

IPS قي بطات عم PXgrid 1.3 رادصإلإ ISE لم اكات PXlog

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الرسم التخطيطي للشبكة وتدفق حركة مرور البيانات](#)

[pxLog](#)

[عمارة](#)

[التثبيت](#)

[شخير](#)

[محرك خدمات كشف الهوية \(ISE\)](#)

[التكوين](#)

[الشخصية والشهادة](#)

[خدمة حماية نقطة النهاية \(EPS\)](#)

[قواعد التحويل](#)

[استكشاف الأخطاء وإصلاحها](#)

[إختبار](#)

[الخطوة 1. التسجيل ل pxGrid](#)

[الخطوة 2. تكوين قواعد pxLog](#)

[الخطوة الثالثة. First Dot1x جلسة](#)

[الخطوة 4. برسل Microsoft Windows PC الحزمة التي تشغل التنبيه](#)

[الخطوة 5. pxLog](#)

[الخطوة 6. عزل ISE](#)

[الخطوة 7. إلغاء عزل PxLog](#)

[الخطوة 8. ISE Unquarantine](#)

[وظيفة pxLog](#)

[متطلبات بروتوكول pxGrid](#)

[مجموعات](#)

[الشهادات ومفتاح Java](#)

[اسم المضيف](#)

[ملاحظة للمطورين](#)

[Syslog](#)

[شخير](#)

[فحص أجهزة الأمان المعدلة \(ASA\) من Cisco](#)

[أنظمة الحماية من التطفل \(NGIPS\) \(Cisco Sourcefire Next Intrusion Prevention Systems\)](#)

[جونير نت شياك](#)

[جونير جونيوس](#)

[منصات لينوكس](#)

[\(FreeBSD IPFirewall \(IPFW](#)

[جاهزية شبكات VPN ومعالجة CoA](#)

[شركاء وحلول pxGrid](#)

[واجهات برمجة تطبيقات REST: ISE مقابل EREST مقابل PXgrid](#)

[التنزيلات](#)

[معلومات ذات صلة](#)

المقدمة

يدعم Identity Services Engine (ISE) 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 استخدام 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 (CoA) RADIUS لتغيير حالة التفويض لنقطة النهاية التي تحد من وصول الشبكة. يحدث كل هذا بشكل شفاف للمستخدم النهائي.

على سبيل المثال، تم استخدام Snort ك IPS، ولكن يمكن استخدام 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 أكتشاف 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 استخدامه أثناء تحسين تنفيذ PxGrid على ISE.

المتطلبات الأساسية

المتطلبات

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

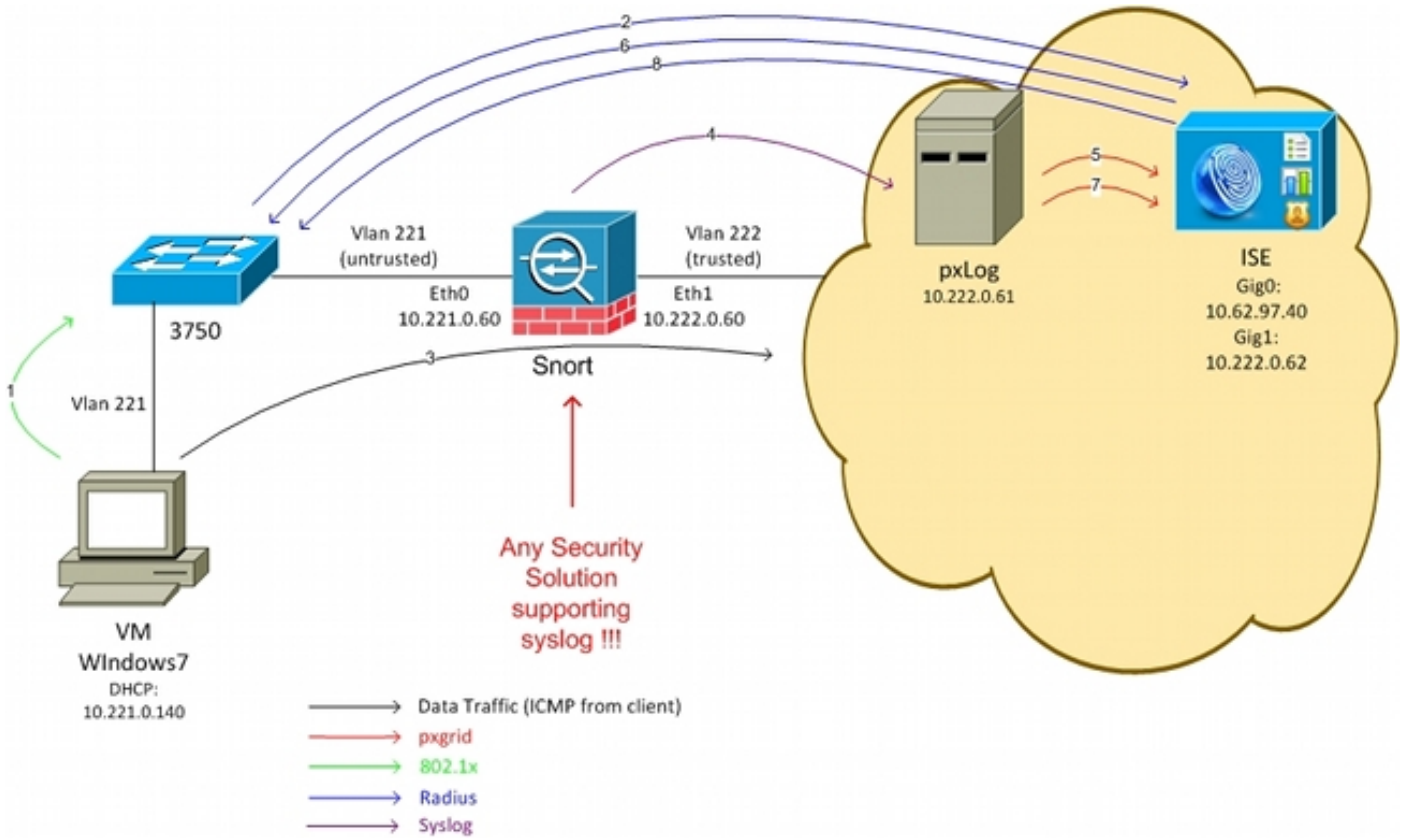
- عمليات نشر ISE وتكوين التفويض
- CLI تشكيل من cisco مادة حفازة مفتاح

المكونات المستخدمة

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

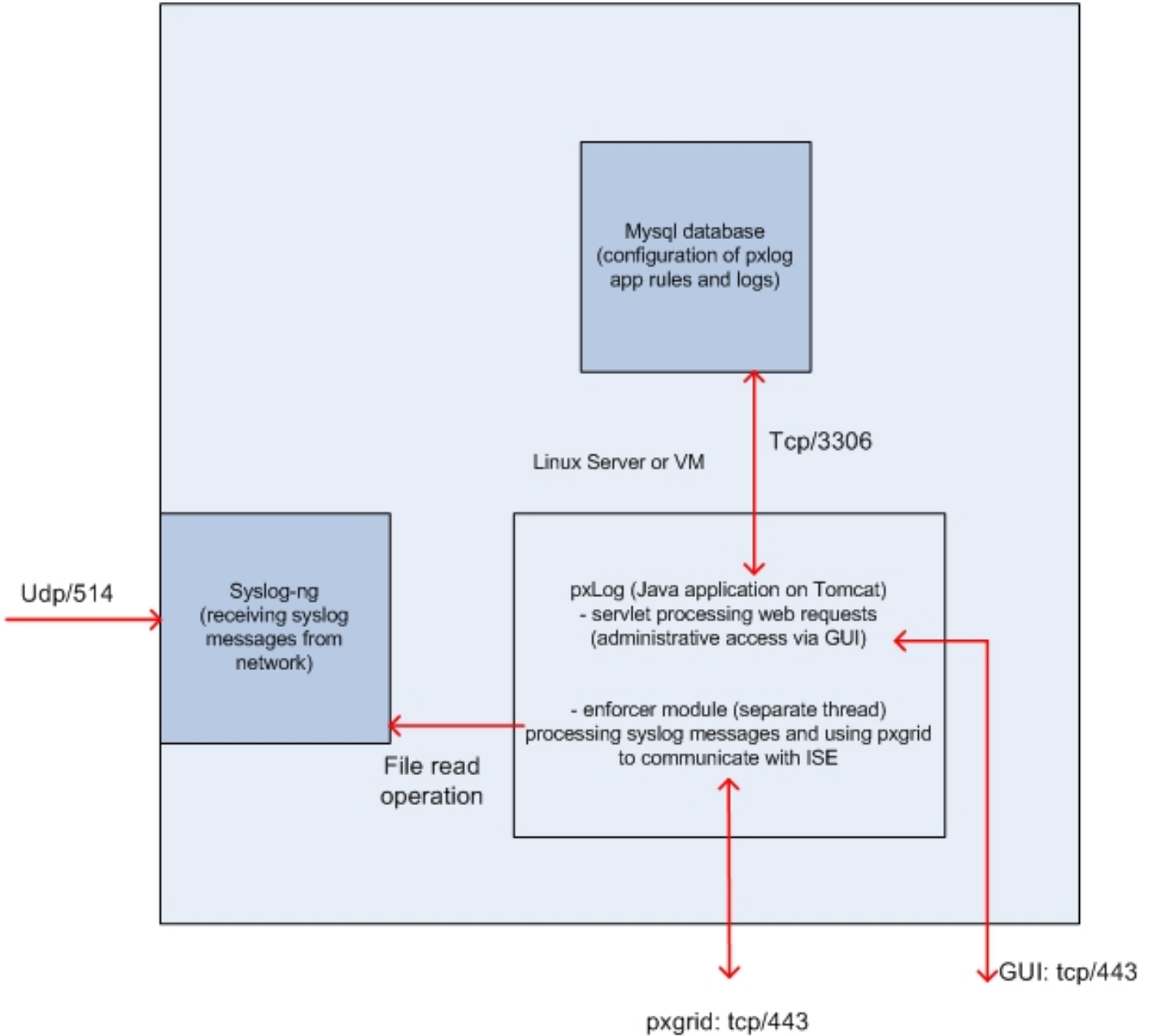
- نظام التشغيل Microsoft Windows 7
- برامج المحول Cisco Catalyst 3750X Series Switch، الإصدارات 15.0 والإصدارات الأحدث
- برنامج Cisco ISE، الإصدارات 1.3 والإصدارات الأحدث
- Cisco AnyConnect Mobile Security باستخدام مدير الوصول إلى الشبكة (NAM)، الإصدار 3.1 والإصدارات الأحدث
- SNORT الإصدار 2.9.6 مع الحصول 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 لـ Dot1x ويتم منح الوصول الكامل إلى الشبكة (DACL: PERMIT_ALL).
3. يحاول المستخدم الاتصال بالشبكة الموثوق بها ويخرق قاعدة الشخ.
4. ونتيجة لذلك، يرسل Snort تنبيهًا 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 التحويل الخاصة به. لأن نقطة النهاية تم عزلها، فإن Session:EPSStatus يساوي شرط العزل يتم استيفاء وملف تعريف تحويل 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 للتزليل (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 بـ 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



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 استخدام 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 وفقاً 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 استخدام هذا بواسطة واجهة برمجة تطبيقات PxGrid التي تستخدم جلسة عمل طبقة مأخذ 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 (`pxLog (/etc/snort/snort.conf`):

```
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 استخدام 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:

Edit Node

General Settings

Profiling Configuration

Hostname **lise**
FQDN **lise.example.com**
IP Address **10.62.97.40**
Node Type **Identity Services Engine (ISE)**

Personas

- Administration Role **STANDALONE** Make Primary
- Monitoring Role PRIMARY Other Monitoring Node
- Policy Service
 - Enable Session Services ⓘ
Include Node in Node Group None ⓘ
 - Enable Profiling Service
- pxGrid ⓘ

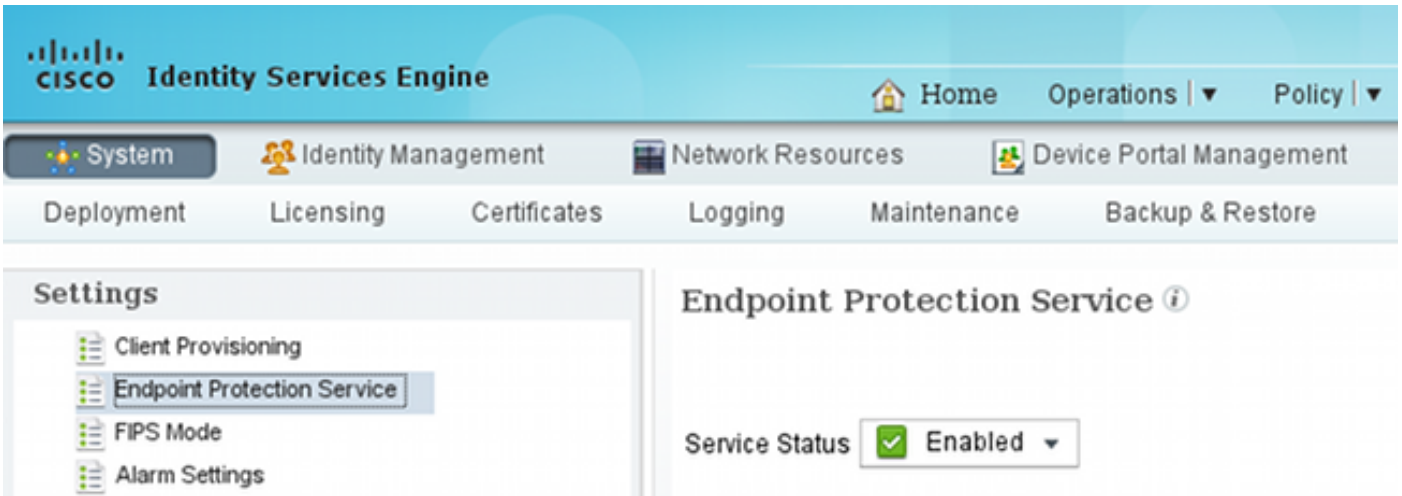
2. دقت إن يكون الشهادات استعملت ل pxGrid تحت إدارة < شهادات > نظام شهادات:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The left sidebar shows a menu with 'Certificate Management' expanded, containing 'Overview', 'System Certificates', 'Endpoint Certificates', 'Trusted Certificates', 'OCSP Client Profile', and 'Certificate Signing Requests'. Below this is 'Certificate Authority' with 'Internal CA Settings', 'Certificate Templates', and 'External CA Settings'. The main content area is titled 'Edit System Certificate' and displays the following configuration details:

- Issuer**
 - * Friendly Name:
 - Description:
 - Subject: CN=lise.example.com
 - Issuer: win2012
 - Valid From: Tue, 26 Aug 2014 12:32:56 CEST
 - Valid To (Expiration): Thu, 25 Aug 2016 12:32:56 CEST
 - Serial Number: 7B 00 00 00 3D 4C D6 27 D1 7D BB DF A6 00 00 00 00 3D
 - Signature Algorithm: SHA1WITHRSA
 - Key Length: 2048
- Usage**
 - EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
 - Admin: Use certificate to authenticate the ISE Admin Portal
 - pxGrid: Use certificate for the pxGrid Controller
 - Portal: Use for portal

خدمة حماية نقطة النهاية (EPS)

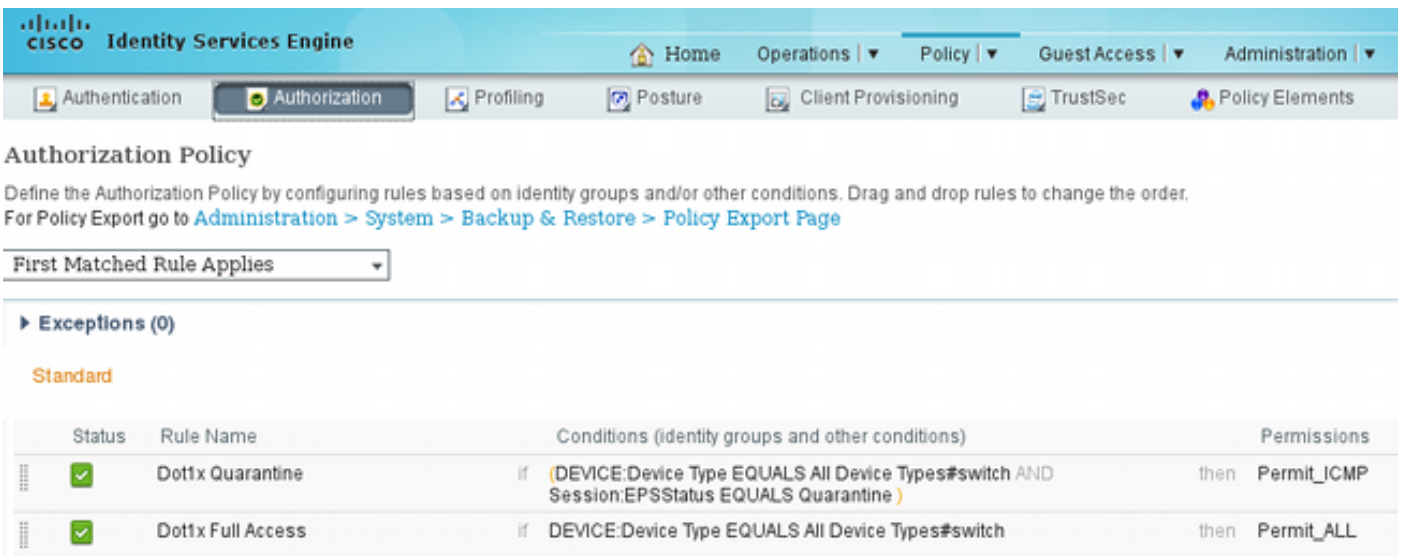
يجب تمكين EPS (معطل بشكل افتراضي) من الإدارة < الإعدادات:



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Device Portal Management'. Under 'System', there are sub-tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', and 'Backup & Restore'. The main content area is titled 'Settings' and shows a list of configuration options: 'Client Provisioning', 'Endpoint Protection Service' (which is selected), 'FIPS Mode', and 'Alarm Settings'. To the right, the 'Endpoint Protection Service' configuration is shown, with a 'Service Status' dropdown menu set to 'Enabled'.

يتيح لك هذا استخدام وظيفة العزل/إلغاء العزل.

قواعد التخويل



The screenshot shows the Cisco Identity Services Engine (ISE) web interface for configuring an Authorization Policy. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization' (which is selected), 'Profiling', 'Posture', 'Client Provisioning', 'TrustSec', and 'Policy Elements'. The main content area is titled 'Authorization Policy' and contains the following text: 'Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)'. Below this, there is a dropdown menu for 'First Matched Rule Applies' set to 'First Matched Rule Applies'. Underneath, there is a section for 'Exceptions (0)' with a sub-section for 'Standard'. A table lists the rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Dot1x Quarantine	if (DEVICE:Device Type EQUALS All Device Types#switch AND Session:EPSStatus EQUALS Quarantine)	then Permit_ICMP
✓	Dot1x Full Access	if DEVICE:Device Type EQUALS All Device Types#switch	then Permit_ALL

يتم مصادفة 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 وpxgrid/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:

The screenshot displays the pxLog - Application integrating IPS interface. At the top left is the Cisco logo. The main heading is "pxLog - Application integrating IPS". Below the heading, there is a description: "This is the homepage of pxgrid application integrating IPS with ISE." A navigation menu is visible on the left side, with the following items: Homepage, Manage Rules, Pxgrid Operations (with a dropdown arrow), Logs, ClearLogs, and Resources (with a dropdown arrow). The Resources dropdown menu is expanded, showing the following options: Register users, Display Sessions, Display Sessions by IP, Display Profiles, Display SGT, Display Users, Check capabilities, Quarantine IP, Quarantine MAC, UnQuarantine IP, and UnQuarantine MAC.

يبدأ التسجيل تلقائيا:



pxLog - Application integrating IPS with Cisco ISE

Homepage

Manage Rules

Pxgrid Operations

Logs

ClearLogs

Resources

Registration

The Registration process has started

Two pxgrid clients are being registered on ISE

One client with Session privileges (to browse session data) and other with EPS privileges (to execute quarantine)

Please login to ISE and approve registration by clicking "Approve"

Content of the page will be updated automatically every 5 seconds to notify if the users are approved on ISE

Waiting for the status to be updated...

Waiting for the status to be updated...

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

Client Name	Client Description	Capabilities	Status	Client Group
ise-admin-lise		Capabilities(3 Pub, 1 Sub)	Online	Administrator
ise-mnt-lise		Capabilities(1 Pub, 0 Sub)	Online	Administrator
pxclient_session	test	Capabilities(0 Pub, 0 Sub)	Pending	Session
pxclient_eps	test	Capabilities(0 Pub, 0 Sub)	Pending	EPS

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

Session user: pxclient_session registered and approved successfully
EPS user: pxclient_eps registered and approved successfully

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:



pxLog - Application integrating

Homepage

Manage Rules

Pxgrid Operations >

Logs

ClearLogs

Resources >

Rules for the Enforcer module.

IPS sending syslog messages, Enforcer receiving and processing.

When the match against configured rules is found

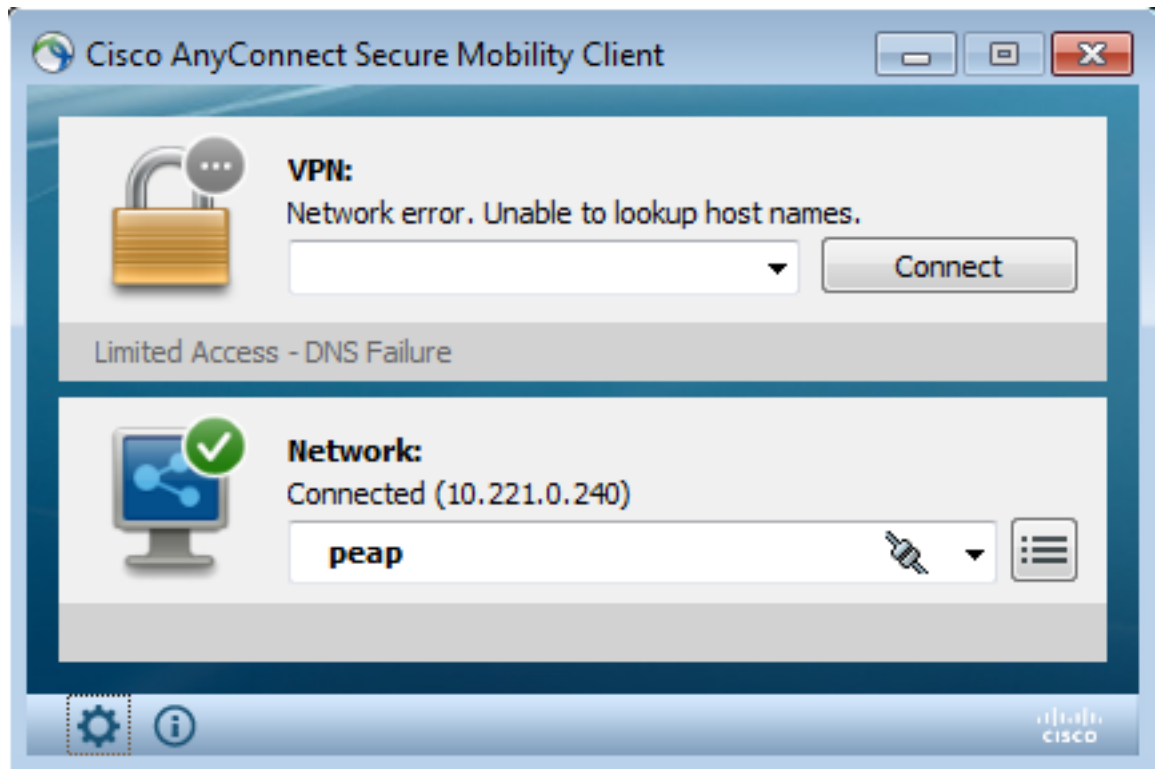
Enforcer is automatically executing quarantine via pxgrid

Rule Id	Rule string	Action
19	snort[<input type="button" value="Remove"/>
New Rule	<input type="text"/>	<input type="button" value="Add New Rule"/>

الآن تبحث وحدة الإنفاذ عن هذا التعبير العادي (RegExp) في رسالة "snort: syslog". 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 استخدام 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 استخدام AnyConnect NAM من Cisco كطالب. تم تكوين أسلوب EAP المحمي بروتوكول المصادقة المتوسع (EAP-PEAP).



تم تحديد ملف تعريف تخويل ISE Dot1x Full Access. 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 تنبيهه. 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، وبالعكس، ويطلب إجراء عزل لعنوان IP هذا. يمكن تأكيد ذلك إذا قمت بفحص السجلات:

Logs from the actions executed by the Enforcer 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:

Report Selector	Endpoint Protection Service Audit							
Favorites ISE Reports Endpoint Protection Service Audit Operation Type: All Time Range: Today Run	From 09/07/2014 12:00:00 AM to 09/07/2014 12:16:48 AM	Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session ID
	2014-09-07 00:10:33.0	00:50:B6:11:ED:31	10.221.0.240	Quarantine	SUCCESS	16	0A01000C000037E6B8267	
	2014-09-07 00:10:32.9	00:50:B6:11:ED:31	10.221.0.240	Quarantine	RUNNING	16	0A01000C000037E6B8267	

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

Cisco Identity Services Engine											
Misconfigured Supplicants		Misconfigured Network Devices		RADIUS Drops		Client Stopped Responding		Repeat Counter			
Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts Refresh: Every 1 minute Show: Latest 20 records with: Last 24 hours											
Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Event
2014-09-07 00:10:34...	●		0	cisco	00:50:B6:11:ED:31			switch			Session State is Started
2014-09-07 00:10:33...	●		0	#ACSACL#IP-Permit_ICMP	00:50:B6:11:ED:31	Default >> Dot1x Quarantine	Permit_ICMP	switch	GigabitEthernet0/17	User Identity Gro...	DACL Download Succeeded
2014-09-07 00:10:33...	●		0	cisco	00:50:B6:11:ED:31			switch			Dynamic Authorization succ.
2014-09-07 00:05:38...	●		0	#ACSACL#IP-Permit_ALL	00:50:B6:11:ED:31			switch			DACL Download Succeeded
2014-09-07 00:05:38...	●		0	cisco	00:50:B6:11:ED:31	Default >> Dot1x Full Access	Permit_ALL	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded

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): 587c fba54769d84f092ffd233b96427
  > 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

```

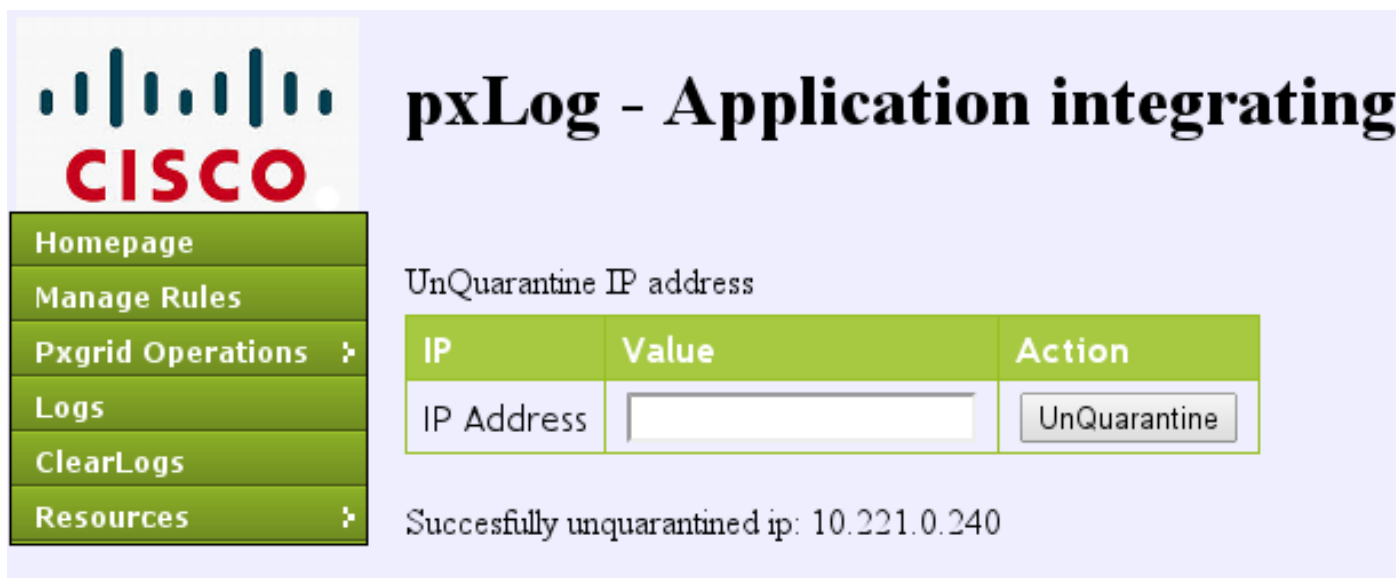
```

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:



pxLog - Application integrating

UnQuarantine IP address

IP	Value	Action
IP Address	<input type="text"/>	UnQuarantine

Successfully unquarantined ip: 10.221.0.240

نفس العملية يستطيع كنت نفذت مباشرة من ال ISE:

Endpoint Protection Service

Endpoint Operation

* IP Address (Example: 1.2.3.4)

* MAC Address

* Operation

Update Information

For a complete list, go to Operations > Reports > Endpoints & Users > Endpoint Protection Service Audit

Last Operation Status

الخطوة 8. ISE Unquarantine

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

Time	Status	Det...	R	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Event
2014-09-07 00:21:11...				osco	00:50:86:11:ED:31						Session State is Started
2014-09-07 00:21:10...				#ACSACL# IP-PERMIT_ALL				switch			DACL Download Succeeded
2014-09-07 00:21:10...				osco	00:50:86:11:ED:31	Default => Dat1= Full Access	Permit_ALL	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded
2014-09-07 00:21:10...				osco	00:50:86:11:ED:31			switch			Dynamic Authorization succeeded
2014-09-07 00:10:33...				#ACSACL# IP-PERMIT_CHMP				switch			DACL Download Succeeded
2014-09-07 00:10:33...				osco	00:50:86:11:ED:31	Default => Dat1= Quarantine	Permit_CHMP	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded
2014-09-07 00:10:33...				osco	00:50:86:11:ED:31			switch			Dynamic Authorization succeeded
2014-09-07 00:05:38...				#ACSACL# IP-PERMIT_ALL				switch			DACL Download Succeeded
2014-09-07 00:05:38...				osco	00:50:86:11:ED:31	Default => Dat1= Full Access	Permit_ALL	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded

ويؤكد التقرير:

Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session ID
2014-09-07 00:21:10.342	00:50:B6:11:ED:31	10.221.0.240	Unquarantine	SUCCESS	17	0A01000C000037E7B8B7D68C
2014-09-07 00:21:10.309	00:50:B6:11:ED:31	10.221.0.240	Unquarantine	RUNNING	17	0A01000C000037E7B8B7D68C
2014-09-07 00:10:33.055	00:50:B6:11:ED:31	10.221.0.240	Quarantine	SUCCESS	16	0A01000C000037E6B8B267CF
2014-09-07 00:10:32.973	00:50:B6:11:ED:31	10.221.0.240	Quarantine	RUNNING	16	0A01000C000037E6B8B267CF

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 (TrustSec (SGTs) المعرفة في ISE
- التحقق من الإصدار (إمكانات pxGrid)
- إجراء عزل استنادا إلى عنوان IP أو MAC
- إلغاء العزل استنادا إلى عنوان IP أو MAC.

فيما يلي بعض لقطات الشاشة من pxLog:



pxLog - Application integrating IPS with

List of the users with active sessions downloaded from ISE via pxgrid

User	Groups
cisco	User Identity Groups:Employee,User Identity Groups:VPN,Unknown



pxLog - Application integrating IPS with Cisco ISE using pxgrid

List of active sessions on ISE

Id	User	Domain	MAC	State	ESPStatus	SGT	Profile	NAS IP	NAS Port	AVP
0	cisco		00:50:B6:11:ED:31	Started			Unknown	10.62.71.140	GigabitEthernet0/17	Acct-Session-Id 00003A72



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

Display session by IP address

IP	Value	Action
IP Address	<input type="text" value="10.221.0.240"/>	<input type="button" value="Display"/>

List of the sessions found by IP

Id	User	Domain	MAC	State	ESPStatus	SGT	Profile	NAS IP	NAS Port	AVP
0	cisco		00:50:B6:11:ED:31	Started			Unknown	10.62.71.140	GigabitEthernet0/17	Acct-Session-Id 00003A72



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

List of SGT tags downloaded from ISE via pxgrid

Id	SGT Name	SGT Description	SGT number
a14bc9f0-3597-11e4-81d2-0050569c3ff3	Marketing		3
0c2ca0f0-3598-11e4-81d2-0050569c3ff3	Quarantined	Users violating policies, limited access	2
9c903db0-3597-11e4-81d2-0050569c3ff3	IT		2
173025d0-3598-11e4-81d2-0050569c3ff3	Development		6
06ce9320-3598-11e4-81d2-0050569c3ff3	VPN	Anyconnect Ikev2 sessions	2
d006f0b0-2c02-11e4-907b-005056bf2f0a	ANY	Any Security Group	65535
cff3b6d0-2c02-11e4-907b-005056bf2f0a	Unknown	Unknown Security Group	0
1c6527d0-3598-11e4-81d2-0050569c3ff3	Finance	Only for audits	2



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

List of the profile download from ISE via pxgrid

Profile Id	Profile Name	Full Profile Name
0e4d9640-2c02-11e4-907b-005056bf2f0a	Xerox-WorkCentre-5020-dn	Xerox-Device:Xerox-WorkCentre-5020-dn
1657b140-2c02-11e4-907b-005056bf2f0a	Cisco-AP-Aironet-1240	Cisco-Device:Cisco-Access-Point:Cisco-AP-Aironet-1240
0a3e9db0-2c02-11e4-907b-005056bf2f0a	Xerox-Phaser-6140dn	Xerox-Device:Xerox-Phaser-6140dn
1f4e0100-2c02-11e4-907b-005056bf2f0a	VMWare-Device	VMWare-Device
ff876410-2c01-11e4-907b-005056bf2f0a	Cisco-WLC	Cisco-Device:Cisco-WLC
0d40e130-2c02-11e4-907b-005056bf2f0a	Xerox-Phaser-8860mfp	Xerox-Device:Xerox-Phaser-8860mfp
0bd6a2d0-2c02-11e4-907b-005056bf2f0a	Xerox-Phaser-7500dx	Xerox-Device:Xerox-Phaser-7500dx
21e43c40-2c02-11e4-907b-005056bf2f0a	Philips-Intellivue	Philips-Device:Philips-Intellivue
15d7f9f0-2c02-11e4-907b-005056bf2f0a	DLINK-DAP-1522	DLINK-Device:DLINK-DAP-1522
0eb5f500-2c02-11e4-907b-005056bf2f0a	Xerox-WorkCentre-5225	Xerox-Device:Xerox-WorkCentre-5225

متطلبات بروتوكول pxGrid

مجموعات

يمكن أن يكون العميل (المستخدم) عضواً في مجموعة واحدة في كل مرة. والفتتان الأكثر استخداماً 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. إنشاء مخزن مفاتيح جذر (موثوق به)، قم باستيراد شهادة CA (**cert-ca.der**) 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، اختر كلمة مرور، والتي يتم استخدامها لاحقا للوصول إلى مخزن المفاتيح.

3. استيراد 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. إنشاء 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
```

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 hostname ISE، 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 استخدام 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 استخدام RegExp متعدد المستويات لتصفية هذه الرسائل واستخراج عنوان IP للمهاجم، الثاني قبل الأخير.

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

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 استخراج 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" elapsedTime="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 استخراج عنوان IP الخاص بالمهاجم بنفس الطريقة.

جونبر جونيوس

وبتشابه 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

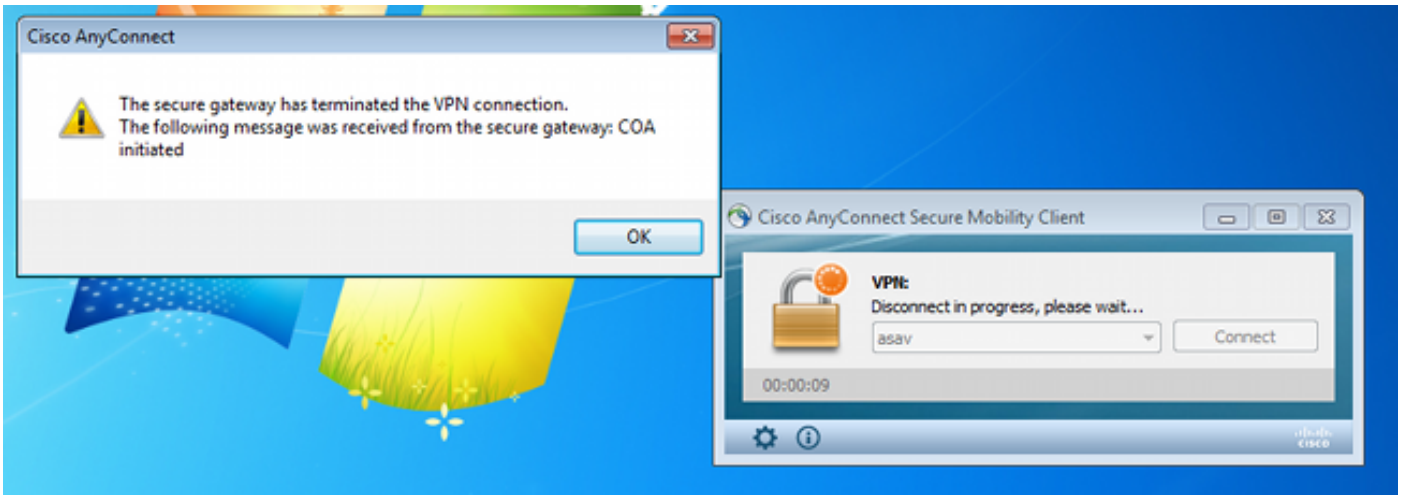
هنا مثال رسالة ل IPFW حظر أجزاء:

```
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 تلقائياً (تم تكوينه في ملف تعريف XML):
 AutoReconnect، والذي يعمل فقط عندما تفقد الاتصال ببوابة الشبكة الخاصة الظاهرية (VPN)، وليس للإجراء الإداري

- دائم التشغيل، والذي يعمل ويفرض على AnyConnect إعادة إنشاء الجلسة تلقائياً 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) أيضاً، لا يمكن استخدام 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
 - Arcsight (SIEM من HP) - 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 (النقاط 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 REST: ISE مقابل EREST مقابل PXgrid

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

واليكم مقارنة:

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

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

التزيلات

يمكن تنزيل pxLog من [Sourceforge](https://sourceforge.net/projects/pxlog/).

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](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل