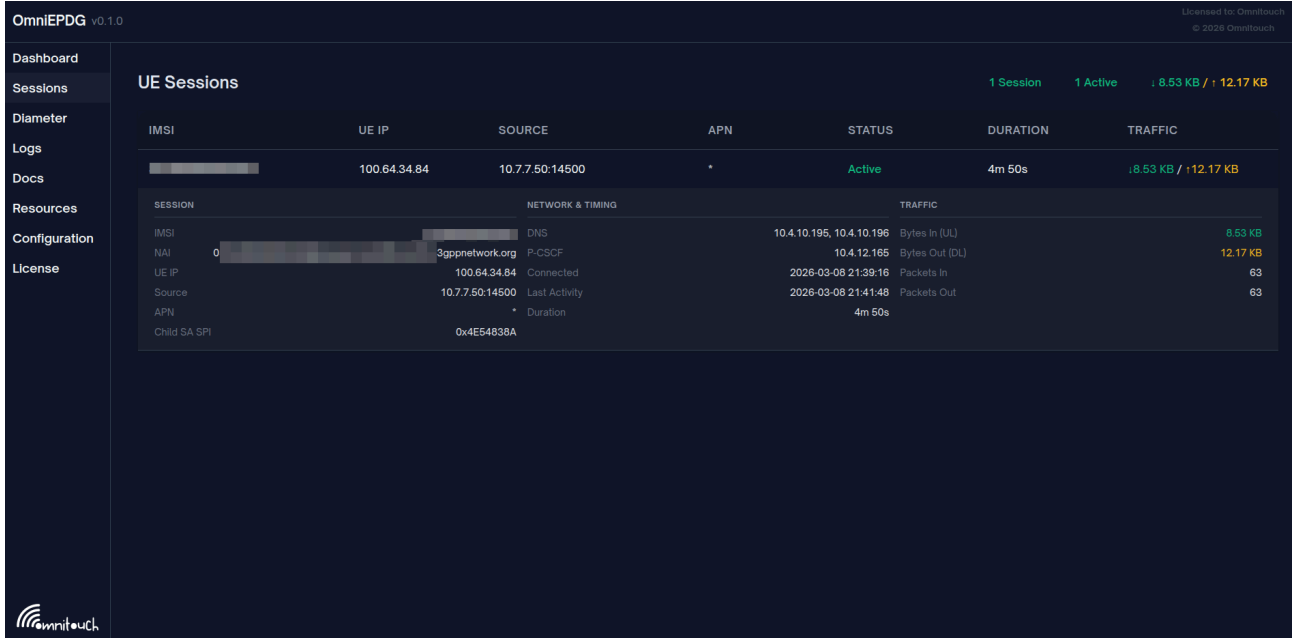


OmniEPDG دليل تشغيل

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



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

SESSION	NETWORK & TIMING	TRAFFIC		
IMSI	DNS	10.4.10.195, 10.4.10.196	Bytes In (UL)	8.53 KB
NAI	P-CSCF	10.4.12.165	Bytes Out (DL)	12.17 KB
UE IP	Connected	2026-03-08 21:39:16	Packets In	63
Source	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 OmniEPDG لوحة التحكم الخاصة بـ الوقت الحقيقي.

وضعين تشغيليين OmniEPDG يدعم

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

الوثائق

التكوين والعمليات

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

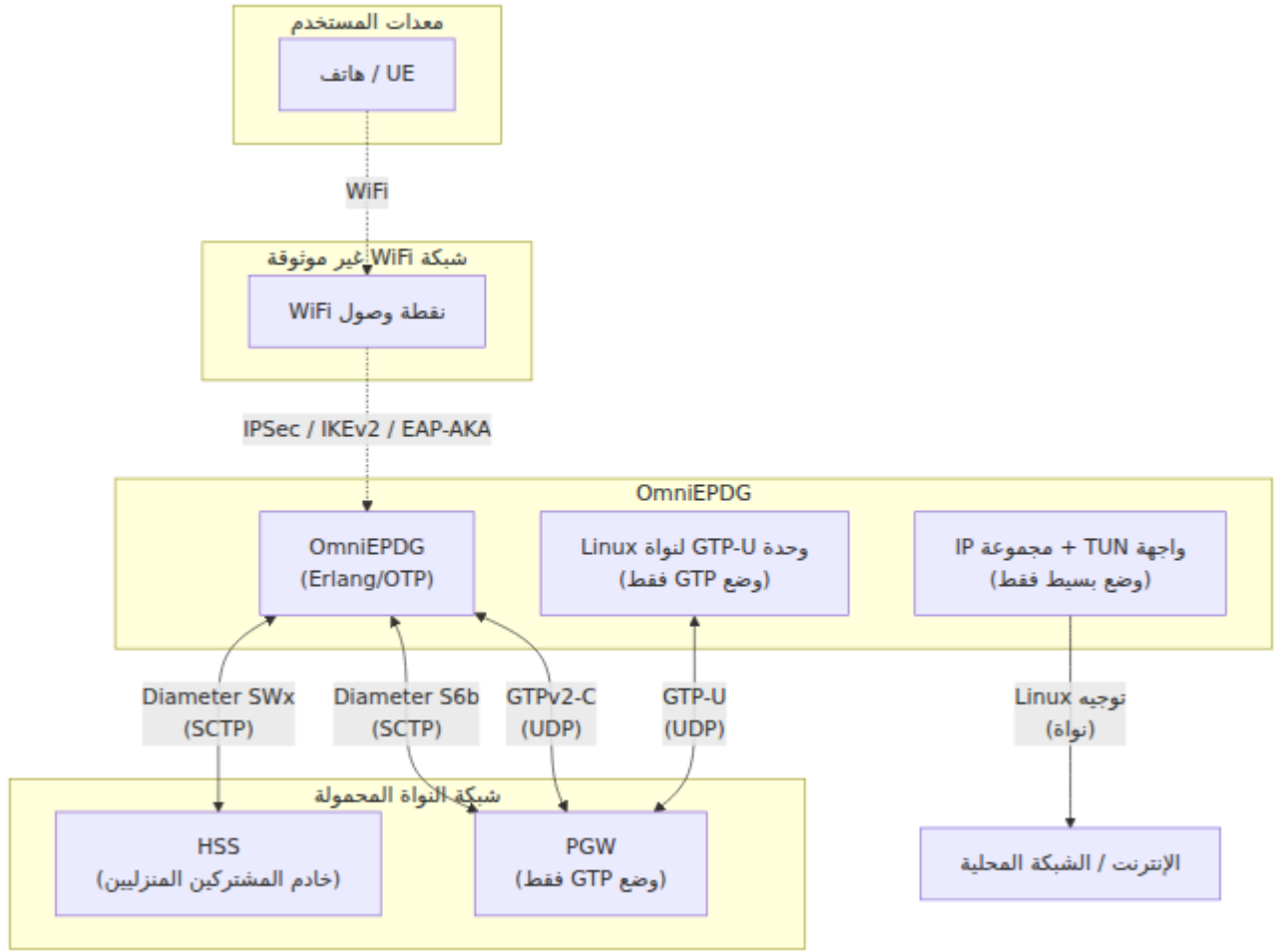
الأمان

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

المراقبة واستكشاف الأخطاء وإصلاحها

- لمراقبة المصادقة، والجلسات، وإشارات Prometheus **مرجع المقاييس** - مقاييس 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 لطبقة المستخدم. هذا متوافق (Linux عبر وحدة نواة) GTP-U للتحكم في الجلسات و GTPv2-C الحالية EPC مناسب لنشر شركات الاتصالات مع بنية GPP تمامًا مع 3.

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

بنية التحتية المطلوبة: HSS, PGW

بسيط VPN وضع

من مجموعة محلية وبوجه حركة مرور المشتركين مباشرة IP بتخصيص عناوين OmniEPDG يقوم أو بنية PGW باستخدام توجيه النواة القياسي. لا حاجة لـ (tun_epdg) Linux TUN عبر 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 لـ) فقط HSS: **البنية التحتية المطلوبة**

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

مقارنة الأوضاع

القدرة	GTP وضع	بسيط VPN وضع
GPP متوافق مع 3	نعم	جزئي، (مع skip_sar) لا (بدون)
PGW مطلوب	نعم	لا
HSS مطلوب	نعم	نعم (للمصادقة فقط)
IP تخصيص	PGW من	(CIDR) مجموعة محلية
طبقة المستخدم	لنواة GTP-U وحدة Linux	توجيه + Linux TUN
دفع الملف الشخصي HSS	نعم (PPR/PPA)	لا
HSS إلغاء تسجيل	نعم (RTR/RTA)	لا (مع skip_sar)
PGW إنهاء مبدوء من	نعم	غير متاح
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 القسم 8	متجهات المصادقة وتعيين الخادم	HSS	كلاهما	SCTP	Diameter	SWx
3GPP TS 29.273 القسم 9	تفويض الجلسة والسياسة	PGW	GTP فقط	SCTP	Diameter	S6b
3GPP TS 29.274	التحكم في النفق وطبقة المستخدم	PGW	GTP فقط	UDP	GTPv2-C / GTP-U	S2b

الميزات

الوظائف الأساسية

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

GTP ميزات وضع

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

- يقوم بإنهاء ePDG ، طلب حذف الحامل PGW يرسل - **PGW إنهاء مبدوء من** UE الجلسة إلى
- يقوم بإنهاء ePDG ، 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 **القسم 7.1.2.5.1 TS 29.273**

بسيط VPN ميزات وضع

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

ميزات الأمان

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

HSS (SWx Diameter) تكامل

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

(فقط GTP وضع) PGW تكامل

Diameter S6b:

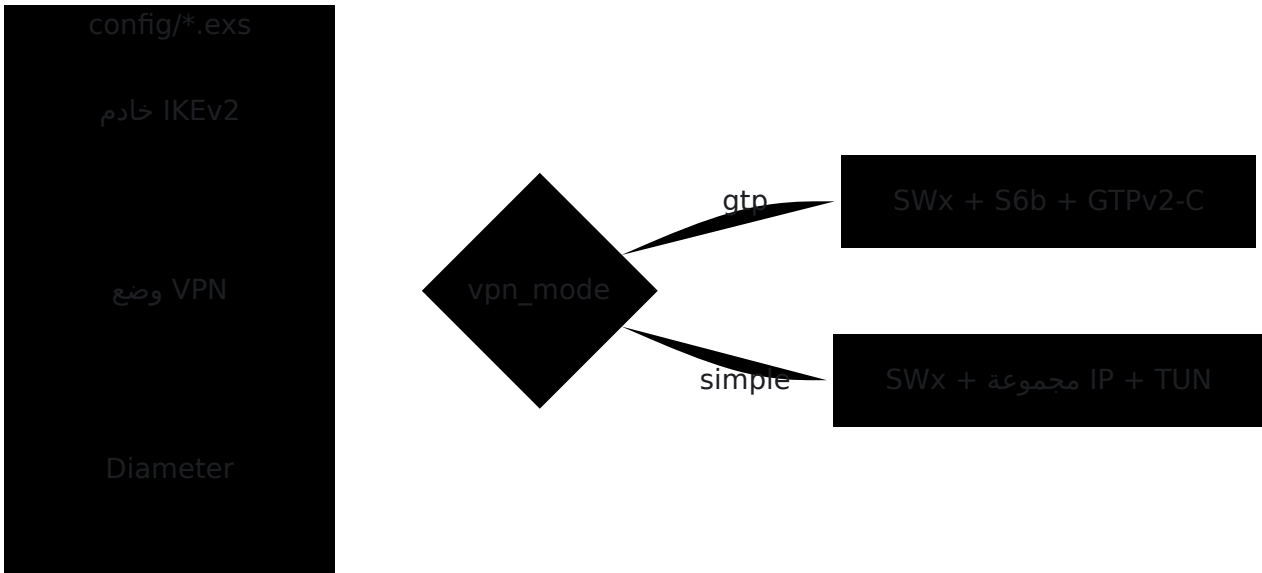
- PGW تفويض جلسات - AA (AAR/AAA) طلب/إجابة
- PGW إنهاء جلسات - (STR/STA) طلب/إجابة إنهاء الجلسة
- إعادة تفويض الجلسات النشطة - (RAR/RAA) طلب/إجابة إعادة التفويض
- إنهاء الجلسات بالقوة - (ASR/ASA) طلب/إجابة إنهاء الجلسة

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

البدء السريع

هيكل التكوين



بين `vpn_mode` أو عبر متغيرات البيئة. يحدد معلمة `config/runtime.exs` يتم التكوين في `config/runtime.exs` في البسيط. انظر مرجع التكوين لوثائق المعلمات الكاملة 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 و S6b 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 ل UE	10.45.0.0/16	قابلة للتكوين لعناوين CIDR مجموعة المشتركين
HSS	10.74.0.21:3868	(للمصادقة فقط) Diameter SWx نظير

3 GPP مواصفات

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

الوثائق حسب الدور

مشغلو الشبكة:

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

مدمجو الأنظمة:

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

OmniEPDG دليل عمليات

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

روابط سريعة

التكوين والنشر

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

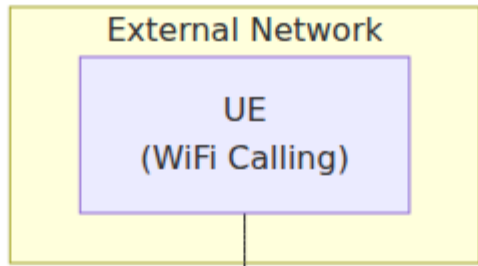
العمليات والمراقبة

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

الأمان

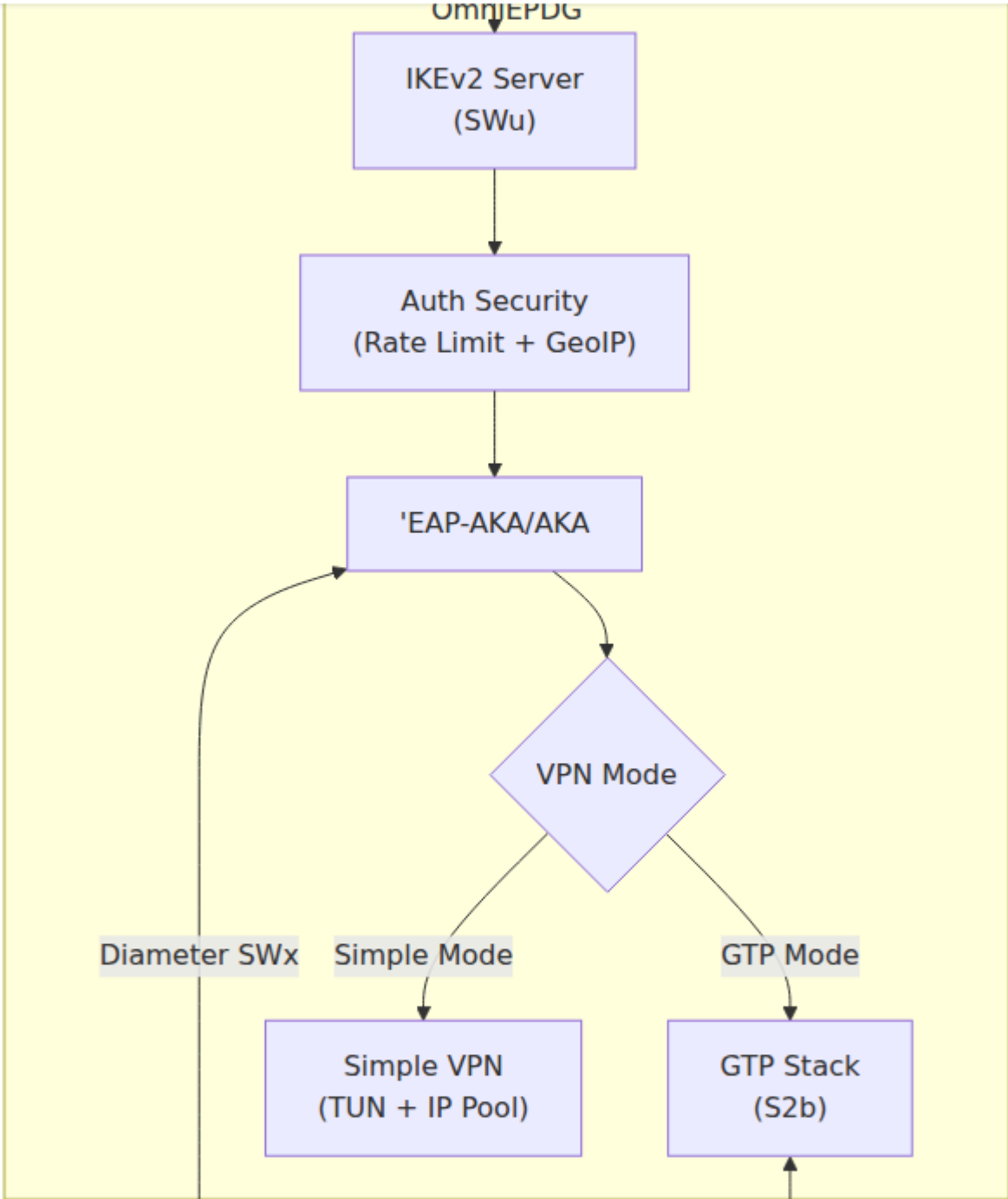
- GeoIP **أمان المصادقة** - تحديد المعدل وحظر الدول عبر

نظرة عامة على المعمارية



IKEv2

Platform OmniCharge OmniRAN OmniCall OmniCore OI
المنصة 5GC

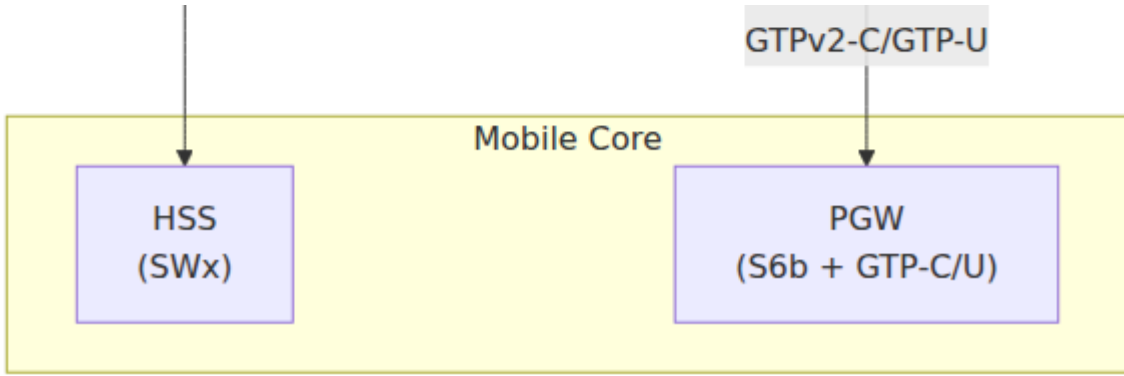


Diameter SWx

Simple Mode

GTP Mode

Diameter S6b



الأوضاع التشغيلية

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

GTP وضع

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

استخدم عندما:

- التكامل مع بنية الشبكة الأساسية المحمولة الحالية
- إدارة الجلسات (إنشاء/حذف/تعديل الجلسة) GTPv2-C
- مطلوب التجوال والتسليم بين المشغلين

المكونات:

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

بسيط VPN وضع

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

استخدم عندما:

- PGW نشر مستقل دون
- الاختبار والتطوير

- سيناريوهات التفريغ المحلي

المكونات:

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

أمان المصادقة

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

تحديد المعدل

:يحمي من هجمات القوة الغاشمة عن طريق 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 الدول عبر

MaxMind GeoLite2: تحكم جغرافي اختياري باستخدام قاعدة بيانات

- **وضع القائمة البيضاء** - السماح فقط بالاتصالات من الدول المحددة
- **وضع القائمة السوداء** - حظر الاتصالات من الدول المحددة
- غير المعروف/الخاص IP معالجة قابلة للتكوين لعنوان
- سلوك الفشل المفتوح أو 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 توثيق كامل للمعلومات.

المراقبة

لوحة التحكم

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

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

راجع دليل **لوحة التحكم** للحصول على التفاصيل.

Prometheus قياسات

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

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

راجع **مرجع القياسات** للحصول على استعلامات وقواعد التنبيه.

استكشاف الأخطاء وإصلاحها

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
إيجابيا  كاذبة في تحديد المعدل	ضبط العتبات	مشكلات تحديد المعدل
GeolIP مشكلات حظر	تحقق من قاعدة البيانات ورموز الدول	GeolIP مشكلات

.راجع دليل استكشاف الأخطاء وإصلاحها للحصول على إجراءات تشخيصية مفصلة

فهرس الوثائق

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

بسيط VPN بنية وضع

لا Linux في TUN بسيط، يتم توجيه حركة مرور المشتركين محليًا عبر واجهة VPN في وضع GTP-U وGTPv2-C وDiameter S6b يتم استبدال مكونات 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
لأغراض المصادقة وعمليات HSS يتصل بـ ملف المشترك	Diameter عميل SWx	aaa_diameter_swx
session Diameter و EAP يوجه رسائل AAA وآلات حالة ePDG بين	SWm Diameter (داخلي)	aaa_diameter_swm
من إشارات ePDG يتعامل مع جانب Diameter الداخلية SWm	SWm معالج ePDG	epdg_diameter_swm

GTP: عمليات إضافية في وضع

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

بسيط VPN عمليات إضافية في وضع:

الوصف	الدور	العملية
IP يشرف على عمليات مدير مجموعة ومدير المسار	مشرف نظام VPN	simple_vpn_supervisor
من IPv4 يخصص ويفرج عن عناوين ETS المكونة باستخدام CIDR مجموعة	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 من آلات الحالة OmniEPDG ينشئ (IMSI معرف بواسطة) لكل مشترك نشط

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

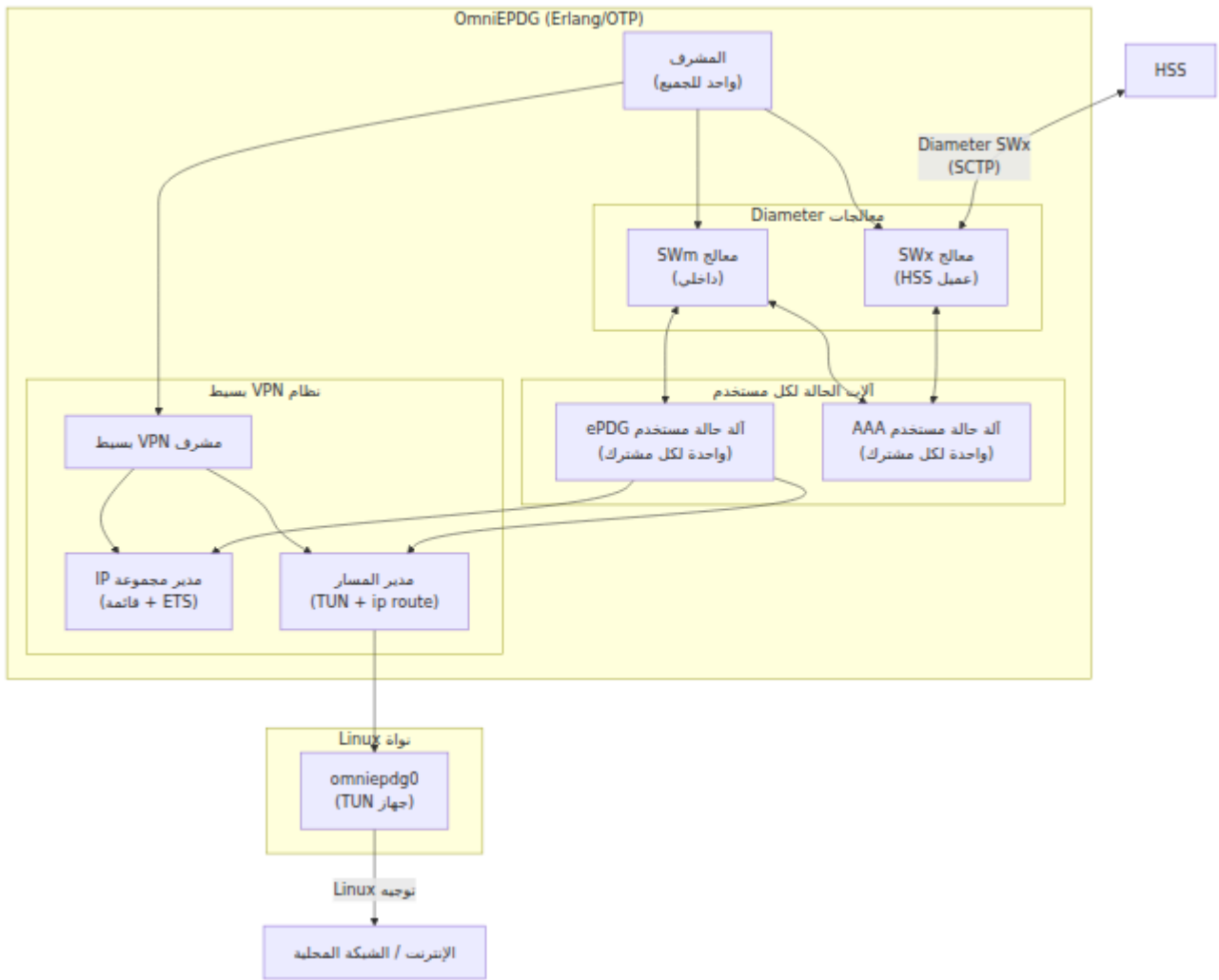
مع وضع رد نداء وظيفة الحالة Erlang في gen_statem تتم تنفيذ كلا الآلتين كعمليات

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 في حالة FSM سلوك diverge إلى الإنهاء. يت

FSM وضع GTP

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



بسيط VPN وضع FSM

بدلاً من إرسال طلب إنشاء `authenticated` اختصاراً في حالة FSM بسيط، تأخذ VPN في وضع من المجموعة المحلية، وإنشاء مسار مضيف على IP بتخصيص عنوان FSM تقوم GTPV2-C جلسة GTP لا يتم استخدام حالات الإنهاء الخاصة بـ `active`. وتنتقل مباشرة إلى TUN واجهة (`wait_create_session_resp`, `wait_delete_session_resp`, `dereg_pgw_wait_cancel`, `dereg_net_wait_s2b_delete`).



new

مهلة (10 ثواني)

خطأ SWm DEA

طلب المصادقة
(إرسال SWm DER)

الحالة الأولية

خطأ اكتمال المصادقة
SWm DEA

wait_auth_resp

طلب مصادقة جديدة
(إعادة المصادقة)

طلب مصادقة إضافي
(إرسال SWm DER)

نجاح SWm DEA
(تم استلام متجهات المصادقة)

طلب مصادقة جديدة
(إعادة المصادقة، إفراج عن
حذف المسار، IP)

authenticating

اكتمال المصادقة
SWm DEA
(تم استلام الملف الشخصي)

authenticated

طلب PurgeMS

طلب نقى
(إضافة مسار، IP، تخصيص)

active

طلب PurgeMS

طلب PurgeMS
(حذف المسار، إفراج عن IP)

تنشط TUN مسار

wait_swm_sta

مهلة (10 ثواني) تم استلام SWm STA



إرسال SWm STR

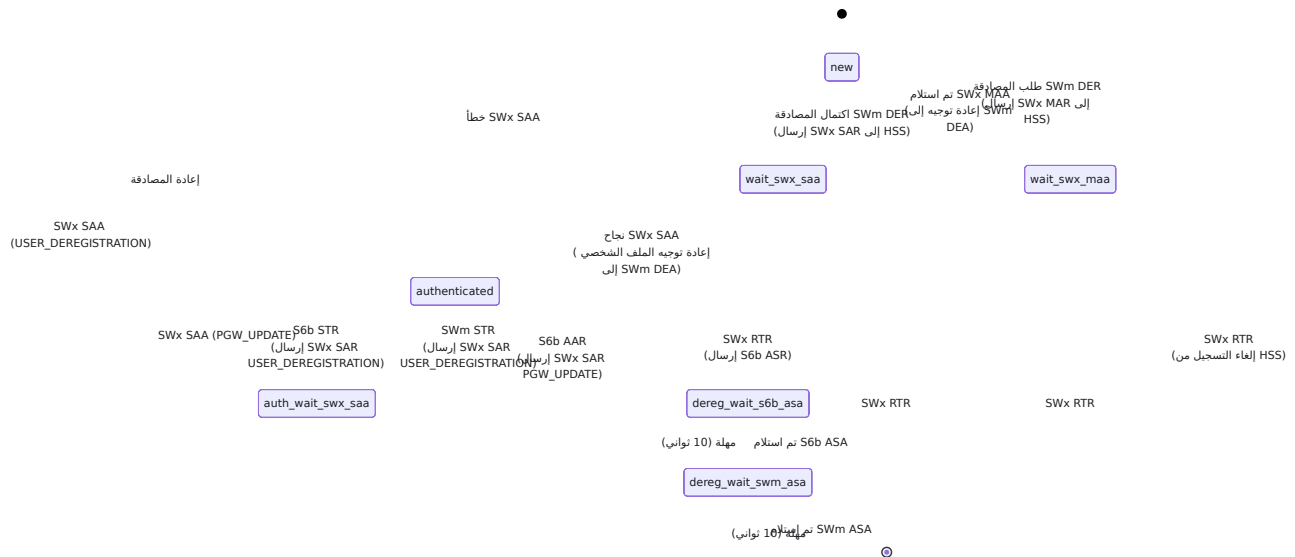
ePDG مرجع حالة آلة حالة مستخدم

الانتظار لـ	الوصف	الوضع	الحالة
طلب المصادقة من UE	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 / اكتمال المصادقة	تم استلام متجهات EAP المصادقة، تبادل جارٍ.	كلاهما	authenticating
طلب النفق من UE	اكتمال المصادقة، تم تنزيل ملف المشترك	كلاهما	authenticated
استجابة إنشاء الجلسة 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 حذف الجلسة من PGW	GTPv2-C Delete Session إلى PGW (UE إنهاء بدء).	GTP	wait_delete_session_resp
SWm STA من AAA	تم إرسال طلب إنهاء SWm جلسة.	كلاهما	wait_swm_sta
نتيجة إلغاء الموقع	إلغاء التسجيل الذي يبدأ تم إرسال PGW. من	GTP	dereg_pgw_wait_cancel

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

AAA حالات آلة حالة مستخدم

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



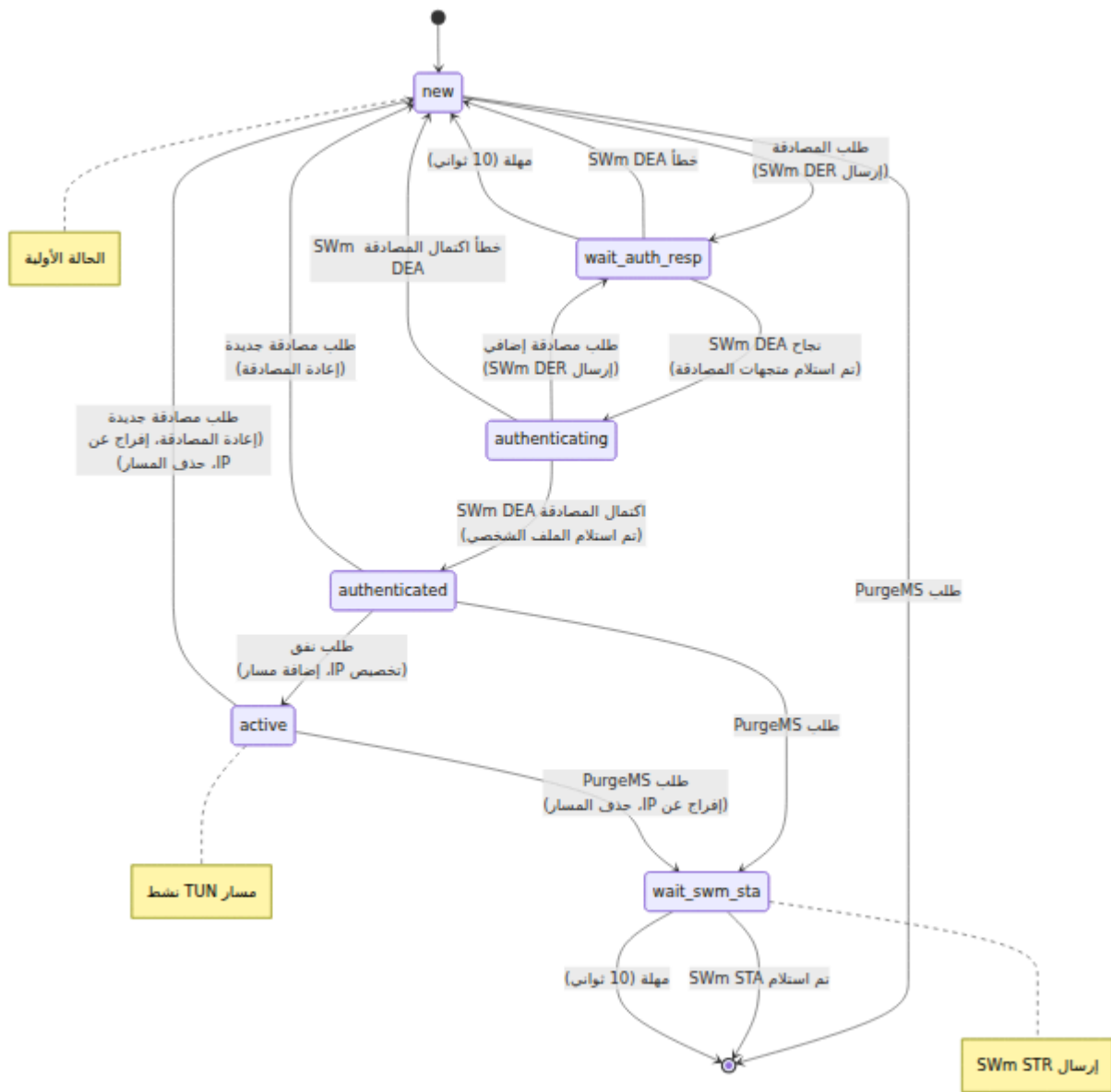
AAA مرجع حالة آلة حالة مستخدم

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

تدفقات المكالمات

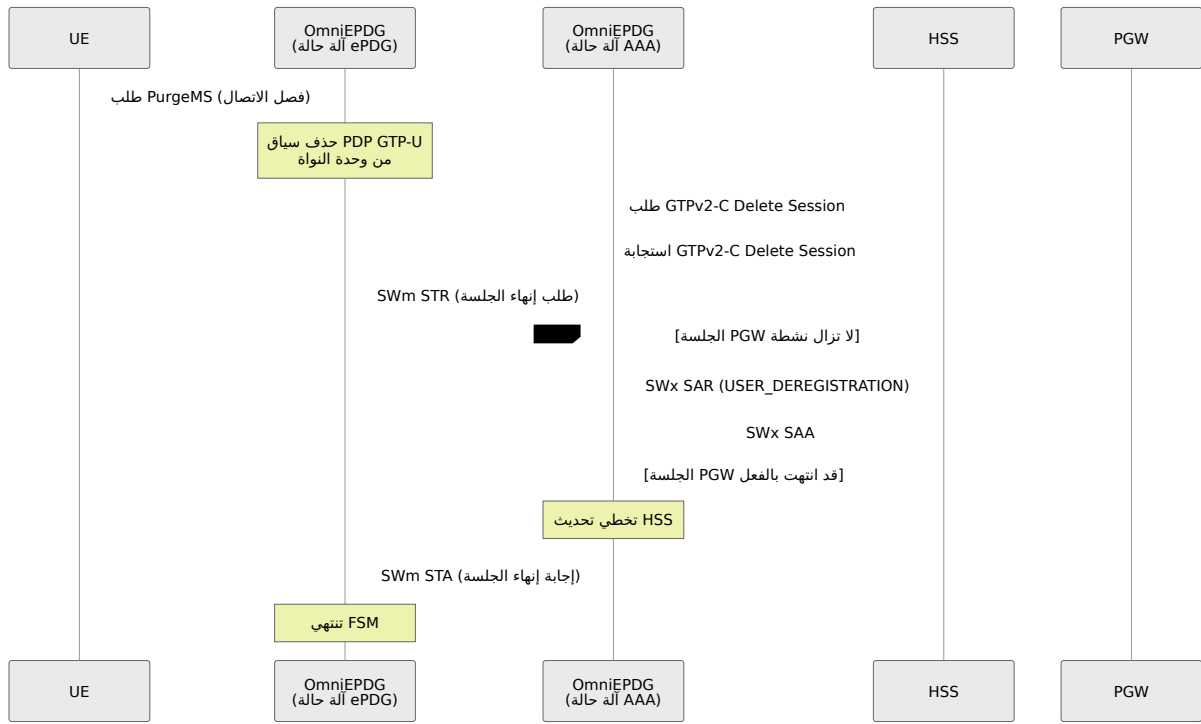
إنشاء جلسة ناجحة: GTP وضع

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



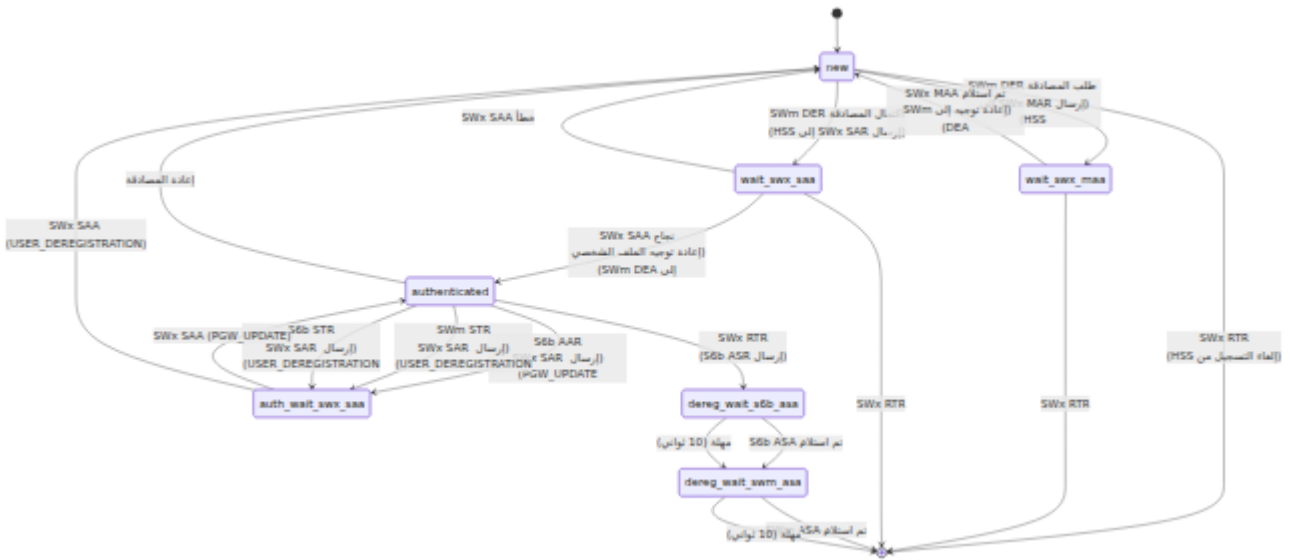
UE إنهاء الجلسة التي يبدأها GTP: وضع

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



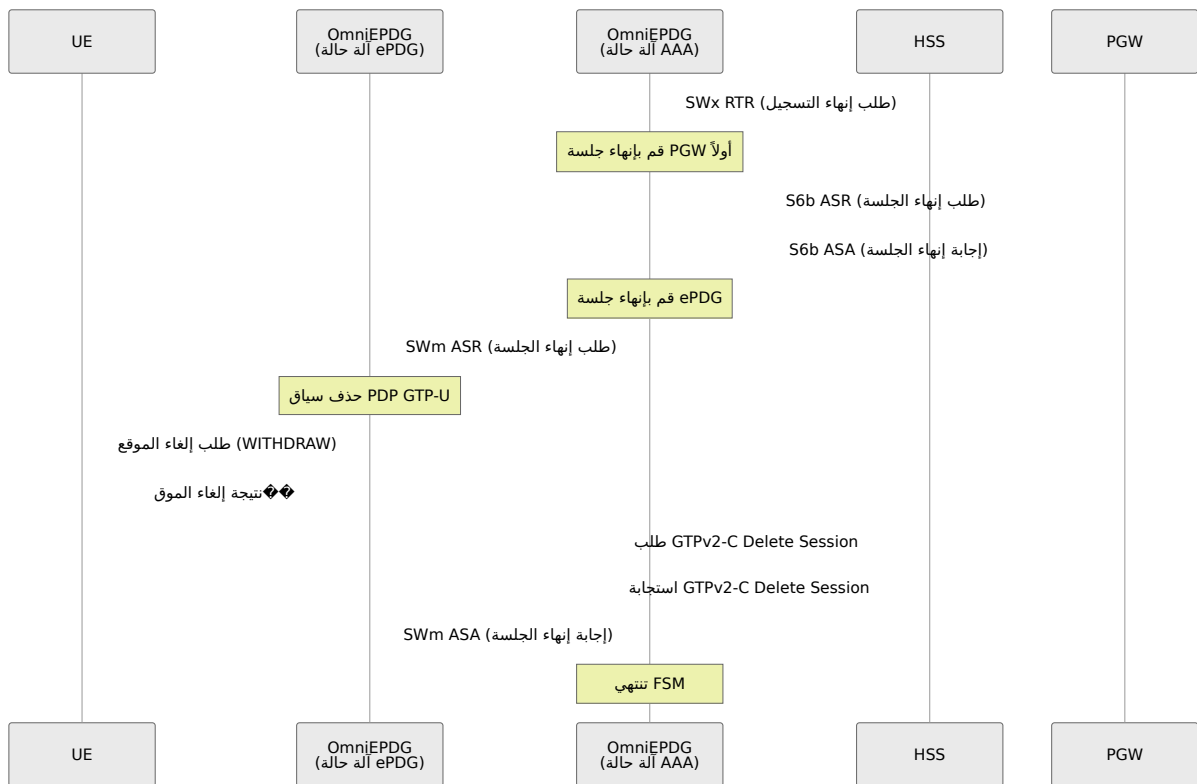
PGW إنهاء الجلسة التي يبدأها GTP: وضع

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



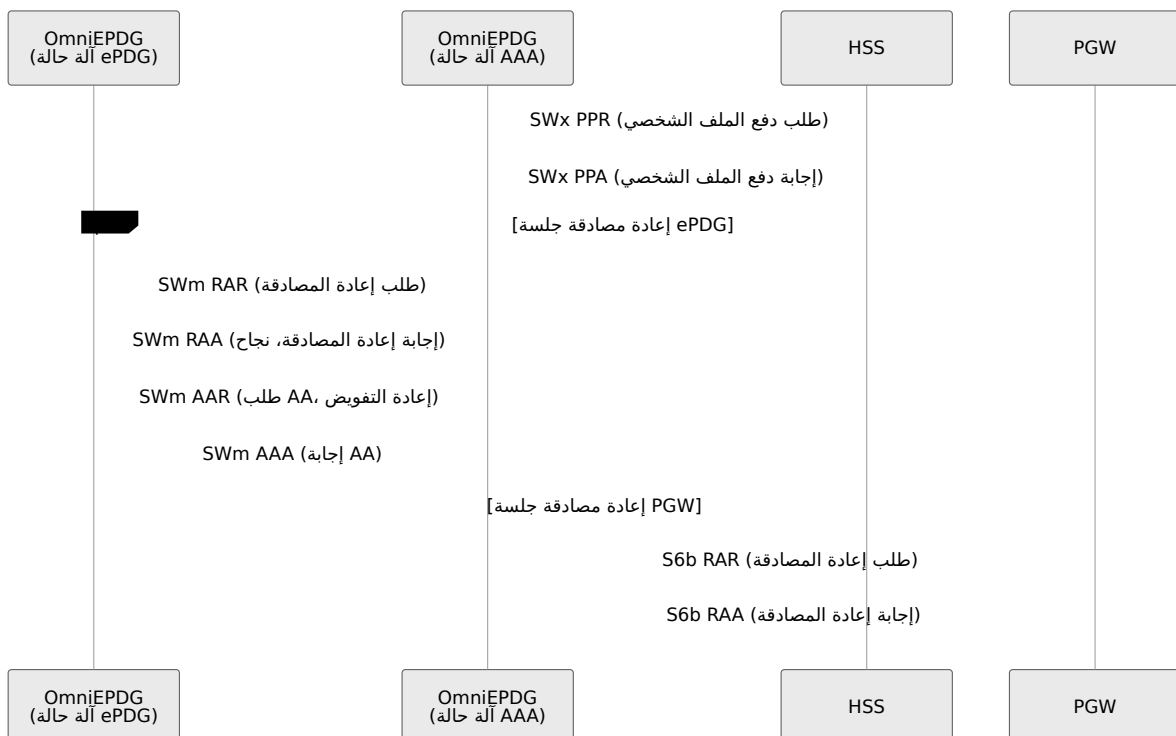
(HSS) إلغاء التسجيل الذي يبدأه الشبكة: وضع GTP

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



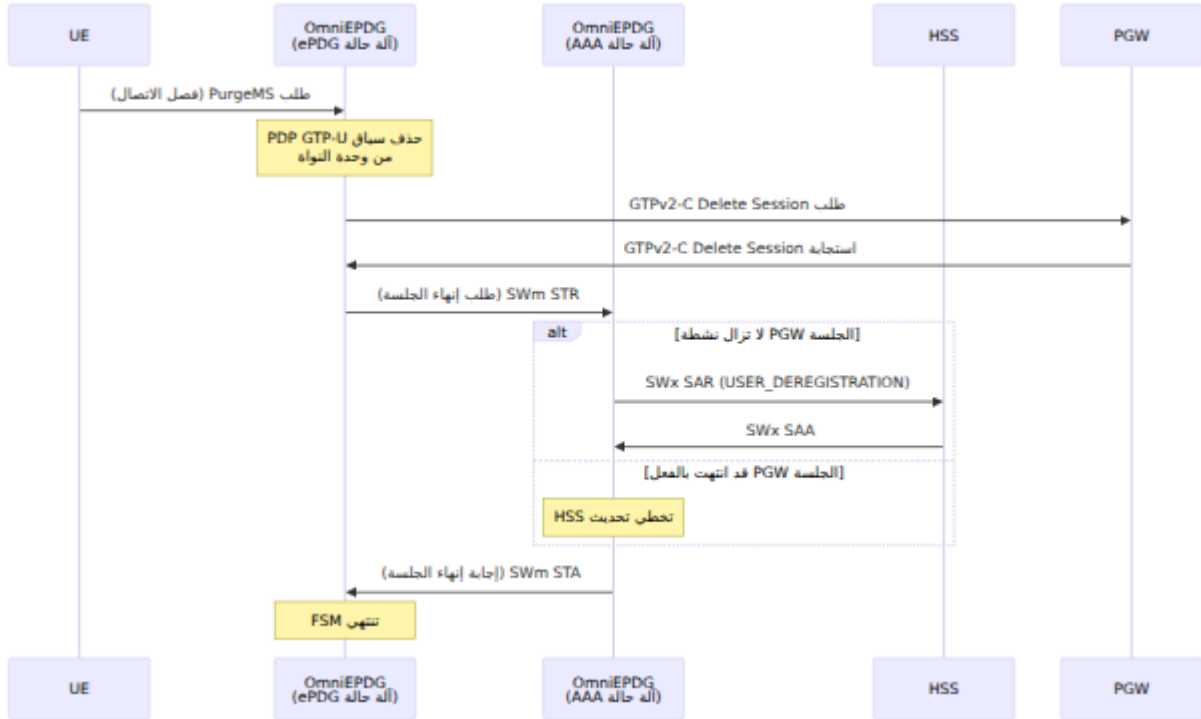
وإعادة المصادقة HSS دفع ملف تعريف: وضع GTP

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



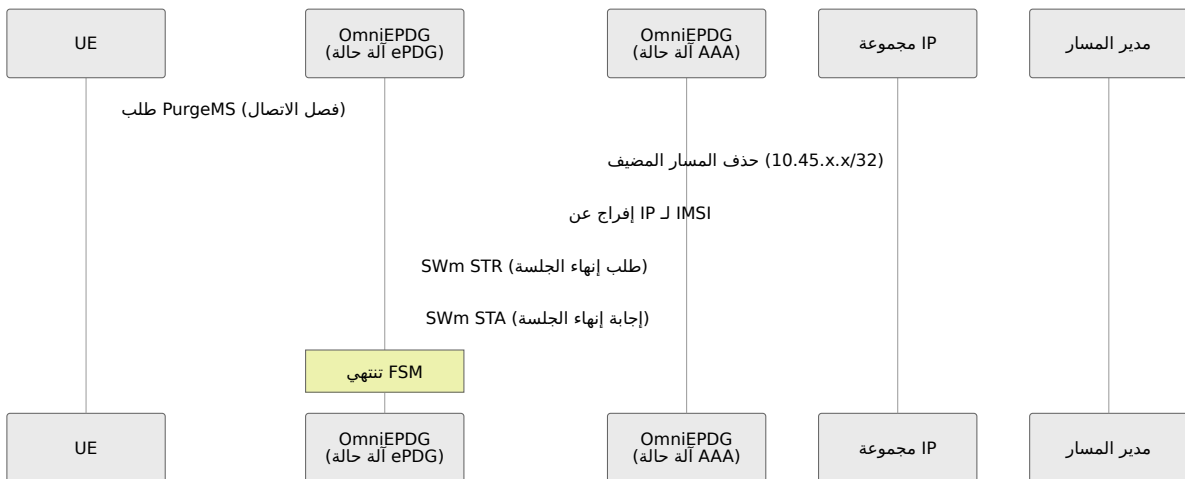
بسيط: إنشاء جلسة ناجحة VPN وضع

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



UE بسيط: إنهاء الجلسة التي يبدأها VPN وضع

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



Diameter معرفات تطبيق

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

Diameter رموز نتائج

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

رموز النت❖❖نج القياسية

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

GPP رموز النتائج التجريبية 3

رمز النتيجة	الاسم	المعنى	رجع
4181	DIAMETER_AUTHENTICATION_DATA_UNAVAILABLE	لا يمكن ل HSS 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 ل STR/AAR القديمة)	RFC 673
5003	DIAMETER_AUTHORIZATION_REJECTED	المشترك غير مصرح له بالخدمة	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 أسباب

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

أسباب النجاح

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

أسباب الخطأ (مختارة)

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

NAI تنسيق

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

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

بادئة الهوية ونوع المصادقة

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

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

البادئة 0 UE تستخدم 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 الخاصة بالمشارك IMSI استخدام.

الخوارزميات التشفيرية

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

IKEv2 خوارزميات ت ❖❖ فير

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
HMAC-SHA1-96	2	بت 160	بت 96	مدعوم (قديم)	RFC 2404
HMAC-MD5-96	1	بت 128	بت 96	مدعوم (قديم)	RFC 2403

خوارزميات PRF IKEv2

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

مجموعات Diffie-Hellman IKEv2

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

(الطفل SA) ESP خوارزميات

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

:الافتراضي ESP تكوين

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

EAP-AKA وظائف التشفير

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

EAP-AKA' وظائف التشفير

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

3 الامتثال لـ GPP

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

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

(فقط GTP وضع) PDP أنواع عنوان

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

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

OmniEPDG مرجع تكوين

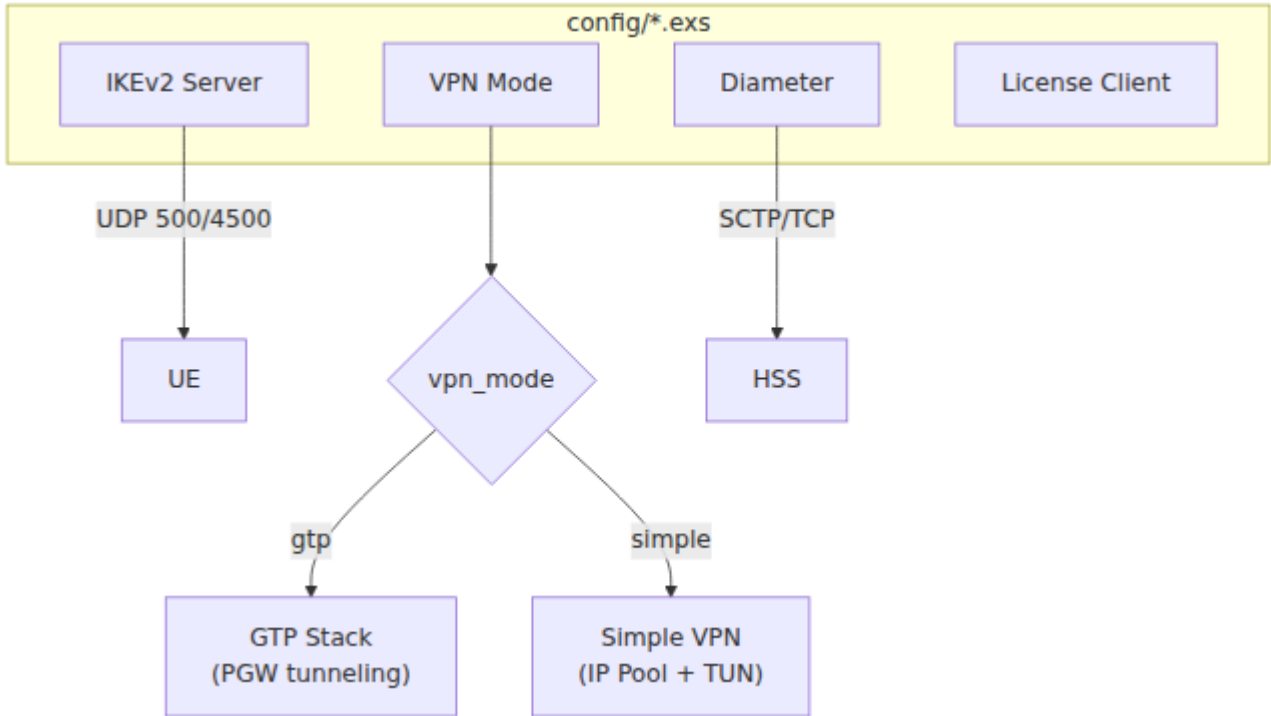
ومتغيرات البيئة. يتم إجراء جميع التكوينات عبر `config/runtime.exs` OmniEPDG يتم تكوين التي تواجه العملاء في وقت التشغيل - القيم الافتراضية في وقت الترجمة مضمنة في الإصدار. وليست مكشوفة.

بالنسبة للتوزيعات المعبأة في حاويات، استخدم متغيرات البيئة كما هو موضح في قسم [مرجع متغيرات البيئة](#).

جدول المحتويات

- [IKEv2 معلمات خادم](#)
- [معلمات أمان المصادقة](#)
- [VPN اختيار وضع](#)
- [بسيطة VPN معلمات](#)
- [Diameter معلمات](#)
- [تكوين عميل الترخيص](#)
- [تكوين لوحة التحكم](#)
- [Prometheus تكوين مقاييس](#)
- [مرجع متغيرات البيئة](#)
- [مرجع المهلة](#)

هيكل التكوين



ملف التكوين

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

مثال على التكوين

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

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

  # البسيط إعدادات VPN
  simple_vpn: [
    pool_ipv4: "10.45.0.0/16",
    pool_ipv6: "2001:db8::/32",
    dns_servers_ipv4: ["8.8.8.8", "8.8.4.4"],
    dns_servers_ipv6: ["2001:4860:4860::8888",
"2001:4860:4860::8844"]
  ]

# 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 معاملات خادم

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

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

المعلمة	النوع	مطلوب	الافتراضي
key_file	String	نعم	/etc/omniepdg/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 المعدل

```
config :omniepdg,  
  # تحديد المعدل لكل IP  
  auth_rate_limit_per_ip: 10,  
  auth_rate_limit_ip_window_ms: 60_000,  
  auth_rate_limit_ip_block_ms: 300_000,  
  
  # تحديد المعدل لكل IMSI  
  auth_rate_limit_per_imsi: 5,  
  auth_rate_limit_imsi_window_ms: 60_000,  
  auth_rate_limit_imsi_block_ms: 600_000
```

المعلمة	النوع	مطلوب	الافتراضي	لوصف
auth_rate_limit_per_ip	Integer	لا	10	الحد الأقصى لمحاولات لمصادقة الفاشلة لكل IP قبل الحظر.
auth_rate_limit_ip_window_ms	Integer	لا	60000	نافذة متحركة لحساب IP فشل (بالمللي ثانية).
auth_rate_limit_ip_block_ms	Integer	لا	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.
auth_rate_limit_imsi_window_ms	Integer	لا	60000	نافذة متحركة

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

معلومات GeolP

```
config :omniepdg,
  geolp_enabled: false,
  geolp_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",
  geolp_mode: :whitelist,
  geolp_countries: ["AU", "NZ"],
  geolp_allow_unknown: false,
  geolp_fail_open: true
```

المعلمة	النوع	مطلوب	الافتراضي
geoup_enabled	Boolean	لا	false
geoup_database_path	String	لا	"/etc/omniepdg/GeoLite2-Country.mmdb"
geoup_mode	Atom	لا	:whitelist
geoup_countries	List	لا	[]
geoup_allow_unknown	Boolean	لا	mode-dependent

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	<p>وضع التشغيل:</p> <p>:simple للاختراق المحلي عبر واجهة TUN, :gtp للتنقل عبر PGW عبر GTPv2-C/GTP-U. راجع دليل العمليات للحصول على مقارنة مفصلة.</p>

بسيطة VPN معلمات

OmniEPDG البسيط. يدعم VPN لوضع DNS و IP في تخصيص simple_vpn تتحكم كتلة تكوين IPv4 و IPv6 كل من مجموعات عناوين.

```
config :omniepdg,  
  simple_vpn: [  
    pool_ipv4: "10.45.0.0/16",  
    pool_ipv6: "2001:db8::/32",  
    dns_servers_ipv4: ["8.8.8.8", "8.8.4.4"],  
    dns_servers_ipv6: ["2001:4860:4860::8888",  
"2001:4860:4860::8844"],  
    p_cscf_ipv4: ["10.4.12.165"],  
    p_cscf_ipv6: [],  
    mtu: 1400,  
    nat_enabled: true  
  ]
```

المعلمة	النوع	مطلوب	الافتراضي	ف
pool_ipv4	String	نعم	"10.45.0.0/16"	موجة ناوين IPv4 سابق CIDF عيص لكل نترك
pool_ipv6	String	لا	"2001:db8::/32"	موجة ناوين IPv6 سابق CIDF بركين تثائيي كدس
dns_servers_ipv4	List	لا	["8.8.8.8", "8.8.4.4"]	توادم IPv4 مة ل UEs PCO رات) كوبن وكول
dns_servers_ipv6	List	لا	["2001:4860:4860::8888", "2001:4860:4860::8844"]	توادم IPv6 مة ل UEs PCO
p_cscf_ipv4	List	لا	[]	ناوين IPv4

المعلمة	النوع	مطلوب	الافتراضي	ف
				CSC Prox VoW مة ل UEs سجيل IMS.
p_cscf_ipv6	List	لا	[]	ناوين IPv6 CSC Prox VoW
mtu	Integer	لا	1400	قيمة واجهة القيم تقلل جزئة
nat_enabled	Boolean	لا	true	مكن مرور ركين. مكن، طبيق نواعد تمويه حركة مرور سادة

Diameter معلمات

عندما تكون (PGW) S6b و (HSS) SWx في واجهات Diameter يتحكم تكوين diameter_enabled true، يبدأ OmniEPDG كومة Diameter المكونة بالأفران المتصل.

```
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

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

معارف التطبيقات

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

تكوين عميل الترخيص

مقابل خادم الترخيص OmniEPDG يحقق عميل الترخيص من صحة

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

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

تكوين لوحة التحكم

توفر لوحة التحكم على الويب قدرات المراقبة والإدارة.

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

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

Prometheus تكوين مقاييس

للمراقبة والتنبيه عبر HTTP 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 ل 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 الطلبات - 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` - المخصصة (حسب النوع) IP عناوين
- `epdg_ip_released_count` - التي تم تحريرها (حسب النوع) IP عناوين

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` - المخصصة حاليًا IPs
- `epdg_ip_pool_available_count` - المتاحة في المجموعة IPs
- `epdg_ip_pool_utilization_ratio` - نسبة استخدام المجموعة (1.0-0.0)
- `epdg_diameter_swx_pending_count` - المعلقة SWx طلبات
- `epdg_diameter_s6b_active_sessions_count` - S6b الجلسات النشطة لـ

مقاييس الهستوغرام (تتبع الكمون)

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

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 الجارية
- `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. تتحكم هذه في المدة التي تنتظر فيها آلات الحالة للحصول FSM جميع مهلات على استجابات قبل اعتبارها فاشلة.

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

مرجع متغيرات البيئة

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

خادم IKEv2

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

VPN وضع

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

Diameter

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

HSS نظير

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

الترخيص، لوحة التحكم، والمقاييس

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

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"

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

لوحة التحكم OmniEPDG

Diameter، لوحة تحكم قائمة على الويب لمراقبة الجلسات، ونظراء OmniEPDG تتضمن سجلات 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 نظراء
- 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 نظراء	Diameter حالة اتصال نظراء
<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:

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

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

روابط سريعة

تنقل مباشر إلى العروض التفصيلية:

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

معلومات النظام

:يعرض التكوين التشغيلي الحالي

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

التحديث التلقائي

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

عرض الجلسات

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

OmniEPDG v0.1.0									
Dashboard	UE Sessions						1 Session	1 Active	8.53 KB / 12.17 KB
Sessions	IMSI	UE IP	SOURCE	APN	STATUS	DURATION	TRAFFIC		
Diameter		100.64.34.84	10.7.7.50:14500	*	Active	4m 50s	8.53 KB / 12.17 KB		
Logs	SESSION		NETWORK & TIMING		TRAFFIC				
Docs	IMSI		DNS	10.4.10.195, 10.4.10.196	Bytes In (UL)	8.53 KB			
Resources	NAI	0	3gppnetwork.org	P-CSCF	10.4.12.165	Bytes Out (DL)	12.17 KB		
Configuration	UE IP	100.64.34.84	Connected		2026-03-08 21:39:16	Packets In	63		
License	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							

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

قائمة الجلسات

:تعرض كل صف من الجلسات

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

مؤشرات الحالة

:تعرض الجلسات الحالة مع شارات ملونة

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

تفاصيل الجلسة

:انقر على أي صف من الجلسات لتوسيع المعلومات التفصيلية

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

قسم الجلسة

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

قسم الشبكة والتوقيت

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

قسم الحركة

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

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 نظراء

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

قائمة النظراء

:تعرض كل صف من النظراء

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

مؤشرات الحالة

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

ملخص عدد النظراء

:يعرض العنوان إجمالي الأعداد

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

تفاصيل النظراء

انقر على أي صف من النظراء لتوسيع المعلومات التفصيلية

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

الحالة الفارغة

عندما لا يتم تكوين أي نظراء، يعرض العرض

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

التحديث التلقائي

تقوم قائمة النظراء بتحديث نفسها تلقائيًا كل ثانية.

عرض السجلات

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

عرض السجلات

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

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

مستويات السجلات

تُرمز السجلات بالألوان حسب الشدة:

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

تصنيف المستويات

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

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

البحث

:تصفية السجلات في الوقت الحقيقي باستخدام مربع البحث

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

التحكم

الوصف	التحكم
تغيير بث السجلات تشغيل/إيقاف	توقف/استئناف
إزالة جميع السجلات المعروضة	مسح
تغيير 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 السجلات إلى إزالة جميع الإدخالات من العرض

الحالة الفارغة

:عندما لا تتطابق أي سجلات مع الفلاتر الحالية

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

التحديث التلقائي

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

عرض الوثائق

OmniEPDG يوفر عرض الوثائق متصفح وثائق مدمج، مما يتيح للمشغلين الوصول إلى جميع وثائق 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
بنية النظام وتدفقات المكالمات	architecture.md
مرجع تكوين كامل	configuration.md
دليل لوحة التحكم هذه	control-panel.md
Prometheus مرجع مقاييس	metrics.md
المشكلات الشائعة وخطوات الحل	troubleshooting.md

عرض Markdown

:بما في ذلك Markdown تُعرض الوثائق بدعم كامل لـ

- العناوين وتنسيق النص
- كتل التعليمات البرمجية مع تمييز الصياغة
- 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 قيد التشغيل

:المحملة مقسمة حسب الفئة OTP تظهر جميع تطبيقات

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

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

عرض التكوين

يعرض عرض التكوين تكوين وقت التشغيل والتطبيقات المحملة.

معلومات البيئة

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

قائمة التطبيقات

:المحملة مع إصداراتها. اختر تطبيقًا لعرض OTP تعرض 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 بتوفير مقاييس OmniEPDG تقوم لتمكين عملية السحب HTTP وصحة النظام. يتم تقديم المقاييس عبر Diameter وإشارات Prometheus بواسطة Prometheus.

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 تجمع
 - VM مقاييس
- Prometheus تكامل
- استعلامات نموذجية
- قواعد التنبيه

نقطة نهاية المقاييس

:بتوفير المقاييس عند OmniEPDG تقوم

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

Prometheus المتوافق مع Prometheus تُرجع نقطة النهاية المقاييس بتنسيق عرض وأدوات المراقبة الأخرى Grafana و.

التكوين

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

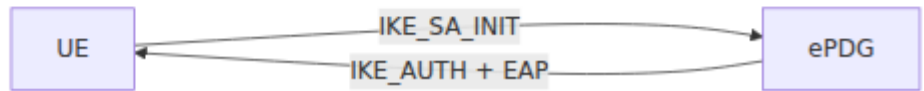
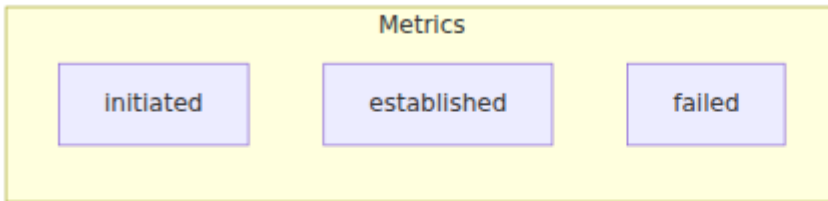
```
config :omniepdg,  
  prometheus: %{  
    port: 9568  
  }
```

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

فئات المقاييس

IKEv2 مقاييس جلسة

SWu على واجهة IKEv2 مقاييس تتبع إنشاء نفق



المقياس: `epdg_ikev2_session_initiated_count`

النوع: عداد

إنشاء النفق UE التي تم البدء بها. يزيد عندما يبدأ `IKE_SA_INIT` الوصف: إجمالي تبادل `IKE_SA_INIT` ت

المقياس: `epdg_ikev2_session_established_count`

النوع: عداد

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

المقياس: `epdg_ikev2_session_failed_count`

النوع: عداد

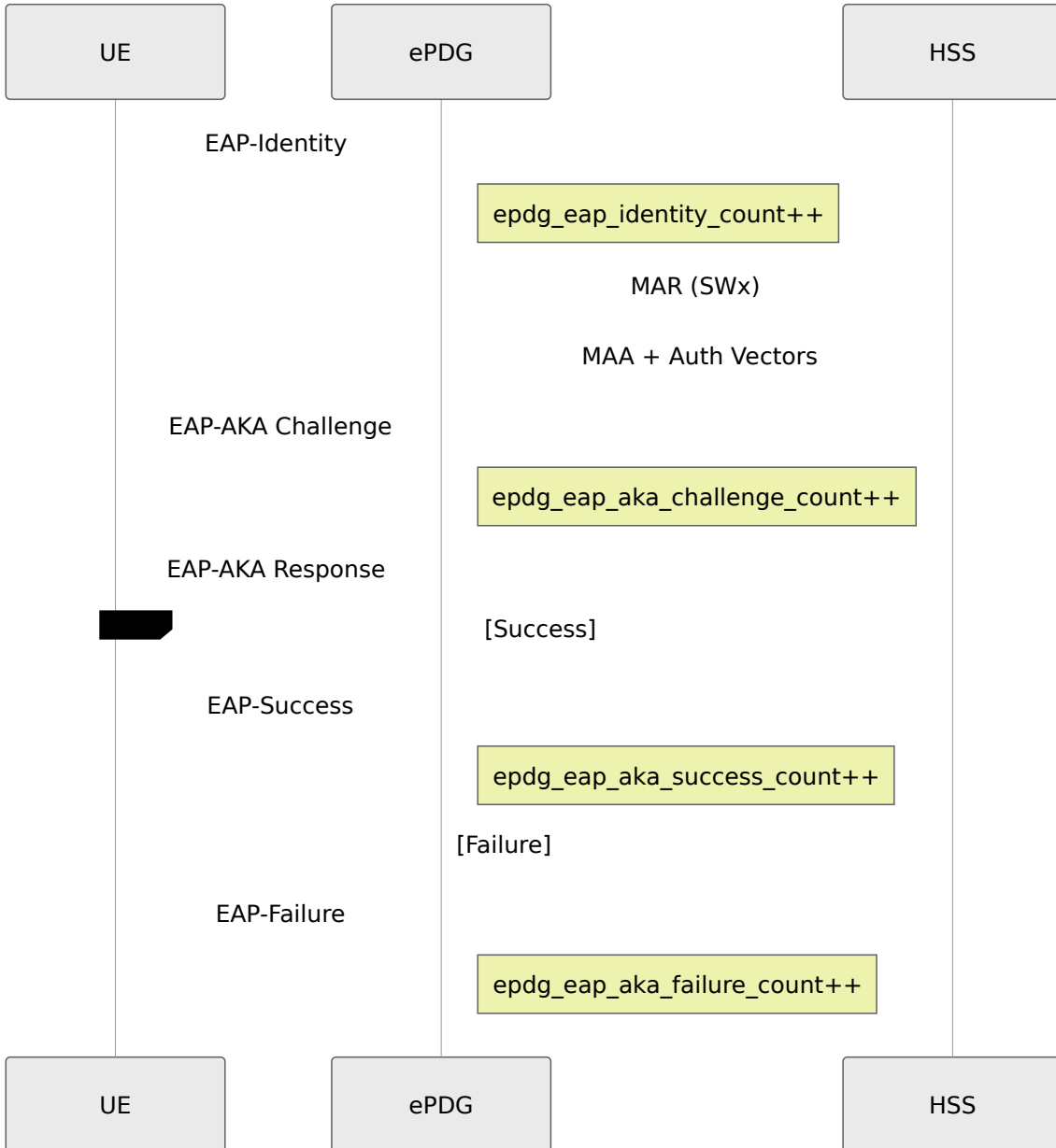
SA IKE **الوصف:** إجمالي حالات فشل إنشاء

التسميات:

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

EAP مقاييس مصادقة

EAP-AKA أيضًا OmniEPDG تدعم. [RFC 4187](#) وفقًا لـ EAP-AKA مقاييس تتبع تدفقات مصادقة UE الخاصة بـ NAI مع اختيار 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: إجمالي تحديثات UEs المرسله إلى EAP-AKA

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** - سبب الفشل (مثل **res_mismatch**, **invalid_identity**, **authentication_rejected**)

المقياس: epdg_eap_aka_sync_failure_count

النوع: عداد

يشير إلى عدم تطابق رقم EAP-AKA (SQN) **الوصف:** 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

تشير إلى هجمات محتملة من نوع AUTH. **الوصف:** إجمالي حالات فشل التحقق من الحمولة 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** - سبب الحجب: **ip** (IP تجاوز الحد لكل) أو **imsi** (IMSI تجاوز الحد لكل)

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_geop_blocked_count

النوع: عداد

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

التسميات:

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

استعلامات نموذجية:

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

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

المقياس: epdg_esp_replay_detected_count

النوع: عداد

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

Diameter SWx مقياس

GPP TS 29.273 وفقًا لـ 3 HSS و ePDG بين SWx مقياس لواجهة

المقياس: epdg_diameter_swx_mar_count

النوع: عداد

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

التسميات:

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

المقياس: `epdg_diameter_swx_sar_count`

النوع: عداد

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

التسميات:

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

المقياس: `epdg_diameter_swx_mar_latency_ms`

النوع: هيسنوجرام

بالملي ثانية **الوصف:** MAR زمن استجابة

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

المقياس: `epdg_diameter_swx_sar_latency_ms`

النوع: هيسنوجرام

بالملي ثانية **الوصف:** SAR زمن استجابة

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

المقياس: `epdg_diameter_swx_pending_count`

النوع: مقياس

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

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 **الوصف:** إجمالي طلبات

التسميات:

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

المقياس: `epdg_diameter_s6b_str_count`

النوع: عداد

الوصف: إجمالي طلبات إنهاء الجلسة المعالجة

المقياس: `epdg_diameter_s6b_active_sessions_count`

النوع: مقياس

الوصف: S6b العدد الحالي للجلسات النشطة

مقاييس دورة حياة الجلسة

PDN مقاييس تتبع إنشاء وإنهاء جلسات

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

المقياس: epdg_auth_duration_ms

النوع: هيستوجرام

إلى الجلسة المنشأة IKE_SA_INIT **الوصف:** مدة تدفق المصادقة الكاملة من

الأقسام: 10000, 5000, 2500, 1000, 500, 250, 100 مللي ثانية

المقياس: epdg_session_duration_seconds

النوع: هيستوجرام

الوصف: عمر الجلسة من الإنشاء إلى الإنهاء

الأقسام: 14400, 7200, 3600, 1800, 900, 300, 60 (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

(إلى الشبكة UE الاتجاه من) التي تم فك تشفيرها بنجاح ESP **الوصف:** إجمالي حزم

المقياس: epdg_esp_packets_out_count

النوع: عداد

(UE الاتجاه من الشبكة إلى) التي تم تشفيرها ESP **الوصف:** إجمالي حزم

المقياس: epdg_esp_bytes_in_total

النوع: مقياس

ESP **الوصف:** إجمالي البايتات التي تم فك تشفيرها من حزم

المقياس: epdg_esp_bytes_out_total

النوع: مقياس

الوصف: إجمالي البايتات التي تم تشفيرها في حزم ESP

IP مقاييس تجميع

البيسبب VPN في وضع IP مقاييس لإدارة تجميع عناوين.

المقياس: epdg_ip_allocated_count

النوع: عداد

المخصصة IP **الوصف:** إجمالي عناوين

التسميات:

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

المقياس: epdg_ip_released_count

النوع: عداد

المفرج عنها IP **الوصف:** إجمالي عناوين

التسميات:

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

المقياس: epdg_ip_pool_allocated_count

النوع: مقياس

المخصصة IP **الوصف:** العدد الحالي لعناوين

المقياس: epdg_ip_pool_available_count

النوع: مقياس

المتاحة في التجميع IP **الوصف:** العدد الحالي لعناوين

المقياس: epdg_ip_pool_utilization_ratio

النوع: مقياس

كنسبة من 0.0 إلى 1.0. تشير القيم التي تقترب من 1.0 إلى خطر IP **الوصف:** استخدام تجميع. نفاذ التجميع.

VM مقاييس

الافتراضية لمراقبة صحة النظام Erlang/BEAM مقاييس آلة

المقياس: vm_memory_total

النوع: مق

الوحدة: بايت

الوصف: VM إجمالي الذاكرة المخصصة بواسطة

المقياس: vm_memory_processes

النوع: مقياس

الوحدة: بايت

الوصف: Erlang 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

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

المقياس: vm_system_info_process_count

النوع: مقياس

الوصف: Erlang النشطة عدد عمليات

المقياس: vm_system_info_port_count

النوع: مقياس

الوصف: عدد المنافذ المفتوحة (المأخذ، مقبض الملفات)

المقياس: `vm_statistics_run_queue`

النوع: مقياس

الوصف: الطول الإجمالي لقوائم تشغيل الجدول. 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 النشر في

```
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 اس جابة 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 تجميع

```
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]))  
  
# إنهاء 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 مصادقة"
        description: "معدل فشل المصادقة هو {{ $value |
humanizePercentage }} خلال آخر 5 دقائق"

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

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

    # مرتفع زمن استجابة HSS
    - alert: OmniEPDGHSSLatencyHigh
      expr: |

```

```
    histogram_quantile(0.95,
sum(rate(epdg_diameter_swx_mar_latency_ms_bucket[5m])) by (le))
    > 1000
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "مرتفع HSS (SWx) زمن استجابة"
    description: "MAR هو الزمن المئوي 95 لاستجابة"
  }}ms"
```

المعلقة SWx تراكم طلبات

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

مرتفعة VM ذاكرة

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

تحميل الجدول مرتفع

```
- alert: OmniEPDGSchedulerOverload
  expr: vm_statistics_run_queue > 10
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "مرتفع Erlang طول قائمة تشغيل جدول"
    description: "عندما {{ $value }} طول قائمة التشغيل هو"
    "يشير إلى تشبع وحدة المعالجة المركزية"
```

لا توجد ج00سات (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 المرتفع (هجوم محتمل)

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

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\" }} محاولات
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: "اكتشاف حالات فشل التحقق من الحمولة"
```

```
    description: "أو خطأ man-in-the-middle هجوم محتمل من نوع"
```

```
"في التنفيذ"
```


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

منافذ الإدارة

تُستخدم هذه المنافذ للمراقبة التشغيلية ويجب تقييدها لشبكات الإدارة.

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

DNS متطلب

ePDG لاكتشاف DNS سجل

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

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، مع إضافة أصفار إلى 3 <MNC> أرقام (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
```

اسم الشهادة الشائعة

FQDN يتطابق مع (SAN) على اسم بديل للموضوع ePDG الخاصة بـ TLS يجب أن تحتوي شهادة IKEv2 أثناء 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 به (تتحقق الأجهزة من السلسلة) CA يجب أن تكون الشهادة موقعة من قبل
- ECDSA P-256 بت أو RSA 2048 الحد الأدنى هو

Diameter DNS مجال

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

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

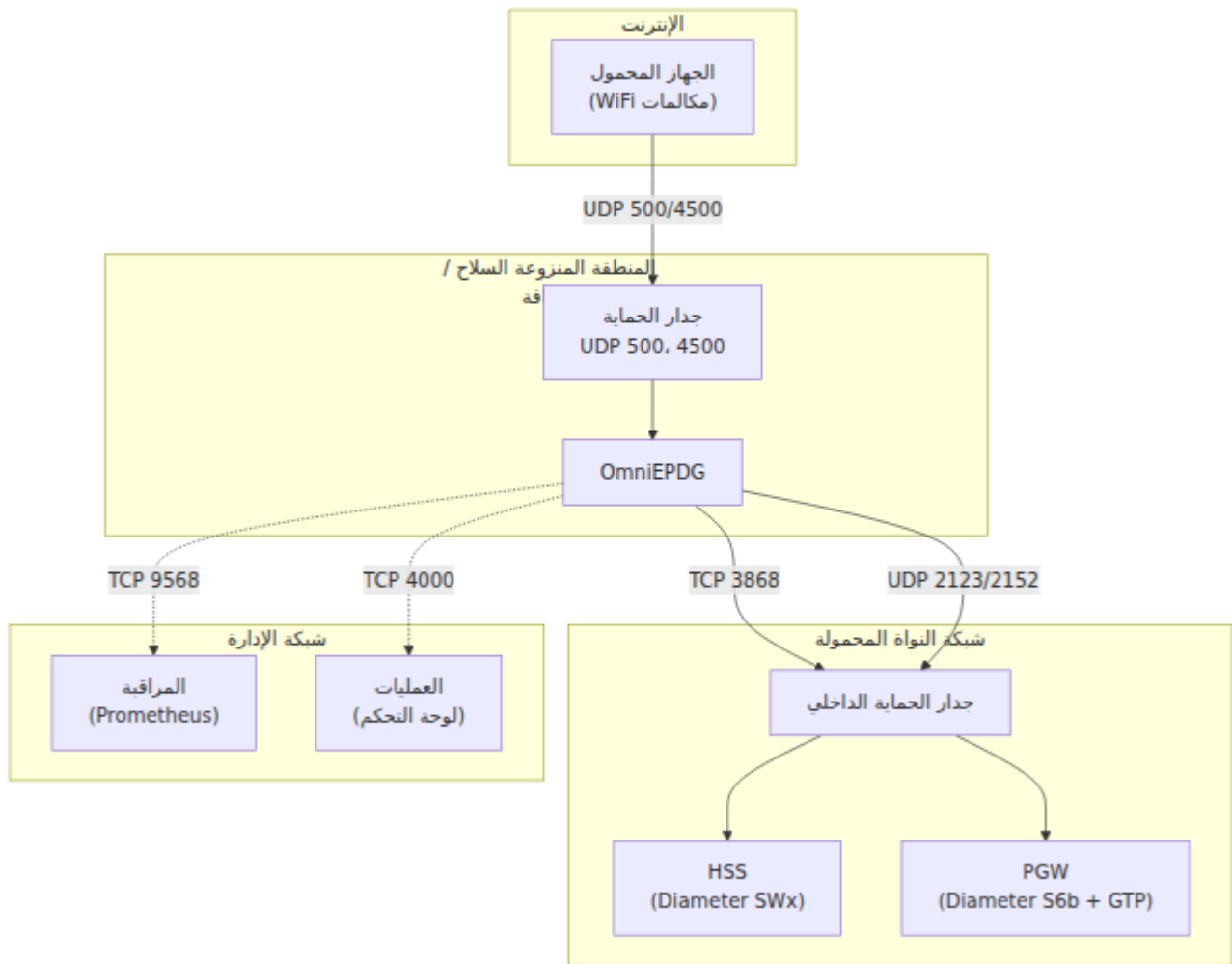
مثال:

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

يتم استخدام هذا المجال في:

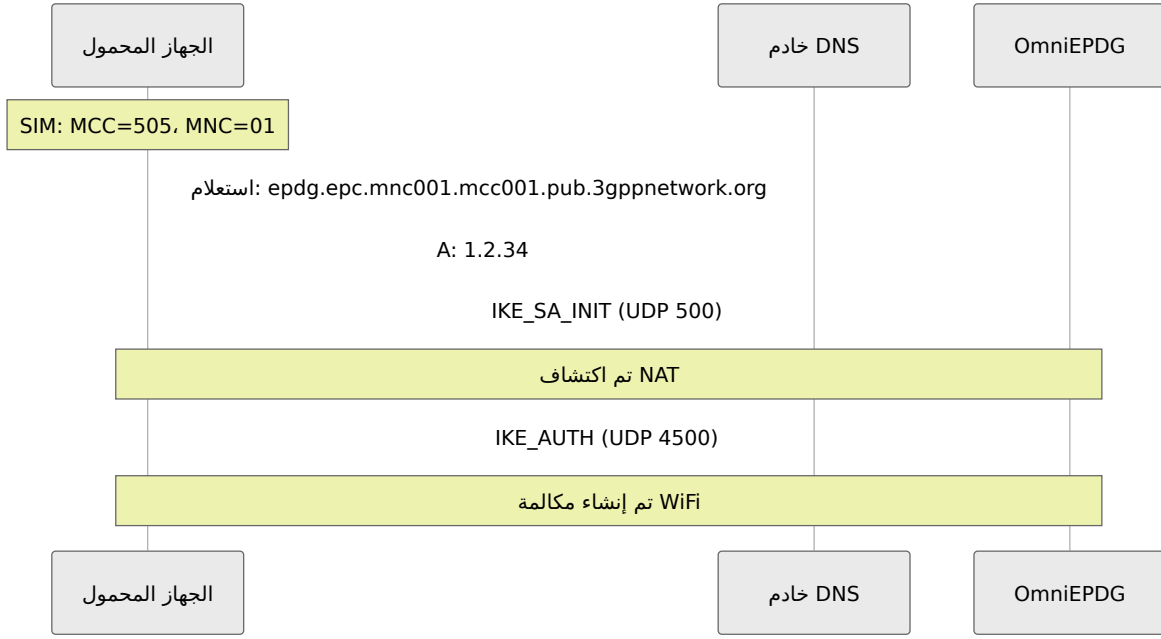
- أثناء المصادقة UE المرسل من (معرف الوصول إلى الشبكة) NAI
- Diameter لمجال الأصل ومجال الوجهة لـ AVPs
- Diameter قرارات توجيه

هيكل الشبكة



DNS تدفق بحث

التالي DNS يحدث حل WiFi، عندما يبدأ جهاز محمول مكالمات



قائمة التحقق

متطلبات مواجهة الإنترنت

- OmniEPDG وارد إلى UDP 500 فتح
- OmniEPDG وارد إلى UDP 4500 فتح
- سجل DNS A:

العام IP عنوان → `epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org`
 ل ePDG

- مطابق SAN مع TLS تثبيت 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 9568 TCP الوصول إلى

المراجع

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

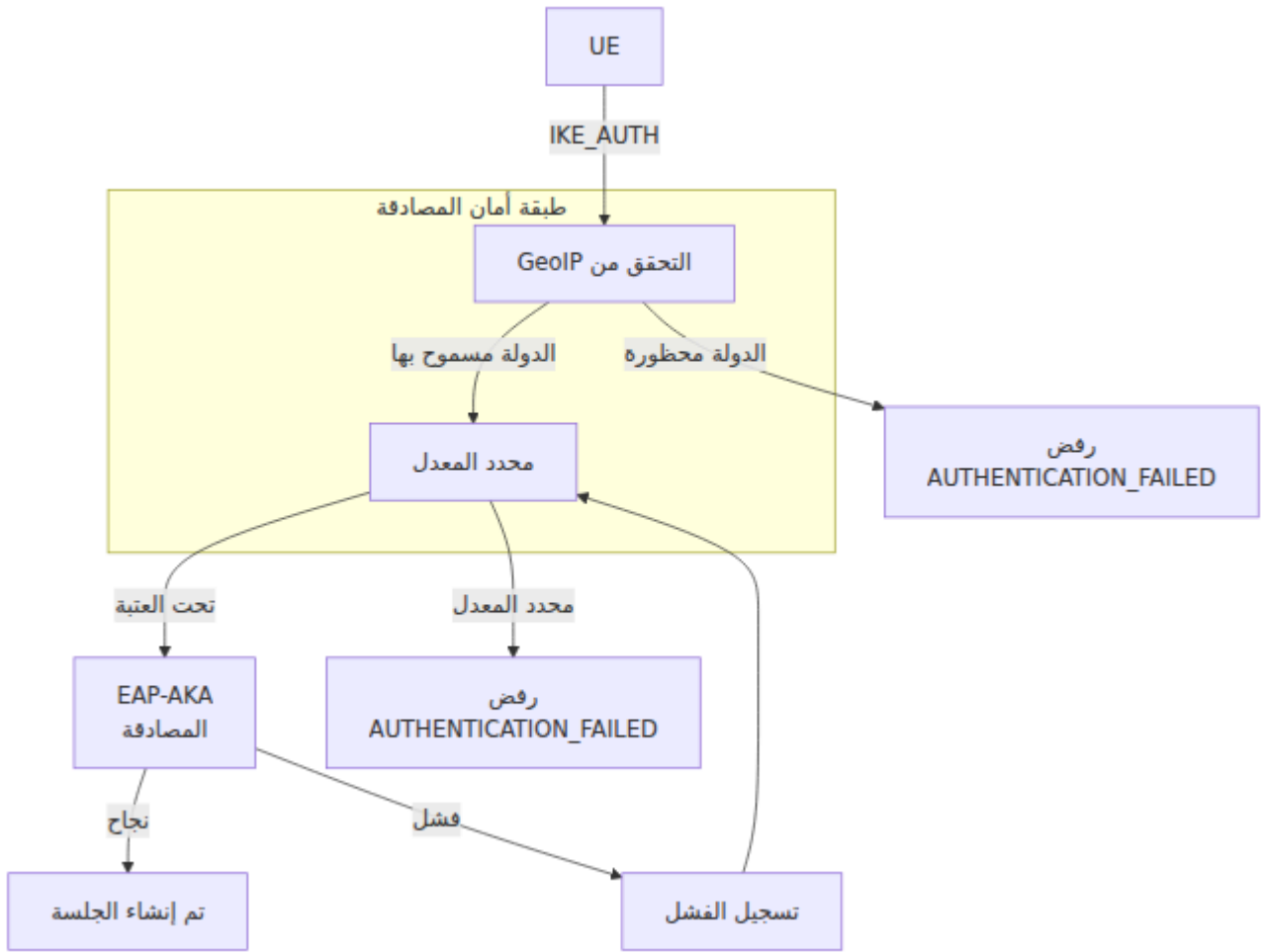
أمان المصادقة في OmniEPDG

تتفيذ 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
- حظر الدول باستخدام GeolIP
- تدفق الأمان
- المقاييس
- استكشاف الأخطاء وإصلاحها

نظرة عامة



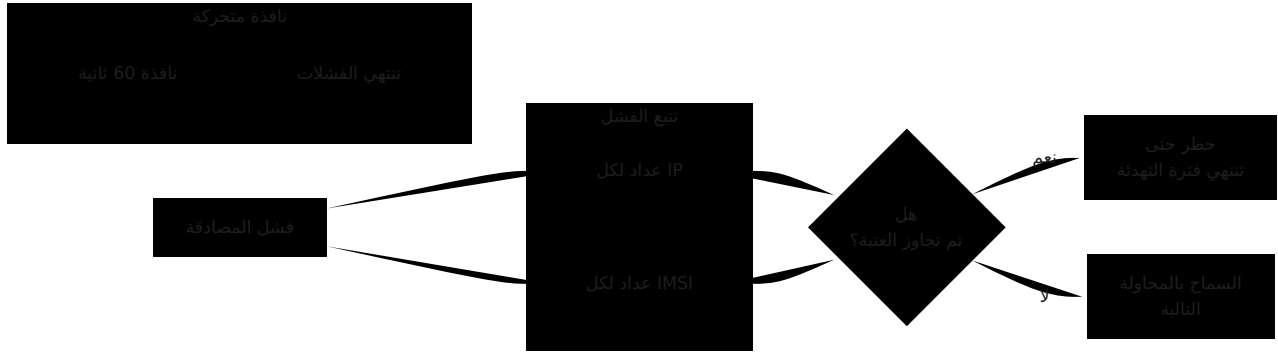
قبل العمليات التشفيرية، إجراء IKE_AUTH فحوصات الأمان في بداية تبادل OmniEPDG تقوم المكلفة:

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

تحديد معدل المصادقة

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

كيف يعمل



يستخدم محدد المعدل خوارزمية النافذة المتحركة

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

تتبع مزدوج

يتم فرض حدين مستقلين في نفس الوقت

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

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

التكوين

```
config :omniepdg,  
  # تحديد المعدل لكل IP  
  auth_rate_limit_per_ip: 10, # الحد الأقصى للفشلات قبل  
  الحظر  
  auth_rate_limit_ip_window_ms: 60_000, # حجم النافذة (1 دقيقة)  
  auth_rate_limit_ip_block_ms: 300_000, # مدة الحظر (5 دقائق)  
  
  # تحديد المعدل لكل IMSI  
  auth_rate_limit_per_imsi: 5, # الحد الأقصى للفشلات قبل  
  الحظر  
  auth_rate_limit_imsi_window_ms: 60_000, # حجم النافذة (1 دقيقة)  
  auth_rate_limit_imsi_block_ms: 600_000 # مدة الحظر (10 دقائق)
```

IP معلمات لكل

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 حظر IP.
auth_rate_limit_ip_window_ms	عدد صحيح	لا	60000	حجم النافذة المتحركة بالمللي ثانية لتعداد IP. الفشلات الأقدم من ذلك لا تُحتسب.
auth_rate_limit_ip_block_ms	عدد صحيح	لا	300000	مدة الحظر بالمللي ثانية لعنوان IP بعد تجاوز العتبة الافتراضي هو 5 دقائق.

IMSI معاملات لكل

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

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

السلوك عند النجاح

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

أمثلة على التكوينات

بيئة عالية الأمان

:حدود صارمة للبيئات ذات التسامح المنخفض مع الفشلات

```
config :omniepdg,  
  auth_rate_limit_per_ip: 5,  
  auth_rate_limit_ip_window_ms: 120_000,    # نافذة 2 دقيقة  
  auth_rate_limit_ip_block_ms: 900_000,     # حظر 15 دقيقة  
  
  auth_rate_limit_per_imsi: 3,  
  auth_rate_limit_imsi_window_ms: 120_000,  
  auth_rate_limit_imsi_block_ms: 1_800_000 # حظر 30 دقيقة
```

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

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

بيئة مريحة

حدود أكثر تساهلاً للتطوير أو الاختبار:

```
config :omniepdg,  
  auth_rate_limit_per_ip: 50,  
  auth_rate_limit_ip_window_ms: 60_000,  
  auth_rate_limit_ip_block_ms: 60_000,      # حظر 1 دقيقة  
  
  auth_rate_limit_per_imsi: 20,  
  auth_rate_limit_imsi_window_ms: 60_000,  
  auth_rate_limit_imsi_block_ms: 120_000   # حظر 2 دقيقة
```

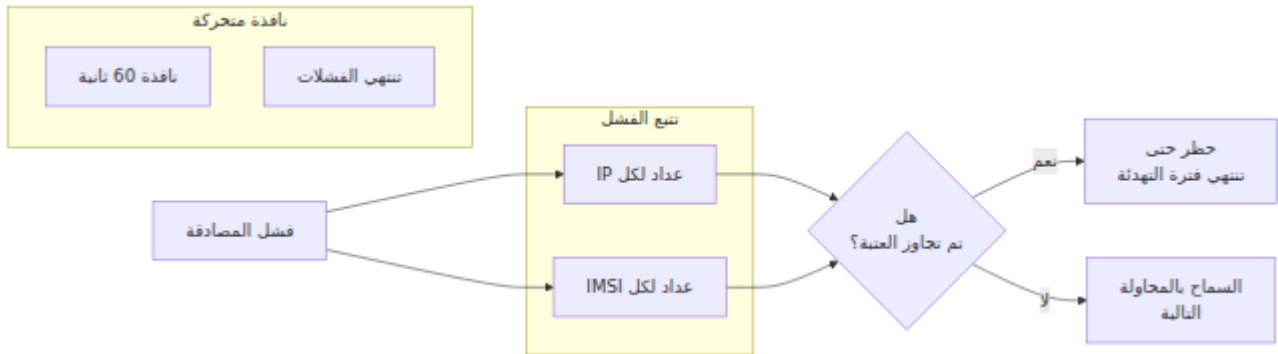
كيف يعمل: تتيح العتبات الأعلى والحظرات الأقصر مزيدًا من المرونة في الاختبار.

حالة الاستخدام: بيئات التطوير، اختبار التكامل.

GeoIP حظر الدول باستخدام

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

نظرة عامة



MaxMind GeoLite2 قاعدة بيانات

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

GeoIP لتفعيل حظر:

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

التكوين

```
config :omniepdg,  
  # تفعيل حظر GeoIP  
  geolip_enabled: true,  
  
  # MaxMind المسار إلى قاعدة بيانات  
  geolip_database_path: "/etc/omniepdg/GeoLite2-Country.mmdb",  
  
  # وضع التحكم في الوصول  
  geolip_mode: :whitelist,  
  
  # قائمة الدول (رموز ISO 3166-1 alpha-2)  
  geolip_countries: ["AU", "NZ"],  
  
  # غير المعروفة IPs التعامل مع  
  geolip_allow_unknown: false,  
  
  # السلوك عند عدم توفر قاعدة البيانات  
  geolip_fail_open: true
```

المعلومات

المعلمة	النوع	مطلوب	الافتراضي
<code>geoup_enabled</code>	Boolean	لا	<code>false</code>
<code>geoup_database_path</code>	String	لا	<code>"/etc/omniepdg/GeoLite2-Country.mmdb"</code>
<code>geoup_mode</code>	Atom	لا	<code>:whitelist</code>

المعلمة	النوع	مطلوب	الافتراضي
<code>geopip_countries</code>	List	لا	<code>[]</code>
<code>geopip_allow_unknown</code>	Boolean	لا	انظر أدناه
<code>geopip_fail_open</code>	Boolean	لا	<code>true</code>

المعلمة	النوع	مطلوب	الافتراضي

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"] # فيجي، نيوزيلندا، أستراليا
```

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

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

وضع القائمة السوداء

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

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

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

حالة الاستخدام: حظر المناطق عالية المخاطر مع السماح بالتجوال العالمي

التعامل مع الدول غير المعروفة

لا يمكن تحديد موقعها IP بعض عناوين

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

في السلوك `geoup_allow_unknown` تتحكم معلمة

الوضع	القيمة الافتراضية لـ <code>geoup_allow_unknown</code>	السلوك
القائمة البيضاء	<code>false</code>	غير معروف = غير موجود في القائمة البيضاء = محظور
القائمة السوداء	<code>true</code>	غير معرف ?? = غير موجود في القائمة السوداء = مسموح

لتجاوز الافتراضي:

```
config :omniepdg,  
  geoup_mode: :whitelist,  
  geoup_allow_unknown: true # غير معروفة حتى في وضع IPs السماح بـ  
  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 المكون
3. يتم إعادة تحميل قاعدة البيانات تلقائيًا في البحث التالي (لا حاجة لإعادة التشغيل).

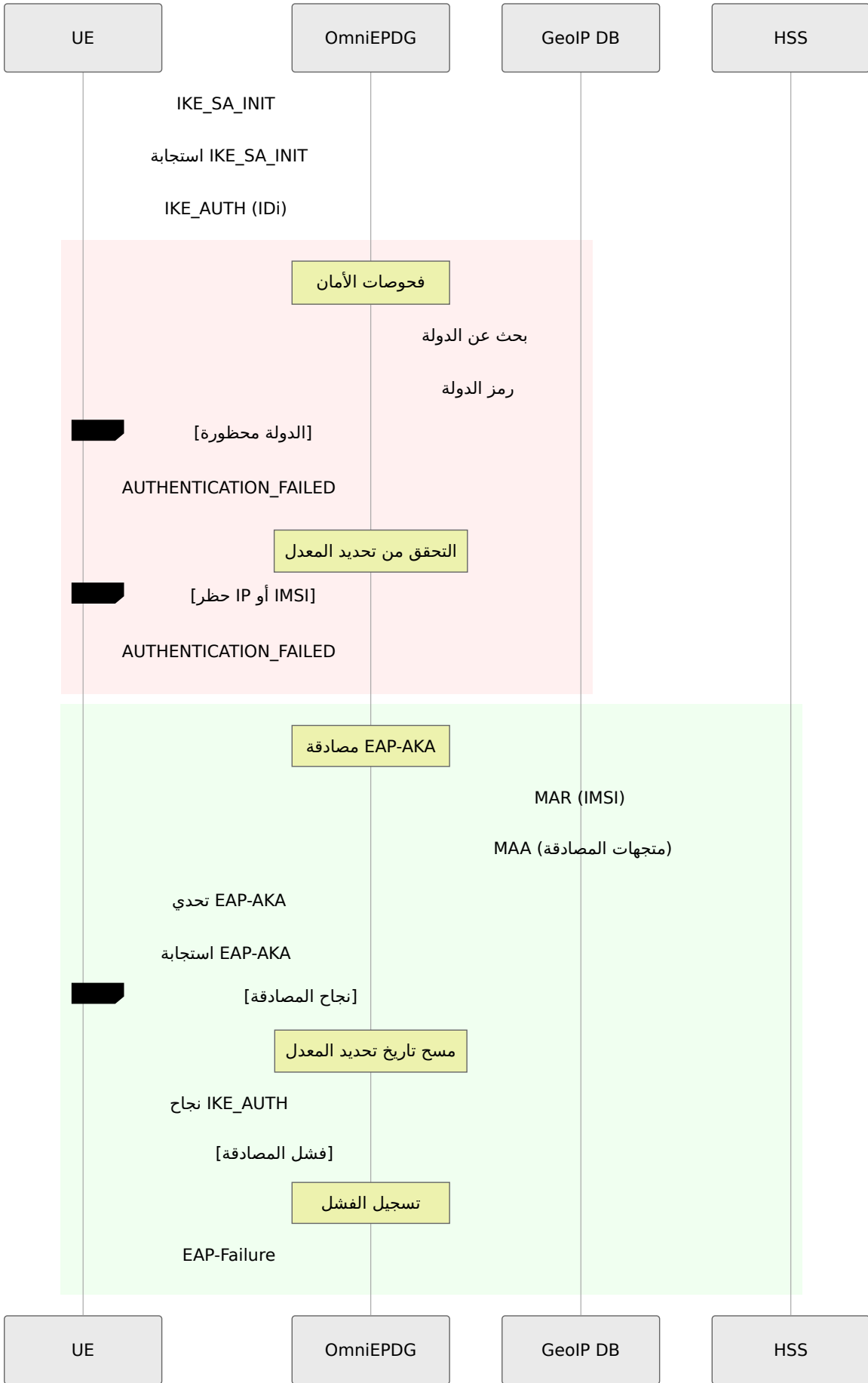
رموز الدول الشائعة

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

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 بواسطة تحديد المعدل التسميات

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

استعلامات المثال:

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

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

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

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` التي لا يمكن IP لعناوين حلها

استعلامات المثال:

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

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

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

استكشاف الأخطاء وإصلاحها

مشاكل تحديد المعدل

حظر المستخدمين الشرعيين

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

الأسباب المحتملة:

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

الحل:

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

معدل مرتفع من 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 لأنماط IP مراجعة عناوين
2. للمهاجمين المستمرين IP اعتد ◆◆ر تنفيذ قواعد جدار حماية على مستوى
3. إذا تأثر المستخدمون الشرعيون HSS تحقق من الاتصال بـ

GeoIP مشاكل

حظر جميع الاتصالات

GeoIP الاتصال بعد تفعيل UE الأعراض: لا يمكن لأي

الأسباب المحتملة:

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

الحل:

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

لا تُحمّل GeoIP قاعدة بيانات

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

الأسباب المحتملة:

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

الحل:

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

حظرات 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

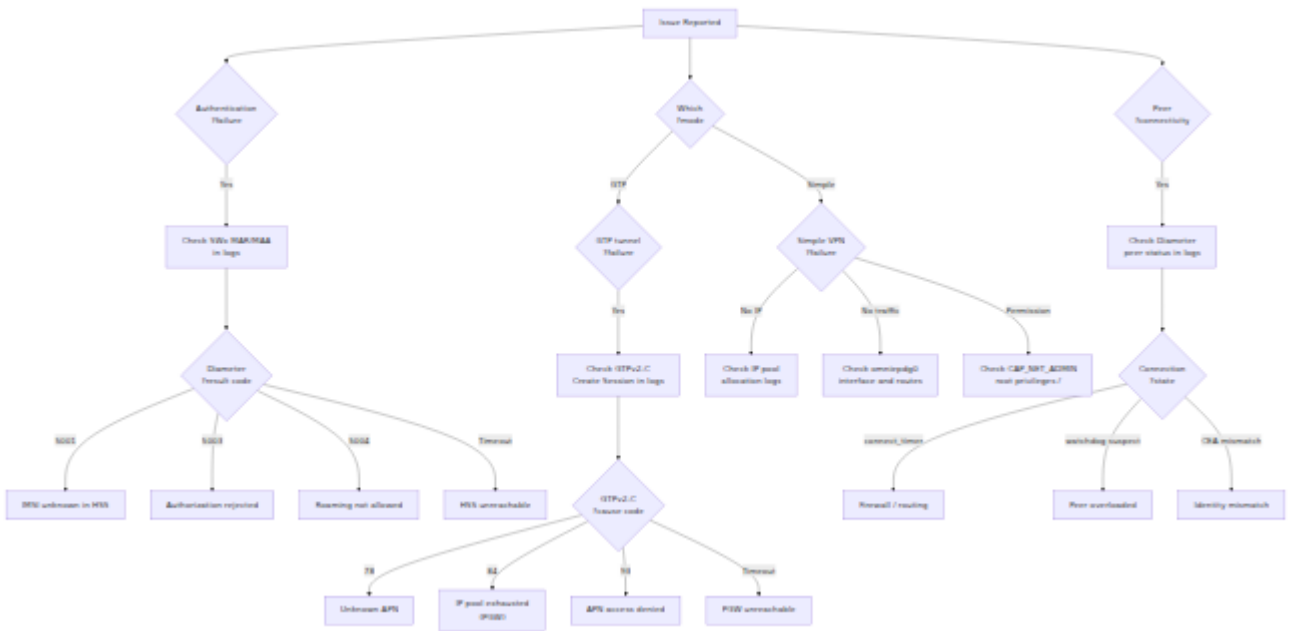
الحل:

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

استكشاف أخطاء وإصلاحها OmniEPDG

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

نظرة عامة على التشخيص



ملفات السجل

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

الغرض	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 للمشاكل النشطة
log/crash.log	التي تتعطل OTP عمليات	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 - وتبادل القدرات Diameter تم الاتصال بنظير
- peer_down - Diameter تم قطع الاتصال بنظير

FSM UE انتقالات حالة:

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

أحداث المهلة:

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

Diameter مشكلات الاتصال

HSS (SWx) فشل الاتصال بـ

HSS الأعراس: لا يمكن لأي مشتركين المصادقة. 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 التكوين غير صحيحة في التكوين
- Diameter غير قيد التشغيل أو لا يقبل اتصالات HSS
- (بشكل افتراضي SCTP بعض الجدران النارية تمنع) غير مفعل على مسار الشبكة SCTP
- CEA مما يؤدي إلى 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، كم بتعيين dia_swx_proto إلى tcp كخيار احتياطي
4. هو اسم نطاق مؤهل يمكن حله ويتطابق مع dia_swx_origin_host تحقق من أن HSS ما يتوقعه
5. Diameter CER/CEA للرسائل الفاشلة في التفاوض على HSS تحقق من سجلات

PGW (S6b) فشل الاتصال بـ

تظهر PGW من AAR أو لم تصل GTP الأعراس: تنجح المصادقة ولكن فشل إنشاء نفق S6b. peer_up السجلات عدم وجود حدث

الأسباب المحتملة:

- PGW الخاص بـ S6b غير مكون للاتصال بمستمتع PGW
- OmniEPDG الخاص بـ S6b على عنوان الربط 3868 SCTP جدار ناري يمنع منفذ
- dia_s6b_local_ip PGW غير قابل للوصول من
- 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 Sctp 3868 تحقق من أن قواعد الجدار الناري تسمح بحركة مرور S6b على عنوان
4. يتطابقان مع `dia_s6b_origin_host` و `dia_s6b_origin_realm` تحقق من أن PGW ما يتوقعه

Diameter فشل مراقبة

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

الأسباب المحتملة:

- عدم استقرار مسار الشبكة أو فقدان الحزم
- ضمن DWR نظير محمّل بشكل زائد ولا يستجيب لـ `dia_swx_watchdog_timer`
- تكوين مراقبة عدواني (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 / dia_s6b_watchdog_config` (على سبيل المثال) `[{okay, 5}, {suspect, 3}]` قم بزيادة عتبات إذا كان من المتوقع فقدان الحزم، قم بزيادة عتبات
3. (الذاكرة، عدد الاتصالات، CPU) تحقق من صحة نظام النظير.

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 SIM UE بين IMSI عدم تطابق
- IMSI غير صحيح، مما يؤدي إلى 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

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

الأسباب المحتملة:

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

الحل:

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

(Diameter 5004) التجوال غير مسموح به

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

الأسباب المحتملة:

- ترفض موقع المشترك 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 به بموجب اتفاقيات التجوال WiFi تحقق مما إذا كان الاتصال عبر

انتهاء مهلة المصادقة

الأعراض: Timeout تتوقف المصادقة ثم تفشل بعد 10 ثوانٍ. تظهر السجلات `srm_der_timeout` في `state_wait_auth_resp`.

الأسباب المحتملة:

- خلال 10 ثوانٍ SWx MAR لا يستجيب لـ HSS
- أثناء الطلب SWx Diameter تم قطع اتصال
- محمّل 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 كافي للكمون الشبكي 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 العكس، EAP-AKA' ولكن الشبكة تتوقع (EAP-AKA) يرسل هوية مع بادئة 0 UE
- خاطئ EAP يعيد متجهات المصادقة لنوع HSS

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

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

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

الحل:

1. في السجلات للتحقق من البادئة UE ل NAI تحقق من هوية.
2. مكون لإعادة المتجهات الصحيحة للمصادقة 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 كخطأ "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 المصادقة الصحيحة HSS تحقق من أن
3. المستلم RES المتوقع مع XRES قم بتمكين تسجيل الأخطاء لمقارنة
4. تتطابق بين OP/OPc و Ki اختبارية، تحقق من أن قيم SIM إذا كنت تستخدم بطاقات SIM و HSS

(فقط GTP وضع) GTP فشل نفق

PGW تم رفض إنشاء جلسة من قبل

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

أكواد الأسباب الشائعة والإجراءات:

كود السبب	الاسم	الإجراء
78	مفقود أو غير APN معروف	ويتطابق مع PGW مكون على APN تحقق من أن ملف تعريف المشترك
82	RAT مرفوض في	WiFi تسمح بنوع وصول PGW تحقق من أن سياسة (GPP غير 3)
84	جميع العناوين الديناميكية مشغولة	؛ قم بتوسيع PGW الخاصة بـ IP نفاد مجموعة المجموعة أو تحقق من التسريبات
92	فشل مصادقة المستخدم	؛ تحقق من تفويض PGW فشل المصادقة من جانب جلسة S6b
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 لدى تم تفويضها S6b جلسة
113	APN ازدحاما	PGW محمّل؛ أعد المحاولة أو تحقق من سعة APN
120	GTP-C ازدحام كيان	PGW تحميل زائد في مستوى التحكم

انتهاء مهلة إنشاء الجلسة

Timeout الأعراض: يتوقف 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 2123 UDP جدار ناري يمنع منفذ
- GTPv2-C محمّل 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 حركة المرور GTP-U نفق

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

الأسباب المحتملة:

- غير محملة GTP-U وحدة نواة
- المعلن GTP-U لا يتطابق مع عنوان نقطة نهاية نفق `gtp_u_kmod` لمقبس IP عنوان إلى PGW
- GTP عدم تكوين التوجيه لجهاز نفق
- (GTP-U) UDP 2152 جدار ناري يمنع منفذ

الحل:

1. GTP تحقق من تحميل وحدة (Linux `lsmod | grep gtp`) في نواة GTP تحقق من تحميل وحدة
2. GTP (`ip link show gtp0`) تأكد من وجود جهاز نفق
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 طرقًا 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` تفتقر إلى قدرة OmniEPDG عملية

- غير محملة TUN/TAP وحدة نواة
- تم إنشاء واجهة أخرى بالفعل باسم `omniepdg0`

الحل:

1. متاحة TUN تحقق من أن وحدة النواة (`lsmod | grep tun`)
2. TUN يعمل بامتيازات كافية لإنشاء واجهات OmniEPDG تأكد من أن
3. موجودة بالفعل من مثيل سابق `omniepdg0` تحقق مما إذا كانت (`ip link show omniepdg0`)
4. للبحث 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 العناوين في مجموعة
- بعد إنهاء الجلسة (تسرب) IP عدم 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 أن الجلسات يتم إنهاؤها بشكل صحيح (`terminating`)
3. أكبر في CIDR إذا كانت المجموعة ممثلة حقًا، قم بتوسيعها باستخدام بادئة (`simple_vpn_pool_ipv4` (يتطلب إعادة التشغيل)
4. التي قد تكون `log/crash.log` أثناء الإنهاء في FSM تحقق من وجود أعطال في IP منعت تحرير

حركة مرور المشترك لا تتدفق

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

الأسباب المحتملة:

- `omniepdg0` للمشارك على IP لم تتم إضافة مسار مضيف لعنوان
- OmniEPDG على مضيف IP لم يتم تمكين توجيهه
- قواعد الجدار الناري تمنع حركة المرور على واجهة `omniepdg0`
- للمشاركين IP مفقودة لحركة المرور الصادرة من نطاق NAT/masquerade قواعد

الحل:

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

طرق قديمة بعد التعطل

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

الأسباب المحتملة:

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

الحل:

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

مشكلات إنهاء الجلسة

يتوقف الإنهاء أثناء إلغاء التسجيل

في حالة FSM UE الأعراس: لا يكتمل إنهاء الجلسة. يتعطل `dereg_*` أو `wait_*`.

الأسباب المحتملة:

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

الحل:

1. تحقق من السجلات للرسائل المهلة في الحالة ذات الصلة.
2. HSS و PGW تحقق من الاتصال بـ.
3. إلى الخطوة التالية في الإنهاء FSM بعد 10 ثوانٍ، يجب أن تنتهي المهلة ويجب أن تنتقل إلى `Unexpected call event` أو تنتهي. إذا لم يحدث ذلك، تحقق من الأحداث غير المتوقعة المسجلة كـ `call event`

اليتيمة PDP GTP-U سياقات

في النواة بعد إنهاء الجلسات. تظهر GTP-U الأعراس: تبقى إدخلات نفق `ip link show gtp0`. 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. للبحث عن أعطال العمليات أثناء الإنهاء `log/crash.log` تحقق من
2. على سبيل FSM إذا تم قتل PDP تنظيف سياق FSM لـ `terminate/3` تحاول دالة قد يكون قد تم تخطي التنظيف، (المثال، إعادة تشغيل المشرف ومسح السياقات GTP-U إلى إعادة إنشاء مقبس OmniEPDG سيؤدي إعادة تشغيل القديمة

مشكلات العملية والنظام

حلقات إعادة تشغيل المشرف

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

الأسباب المحتملة:

- خطأ تكوين مستمر يتسبب في تعطل معالج عند بدء التشغيل
- (غير موجودة gen_socket على سبيل المثال، مكتبة) اعتماد خارجي غير متاح
- رسائل مشوهة تتسبب في تعطل المعالجات Diameter إرسال نظير

الحل:

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

استخدام الذاكرة العالي

مع مرور الوقت VM Erlang **الأعراض**: تزداد استهلاك الذاكرة في

الأسباب المحتملة:

- بعد إنهاء الجلسة FSM UE عدم تنظيف عمليات
- تراكم رسائل السجل في صناديق البريد
- عدد كبير من الجلسات المتزامنة

الحل:

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