أستكشاف أخطاء ISE وحل FirePOWER لخدمات الهوية والإصلاحها

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين سياسات دعم TrustSec واستكشاف أخطائها وإصلاحها على نظام الحماية من التطفل من الجيل التالي (NGIPS) من Cisco. يدعم NGIPS الإصدار 6.0 المتكامل مع Identity Services Engine (ISE) الذي يسمح بإنشاء سياسات دعم الهوية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين جهاز الأمان القابل للتكيف (ASA) VPN من Cisco
- تكوين Cisco AnyConnect Secure Mobility Client
- التكوين الأساسي لمركز إدارة FirePOWER من Cisco
- تكوين Cisco ISE
- حلول Cisco TrustSec

المكونات المستخدمة

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

- نظام التشغيل Microsoft Windows 7
- المرجع المصدق لشهادة نظام التشغيل Microsoft Windows 2012 (CA)
- ASA الإصدار 9.3 من Cisco
- برنامج Cisco ISE، الإصدارات 1.4
- Cisco AnyConnect Secure Mobility Client، الإصدار 4.2
- مركز إدارة FirePOWER (FMC) من Cisco، الإصدار 6.0
- Cisco FirePOWER NGIPS، الإصدار 6.0

التكوين

يعد مركز إدارة FirePOWER (FMC) النظام الأساسي لإدارة FirePOWER. هناك نوعان من الوظائف المتعلقة بتكامل خدمات التوظيف والتسوية:

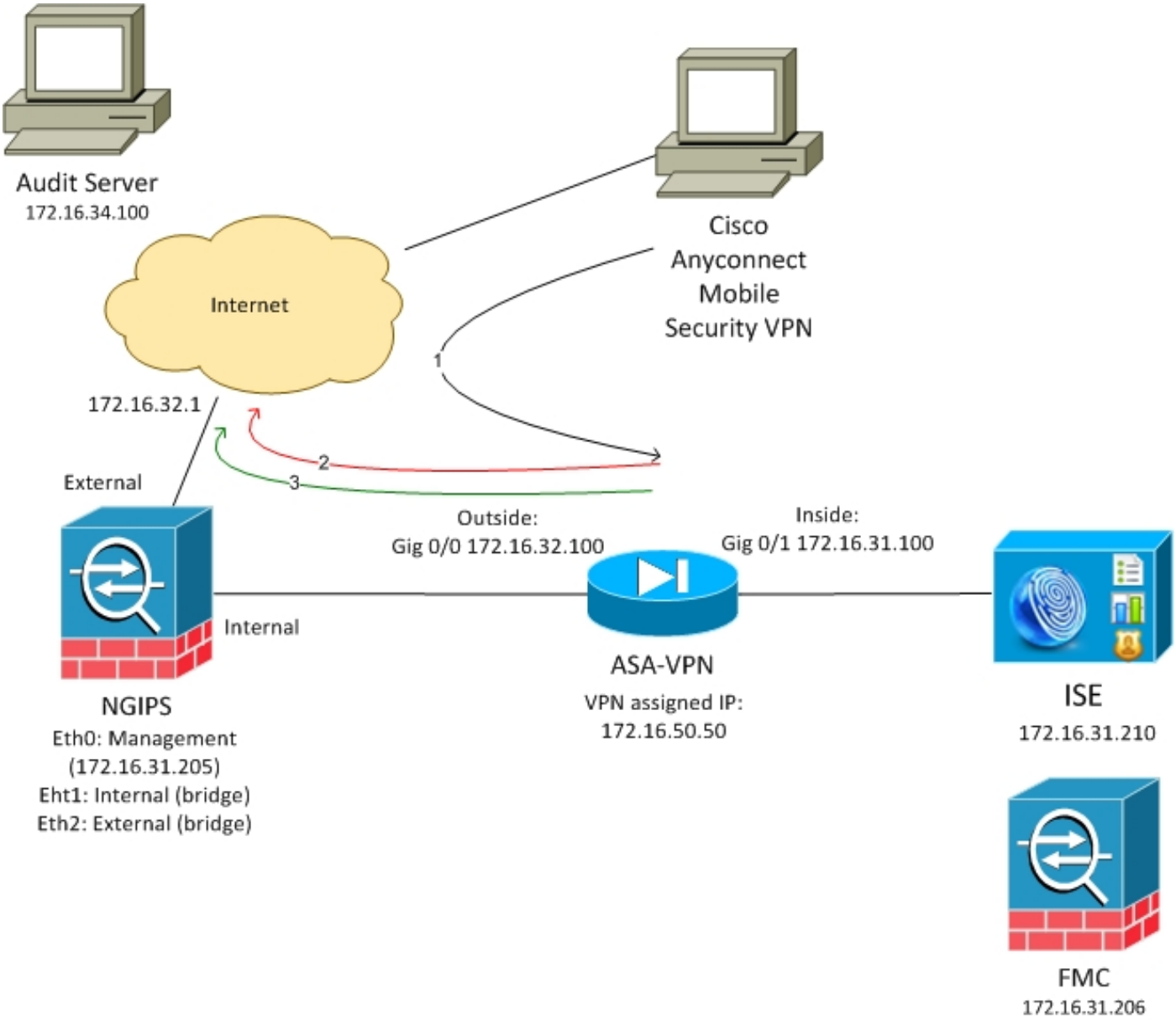
- الإصلاح - يسمح لـ FMC عزل المهاجم عبر ISE، التي تعمل على تغيير حالة التخويل بشكل ديناميكي على جهاز الوصول الذي يوفر وصول محدود إلى الشبكة. هناك جيلان من هذا الحل:

  1. برنامج نصي لـ Perl القديم باستخدام إستدعاء واجهة برمجة التطبيقات (API) لخدمة حماية النقطة الطرفية (EPS) إلى ISE.
  2. إستدعاء وحدة نمطية أحدث باستخدام بروتوكول pxGrid لـ ISE (هذه الوحدة النمطية مدعومة في الإصدار 5.4 - غير مدعومة في 6.0، الدعم الأصلي المخطط في 6.1).

- النهج - يسمح لـ FMC بتكوين السياسات استنادا إلى علامات مجموعة أمان TrustSec (SGT).

تركز هذه المقالة على الوظيفة الثانية. من أجل مثال الإصلاح، الرجاء قراءة قسم المراجع

الرسم التخطيطي للشبكة



يتم تكوين FMC باستخدام نهج التحكم في الوصول الذي يحتوي على قاعدتين:

- رفض حركة مرور HTTP باستخدام URL مخصص (attack-url)
- السماح بحركة مرور HTTP باستخدام URL مخصص (attack-url) ولكن فقط في حالة تعيين المستخدم العلامة رقيب التدقيق (9) بواسطة ISE

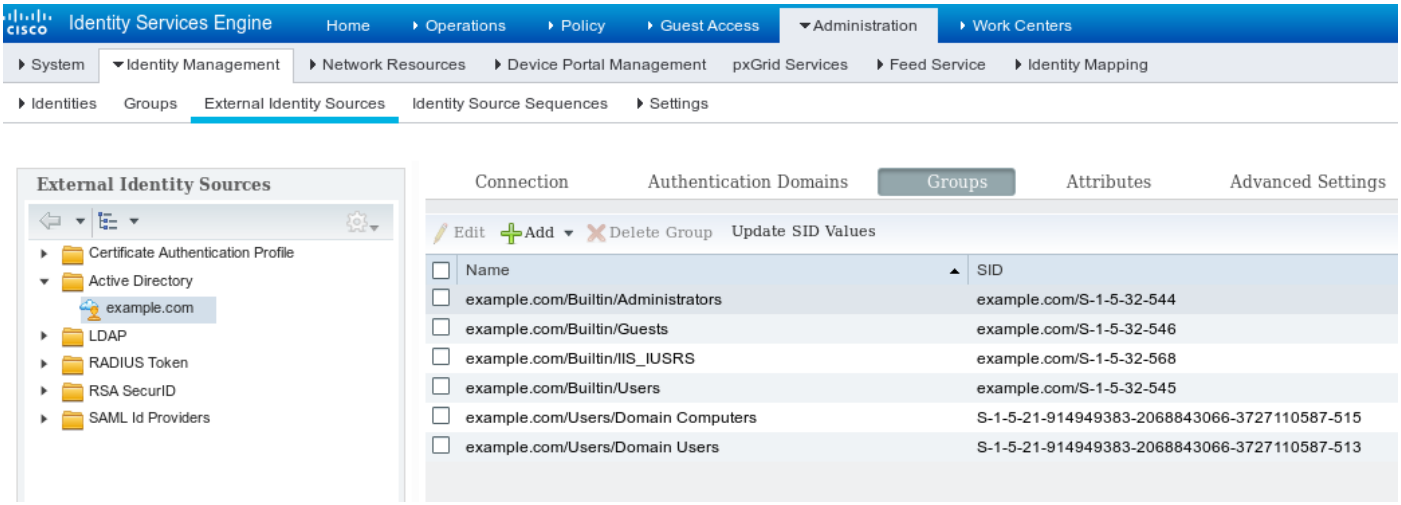
يقرر ISE تعيين علامة تدقيق إلى جميع مستخدمي Active Directory الذين ينتمون إلى مجموعة المسؤولين ويستخدم جهاز ASA-VPN للوصول إلى الشبكة.

وصول المستخدم إلى الشبكة عبر اتصال VPN على ASA. ثم يحاول المستخدم الوصول إلى الخادم الذي تم تدقيقه باستخدام عنوان URL للهجوم - ولكنه يفشل لأنه لم يتم تعيينه إلى مجموعة رقيب التدقيق. وبمجرد إصلاح ذلك، ينجح الاتصال.

محرك خدمات كشف الهوية (ISE)

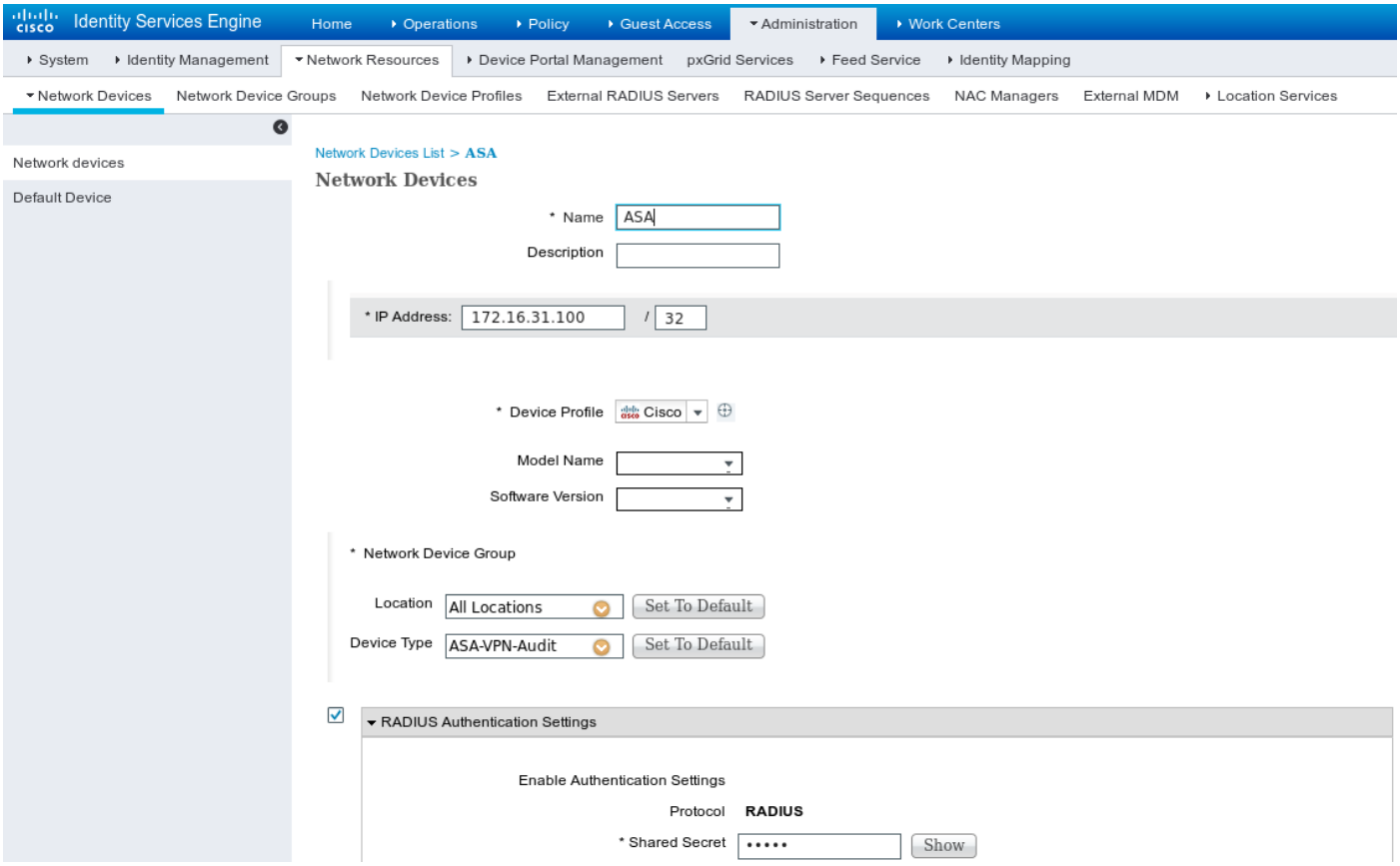
خدمة Active Directory

يجب تكوين تكامل AD ويجب إحضار المجموعات الصحيحة (يتم إستخدام مجموعة Administrators لشرط قاعدة التخويل):



جهاز الوصول إلى الشبكة

تتم إضافة ASA كجهاز شبكة. يتم إستخدام ASA-VPN-Audit للمجموعة المخصصة، كما هو موضح في هذه الصورة:



شهادات ل pxGrid و MnT

تستخدم وحدة التحكم في إدارة الهيكل (FMC) الخدمتين على ISE:

- pxGrid لاستعلام بيانات SGT و PROFILE
- المراقبة وإعداد التقارير (MnT) لتنزيل جلسة العمل المجمعة

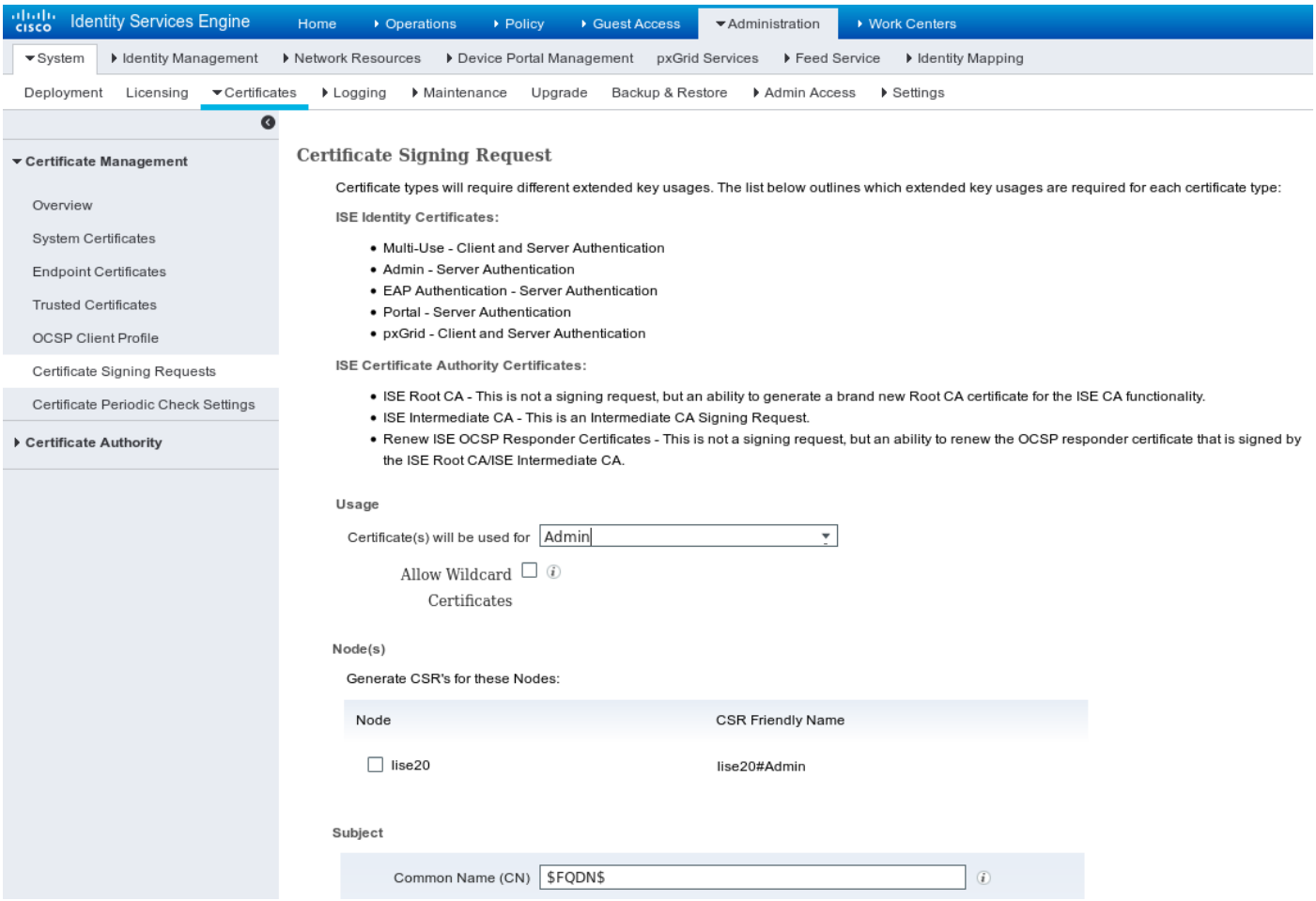
توفر MNt مهم جدا لأنه بهذه الطريقة يتم إعلام FMC بعنوان IP للجلسة المصدق عليها، أيضا اسم المستخدم والرقم المميز. واستنادا إلى ذلك، يمكن تطبيق السياسات الصحيحة. يرجى ملاحظة أن NGIPS لا يدعم بطبيعته علامات الرقيب (وضع العلامات على

الحروف) مثل ASA. على عكس أدارة الاسماء فإنها تدعم اسماء الرقيب بدلا من الارقام فقط.

وبسبب هذه المتطلبات، يحتاج كل من ISE و FMC إلى الثقة في الخدمة الأخرى (شهادة). يستخدم MnT الشهادة الجانبية للخادم فقط، وتستخدم PxGrid الشهادة الجانبية لكل من العميل والخادم.

يستخدم Microsoft CA لتوقيع كافة الشهادات.

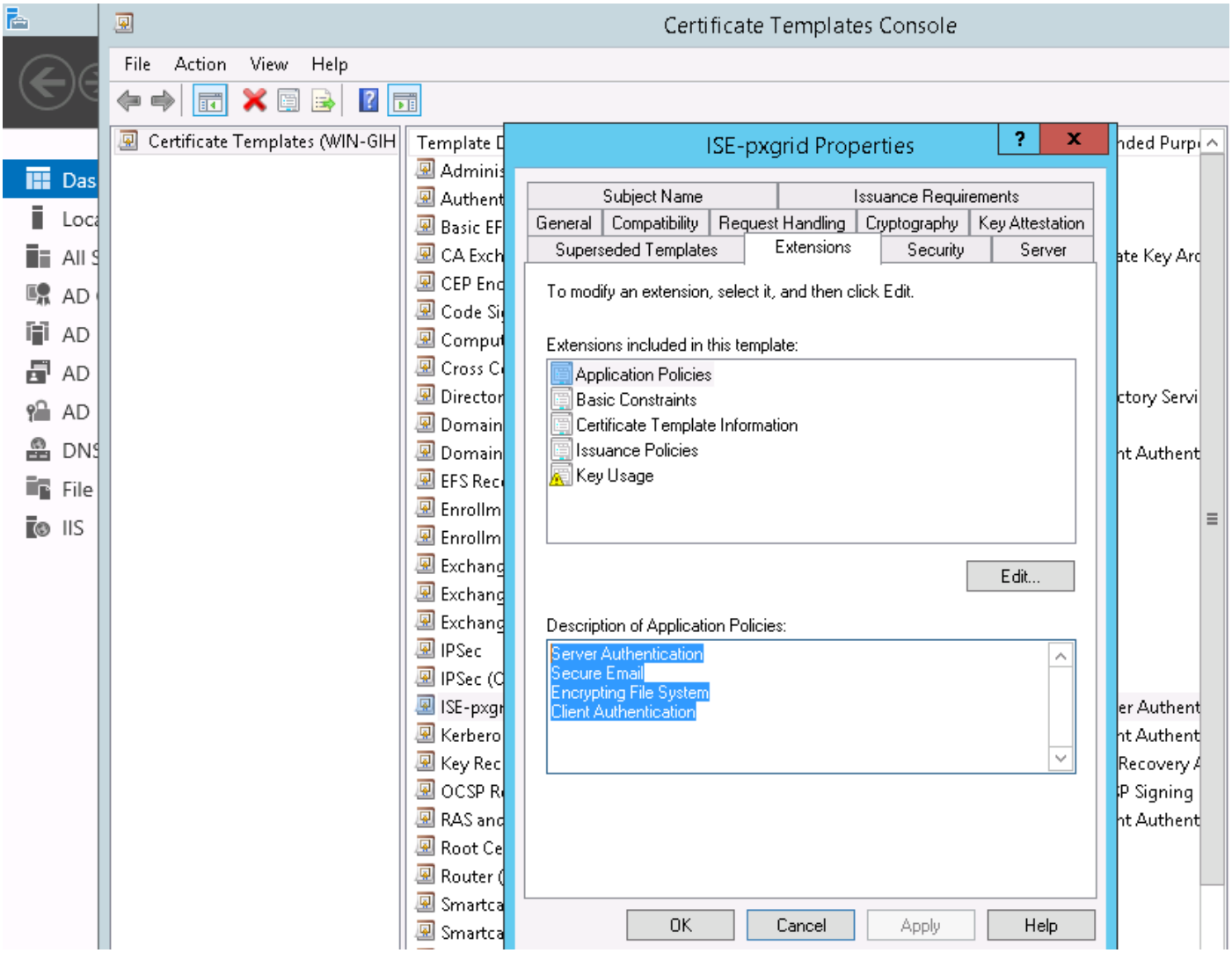
بالنسبة إلى MnT (دور المسؤول)، يجب أن يقوم ISE بإنشاء طلب توقيع الشهادة (CSR)، كما هو موضح في هذه الصورة:



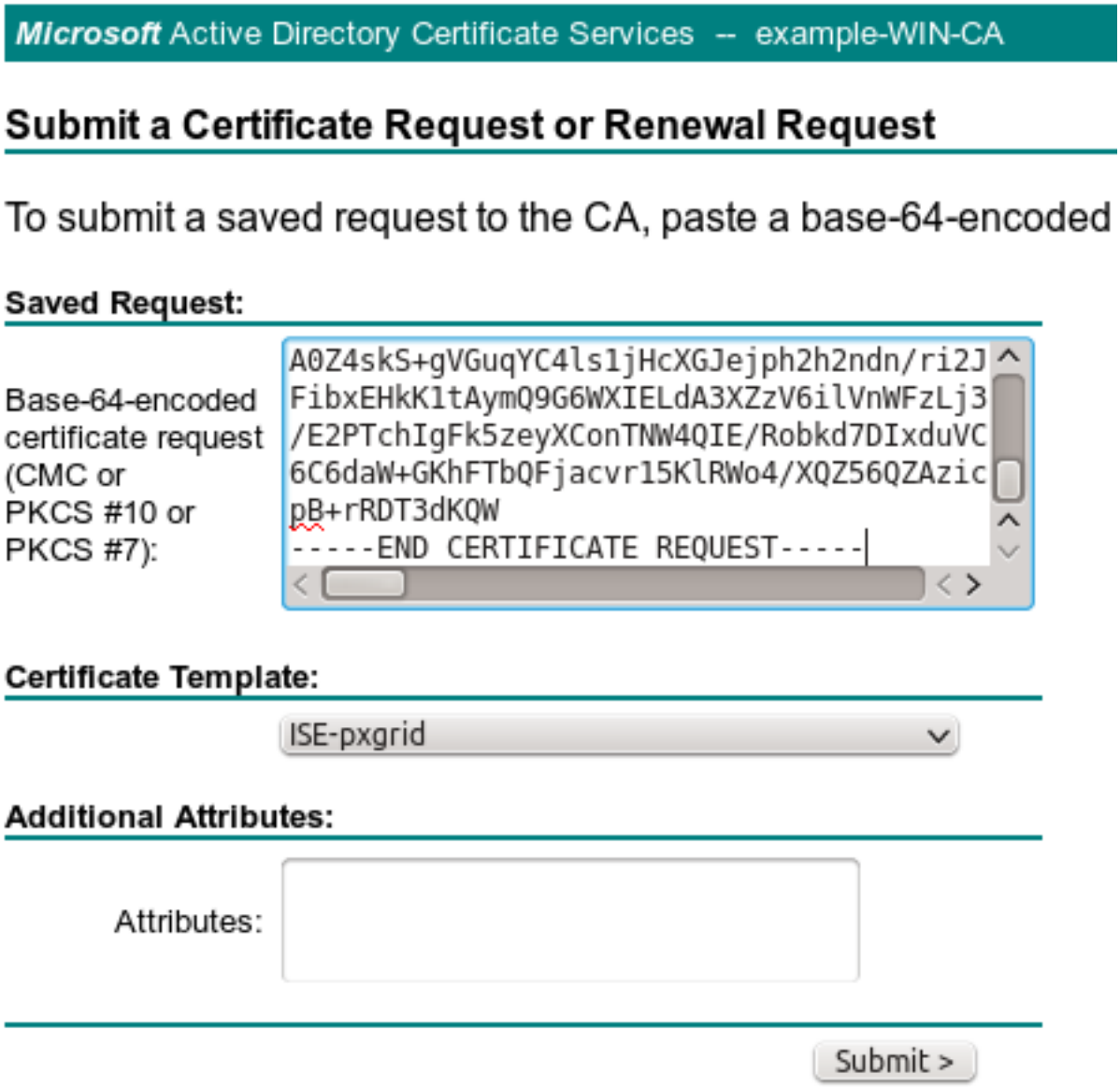
بعد التوقيع بواسطة Microsoft CA يجب إستيراده عبر خيار **ربط الشهادة**.
يجب اتباع عملية مماثلة لخدمة pxGrid. للخيار يجب **سيتم إستخدام الشهادة (الشهادات)** تحديد pxGrid.
بما أنه لا يمكن أن تكون هناك ترخيصين لهما اسم موضوع متطابق، فمن المقبول تماما إضافة قيمة مختلفة لقسم "أنت" أو "o" (على سبيل المثال pxGrid).

> **ملاحظة**: الرجاء التأكد من تكوين سجل DNS الصحيح على خادم DNS لكل اسم مجال مؤهل بالكامل (FQDN) لكل من ISE و FMC.

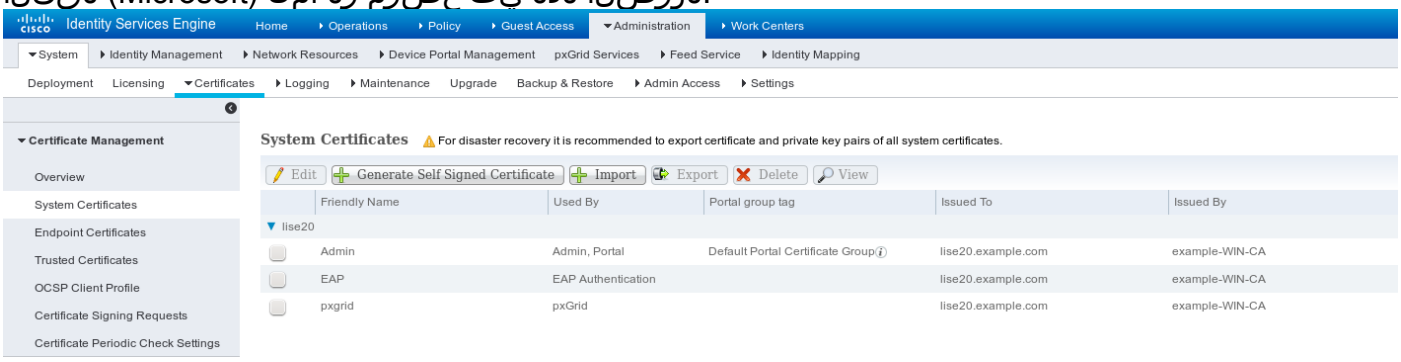
الفرق الوحيد بين شهادة Admin وشهادة PxGrid هو في عملية التوقيع. بما أن شهادات PxGrid يجب أن تتضمن خيارات إستخدام مفتاح موسع لكل من القالب المخصص لمصادقة العميل والخادم على Microsoft CA يمكن إستخدامه لذلك:



تظهر كيفية إستخدام خدمة ويب من Microsoft لتوقيع CSR pxGrid في هذه الصورة:

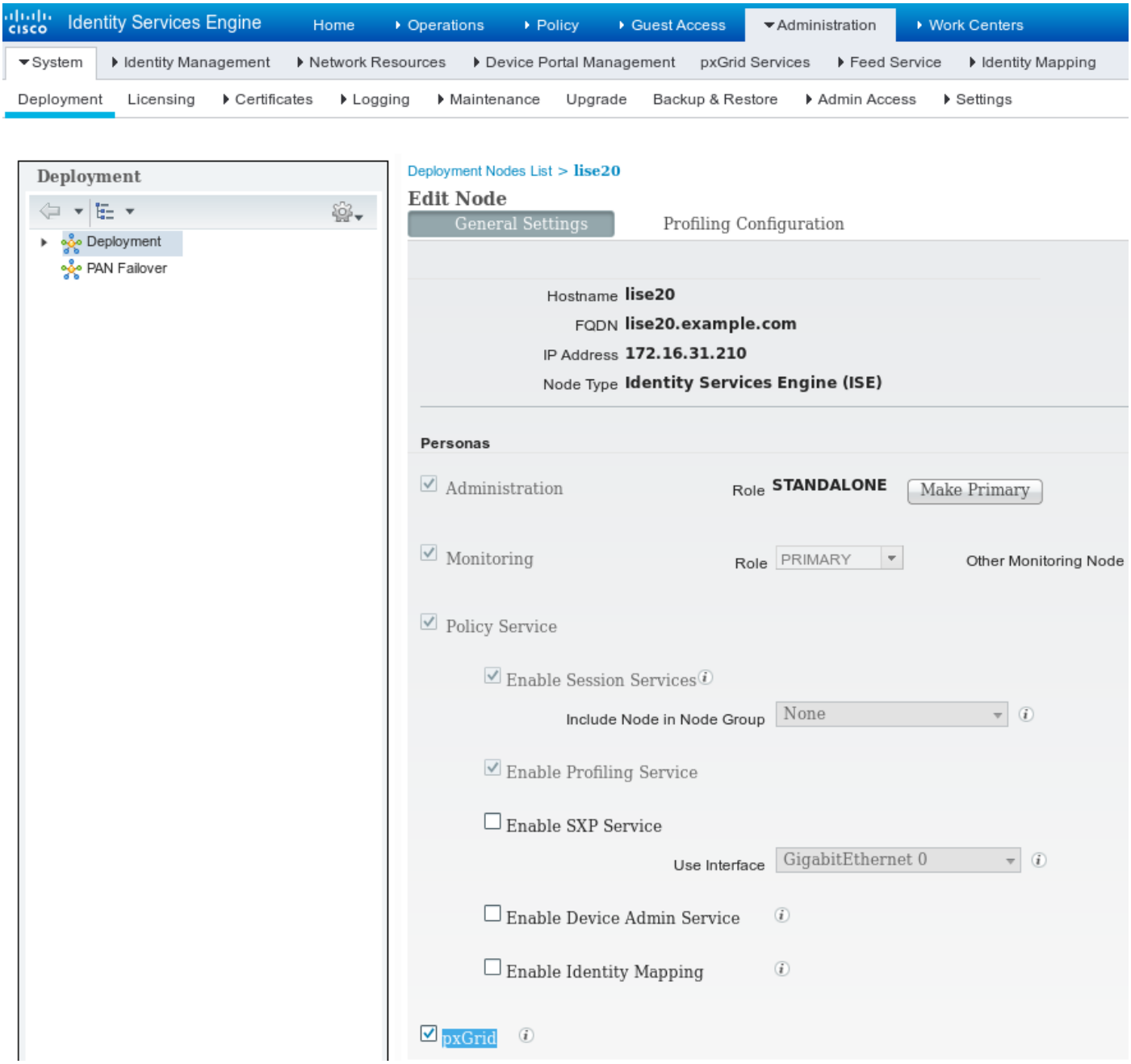


في النهاية ISE ينبغي أن يحتوي على شهادات Admin و pxGrid موقعة من المرجع المصدق الثقة (Microsoft) كما هو موضح في هذه الصورة:

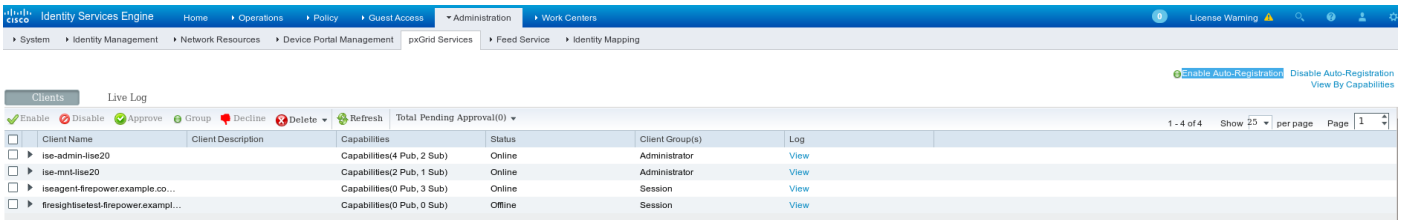


خدمة pxGrid

يجب تمكين دور الشهادات pxGrid الصحيح لعقدة معينة، كما هو موضح في هذه الصورة:



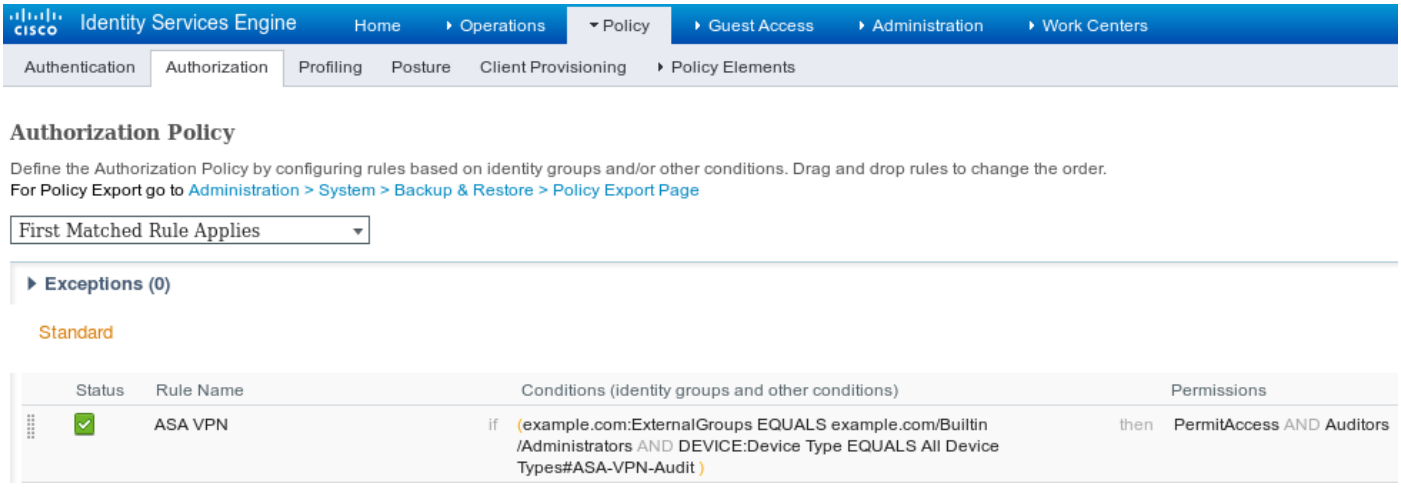
ويجب تعيين الموافقة التلقائية على تمكين:



سياسة التخويل

يتم إستخدام نهج المصادقة الافتراضي (يتم إجراء بحث AD في حالة عدم العثور على المستخدم المحلي).

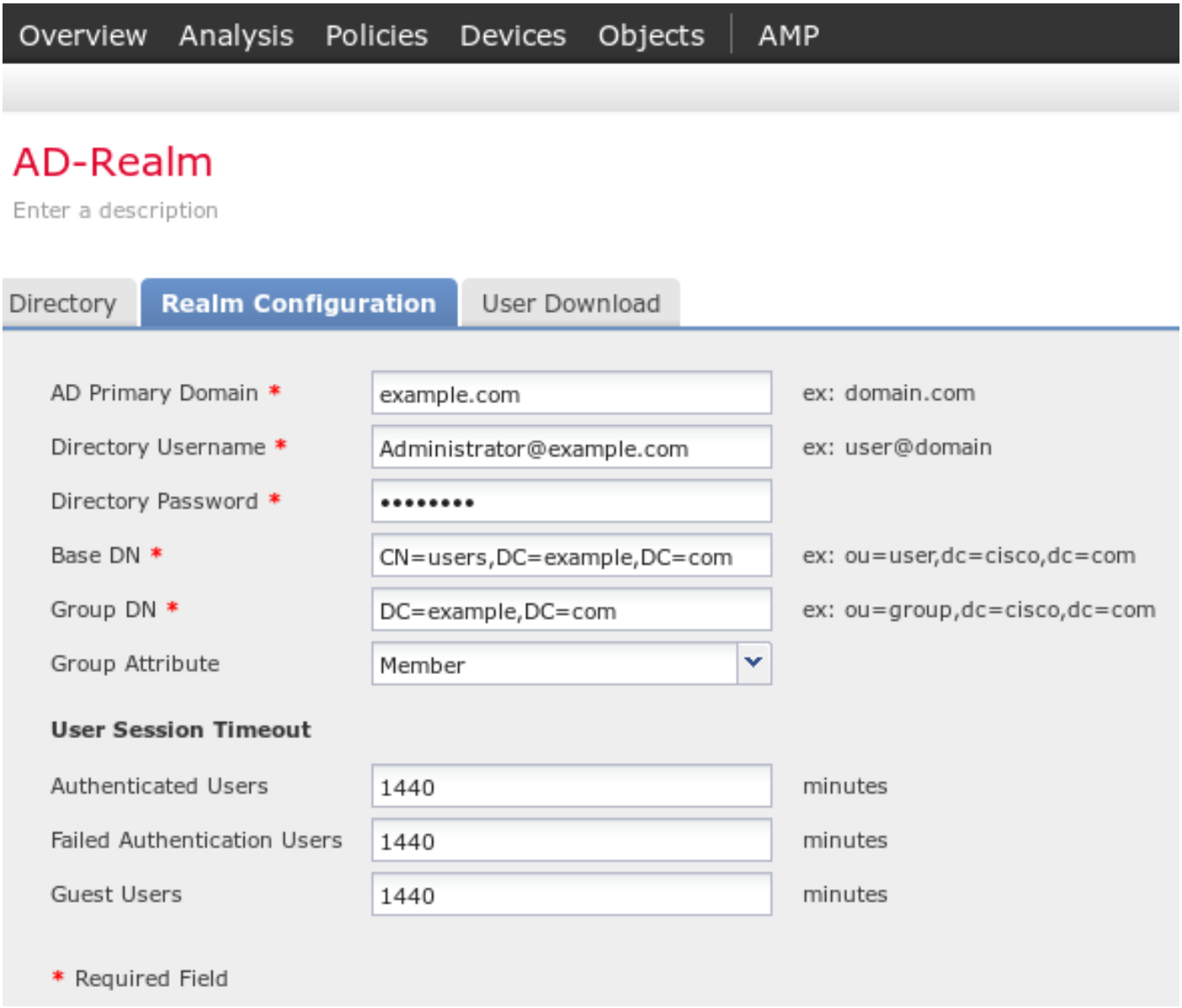
تم تكوين نهج التخويل لتوفير الوصول الكامل إلى الشبكة (الإذن: PermitAccess) للمستخدمين الذين يتم المصادقة عليهم عبر ASA-VPN وينتسبون إلى Active Directory Group Administrators - بالنسبة لهؤلاء المستخدمين يتم إرجاع مدقق Sgt Tag:



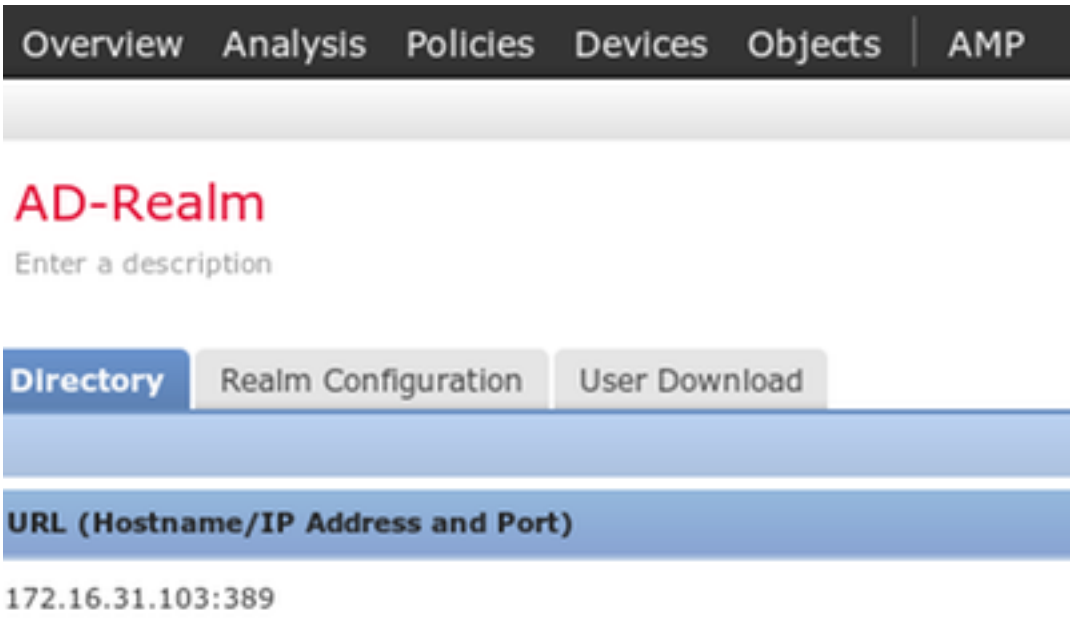
FMC

نطاق Active Directory

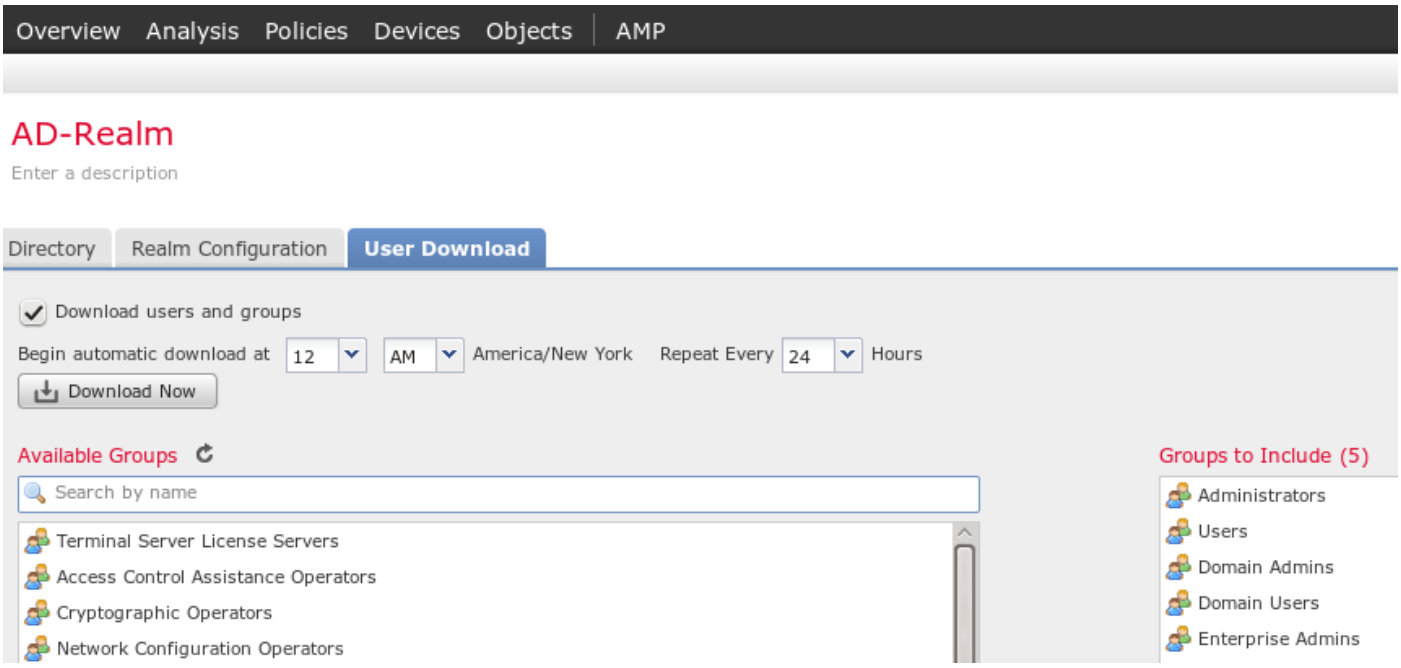
يلزم تكوين النطاق للعمل مع تكامل ISE (لاستخدام سياسات الهوية واسترداد عضوية المجموعة للمستخدمين الذين تمت مصادقتهم بشكل سلبي). يمكن تكوين النطاق لـ Active Directory أو البروتوكول الخفيف للوصول للدليل (LDAP). في هذا المثال، يتم إستخدام AD. من **النظام > التكامل > النطاق**:



يتم إستخدام إعدادات الدليل القياسية:

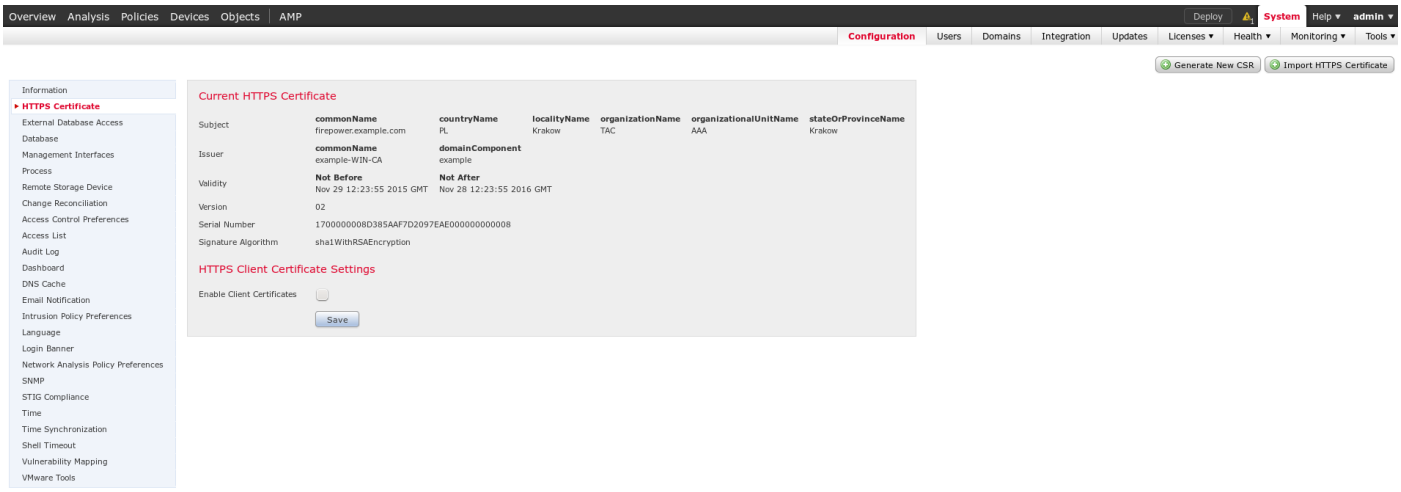


ويتم إستدراد بعض مجموعات AD (الاستخدامها كشرط إضافي في قواعد التحكم بالوصول):



شهادات ل Admin و pxGrid

على الرغم من أنها غير مطلوبة، إلا أنها ممارسة جيدة لإنشاء CSR لوصول المسؤول. قم بالتوقيع على CSR باستخدام AD موثوق به، قم باستيراد الشهادة الموقعة مرة أخرى، كما هو موضح في هذه الصورة:



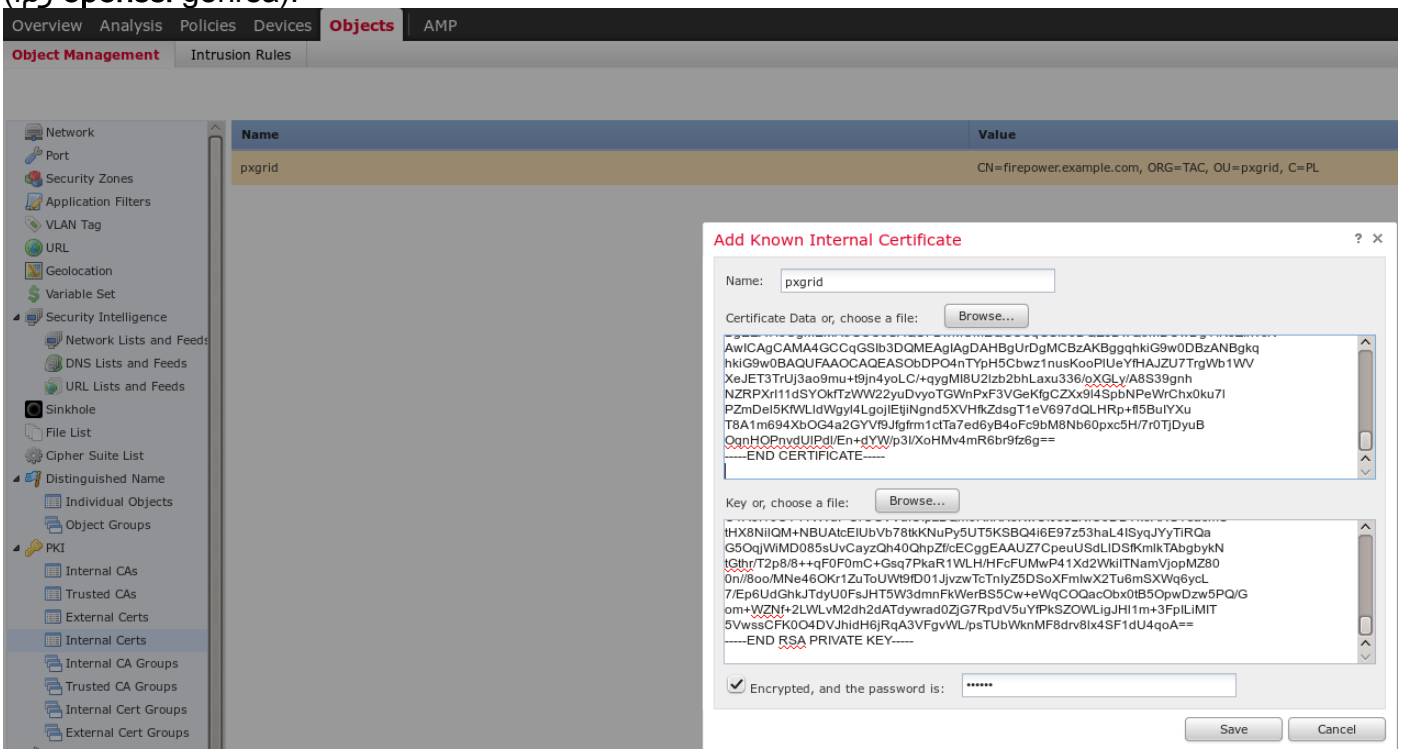
يلزم إضافة شهادة المرجع المصدق إلى مخزن موثوق به:

تتمثل الخطوة الأخيرة في إنشاء شهادة PXgrid التي تستخدمها وحدة التحكم في إدارة

الإطاراات (FMC) لتخويل خدمة ISE pxGrid. لإنشاء واجهة سطر أوامر (CLI) CSR يجب إستخدامها (أو أي جهاز خارجي آخر باستخدام أداة OpenSSL).

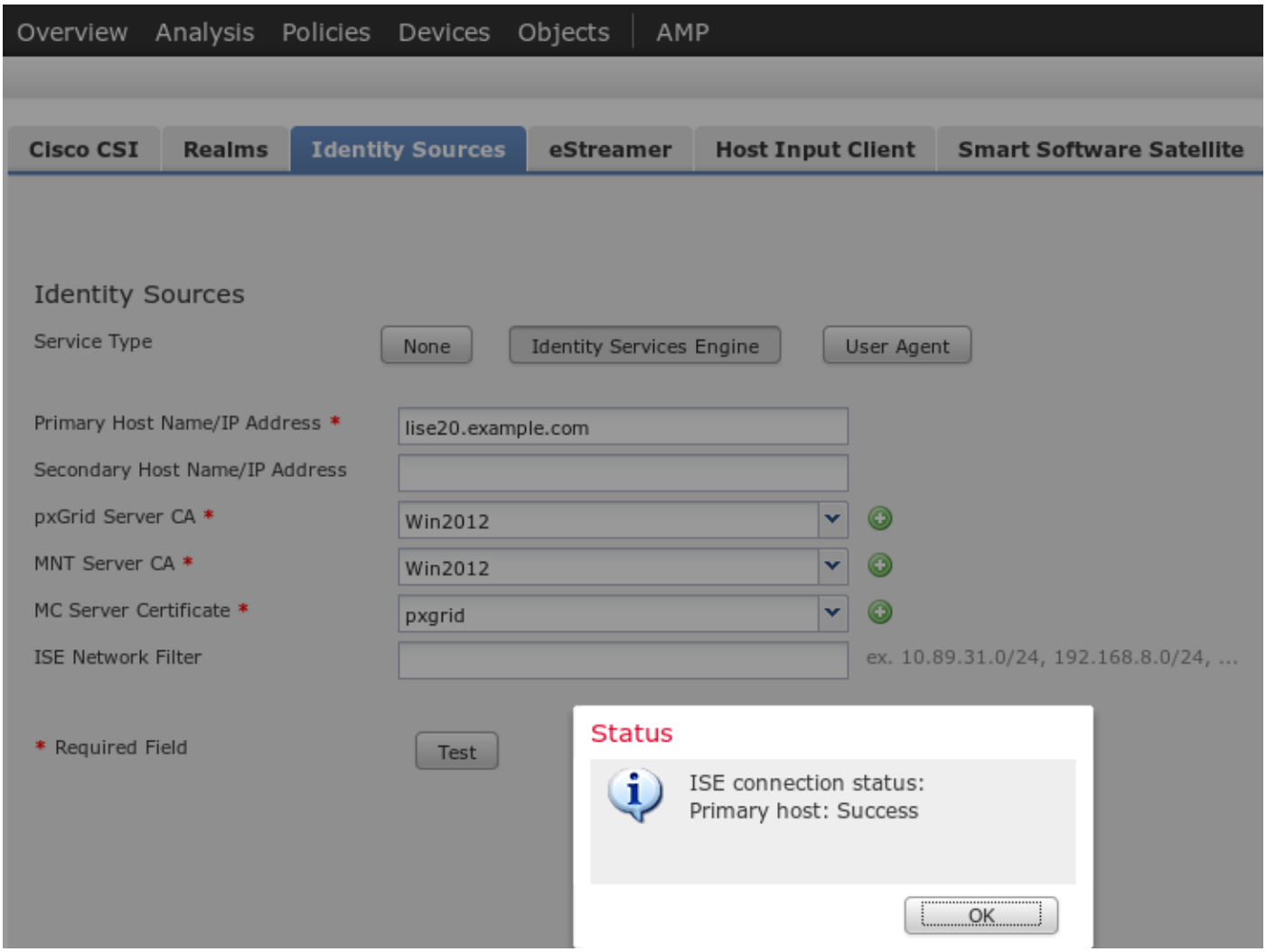
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#
root@firepower:~# openssl req -new -key fire.key -out fire.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Code []:PL
State or Province Name []:
Locality Name []:
Organization Name []:Cisco
Organizational Unit Name []:TAC
Common Name []:firepower.example.com
Email Address []:
root@firepower:~#
```

قم بالتوقيع على Fire.csr بمجرد إنشائه باستخدام Microsoft CA (قالب pxGrid). قم باستيراد المفاتح الخاص (fire.key) والشهادة الموقعة (fire.pem) إلى مخزن الشهادات الداخلي ل FMC. بالنسبة للمفاتح الخاص أستخدم كلمة المرور التي تم إعدادها أثناء إنشاء المفاتح (أمر openssl genrsa):



تكامل ISE

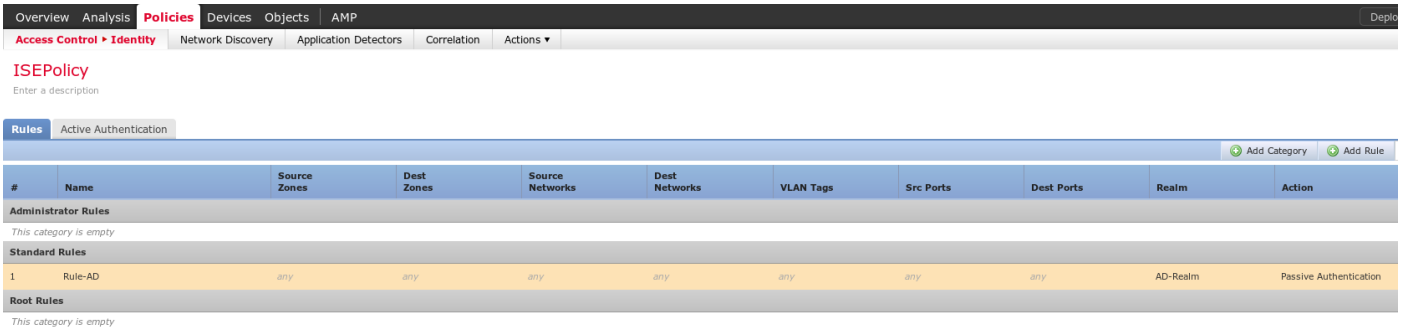
بمجرد تثبيت جميع الشهادات، قم بتكوين تكامل ISE من **النظام > التكامل**:



أستخدم المرجع المصدق المستورد لكل من التحقق من صحة شهادات خدمات PXgrid و MnT. ولوحدة التحكم الإدارية (MC) إستخدام شهادة داخلية تم إنشاؤها ل pxGrid.

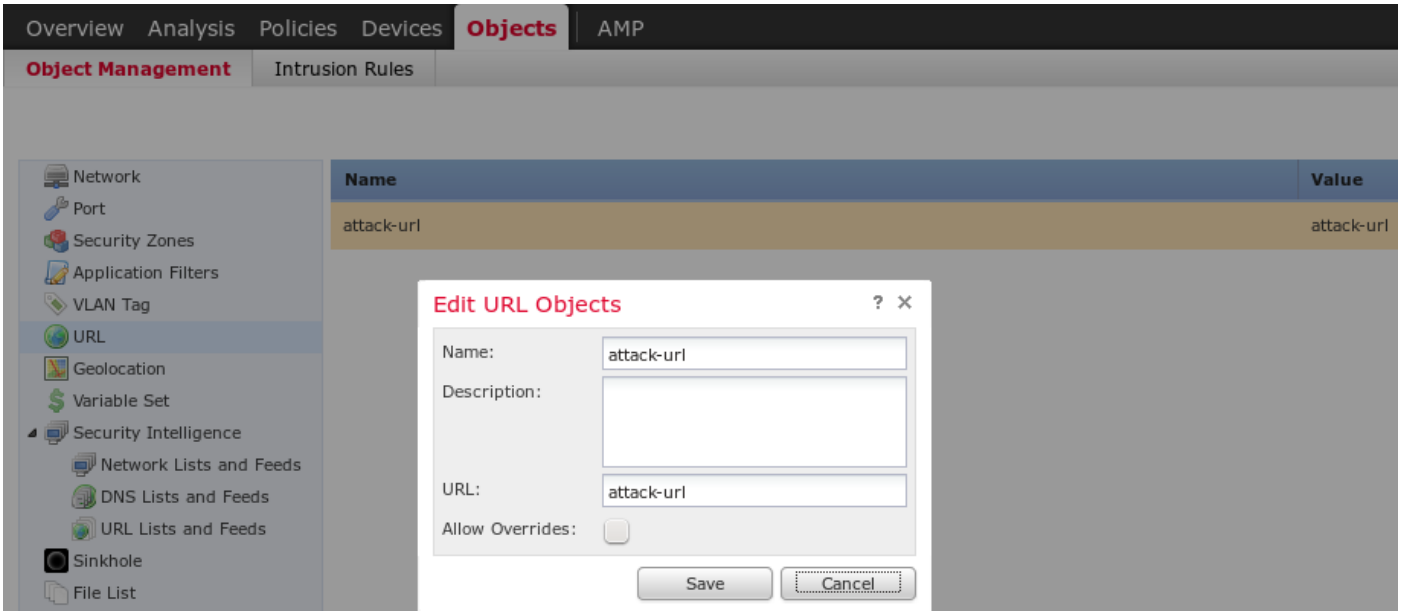
سياسة الهوية

تكوين نهج الهوية الذي يستخدم نطاق AD المكون مسبقا للمصادقة الخاملة:

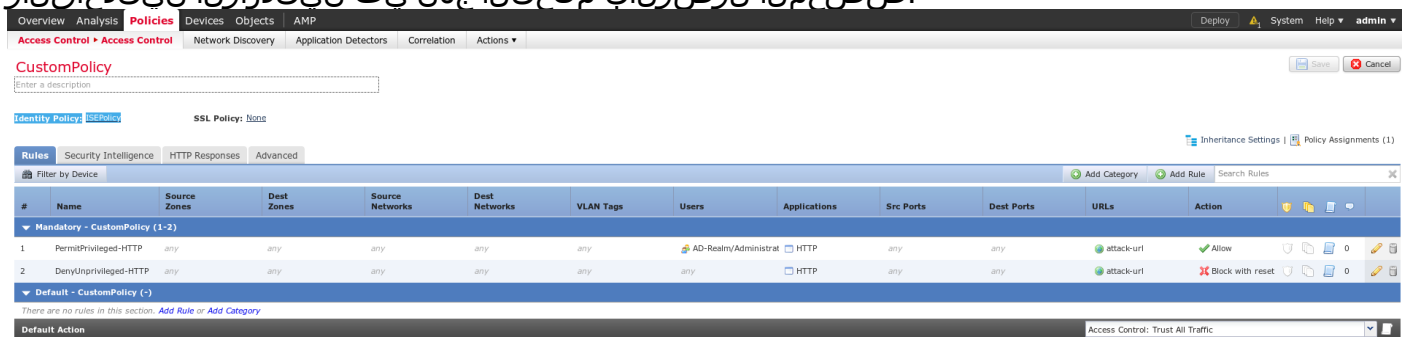


سياسة التحكم في الوصول

لهذا المثال، تم إنشاء عنوان URL المخصص:



والقاعدتين الواردتين في نهج التحكم بالوصول المخصص:

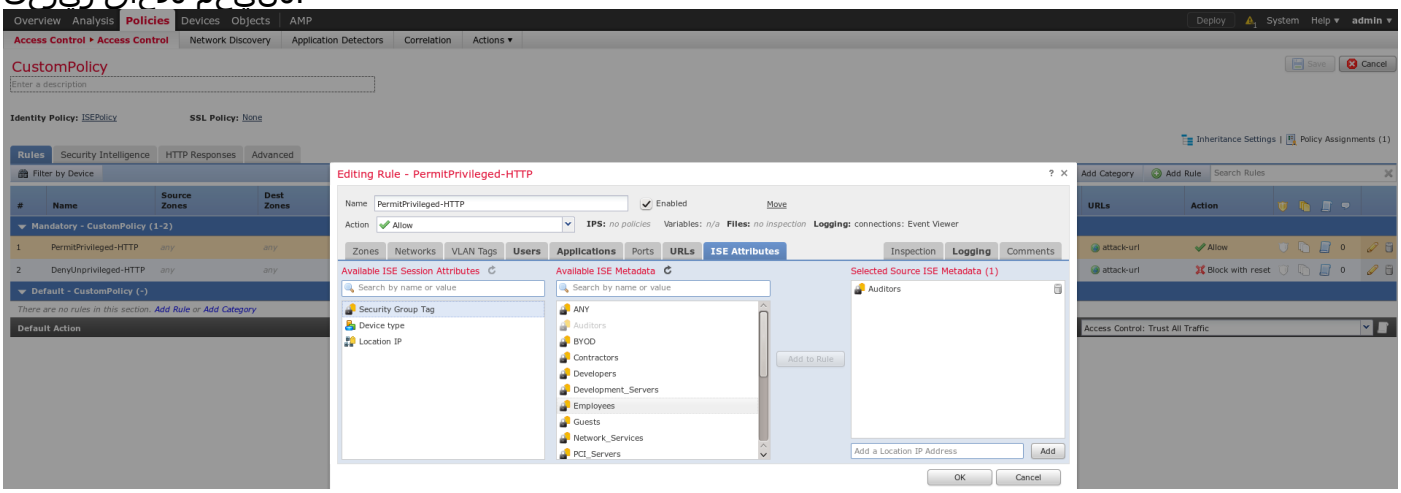


تسمح قاعدة PermitPrivileged-HTTP لجميع المستخدمين الذين ينتمون إلى مجموعة مسؤولي AD الذين تم تعيين علامة SGT لهم. المدققون لتنفيذ هجوم HTTP على كافة الأهداف.

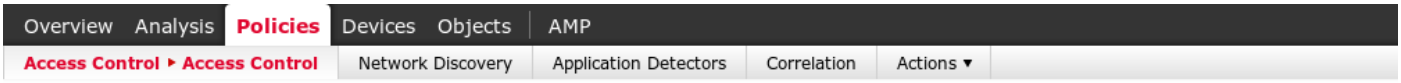
رفض DenyUnprivileged-HTTP هذا الإجراء لكافة المستخدمين الآخرين.

لاحظ أيضا أنه قد تم تعيين نهج الهوية الذي تم إنشاؤه مسبقا لنهج التحكم بالوصول هذا.

في علامة التبويب هذه، من غير الممكن رؤية علامات الرقيب، ولكنها مرئية أثناء إنشاء أو تحرير قاعدة معينة:

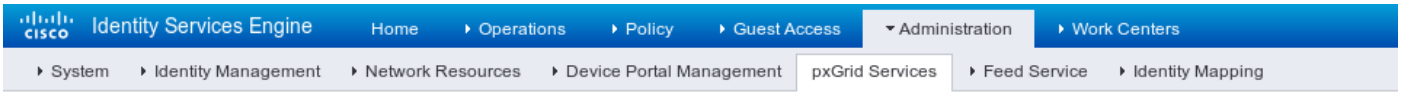


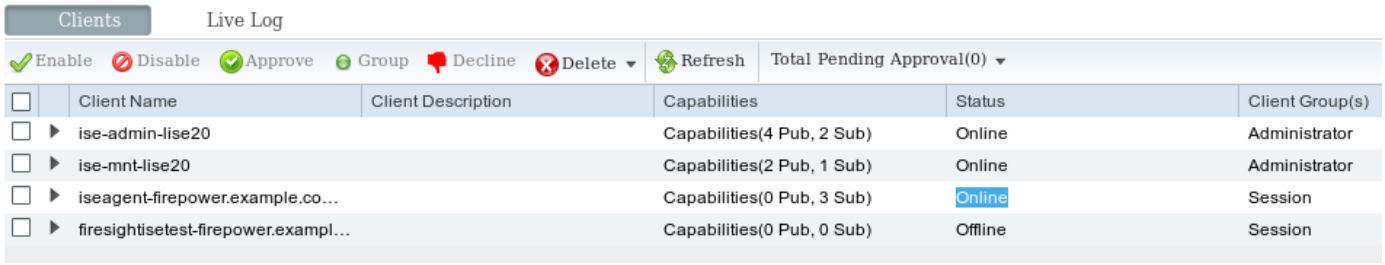
تأكد من تعيين السياسة إلى NGIPS وتم نشر جميع التغييرات:



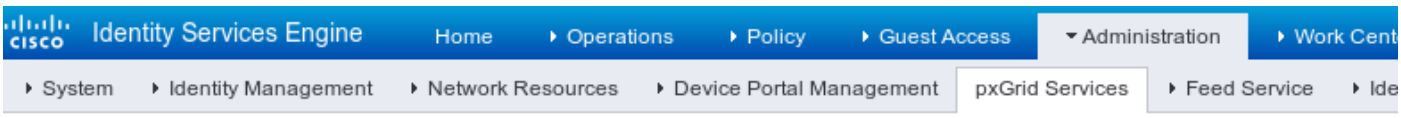
التحقق من الصحة

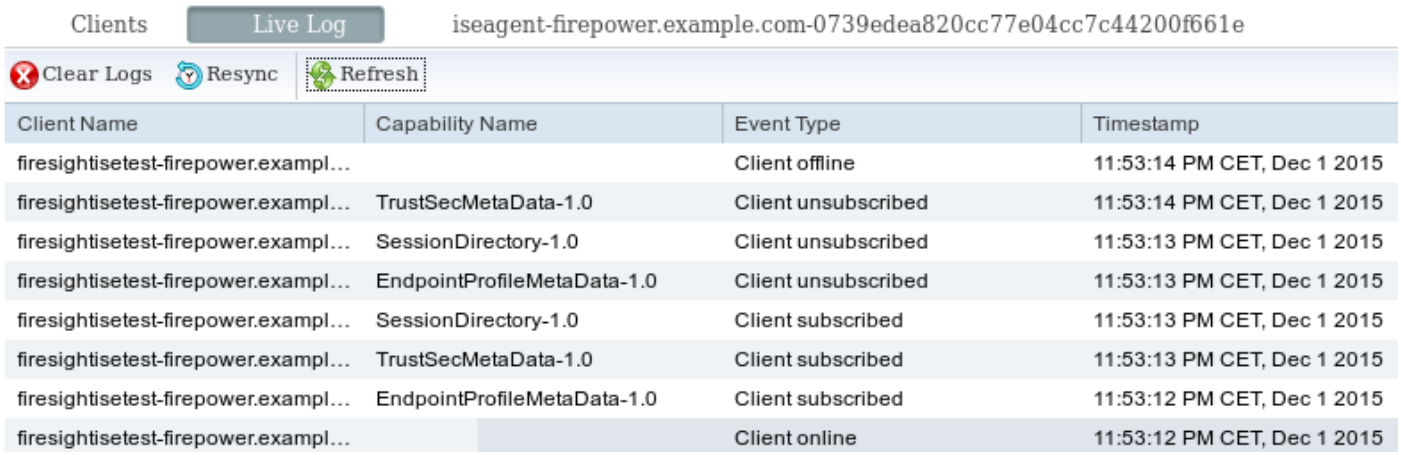
بعد تكوين كل شيء بشكل صحيح، يجب أن يرى ISE اشتراك عميل pxGrid في خدمة جلسة العمل (الحالة عبر الإنترنت).





من السجلات يمكنك أيضا تأكيد أن FMC قد اشترك في خدمة TrustSecMetaData (عالمات SGT) - حصلت على جميع عالمات التمييز وتم إلغاء الاشتراك.

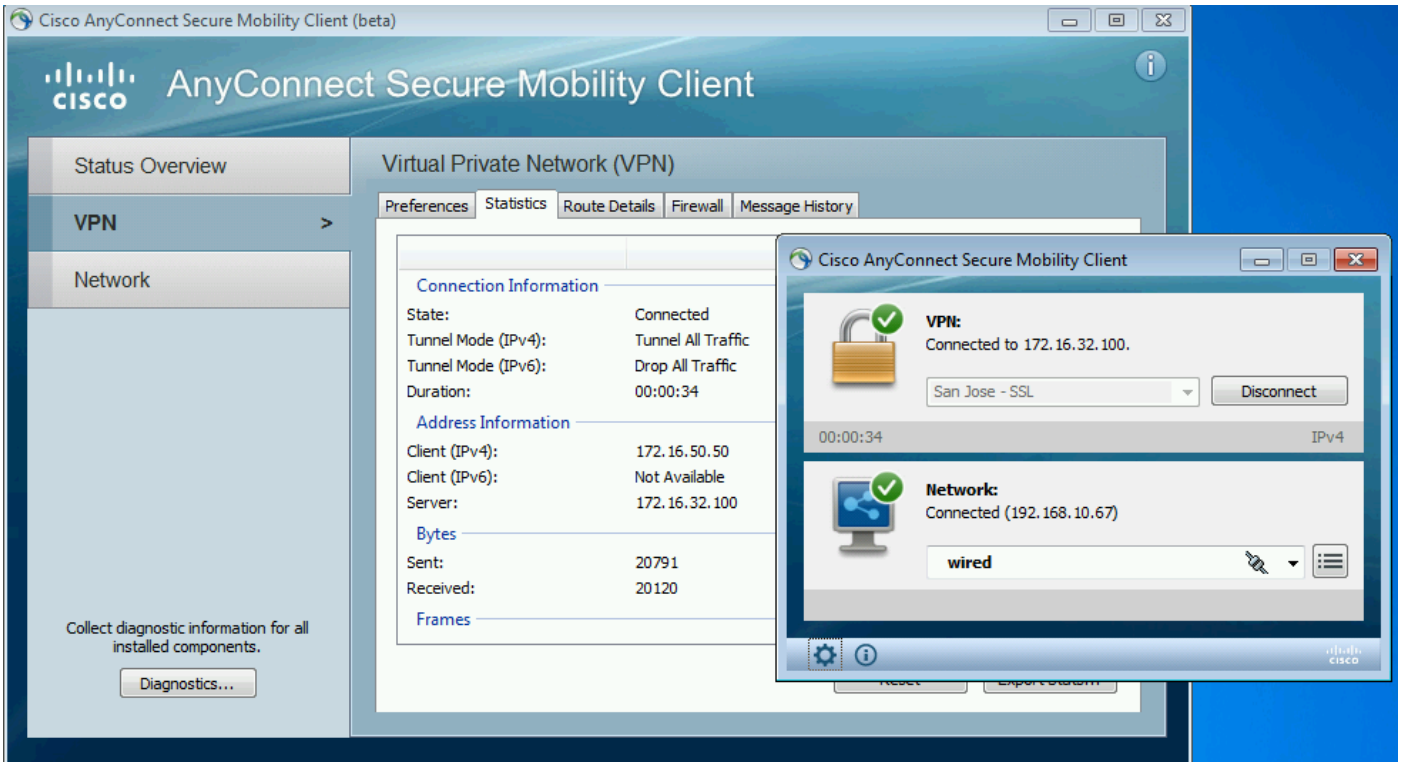




إنشاء جلسة VPN

يتم إجراء الاختبار الأول لسيناريو عندما لا يقوم التفويض على ISE بإرجاع عالمة SGT الصحيحة (لا تسمح بطاقات NGIPS باختبارات التدقيق).

ام إن VPN جلسة up AnyConnect مستعمل قارن (UI) يستطيع زودت كثير تفاصيل:



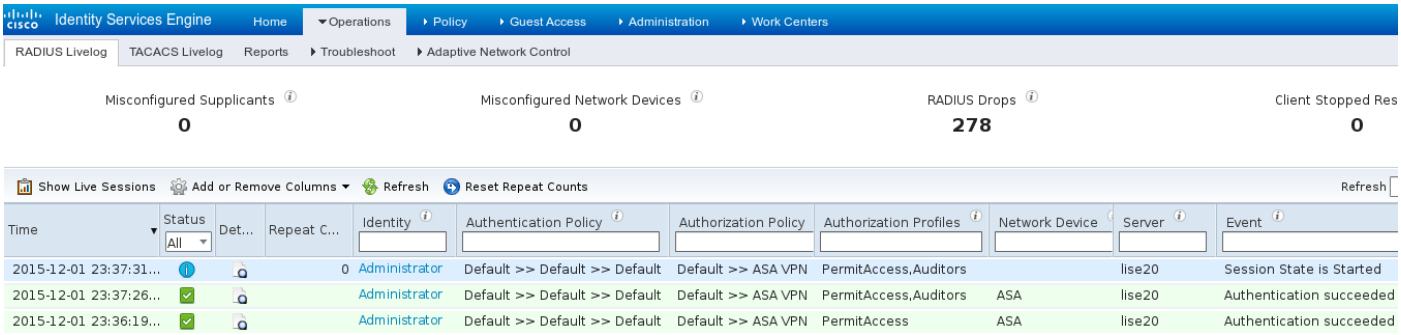
يمكن ل ASA تأكيد تأسيس الجلسة:

```
asav# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Administrator          Index        : 1
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.67
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel:
(1)AES128

Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel:
(1)SHA1

Bytes Tx     : 11428                  Bytes Rx     :
24604

Group Policy : POLICY                 Tunnel Group :
SSLVPN

Login Time   : 12:22:59 UTC Wed Dec 2
2015

Duration     :
0h:01m:49s


Inactivity   :
0h:00m:00s


VLAN Mapping : N/A                    VLAN         :
none
```

```
Audt Sess ID : ac101f6400001000565ee2a3
```

يرجى ملاحظة أن ASA ال يرى أي رقم رقيب تم إرجاعه لهذه المصادقة. لم يتم تكوين ASA ل TrustSec - حتى يتم تخطي المعلومات على أي حال.

يقوم ISE أيضا بالإبلاغ عن التفويض الناجح (السجل في تمام الساعة 23:36:19) - لم يتم إرجاع أية علامة رقيب:



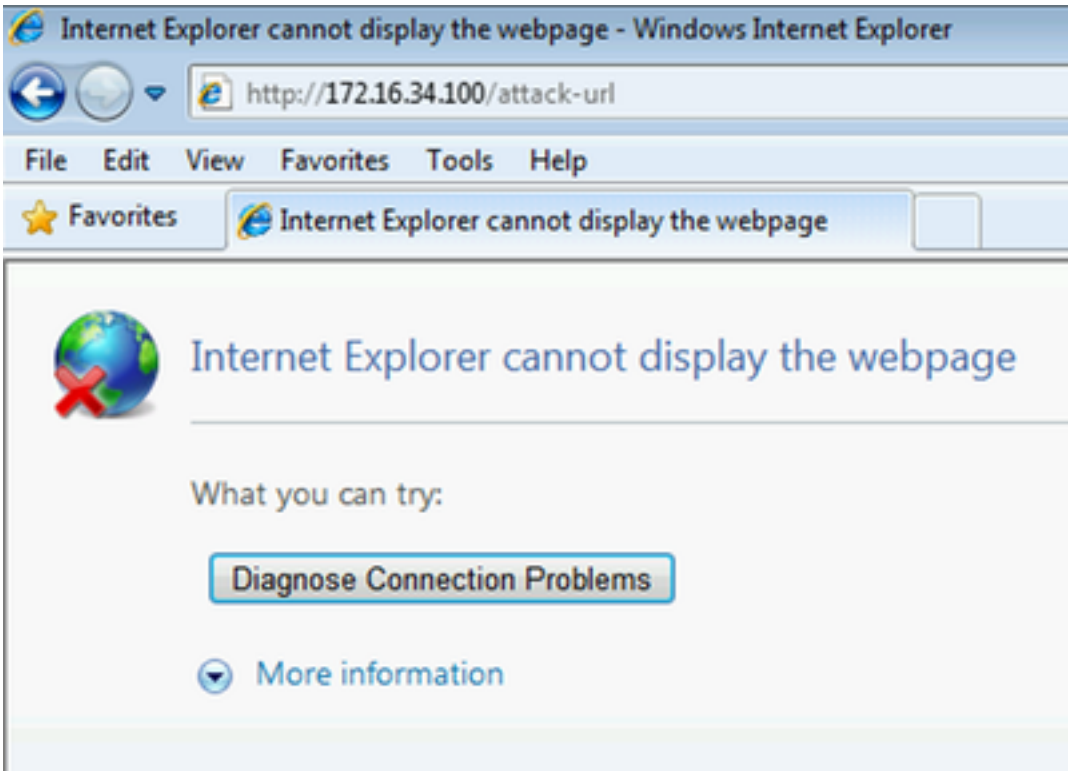
FMC يحصل على بيانات الجلسة من MnT

في تلك المرحلة، يرسل FMC في /var/log/messages تقريرا عن جلسة عمل جديدة (تم تلقيها كمشترك لخدمة pxGrid) لاسم مستخدم المؤول وبحث AD للنموذج الأساسي لعضوية المجموعة:

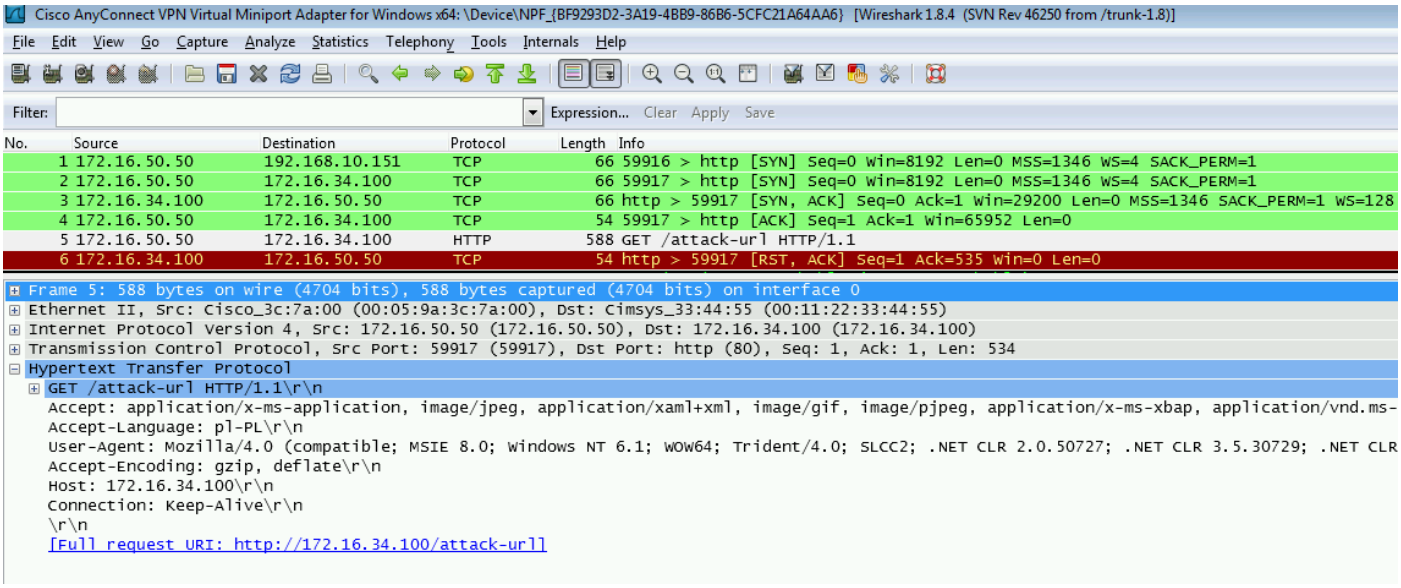
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

الوصول إلى الشبكة دون أي امتيازات أو امتيازات

عندما يحاول المستخدم في هذه المرحلة فتح مستعرض ويب والوصول إلى الخادم الذي تم تدقيقه، سيتم إنهاء الاتصال:



يمكن تأكيدها بواسطة التقاط الحزمة التي تم أخذها من العميل (إرسال TCP RST وقفا لتكوين FMC):

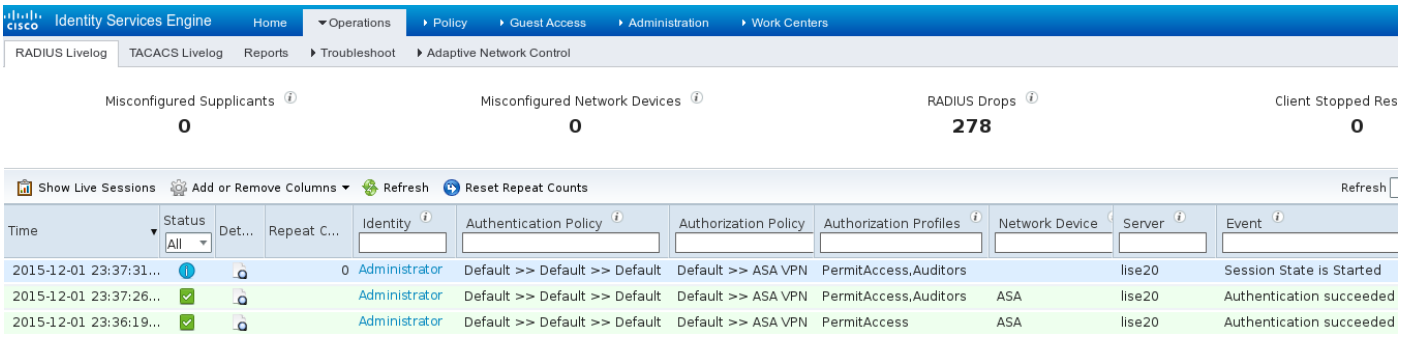


ما إن شكلت ISE يكون أن يرجع، التدقيق بطاقة ASA جلسة تقارير:

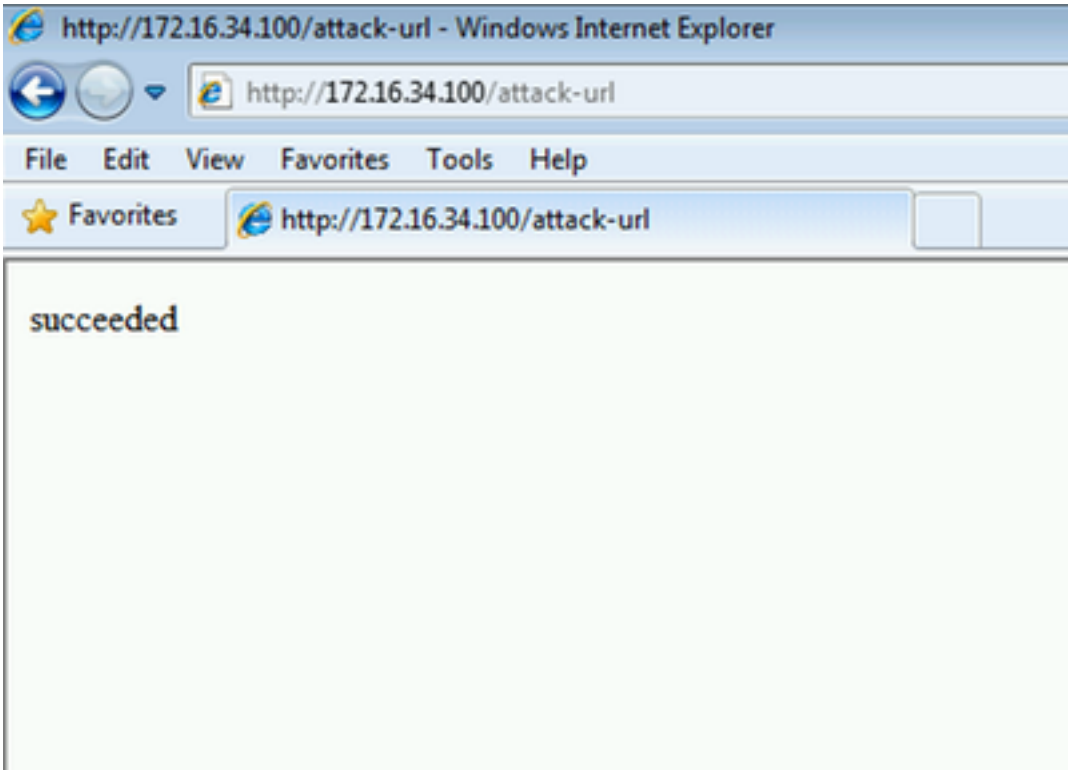
```
asav# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Administrator          Index        : 1
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.67
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel:
(1)AES128

Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel:
(1)SHA1

Bytes Tx     : 11428                  Bytes Rx     :
24604

Group Policy : POLICY                 Tunnel Group :
SSLVPN

Login Time   : 12:22:59 UTC Wed Dec 2
2015

Duration     :
0h:01m:49s


Inactivity   :
0h:00m:00s


VLAN Mapping : N/A                    VLAN         :
none

Audt Sess ID : ac101f6400001000565ee2a3
Security Grp : 9
```

يقوم ISE أيضا بالإعلام عن نجاح التفويض (السجل في تمام الساعة 23:37:26) - يتم إرجاع

مدقق العلامة SGT:

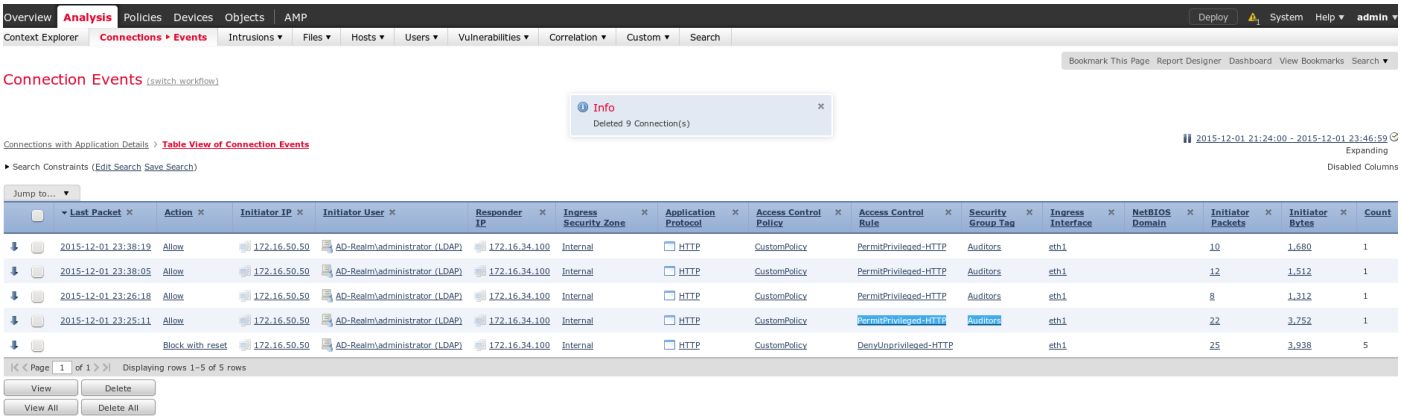


ويمكن للمستخدم الوصول إلى الخدمة المذكورة:



الوصول إلى تسجيل FMC

يمكن تأكيد هذا النشاط بواسطة تقرير حدث الاتصال:



أولا، لم يكن المستخدم قد تم تعيين رقيب وكان يضرب قاعدة DenyUnprivileged-HTTP. بمجرد تعيين علامة المدقق بواسطة ISE (واستعادتها بواسطة قاعدة FMC)، يتم إستخدام PermitPrivileged-HTTP ويتم السماح بالوصول.

ةدعاق ضرع متي ام ةداع هنأل ةددعتم ةدمعأ ةلازإ تمت ،ضرعلا ىلع لوصحلل هنأ اضيأ ظحال ريرمتلا طيرش مادختسإ بجيو) ةريخألا ةدمعألا دحأك نامألا ةعومجم ةمالعو لوصولاب مكحتلا يقفألا). نكمي ظفح ةقيرط ضرعلا ةصصخملا هذه ةداعإو اهمادختسإ يف لبقتسملا.

اهحالصإو ءاطخألا فاشكتسا

تصحيح أخطاء FMC

ققحتلل نم تالجس نوكم ADI لوؤسملا نع ققحتلا نم تامدخ ةيوهلا /var/log/messages file:

```
[23509] ADI_ISE_Test_Help:ADI_ISE_Test_Help [INFO] Parsing command line arguments...
[23509] ADI_ISE_Test_Help:adi.DirectoryTestHandler [INFO] test: ISE connection.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing ISE Connection objects...

[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing subscription objects...

[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
EndpointProfileMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
EndpointProfileMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
TrustSecMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
TrustSecMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
SessionDirectoryCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
SessionDirectoryCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Connecting to ISE server...
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Beginning to connect to ISE server...

[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: _reconnection_thread started
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: pxgrid connection init done successfully
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: connecting to host lise20.example.com .......
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: stream opened
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: EXTERNAL authentication complete
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: authenticated successfully (sasl mechanism: EXTERNAL)
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: successfully subscribed
message repeated 2 times
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Queried 1 bulk download
hostnames:lise20.example.com:8910
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] ...successfully connected to ISE
server.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Starting bulk download
[23514] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: curl_easy_setopt() for CURLOPT_URL:
'https://lise20.example.com:8910/pxgrid/mnt/sd/getSessionListByTime'
[8893] ADI:ADI [INFO] : sub command emits:'* Trying 172.16.31.210...'
[8893] ADI:ADI [INFO] : sub command emits:'* Connected to lise20.example.com (172.16.31.210)
port 8910 (#0)'
[8893] ADI:ADI [INFO] : sub command emits:'* Cipher selection:
ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH'
```

```
[8893] ADI:ADI [INFO] : sub command emits:'* SSL connection using TLSv1.2 / DHE-RSA-AES256-
SHA256'
[8893] ADI:ADI [INFO] : sub command emits:'* Server certificate:'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I subject: CN=lise20.example.com'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I start date: 2015-11-21 14:40:36 GMT'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I expire date: 2017-11-20 14:40:36 GMT'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I common name: lise20.example.com (matched)'

[8893] ADI:ADI [INFO] : sub command emits:'* ^I issuer: DC=com; DC=example; CN=example-WIN-
CA'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I SSL certificate verify ok.'
[8893] ADI:ADI [INFO] : sub command emits:'> POST /pxgrid/mnt/sd/getSessionListByTime
HTTP/1.1^M'
[8893] ADI:ADI [INFO] : sub command emits:'Host: lise20.example.com:8910^M'
[8893] ADI:ADI [INFO] : sub command emits:'Accept: */*^M'
[8893] ADI:ADI [INFO] : sub command emits:'Content-Type: application/xml^M'
[8893] ADI:ADI [INFO] : sub command emits:'user:firesightisetest-firepower.example.com-
0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com^M'
[8893] ADI:ADI [INFO] : sub command emits:'Content-Length: 269^M'
[8893] ADI:ADI [INFO] : sub command emits:'^M'
[8893] ADI:ADI [INFO] : sub command emits:'* upload completely sent off: 269 out of 269 bytes'

[8893] ADI:ADI [INFO] : sub command emits:'< HTTP/1.1 200 OK^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Date: Tue, 01 Dec 2015 23:10:45 GMT^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Content-Type: application/xml^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Content-Length: 1287^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Server: ^M'
[8893] ADI:ADI [INFO] : sub command emits:'< ^M'
[8893] ADI:ADI [INFO] : sub command emits:'* Connection #0 to host lise20.example.com left
intact'
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] bulk download processed 0 entries.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] disconnecting pxgrid
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: Starting reconnection stop
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: _reconnection_thread exited
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: stream closed; err_dom=(null) 2015-12-01T23:10:45 [ INFO]: clientDisconnectedCb ->
destroying client object
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: pxgrid connection shutdown done successfully
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: Exiting from event base loop
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: successfully disconnected
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: connection disconnect done .....
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying pxgrid reconnection
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying underlying pxgrid
connection
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying pxgrid config
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] ISE identity feed destructor called

[23509] ADI_ISE_Test_Help:ADI_ISE_Test_Help [INFO] /usr/local/sf/bin/adi_iseTestHelp cleanly
exits.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: pxgrid library has been uninitialized
[8893] ADI:ADI [INFO] Parent done waiting, child completed with integer status 0
```

للحصول على تصحيح أكثر تفصيلاً، من الممكن قتل العملية اليومية (من الجذر بعد السدود) وتشغيلها باستخدام وسيطة تصحيح الأخطاء:

```
root@firepower:/var/log# ps ax | grep adi
```

```
24047 ?        Sl     0:00 /usr/local/sf/bin/adi
24090 pts/0    S+     0:00 grep adi
root@firepower:/var/log# kill -9 24047
root@firepower:/var/log# /usr/local/sf/bin/adi --debug
Dec 01 23:14:34 firepower SF-IMS[24106]: [24106] ADI:adi.Adi [DEBUG] adi.cpp:319:HandleLog():
ADI Created, awaiting config
Dec 01 23:14:34 firepower SF-IMS[24106]: [24106] ADI:config [DEBUG]
config.cpp:289:ProcessConfigGlobalSettings(): Parsing global settings
<..........a lot of detailed output with data.......>
```

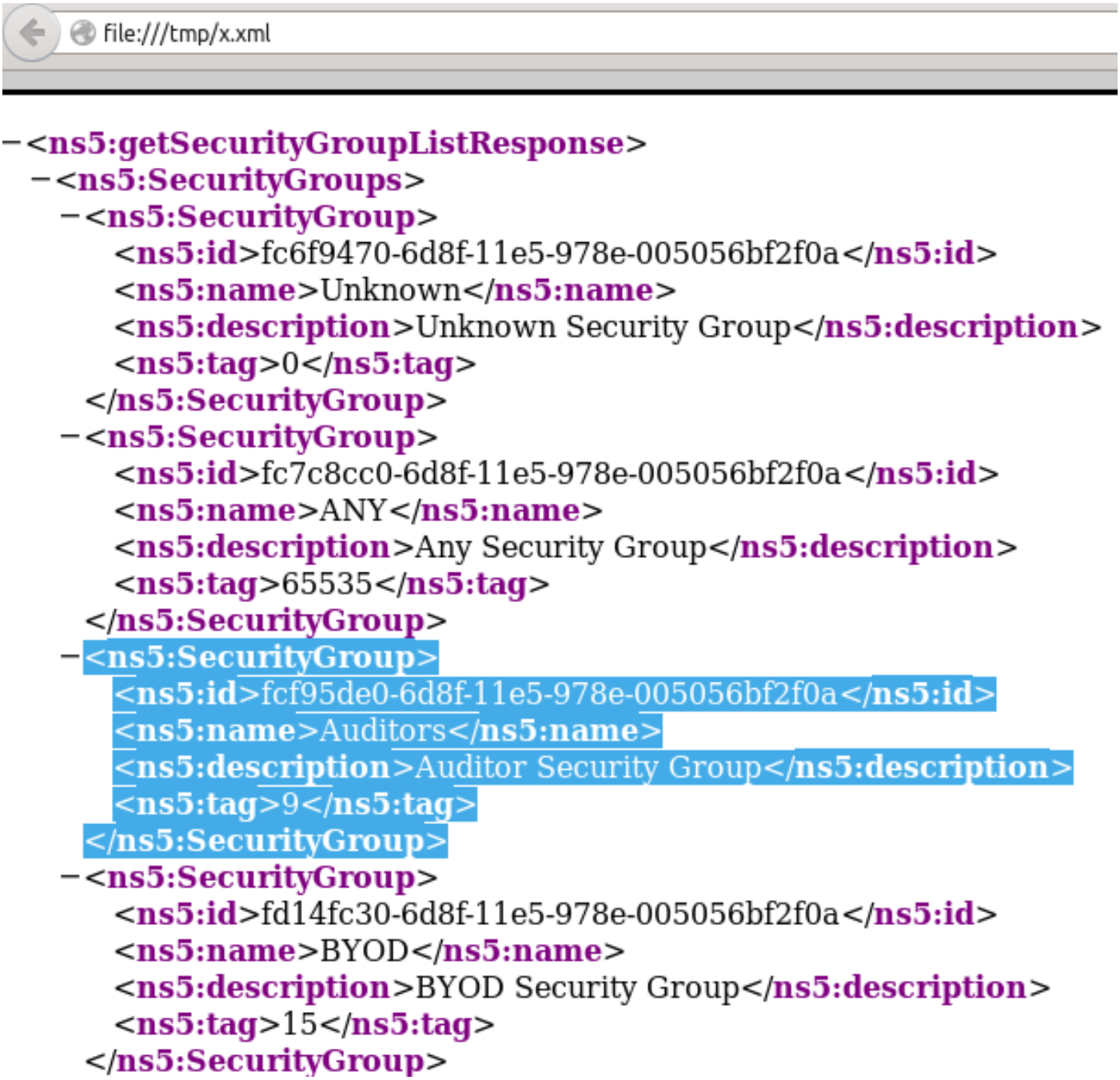
استعلام SGT عبر PXgrid

يتم تنفيذ العملية عند النقر فوق زر **الاختبار** في قسم **تكامل ISE** أو عند تحديث قائمة الرقيب، أثناء إضافة قاعدة في نهج التحكم بالوصول.

```
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): Querying Security Group metaData...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): pxgrid_connection_query(connection*:0x10c7da0, capability: 0x1064510,
request:<getSecurityGroupListRequest xmlns='http://www.cisco.com/pxgrid/identity'/>)...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK|<ns5:getSecurityGroupListResponse
xmlns:ns2='http://www.cisco.com/pxgrid' xmlns:ns3='http://www.cisco.com/pxgrid/net'
xmlns:ns4='http://www.cisco.com/pxgrid/admin' xmlns:ns5='http://www.cisco.com/pxgrid/identity'
xmlns:ns6='http://www.cisco.com/pxgrid/eps' xmlns:ns7='http://www.cisco.com/pxgrid/netcap'
xmlns:ns8='http://www.cisco.com/pxgrid/anc'><ns5:SecurityGroups><ns5:SecurityGroup><ns5:id>fc6f9
470-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Unknown</ns5:name><ns5:description>Unknown
Security
Group</ns5:description><ns5:tag>0</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc7c8c
c0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>ANY</ns5:name><ns5:description>Any Security
Group</ns5:description><ns5:tag>65535</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc
f95de0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Auditors</ns5:name><ns5:description>Auditor
Security
Group</ns5:description><ns5:tag>9</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd14fc
30-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>BYOD</ns5:name><ns5:description>BYOD Security
Group</ns5:description><ns5:tag>15</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd2fb
020-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Contractors</ns5:name><ns5:description>Contractor Security
Group</ns5:description><ns5:tag>5</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd4e34
a0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Developers</ns5:name><ns5:description>Developer
Security
Group</ns5:description><ns5:tag>8</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd6d2e
50-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Development_Servers</ns5:name><ns5:description>Development
Servers Security
Group</ns5:description><ns5:tag>12</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fda10
f90-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Employees</ns5:name><ns5:description>Employee
Security
Group</ns5:description><ns5:tag>4</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdbcd4
f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Guests</ns5:name><ns5:description>Guest
Security
Group</ns5:description><ns5:tag>6</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdd9ab
c0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Network_Services</ns5:name><ns5:description>Network Services
Security
Group</ns5:description><ns5:tag>3</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdf4d4
e0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>PCI_Servers</ns5:name><ns5:description>PCI
Servers Security
Group</ns5:description><ns5:tag>14</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe11a
bb0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Point_of_Sale_Systems</ns5:name><ns5:description>Point of Sale
Security
```

Group</ns5:description><ns5:tag>10</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe2d2
2f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Servers</ns5:name><ns5:description>Production Servers
Security
Group</ns5:description><ns5:tag>11</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe487
320-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Users</ns5:name><ns5:description>Production User
Security
Group</ns5:description><ns5:tag>7</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe62d8
f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Quarantined_Systems</ns5:name><ns5:description>Quarantine
Security
Group</ns5:description><ns5:tag>255</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe7d
3ec0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Test_Servers</ns5:name><ns5:description>Test
Servers Security
Group</ns5:description><ns5:tag>13</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe99c
770-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>TrustSec_Devices</ns5:name><ns5:description>TrustSec Devices
Security
Group</ns5:description><ns5:tag>2</ns5:tag></ns5:SecurityGroup></ns5:SecurityGroups></ns5:getSec
urityGroupListResponse>]

للحصول على عرض أفضل لمحتوى xml من ذلك السجل يمكن نسخه إلى ملف xml وفتحه من خلال متصفح ويب. إنك تستطيع أن تتأكد من أن الرقيب المحدد (المدقق) قد تم إستلامه بنفس القدر الذي تلقاه كل الرقيب الآخر المعرف بالرقيب المدمج (ISE):



استعلام جلسة العمل عبر REST API إلى MnT

وهذا أيضا جزء من عملية الاختبار (الرجاء ملاحظة تمرير اسم مضيف ومنفذ MnT عبر pxGrid). يتم إستخدام تنزيل جلسة العمل المجمعة:

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK, p_node*:0x7f0ea6ffa8a8(<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E
6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name
```

```
xmlns='http://www.cisco.com/pxgrid'>Administrator</name><ADUserDNSDomain>example.com</ADUserDNSD
omain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfi
le>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>)]
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): bulk download invoking callback on entry# 1
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.ISESessionEntry [DEBUG]
adi.cpp:319:HandleLog(): parsing Session Entry with following text:<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E
6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name
xmlns='http://www.cisco.com/pxgrid'>Administrator</name><ADUserDNSDomain>example.com</ADUserDNSD
omain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfi
le>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>
```

والنتيجة التي تم تحليلها (تم إستالم جلسة عمل نشطة واحدة):

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.ISESessionEntry [DEBUG]
adi.cpp:319:HandleLog(): Parsing incoming DOM resulted in following ISESessionEntry:
{gid = ac101f6400007000565d597f, timestamp = 2015-12-01T23:37:31.191+01:00,
state = Started, session_id = 91200007, nas_ip = 172.16.31.100,
mac_addr = 08:00:27:23:E6:F2, ip = 172.16.50.50, user_name = Administrator,
sgt = Auditors, domain = example.com, device_name = Windows7-Workstation}
```

في تلك المرحلة، يحاول NGIPS ربط اسم المستخدم (والمجال) باسم مستخدم Realm-AD:

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.RealmContainer [DEBUG] adi.cpp:319
:HandleLog(): findRealm: Found Realm for domain example.com
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.ISEConnectionSub [DEBUG]
adi.cpp:319:HandleLog(): userName = 'Administrator' realmId = 2, ipAddress = 172.16.50.50
```

يتم إستخدام LDAP للعثور على عضوية المستخدم والمجموعة:

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [INFO] adi.cpp:322:
HandleLog(): search '(|(sAMAccountName=Administrator))' has the following
DN: 'CN=Administrator,CN=Users,DC=example,DC=com'.
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [DEBUG] adi.cpp:319:
HandleLog(): getUserIdentifier: searchfield sAMAccountName has display naming attr:
Administrator.
```

تصحيح أخطاء ISE

بعد تمكين تصحيح أخطاء مستوى التتبع لمكونات pxGrid، من الممكن التحقق من كل عملية (ولكن بدون حمولة/بيانات مثل FMC).

مثال مع إستعادة عالمة رقيب:

```
2015-12-02 00:05:39,352 DEBUG  [pool-1-thread-14][]
cisco.pxgrid.controller.query.CoreAuthorizationManager -::
:::- checking core authorization (topic=TrustSecMetaData, user=firesightisetest-
firepower.example.com
-0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com, operation=subscribe)...
```

```
2015-12-02 00:05:39,358 TRACE  [pool-1-thread-14][] cisco.pxgrid.controller.common.
LogAdvice -:::::- args: [TrustSecMetaData, subscribe, firesightisetest-firepower.example.com-
0739edea820cc77e04cc7c44200f661e@xg
rid.cisco.com]
2015-12-02 00:05:39,359 DEBUG  [pool-1-thread-14][] cisco.pxgrid.controller.persistence.
XgridDaoImpl -:::::-  groups [Any, Session] found for client firesightisetest-firepower.
example.com-0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com
2015-12-02 00:05:39,360 DEBUG  [pool-1-thread-14][] cisco.pxgrid.controller.persistence.
XgridDaoImpl -:::::- permitted rule found for Session TrustSecMetaData subscribe.
total rules found 1
```

حشرات

CSCuv32295 - يجوز أن يرسل ISE معلومات المجال في حقول اسم المستخدم

CSCus53796 - يتعذر الحصول على FQDN الخاص بالمضيف لاستعلام REST المجمع

CSCuv43145 - إعادة تشغيل خدمة PXGRID وتخطي الهوية، إستيراد/حذف مخزن الثقة

المراجع

- تكوين خدمات الإصلاح باستخدام تكامل ISE و FirePOWER
- تكوين pxGrid في بيئة ISE الموزعة
- كيفية نشر الشهادات باستخدام Cisco PXgrid: تكوين عقدة ISE PXgrid الموقعة من CA وعميل CA-Signed PXgrid
- تكامل ISE الإصدار 1.3 PXgrid مع تطبيق IPS PXlog
- دليل مسؤول محرك خدمات الهوية من Cisco، إصدار 2.0
- دليل مرجع واجهة برمجة التطبيقات (API) لمحرك خدمات الهوية من Cisco، الإصدار 1.2 - مقدمة إلى RESTful S الخارجي...
- الدليل المرجعي لواجهة برمجة التطبيقات (API) لمحرك خدمات الهوية من Cisco، الإصدار 1.2 - مقدمة إلى Monitoring RES...
- دليل مسؤول محرك خدمات الهوية من Cisco، الإصدار 1.3
- دعم & توثيق - سيسكو سيستمز

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).