تكوين FTD Remote Access VPN مع MSCHAPv2 عبر RADIUS

المحتويات

المقدمة

يوضح هذا المستند كيفية تمكين بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي ل Microsoft الإصدار 2 (MS-CHAPv2) كطريقة مصادقة عبر مركز إدارة FirePOWER (FMC) لعملاء شبكة VPN للوصول عن بعد باستخدام مصادقة خدمة طلب اتصال المستخدم البعيد (RADIUS).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Firepower Threat Defense (FTD)
- مركز إدارة Firepower (FMC)
- محرك خدمات الهوية (ISE)
- Cisco AnyConnect Secure Mobility Client
- بروتوكول RADIUS

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- FMCv - 7.0.0 (بنية 94)
- FTDv - 7.0.0 (البنية 94)
- ISE - 2.7.0.356

- AnyConnect - 4.10.02086
- نظام التشغيل Windows 10 Pro

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

افتراضيا، يستخدم FTD بروتوكول مصادقة كلمة المرور (PAP) كطريقة مصادقة مع خوادم RADIUS لاتصالات AnyConnect VPN.

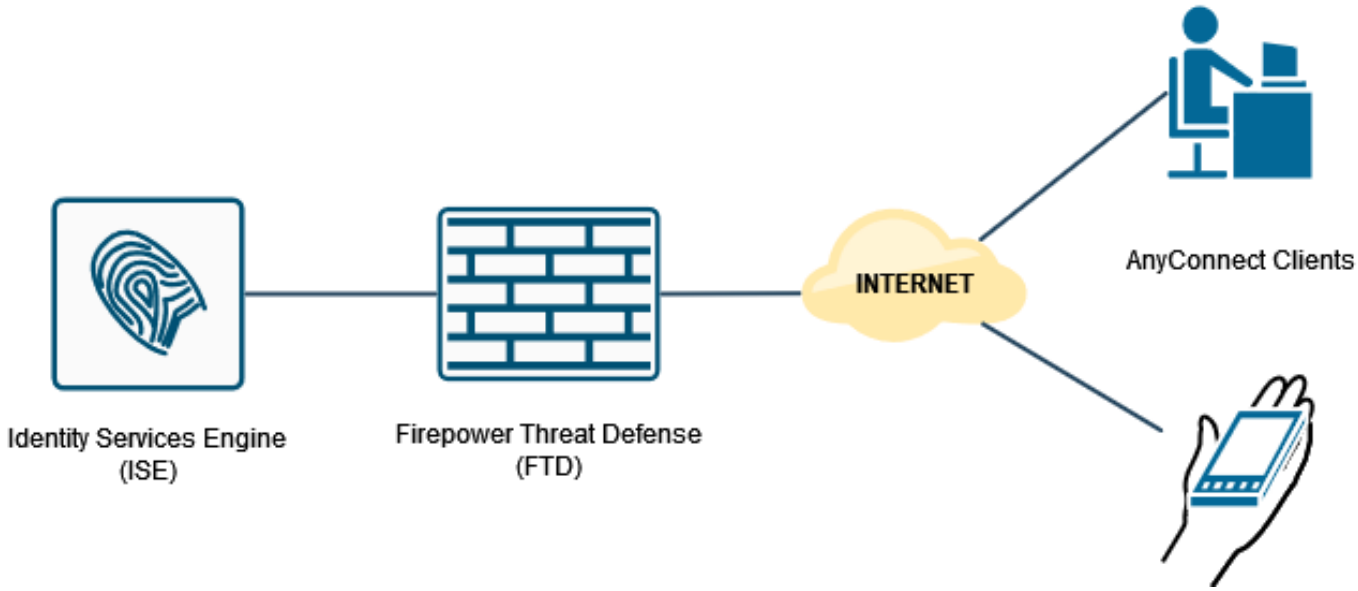
توفر PAP طريقة بسيطة للمستخدمين لإثبات هويتهم من خلال مصافحة ثنائية الإتجاه. يتم تشفير كلمة مرور PAP بسر مشترك وهي بروتوكول المصادقة الأقل تطورا. PAP ليست طريقة مصادقة قوية لأنها توفر حماية قليلة من هجمات التجربة والخطأ المتكررة.

توفر مصادقة MS-CHAPv2 مصادقة متبادلة بين الأقران وميزة تغيير كلمة المرور.

لتمكين MS-CHAPv2 كبروتوكول مستخدم بين ASA وخادم RADIUS لاتصال VPN، يجب تمكين إدارة كلمة المرور في ملف تعريف الاتصال. يؤدي تمكين إدارة كلمة المرور إلى إنشاء طلب مصادقة MS-CHAPv2 من FTD إلى خادم RADIUS.

التكوين

الرسم التخطيطي للشبكة

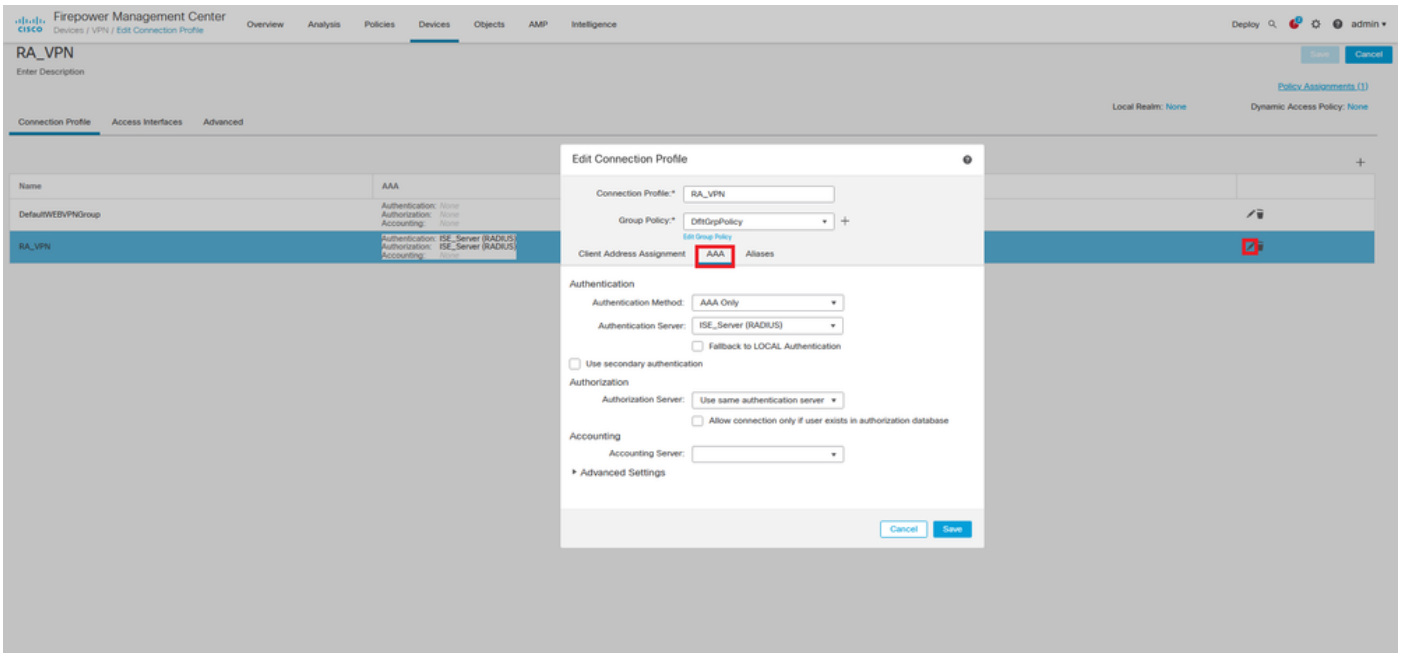


تكوين شبكة VPN RA باستخدام مصادقة AAA/RADIUS عبر FMC

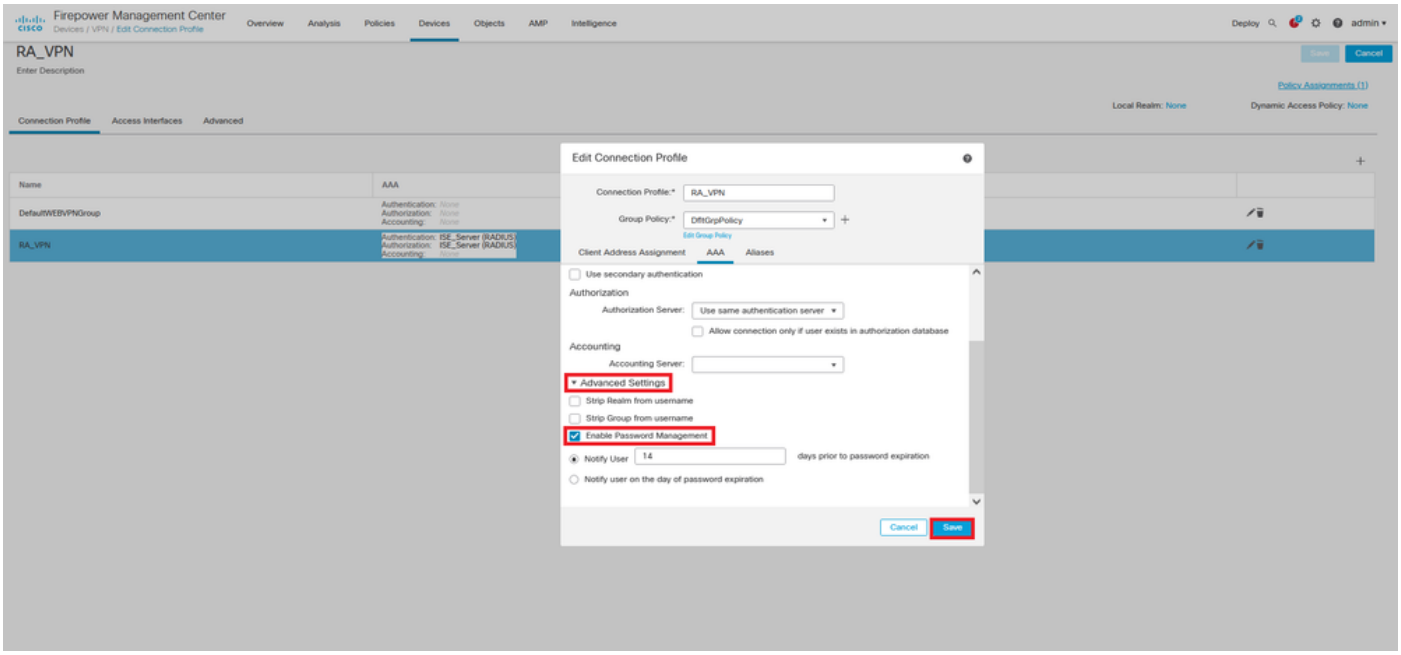
للحصول على إجراء مفصل خطوة بخطوة، ارجع إلى هذا المستند وهذا الفيديو:

- تكوين AnyConnect Remote Access VPN على FTD
- تكوين AnyConnect الأولي لـ FTD المدار بواسطة FMC

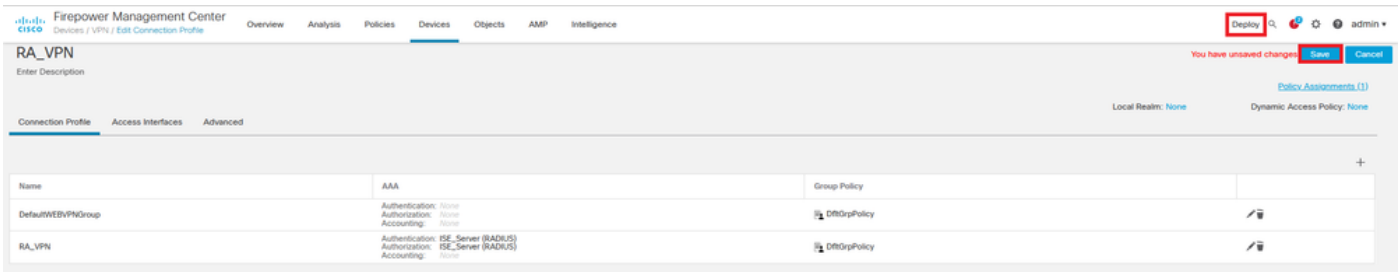
الخطوة 1. بمجرد تكوين شبكة VPN للوصول عن بعد، انتقل إلى **الأجهزة > الوصول عن بعد**، وحرر ملف تعريف الاتصال الذي تم إنشاؤه حديثا، ثم انتقل إلى علامة التبويب **AAA**.



مددت **الإعدادات المتقدمة** قسم وطقطقت **الـ enable كلمة إدارة** تدقيق صندوق. طقطقة **حفظ**.



حفظ ونشر.



تكوين VPN للوصول عن بعد على FTD CLI:

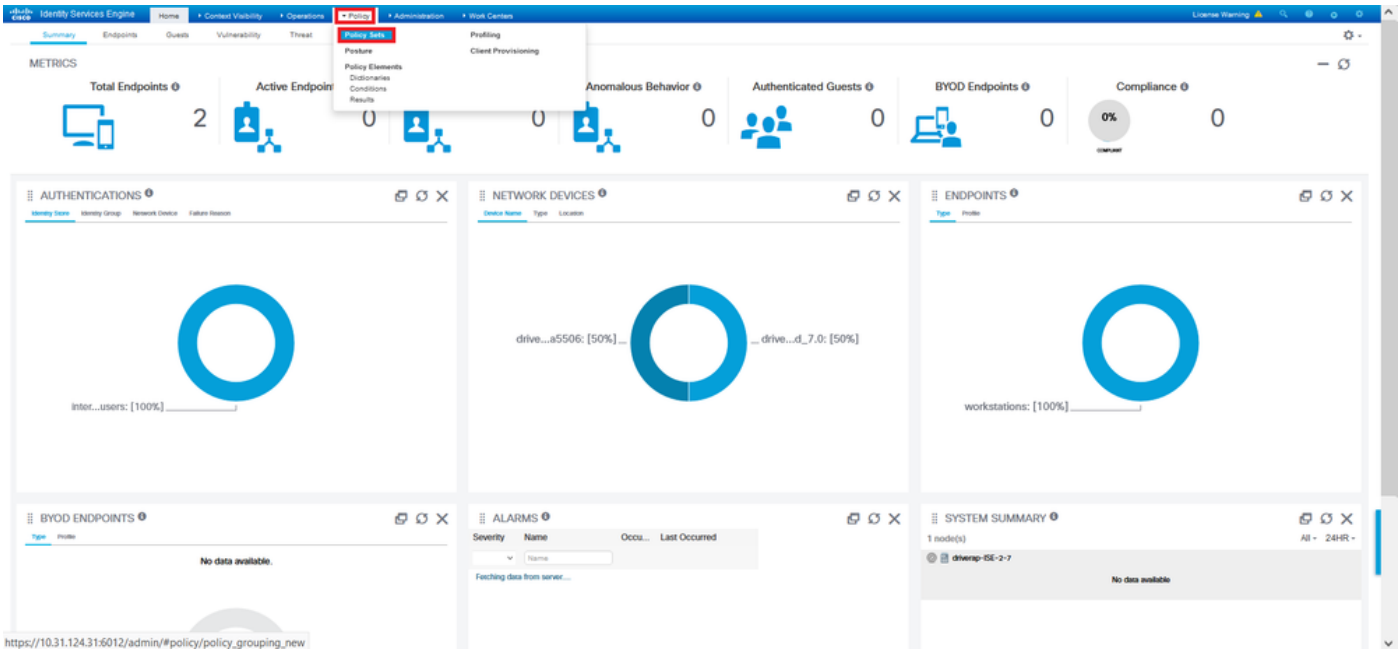
```
ip local pool AC_Pool 10.0.50.1-10.0.50.100 mask 255.255.255.0

interface GigabitEthernet0/0
nameif Outside_Int
security-level 0
ip address 192.168.0.100 255.255.255.0

aaa-server ISE_Server protocol radius
aaa-server ISE_Server host 172.16.0.8
key *****
authentication-port 1812
accounting-port 1813

crypto ca trustpoint RAVPN_Self-Signed_Cert
enrollment self
fqdn none
subject-name CN=192.168.0.100
keypair <Default-RSA-Key>
crl configure

ssl trust-point RAVPN_Self-Signed_Cert

webvpn
enable Outside_Int
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.10.02086-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
no disable
error-recovery disable

group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev2 ssl-client
user-authentication-idle-timeout none
webvpn
anyconnect keep-installer none
anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none

tunnel-group RA_VPN type remote-access
tunnel-group RA_VPN general-attributes
address-pool AC_Pool
authentication-server-group ISE_Server
password-management
tunnel-group RA_VPN webvpn-attributes
group-alias RA_VPN enable
```

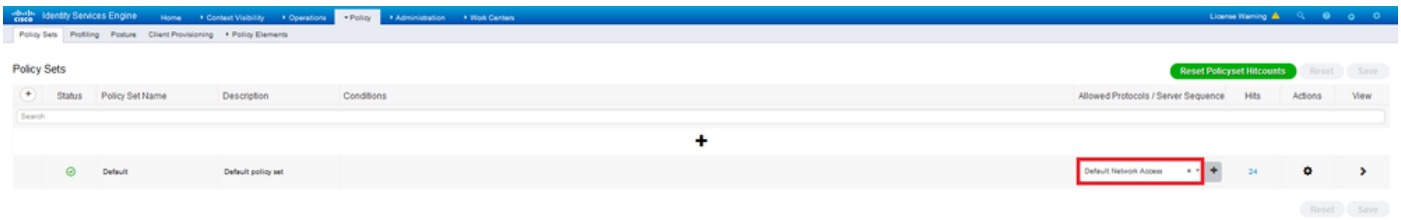
تكوين ISE لدعم MS-CHAPv2 كبروتوكول مصادقة

يفترض ما يلي:

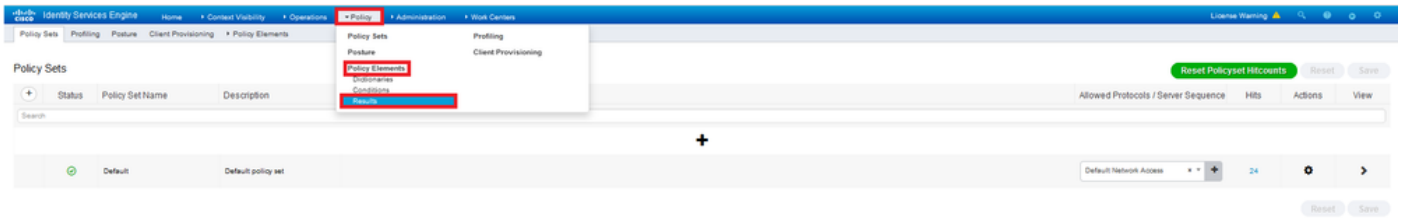
1. تمت إضافة FTD بالفعل كجهاز شبكة على ISE حتى يمكنه معالجة طلبات الوصول إلى RADIUS من FTD.
2. هناك على الأقل مستخدم واحد متوفر لـ ISE لمصادقة عميل AnyConnect.

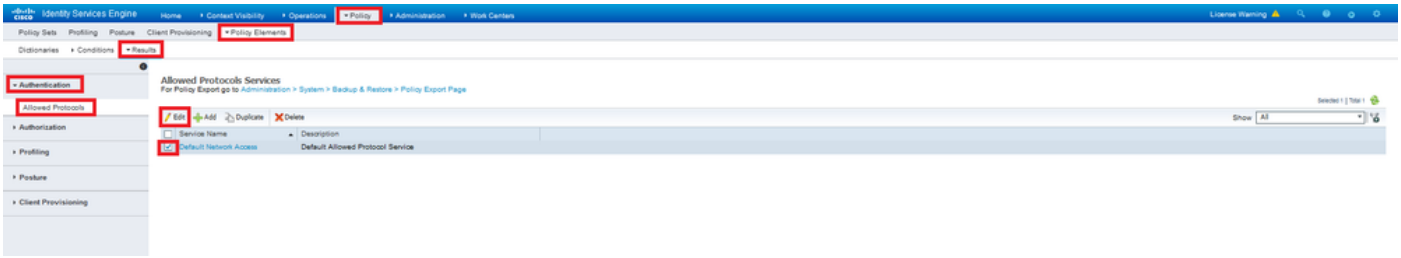
الخطوة 2. انتقل إلى **النهج > مجموعات النهج** وابحث عن نهج **البروتوكولات المسموح بها** المرفق بمجموعة النهج حيث يتم مصادقة مستخدمي AnyConnect لديك. في هذا المثال، توجد مجموعة نهج واحدة فقط لذلك يكون النهج قيد البحث هو *Default Network Access*.



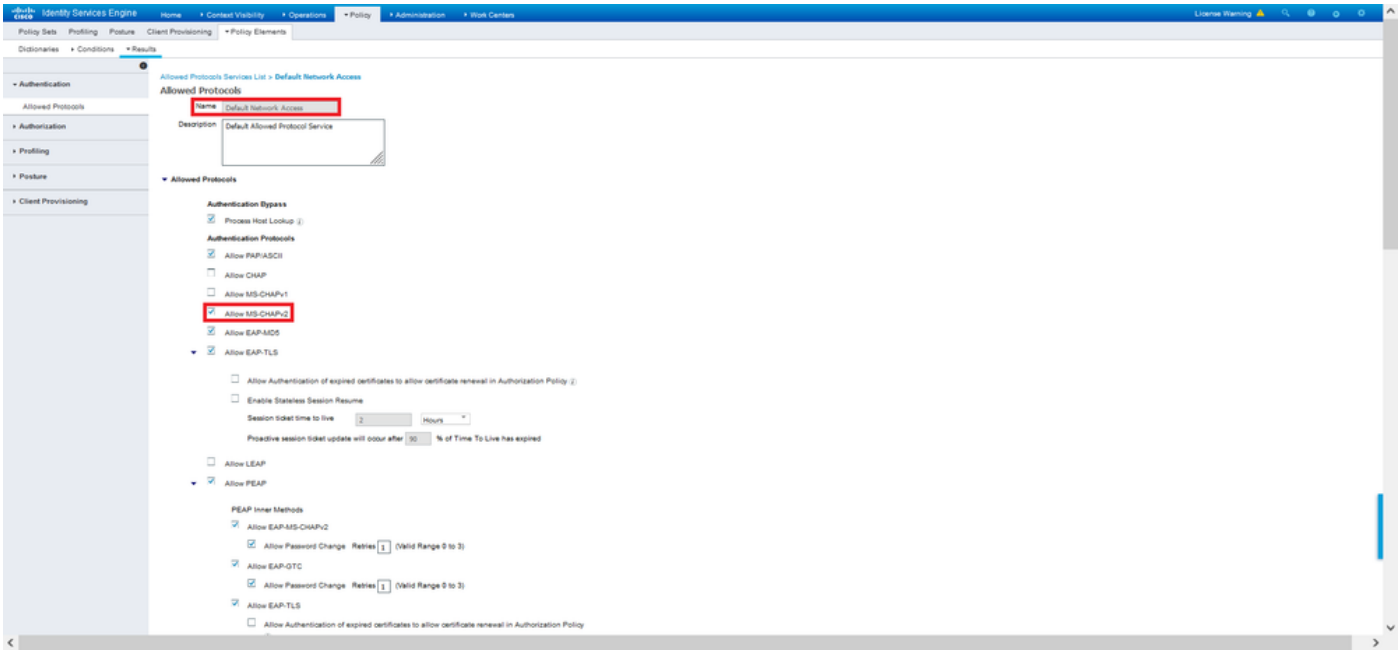


الخطوة 3. انتقل إلى **السياسة > عناصر السياسة > النتائج**. تحت **المصادقة > البروتوكولات المسموح بها** أختر **وصول الشبكة الافتراضي** وقم بتحريره.



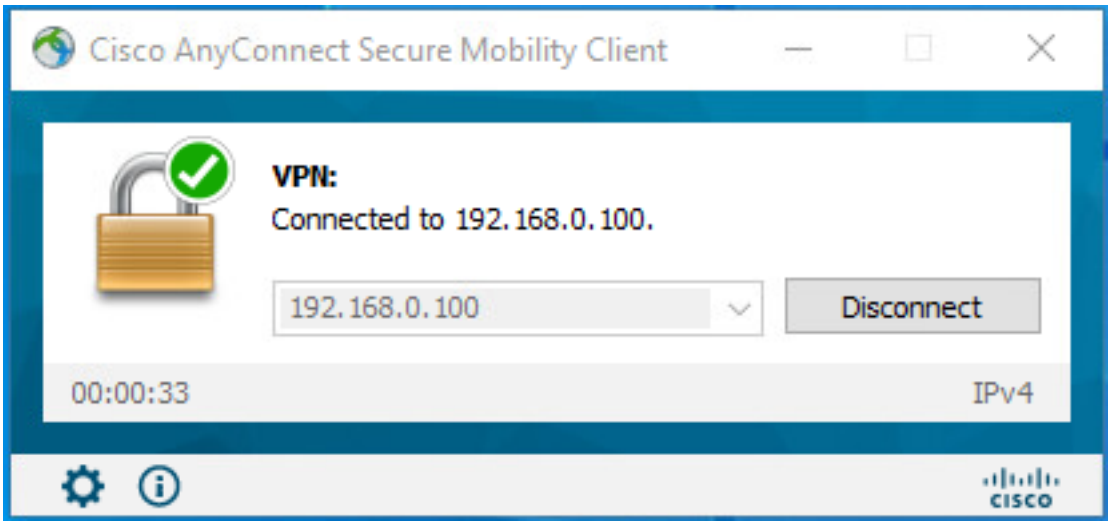


تأكد من تحديد خانة الاختياري **السماح ب MS-CHAPv2**. انزلق إلى الأسفل **واحفظها**.

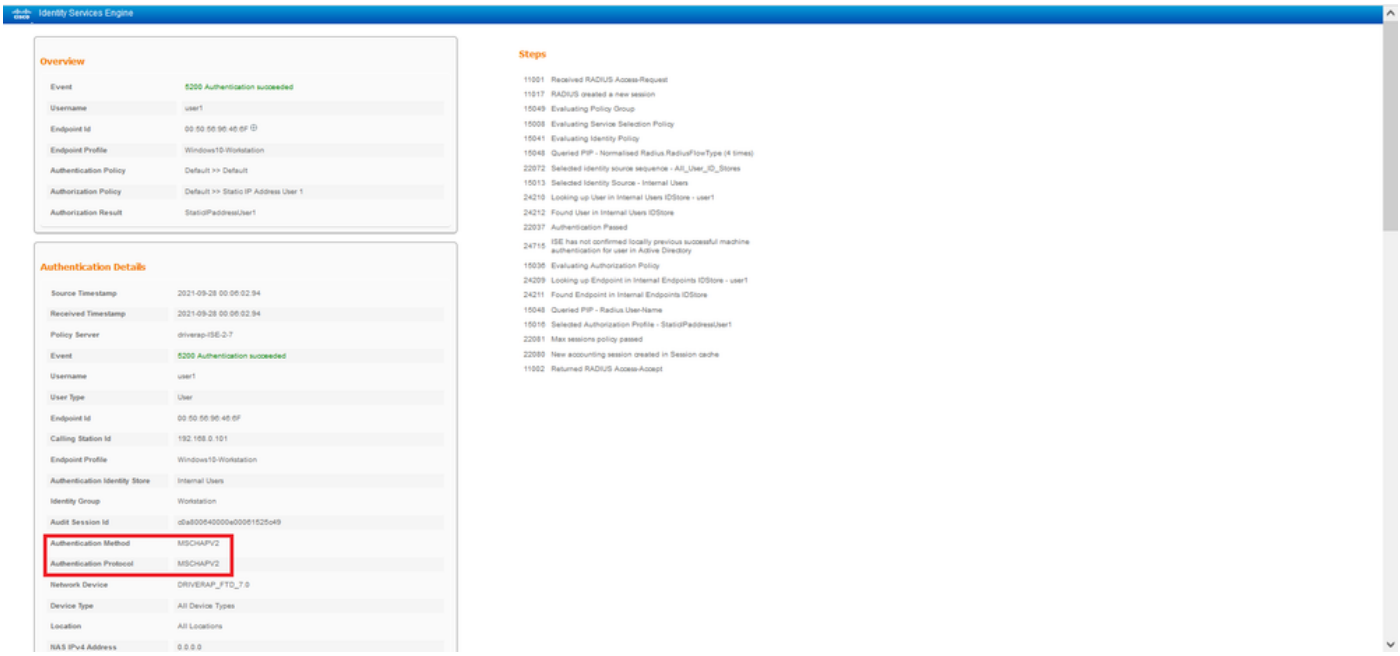


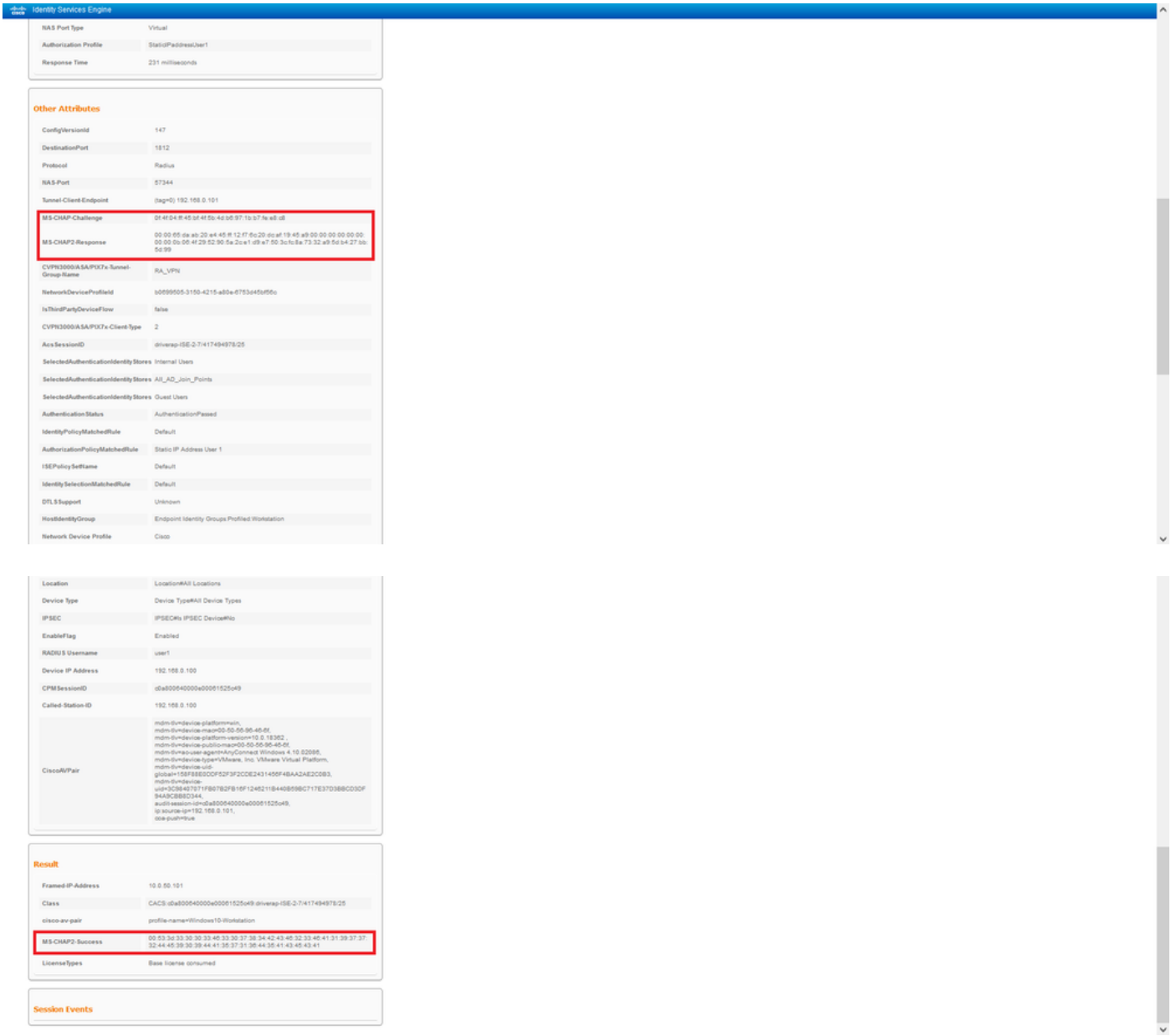
التحقق من الصحة

انتقل إلى جهاز العميل حيث تم تثبيت Cisco AnyConnect Secure Mobility Client. قم بالاتصال ب "وحدة الاستقبال والبث الخاصة ب FTD" (يتم إستخدام جهاز Windows في هذا المثال) واكتب بيانات اعتماد المستخدم.



سجل RADIUS Live على عرض ISE:





ملاحظة: يستخدم أمر **مصادقة AAA-Server** دائما PAP لإرسال طلبات المصادقة إلى خادم

اذه باستخدام MS-CHAPv2 إستخدام الحماية على إجبار جدار الحماية إلى طريقة دجوت الو، RADIUS الأمر.

Firepower# **إختبار مصادقة AAA-Server ISE_Server Host 172.16.0.8 username user1 كلمة مرور xxxxxx**
المعلومات: محاولة إختبار المصادقة إلى عنوان IP (172.16.0.8) (المهلة: 12 ثانية)
المعلومات: المصادقة ناجحة

ملاحظة: الآن قم بتعديل **سمات PPP لمجموعة النفق** عبر Flex-config حيث أنه بعد ذلك تؤثر على بروتوكولات المصادقة التي يتم التفاوض عليها عبر RADIUS اتصالات AnyConnect VPN (SSL و IPSec).

سمات PPP ل Tunnel-group RA_VPN
لا توجد مصادقة حزمة مصادقة
CHAP لبروتوكول المصادقة
ms-chap-v1 المصادقة
ms-chap-v2 توجد مصادقة
لا يوجد وكيل مصادقة

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم المعلومات التي يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

على Fتي دي:

- **debug radius all**

على ISE:

- سجلات RADIUS المباشرة

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).