تكوين تكامل Active Directory باستخدام FirePOWER Appliance لمصادقة الدخول الأحادي لمصادقة المدخل المتنقل و AMP و

المحتويات

المقدمة

يصف هذا المستند تكوين مصادقة البوابة المقيدة (المصادقة النشطة) وتسجيل الدخول الأحادي (المصادقة الخاصة).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أجهزة Sourcefire Firepower
- نماذج الأجهزة الظاهرية
- خدمة دليل الوزن الخفيف (LDAP)
- Firepower UserAgent

المكونات المستخدمة

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

- مركز إدارة Firepower (FMC)، الإصدار 6.0.0 والإصدارات الأحدث
- مستشعر Firepower الإصدار 6.0.0 والإصدار الأحدث

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

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

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

ملاحظة: بالنسبة لمصادقة البوابة المقيدة، يجب أن يكون الجهاز في الوضع الموجه.

التكوين

الخطوة 1. تكوين وكيل مستخدم Firepower لتسجيل الدخول الأحادي

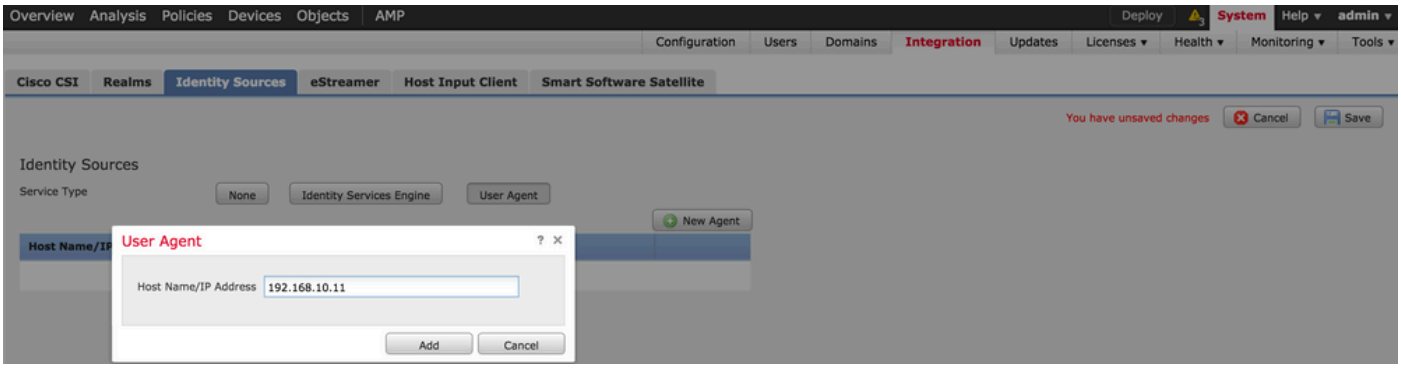
يشرح هذا المقال كيفية تكوين "وكيل مستخدم FirePOWER" في جهاز Windows:

تثبيت وكيل مستخدم Sourcefire وإلغاء تثبيته

الخطوة 2. دمج مركز إدارة Firepower (FMC) مع وكيل المستخدم

سجل الدخول إلى مركز إدارة Firepower، انتقل إلى النظام > الدمج > مصادر الهوية. انقر فوق خيار الوكيل الجديد. قم بتكوين عنوان IP لنظام وكيل المستخدم وانقر فوق الزر إضافة.

انقر فوق الزر حفظ لحفظ التغييرات.



الخطوة 3. دمج FirePOWER مع Active Directory

الخطوة 3.1 إنشاء المجال

سجل الدخول إلى FMC، انتقل إلى النظام > التكامل > النطاق. انقر فوق خيار إضافة حيز جديد.

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

الكتابة: الإعلان

المجال الأساسي ل AD: اسم مجال Active Directory

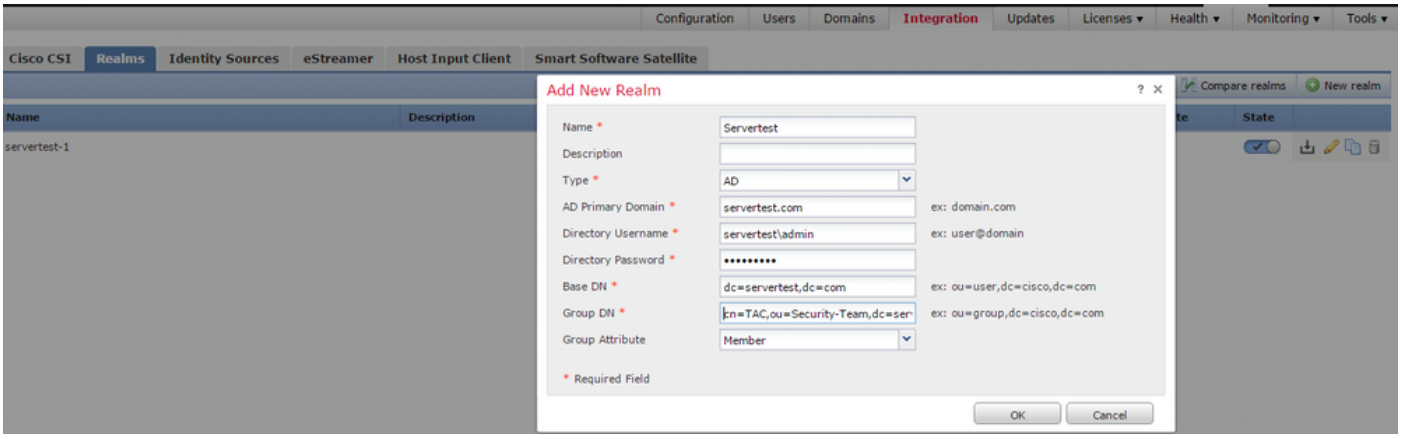
اسم مستخدم الدليل: <username>

كلمة مرور الدليل: <password>

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

DN للمجموعة: DN للمجموعة

سمة المجموعة: عضو



تساعدك هذه المقالة على معرفة قيم DN الأساسية و DN الخاصة بالمجموعة.

[تعريف سمات كائن LDAP لخدمة Active Directory]

الخطوة 3.2 أضف خادم الدليل

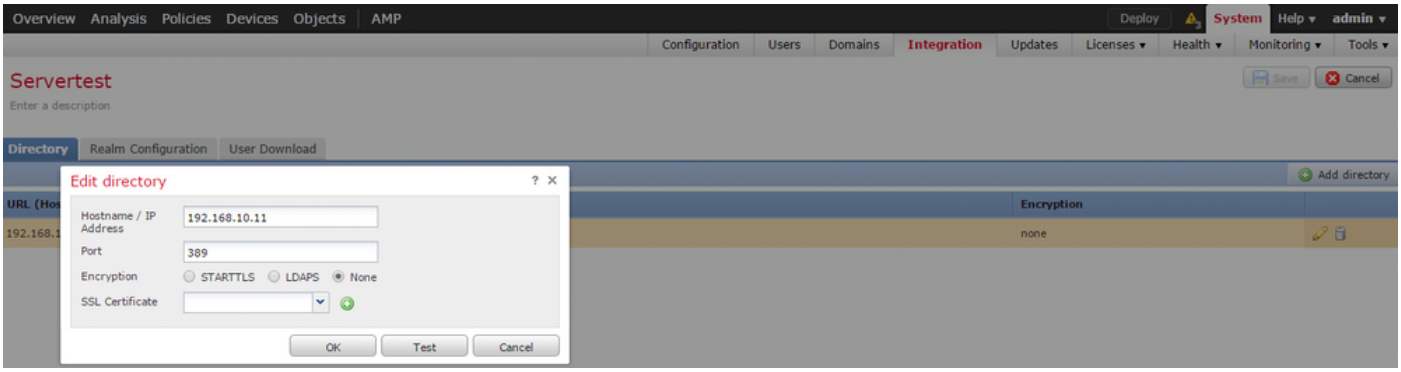
انقر فوق الزر إضافة للتنقل إلى الخطوة التالية ثم انقر فوق خيار إضافة دليل.

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

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

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

المقالة: التحقق من كائن المصادقة في نظام FireSIGHT لمصادقة Microsoft AD عبر SSL/TLS



انقر فوق زر الاختبار للتحقق من قدرة FMC على الاتصال بخادم AD.

الخطوة 3.3 قم بتعديل تكوين النطاق

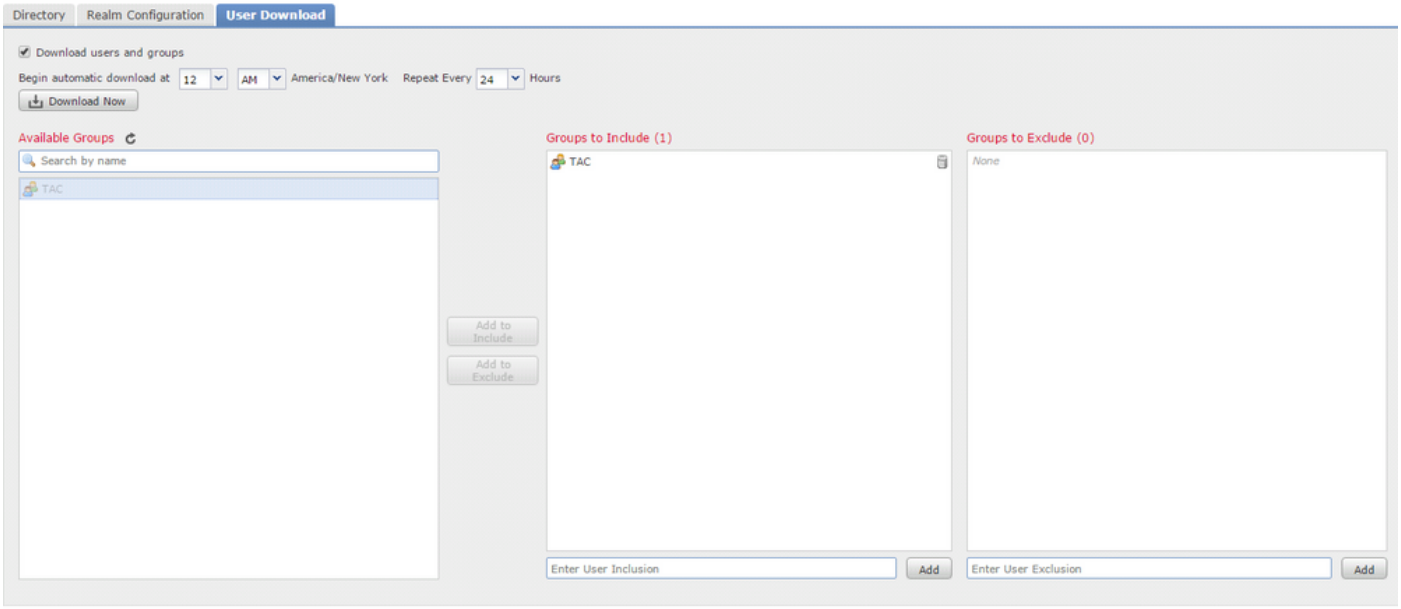
انتقل إلى تكوين النطاق للتحقق من تكوين التكامل لخادم AD ويمكنك تعديل تكوين AD.

الخطوة 3.4 تنزيل قاعدة بيانات المستخدم

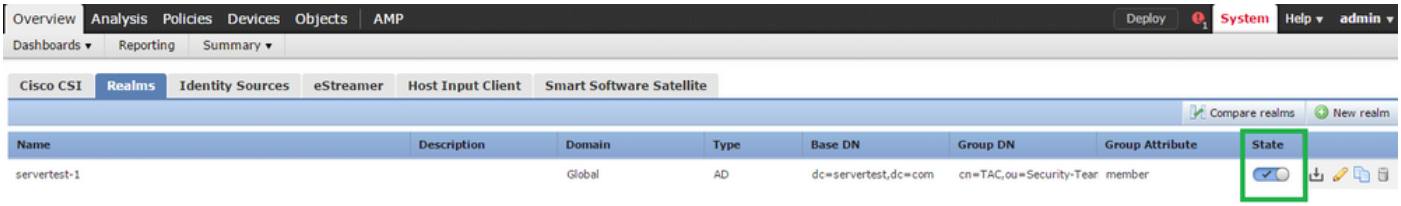
انتقل إلى خيار تنزيل المستخدم لجلب قاعدة بيانات المستخدم من خادم AD.

قم بتمكين خانة الاختيار لتنزيل تنزيل المستخدمين والمجموعات وتحديد الفاصل الزمني حول تكرار جهات اتصال FMC AD لتنزيل قاعدة بيانات المستخدم.

حدد المجموعة ووضعها في خيار التضمين الذي تريد تكوين المصادقة له.



كما هو موضح في الصورة، قم بتمكين حالة AD:



الخطوة 4. تكوين 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)

تطلب المصادقة النشطة اسم المستخدم/كلمة المرور في المستعرض لتعريف هوية المستخدم للسماح بأي اتصال. يقوم المستعرض بمصادقة المستخدم باستخدام صفحة مصادقة أو إجراء المصادقة دون أدنى تردد باستخدام مصادقة NTLM. 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 من خلال مستعرض ويب. تحتاج إلى تمكين مصادقة NTLM في المستعرض. تحدث مصادقة المستخدم بشفافية دون مطالبة ببيانات الاعتماد. وهو يوفر تجربة تسجيل دخول واحدة للمستخدمين.
3. تفاوض HTTP: في هذا النوع، يحاول النظام المصادقة باستخدام NTLM. في حالة فشله، يستخدم المستشعر نوع مصادقة HTTP الأساسية كطريقة إحتياطية ويطلب مربع حوار ببيانات اعتماد المستخدم.
4. صفحة إستجابة HTTP: هذا مماثل للنوع الأساسي HTTP، ومع ذلك، يتم مطالبة

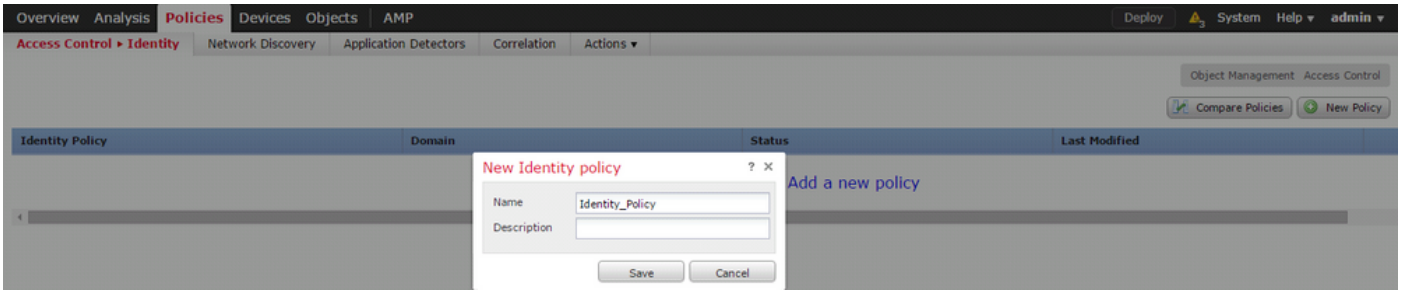
المستخدم هنا بتعبئة المصادقة في نموذج HTML يمكن تخصيصه.

يحتوي كل مستعرض على طريقة خاصة لتمكين مصادقة NTLM وبالتالي فإنه يتقيد بإرشادات المستعرض لتمكين مصادقة NTLM.

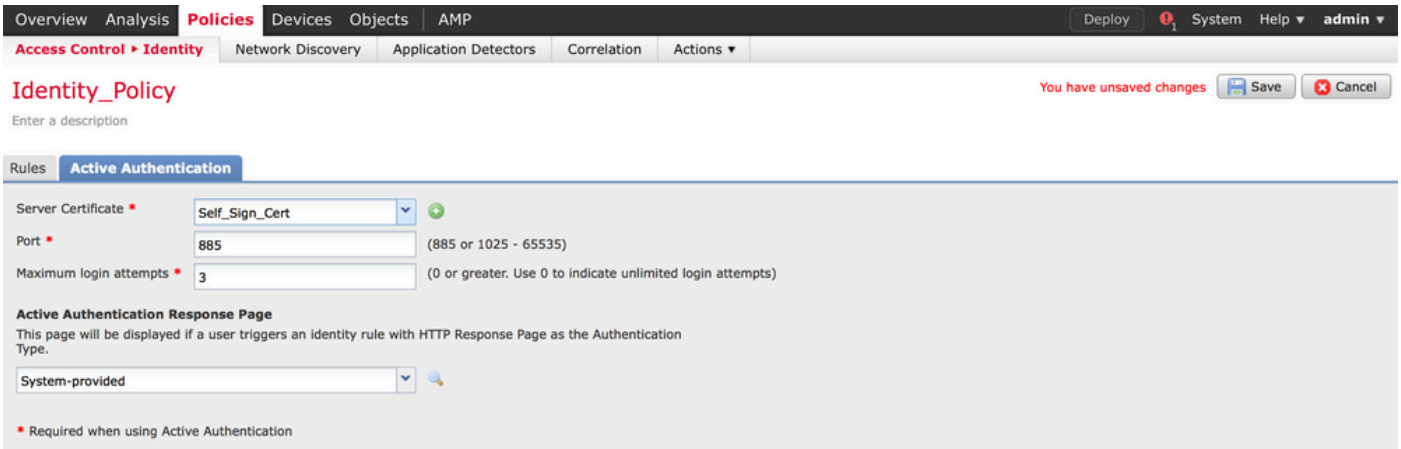
لمشاركة بيانات الاعتماد بشكل آمن مع المستشعر الموجه، تحتاج إلى تثبيت إما شهادة خادم موقعة ذاتيا أو شهادة خادم موقعة بشكل عام في نوع الهوية.

```
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 السياسات > التحكم في الوصول > الهوية. انقر فوق إضافة النهج وأعط اسما للنهج واحفظه.



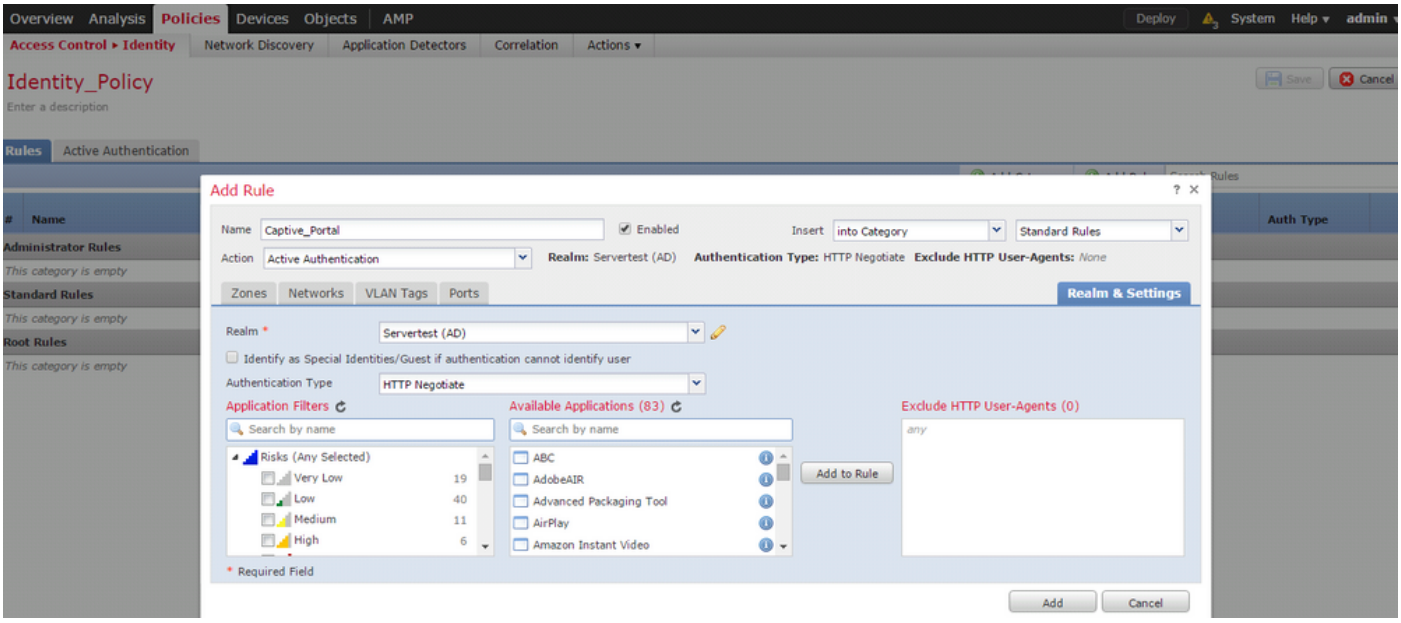
انتقل إلى علامة التبويب المصادقة النشطة وفي خيار شهادة الخادم، انقر على الرمز (+) وقم بتحميل الشهادة والمفتاح الخاص اللذين قمت بتوليدهما في الخطوة السابقة باستخدام OpenSSL.



انقر الآن على الزر إضافة قاعدة وأعط اسما للقاعدة واختر الإجراء كمصادقة نشطة. قم

بتعريف منطقة المصدر/الوجهة، وشبكة المصدر/الوجهة التي تريد تمكين مصادقة المستخدم لها.

حدد النطاق، الذي قمت بتكوينه في الخطوة السابقة ونوع المصادقة الذي يناسب بيئتك على أفضل وجه.



تكوين ASA للمدخل المقيد

بالنسبة للوحدة النمطية ASA FirePOWER، قم بتكوين هذه الأوامر على ASA لتكوين المدخل المأسور.

```
ASA(config)# captive-portal global port 1055
```

تأكد من تكوين منفذ الخادم، بروتوكول TCP 1055 في خيار المنفذ الخاص بعلامة التبويب مصادقة نشطة لنهج الهوية.

للتحقق من القواعد النشطة وعدد مرات الوصول إليها، قم بتشغيل الأمر:

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

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

الخطوة 4.2 تسجيل الدخول الأحادي (المصادقة الخاملة)

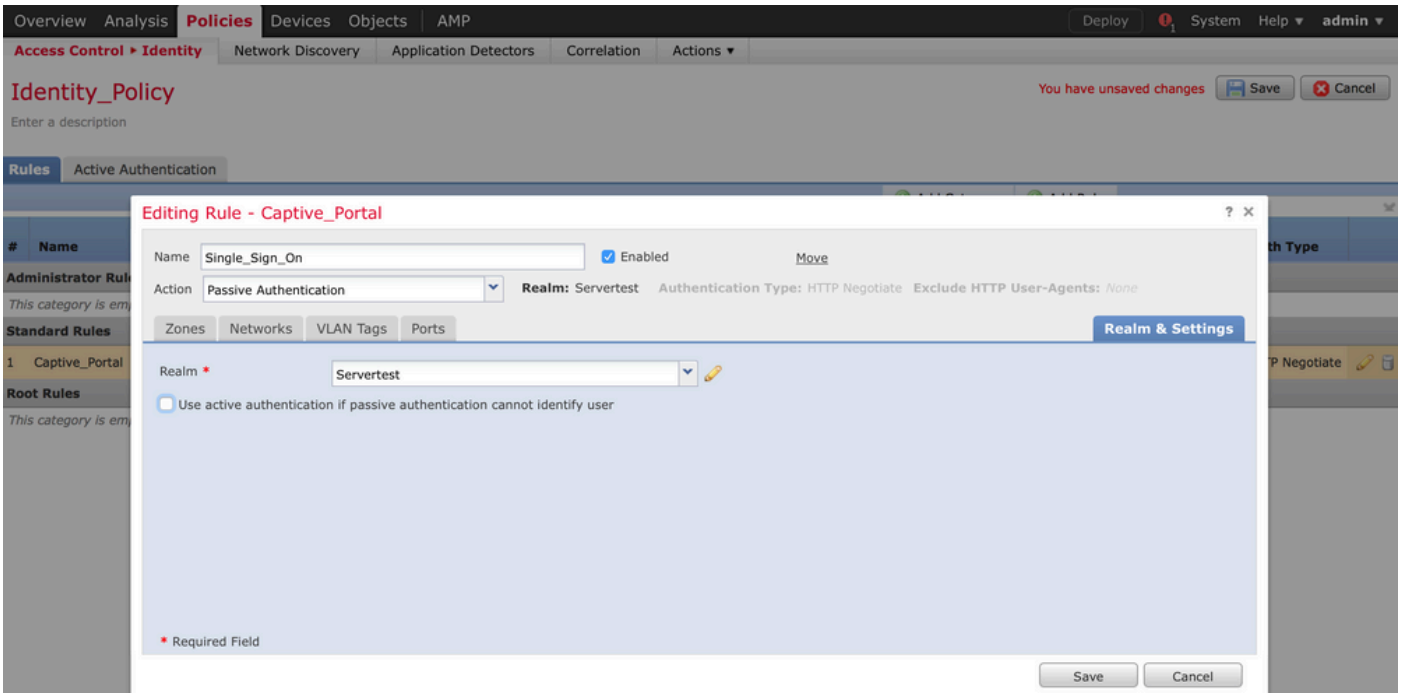
في المصادقة السلبية، عندما يقوم مستخدم المجال بتسجيل الدخول ويكون قادرا على مصادقة AD، يقوم "عميل مستخدم FirePOWER" بفحص تفاصيل تخطيط المستخدم-IP من سجلات أمان AD ويشارك هذه المعلومات مع مركز إدارة Firepower (FMC). ترسل FMC هذه

التفاصيل إلى المستشعر لفرض التحكم في الوصول.

انقر فوق الزر إضافة قاعدة وأعط اسما للقاعدة واختر الإجراء كمصادقة خاملة. قم بتعريف منطقة المصدر/الوجهة، وشبكة المصدر/الوجهة التي تريد تمكين مصادقة المستخدم لها.

حدد النطاق الذي قمت بتكوينه في الخطوة السابقة ونوع المصادقة الذي يعمل على أفضل تجميع لبيئتك، كما هو موضح في هذه الصورة.

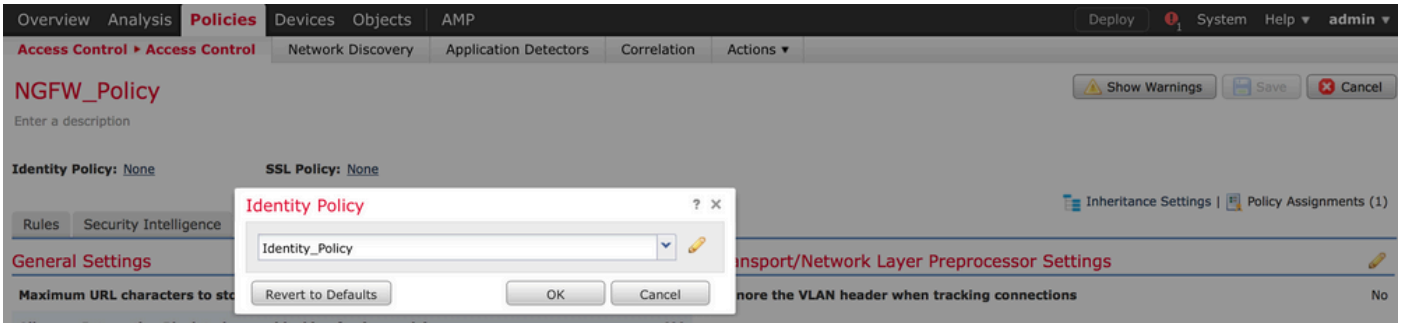
هنا يمكنك إختيار طريقة التراجع كمصادقة نشطة إذا لم تتمكن المصادقة الخاملة من تعريف هوية المستخدم.



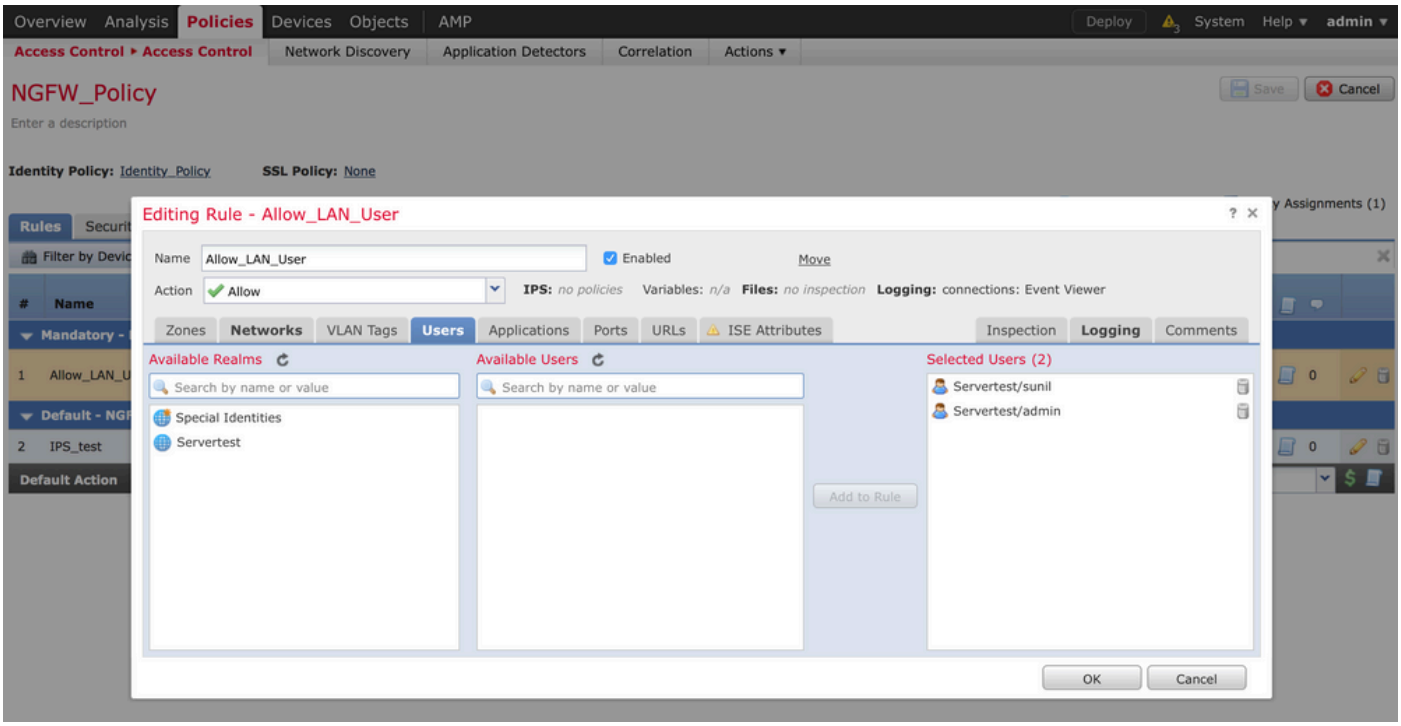
الخطوة 5. تكوين سياسة التحكم في الوصول

انتقل إلى السياسات > التحكم في الوصول > إنشاء/تحرير سياسة.

انقر سياسة الهوية (الجانب الأيسر في الركن الأعلى)، واختر تعريف النهج الذي قمت بتكوينه في الخطوة السابقة وانقر فوق زر موافق، كما هو موضح في هذه الصورة.

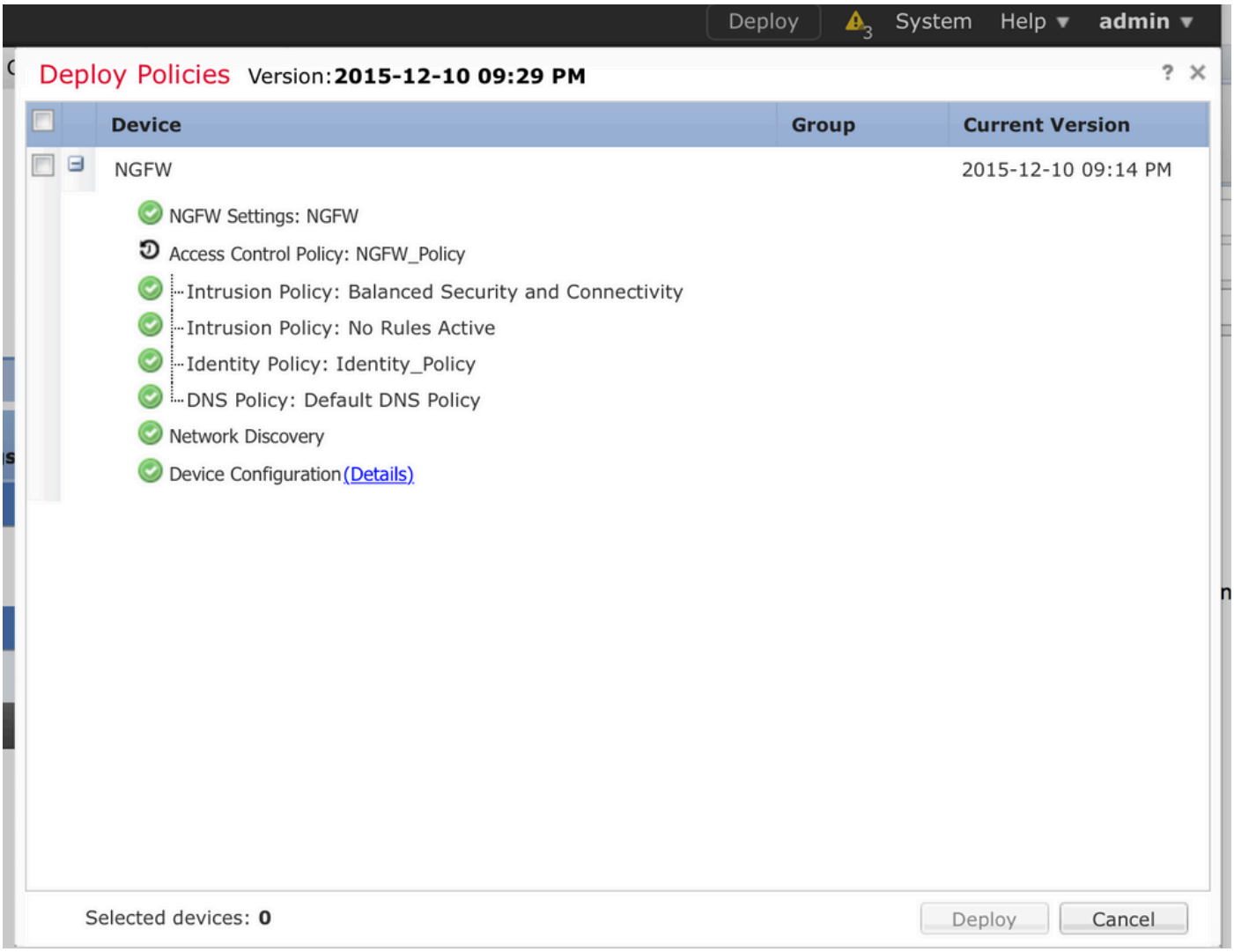


انقر فوق الزر إضافة قاعدة لإضافة قاعدة جديدة. انتقل إلى المستخدمين وحدد المستخدمين الذين يتم فرض قاعدة التحكم في الوصول لهم، كما هو موضح في هذه الصورة. انقر فوق موافق وانقر فوق حفظ لحفظ التغييرات.



الخطوة 6. نشر سياسة التحكم في الوصول

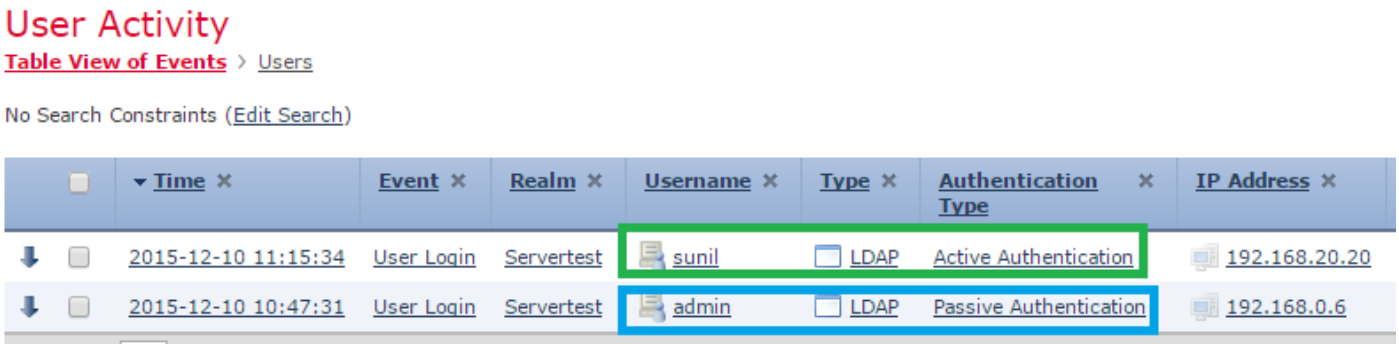
انتقل إلى خيار النشر، واختر الجهاز وانقر فوق خيار النشر لدفع تغييرات التكوين إلى المستشعر. قم بمراقبة نشر النهج من رمز مركز الرسائل (رمز بين خيار النشر والنظام) وتأكد من أنه يجب تطبيق النهج بنجاح، كما هو موضح في هذه الصورة.



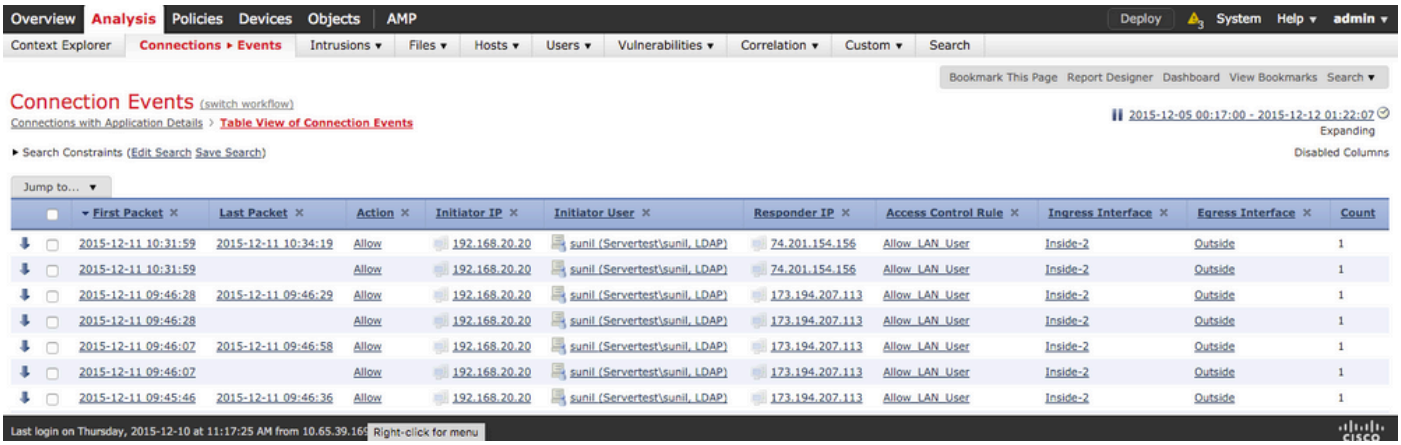
الخطوة 7. مراقبة أحداث المستخدم وأحداث الاتصالات

تتوفر جلسات عمل المستخدم النشطة حاليا في قسم تحليل > مستخدمون > مستخدمون.

تساعد مراقبة نشاط المستخدم في تحديد المستخدم المقترن بأي عنوان IP وكيف يتم اكتشاف المستخدم بواسطة النظام إما من خلال المصادقة النشطة أو السلبية. تحليل > مستخدمون > نشاط المستخدم



انتقل إلى Analysis (تحليل) > Connections > Events، لمراقبة نوع حركة المرور التي يستخدمها المستخدم.



التحقق من الصحة واستكشاف الأخطاء وإصلاحها

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

التحقق من الاتصال بين FMC ووكيل المستخدم (المصادقة الخاملة)

يستخدم مركز إدارة Firepower (FMC) منفذ TCP 3306، لتلقي بيانات سجل نشاط المستخدم من وكيل المستخدم.

للتحقق من حالة خدمة FMC، 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
```

انتقل إلى Analysis (تحليل) > Users (مستخدمون) > User Activity (نشاط المستخدم)
للتحقق مما إذا كانت وحدة التحكم في إدارة الوحة الأساسية (FMC) تتلقى تفاصيل تسجيل دخول المستخدم من وكيل المستخدم.

التحقق من الاتصال بين FMC و Active Directory

تستخدم FMC منفذ TCP 389 لاسترداد قاعدة بيانات المستخدم من خدمة Active Directory.

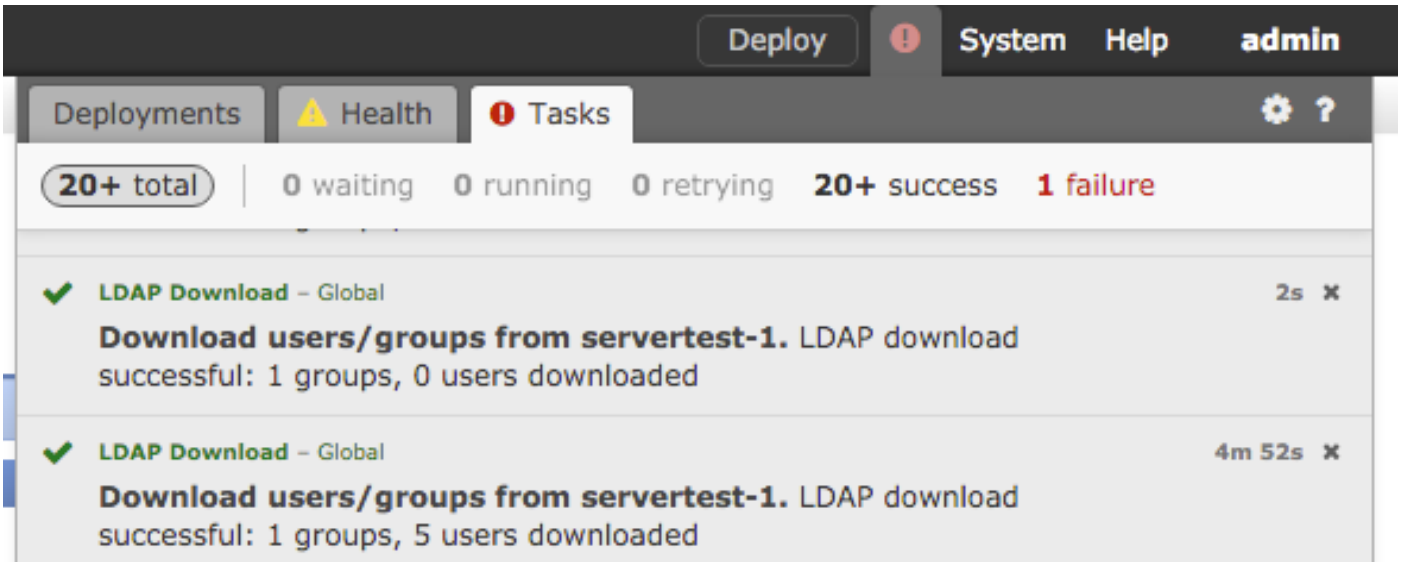
قم بتشغيل التقاط الحزمة على FMC للتحقق من الاتصال ب Active Directory.

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

تأكد من أن بيانات اعتماد المستخدم المستخدمة في تكوين نطاق FMC بها امتياز كاف لجلب قاعدة بيانات مستخدم AD.

تحقق من تكوين نطاق FMC، وتأكد من تنزيل المستخدمين/المجموعات ومن تكوين مدة جلسة عمل المستخدم بشكل صحيح.

انتقل إلى مركز الرسائل > المهام وتأكد من اكتمال تنزيل مستخدمي/مجموعات المهام بنجاح، كما هو موضح في هذه الصورة.



التحقق من الاتصال بين مستشعر FirePOWER والنظام الطرفي (المصادقة النشطة)

بالنسبة للمصادقة النشطة، تأكد من تكوين الشهادة والمنفذ بشكل صحيح في نهج تعريف FMC.افتراضيا، يستمع مستشعر Firepower على منفذ TCP 885 للمصادقة النشطة.

التحقق من تكوين النهج ونشر النهج

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 مركز الرسائل > المهام وتأكد من إكمال نشر النهج بنجاح.

تحليل سجلات الأحداث

يمكن إستخدام "الاتصال" أو أحداث "نشاط المستخدم" لتشخيص ما إذا كان تسجيل دخول المستخدم ناجحا أم لا.هذه الأحداث

كما يمكن التحقق من قاعدة التحكم في الوصول التي يتم تطبيقها على التدفق.

انتقل إلى تحليل > مستخدم للتحقق من سجلات أحداث المستخدم.

انتقل إلى Analysis (تحليل) > أحداث الاتصال للتحقق من أحداث الاتصال.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).