تكوين تكامل Active Directory مع ASDM لمصادقة الدخول الأحادي ومصادقة البوابة المقيدة (الإدارة في المربع)

المحتويات

المقدمة

يصف هذا المستند تكوين مصادقة البوابة المقيدة (المصادقة النشطة) وتسجيل الدخول الأحادي (المصادقة الخاملة) على الوحدة النمطية FirePOWER باستخدام ASDM (مدير أجهزة الأمان القابل للتكيف).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة جدار حماية ASDM (جهاز الأمان القابل للتكيف)
- معرفة وحدة FirePOWER
- خدمة دليل الوزن الخفيف (LDAP)
- Firepower UserAgent

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الوحدات النمطية ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA 5516-X) التي تشغل الإصدار 5.4.1 أو أعلى.
- الوحدة النمطية ASA FirePOWER (ASA 5515-X، ASA 5525-X، ASA 5545-X، ASA 5555-X) التي تشغل الإصدار 6.0.0 أو أعلى من البرنامج.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

توزع مصادقة المدخل المقيدة أو المصادقة النشطة بصفحة تسجيل دخول ويلزم توفر بيانات اعتماد المستخدم للمضيف للوصول إلى الإنترنت.

توفر المصادقة السالبة أو الدخول الأحادي مصادقة سلسة لمستخدم لموارد الشبكة والوصول إلى الإنترنت دون إدخال بيانات اعتماد المستخدم عدة مرات. يمكن تحقيق مصادقة تسجيل الدخول الأحادي إما من خلال وكيل مستخدم FirePOWER أو مصادقة مستعرض NTLM.

ملاحظة: مصادقة البوابة المقيدة، يجب أن يكون ASA في الوضع الموجه.

ملاحظة: يتوفر الأمر Captive Portal في الإصدار 9.5(2) من ASA والإصدارات المتأخرة.

التكوين

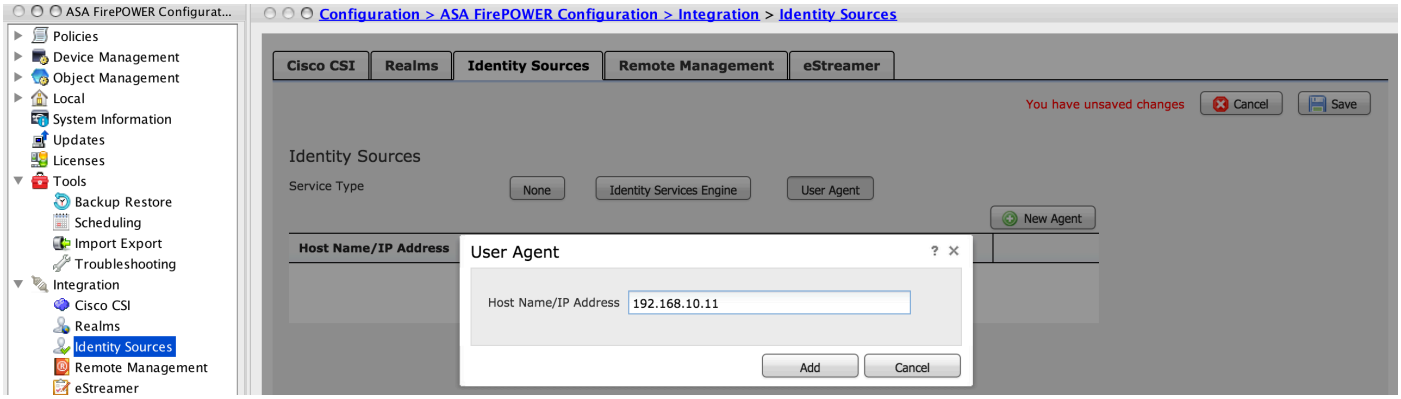
الخطوة 1. تكوين وكيل مستخدم Firepower لتسجيل الدخول الأحادي.

يشرح هذا القسم كيفية تكوين "وكيل مستخدم FirePOWER" في جهاز Windows:

[تثبيت وكيل مستخدم Sourcefire وإلغاء تثبيته]

الخطوة 2. دمج الوحدة النمطية FirePOWER (ASDM) مع وكيل المستخدم.

سجل الدخول إلى ASDM، انتقل إلى **التكوين > ASA FirePOWER Configuration > التكامل > مصادر الهوية** وانقر فوق خيار **وكيل المستخدم**. بعد النقر فوق خيار **وكيل المستخدم** وتكوين عنوان IP لنظام وكيل المستخدم. انقر فوق **إضافة**، كما هو موضح في الصورة:



انقر فوق الزر **حفظ** لحفظ التغييرات.

الخطوة 3. دمج FirePOWER مع Active Directory.

الخطوة 3.1 أنشئ المجال.

سجل الدخول إلى ASDM، انتقل إلى **التكوين > ASA FirePOWER Configuration > التكامل > Realms**. انقر فوق **إضافة حيز جديد**.

الاسم والوصف: قم بإعطاء اسم/وصف لتعريف النطاق بشكل فريد.

الكتابة: الإعلان

مجال AD الأساسي: اسم مجال Active Directory (اسم NETBIOS).

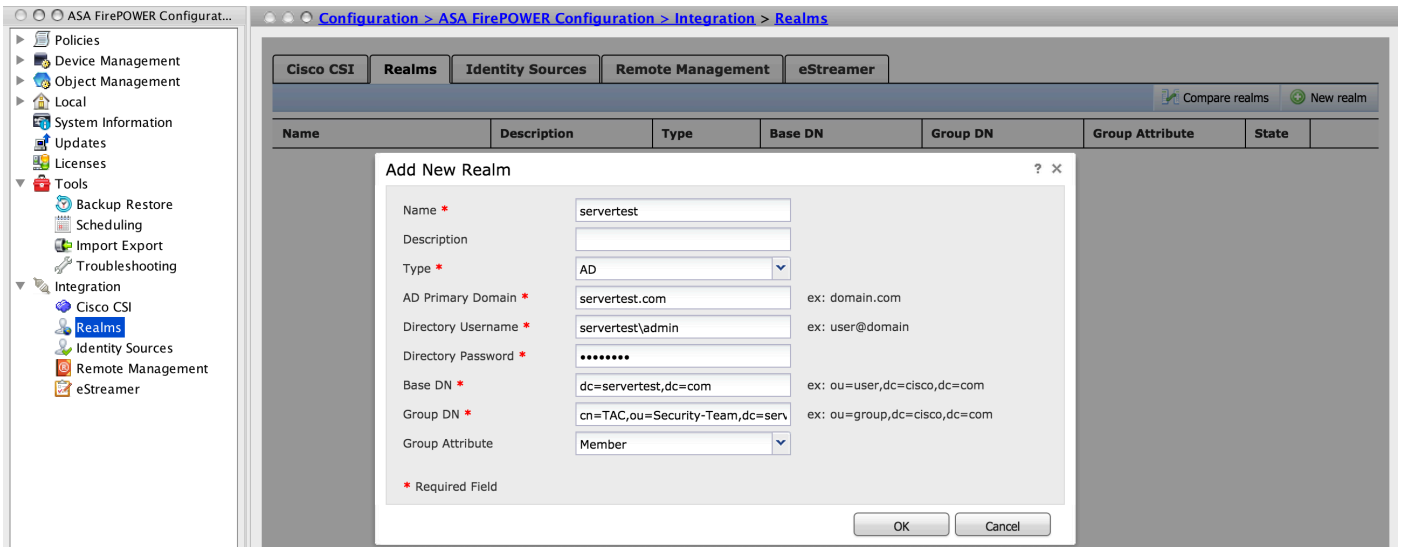
اسم مستخدم الدليل: حدد <*username*>.

كلمة مرور الدليل: حدد <*كلمة المرور*>.

شبكة DN الأساسية: المجال أو شبكة OU محددة من حيث سيبدأ النظام البحث في قاعدة بيانات LDAP.

DN للمجموعة: حدد DN للمجموعة.

سمة المجموعة: حدد عضو الخيار من القائمة المنسدلة.



انقر على **موافق** لحفظ التكوين.

يمكن أن تساعدك هذه المقالة على اكتشاف قيم DN الأساسية و DN الخاصة بالمجموعة.

[تعريف سمات كائن LDAP لخدمة Active Directory]

الخطوة 3.2 أضف عنوان IP/اسم المضيف لخادم الدليل.

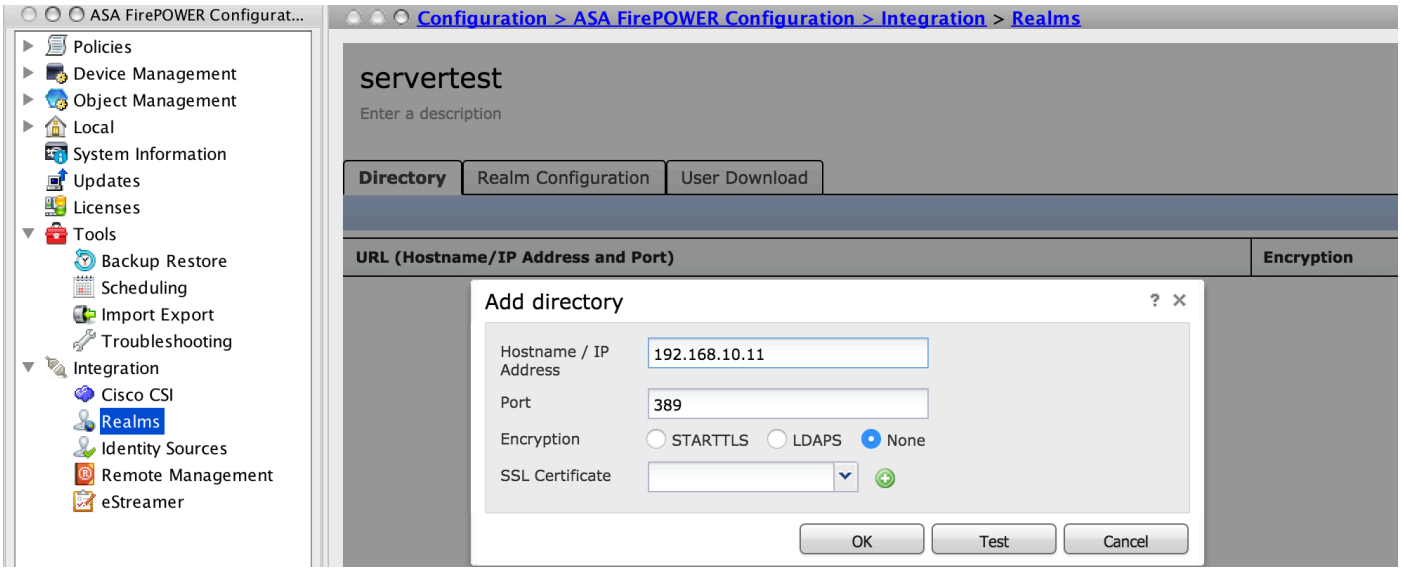
لتحديد AD Server IP/اسم المضيف، انقر فوق **إضافة دليل**.

اسم المضيف/عنوان IP: قم بتكوين عنوان IP/اسم المضيف لخادم AD.

المنفذ: حدد رقم منفذ LDAP الخاص ب Active Directory (الافتراضي 389).

شهادة التشفير/SSL: (إختياري) لتشفير الاتصال بين خادم FMC وخادم AD، ارجع إلى هذه المقالة:

[التحقق من كائن المصادقة على نظام FireSIGHT لمصادقة Microsoft AD عبر SSL/T...]



انقر **إختبار** للتحقق من اتصال FMC بخادم AD. انقر الآن فوق **موافق** لحفظ التكوين.

الخطوة 3.3 قم بتعديل تكوين النطاق.

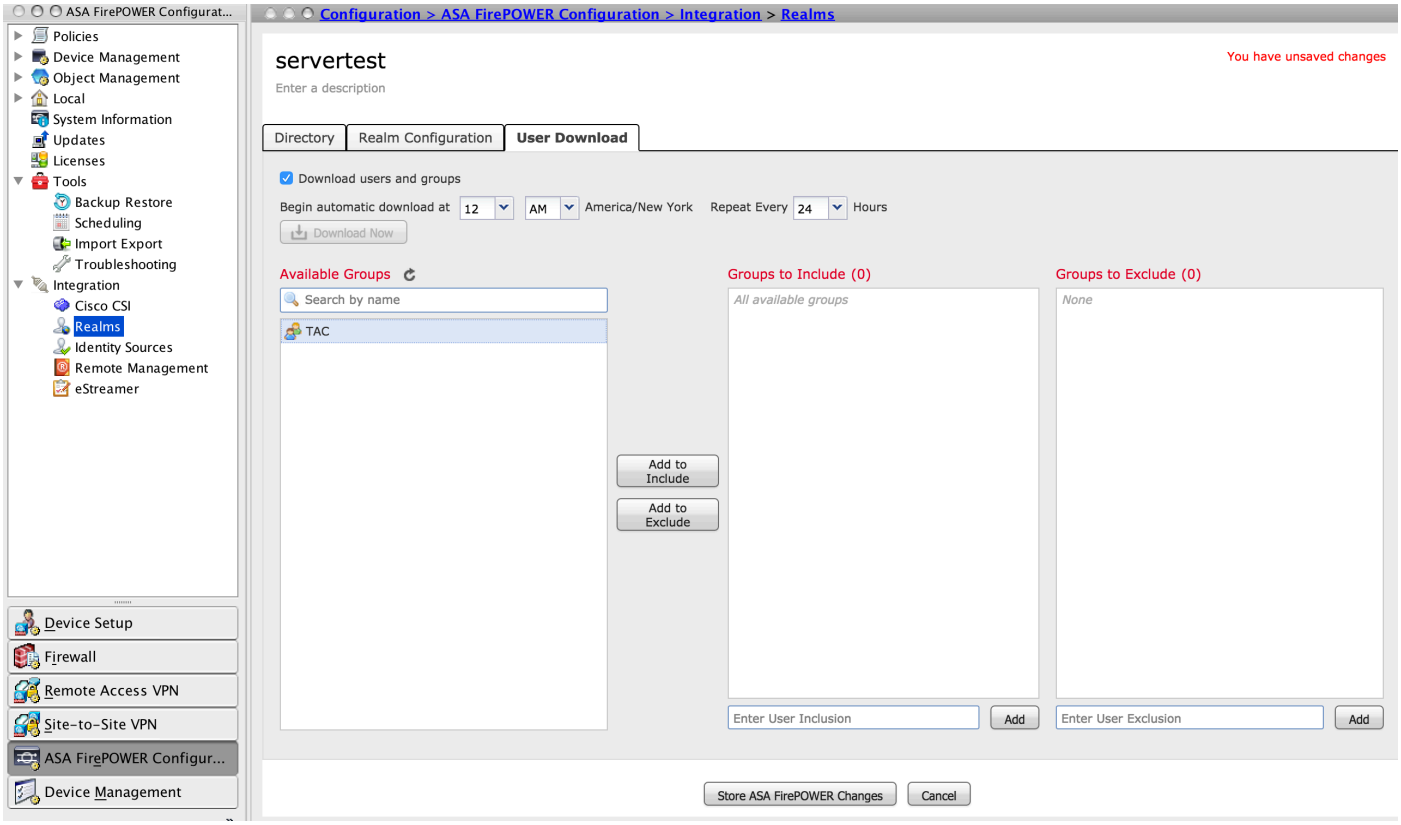
لتعديل تكوين التكامل لخادم AD والتحقق من صحته، انتقل إلى **تكوين النطاق**.

الخطوة 3.4 تنزيل قاعدة بيانات المستخدم.

انتقل إلى **تنزيل المستخدم** لجلب قاعدة بيانات المستخدم من خادم AD.

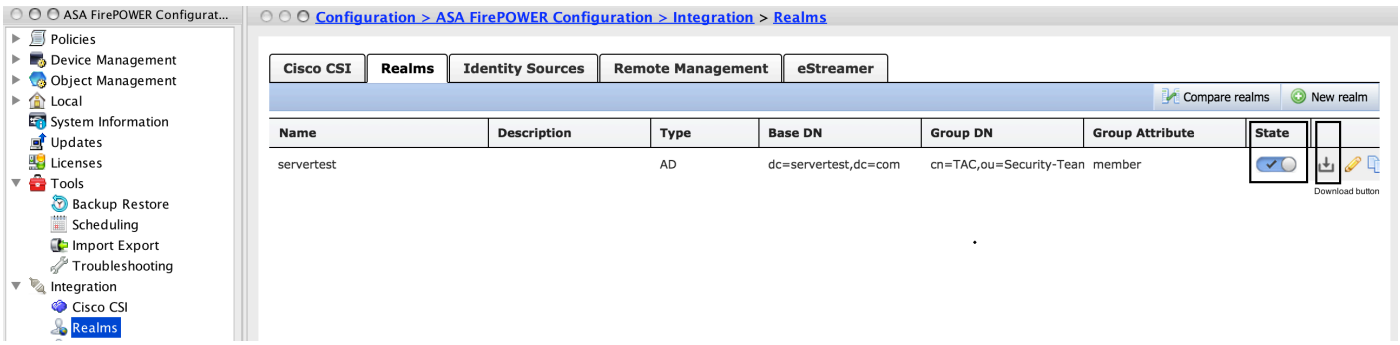
قم بتمكين خانة الاختيار لتنزيل **تنزيل المستخدمين والمجموعات** وتحديد الفاصل الزمني حول عدد مرات اتصال وحدة FirePOWER النمطية بخادم AD لتنزيل قاعدة بيانات المستخدم.

حدد المجموعة وأضفها إلى خيار **التضمين** الذي تريد تكوين المصادقة له. بشكل افتراضي، يتم تحديد كل المجموعات إذا لم تقم باختيار أن تقوم بتضمين المجموعات.



انقر فوق **تغييرات Store ASA FirePOWER** لحفظ تكوين النطاق.

قم بتمكين حالة النطاق وانقر فوق زر التنزيل لتنزيل المستخدمين والمجموعات، كما هو موضح في الصورة.



الخطوة 4. قم بتكوين نهج الهوية.

يقوم نهج الهوية بإجراء مصادقة المستخدم. في حالة عدم مصادقة المستخدم، يتم رفض الوصول إلى موارد الشبكة. يؤدي هذا إلى فرض التحكم في الوصول المستند إلى الأدوار (RBAC) على شبكة مؤسستك وموارده.

الخطوة 4.1 البوابة المقيدة (المصادقة النشطة).

تتطلب المصادقة النشطة اسم المستخدم وكلمة المرور في المستعرض لتعريف هوية المستخدم للسماح بأي اتصال. يقوم المستعرض بمصادقة المستخدم إما عن طريق عرض صفحة المصادقة أو بمصادقة NTLM في صمت. يستخدم NTLM مستعرض الويب لإرسال معلومات المصادقة واستقبالها. تستخدم المصادقة النشطة أنواعا مختلفة للتحقق من هوية المستخدم. الأنواع المختلفة للمصادقة هي:

1. **http basic: في هذه الطريقة، يوعز المستعرض بإدخال بيانات اعتماد المستخدم.**

2. **NTLM:** يستخدم NTLM بيانات اعتماد محطة عمل Windows ويفاوض عليها مع Active Directory باستخدام مستعرض ويب. تحتاج إلى تمكين مصادقة NTLM في المستعرض. تحدث مصادقة المستخدم بشفافية دون مطالبة بيانات الاعتماد. وهو يوفر تجربة تسجيل دخول واحدة للمستخدمين.
3. **تفاوض HTTP:** في هذا النوع، يحاول النظام المصادقة باستخدام NTLM، إذا فشل ثم يستخدم المستشعر نوع مصادقة HTTP الأساسية كطريقة إحتياطية ويطلب مربع حوار لبيانات اعتماد المستخدم.
4. **صفحة إستجابة HTTP:** هذا مماثل للنوع الأساسي HTTP، ومع ذلك، يتم مطالبة المستخدم هنا بتعبئة المصادقة في نموذج HTML يمكن تخصيصه.

يحتوي كل مستعرض على طريقة خاصة لتمكين مصادقة NTLM، وبالتالي، يمكنك اتباع إرشادات المستعرض لتمكين مصادقة NTLM.

لمشاركة بيانات الاعتماد بشكل آمن مع المستشعر الموجه، تحتاج إلى تثبيت إما شهادة خادم موقعة ذاتيا أو شهادة خادم موقعة بشكل عام في نوع الهوية.

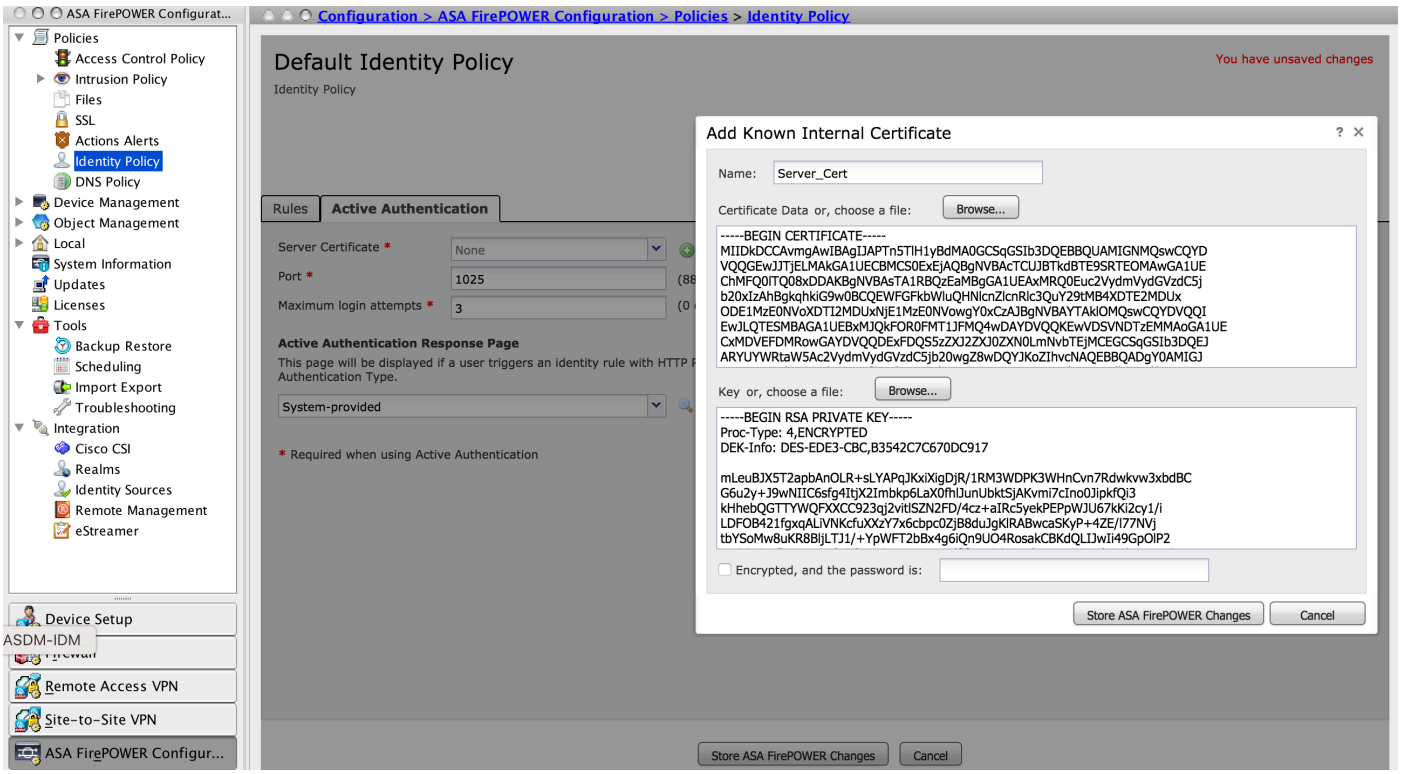
```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
              openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
              openssl req -new -key server.key -out server.csr

Step 3.   Generate the self-signed Certificate.
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

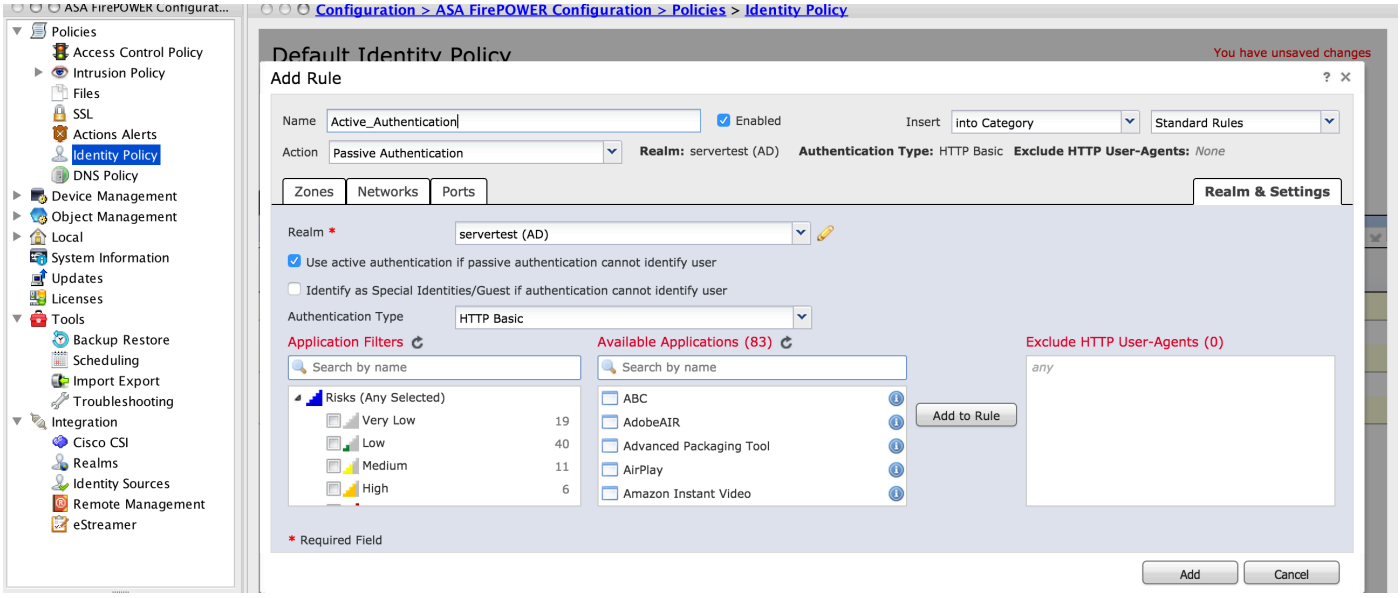
انتقل إلى **التكوين > ASA FirePOWER Configuration > السياسات > سياسة الهوية**. انتقل الآن إلى علامة التبويب **المصادقة النشطة** وفي خيار **شهادة الخادم** انقر على **الأيقونة (+)** وتحميل الشهادة والمفتاح الخاص اللذين قمت بتوليدهما في الخطوة السابقة باستخدام OpenSSL، كما هو موضح في الصورة:



انقر الآن فوق **إضافة قاعدة** إلعطاء اسم للقاعدة واختر الإجراء كمصادقة **نشطة**. قم بتعريف منطقة المصدر/الوجهة، وشبكة المصدر/الوجهة التي تريد تمكين مصادقة

المستخدم لها.

انتقل إلى علامة التبويب **النطاق والإعدادات**. حدد **النطاق** من القائمة المنسدلة التي قمت بتكوينها في الخطوة السابقة وحدد **نوع المصادقة** من القائمة المنسدلة التي تلائم بيئة الشبكة على أفضل وجه.



الخطوة 4.2 تكوين ASA للمدخل المتنقل.

الخطوة 1. حدد حركة المرور المثيرة للاهتمام التي سيتم إعادة توجيهها إلى Sourcefire للتفتيش.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
ASA(config-cmap)# match access-list SFR_ACL
```

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

الخطوة 2. شكلت هذا أمر على ال ASA in order to مكنت المدخل أسير.

```
ASA(config)# captive-portal interface inside port 1025
```

تلميح: يمكن تمكين البوابة المقيدة بشكل عام أو لكل واجهة.

تلميح: تأكد من تكوين منفذ الخادم، بروتوكول TCP 1025 في علامة التبويب "المصادقة النشطة" الخاصة بنهج الهوية في خيار المنفذ.

الخطوة 4.3 تسجيل الدخول الأحادي (المصادقة الخاملة).

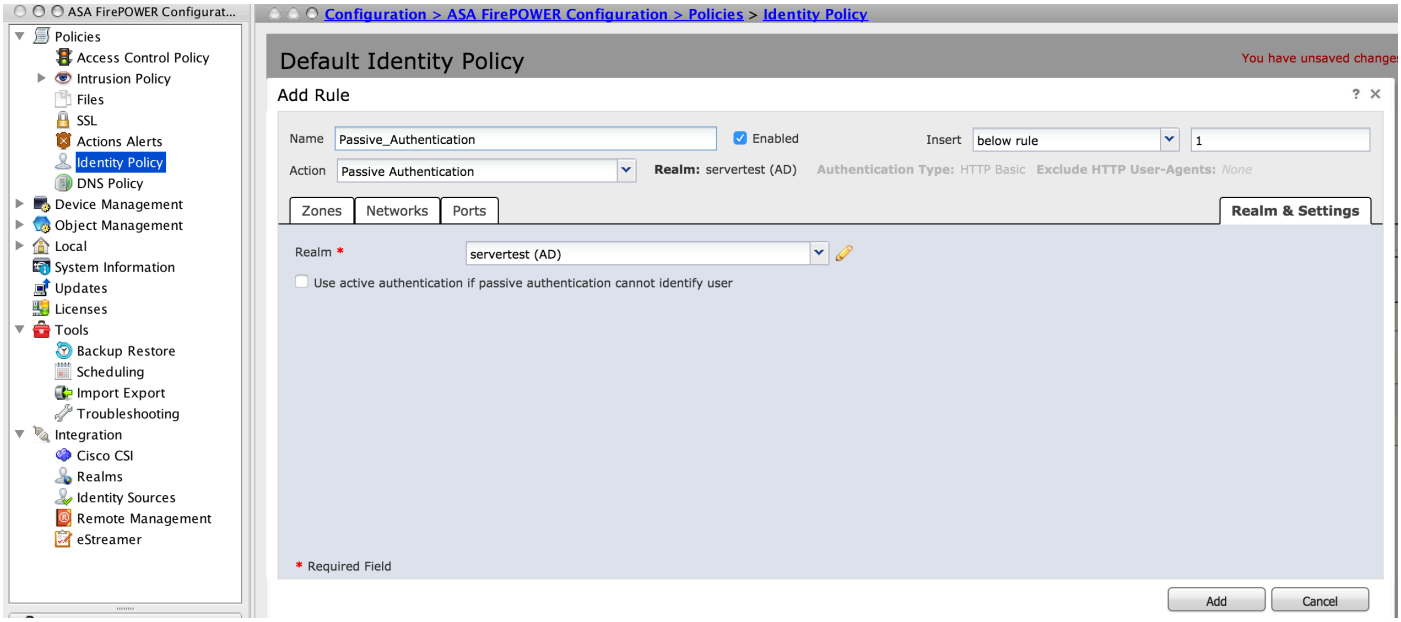
في المصادقة السلبية، عندما يقوم مستخدم المجال بتسجيل الدخول ويكون قادرا على

مصادقة AD، يقوم "عميل مستخدم FirePOWER" بفحص تفاصيل تعيين المستخدم-IP من سجلات أمان AD ويشاركان هذه المعلومات مع وحدة FirePOWER. تستخدم الوحدة النمطية Firepower هذه التفاصيل من أجل فرض التحكم في الوصول.

لتكوين قاعدة المصادقة الخاملة، انقر على **إضافة قاعدة** لإعطاء اسم للقاعدة ثم أختر **الإجراء** كمصادقة **خاملة**. قم بتعريف منطقة المصدر/الوجهة، وشبكة المصدر/الوجهة التي تريد تمكين مصادقة المستخدم لها.

انتقل إلى **النطاق والإعدادات** علامة تبويب. حدد **مملكة** من القائمة المنسدلة التي قمت بتكوينها في الخطوة السابقة.

هنا يمكنك إختيار طريقة التراجع **كمصادقة نشطة إذا لم تتمكن المصادقة الخاملة من تعريف هوية المستخدم**، كما هو موضح في الصورة:

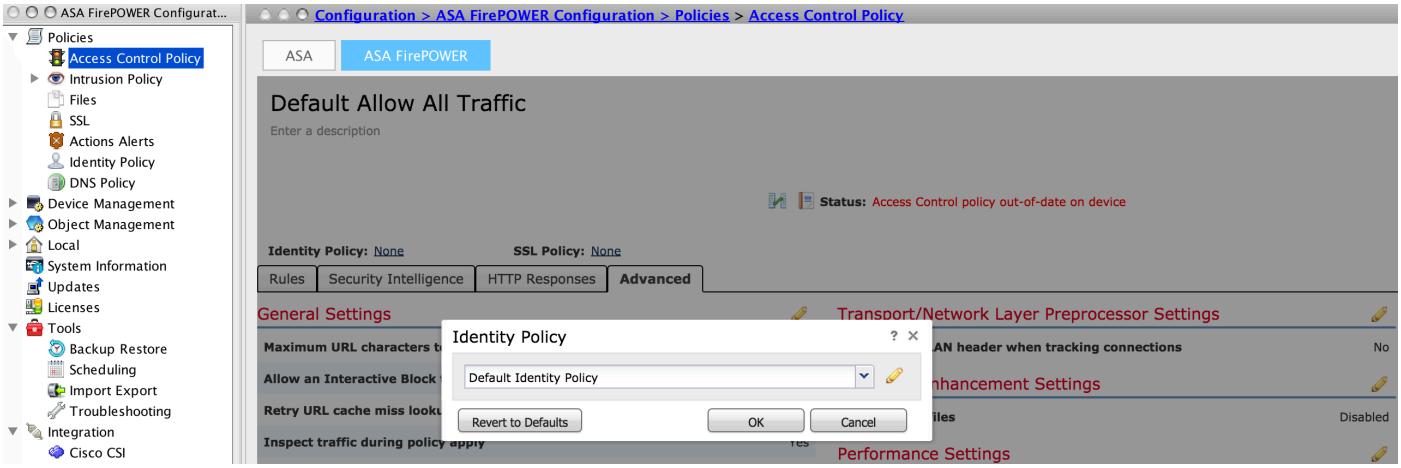


انقر الآن على **تغييرات Store ASA FirePOWER** لحفظ تكوين نهج الهوية.

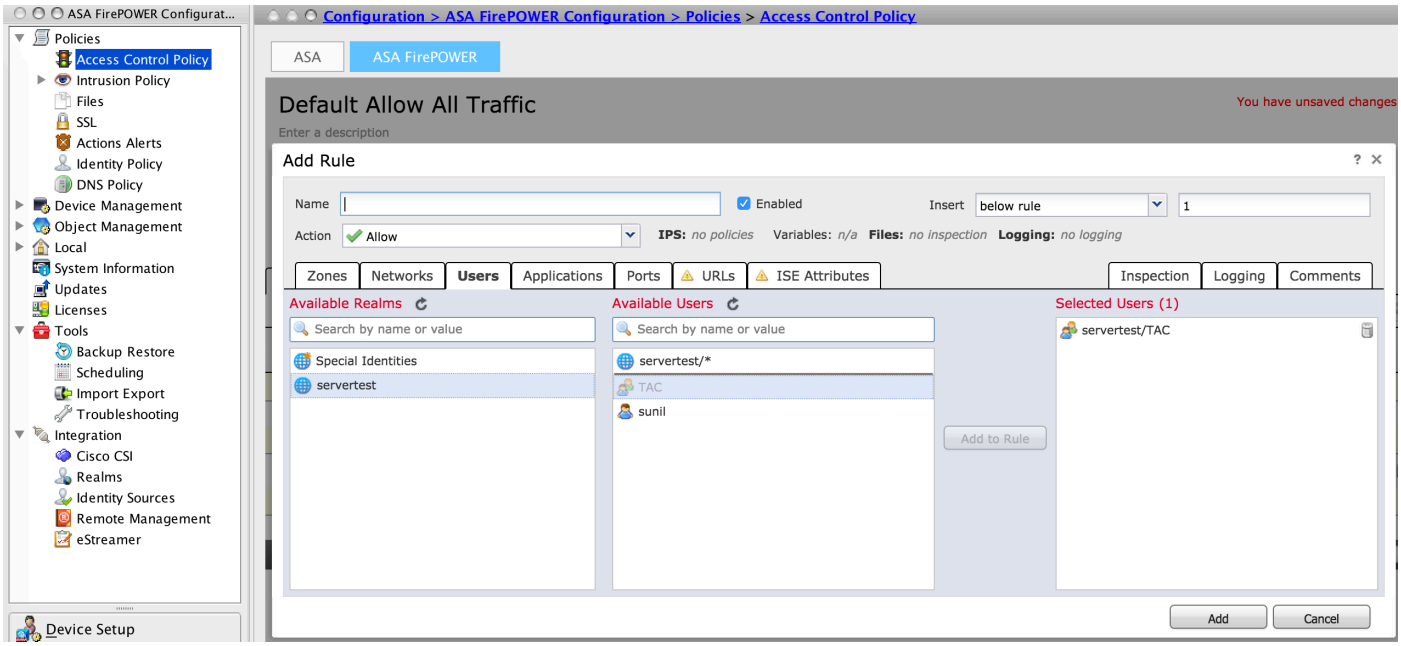
الخطوة 5. تكوين نهج التحكم في الوصول.

انتقل إلى **التكوين > ASA FirePOWER Configuration > السياسات > سياسة التحكم في الوصول.**

انقر فوق **نهج الهوية** (الجانب الأيسر في الركن العلوي)، وحدد تعريف النهج الذي قمت بتكوينه في الخطوة السابقة من القائمة المنسدلة وانقر فوق **موافق**، كما هو موضح في هذه الصورة.



انقر فوق **إضافة قاعدة** لإضافة قاعدة جديدة، انتقل إلى **المستخدمون** وحدد المستخدمين الذين سيتم فرض قاعدة التحكم بالوصول الخاصة بهم، كما هو موضح في هذه الصورة، ثم انقر فوق **إضافة**.



انقر فوق **تخزين تغييرات ASA FirePOWER** لحفظ تكوين نهج التحكم في الوصول.

الخطوة 6. نشر سياسة التحكم بالوصول.

يجب نشر نهج التحكم بالوصول. قبل تطبيق النهج، ستر نهج التحكم بالوصول للإشارة قديم على الوحدة النمطية. لنشر التغييرات على المستشعر، انقر فوق **نشر** واختر **نشر خيار تغييرات FirePOWER** ثم انقر فوق **نشر** في الإطار المنبثق.

> **ملاحظة**: في الإصدار 5.4.x، لتطبيق سياسة الوصول على المستشعر، يلزمك النقر فوق تطبيق تغييرات ASA FirePOWER

> **ملاحظة**: انتقل إلى المراقبة > مراقبة ASA FirePOWER > حالة المهمة. تأكد من أن المهمة يجب أن تكمل تطبيق تغيير التكوين.

الخطوة 7. مراقبة أحداث المستخدم.

انتقل إلى **المراقبة > مراقبة ASA FirePOWER > الإيضاح في الوقت الفعلي**، لمراقبة نوع حركة المرور التي يستخدمها المستخدم.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

انتقل إلى **تحليل > مستخدمون** للتحقق من نوع مصادقة/مصادقة المستخدم/تعيين/قاعدة حركة المرور المقترنة بتدفق حركة المرور لمستخدم IP وصول.

الاتصال بين الوحدة النمطية Firepower ووكيل المستخدم (المصادقة الخاملة)

تستخدم الوحدة النمطية Firepower منفذ TCP 3306، لتلقي بيانات سجل نشاط المستخدم من وكيل المستخدم.

للتحقق من حالة خدمة وحدة FirePOWER النمطية، أستخدم هذا الأمر في FMC.

```
admin@firepower:~$ netstat -tan | grep 3306
```

قم بتشغيل التقاط الحزمة على FMC للتحقق من الاتصال مع وكيل المستخدم.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

الاتصال بين FMC و Active Directory

تستخدم الوحدة النمطية Firepower منفذ TCP 389 لاسترداد قاعدة بيانات المستخدم من Active Directory.

قم بتشغيل التقاط الحزمة على الوحدة النمطية Firepower للتحقق من الاتصال ب Active Directory.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

تأكد من أن بيانات اعتماد المستخدم المستخدمة في تكوين النطاق لها امتياز كاف لجلب قاعدة بيانات مستخدم AD.

تحقق من تكوين النطاق، وتأكد من تنزيل المستخدمين/المجموعات ومن تكوين مهلة جلسة المستخدم بشكل صحيح.

انتقل إلى "مراقبة حالة مهمة مراقبة ASA FirePOWER" وتأكد من اكتمال تنزيل مستخدمي/مجموعات المهام بنجاح، كما هو موضح في هذه الصورة.

الاتصال بين ASA والنظام الطرفي (المصادقة النشطة)

المصادقة النشطة، تأكد من تكوين الشهادة والمنفذ بشكل صحيح في نهج تعريف وحدة FirePOWER النمطية وأمر ASA (Captive-portal). بشكل افتراضي، تستمع الوحدة النمطية TCP 885 للمصادقة النشطة.

للتحقق من القواعد النشطة وعدد مرات الوصول إليها، قم بتشغيل هذا الأمر على ASA.

```
ASA# show asp table classify domain captive-portal

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

تكوين السياسة ونشر السياسة

تأكد من تكوين النطاق ونوع المصادقة ووكيل المستخدم وحقول الإجراء بشكل صحيح في نهج الهوية.

تأكد من أن نهج الهوية مرتبط بشكل صحيح بنهج التحكم بالوصول.

انتقل إلى مراقبة > مراقبة ASA FirePOWER > حالة المهمة وتأكد من اكتمال نشر السياسة بنجاح.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems
- تكوين تكامل Active Directory باستخدام جهاز FirePOWER لمصادقة الدخول الأحادي ومصادقة البوابة المقيدة

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).