دليل عمليات ونشر OmniTWAG

أنشأه Omnitouch

هذا الدليل مخصص لمشغلي الشبكات، ومديري الأنظمة، والعملاء الذين يقومون بنشر OmniTWAG.

جدول المحتويات

1. مقدمة
2. ما هو تحميل WiFi؟
3. معمارية النشر
4. تدفق الشحن
5. تدفق المصادقة
6. دليل التكوين
7. إعداد نقطة الوصول
8. تكامل Hotspot 2.0
9. المراقبة والإدارة
10. استكشاف الأخطاء وإصلاحها
11. الامتثال للمعايير

مقدمة

OmniTWAG (بوابة الوصول الموثوق WiFi) هو تنفيذ متوافق مع المعايير لـ 3GPP TWAG الذي يمكّن ��شغلي الشبكات المحمولة من تحميل حركة مرور المشتركين من الشبكات الخلوية إلى نقاط الوصول WiFi بشكل آمن مع الحفاظ على مصادقة آمنة تعتمد على SIM.

يقوم TWAG بمصادقة مشتركي WiFi باستخدام بيانات اعتماد SIM الخاصة بهم عبر EAP-AKA (بروتوكول المصادقة القابل للتوسيع - المصادقة واتفاقية المفاتيح)، وهو نفس آلية المصادقة المستخدمة في الشبكات الخلوية. وهذا يوفر وصولاً سلسًا وآمنًا إلى WiFi للمشتركين المحمولين دون الحاجة إلى كلمات مرور WiFi منفصلة.

الفوائد الرئيسية

للمستخدمين النهائيين:

- **تكوين صفر**: يعمل مباشرة مع SIM متوافق
- **تجربة سلسة**: اتصال تلقائي مثل الخلوية
- **آمن**: يستخدم دائمًا WiFi مشفر (WPA2)
- **بدون كلمات مرور**: مصادقة تعتمد على SIM

لمشغلي الشبكات:

- **تخفيف سعة الشبكة**: يقلل الحمل على محطات القاعدة الخلوية
- **تحميل محكوم**: يمكن فقط للمشتركين المصرح لهم الات��ال
- **تحسين تجربة المستخدم**: عادةً ما توفر WiFi عرض نطاق ترددي أعلى
- **كفاءة التكلفة**: بنية WiFi التحتية أقل تكلفة من الخلوية
- **هوية منسقة**: نفس IMSI المستخدمة لـ WiFi والخلوية
- **تكامل الفوترة**: يمكن شحن استخدام WiFi إذا رغبت في ذلك

للمواقع/الشركات:

- **أمان على مستوى المشغل**: لا يوجد خطر من مشاركة كلمات المرور
- **قابلية التوسع**: دعم لآلاف المستخدمين دون توفير يدوي
- **إدارة مبسطة**: لا حاجة لتوزيع كلمات مرور WiFi

ما هو تحميل WiFi؟

يسمح تحميل WiFi لمشغلي الشبكات المحمولة بإعادة توجيه حركة بيانات المشتركين من الشبكات الخلوية المزدحمة إلى شبكات WiFi.

كيف يمكّن TWAG التحميل

يعمل TWAG كبوابة مصادقة بين:

- **نقاط وصول WiFi** (عبر بروتوكول RADIUS)
- **شبكة النواة المحمولة** HSS/HLR (عبر واجهة Diameter SWx)

عندما يتصل جهاز المشترك بنقطة وصول WiFi مكونة للتحميل:

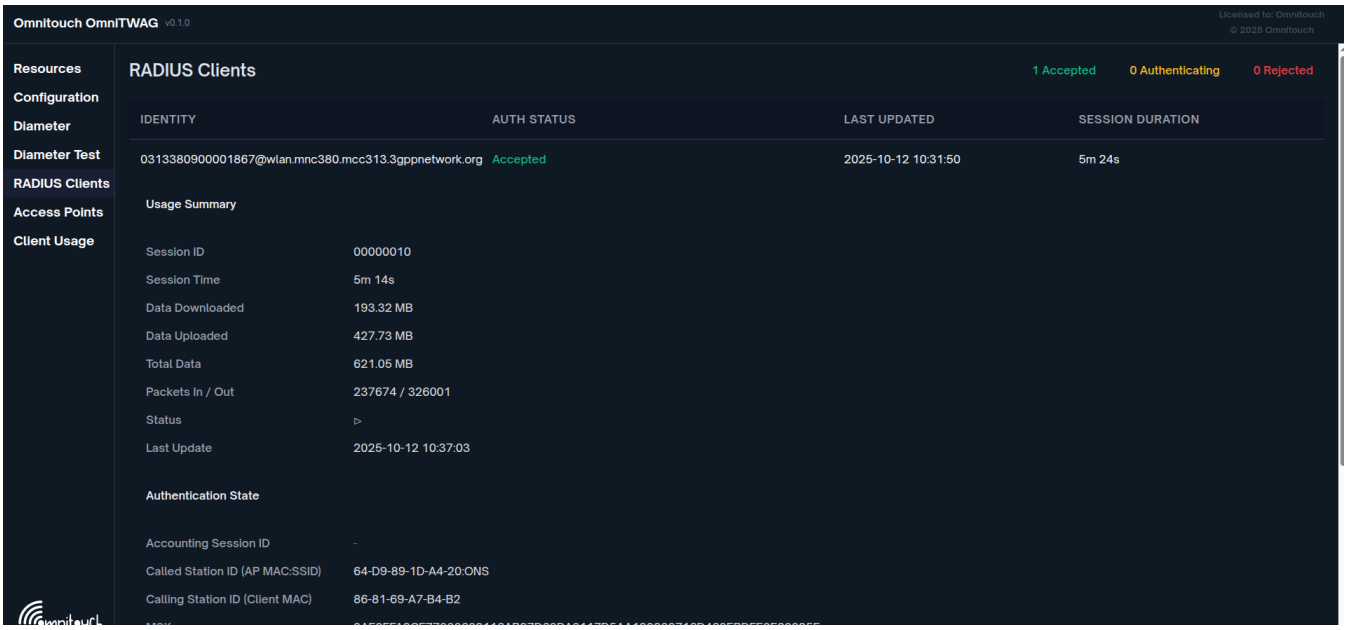
1. يقوم الجهاز بالتعريف عن نفسه باستخدام IMSI الخاص به (من بطاقة SIM)
2. تقوم نقطة وصول WiFi بإرسال طلبات المصادقة إلى TWAG عبر RADIUS
3. يتواصل TWAG مع HSS الخاص بالمشغل لاسترداد متجهات المصادقة
4. تحدث المصادقة بتحدي-استجابة EAP-AKA بين الجهاز وTWAG
5. عند المصادقة الناجحة، يتم منح الجهاز وصول WiFi
6. اختياريًا، يمكن أن يتم نقل الحركة مرة أخرى إلى النواة المحمولة أو الخروج محليًا

معمارية النشر

طوبولوجيا الشبكة

أسطورة الواجهة:

- **STa***: واجهة RADIUS/Diameter بين نقطة وصول WiFi وTWAG (غير 3GPP إلى AAA)
- **SWx**: واجهة Diameter بين TWAG (خادم 3GPP AAA) وHSS
- **S2a/S2b**: واجهة نفق GTP للعودة إلى الشبكة المنزلية (اختياري)
- **SGi**: واجهة إلى الشبكات الخارجية للبيانات الخ��م (الإنترنت)
- **802.11**: واجهة راديو WiFi
- **EAPOL**: EAP عبر LAN (المصادقة 802.1X)



سيناريوهات النشر

السيناريو 1: الخروج المحلي (موصى به للأداء)

الفوائد:

•زمن انتقال أقل (لا يوجد توجيه إلى النواة)
•تقليل الحمل على الشبكة الأساسية
•تجربة أفضل للمستخدمين في التطبيقات ذات النطاق الترددي العالي
•توفير التكاليف على سعة العودة

السيناريو 2: توجيه الشبكة المنزلية (نفق GTP)

الفوائد:

•تنفيذ سياسة متسقة
•فوترة/شحن مركزي
•تطبيق سياسات VPN/الأمان المؤسسية
•تنقل سلس بين WiFi والخلوية

خيارات اتصال SWx

الخيار 1: اتصال مباشر بـ HSS

حالة الاستخدام: نشرات بسيطة، بيئات مختبرية، HSS واحد

الفوائد:

•زمن انتقال أقل (لا يوجد قفز عبر DRA)
•تكوين مبسط
•سهولة استكشاف الأخطاء

الخيار 2: عبر DRA (وكيل توجيه Diameter)

حالة الاستخدام: نشرات متعددة HSS، سيناريوهات التجوال، الشبكات الكبيرة

الفوائد:

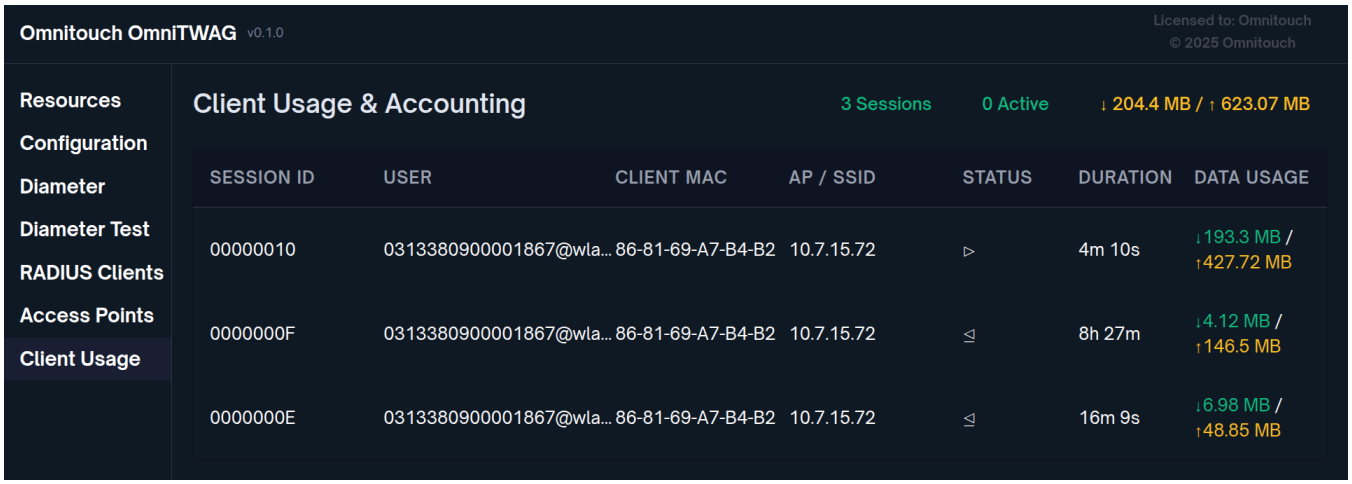
•منطق توجيه مركزي
•توازن الحمل عبر HSS متعددة
•دعم التجوال (التوجيه إلى HSS المنزلية)
•التكرار والتبديل
•ثبات الجلسة

تدفق الشحن

يمكن دمج TWAG بالكامل لإرسال طلبات الشحن عبر Diameter Gy إلى نظام الشحن عبر الإنترنت (OCS).

يسمح ذلك بمحاسبة جميع البيانات المستهلكة على WiFi، مقابل رصيد العميل، ويتم تسليمها عبر AP على RADIUS وتحويلها إلى Gy بواسطة TWAG وإعادة توجيهها إلى DRA/OCS.

في جميع الأوضاع، يتم تتبع الاستخدام بواسطة مقاييس TWAG.



أوضاع الشحن

يدعم TWAG ثلاثة أوضاع شح�ن عبر الإنترنت:

1. الشحن معطل

لا يتم إرسال طلبات التحكم في الائتمان. لا يتم إجراء أي مصادقة لرصيد الحساب.

حالات الاستخدام:

- شبكات WiFi مفتوحة/مجانية
- بيئات مختبرية/اختبار
- الشبكات التي تعتمد على الشحن غير المتصل فقط (محاسبة RADIUS إلى الفوترة)

التدفق:

2. المصادقة فقط

يتم إرسال CCR-Initial (طلب التحكم في الائتمان) إلى OCS في بداية جلسة WiFi للتحقق من أن المشترك لديه رصيد، ولكن لا يتم سحب الرصيد خلال الجلسة.

حالات الاستخدام:

- التحقق من أن المشترك لديه حساب/رصيد نشط
- منع وصول WiFi للحسابات المعلقة
- التحقق من أهلية الخدمة دون تتبع الحصص
- السماح لـ WiFi كخدمة مكافأة/غير محدودة للعملاء الذين يدفعون

التدفق:

التكوين:

- يتم استعلام OCS في بداية الجلسة (CCR-I) ونهايتها (CCR-T)
- لا يتم إرسال رسائل CCR-Update خلال الجلسة
- يتم اعتماد المشترك بناءً على حالة الحساب، وليس الحصة
- يتم الإبلاغ عن الاستخدام في نهاية الجلسة لأغراض معلوماتية فقط

3. شحن Gy عبر الإنترنت بالكامل (تنفيذ كامل)

يتم اتباع تدفق الشحن القياسي 3GPP عبر الإنترنت. يتم تمرير جميع الاستخدامات على WiFi إلى OCS للشحن، مع قطع المشتركين بمجرد تجاوزهم حصتهم.

حالات الاستخدام:

- خدمات البيانات المدفوعة مسبقًا
- WiFi حسب الاستخدام
- خطط قائمة على الحصص (مثل، 10 جيجابايت شهريًا)
- شحن في الوقت الحقيقي وقطع الاتصال

التدفق:

التكوين:

- يتم استعلام OCS في بداية الجلسة (CCR-I)، خلال الجلسة (CCR-U)، وفي النهاية (CCR-T)
- يتم طلب الحصة في كتل قابلة للتكوين (مثل، 10MB، 50MB، 100MB)
- يتم تفعيل CCR-Update عند عتبة قابلة للتكوين (مثل، 80% من الحصة الممنوحة)
- يتم تفعيل مؤقت الصلاحية لإعادة المصادقة إذا لم يتم استنفاد الحصة
- يتم قطع الاتصال بشكل قسري عند استنفاد الحصة
- خصم الرصيد في الوقت الحقيقي

تدفق المصادقة

تسلسل المصادقة الكامل EAP-AKA

النقاط الرئيسية في تدفق المصادقة

1. **MAR/MAA هي نهاية الاتصال مع HSS**: بعد تلقي MAA (استجابة المصادقة المتعددة الوسائط) مع XRES، يتولى TWAG جميع عمليات التحقق اللاحقة محليًا.

2. **يقوم TWAG بإجراء التحقق من RES**: يوفر HSS الاستجابة المتوقعة (XRES)، ولكن يقوم TWAG بمقارنتها مع RES الفعلي من UE. لا يشارك HSS في هذه المقارنة.

3. **تحدث المصادقة في TWAG**: هذا يختلف عن بعض الرسوم البيانية التي تظهر HSS تقوم بالتحقق - في الهيكلية الفعلية 3GPP، يقوم خادم AAA (TWAG) بإجراء المقارنة.

تنسيق الهوية

يستجيب الجهاز بهويته الدائمة (IMSI) بتنسيق NAI:

```
wlan.mnc057.mcc505.3gppnetwork.org@505570000000000001
```

التنسيق: lt;IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org&0

ملاحظة - الرقم الأول، قبل IMSI هو الهوية، وعادة ما يكون 0 ولكن قد يكون رقمًا فرديًا آخر لبطاقات SIM / الهواتف متعددة IMSI.

مفتاح الجلسة الرئيسي (MSK)

مفتاح الجلسة الرئيسي (MSK) هو مفتاح تشفير بطول 512 بت (64 بايت) يتم اشتقاقه خلال مصادقة EAP-AKA. يعمل كمادة المفتاح الجذرية لتأمين اتصال WiFi.

اشتقاق MSK:

1. يقوم كل من UE وTWAG باشتقاق نفس MSK بشكل مستقل
2. يقوم UE بالاشتقاق من CK/IK المحسوبة بواسطة SIM
3. يقوم TWAG بالاشتقاق من CK/IK المستلمة من HSS
4. MSK = PRF'(CK || IK, "Full Authentication", IMSI, ...)

استخدام MSK:

1. **اشتقاق PMK**: PMK = أول 256 بت (32 بايت) من MSK
2. **مصافحة WPA2 الرباعية**: يستخدم كل من UE وAP PMK لاشتقاق PTK
3. **تشفير البيانات**: جميع إطارات بيانات WiFi مشفرة باستخدام المفتاح الرمزي (TK) من PTK

لماذا MSK حاسم:

- **السرية**: بدون MSK، ستكون حركة مرور WiFi غير مشفرة

•**السلامة**: تمنع التلاعب بإطارات WiFi
•**ربط المصادقة**: تربط مصادقة EAP بتشفير WiFi
•**حماية من إعادة التشغيل**: يمنع MSK الجديد هجمات إعادة التشغيل
•**سرية متالية للأمام**: لا يؤثر اختراق MSK واحد على الآخرين

استعادة التزامن

إذا اكتشف الجهاز عدم تطابق رقم التسلسل (SQN خارج التزامن)، يبدأ استعادة التزامن:

1.يحسب الجهاز AUTS (رمز المصادقة - التزامن)
2.يرسل EAP-AKA Synchronization-Failure مع AT-AUTS
3.يقوم TWAG بإعادة توجيه AUTS إلى HSS
4.يقوم HSS بإعادة مزامنة رقم ��تسلسل وتوليد متجهات جديدة
5.يتم إعادة محاولة المصادقة باستخدام متجهات جديدة

هذا يكون شفافًا للمستخدم النهائي ولا يتطلب تدخل المشغل.

دليل التكوين

يتم تكوين TWAG عبر ملفات تكوين Elixir في دليل `config/`. التكوين الرئيسي للتشغيل موجود في `config/runtime.exs`.

بالنسبة لنشر الإنتاج، يتم إدارة التكوين مركزيًا. أدناه هو مرجع فقط، أي قيم تم تغييرها على عقدة الإنتاج ستفقد في المرة القادمة التي يتم فيها تشغيل التنسيق الآلي.

تكوين Diameter

موجود في `config :diameter_ex`:

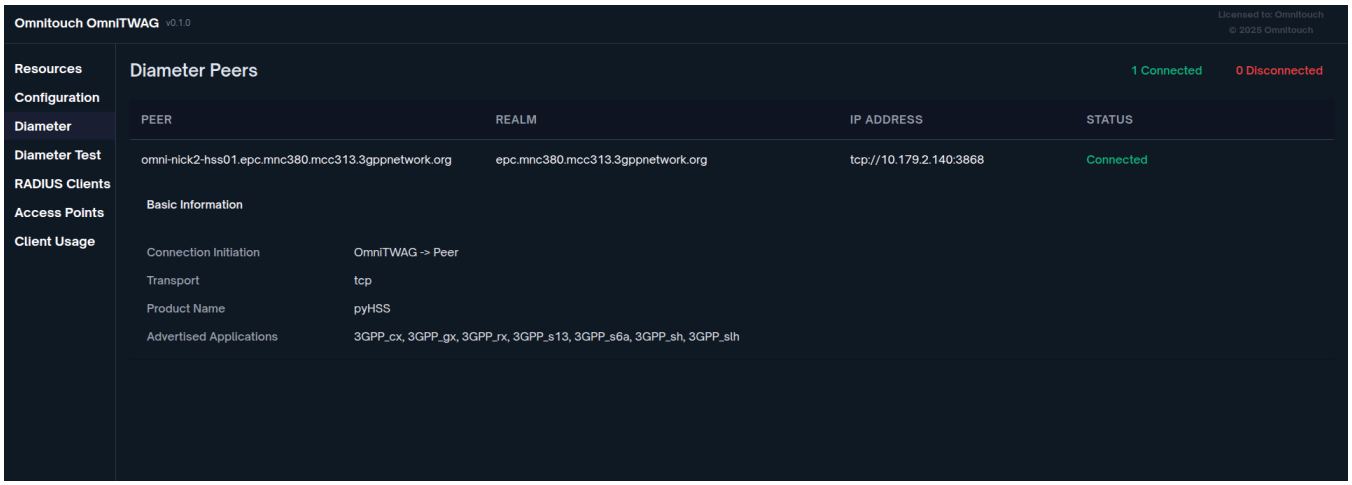
```
config :diameter_ex,
  diameter: [
    {
      # اسم الخدمة لستاك Diameter
      service_name: :omnitouch_twag,

      # عنوان IP المحلي لربط خدمة Diameter
      listen_ip: "10.5.198.200",

      # المنفذ المحلي لاتصالات Diameter (القياسي هو 3868)
      listen_port: 3868,

      # مضيف Diameter Origin-Host
      host: "omnitwag",

      # مجال Diameter Origin-Realm (يتطابق مع مجال شبكتك)
      realm: "epc.mnc057.mcc505.3gppnetwork.org",

      # أقران Diameter (HSS، خوادم AAA)
      peers: [
        {
          # مضيف Diameter Origin-Host
          host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",

          # مجال Diameter Origin-Realm
          realm: "epc.mnc057.mcc505.3gppnetwork.org",

          # عنوان IP للقرين (يمكن أن يكون HSS مباشرة أو DRA)
          ip: "10.179.2.140",

          # منفذ القرين (القياسي هو 3868)
          port: 3868,

          # استخدام TLS لأمان النقل
          tls: false,

          # بروتوكول النقل (diameter_tcp: أو diameter_sctp:)
          transport: :diameter_tcp,

          # بدء الاتصال بالقرين (true) أو الانتظار حتى يتصل القرين (false)
          initiate_connection: true
        }
      ]
    }
```

تنسيق المجال يتبع 3GPP TS 23.003:

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

حيث:

•MNC = رمز الشبكة المحمولة (مثل، 057)
•MCC = رمز الدولة المحمولة (مثل، 505 لأستراليا)

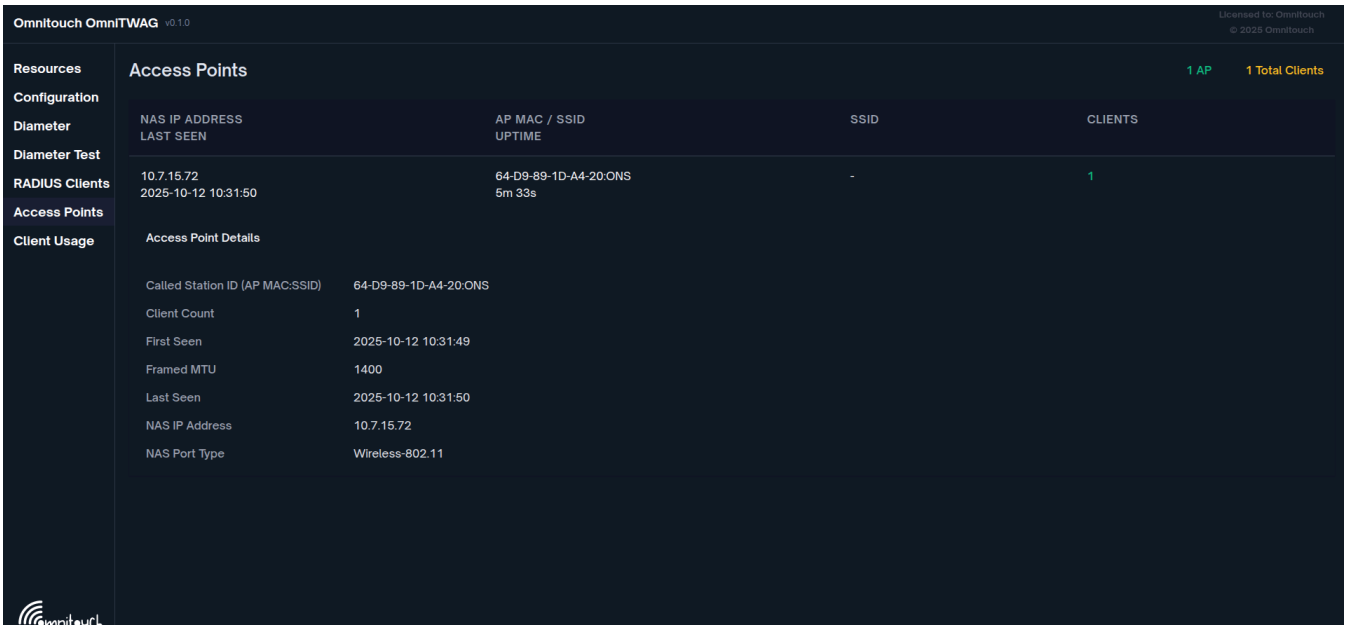


ملاحظة حول استخدام DRA: لاستخدام OmniDRA، قم بتكوين عنوان IP للقرين للإشارة إلى DRA بدلاً من الإشارة مباشرة إلى HSS. سيقوم DRA بعد ذلك بتوجيه الرسائل إلى HSS المناسب بناءً على قواعد التوجيه (مجال الوجهة، نطاق IMSI، إلخ).

تكوين RADIUS

موجود في `config :omnitwag`:

```
config :omnitwag,
  radius_config: [
    # قائمة الشبكات الفرعية المسموح بها لمصادر عملاء RADIUS
    # قائمة فارغة = السماح للجميع (غير موصى به للإنتاج)
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],

    # السر المشترك لعملاء RADIUS
    # يجب أن تستخدم جميع نقاط الوصول هذا السر
    secret: "YOUR_STRONG_SECRET_HERE"
  ]
```



أفضل الممارسات الأمنية:

- استخدم أسرار RADIUS مشتركة قوية (20+ حرف)
- قم بتكوين `allowed_source_subnets` لتقييد وصول AP
- استخدم قواعد جدار الحماية لتقييد الوصول إلى المنافذ 1812/1813

مثال على تكوين الشبكة الفرعية:

```
allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"]
```

إذا كانت فارغة، يتم السماح بجميع المصادر (مناسب فقط للمختبر/الاختبار).

تكوين مراقبة Prometheus

موجود في `config :omnitwag`:

```
config :omnitwag,
  prometheus: %{
    # المنفذ لنقطة نهاية مقاييس Prometheus
    port: 9568
  }
```

يمكن الوصول إلى المقاييس على: `http://<twag-ip>:9568/metrics`

ملخص المنافذ

البروتوكول	المنفذ	الغرض
UDP	1812	مصادقة RADIUS
UDP	1813	محاسبة RADIUS
TCP	3868	Diameter (SWx) إلى (HSS/DRA)
TCP	443	لوحة التحكم HTTPS
TCP	8444	واجهة REST HTTPS
TCP	9568	مقاييس Prometheus

إعداد نقطة الوصول

نقاط الوصول المدعومة

يعمل OmniTWAG مع أي نقطة وصول WiFi تدعم:

- **WPA2-Enterprise** (المصادقة 802.1X)
- **وظيفة عميل RADIUS**
- **طريقة المصادقة EAP-AKA**

المنصات المختبرة: Cisco Aironet، Aruba، Ubiquiti UniFi، Ruckus، نقاط الوصول المعتمدة على hostapd

متطلبات تكوين AP العامة

1. وضع الأمان **WPA2-Enterprise (802.1X)**
2. **خادم RADIUS** يشير إلى عنوان IP لـ TWAG
3. **منفذ مصادقة RADIUS**: 1812
4. **منفذ محاسبة RADIUS**: 1813 (اختياري ولكن موصى به)
5. **السر المشترك لـ RADIUS**: يجب أن يتطابق مع تكوين TWAG
6. **طريقة EAP**: EAP-AKA (أو "الجميع")

مثال تكوين AP Cisco

تكوين CLI:

```
! تكوين خادم RADIUS
radius-server host 10.5.198.200 auth-port 1812 acct-port 1813 key YOUR_SHARED_SECRET

! تكوين SSID مع 802.1X
dot11 ssid OPERATOR-WIFI
   vlan 10
   authentication open eap eap_methods
   authentication network-eap eap_methods
authentication key-management wpa version 2

! ربط SSID بواجهة الراديو
interface Dot11Radio0
 encryption mode ciphers aes-ccm
 ssid OPERATOR-WIFI
```

واجهة الويب:

1. انتقل إلى **الأمان → AAA → خادم RADIUS**
2. أضف خادم RADIUS: `10.5.198.200:1812` مع السر المشترك
3. انتقل إلى تكوين **WLAN**
4. اضبط الأمان على **WPA2-Enterprise**
5. اضبط طريقة EAP على **EAP-AKA** أو **الجميع**
6. قم بتعيين مجموعة خادم RADIUS

مثال تكوين hostapd

لنقاط الوصول المعتمدة على Linux (OpenWrt، الأنظمة المدمجة):

```
# /etc/hostapd/hostapd.conf
```

```
interface=wlan0
driver=nl80211
ssid=OPERATOR-WIFI

WPA2-Enterprise #
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
ieee8021x=1

# تكوين RADIUS
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# تكوين EAP
eap_server=0

# Hotspot 2.0 (اختياري - للتحميل التلقائي)
interworking=1
internet=1
anqp_3gpp_cell_net=505,057
domain_name=wlan.mnc057.mcc505.3gppnetwork.org
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
roaming_consortium=505057
hs20=1
```

أفضل ممارسات بنية الشبكة

مهم: ضع نقاط الوصول وTWAG في مقاطع الشبكة الموثوقة. استخدم قواعد جدار الحماية لـ:

•السماح فقط لنقاط الوصول بالوصول إلى منافذ TWAG 1812/1813
•السماح لـ TWAG بالوصول إلى منفذ HSS 3868
•تقييد الوصول الإداري إلى لوحة التحكم في TWAG (المنفذ 443)

تكامل Hotspot 2.0

نظرة عامة على Hotspot 2.0 (Passpoint)

Hotspot 2.0 (يسمى أيضًا Passpoint أو 802.11u) هو معيار من اتحاد WiFi يمكّن اكتشاف الشبكات WiFi الآمنة والتلقائية والاتصال دون تفاعل المستخدم. إنها التقنية الرئيسية لتحميل WiFi السلس.

الميزات الرئيسية:

•**اكتشاف الشبكة التلقائي**: يجد الجهاز الشبكات المتوافقة بناءً على المعايير
•**المصادقة التلقائية**: يستخدم بيانات اعتماد SIM (EAP-AKA) دون إدخال المستخدم
•**الارتباط الأولي المشفر**: OSEN (المصادقة فقط لخادم OSU) لتوفير أمن
•**اتفاقيات التجوال**: يدعم الشبكات التي تمت زيارتها (مثل التجوال الخلوي)
•**الأولوية**: يفضل الجهاز الشبكات المملوكة للمشغل

تكوين AP لـ Hotspot 2.0

متطلبات AP:

1.**دعم 802.11u**: قدرة استعلام/استجابة ANQP
2.**WPA2-Enterprise**: المصادقة 802.1X
3.**دعم EAP-AKA**: يجب أن يدعم طريقة EAP-AKA
4.**تكوين ANQP**: الإعلان عن معلومات المشغل الصحيحة

مثال على التكوين (AP المعتمد على hostapd):

```
# تكوين Hotspot 2.0 / Passpoint
interworking=1
internet=1
asra=0
esr=0
uesa=0

# تكوين ANQP
anqp_3gpp_cell_net=505,057
domain_name=omnitouchns.com,wlan.mnc057.mcc505.3gppnetwork.org

# تكوين مجال NAI
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# التنسيق: <التشفير>,<المجال>,<طريقة-eap>[معرف-المصادقة:قيمة-المصادقة]
# EAP-AKA = 21
# 2:1 = نوع الاعتماد: SIM
# 5:7 = طريقة EAP الموجهة: لا شيء (EAP-AKA مباشر)

# اتحاد التجوال
roaming_consortium=505057
# MCC=505 (الولايات المتحدة)، MNC=057 (م��دد للمشغل)

# معلومات المكان (اختياري)
venue_group=1
venue_type=8
venue_name=eng:Operator Public WiFi

# تكوين WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
rsn_pairwise=CCMP
ieee8021x=1

# تكوين RADIUS (يشير إلى OmniTWAG)
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# تكوين SSID
ssid=OperatorWiFi
utf8_ssid=1

# إشارة Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:Operator WiFi Network
```

سلوك التحميل التلقائي

كيف يعمل التحميل التلقائي:

1.يقوم الجهاز الذي يحتوي على ملف تعريف Passpoint بإجراء مسح WiFi دوري
2.يرسل استعلام ANQP إلى نقاط الوصول المكتشفة
3.إذا كانت استجابة ANQP تتطابق مع الملف الشخصي (MCC/MNC، اتحاد التجوال):
◦تكون الأولوية عالية (الشبكة المنزلية) أو متوسطة (شريك التجوال)
4.إذا كانت الأولوية ≥ العتبة والإشارة > الحد الأدنى:
◦مصادقة EAP-AKA تلقائية
5.إذا كانت المصادقة ناجحة والأولوي�ة > الاتصال الحالي:
◦التحويل إلى WiFi، قطع بيانات الخلوية
6.مراقبة جودة الإشارة والحفاظ على الاتصال

عوامل الأولوية:

1.**الوطن مقابل التجوال**: تفضل الشبكة المنزلية (مطابقة MCC/MNC) على التجوال
2.**قوة الإشارة**: تفضل الإشارة الأقوى
3.**الأمان**: تفضل WPA2-Enterprise على الشبكات المفتوحة/WPA2-PSK
4.**السياسة**: يمكن للمشغل تكوين الشبكات المفضلة
5.**تجاوز المستخدم**: يمكن للمستخدم تعطيل WiFi يدويًا أو تفضيل الخلوية

المراقبة والإدارة

لوحة التحكم على الويب

يمكن الوصول إلى لوحة المراقبة في الوقت الحقيقي على: https://<twag-ip>/

الميزات:

- **عرض عملاء RADIUS**: المشتركين النشطين، حالة المصادقة، تفاصيل الجلسة
- **عرض نقاط الوصول**: نقاط الوصول المتصلة، عدد العملاء، معلومات SSID
- **عرض استخدام العملاء**: بيانات المحاسبة، وقت الجلسة، استخدام البيانات
- **عرض أقران Diameter**: حا��ة الاتصال HSS/DRA

تكامل Prometheus

قم بتكوين Prometheus لجمع مقاييس TWAG:

```
# prometheus.yml
scrape_configs:
  - job_name: 'omnitwag'
    static_configs:
      - targets: ['10.5.198.200:9568']
    metrics_path: '/metrics'
    scrape_interval: 15s
```

المقاييس المتاحة:

مقاييس خادم RADIUS:

- `radius_access_request_count` - إجمالي حزم طلب وصول RADIUS المستلمة
- `radius_access_accept_count` - إجمالي حزم قبول الوصول المرسلة
- `radius_access_reject_count` - إجمالي حزم رفض الوصول المرسلة
- `radius_access_challenge_count` - إجمالي حزم التحدي المرسلة
- `radius_accounting_request_count{status_type}` - إجمالي حزم طلب المحاسبة (موسومة حسب الحالة: بدء، إيقاف، تحديث مؤقت، المحاسبة على، المحاسبة خارج)
- `radius_active_clients_count` - العملاء المعتمدون حاليًا (يتم الاستطلاع كل 5 ثوانٍ)
- `radius_access_points_count` - نقاط الوصول المسجلة (يتم الاستطلاع كل 5 ثوانٍ)

مقاييس مصادقة EAP-AKA:

- `eap_aka_identity_count` - تبادلات هوية EAP-AKA
- `eap_aka_challenge_count` - تبادلات تحدي EAP-AKA
- `eap_aka_sync_failure_count` - حالات فشل التزامن (أحداث إعادة مزامنة SQN)
- `eap_aka_auth_success_count` - المصادقات الناجحة
- `eap_aka_auth_reject_count` - المصادقات المرفوضة

مقاييس بروتوكول Diameter:

- `diameter_message_count{application, command, direction}` - إجمالي رسائل Diameter (موسومة حسب التطبيق، نوع الأمر، والاتجاه)

مقاييس ذاكرة VM Erlang:

- `vm_memory_total` - إجمالي كمية الذاكرة المخصصة (بايت)
- `vm_memory_processes` - الذاكرة المستخدمة بواسطة عمليات Erlang (بايت)
- `vm_memory_processes_used` - الذاكرة المستخدمة بواسطة عمليات Erlang باستثناء الذاكرة المخصصة غير المستخدمة (بايت)
- `vm_memory_system` - الذاكرة المستخدمة بواسطة نظام تشغيل Erlang (بايت)
- `vm_memory_atom` - الذاكرة المستخدمة بواسطة الذرات (بايت)
- `vm_memory_atom_used` - الذاكرة المستخدمة بواسطة الذرات باستثناء الذاكرة المخصصة غير المستخدمة (بايت)
- `vm_memory_binary` - الذاكرة المستخدمة بواسطة الثنائيات (باي��)
- `vm_memory_code` - الذاكرة المستخدمة بواسطة الكود المحمل (بايت)
- `vm_memory_ets` - الذاكرة المستخدمة بواسطة جداول ETS (بايت)

مقاييس نظام VM Erlang:

- `vm_system_info_process_count` - العدد الحالي لعمليات Erlang
- `vm_system_info_port_count` - العدد الحالي للمنافذ
- `vm_system_info_atom_count` - العدد الحالي للذرات
- `vm_system_info_schedulers` - عدد خيوط المجدول
- `vm_system_info_schedulers_online` - عدد المجدولين المتصلين حاليًا

مقاييس جدولة VM Erlang:

- `vm_statistics_run_queue` - الطول الإجمالي لجميع قوائم التشغيل
- `vm_total_run_queue_lengths_total` - الطول الإجمالي لجميع قوائم التشغيل (مجدولين إجماليين)
- `vm_total_run_queue_lengths_cpu` - الطول الإجمالي لقوائم تشغيل المجدول CPU
- `vm_total_run_queue_lengths_io` - الطول الإجمالي لقوائم تشغيل المجدول IO

جمع المقاييس:

- يتم إصدار مقاييس RADIUS وEAP-AKA في الوقت الحقيقي عند حدوث الأحداث
- يتم استطلاع عدد العملاء ونقاط الوصول النشطة كل 5 ثوانٍ
- ي��تم استطلاع مقاييس VM كل 5 ثوانٍ من وقت تشغيل Erlang
- يتم عرض جميع المقاييس بتنسيق Prometheus على `http://<twag-ip>:9568/metrics`

التسجيل

يستخدم TWAG مسجل Elixir للتسجيل المنظم.

عرض السجلات (systemd):

```
# متابعة السجل في الوقت الحقيقي
journalctl -u twag -f

# آخر 100 سطر
journalctl -u twag -n 100

# السجلات منذ آخر تشغيل
journalctl -u twag -b

# السجلات لفترة زمنية محددة
"journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-12 11:00:00
```

رسائل السجل الرئيسية:

- `خادم RADIUS يستمع على المنفذ 1812` - بدء تشغيل الخادم
- `من {IP}: تم استلام طلب الوصول` - طلب RADIUS من AP
- `المرحلة 1: استجابة الهوية - EAP` الهوية الأولية
- `المرحلة 2: تحدي AKA` - تم إرسال التحدي إلى الجهاز
- `المصادقة مقبولة` - مصادقة ناجحة
- `المصادقة مرفوضة` - فشلت المصادقة
- `AP مسجلة: {IP}` - تم اكتشاف AP جديدة

استكشاف الأخطاء وإصلاحها

فشل المصادقة

الأعراض: لا يمكن للعميل الاتصال بـ WiFi

خطوات التشخيص:

1. تحقق من سجلات TWAG: `journalctl -u twag -f`
2. تحقق من تطابق السر المشترك لـ RADIUS بين AP وTWAG
3. تأكد من وصول حزم RADIUS إلى TWAG: `tcpdump -i eth0 port 1812`
4. تحقق من توفير المشترك في HSS/التكوين

الأسباب الشائعة:

- السر المشترك لـ RADIUS غير صحيح
- جدار الحماية يمنع UDP 1812/1813
- عدم تطابق RES/XRES (Ki خاطئ أو تكوين HSS خاطئ)
- رقم التسلسل (SQN) خارج التزامن (يجب أن يتعافى تلقائيًا عبر إعادة المزامنة)
- مشاكل في الاتصال الشبكي بين AP وTWAG

مشاكل اتصال Diameter

الأعراض: عدم اتصال القرين Diameter بـ HSS/DRA

خطوات التشخيص:

1.تحقق من الاتصال الشبكي: `telnet <hss-ip> 3868`
2.تحقق من تكوين Diameter (Origin-Host، Origin-Realm، IP القرين)
3.راجع سجلات HSS/DRA لمحاولات الاتصال
4.تحقق من جدار الحماية للسماح بـ TCP 3868

الأسباب الشائعة:

•IP/المنفذ غير صحيح للقرين في التكوين
•جدار الحماية يمنع TCP 3868
•عدم تطابق Origin-Host/Realm
•HSS/DRA لا تقبل الاتصال من TWAG

مشاكل الأداء

الأعراض: مصادقة بطيئة (>5 ثوانٍ)

خطوات التشخيص:

1.تحقق من زمن استجابة HSS
2.قياس زمن الانتقال الشبكي: `ping <hss-ip>`, `mtr <hss-ip>`
3.مراقبة استخدام موارد TWAG: `top`, `htop`
4.مراجعة إعدادات مهلة طلب Diameter

الأسباب الشائعة:

•مهلة استعلام HSS أو استجابة بطيئة
•زمن انتقال شبكي مرتفع
•استنفاد موارد TWAG (CPU/ذاكرة)
•عدد كبير جدًا من المصادقات المتزامنة

أدوات التصحيح

التقاط الحزم

```
# التقاط حركة مرور RADIUS
tcpdump -i eth0 -n port 1812 or port 1813 -w radius.pcap

# التقاط حركة مرور Diameter
tcpdump -i eth0 -n port 3868 -w diameter.pcap

# الالتقاط من AP محدد
tcpdump -i eth0 -n host 10.7.15.72 and port 1812 -w radius-ap1.pcap
```

تحليل باستخدام Wireshark (بدعم محللات RADIUS وDiameter).

وحدة التحكم التفاعلية

قم بالاتصال بـ TWAG الجاري للتصحيح المباشر:

```
# قشرة عن بُعد إلى TWAG الجاري
<iex --sname debug --remsh twag@hostname --cookie <cookie
```

من وحدة تحكم IEx:

```
# قائمة بجميع العملاء المعتمدين
CryptoState.keys()

# الحصول على حالة عميل محدد
CryptoState.get("050533805790001867@wlan.mnc057.mcc505.3gppnetwork.org")

# قائمة بجميع APs
APState.list()

# قائمة بجلسات المحاسبة
ClientUsage.list()
```

رسائل الخطأ الشائعة

رسالة الخطأ	المعنى	الحل
فشل التحقق من Message-Authenticator	عدم تطابق السر المشترك	تحقق من تطابق السر المشترك لـ RADIUS بين AP وTWAG
فشل التحقق من RES: المتوقع <XRES>، حصلت على <RES>	الاستجابة للمصادقة غير صحيحة	تحقق من Ki لـ SIM، تحقق من توفير HSS
مهلة اتصال القرين Diameter	لا يمكن الوصول إلى HSS	تحقق من الشبكة، جدار الحماية، تكوين HSS
فشل فك تشفير رسالة EAP	حزمة EAP غير صحيحة	تحقق من البرنامج الثابت لـ AP، قد تحتاج إلى تحديث AP
نوع EAP-AKA غير معروف	رسالة EAP-AKA غير مدعومة	يستخدم الجهاز إصدار غير قياسي من EAP-AKA
يتطلب إعادة مزامنة رقم التسلسل	SQN خارج التزامن	طبيعي، سيقوم الجهاز بإعادة المزامنة تلقائيًا

الامتثال للمعايير

يطبق OmniTWAG المواصفات التالية من 3GPP وIETF:

•**3GPP TS 23.402**: تحسينات المعمارية للوصولات غير 3GPP
•**3GPP TS 24.302**: الوصول إلى EPC عبر الشبكات غير 3GPP
•**3GPP TS 29.273**: واجهات SWx/SWm المعتمدة على Diameter
•**3GPP TS 33.402**: جوانب الأمان للوصولات غير 3GPP
•**3GPP TS 35.206**: مواصفة خوارزمية Milenage
•**RFC 2865**: مصادقة RADIUS
•**RFC 2866**: محاسبة RADIUS
•**RFC 3579**: دعم RADIUS لـ EAP
•**RFC 4187**: بروتوكول المصادقة EAP-AKA
•**RFC 5448**: EAP-AKA' (الإصدار المحسن)

ملخص

يوفر OmniTWAG، الذي أنشأته Omnitouch، حلاً كاملاً متوافقًا مع المعايير لتحميل WiFi 3GPP:

1.**نشر مرن**: يدعم الخروج المحلي أو حركة المرور الموجهة إلى المنزل
2.**معتمد على المعايير**: ينفذ بروتو��ولات 3GPP SWx، EAP-AKA، RADIUS
3.**مصادقة آمنة**: مصادقة متبادلة تعتمد على SIM مع إعادة مزامنة تلقائية
4.**تشفير قوي**: مفاتيح مشتقة من MSK توفر تشفير WPA2
5.**جاهز لـ Hotspot 2.0**: يمكّن التحميل التلقائي بالكامل بدون لمس
6.**تحكم المشغل**: يحافظ على الهوية، والسياسة، والفوترة اختياريًا
7.**اتصال مرن**: اتصال مباشر بـ HSS أو عبر OmniDRA للتوجيه/توازن الحمل

إصدار الوثيقة: 2.0 آخر تحديث: 2025 OmniTWAG - بوابة الوصول الموثوق WiFi حقوق الطبع والنشر © 2025 Omnitouch. جميع الحقوق محفوظة.