OmniEPDG يتضمن [دليل الأمان](#) للحصول على وثائق مفصلة.

معلومات تحديد معدل الطلبات

```
config :omniepdg,  
  # تحديد معدل الطلبات 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 معدل الطلبات 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	الوصف
auth_rate_limit_per_ip	Integer	لا	10	الحد الأقصى لمحاولات لمصادقة الفاشلة لكل IP قبل الحظر.
auth_rate_limit_ip_window_ms	Integer	لا	60000	نافذة متحركة لعدد الفشل في IP (بالمللي ثانية).
auth_rate_limit_ip_block_ms	Integer	❖❖	300000	مدة لحظر لـ IPs التي تتجاوز لعتبة (5 دقائق).
auth_rate_limit_per_imsi	Integer	لا	5	الحد الأقصى لمحاولات لمصادقة الفاشلة لكل IMSI قبل الحظر.

المعلمة	النوع	مطلوب	الافتراضي	لوصف
auth_rate_limit_imsi_window_ms	Integer	لا	60000	نافذة متحركة لعدد الفشل في IMS (بالملي ثانية).
auth_rate_limit_imsi_block_ms	Integer	لا	600000	مدة لحظر ل-IMSI التي تتجاوز العتبة (10 دقائق).

معلومات 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	
geoup_enabled	Boolean	لا	false	ر ة ة ن M C
geoup_database_path	String	لا	"/etc/omniepdg/GeoLite2-Country.mmdb"	ة ن M C C (M
geoup_mode	Atom	لا	:whitelist	((ن ة (ة
geoup_countries	List	لا	[]	ن L ة (" "
geoup_allow_unknown	Boolean	لا	mode-dependent	- ن L .

المعلمة	النوع	مطلوب	الافتراضي
geoip_fail_open	Boolean	لا	true

VPN اختيار وضع

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 عبر PGW GTPv2- C/GTP-U. راجع دليل العمليات للحصول على مقارنة مفصلة.

البسيطة VPN معلمات

OmniEPDG البسيط. يدعم VPN لوضع DNS و IP في تخصيص simple_vpn تتحكم كتلة تكوين IPv4 و IPv6 كل من تجمعات عن   وين.

```
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  
  ]
```

ف	الافتراضي	مطلوب	النوع	المعلمة
ناوين IPv4 تدوين CIDF عبيص عنوان لكل شترك	"10.45.0.0/16"	نعم	String	pool_ipv4
ناوين IPv6 تدوين CIDF بركين ثنائي	"2001:db8::/32"	لا	String	pool_ipv6
توادم IPv4 ممة لـ UEs PCO (رات كوبن وكول	["8.8.8.8", "8.8.4.4"]	لا	List	dns_servers_ipv4
توادم IPv6 ممة لـ UEs PCO	["2001:4860:4860::8888", "2001:4860:4860::8844"]	لا	List	dns_servers_ipv6
ناوين CSC Prox IPv4	[]	لا	List	p_cscf_ipv4

المعلمة	النوع	مطلوب	الافتراضي	ف
				VoW مة ل UEs سجل IMS.
p_cscf_ipv6	List	لا	[]	ناوين CSC Prox IPv6 VoW
mtu	Integer	لا	1400	قيمة واجهة القيم تقلل جزئة
nat_enabled	Boolean	لا	true	مكين مرور ركين. تكون ،، يتم طابق قواعد تمويه حركة مرور مادة

Diameter معلومات

عندما تكون (PGW) S6b و (HSS) SWx في واجهات Diameter يتحكم تكوين diameter_enabled يبدأ OmniEPDG صحيحة،

```
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}  
    ]  
  }  
}
```

معلومات الخدمة

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

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

معلومات الأقران

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

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

معرفات التطبيقات

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

تكوين عميل الترخيص

مقابل خادم الترخيص OmniEPDG يتحقق عميل الترخيص من

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

صف	متغير البيئة	الافتراضي	مطلوب	النوع	المعلمة
عنوان URL نقطة نهاية واجهة برمجة تطبيقات خادم خاص	LICENSE_SERVER_URL	-	نعم	String	server_url
معرف المنتج تحقق من خاص	-	"omniepdg"	لا	String	product

تكوين لوحة التحكم

.توفر لوحة التحكم على الويب قدرات المراقبة والإدارة

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

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

Prometheus تكوين مقاييس

للمراقبة والتنبيه HTTP عبر Prometheus مقاييس OmniEPDG يعرض.

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

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

المقاييس المعروضة

مقاييس العد (مدفوعة بالأحداث):

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

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

مقاييس القياس (يتم استقصاؤها كل 5 ثواني)

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

مقاييس الهيستوغرام (تتبع الكمون)

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

VM مقاييس

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

Prometheus تكوين استقصاء

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

مرجع المهلة

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

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

مرجع متغيرات البيئة

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

IKEv2 خادم

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

VPN وضع

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

Diameter

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

HSS نظير

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

الترخيص، لوحة التحكم، والمقاييس

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

مثال: Docker Compose

```
services:
  omniepdg:
    image: omniepdg:latest
    environment:
      # IKEv2
      EPDG_LISTEN_IP: "0.0.0.0"
      EPDG_CERT_FILE: "/certs/epdg.crt"
      EPDG_KEY_FILE: "/certs/epdg.key"

      # 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"

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

OmniEPDG لوحة التحكم

Diameter لوحة تحكم قائمة على الويب لمراقبة الجلسات والأقران OmniEPDG تتضمن 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
- Diameter عرض الأقران
- عرض السجلات
- عرض الوثائق
- عرض الموارد
- عرض التكوين

الوصول إلى لوحة التحكم

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

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

التنقل

:توفر لوحة التحكم شريط جانبي يحتوي على روابط لجميع العروض

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

لوحة المعلومات

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

بطاقات الإحصائيات

تظهر لوحة المعلومات أربع إحصائيات رئيسية

الوصف	الإحصائية
التي تم إنشاؤها UE العدد الحالي للجلسات	الجلسات النشطة
UEs إجمالي البايتات المستلمة من (اتجاه الرفع)	(UL) البيانات المستلمة
UEs إجمالي البايتات المرسل إلى (اتجاه التنزيل)	(DL) البيانات المرسل
الأقران المتصلة / الأقران المكونة الكلية	Diameter الأقران

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

الروابط السريعة

الانتقل المباشر إلى العروض التفصيلية

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

معلومات النظام

يعرض التكوين التشغيلي الحالي

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

التحديث التلقائي

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

عرض الجلسات

النشطة مع معلومات تفصيلية لكل مشترك UE يعرض عرض الجلسات جميع جلسات

OmniEPDG v0.1.0

Licensed to: Omnitouch
© 2020 Omnitouch

Dashboard

Sessions

Diameter

Logs

Docs

Resources

Configuration

License

UE Sessions

1 Session1 Active↓ 8.53 KB / ↑ 12.17 KB

IMSI

UE IP

SOURCE

APN

STATUS

DURATION

TRAFFIC

100.64.34.84

10.7.7.50:14500

*

Active

4m 50s

↓ 8.53 KB / ↑ 12.17 KB

SESSION

NETWORK & TIMING

TRAFFIC

IMSI

NAI

UE IP

Source

APN

Child SA SPI

DNS

P-CSCF

Connected

Last Activity

* Duration

10.4.10.195, 10.4.10.196

10.4.12.165

2026-03-08 21:39:16

2026-03-08 21:41:48

4m 50s

Bytes In (UL)

Bytes Out (DL)

Packets In

Packets Out

8.53 KB

12.17 KB

63

63



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

قائمة الجلسات

:تعرض كل صف من الجلسات

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

مؤشرات الحالة

:تعرض الجلسات الحالة مع شارات ملونة

الوصف	اللون	الحالة
الجلسة تم إنشاؤها بالكامل وتعمل	أخضر	نشطة
جاري إنشاء الجلسة	أصفر	جارٍ الاتصال
تم إنهاء الجلسة أو فشلت	أحمر	غير نشطة

تفاصيل الجلسة

:انقر على أي صف من الجلسات لتوسيع المعلومات التفصيلية

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

قسم الجلسة

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

قسم الشبكة والتوقيت

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

قسم الحركة

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

الحالة الفارغة

:عندما لا تكون هناك جلسات نشطة، يعرض العرض

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

التحديث التلقائي

.تقوم قائمة الجلسات بتحديث نفسها تلقائيًا كل ثانية.

Diameter عرض الأقران

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

قائمة الأقران

تعرض كل صف من الأقران:

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

مؤشرات الحالة

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

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

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

الحالة الفارغة

:عندما لا تكون هناك أقران مكونة، يعرض العرض

- مفعلاً Diameter مكونة" إذا كان Diameter لا توجد أقران"
- معطل" مع تلميح التكوين إذا كان معطلاً Diameter"

التحديث التلقائي

.تقوم قائمة الأقران بتحديث نفسها تلقائيًا كل ثانية

عرض السجلات

.يوفر عرض السجلات بُنًى 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

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

مستويات السجلات

تُرمز السجلات بالألوان حسب الخطورة

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

تصفية المستوى

يمكن تصفية السجلات حسب الحد الأدنى لمستوى الخطورة باستخدام القائمة المنسدلة

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

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

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

مخزن السجلات

- يتم الاحتفاظ بحد أقصى 1000 إدخال سجل
- تتم إزالة أقدم الإدخالات عند الوصول إلى الحد
- يؤدي مسح السجل   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 إيقاف)

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

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

عرض Markdown

بما في ذلك Markdown تُعرض الوثائق بدعم كامل من

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

عرض الموارد

OTP والتطبيقات التي تعمل على BEAM VM يعرض عرض الموارد إحصائيات

مقاييس النظام

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

التطبيقات التي تعمل

:المحملة مقسمة حسب الفئة OTP تدرج جميع تطبيقات

الفئة	الوصف
الرئيسية	OmniEPDG تطبيق
النظام	الأساسية Elixir و Erlang/OTP تطبيقات

.انقر على تطبيق لعرض تفاصيله بما في ذلك الإصدار والوصف والاعتمادات

عرض التكوين

.يعرض عرض التكوين تكوين وقت التشغيل والتطبيقات المحملة

معلومات البيئة

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

قائمة التطبيقات

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

- وصف التطبيق
- معلومات الإصدار
- الاعتمادات
- معلومات التكوين

تكوين لوحة التحكم

HTTP منفذ

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

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

المعلمة	النوع	الافتراضي	الوصف
<code>port</code>	عدد صحيح	4000	لواجهة التحكم HTTP منفذ

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

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

جدول المحتويات

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

نقطة نهاية المقاييس

:المقاييس في OmniEPDG يقدم

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

Prometheus المتوافق مع Prometheus ترجع نقطة النهاية المقاييس بتنسيق عرض
وآدوات المراقبة الأخرى Grafana.

التكوين

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

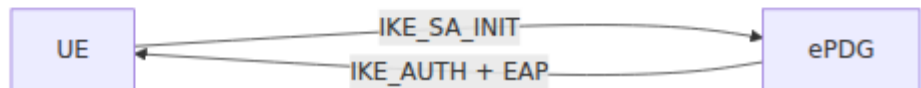
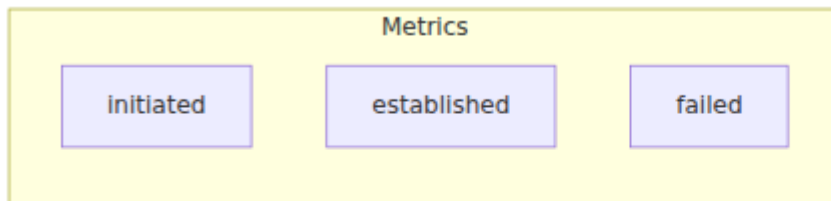
```
config :omniepdg,  
  prometheus: %{  
    port: 9568  
  }
```

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

فئات المقاييس

IKEv2 مقاييس جلسة

SWu على واجهة IKEv2 مقاييس تتبع إنشاء نفق.



المقياس: `epdg_ikev2_session_initiated_count`

النوع: عداد

يبدء إنشاء النفق UE التي تم بدعها. يزيد عندما يقوم IKE_SA_INIT **الوصف:** إجمالي تبادلات

المقياس: `epdg_ikev2_session_established_count`

النوع: عداد

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

المقياس: `epdg_ikev2_session_failed_count`

النوع: عداد

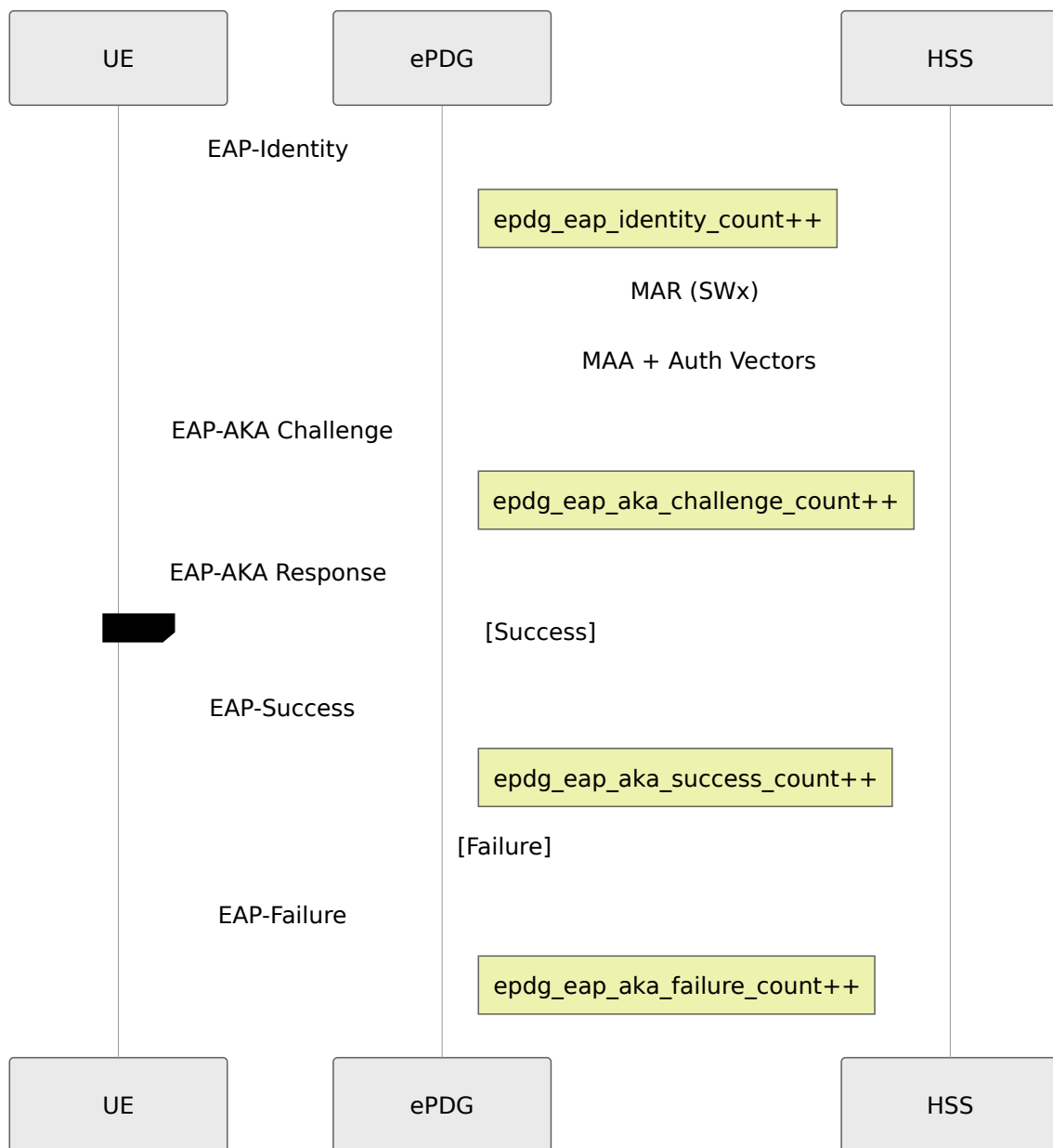
الوصف: إجمالي حالات فشل إنشاء IKE SA

التسميات:

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

EAP مقاييس مصادقة

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



المقياس: epdg_eap_identity_count

النوع: عداد

الوصف: إجمالي طلبات EAP-Identity من UEs المستلمة

المقياس: epdg_eap_aka_challenge_count

النوع: عداد

الوصف: المرسلات إلى EAP-AKA من UEs إجمالي تحديثات

المقياس: epdg_eap_aka_success_count

النوع: عداد

الوصف: إجمالي المصادقات الناجحة باستخدام EAP-AKA

المقياس: epdg_eap_aka_failure_count

النوع: عداد

الوصف: EAP-AKA إجمالي المصادقات الفاشلة باستخدام

التسميات:

- reason (مثل res_mismatch, invalid_identity, authentication_rejected)

المقياس: epdg_eap_aka_sync_failure_count

النوع: عداد

الوصف: EAP-AKA (SQN) يشير إلى عدم تطابق رقم. إجمالي حالات فشل مزامنة رقم تسلسل مما يتطلب إعادة المزامنة USIM/HSS تسلسل.

مقاييس أمان المصادقة

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

المقياس: epdg_auth_verification_failed_count

النوع: عداد

الوصف: AUTH. إجمالي حالات فشل التحقق من الهوية. يشير إلى هجمات محتملة من نوع. أو أخطاء في التنفيذ man-in-the-middle.

المقياس: epdg_auth_rate_limited_count

النوع: عداد

الوصف: إجمالي محاولات المصادقة المحجوبة بواسطة تحديد المعدل

التسميات:

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

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

حسب الدولة GeoIP **الوصف:** إجمالي محاولات المصادقة المحجوبة بواسطة تصفية

التسميات:

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

استعلامات نموذجية:

```
# لكل دقيقة GeoIP حجب
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

يشير (RFC 4303 وفقًا لـ) المرفوضة بسبب اكتشاف إعادة التشغيل ESP **الوصف:** إجمالي حزم إلى هجمات محتملة من نوع إعادة التشغيل أو مشاكل في الشبكة تسبب إعادة ترتيب الحزم.

Diameter SWx مقاييس

GPP TS 29.273 وفقًا لـ 3 HSS و ePDG بين SWx مقاييس لمواجهة

المقياس: epdg_diameter_swx_mar_count

النوع: عداد

لاسترجاع متجهات HSS المرسل إلى Multimedia-Auth-Requests **الوصف:** إجمالي طلبات

المصادقة

التسميات:

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

المقياس: `epdg_diameter_swx_sar_count`

النوع: عداد

للتسجيل/إلغاء HSS المرسل إلى Server-Assignment-Requests **الوصف:** إجمالي طلبات التسجيل

التسميات:

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

المقياس: `epdg_diameter_swx_mar_latency_ms`

النوع: هيسٲوآرام

بالميلي ثانية MAR **الوصف:** زمن استجابة

الأقسام: 50, 100, 250, 500, 1000, 2500 مللي ثانية

المقياس: `epdg_diameter_swx_sar_latency_ms`

النوع: هيسٲوآرام

بالميلي ثانية SAR **الوصف:** زمن استجابة

الأقسام: 50, 100, 250, 500, 1000, 2500 مللي ثانية

المقياس: `epdg_diameter_swx_pending_count`

النوع: مقياس

المعلقة في انتظار الاستجابة. تشير القيم العالية إلى ازدحام SWx **الوصف:** العدد الحالي لطلبات HSS أو مشاكل في الاتصال

Diameter S6b مقاييس

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

المقياس: epdg_diameter_s6b_aar_count

النوع: عداد

المعالجة لتفويض الجلسة AA-Requests **الوصف:** إجمالي طلبات

التسميات:

- result - نتيجة الطلب: success أو failure
-

المقياس: epdg_diameter_s6b_str_count

النوع: عداد

المعالجة Session-Termination-Requests **الوصف:** إجمالي طلبات

المقياس: epdg_diameter_s6b_active_sessions_count

النوع: مقياس

S6b **الوصف:** العدد الحالي للجلسات النشطة

مقاييس دورة حياة الجلسة

.وإنها PDN مقاييس تتبع إنشاء الجلسة

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: FSM الجلسات مجمعة حسب حالة

التسميات:

- state (مثل init, eap_identity, eap_aka_challenge, authenticated, established)
-

المقياس: epdg_auth_duration_ms

النوع: هيسٲوكرام

إلى الجلسة المنشأة IKE_SA_INIT **الوصف:** مدة تدفق المصادقة الكاملة من
الأقسام: 100, 250, 500, 1000, 2500, 5000, 10000 مللي ثانية

المقياس: epdg_session_duration_seconds

النوع: هيسٲوكرام

الوصف: عمر الجلسة من الإنشاء إلى الإنهاء

الأقسام: 60, 300, 900, 1800, 3600, 7200, 14400 ثانية (من 1 دقيقة إلى 4 ساعات)

ESP مقاييس بيانات

RFC 4303 وفقًا لـ ESP مقاييس لمعالجة حزم

المقياس: epdg_esp_packets_in_count

النوع: عداد

(الشبكة → UE اتجاه) التي تم فك تشفيرها بنجاح ESP **الوصف:** إجمالي حزم

المقياس: epdg_esp_packets_out_count

النوع: عداد

(UE → اتجاه الشبكة) التي تم تشفيرها ESP **الوصف:** إجمالي حزم

المقياس: epdg_esp_bytes_in_total

النوع: مقياس

ESP الوصف: إجمالي البايتات المفككة من حزم

المقياس: epdg_esp_bytes_out_total

النوع: مقياس

ESP الوصف: إجمالي البايتات المشفرة في حزم

IP مقاييس مجموعة

البسيط VPN في وضع IP مقاييس لإدارة مجموعة عناوين

المقياس: epdg_ip_allocated_count

النوع: عداد

IP الوصف: إجمالي عناوين

التسميات:

- type أو ipv4: نوع العنوان - ipv6
-

المقياس: epdg_ip_released_count

النوع: عداد

IP الوصف: التي تم تحريرها إجمالي عناوين

التسميات:

- type أو ipv4: نوع العنوان - ipv6
-

المقياس: epdg_ip_pool_allocated_count

النوع: مقياس

IP الوصف: العدد الحالي لعناوين

المقياس: epdg_ip_pool_available_count

النوع: مقياس

IP الوصف: المتاحة في المجموعة IP العدد الحالي لعناوين

المقياس: epdg_ip_pool_utilization_ratio

النوع: مقياس

كنسبة من 0.0 إلى 1.0. تشير القيم القريبة من 1.0 إلى خطر IP **الوصف:** استخدام مجموعة استنفاد المجموعة.

VM مقاييس

.لمراقبة صحة النظام Erlang/BEAM مقاييس آلة افتراضية

المقياس: vm_memory_total

النوع: مقياس

الوحدة: بايت

VM الوصف: إجمالي الذاكرة المخصصة بواسطة

المقياس: vm_memory_processes

النوع: مقياس

الوحدة: بايت

Erlang الوصف: الذاكرة المستخدمة بواسطة عمليات

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

(حالة الجلسة، السجلات) **ETS الوصف:** الذاكرة المستخدمة بواسطة جداول

المقياس: vm_system_info_process_count

النوع: مقياس

Erlang الوصف: عدد عمليات النشطة

المقياس: `vm_system_info_port_count`

النوع: مقياس

الوصف: عدد المنافذ المفتوحة (المأخذ، مقبضات الملفات)

المقياس: `vm_statistics_run_queue`

النوع: مقياس

الوصف: الطول الإجمالي لقوائم تشغيل الجدولة. تشير القيم العالية إلى تشبع وحدة المعالجة المركزية.

Prometheus تكامل

تكوين السحب

الخاص بك `prometheus.yml` إلى ملف OmniEPDG أضف

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

اكتشاف الخدمة

استخدم اكتشاف الخدمة، Kubernetes، لعمليات نشر

```

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])

```

(p95) زمن استجابة المصادقة

```

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

```

HSS (p99) زمن استجابة

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

الجلسات النشطة

```
epdg_sessions_active_count
```

IP استخدام مجموعة

```
epdg_ip_pool_utilization_ratio * 100
```

ESP معدل نقل

```
# 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

```
# حسب السبب EAP فشل  
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

Prometheus J OmniEPDG: قواعد تنبيه نموذجية لـ

```

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: "%فوق 90 IP استخدام مجموعة"
        description: "مستخدمة بنسبة IP مجموعة" {{ $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: "مرتفع HSS (SWx) زمن استجابة"
  description: "{{ $value }} في النسبة المئوية 95 هو MAR زمن استجابة"
$value }}ms"
```

المعلقة SWx تراكم طلبات

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

مرتفعة VM ذاكرة

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

تحميل زائد على الجدولة

```
- alert: OmniEPDGSchedulerOverload
  expr: vm_statistics_run_queue > 10
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "مرتفع Erlang طول قائمة تشغيل جدولة"
    description: "{{ $value }} طول قائمة التشغيل هو، 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"

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

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

```

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

متطلبات الشبكة

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

منافذ جدار الحماية

(UE ↔ ePDG) المنافذ المواجهة للإنترنت

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

المنفذ	البروتوكول	الاتجاه	الغرض
500	UDP	وارد	(IKE_SA_INIT, IKE_AUTH) الأولي IKEv2 تبادل
4500	UDP	وارد	IKEv2 NAT-Traversal و ESP-in-UDP encapsulation

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

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

(ePDG ↔ Core) منافذ الشبكة الداخلية

وشبكة النواة المحمولة. يجب أن تكون متاحة من OmniEPDG تستخدم هذه المنافذ للتواصل بين 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	(HTTP) واجهة الويب الخاصة بلوحة التحكم
443	TCP	(HTTPS، الإنتاج) واجهة الويب الخاصة بلوحة التحكم
9568	TCP	Prometheus نقطة نهاية مقاييس

DNS متطلبات

ePDG لاكتشاف DNS سجل

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

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

حيث:

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

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

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

الاسم الشائع للشهادة

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

متطلبات الشهادة:

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

DNS مجال Diameter

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

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

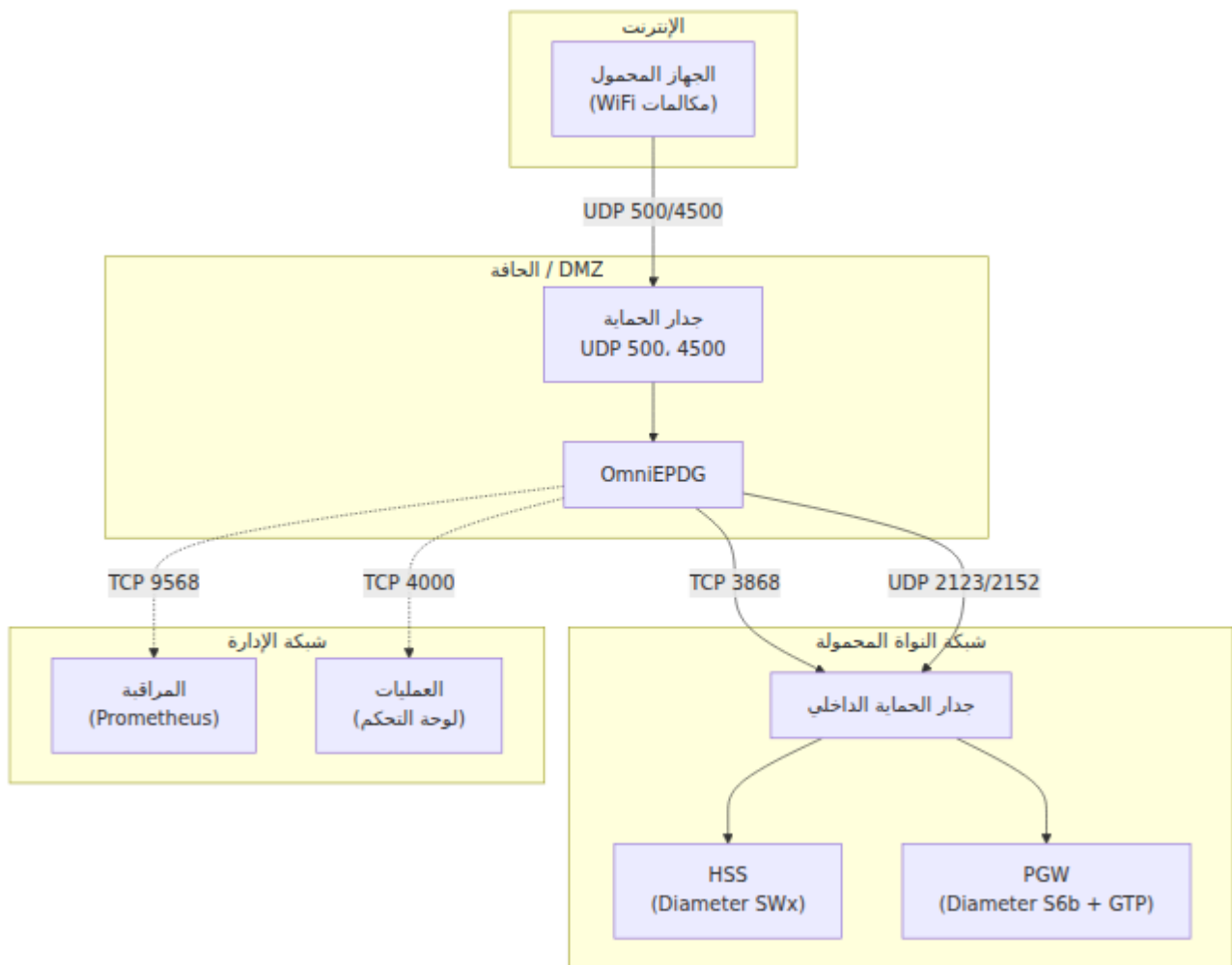
مثال:

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

يستخدم هذا المجال في:

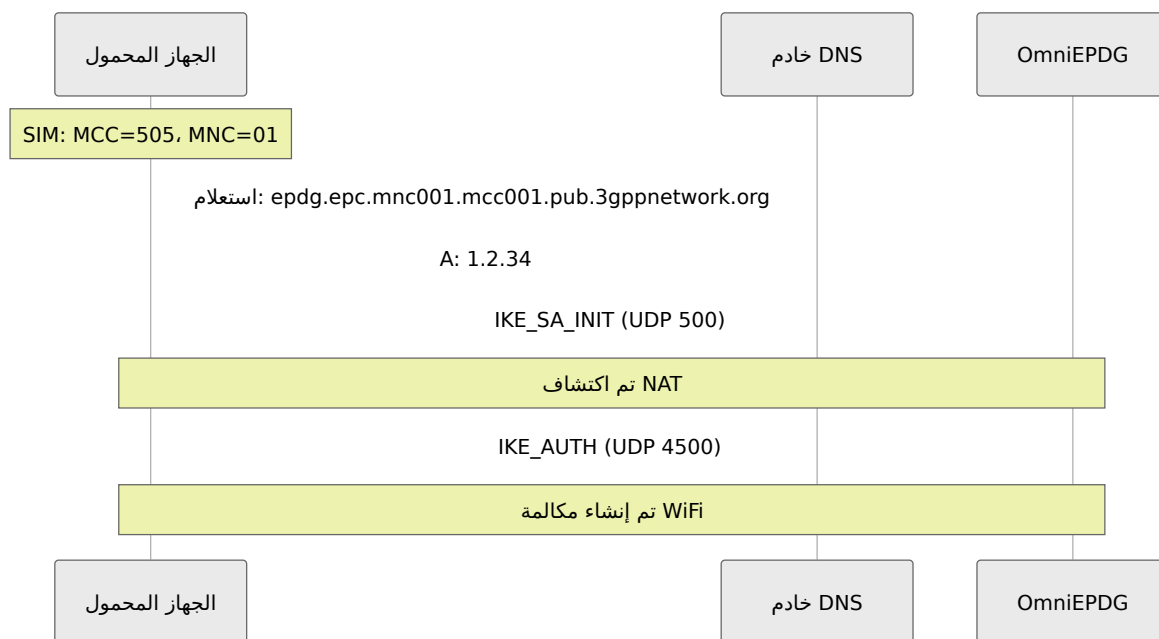
- خلال المصادقة UE المرسل بواسطة (معرف الوصول إلى الشبكة) NAI
- AVPs Diameter Origin-Realm و Destination-Realm
- Diameter قرارات توجيه

هندسة الشبكة



DNS تدفق بحث

التالي DNS يحدث حل، WiFi، عندما يبدأ جهاز محمول مكالمات



قائمة التحقق

متطلبات المواجهة للإنترنت

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

متطلبات شبكة النواة

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

متطلبات الإدارة

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

المراجع

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

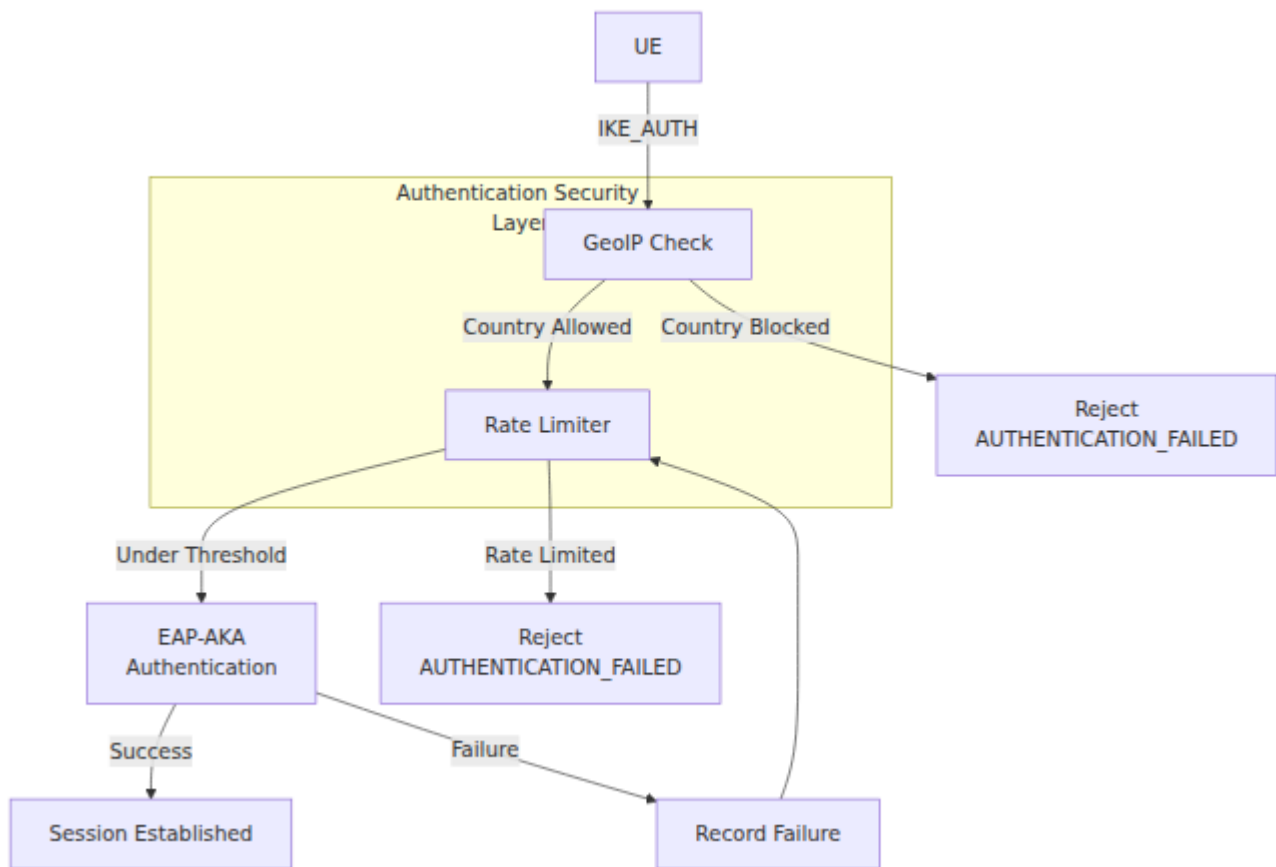
أمان المصادقة في OmniEPDG

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

جدول المحتويات

- نظرة عامة
- تحديد معدل المصادقة
- GeolIP حظر الدول باستخدام
- تدفق الأمان
- المقاييس
- استكشاف الأخطاء وإصلاحها

نظرة عامة



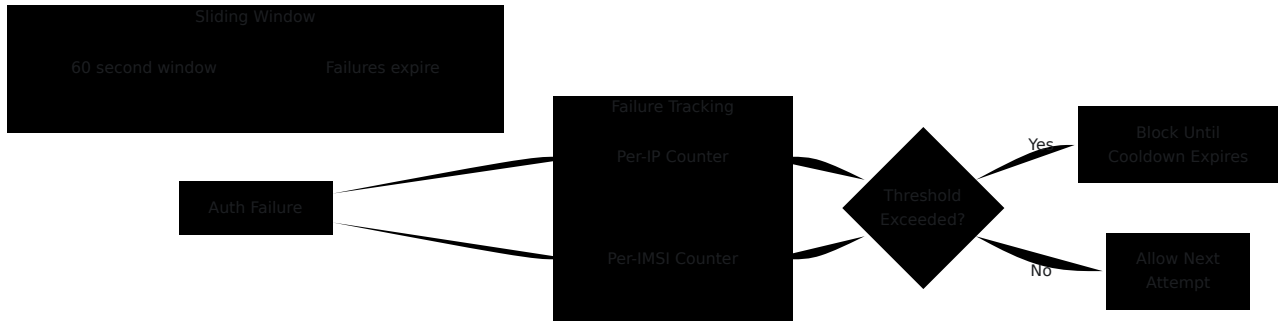
قبل العمليات التشفيرية، IKE_AUTH بإجراء فحوصات الأمان في بداية تبادل OmniEPDG تقوم المكلفة:

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

تحديد معدل المصادقة

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

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	فشل / 10 دقيقة	دقائق 5
Per-IMSI	يلتقط الهجمات المستهدفة على المشاركين المحددين	فشل / دقيقة 5	دقائق 10

يجب أن تمر كلت **❖❖** 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)
```

Per-IP معلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
auth_rate_limit_per_ip	عدد صحيح	لا	10	الحد الأقصى لمحاولات المصادقة الفاشلة المسموح بها من IP عنوان واحد خلال فترة النافذة قبل الحظر.
auth_rate_limit_ip_window_ms	عدد صحيح	لا	60000	حجم النافذة المنزلقة بالمللي ثانية لعد الفشل في IP. الفشل الأقدم من  لك لا يتم احتسابه.
auth_rate_limit_ip_block_ms	عدد صحيح	لا	300000	مدة الحظر بالمللي ثانية لعنوان IP بعد تجاوز العتبة. الافتراضي

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				هو 5 دقائق.

Per-IMSI معالمات

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 بعد IMSI تجاوز العتبة. الافتراضي هو 10

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

السلوك عند النجاح

وهذا IP/IMSI. عند نجاح المصادقة، يقوم محدد المعدل بمسح جميع سجلات الفشل لذلك الزوج من يسمح للمستخدمين 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
```

خلال نافذة مدتها دقيقتان. IMSI أو 3 فشل لكل IP **كيف يعمل**: يُسمح فقط بـ 5 فشل لكل 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
```

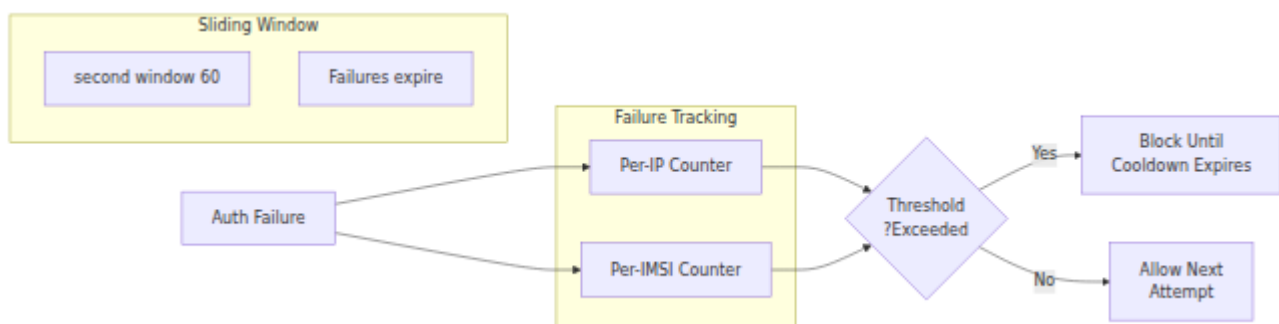
كيف يعمل: عتبات أعلى وحظورات أقصر تسمح بمزيد من المرونة في الاختبار.

حالة الاستخدام: بيئات التطوير، اختبار التكامل.

GeoIP حظر الدول باستخدام

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

نظرة عامة



IP قاعدة بيانات تحديد موقع

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

mix يتم تنزيلها عند الطلب عبر اختصار). إصدار، لذا يتم شحن كل حزمة بقاعدة بيانات حالة 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.
- فقط فيما إذا كانت الاتصالات محظورة حسب الدولة. يتم geoip_enabled يتحكم 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>) DB-IP/MaxMind MMDB. إذا كانت الملف المحدد مفقودًا، يتم استخدام البيانات المدمجة (المحملة). ملاحظة: لا تسمح اتفاقية استخدام MaxMind GeoLite2 قًا البيانات المدمجة (المحملة). ملاحظة: لا تسمح اتفاقية استخدام بدلاً من ذلك (CC BY 4.0) DB-IP Lite بإعادة توزيعها داخل منتج، ولهذا السبب يتم استخدام

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

```
mix geoip.fetch
```

التكوين

```
config :omniepdg,  
  # حظر الاتصالات حسب الدولة (تحديد الموقع الجغرافي دائمًا مفعّل)  
  geoip_enabled: true,  
  
  # MMDB اختياري: تجاوز قاعدة البيانات المدمجة بقاعدة بيانات  
  # الخاصة بك (دولة أو مدينة)  
  # 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"],  
  
  # غير المعروفة IPs التعامل مع  
  geoip_allow_unknown: false,  
  
  # السلوك عند عدم توفر قاعدة البيانات  
  geoip_fail_open: true
```

المعلومات

المعلومة	النوع	مطلوب	الافتراضي	الوصف
<code>geoup_enabled</code>	Boolean	لا	<code>false</code>	تمكين أو تعطيل التحكم في الوصول القائم على GeolP * عندما (الحظر). <code>false</code> تكون، يتم السماح IP، بجميع عناوين ولكن تظل الجلسات محددة جغرافيًا.
<code>geoup_database_path</code>	String	لا	قاعدة البيانات المدمجة <code>dbip-country-lite.mmdb</code>	مسار لقاعدة بيانات بتنسيق MMDB (دولة أو مدينة) يتراجع إلى قاعدة بيانات المدمجة DB-IP إذا لم يتم تعيينها أو كانت مفقودة.
<code>geoup_mode</code>	Atom	لا	<code>:whitelist</code>	وضع التحكم في الوصول: <code>:whitelist</code> (يسمح فقط) (بالدول المدرجة) أو <code>:blacklist</code> (يمنع الدول) (المدرجة، ويسمح بالباقي).
<code>geoup_countries</code>	List	لا	<code>[]</code>	قائمة رموز الدول ISO 3166-1

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

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

لمناطق الخدمة المرخصة WiFi **حالة الاستخدام**: المشغلون الذين يرغبون في تقييد مكالمات 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

:لا يمكن تحديد موقعها IP بعض عناوين

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

:في السلوك `geoip_allow_unknown` تتحكم معلمة

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

لتجاوز الافتراضي:

```
config :omniepdg,
  geoip_mode: :whitelist,
  geoip_allow_unknown: true # غير المعروفة حتى IPs الـ 0000 بالـ #
  في وضع القائمة البيضاء
```

تحديثات قاعدة البيانات

أسبوعيًا. للتحديث GeoLite2 بتحديث قاعدة بيانات MaxMind تقوم

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

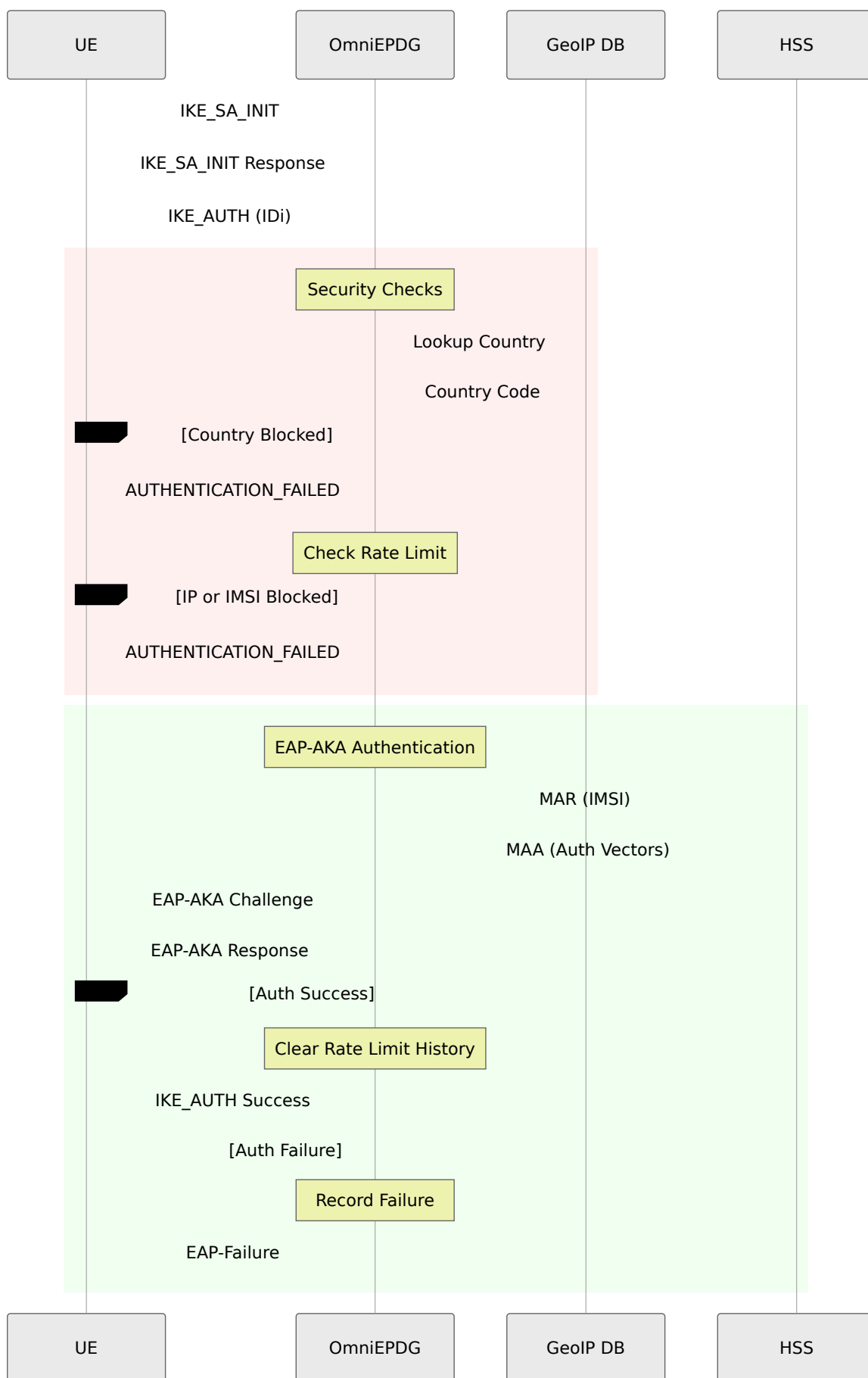
رموز الدول الشائعة

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



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` (IP تم تجاوز عتبة) أو `imsi` (IMSI تم تجاوز عتبة)

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
```

GeoIP مقاييس

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

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

استعلامات المثال:

```
# في الدقيقة GeoIP حظر
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. المتأثر IP/IMSI تحقق من المقاييس لعنوان
2. اعتبر زيادة العتبات إذا كانت الإيجابيات الكاذبة شائعة
3. بعد إصلاح السبب الجذري، ستنتهي الحظر تلقائيًا

ارتفاع معدل المحاولات المحظورة

تزداد بسرعة `epdg_auth_rate_limited_count`: **الأعراض**

الأسباب المحتملة:

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

الحل:

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

GeolP مشكلات

حظر جميع الاتصالات

GeolP الاتصال بعد تمكين UE **الأعراض**: لا يمكن لأي

الأسباب المحتملة:

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

الحل:

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

لا يتم تحميلها GeolP قاعدة بيانات

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

الأسباب المحتملة:

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

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. MaxMind تحقق من سلامة الملف عن طريق تنزيل نسخة جديدة من

حظر دول غير متوقعة

الأعراض: يتم حظر المستخدمين من الدول المسموح بها

:الأسباب المحتملة

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

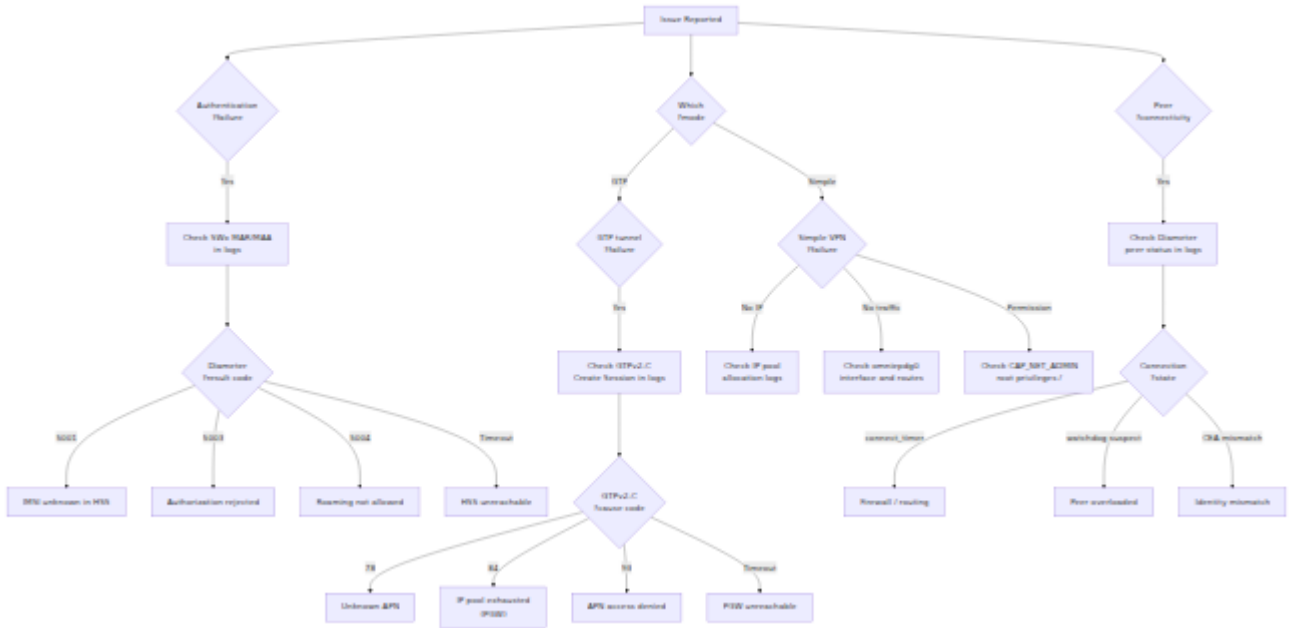
:الحل

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

استكشاف أخطاء وإصلاحها OmniEPDG

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

نظرة عامة على التشخيص



ملفات السجل

بالنسبة لدليل العمل الخاص بالتطبيق، راجع [مرجع log/](#) السجلات إلى الدليل OmniEPDG تكتب [التكوين](#) للحصول على تفاصيل تكوين السجل.

الهدف	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	OTP أعطال عملية	عندما يتم إعادة تشغيل العمليات بشكل غير متوقع
log/erlang.log	Erlang مسجل نواة	على Erlang/OTP مشكلات مستوى منخفض

أنماط السجل الرئيسية

Diameter أحداث اتصال نظير:

- peer_up - تبادل القدرات Diameter تم الاتصال بنظير
- peer_down - Diameter تم قطع الاتصال بنظير

FSM UE انتقالات حالة:

- ue_fsm state_<name> event=<event> - FSM معالجة حدثًا في حالة معينة
- ue_fsm init(<IMSI>) - للمشارك FSM تم إنشاء مثل جديد من
- terminating epdg_ue_fsm with reason <reason> - FSM إيقاف تشغيل

أحداث انتهاء الوقت:

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

Diameter مشكلات الاتصال

HSS (SWx) فشل الاتصال بـ

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

الأسباب المحتملة:

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

الحل:

1. HSS و منفذ IP تحقق من الاتصال الشبكي بعنوان
2. يتطابقان مع تكوين dia_swx_remote_ip و dia_swx_remote_port تأكد من أن HSS
3. مسموح بها عبر جميع الجدران النارية. إذا تم حظر SCTP تحقق من أن حركة مرور SCTP كخيار احتياطي tcp إلى dia_swx_proto قم بتعيين
4. هو اسم نطاق مؤهل يمكن حله ويتطابق مع dia_swx_origin_host تحقق من أن HSS ما يتوقعه
5. Diameter CER/CEA لعمليات التفاوض الفاشلة لـ HSS تحقق من سجلات

PGW (S6b) فشل الاتصال بـ

تظهر PGW. من AAR أو لا ❖❖ صل GTP **الأعراض:** تنجح المصادقة ولكن فشل إنشاء نفق S6b. L peer_up السجلات عدم وجود حدث

الأسباب المحتملة:

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

الحل:

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

Diameter فشل مراقبة

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

الأسباب المحتملة:

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

الحل:

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

IKEv2 فشل مفاوضة

لا اقتراح مختار

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

الأسباب المحتملة:

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

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

الحل:

1. UE الخاص بـ SA لتحميل IKEv2 packet وتفقد حدث debug: قم بتمكين تسجيل التحويلات المعروضة بالضبط payloads[].proposals[] تسرد حقول المعروضة تظهر كمدعومة في جداول DH / PRF / تأكد من أن التشفير / النزاهة. 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)

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

الأسباب المحتملة:

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

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

الحل:

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

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

فشل المصادقة

(Diameter 5001) غير معروف IMSI

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

الأسباب المحتملة:

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

الحل:

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

(Diameter 5003) تم رفض التفويض

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

الأسباب المحتملة:

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

الحل:

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

(Diameter 5004) التجوال غير مسموح

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

الأسباب المحتملة:

- ترفض ❖❖ وقع المشارك الحالي HSS سياسة التجوال في
- غير مسموح به للمشاركين المتجولين WiFi الاتصال عبر

الحل:

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

انتهاء وقت المصادقة

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

الأسباب المحتملة:

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

الحل:

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

EAP-AKA عدم تطابق نوع

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

الأسباب المحتملة:

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

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

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

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

الحل:

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

EAP-AKA RES عدم تطابق

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

الأسباب المحتملة:

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

الحل:

1. صالحة وليست تالفة SIM تحقق من أن بطاقة

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

(فقط GTP وضع) GTP فشل نفق

PGW تم رفض إنشاء الجلسة بواسطة

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

رموز الأسباب الشائعة والإجراءات:

رمز السبب	الاسم	الإجراء
78	مفقود أو غير APN معروف	ويتطابق مع ملف PGW على APN تحقق من تكوين تعريف المشترك
82	RAT مرفوض في	تسمح بنوع الوصول PGW تحقق من أن سياسة GPP (غير 3) WiFi عبر
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	غير معروف IMSI/IMEI	؛ تحقق من أن PGW المشترك غير معروف لـ تم تفويضها S6b 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: Timeout يتعطل إنشاء النفق لمدة 10 ثوانٍ ثم يفشل. تظهر السجلات `create_session_timeout` في `state_wait_create_session_resp`.

الأسباب المحتملة:

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

الحل:

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

لا ينقل الحركة GTP-U نفق

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

الأسباب المحتملة:

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

الحل:

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

البسيط VPN وضع) البسيط VPN فشل فقط

TUN لم يتم إنشاء واجهة

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

الأسباب المحتملة:

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

الحل:

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

IP نفاذ مجموعة

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

الأسباب المحتملة:

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

الحل:

1. النشطة مقارنة بحجم المجموعة epdg_ue_fsm تحقق من عدد عمليات
2. (تحقق من رسائل السجل) تحقق من أنه يتم إنهاء الجلسات بشكل صحيح (terminating)
3. أكبر في CIDR إذا كانت المجموعة ممتلئة حقًا، قم بتوسيعها باستخدام بادئة (simple_vpn_pool_ipv4 (يتطلب إعادة تشغيل)
4. التي قد تكون log/crash.log أثناء إنهاء الجلسة في FSM تحقق من وجود أعطال IP منعت تحرير

حركة مرور المشترك لا تتدفق

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

الأسباب المحتملة:

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

الحل:

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

طرق قديمة بعد العطل

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

الأسباب المحتملة:

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

الحل:

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

مشكلات إنهاء الجلسة

يتعطل إنهاء الجلسة أثناء إلغاء التسجيل

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

الأسباب المحتملة:

- لا يستجيب لطلب حذف الجلسة PGW
- ASR أو STR لا يستجيب لـ Diameter نظير
- 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. HSS و PGW تحقق من الاتصال بـ.
3. وواصل الخطوة التالية لإنهاء الجلسة أو إنهاؤها. إذا لم FSM بعد 10 ثوانٍ، يجب أن ينتهي Unexpected call event يحدث ذلك، تحقق من الأحداث غير المتوقعة المسجلة كـ

التيمة PDP GTP-U سياقات

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

الأسباب المحتملة:

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

الحل:

1. بحثًا عن أعطال العمليات أثناء إنهاء الجلسة log/crash.log تحقق من
2. FSM إذا تم قتل PDP تنظيف سياق FSM الخاصة بـ terminate/3 تحاول وظيفة قد يكون قد تم تخطي التنظيف، (على سبيل المثال، إعادة تشغيل المشرف)
3. السياقات القديمة []وت GTP-U إنشاء مقبس OmniEPDG ستعيد إعادة تشغيل.