IPS قيبطت عم PXgrid 1.3 رادصإلا ISE لماكت PXlog

المحتويات

المقدمة

يدعم ISE (Identity Services Engine) الإصدار 1.3 واجهة برمجة تطبيقات (API) جديدة تسمى PxGrid. يتيح هذا البروتوكول العصري والمرن الذي يدعم المصادقة والتشفير والامتيازات (المجموعات) إمكانية الدمج بسهولة مع حلول الأمان الأخرى. يصف هذا المستند إستخدام تطبيق pxLog الذي تمت كتابته كدليل على المفهوم. يمكن ل PxLog تلقي رسائل syslog من نظام منع التسلل (IPS) وإرسال رسائل pxGrid إلى ISE من أجل عزل المهاجم. ونتيجة لذلك، يستخدم ISE تغيير تفويض RADIUS (CoA) لتغيير حالة التفويض لنقطة النهاية التي تحد من وصول الشبكة. يحدث كل هذا بشكل شفاف للمستخدم النهائي.

على سبيل المثال، تم إستخدام Snort ك IPS، ولكن يمكن إستخدام أي حل آخر. في الواقع، لا يجب أن يكون نظام منع الاختراق. كل ما هو مطلوب أن يرسل ال syslog رسالة إلى pxLog مع العنوان من المهاجم. وهذا يتيح إمكانية دمج عدد كبير من الحلول.

يقدم هذا المستند أيضا كيفية أستكشاف أخطاء حلول PXgrid وإصلاحها واختبارها، مع المشاكل والقيود النموذجية.

إخلاء المسؤولية: لا تدعم Cisco تطبيق pxLog. وقد كتبت هذه المادة كدليل على المفهوم. وكان الغرض الأساسي من ذلك هو إستخدامه أثناء تحسين تنفيذ PxGrid على ISE.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت خبرة مع cisco ise تشكيل ومعرفة الأساسية من هذا موضوع:

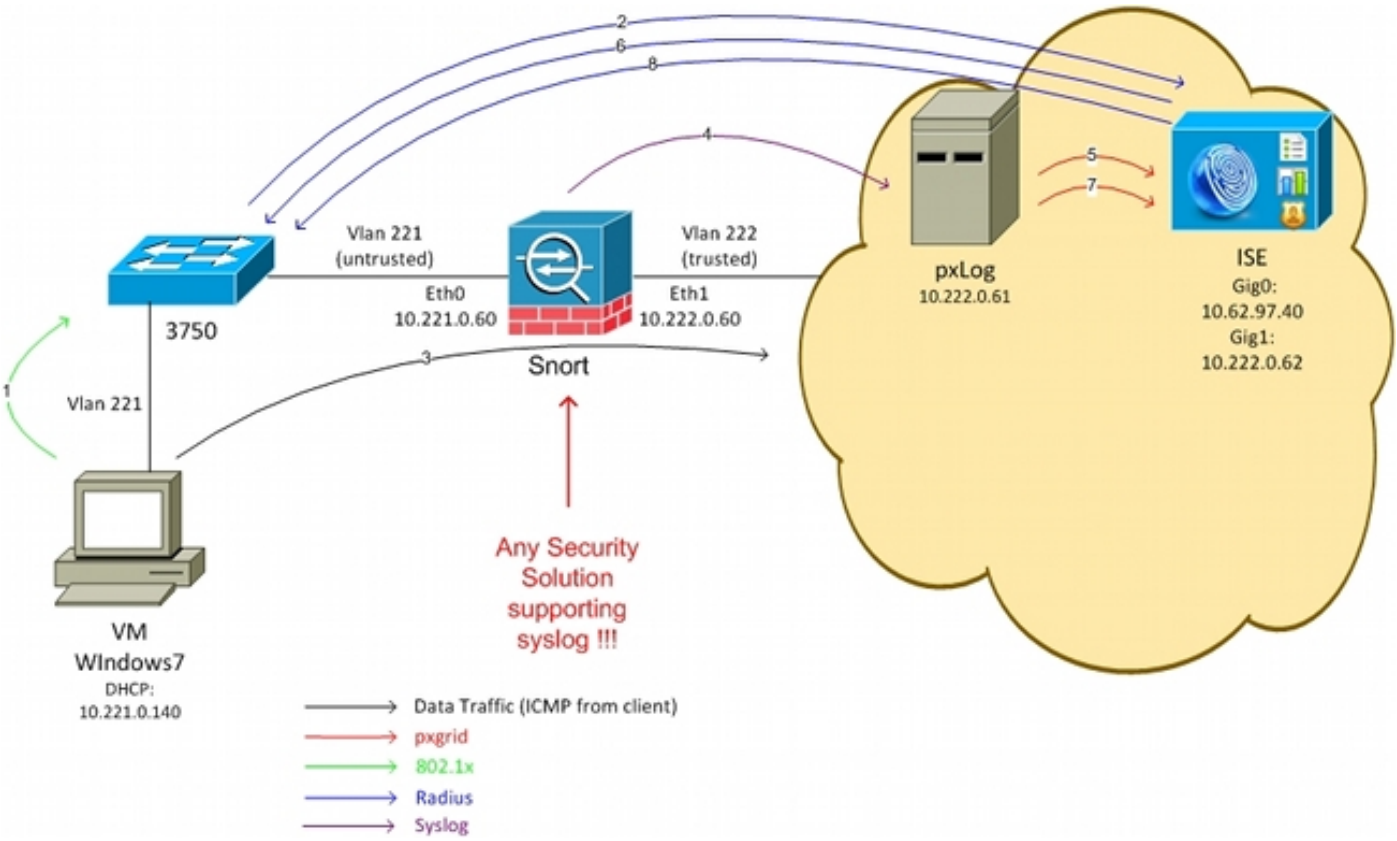
- عمليات نشر ISE وتكوين التفويض
- CLI تشكيل من cisco مادة حفازة مفتاح

المكونات المستخدمة

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

- نظام التشغيل Microsoft Windows 7
- برامج المحول Cisco Catalyst 3750X Series Switch، الإصدارات 15.0 والإصدارات الأحدث
- برنامج Cisco ISE، الإصدارات 1.3 والإصدارات الأحدث
- Cisco AnyConnect Mobile Security باستخدام مدير الوصول إلى الشبكة (NAM)، الإصدار 3.1 والإصدارات الأحدث
- SNORT الإصدار 2.9.6 مع الحصول على البيانات (DAQ)
- تم تثبيت تطبيق pxLog على Tomcat 7 باستخدام MySQL الإصدار 5

الرسم التخطيطي للشبكة وتدفق حركة مرور البيانات



وفيما يلي تدفق حركة المرور، كما هو موضح في الرسم التخطيطي للشبكة:

1. يتصل مستخدم Microsoft Windows 7 بالمحول ويقوم بتنفيذ مصادقة 802.1x.

2. يستخدم المحول ISE كخادم المصادقة والتفويض والمحاسبة (AAA). تمت مطابقة قاعدة تفويض **الوصول الكامل ل Dot1x** ويتم منح الوصول الكامل إلى الشبكة (DACL: PERMIT_ALL).

3. يحاول المستخدم الاتصال بالشبكة الموثوق بها ويخرق قاعدة الشخر.

4. ونتيجة لذلك، يرسل Snort تنبيها إلى تطبيق pxLog (عبر syslog).

5. يقوم تطبيق pxLog بإجراء التحقق مقابل قاعدة البيانات المحلية الخاصة به. يتم تكوينها من أجل التقاط رسائل syslog التي يتم إرسالها بواسطة Snort واستخراج عنوان IP الخاص بالمهاجم. ثم تستخدم pxGrid لإرسال طلب نحو ISE لحظر عنوان IP للمهاجم (ISE هو وحدة تحكم pxGrid).

6. يقوم ISE بإعادة تقييم سياسة التخويل الخاصة به. لأن نقطة النهاية تم عزلها، فإن **Session:EPSStatus يساوي** شرط **العزل** يتم استيفاء وملف تعريف تخويل مختلف (**Dot1x Quarantine**). يرسل ISE CoA Terminate إلى المحول لإنهاء الجلسة. هذا يؤدي إلى تشغيل إعادة المصادقة ويتم تطبيق قائمة تحكم في الوصول (DACL) جديدة قابلة للتنزيل (PERMIT_ICMP)، والتي توفر وصول الشبكة المحدود إلى المستخدم النهائي.

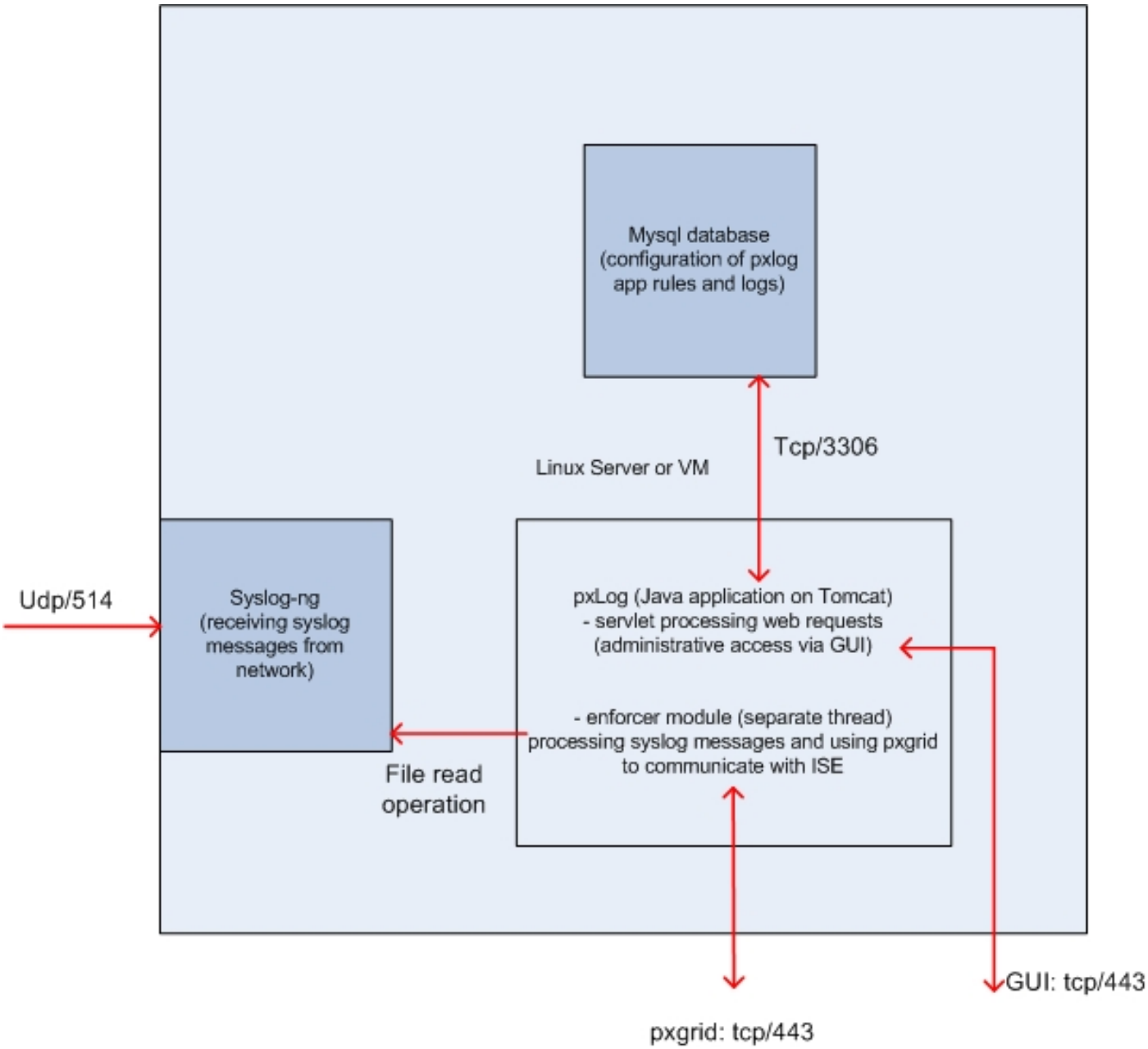
7. في هذه المرحلة، قد يقرر المسؤول إلغاء عزل نقطة النهاية. ويمكن تحقيق ذلك عبر واجهة المستخدم الرسومية (GUI) الخاصة ب pxLog. مرة أخرى، يتم إرسال رسالة pxGrid باتجاه ISE.

8. تقوم ISE بعملية مماثلة في الخطوة 6. هذه المرة، لم تعد نقطة النهاية خاضعة للحجر الصحي ويتم توفير

الوصول الكامل.

pxLog

عمارة



الحل هو تثبيت مجموعة من التطبيقات على جهاز لينوكس:

1. تم كتابة تطبيق pxLog في Java ونشره على خادم Tomcat. يتألف هذا التطبيق من:

الخادم الذي يعالج طلبات الويب - يتم إستخدام هذا للوصول إلى اللوحة الإدارية عبر مستعرض الويب.

Enforcement Module - مؤشر الترابط الذي يتم بدؤه مع الخادم. يقرأ Enforcement رسائل syslog من الملف (محسن)، ويعالج تلك الرسائل وفقا للقواعد التي تم تكوينها، ويقوم بتنفيذ الإجراءات (مثل إجراء الفحص عبر pxGrid).

2. قاعدة بيانات MySQL التي تحتوي على تكوين pxLog (القواعد والسجلات).

3. خادم syslog الذي يستقبل رسائل syslog من أنظمة خارجية ويكتبها إلى ملف.

التثبيت

يستخدم تطبيق pxLog هذه المكتبات:

- jQuery (لدعم AJAX)
- مكتبة علامات تمييز صفحات خادم JSTL) JavaServer) (نموذج وحدة تحكم عرض النموذج (MVC)، البيانات يتم فصلها عن المنطق: تستخدم شفرة صفحة خادم JSP) JavaServer) للتجسيد فقط، بدون شفرة HTML في فئات Java)
- LOG4j كنظام فرعي للتسجيل
- موصل MySQL
- DisplayTag لجداول العرض/الفرز
- PxGrid API بواسطة Cisco (حاليا الإصدار ألفا 147)

جميع هذه المكتبات موجودة بالفعل في دليل الملف البرمجي للمشروع لذلك لا حاجة لتنزيل المزيد من ملفات Java ArChive (JAR).

لتثبيت التطبيق:

1. قم بإلغاء حزمة الدليل بالكامل إلى دليل Tomcat WebApp.

2. قم بتحرير ملف **WEB-INF/web.xml**. التغيير الوحيد المطلوب هو متغير **Serverify**، والذي يجب أن يشير إلى ISE. أيضا قد يتم إنشاء KeyStores لشهادات جافا (واحد للهوية الموثوق بها والآخر للهوية) (بدلا من الافتراضي). يتم إستخدام هذا بواسطة واجهة برمجة تطبيقات PxGrid التي تستخدم جلسة عمل طبقة مآخذ التوصيل الآمنة (SSL) مع كل من شهادات العميل والخادم. يتعين على كلا جانبي الاتصال تقديم الشهادة مع بعضهما البعض، كما يتعين عليهما الثقة في بعضهما البعض. أحلت ال pxGrid بروتوكول متطلب قسم ل كثير معلومة.

3. تأكد من أن اسم مضيف ISE تم حله بشكل صحيح على pxLog (راجع السجل في خادم اسم المجال (DNS) أو **/وما إلى ذلك/إدخال الأجهزة المضيفة**). أحلت ال pxGrid بروتوكول متطلب قسم ل كثير معلومة.

4. قم بتكوين قاعدة بيانات MySQL باستخدام البرنامج النصي **mysql/init.sql**. يمكن تغيير بيانات الاعتماد ولكن يجب أن تنعكس في الملف **WEB-INF/web.xml**.

شخير

لا تركز هذه المقالة على أي عناوين IPS محددة، ولهذا السبب لا يقدم سوى شرح موجز.

تم تكوين SNORT على أنه مضمن مع دعم DAQ. تتم إعادة توجيه حركة المرور باستخدام الجداول:

```
iptables -I FORWARD -j ACCEPT
iptables -I FORWARD -j NFQUEUE --queue-num 1
```

ثم بعد الفحص، يتم حقنه وإعادة توجيهه وفقا لقواعد جدول البيانات الافتراضية.

تم تكوين عدد قليل من قواعد المسامير المخصصة (يتم تضمين ملف **/etc/snort/rules/test.rules** في التكوين العام).

```
(alert icmp any any -> any any (itype:8; dsize:666<>686; sid:100122
(alert icmp any any -> any any (itype:8; ttl: 6; sid:100124
```

يرسل snort رسالة syslog عندما يكون وقت البقاء (TTL) من الحزمة يساوي 6 أو حجم الحمولة بين 666 و 686. لم يتم حظر حركة المرور من قبل شركة snort.

كما يجب إعداد الحدود للتأكد من عدم تشغيل التنبيهات بشكل متكرر (**/etc/snort/threshold.conf**):

```
event_filter gen_id 1, sig_id 100122, type limit, track by_src, count 1, seconds 60
event_filter gen_id 1, sig_id 100124, type limit, track by_src, count 1, seconds 60
```

ثم يشير خادم syslog إلى جهاز **/etc/snort/snort.conf**) pxLog):

```
output alert_syslog: host=10.222.0.61:514, LOG_AUTH LOG_ALER
```

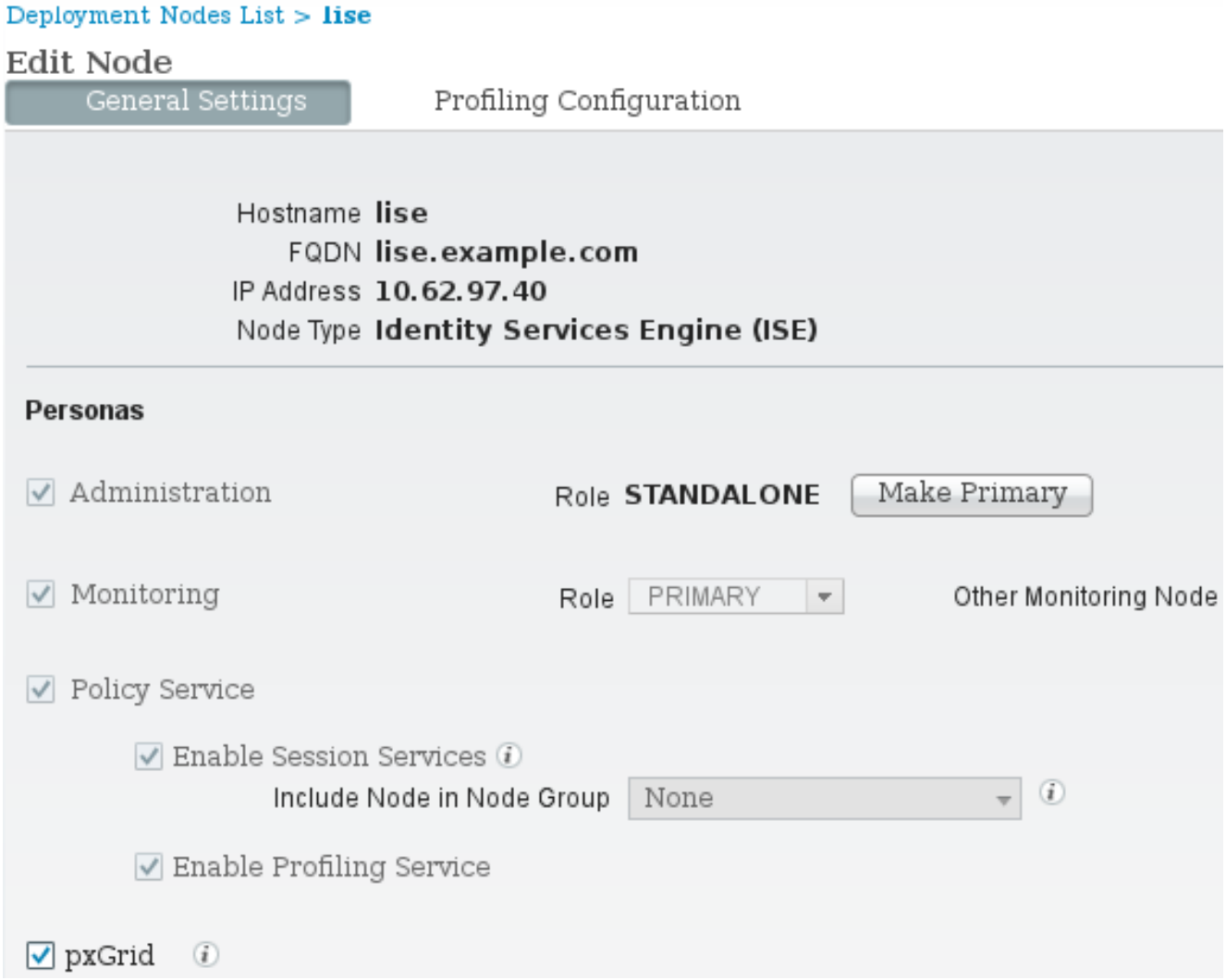
بالنسبة لبعض الإصدارات من snort، هناك أخطاء مرتبطة بتكوين syslog، ومن ثم يمكن إستخدام الإعدادات الافتراضية التي تشير إلى المضيف المحلي ويمكن تكوين syslog-ng لإعادة توجيه رسائل معينة إلى مضيف pxLog.

محرك خدمات كشف الهوية (ISE)

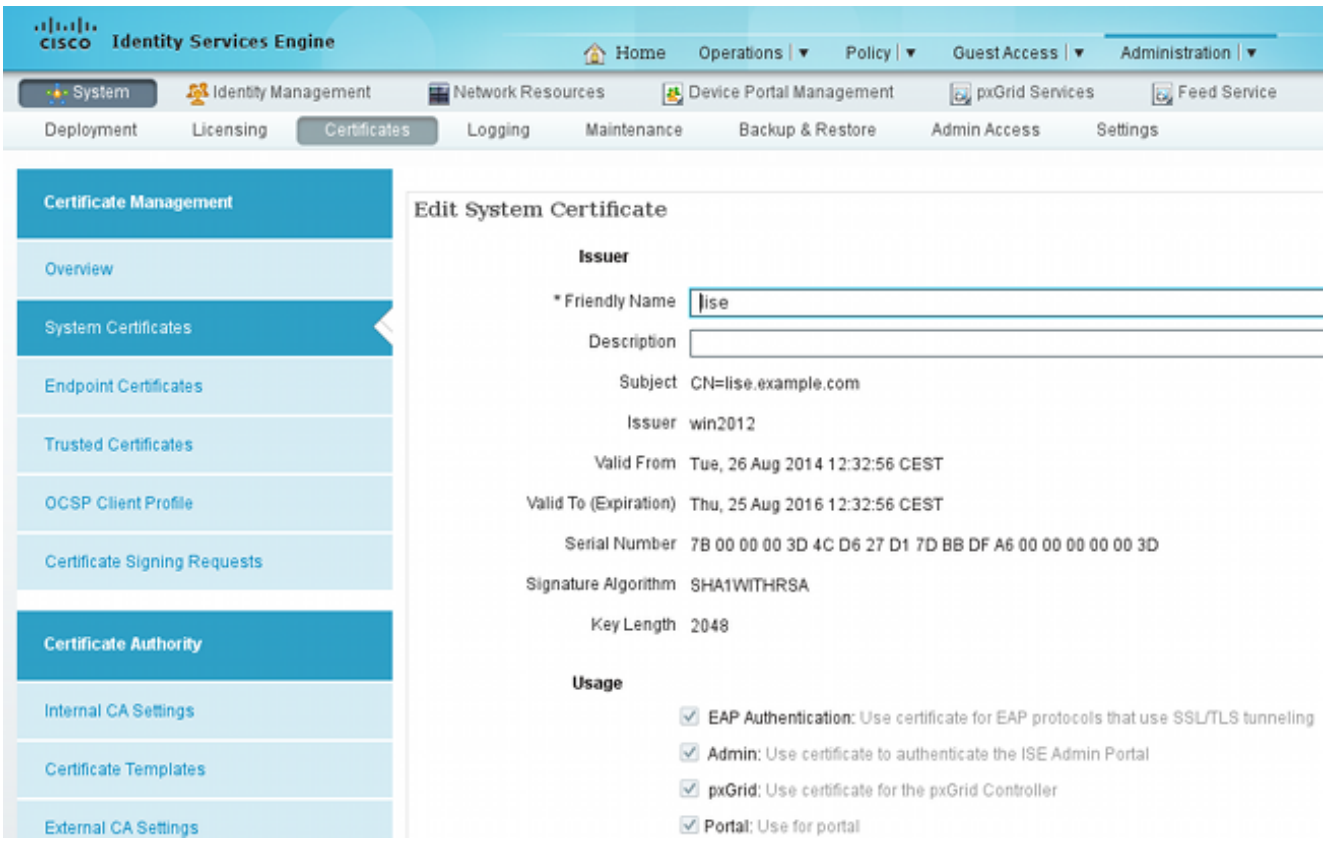
التكوين

الشخصية والشهادة

1. مكنت ال pxGrid دور، أي يكون معأق على ال ISE افتراضيا، تحت **إدارة > نشر**:

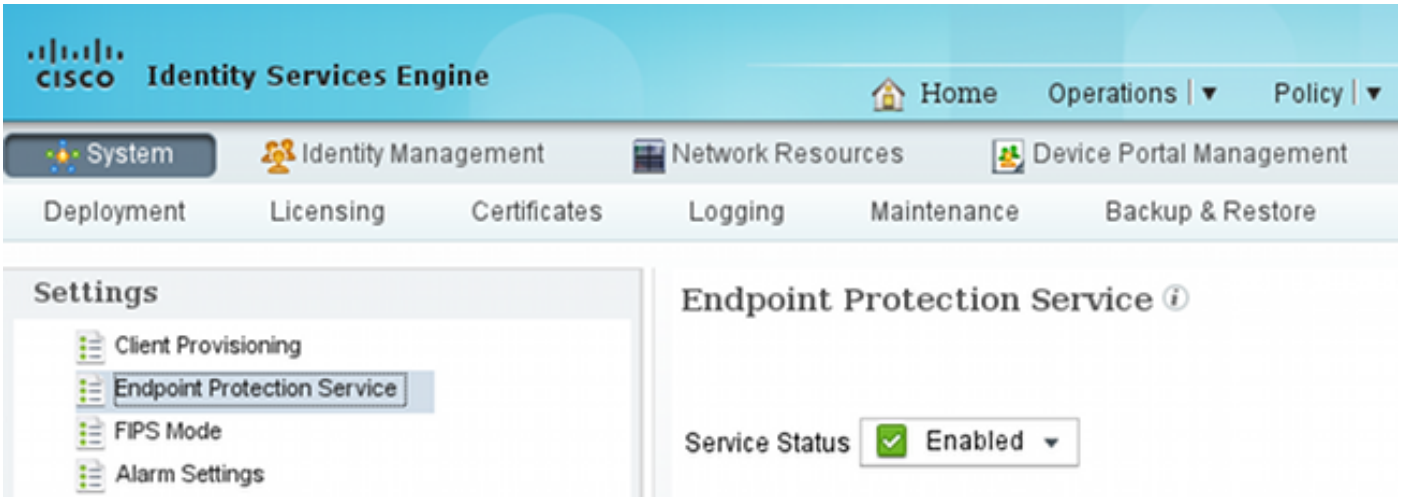


2. دققت إن يكون الشهادات استعملت ل pxGrid تحت **إدارة > شهادات > نظام شهادات**:



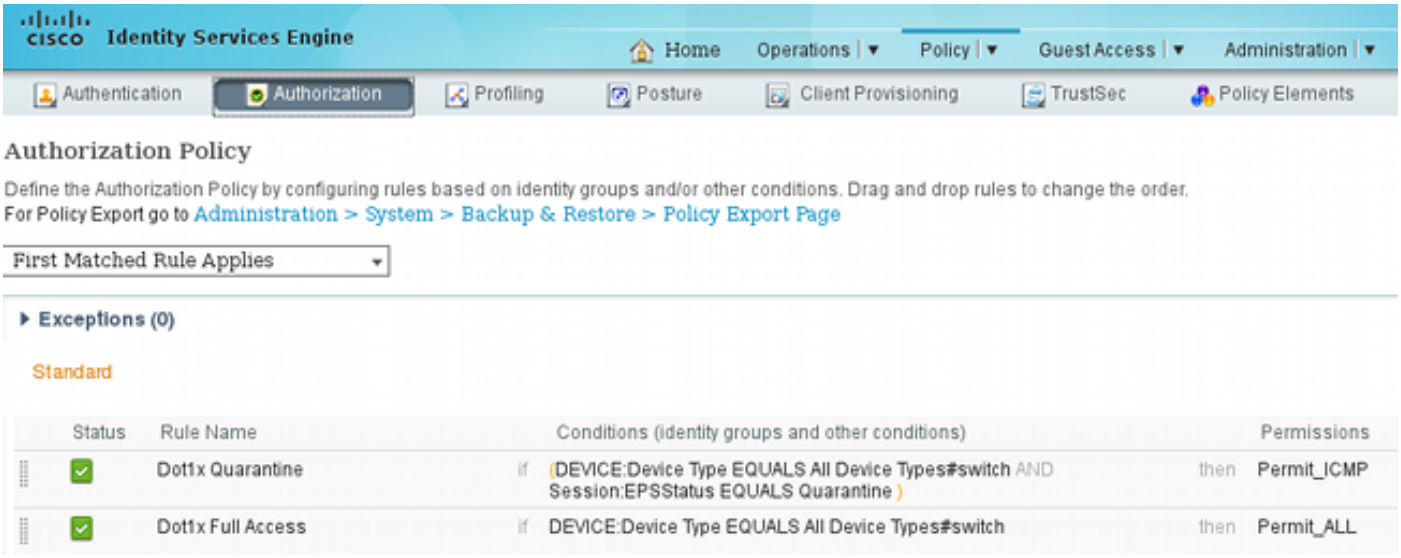
خدمة حماية نقطة النهاية (EPS)

يجب تمكين EPS (معطل بشكل افتراضي) من **الإدارة > الإعدادات**:



يتيح لك هذا إستخدام وظيفة العزل/إلغاء العزل.

قواعد التخويل



يتم مصادقة القاعدة الأولى فقط عند عزل نقطة النهاية. ثم يتم فرض الوصول المحدود ديناميكيا بواسطة RADIUS CoA. كما يجب إضافة المحول إلى أجهزة الشبكة باستخدام السر المشترك الصحيح.

استكشاف الأخطاء وإصلاحها

يمكن التحقق من حالة PxGrid باستخدام CLI:

```
lise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          6717
Database Server                        running          51 PROCESSES
```

```
 Application Server                    running          9486
 Profiler Database                     running          7804
AD Connector                          running         10058
 M&T Session Database                  running          7718
 M&T Log Collector                     running          9752
 M&T Log Processor                     running          9712
 Certificate Authority Service         running          9663
pxGrid Infrastructure Service         running         14979
pxGrid Publisher Subscriber Service   running         15281
pxGrid Connection Manager             running         15248
pxGrid Controller                     running         15089
 Identity Mapping Service              running          9962
```

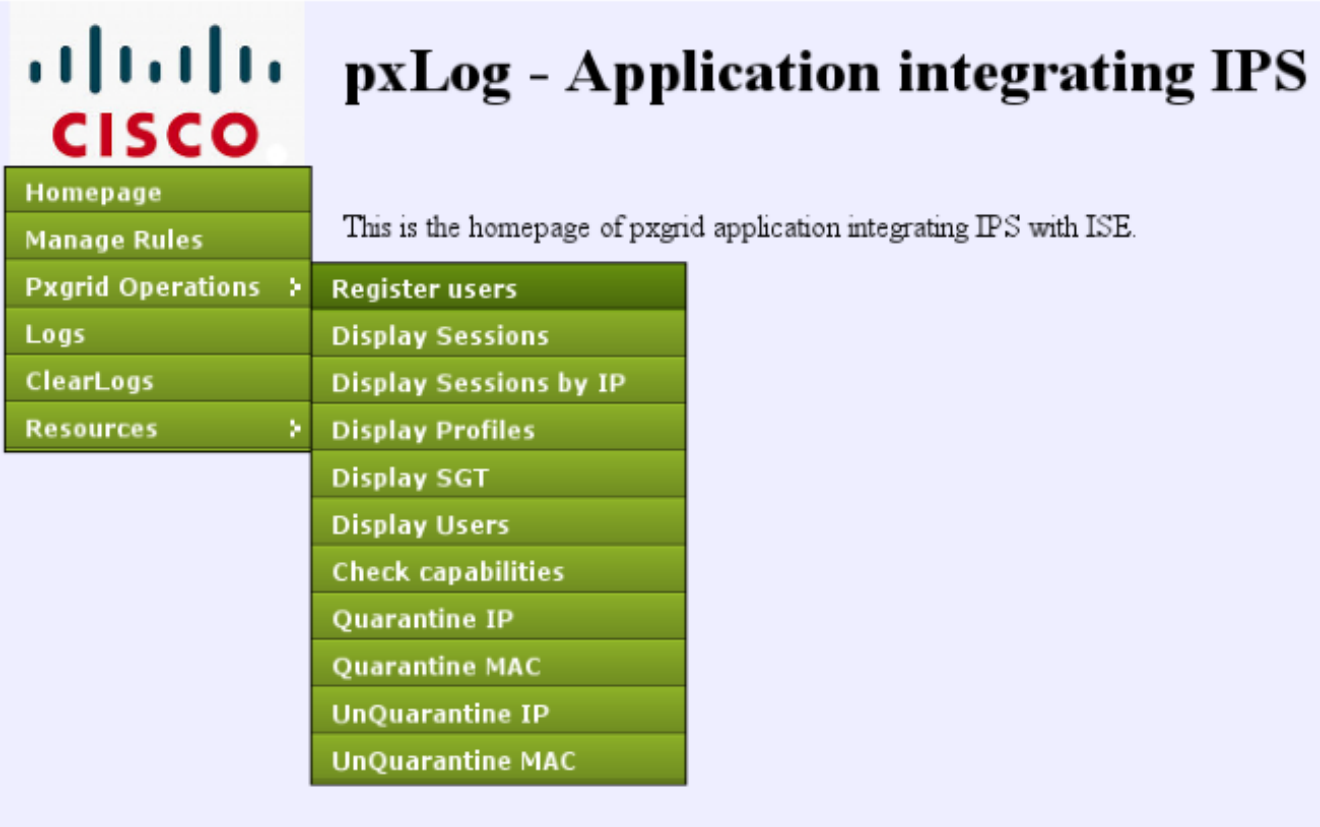
هناك أيضا تصحيح أخطاء منفصل ل pxGrid (**إدارة > تسجيل > تكوين سجل تصحيح الأخطاء > pxGrid**). يتم تخزين ملفات تصحيح الأخطاء في دليل pxGrid. أهم البيانات هي في **pxgrid/pxgrid-jabberd.log** و**pxgrid/pxgrid-controller.log**.

إختبار

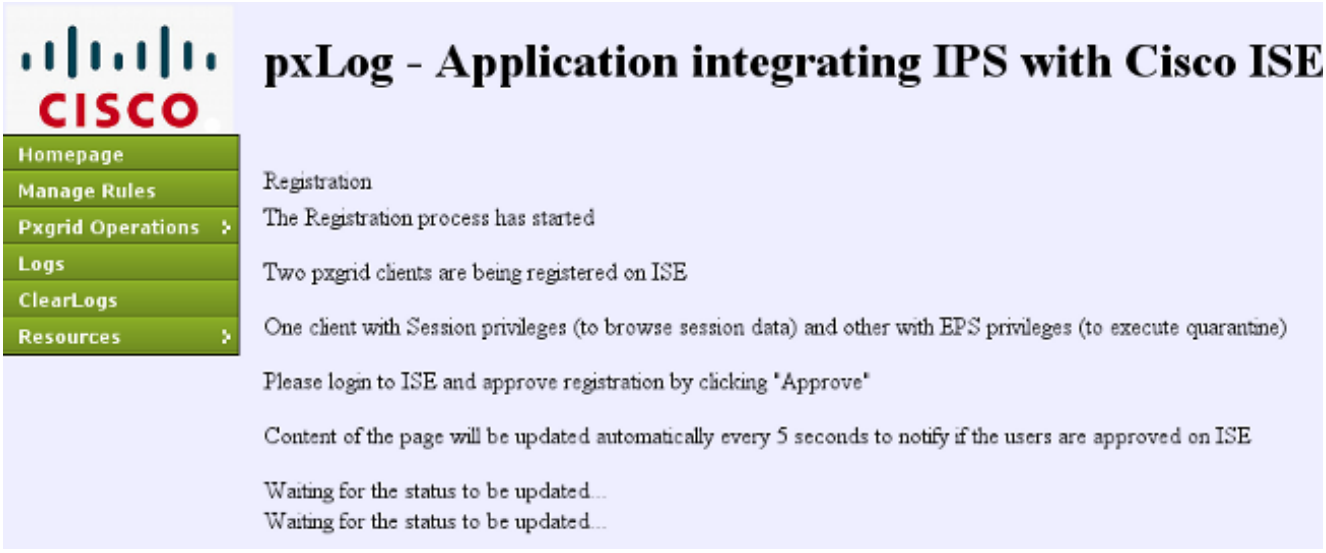
الخطوة 1. التسجيل ل pxGrid

يتم نشر تطبيق pxLog تلقائيا عند بدء تشغيل Tomcat.

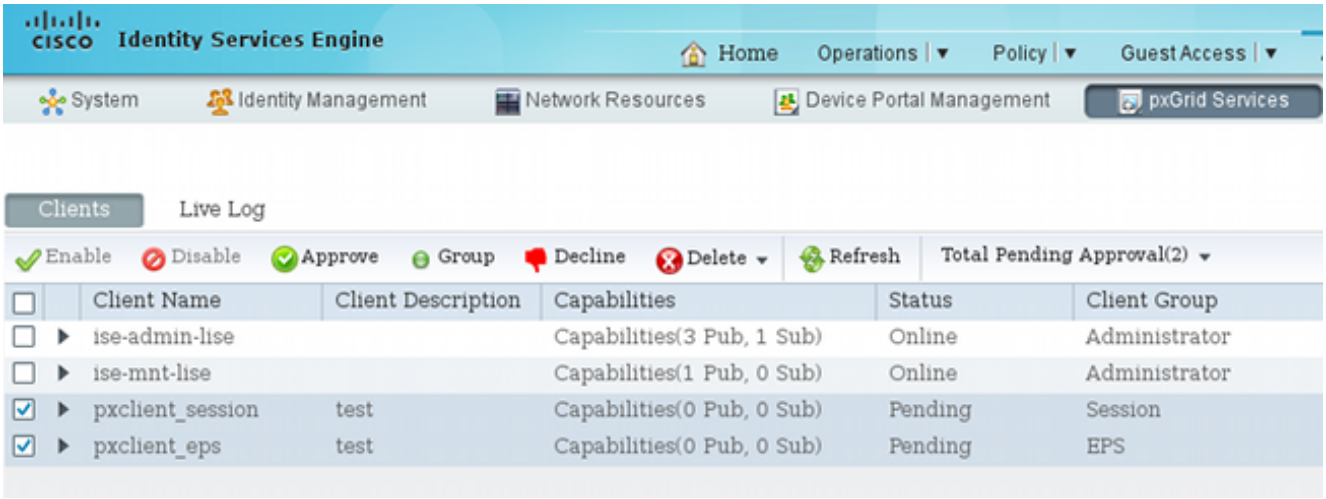
لاستخدام pxGrid، قم بتسجيل إثنين من المستخدمين في ISE (واحد مع الوصول إلى جلسة العمل، وواحد مع العزل). يمكن إكمال ذلك من **عمليات PxGrid > تسجيل المستخدمين**:



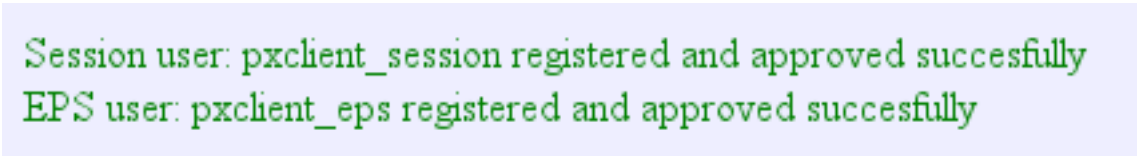
يبدأ التسجيل تلقائيا:



2. في هذه المرحلة، من الضروري الموافقة على المستخدمين المسجلين على ISE (يتم تعطيل الموافقة التلقائية بشكل افتراضي):



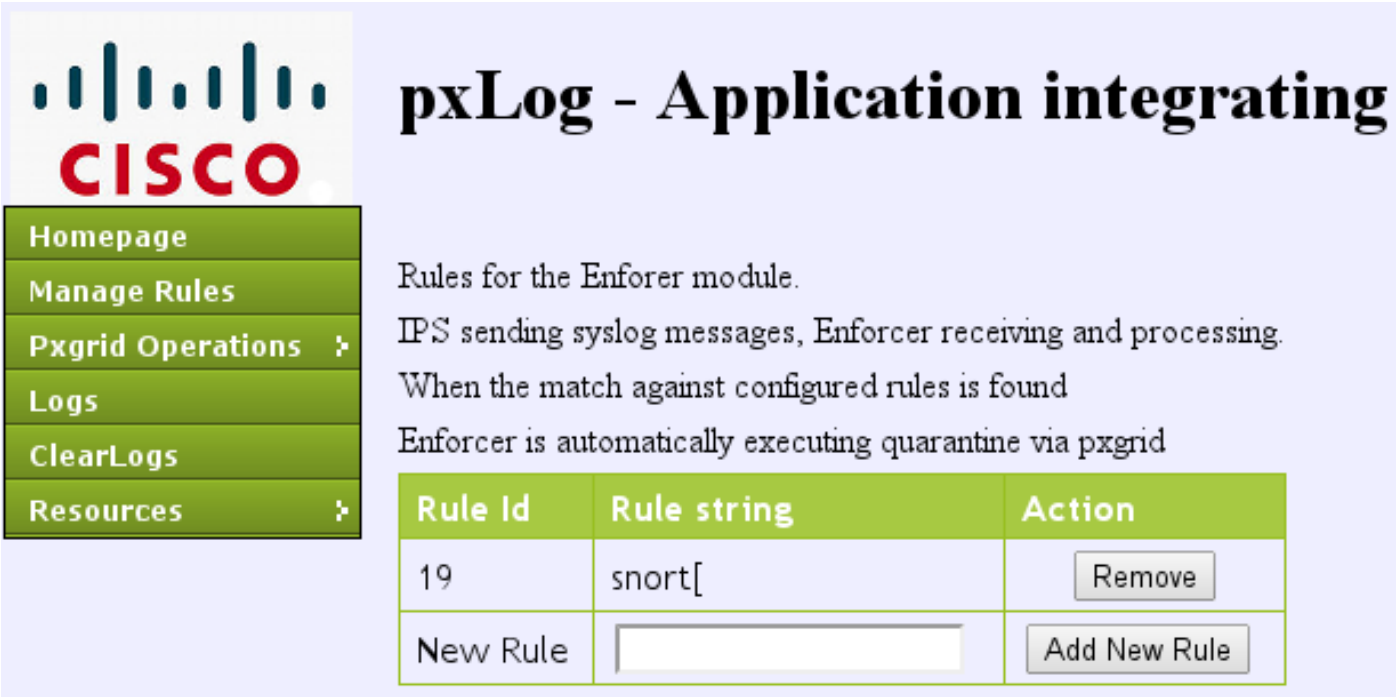
بعد الاعتماد، يقوم PxLog تلقائيا بإعلام المسؤول (عبر اتصال AJAX):



يعرض ISE حالة هذين المستخدمين ك Online أو Offline (غير معلق بعد الآن).

الخطوة 2. تكوين قواعد pxLog

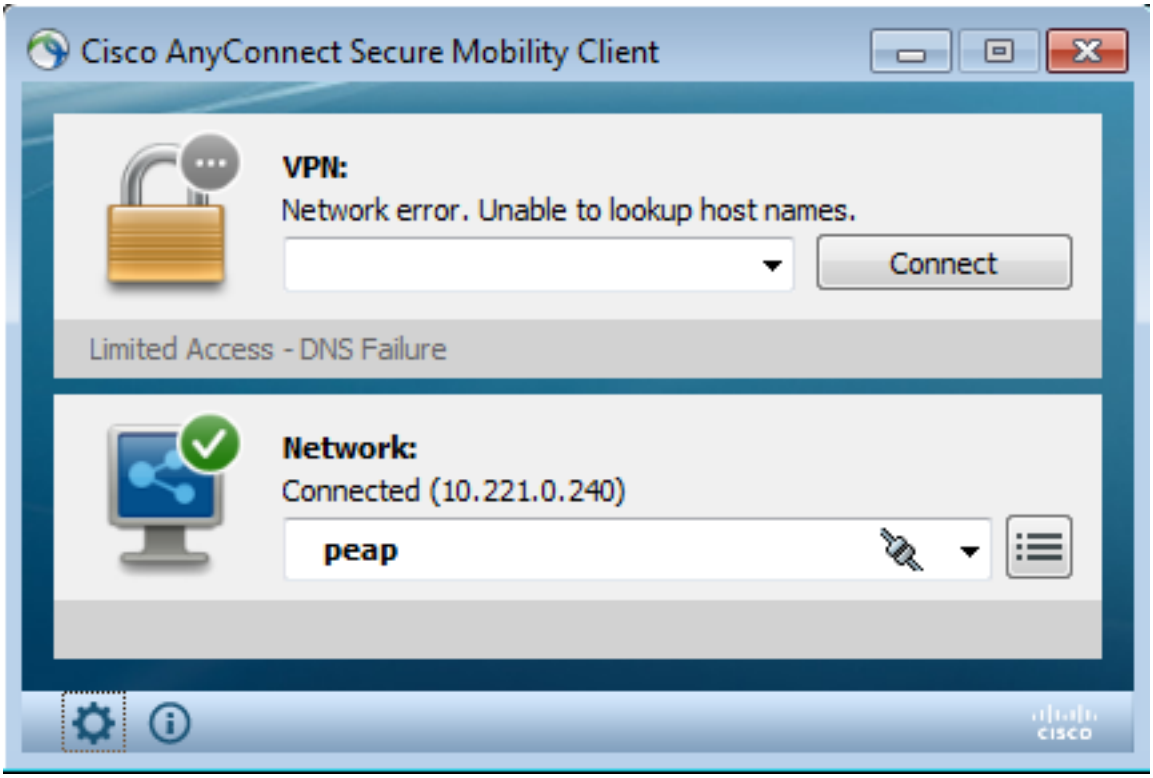
يجب أن يقوم pxLog بمعالجة رسائل syslog وتنفيذ الإجراءات المستندة إليه. لإضافة قاعدة جديدة، حدد **قواعد الإدارة**:



الآن تبحث وحدة الإنفاذ عن هذا التعبير العادي (RegExp) في رسالة syslog: "snort["]. إذا تم العثور عليه، فإنه يبحث في جميع عناوين IP ويحدد العنوان السابق له. وهذا يطابق معظم حلول التأمين. راجع قسم syslog للحصول على مزيد من المعلومات. يتم عزل عنوان IP (المهاجم) عبر PXgrid. كما يمكن إستخدام قاعدة أكثر دقة (على سبيل المثال، قد تتضمن رقم التوقيع).

الخطوة الثالثة. First Dot1x جلسة

تقوم محطة Microsoft Windows 7 بتهيئة جلسة عمل Dot1x سلكية. تم إستخدام AnyConnect NAM من Cisco كطالب. تم تكوين أسلوب EAP المحمي ببروتوكول المصادقة المتوسع (EAP-PEAP).



تم تحديد ملف تعريف تخويل **Dot1x Full Access** ISE. يقوم المحول بتنزيل قائمة الوصول لمنح الوصول الكامل:

```
3750#show authentication sessions interface g0/17
       Interface:  GigabitEthernet0/17
          MAC Address:  0050.b611.ed31
            IP Address:  10.221.0.240
                User-Name:  cisco
              Status:  Authz Success
                Domain:  DATA
              Security Policy:  Should Secure
                  Security Status:  Unsecure
             Oper host mode:  single-host
                Oper control dir:  both
        Authorized By:  Authentication Server
                 Vlan Policy:  N/A
ACS ACL:  xACSACLx-IP-PERMIT_ALL-53fc9dbe
                 Session timeout:  N/A
                 Idle timeout:  N/A
      Common Session ID:  0A01000C000037E6BAB267CF
                Acct Session ID:  0x00003A70
                Handle:  0xA100080E

                    :Runnable methods list
                      Method   State
                dot1x    Authc Success

3750#show ip access-lists interface g0/17
                     permit ip any any
```

الخطوة 4. يرسل Microsoft Windows PC الحزمة التي تشغل التنبيه

وهذا يوضح ما يحدث إذا قمت بالإرسال من حزمة Microsoft Windows مع TTL = 7:

```
c:\> ping 10.222.0.61 -i 7 -n 1
```

ويتم تقليل هذه القيمة عند الشخير في سلسلة إعادة التوجيه ويتم رفع تنبيه. ونتيجة لذلك، يتم إرسال رسالة syslog نحو pxLog:

```
<- Sep  6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240
10.222.0.61
```

الخطوة 5. pxLog

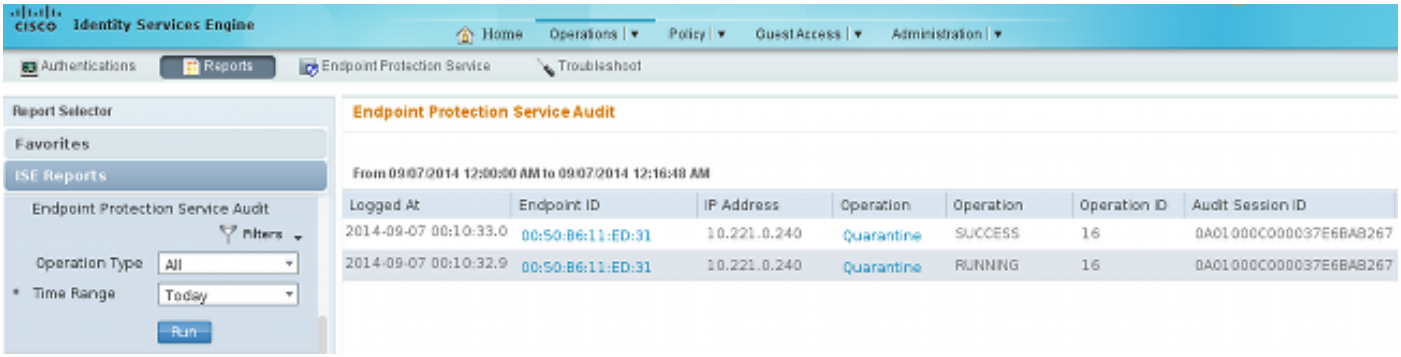
يستقبل pxLog رسالة syslog، ويعالجها، ويطلب إجراء عزل لعنوان IP هذا. يمكن تأكيد ذلك إذا قمت بفحص السجلات:

Logs from the actions executed by the Enforer module

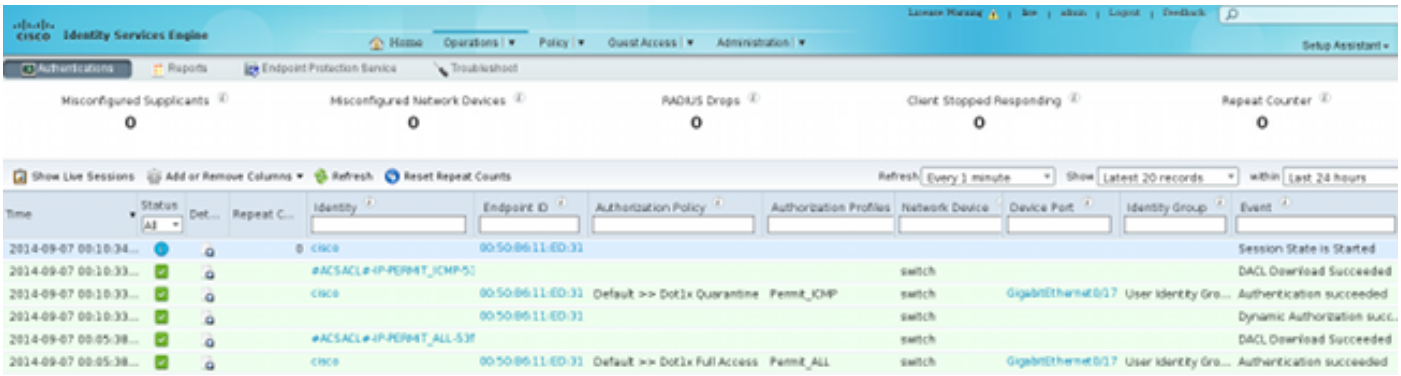
Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

الخطوة 6. عزل ISE

يقوم ISE بالإعلام عن عزل عنوان IP:



ونتيجة لذلك، فإنه يراجع سياسة التخويل، ويختار العزل، ويرسل RADIUS CoA لتحديث حالة التخويل على المحول لتلك النقطة الطرفية المحددة.



هذه هي رسالة CoA التي تجبر المتلقي على بدء جلسة جديدة والحصول على وصول محدود (Permit_ICMP):

No.	Source	Destination	Protocol	Length	Info
580	10.62.71.140	10.62.97.40	RADIUS	326	Accounting-Request(4) (id=157, l=284)
581	10.62.97.40	10.62.71.140	RADIUS	238	Access-Accept(2) (id=113, l=196)
582	10.62.97.40	10.62.71.140	RADIUS	62	Accounting-Response(5) (id=157, l=20)
2536	10.62.97.40	10.62.71.140	RADIUS	176	Disconnect-Request(40) (id=3, l=134)
2537	10.62.71.140	10.62.97.40	RADIUS	62	Disconnect-ACK(41) (id=3, l=20)
2538	10.62.71.140	10.62.97.40	RADIUS	394	Accounting-Request(4) (id=158, l=352)
2541	10.62.97.40	10.62.71.140	RADIUS	62	Accounting-Response(5) (id=158, l=20)
2545	10.62.71.140	10.62.97.40	RADIUS	272	Access-Request(1) (id=114, l=230)
2546	10.62.97.40	10.62.71.140	RADIUS	160	Access-Challenge(11) (id=114, l=118)

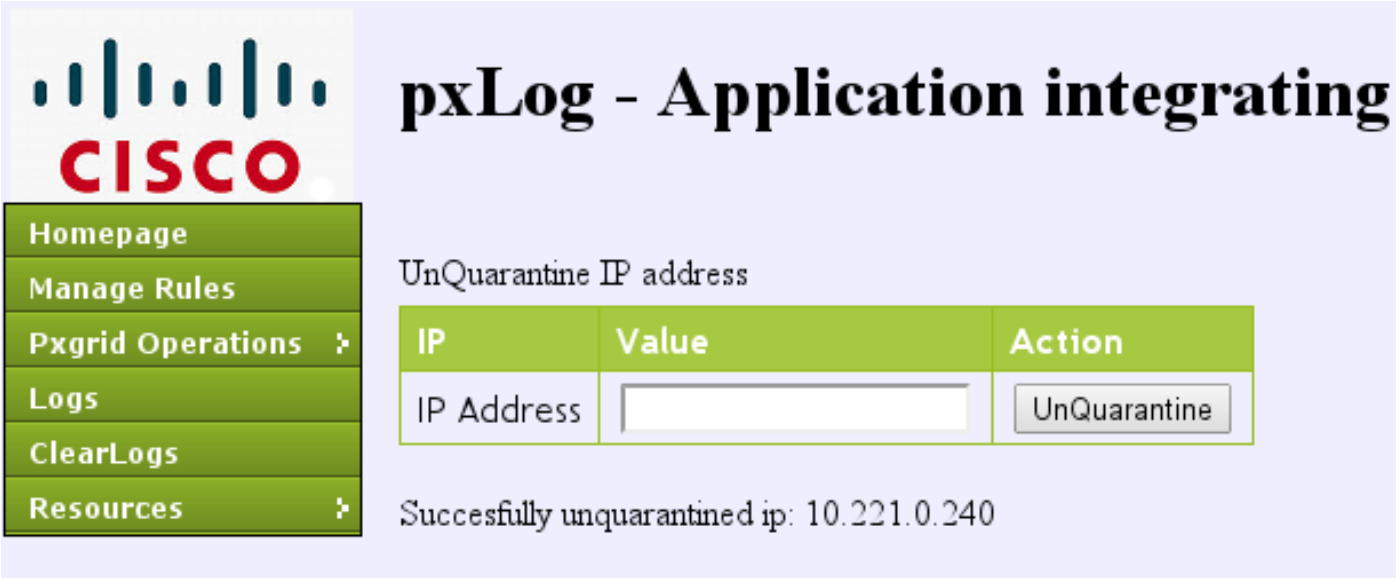
```
▸ Internet Protocol Version 4, Src: 10.62.97.40 (10.62.97.40), Dst: 10.62.71.140 (10.62.71.140)
▸ User Datagram Protocol, Src Port: 45006 (45006), Dst Port: mps-raft (1700)
▾ Radius Protocol
    Code: Disconnect-Request (40)
    Packet identifier: 0x3 (3)
    Length: 134
    Authenticator: 21ed5cda0eacbf87659a5e1dce9d0598
    [The response to this request is in frame 2537]
  ▾ Attribute Value Pairs
    ▸ AVP: l=6  t=NAS-IP-Address(4): 10.62.71.140
    ▸ AVP: l=19  t=Calling-Station-Id(31): 00:50:B6:11:ED:31
    ▸ AVP: l=10  t=Acct-Session-Id(44): 00003A6B
    ▸ AVP: l=6  t=Acct-Terminate-Cause(49): Admin-Reset(6)
    ▸ AVP: l=6  t=Event-Timestamp(55): Sep  7, 2014 00:00:00.000000000 CEST
    ▸ AVP: l=18  t=Message-Authenticator(80): 587cfbaf54769d84f092ffd233b96427
    ▸ AVP: l=49  t=Vendor-Specific(26) v=ciscoSystems(9)
```

يمكن تأكيد النتيجة على المحول (الوصول المحدود لنقطة النهاية):

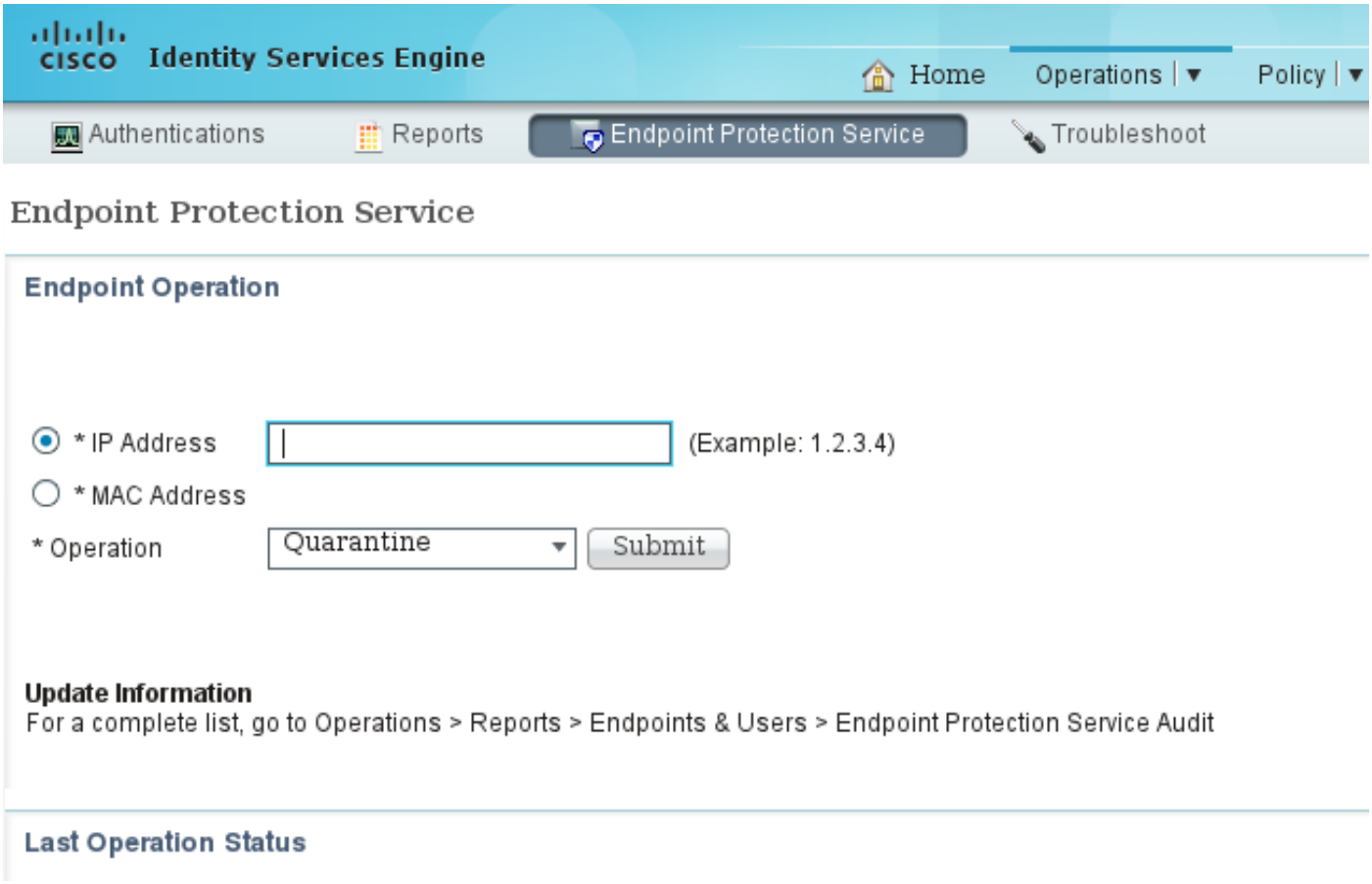
```
3750#show authentication sessions interface g0/17
       Interface:  GigabitEthernet0/17
     MAC Address:  0050.b611.ed31
      IP Address:  10.221.0.240
        User-Name:  cisco
          Status:  Authz Success
          Domain:  DATA
  Security Policy:  Should Secure
  Security Status:  Unsecure
  Oper host mode:  single-host
  Oper control dir:  both
  Authorized By:  Authentication Server
  Vlan Policy:  N/A
ACS ACL:  xACSACLx-IP-PERMIT_ICMP-53fc9dc5
  Session timeout:  N/A
  Idle timeout:  N/A
Common Session ID:  0A01000C000037E7BAB7D68C
  Acct Session ID:  0x00003A71
  Handle:  0xE000080F

:Runnable methods list
  Method   State
dot1x    Authc Success

3750#show ip access-lists interface g0/17
  permit icmp any any
```

الخطوة 7. إلغاء عزل PxLog

في هذه المرحلة، يقرر المسؤول إلغاء عزل نقطة النهاية هذه:

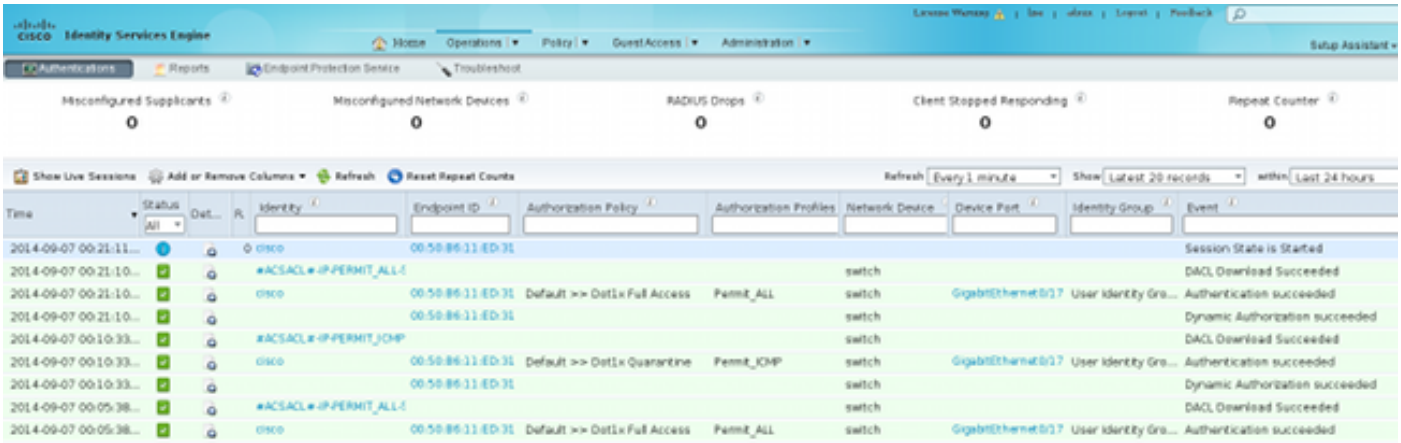


نفس العملية يستطيع كنت نفذت مباشرة من ال ISE:

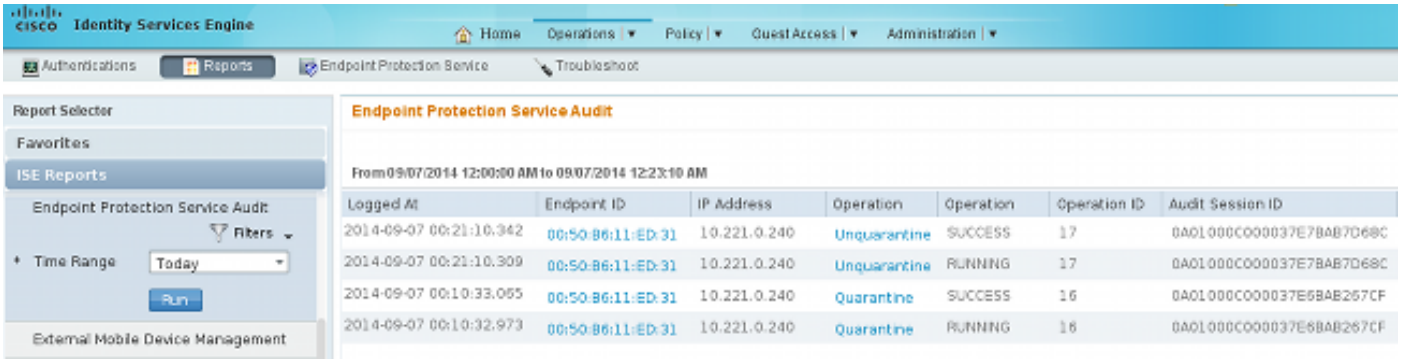


الخطوة 8. ISE Unquarantine

يقوم ISE مرة أخرى بمراجعة القواعد وتحديث حالة التفويض على المحول (يتم منح حق الوصول الكامل إلى الشبكة):



ويؤكد التقرير:



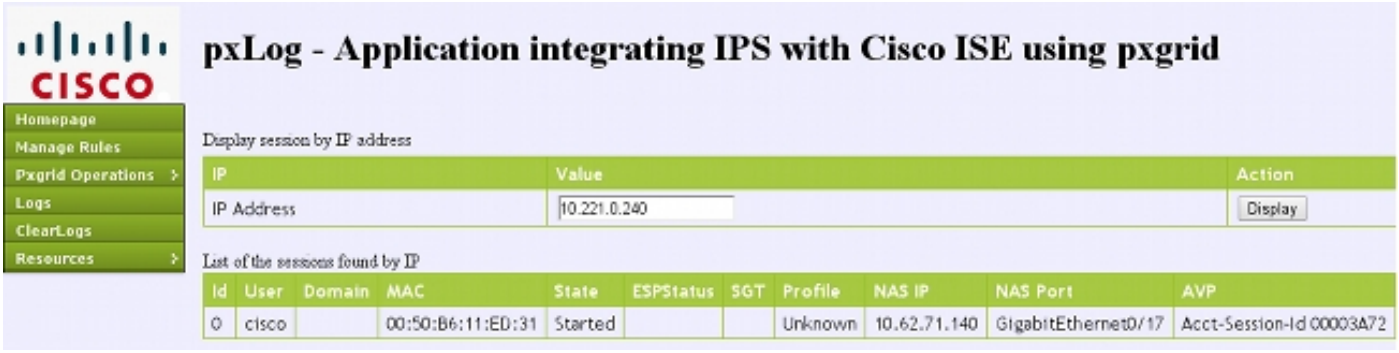
وظيفة pxLog

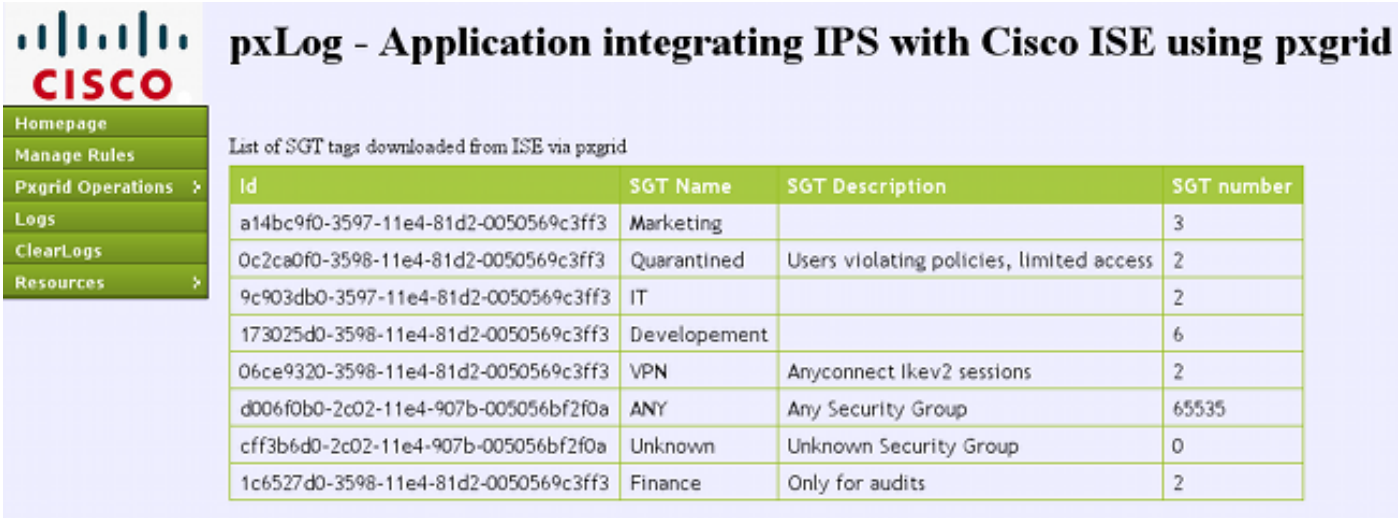
تمت كتابة تطبيق pxLog لتوضيح وظائف PxGrid API. فهي تسمح لك بما يلي:

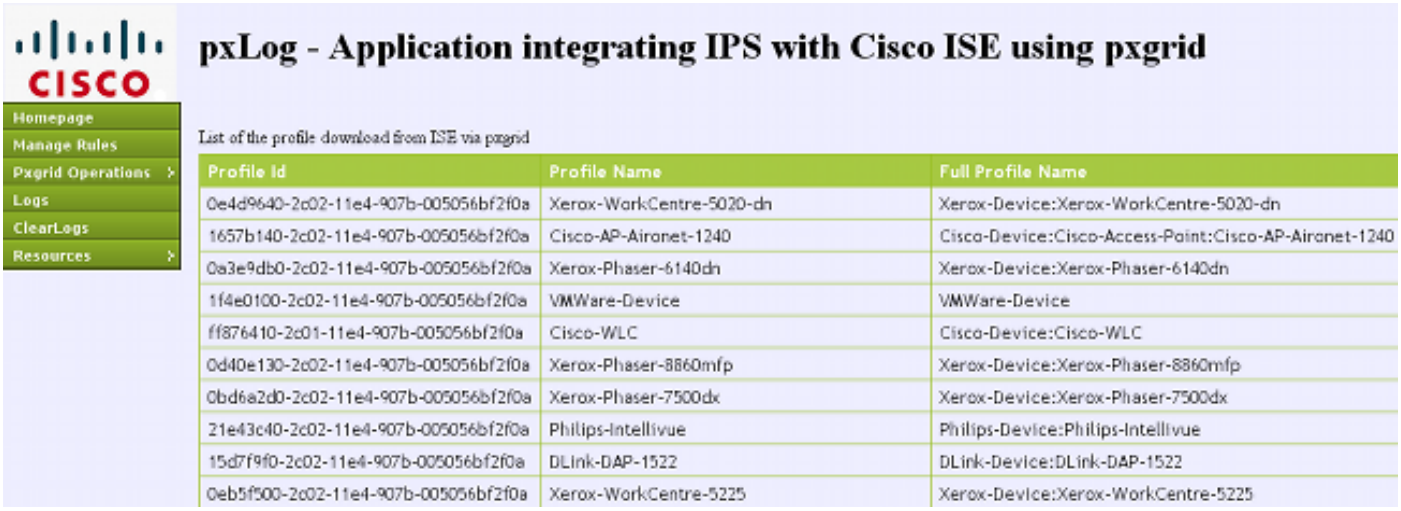
- تسجيل مستخدمي جلسة العمل و EPS على ISE
- تنزيل معلومات حول جميع جلسات العمل النشطة على ISE
- تنزيل معلومات حول جلسة عمل نشطة معينة على ISE (حسب عنوان IP)
- تنزيل معلومات حول مستخدم نشط محدد على ISE (حسب اسم المستخدم)
- عرض معلومات عن كل التوصيفات (منشئ ملفات التعريف)
- عرض معلومات حول علامات مجموعة أمان (SGTs TrustSec) المعرفة في ISE
- التحقق من الإصدار (إمكانيات pxGrid)
- إجراء عزل استنادا إلى عنوان IP أو MAC
- إلغاء العزل استنادا إلى عنوان IP أو MAC

تم التخطيط لمزيد من الوظائف في المستقبل.

فيما يلي بعض لقطات الشاشة من pxLog:







متطلبات بروتوكول pxGrid

مجموعات

يمكن أن يكون العميل (المستخدم) عضوا في مجموعة واحدة في كل مرة. والفئتان الأكثر إستخداما هما:

- جلسة العمل - تستخدم لاستعراض/تنزيل المعلومات المتعلقة بجلسات العمل/ملفات التعريف/الرقيب
- EPS - يستخدم لتنفيذ العزل

الشهادات ومفتاح Java

وكما ذكر سابقا، يجب أن يكون لدى كل من تطبيقات العميل، وحدة التحكم pxLog و ISE) pxGrid)، شهادات تم تكوينها للاتصال. يحتفظ تطبيق pxLog بتلك الموجودة في ملفات Java KeyStore:

- **store/client.jks** - يشمل شهادات العميل والمراجع (CA)
- **store/root.jks** - يتضمن سلسلة ISE: هوية عقدة المراقبة واستكشاف الأخطاء وإصلاحها (MNt) وشهادة CA

تتم حماية الملفات بكلمة مرور (الافتراضي: Cisco123). يمكن تغيير موقع الملف وكلمات المرور في **WEB-INF/web.xml**.

فيما يلي الخطوات لإنشاء مخزن مفاتيح جافا جديد:

1. لإنشاء مخزن مفاتيح جذر (موثوق به)، قم باستيراد شهادة **cert-ca.der**) CA يجب أن تكون بتنسيق DER):

```
pxgrid store # keytool -import -alias ca -keystore root.jks -file cert-ca.der
```

2. عندما تقوم بإنشاء مخزن مفاتيح جديد، أختر كلمة مرور، والتي يتم إستخدامها لاحقا للوصول إلى مخزن المفاتيح.

3. إستيراد شهادة هوية MnT إلى مخزن مفاتيح الجذر (**cert-mnt.der** هو شهادة الهوية المأخوذة من ISE ويجب أن تكون بتنسيق DER):

```
pxgrid store # keytool -import -alias mnt -keystore root.jks -file cert-mnt.der
```

4. لإنشاء مخزن مفاتيح العميل، قم باستيراد شهادة CA:

```
pxgrid store # keytool -import -alias ca -keystore client.jks -file cert-ca.der
```

5. إنشاء مفتاح خاص في مخزن مفاتيح العميل:

```
- pxgrid store # keytool -genkey -alias clientcert -keyalg RSA -keystore client.jks
keysize 2048
```

6. إنشاء طلب توقيع شهادة (CSR) في مخزن مفاتيح العميل:

```
- pxgrid store # keytool -certreq -alias clientcert -keystore client.jks
file cert-client.csr
```

7. وقع على **cert-client.csr** واستورد شهادة العميل الموقعة:

```
-pxgrid store # keytool -import -alias clientcert -keystore client.jks -file cert
```

```
client.der
```

8. تحقق من إحتواء كل من المفاتيح على الشهادات الصحيحة:

```
pxgrid store # keytool -list -v -keystore client.jks
pxgrid store # keytool -list -v -keystore root.jks
```

تحذير: عند ترقية عقدة ISE 1.3، هناك خيار للاحتفاظ بشهادة الهوية، لكن تتم إزالة توقيع CA. ونتيجة لذلك، يستخدم ISE الذي تمت ترقيته شهادة جديدة ولكنه لا يرفق شهادة CA أبدا في رسالة SSL/ServerHello. وهذا يؤدي إلى تشغيل الفشل على العميل الذي يتوقع (وفقا ل RFC) رؤية سلسلة كاملة.

اسم المضيف

يقوم PxGrid API لعدة وظائف (مثل تنزيل جلسة العمل) بإجراء تحقق إضافي. يتصل العميل ب ISE ويستلم ال ISE hostname، أي يكون عينت ب ال hostname أمر في ال CLI. ثم يحاول العميل إجراء تحليل DNS لاسم المضيف هذا ويحاول الاتصال بالبيانات وجلبها من عنوان IP هذا. في حالة فشل تحليل DNS لاسم مضيف ISE، لا يحاول العميل الحصول على أي بيانات.

تحذير: لاحظ أنه يتم إستخدام اسم المضيف فقط لهذا الحل، وهو **موجود** في هذا السيناريو، وليس اسم المجال المؤهل بالكامل (FQDN)، وهو **lise.example.com** في هذا السيناريو.

ملاحظة للمطورين

تقوم Cisco بنشر واجهة برمجة تطبيقات PxGrid ودعمها. هناك حزمة واحدة تسمى:

pxgrid-sdk-1.0.0-167

في الداخل هناك:

- ملفات pxGrid JAR ذات فئات، والتي يمكن فك تشفيرها بسهولة لملفات Java للتحقق من التعليمات البرمجية
- نموذج لمفاتيح Java مع التراخيص
- نموذج نصوص تفاعلية تستخدم نموذج Java Class التي تستخدم pxGrid

Syslog

وفيما يلي قائمة حلول الأمان التي ترسل رسائل syslog باستخدام عنوان IP للمهاجم. ويمكن دمج هذه العناصر بسهولة مع pxLog طالما أنك تستخدم قاعدة RegExp الصحيحة في التكوين.

شخير

يرسل snort تنبيهات syslog بهذا التنسيق:

```
[host[id] [sig_gen, sig_id, sig_sub] [action] [msg] [proto] [src] [dst
```

فيما يلي مثال:

```
snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61
```

دائما ما يكون عنوان IP للمهاجم هو الثاني قبل الأخير (الوجهة). من السهل بناء RegExp متعدد المستويات لتوقيع محدد واستخراج عنوان IP للمهاجم. هنا مثال RegExp للتوقيع 100124 وبرتوكول رسائل التحكم في الإنترنت (ICMP) للرسائل:

```
*.snort[\.*:100124:.*ICMP
```

فحص أجهزة الأمان المعدلة (ASA) من Cisco

عندما يتم تكوين ASA للتفتيش على HTTP (على سبيل المثال)، تبدو رسالة syslog المقابلة كما يلي:

```
:Mar 12 2014 14:36:20: %ASA-5-415006: HTTP - matched Class 23
- MS13-025_class in policy-map MS_Mar_2013_policy, URI matched
Dropping connection from inside:192.168.60.88/2135 to
outside:192.0.2.63/80
```

مرة أخرى، يمكن إستخدام RegExp متعدد المستويات لتصفية هذه الرسائل واستخراج عنوان IP للمهاجم، الثاني قبل الأخير.

أنظمة الحماية من التطفل Cisco Sourcefire Next Intrusion Prevention Systems (NGIPS)

فيما يلي مثال على الرسالة التي تم إرسالها بواسطة مستشعر Sourcefire:

```
Jan 28 19:46:19 IDS01 SFIMS: [CA IDS][Policy1][119:15:1] http_inspect: OVERSIZE
[REQUEST-URI DIRECTORY [Classification: Potentially Bad Traffic] [Priority: 2
TCP} 10.12.253.47:55504 -> 10.15.224.60:80}
```

لذلك مرة أخرى، من السهل إستخراج عنوان IP للمهاجم لأن نفس المنطق يطبق. كما يتم توفير اسم النهج والتوقيع، حتى يمكن أن تكون قاعدة pxLog متعددة المستويات.

جونبر نت شباك

وفيما يلي مثال على الرسالة التي أرسلها النازحون داخليا من شركة Juniper القديمة للكشف عن الاقتحام والوقاية منه:

```
dayId="20061012" recordId="0" timeRecv="2006/10/12
"timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0 "21:52:21
"device_ip="10.209.83.4" cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN
"srcZn="NULL" srcIntf="NULL" srcAddr="192.168.170.20" srcPort="63396
"natSrcAddr="NULL" natSrcPort="0" dstZn="NULL" dstIntf="NULL
"dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL" natDstPort="0
"protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS
"ruleNo="4" action="NONE" severity="LOW" alert="no" elaspedTime="0" inbytes="0
"outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0
"packetData="no" varEnum="31" misc="<017>'interface=eth2" user="NULL
"app="NULL" uri="NULL
```

يمكن إستخراج عنوان IP الخاص بالمهاجم بنفس الطريقة.

جونبر جونيوس

ويتشابه نظام التشغيل JunOS:

```
:[Jul 16 10:09:39 JuniperJunOS: asp[8265
,(ASP_IDS_TCP_SYN_ATTACK: asp 3: proto 6 (TCP
ge-0/0/1.0 10.60.0.123:2280 -> 192.168.1.12:80, TCP
SYN flood attack
```

منصات لينوكس

هنا مثال على منصات لينوكس.

```
=Jun 15 23:37:33 netfilter kernel: Inbound IN=lo OUT
MAC=00:13:d3:38:b6:e4:00:01:5c:22:9b:c2:08:00 src=10.0.0.1 DST=10.0.0.100 LEN=60
TOS=0x10 PREC=0x00 TTL=64 ID=47312 DF PROTO=TCP SPT=40945 DPT=3003 WINDOW=32767
RES=0x00 SYN URGP=0
```

يمكنك إرسال معلومات syslog لأي نوع من الحزم باستخدام الوظائف المتقدمة التي توفرها الوحدات النمطية المجدولة مثل تعقب الاتصال، و xtables، و rpfilter، ومطابقة الأنماط، وما إلى ذلك.

(FreeBSD IPFirewall (IPFW

هنا مثال رسالة ل IPFW حظر أجزاء:

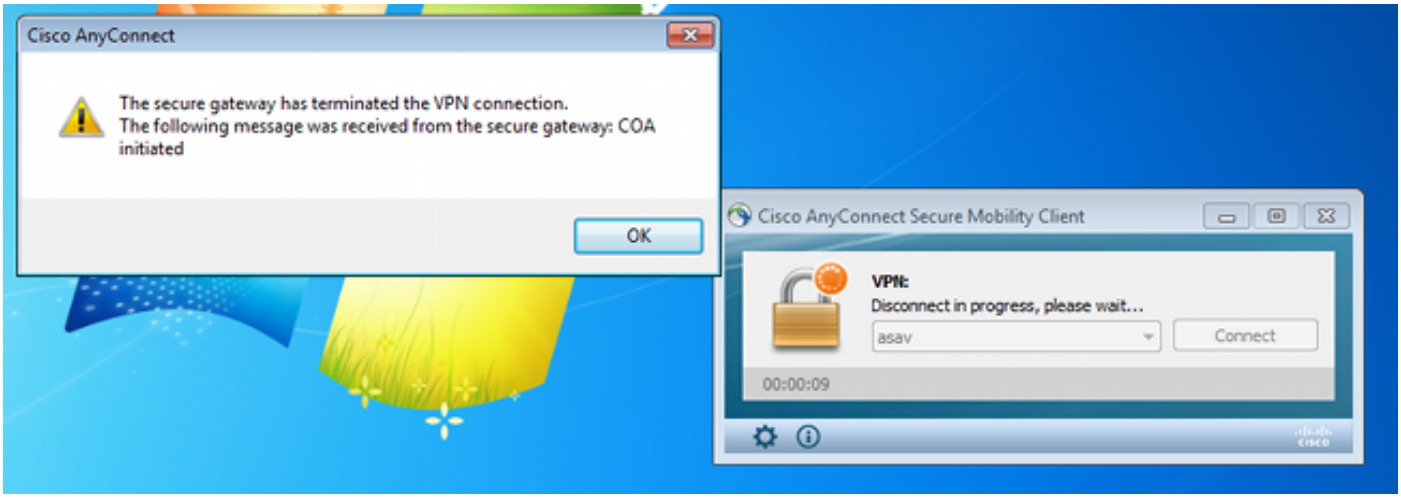
```
Sep  7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0
(frag 52639:519@1480)
```

جاهزية شبكات VPN ومعالجة CoA

ويستطيع ISE التعرف على نوع الجلسات من حيث معالجة CoA.

- بالنسبة لمدخل جانبي لمصادقة MAB) 802.1x/MAC) سلكي، يرسل ISE إعادة مصادقة CoA، والتي تقوم بتشغيل مصادقة ثانية.
- بالنسبة للشبكة اللاسلكية 802.1x/MAB، يرسل ISE إنهاء CoA، مما يؤدي إلى تشغيل مصادقة ثانية.
- بالنسبة لشبكة ASA VPN، يرسل ISE CoA مع إرفاق قائمة تحكم في الوصول (DACL) جديدة (لا توجد مصادقة ثانية).

وحدة EPS بسيطة. عندما يقوم بتنفيذ عزل، فإنه يرسل دائما حزمة CoA. بالنسبة للجلسات السلكية/اللاسلكية، لا تمثل هذه المشكلة (يمكن لجميع ملحقات 802.1x بدء جلسة EAP ثانية بشكل شفاف). ولكن عندما يستلم ASA CoA، فإنه يسقط جلسة VPN ويتم تقديم المستخدم النهائي مع هذا:



هناك حلان محتملان لإجبار AnyConnect VPN على إعادة الاتصال تلقائيا (تم تكوينه في ملف تعريف XML):

AutoReconnect، والذي يعمل فقط عندما تفقد الاتصال ببوابة الشبكة الخاصة الظاهرية (VPN)، وليس للإنهاء الإداري

- دائم التشغيل، والذي يعمل ويفرض على AnyConnect إعادة إنشاء الجلسة تلقائيا

وحتى عند إنشاء الجلسة الجديدة، يختار ASA معرف جلسة عمل التدقيق الجديد. من وجهة نظر ISE، هذه جلسة جديدة ولا توجد فرصة لمواجهة قاعدة الحجر الصحي. بالنسبة للشبكات الخاصة الظاهرية (VPNs) أيضا، لا يمكن إستخدام عنوان MAC الخاص بنقطة النهاية كهوية، بدلا من النقطة dot1x السلكية/اللاسلكية.

الحل هو إجبار EPS على التصرف مثل ISE وإرسال النوع الصحيح من CoA بناء على الجلسة. سيتم إدخال هذه الوظيفة في الإصدار 1.3.1 من ISE.

شركاء وحلول pxGrid

فيما يلي قائمة بشركاء PxGrid وحلولها:

- LogRhythm (معلومات الأمان وإدارة الأحداث (SIEM)) - يدعم واجهة برمجة تطبيقات نقل الحالة التمثيلية (REST)
- Splunk (SIEM) - يدعم REST API
- برنامج Arcsight من HP (SIEM) - يدعم واجهة برمجة تطبيقات REST
- Sentinel NetIQ (SIEM) - خطط دعم PXgrid
- Lancope StealthWatch (SIEM) - خطط دعم PXgrid
- Cisco Sourcefire - خطط دعم PXgrid 1HCY15
- جهاز أمان الويب (WSA) من Cisco - خطط لدعم PxGrid في أبريل 2014

فيما يلي شركاء وحلول أخرى:

- ثابتة (تقييم قابلية التأثر)
- Emulex (التقاط الحزم والتحليلات الجنائية)
- شبكات Bayshore (منع فقدان البيانات (DLP) وسياسة إنترنت الأشياء (IoT))
- هوية إختبار الاتصال (إدارة الوصول والهوية (IAM)/تسجيل الدخول الأحادي (SSO))
- رادار SIEM) QRata)
- LogLogic (SIEM)
- Symantec (إدارة الجهاز المحمول (MDM) SIEM AMD)

ارجع إلى كتالوج حلول السوق للحصول على القائمة الكاملة لحلول الأمان.

واجهات برمجة تطبيقات ISE: REST مقابل EREST مقابل PXgrid

هناك ثلاثة أنواع من واجهة برمجة التطبيقات (API) متوفرة في الإصدار 1.3 من ISE.

وإليكم مقارنة:

	إستراحة	الراحة الخارجية	pxGrid
مصادقة العميل	اسم المستخدم + كلمة المرور (مصادقة HTTP الأساسية)	اسم المستخدم + كلمة المرور (مصادقة HTTP الأساسية)	شهادة
فصل الامتياز	لا	محدود (ERS Admin)	نعم (مجموعات)
الوصول	MNt	MNt	MNt
النقل	بروتوكول TCP/443 ((HTTPS	بروتوكول TCP/9060 ((HTTPS	بروتوكول XMPP) TCP/5222)
أسلوب HTTP	إحضار	الحصول/النشر/وضع	الحصول/النشر
ممكن بشكل افتراضي	نعم	لا	لا
عدد العمليات	القليل	كثير	القليل
إنهاء CoA	سوند	لا	سوند
إعادة مصادقة CoA	سوند	لا	مدعوم *
عمليات المستخدم	لا	نعم	لا
عمليات نقطة النهاية	لا	نعم	لا
عمليات مجموعة هوية النقطة الطرفية	لا	نعم	لا
عزل (IP، MAC)	لا	لا	نعم
UnQuarantine (IP، MAC)	لا	لا	نعم
PortBounce/Shutdown	لا	لا	نعم
عمليات المستخدم الضيف	لا	نعم	لا
عمليات بوابة الضيوف	لا	نعم	لا
عمليات جهاز الشبكة	لا	نعم	لا
عمليات مجموعة أجهزة الشبكة	لا	نعم	لا

* يستخدم الحجر الصحي دعم CoA الموحد من ISE الإصدار 1.3.1.

التنزيلات

يمكن تنزيل pxLog من Sourceforge .

مجموعة أدوات تطوير البرامج (SDK) مضمنة بالفعل. للحصول على أحدث وثائق SDK و API ل PXgrid، اتصل بالشريك أو فريق حساب Cisco.

معلومات ذات صلة

- Cisco ISE 1.2 REST API
- Cisco ISE 1.2 External RestFull API
- دليل مسؤولي Cisco ISE 1.3
- 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).