

Integración del pxGrid de la versión 1.3 ISE con la aplicación del pxLog IPS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red y flujo de tráfico](#)

[pxLog](#)

[Arquitectura](#)

[Instalación](#)

[Snort](#)

[ISE](#)

[Configuración](#)

[Personaje y certificado](#)

[Servicio de protección del punto final \(EP\)](#)

[Reglas de la autorización](#)

[Troubleshooting](#)

[Prueba](#)

[Step1. Registro para el pxGrid](#)

[Step2. el pxLog gobierna la configuración](#)

[Step3. Primera sesión del dot1x](#)

[Step4. Microsoft Windows PC envía el paquete que acciona la alarma](#)

[Step5. pxLog](#)

[Step6. Cuarentena ISE](#)

[Step7. pxLog Unquarantine](#)

[Step8. ISE Unquarantine](#)

[funciones del pxLog](#)

[requerimientos del protocolo del pxGrid](#)

[Grupos](#)

[Certificados y Javas KeyStore](#)

[Hostname](#)

[Observe para los desarrolladores](#)

[Syslog](#)

[Snort](#)

[Examen adaptante del dispositivo de seguridad de Cisco \(ASA\)](#)

[Sistemas de prevención de intrusiones de la última generación de Cisco Sourcefire \(NGIPS\)](#)

[NetScreen del enebro](#)

[Enebro JunOS](#)

[Iptables de Linux](#)

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

[Disposición VPN y dirección CoA](#)

[Partners y soluciones del pxGrid](#)

[ISE API: RESTO contra EREST contra el pxGrid](#)

[Downloads](#)

[Información Relacionada](#)

Introducción

La versión 1.3 del Identity Services Engine (ISE) soporta un nuevo pxGrid llamado API. Este protocolo que soporta la autenticación, cifrado, y privilegios modernos y flexibles (grupos) permite la integración fácil con otras soluciones acerca de la seguridad. Este documento describe el uso de la aplicación del pxLog que se ha escrito como prueba de concepto. el pxLog puede recibir los mensajes de Syslog del Sistema de prevención de intrusiones (IPS) y enviar los mensajes del pxGrid al ISE para quarantine el atacante. Como consecuencia, el ISE utiliza el cambio RADIUS de la autorización (CoA) para cambiar el estatus de autorización del punto final que limita el acceso a la red. Todo el esto sucede transparente al usuario final.

Por este ejemplo, el Snort se ha utilizado como el IPS, pero cualquier otra solución podría ser utilizada. No tiene que realmente ser un IPS. Todo se requiere que es enviar el mensaje de Syslog al pxLog con la dirección IP del atacante. Esto crea una posibilidad de la integración de un gran número de soluciones.

Este documento también presenta cómo resolver problemas y probar las soluciones del pxGrid, con los problemas comunes y las limitaciones.

Descargo: La aplicación del pxLog no es soportada por Cisco. Este artículo se ha escrito como prueba de concepto. El propósito primario era utilizarlo durante betatesting de la implementación del pxGrid en el ISE.

Prerequisites

Requisitos

Cisco recomienda que usted tiene experiencia con la configuración de Cisco ISE y el conocimiento básico de estos temas:

- Implementaciones y configuración de la autorización ISE
- Configuración CLI del Switches del Cisco Catalyst

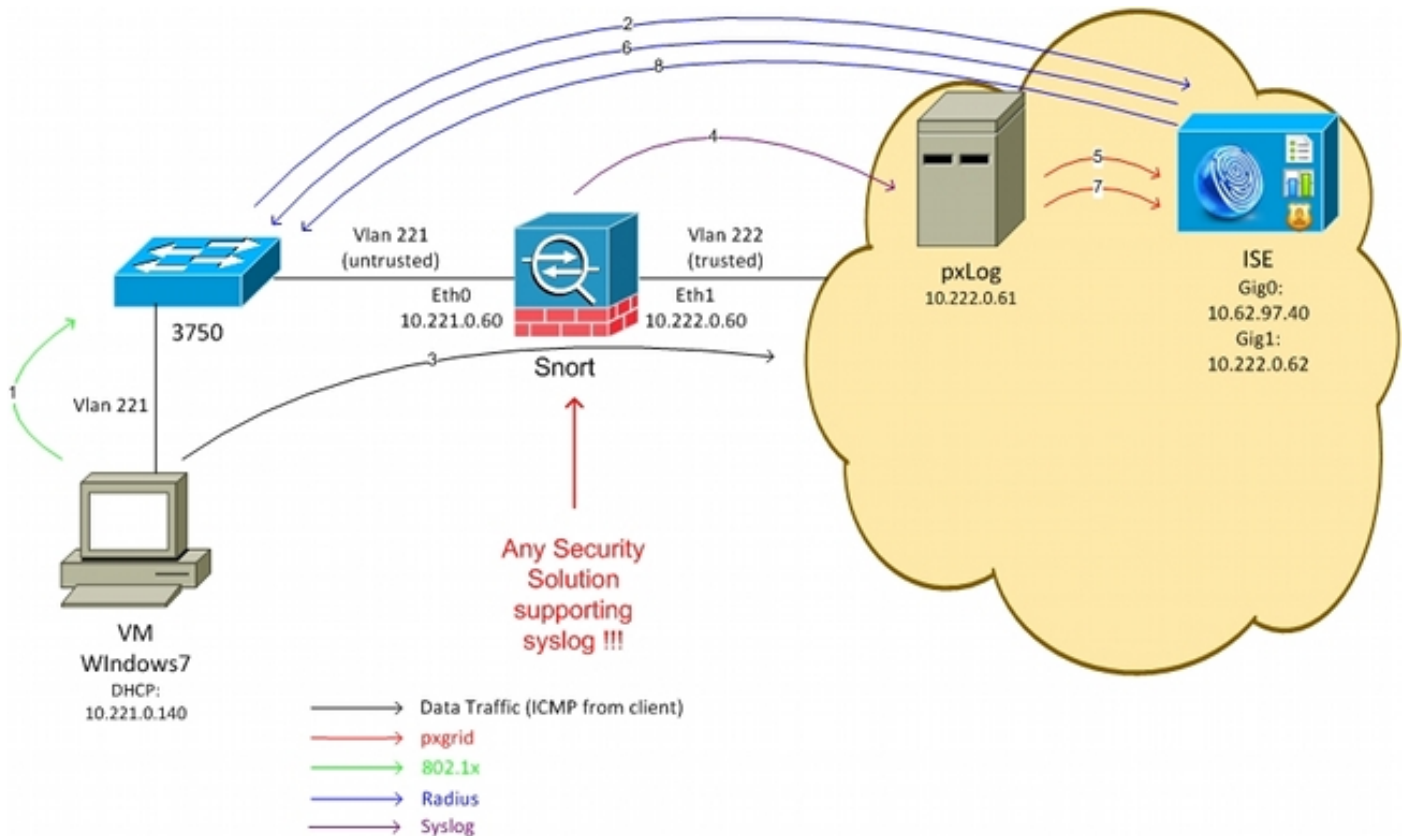
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7

- Software del Cisco Catalyst 3750X Series Switch, versiones 15.0 y posterior
- Software de Cisco ISE, versiones 1.3 y posterior
- Mobile Security de Cisco AnyConnect con el administrador del acceso a la red (NAM), versión 3.1 y posterior
- Versión 2.9.6 del Snort con de adquisición de datos (DAQ)
- aplicación del pxLog instalada en Tomcat 7 con la versión 5 de MySQL

Diagrama de la red y flujo de tráfico



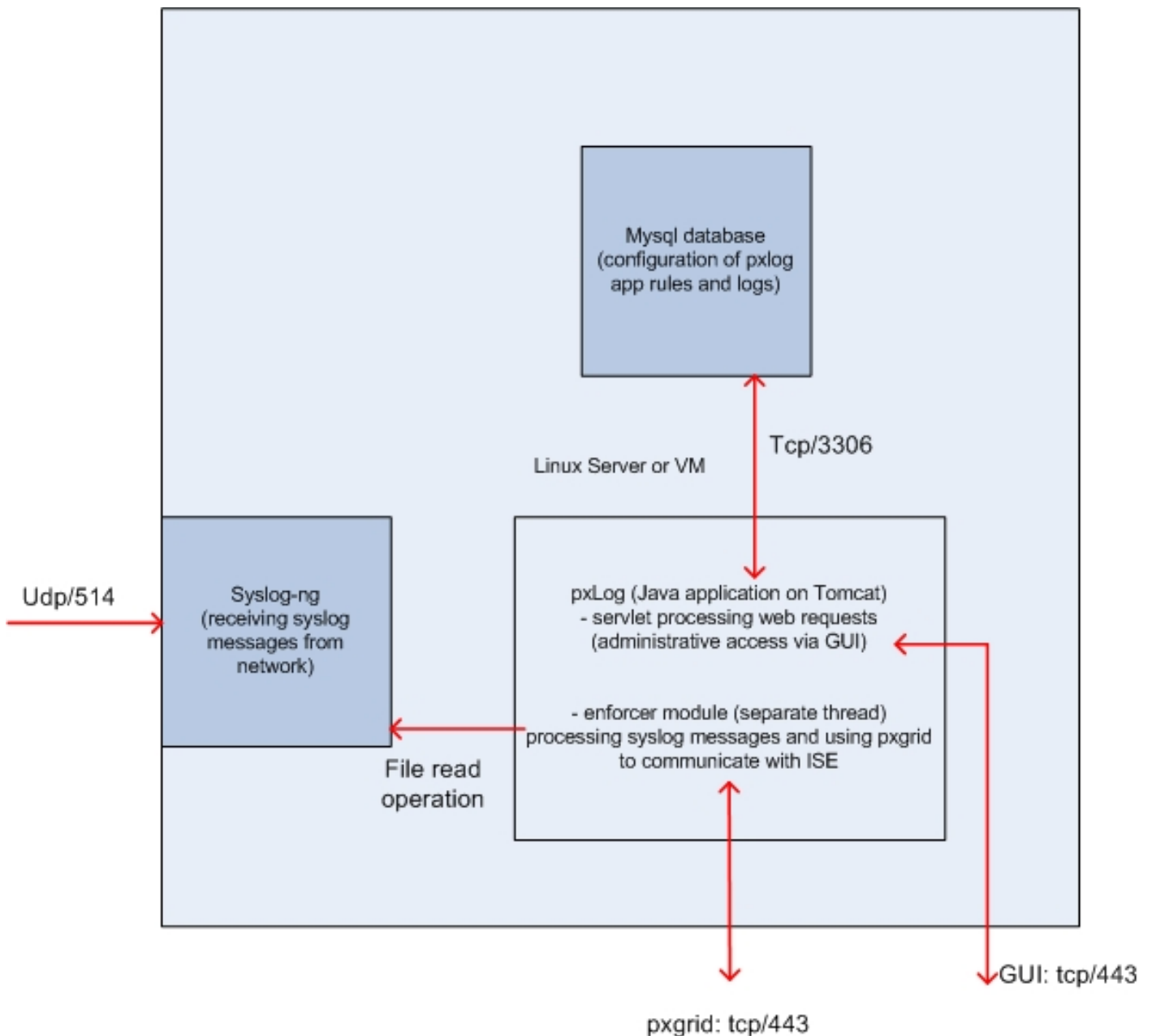
Aquí está el flujo de tráfico, como se ilustra en el diagrama de la red:

1. Un usuario de Microsoft Windows 7 conecta con el Switch y realiza la autenticación del 802.1x.
2. El Switch utiliza el ISE como el servidor del Authentication, Authorization, and Accounting (AAA). Se corresponde con la regla **de total acceso de la** autorización del **dot1x** y se concede el acceso a la red completo (DACL: PERMIT_ALL).
3. El usuario intenta conectar con la red de confianza y viola la regla del Snort.
4. Como consecuencia, el Snort envía una alerta a la aplicación del pxLog (vía el Syslog).
5. La aplicación del pxLog realiza la verificación contra su base de datos local. Se configura para coger los mensajes de Syslog enviados por el Snort y extraer la dirección IP del atacante. Entonces utiliza el pxGrid para enviar una petición hacia el ISE para quarantine la dirección IP del atacante (el ISE es regulador del pxGrid).

6. El ISE evalúa de nuevo su directiva de la autorización. Porque el punto final quarantined, la **sesión**: Se cumple la condición de la **cuarentena de los IGUALES de EPSStatus** y se corresponde con un diverso perfil de la autorización (**cuarentena del dot1x**). El ISE envía un CoA termina al Switch para terminar la sesión. Esto acciona la reautenticación y un nuevo ACL descargable (DACL) (PERMIT_ICMP) es aplicado, que proporciona el acceso a la red limitado al usuario final.
7. En esta etapa, el administrador pudo decidir al unquarantine el punto final. Esto se puede alcanzar vía el GUI del pxLog. Una vez más el mensaje del pxGrid hacia el ISE se envía.
8. El ISE realiza una operación similar como en el paso 6. Esta vez, el punto final quarantined no más y se proporciona el acceso total.

pxLog

Arquitectura



La solución es instalar un conjunto de las aplicaciones en una máquina de Linux:

1. La aplicación del pxLog escrita en las Javas y desplegada en el servidor de Tomcat. Esa aplicación consiste en:

Servlet ese solicitudes web de los procesos - Esto se utiliza para acceder el panel administrativo vía el buscador Web.

Módulo del guardián - Rosque que se comienza así como el servlet. El guardián lee los mensajes de Syslog del archivo (optimizado), procesa esos mensajes según las reglas configuradas, y ejecuta las acciones (como la cuarentena vía el pxGrid).

2. La base de datos MySQL que contiene la configuración para el pxLog (las reglas y los registros).

3. El servidor de Syslog que recibe los mensajes de Syslog de los sistemas externos y los escribe a un archivo.

Instalación

La aplicación del pxLog utiliza estas bibliotecas:

- jQuery (para el soporte de AJAX)
- JavaServer pagina la biblioteca estándar de la etiqueta (JSTL) (el modelo modelo del regulador de la visión (MVC), los datos se separa de la lógica: No se utiliza el código de la página de JavaServer (JSP) para rendir solamente, ningún código HTML en las clases Java)
- Log4j como subsistema del registro
- Conector de MySQL
- displaytag para las tablas de la representación/de clasificación
- pxGrid API por Cisco (actualmente alfa 147 de la versión)

Todas esas bibliotecas están en el directorio lib del proyecto tan allí no son ya ninguna necesidad de descargar más archivos del Java Archive (TARRO).

Para instalar la aplicación:

1. Desempaquete el directorio entero al directorio de Tomcat Webapp.
2. Edite el **archivo WEB-INF/web.xml**. El único cambio obligatorio es el serveripvariable, que deben señalar al ISE. También las Javas certifican KeyStores (uno para de confianza y uno para la identidad) pudieron ser generadas (en vez del valor por defecto). Esto es utilizada por el pxGrid API que utiliza la sesión de Secure Sockets Layer (SSL) con ambos los Certificados de cliente y servidor. Ambos lados de la necesidad de comunicación de presentar con el certificado y de necesitar confiarse en. Refiera a la sección de los requerimientos del protocolo del pxGrid para más información.
3. Asegurese el nombre de host ISE se resuelve correctamente en el pxLog (refiera al expediente en el Domain Name Server (DNS) o la **entrada de /etc/hosts**). Refiera a la sección de los requerimientos del protocolo del pxGrid para más información.
4. Configure la base de datos MySQL con el **script mysql/init.sql**. Las credenciales se pueden cambiar pero se deben reflejar en el **archivo WEB-INF/web.xml**.

Snort

Este artículo no se centra en ningún IPS específico, que es porqué solamente se proporciona una explicación abreviada.

El Snort se configura como en línea con el soporte DAQ. El tráfico se reorienta con los iptables:

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

Entonces, después del examen, se inyecta y se remite según las reglas iptable predeterminadas.

Se han configurado algunas reglas de encargo del Snort (el archivo de `/etc/snort/rules/test.rules` se incluye en la configuración global).

```
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)
```

El Snort envía un mensaje de Syslog cuando el Time to Live (TTL) del paquete es igual a 6 o el tamaño del payload está entre 666 y 686. El tráfico no es bloqueado por el Snort.

También los umbrales se deben configurar para asegurarse las alertas no se accionan demasiado a menudo (`/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
```

Entonces el servidor de Syslog señala a la máquina del pxLog (`/etc/snort/snort.conf`):

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

Para algunas versiones del Snort, hay bug relacionados con la configuración de syslog, y entonces las configuraciones predeterminadas podrían ser utilizadas que señalan al localhost y el Syslog-NG se podría configurar para remitir los mensajes específicos al host del pxLog.

ISE

Configuración

Personaje y certificado

1. Habilite el papel del pxGrid, que se inhabilita en el ISE por abandono, bajo la **administración** > **despliegue**:

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**

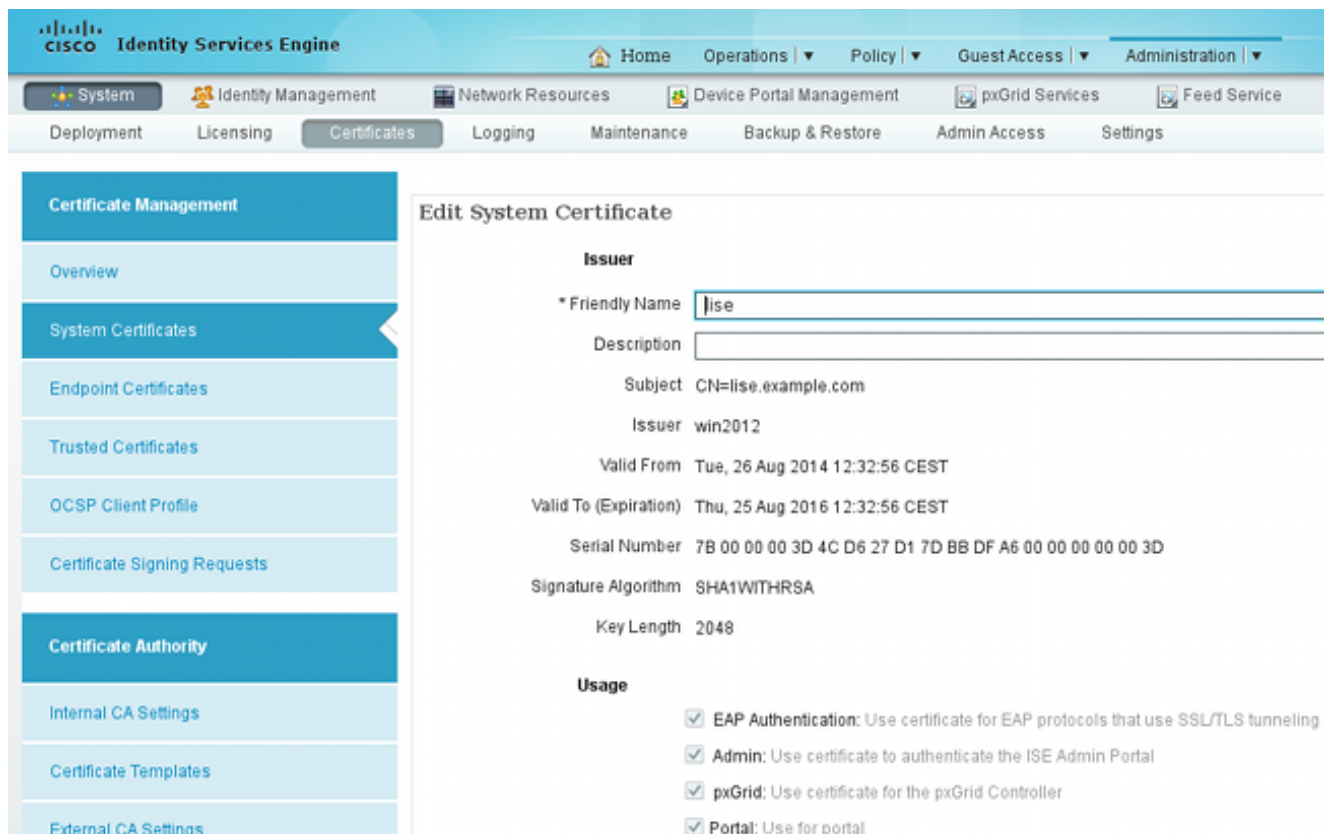
- Monitoring Role Other Monitoring Node

- Policy Service
 - Enable Session Services ⓘ
 Include Node in Node Group ⓘ

 - Enable Profiling Service

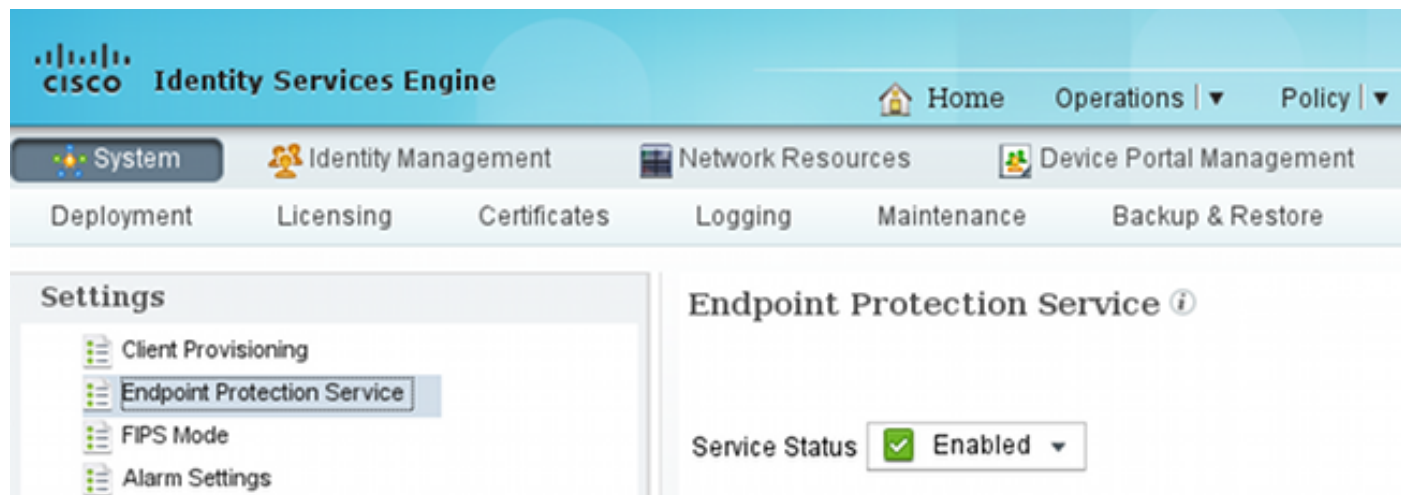
- pxGrid ⓘ

2. Verifique si los Certificados se utilizan para el pxGrid conforme a la **administración > a los Certificados > a los Certificados del sistema**:



Servicio de protección del punto final (EP)

Los EP se deben habilitar (inhabilitado por abandono) de la **administración > de las configuraciones**:



Esto permite que usted utilice las funciones de la cuarentena/del unquarantine.

Reglas de la autorización

Authorization Policy

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](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

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

Se encuentra la primera regla solamente cuando el punto final quarantine. El acceso entonces limitado es aplicado dinámicamente por el CoA RADIUS. El Switch también se debe agregar a los dispositivos de red con el secreto compartido correcto.

Troubleshooting

El estatus del pxGrid se puede verificar con el 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

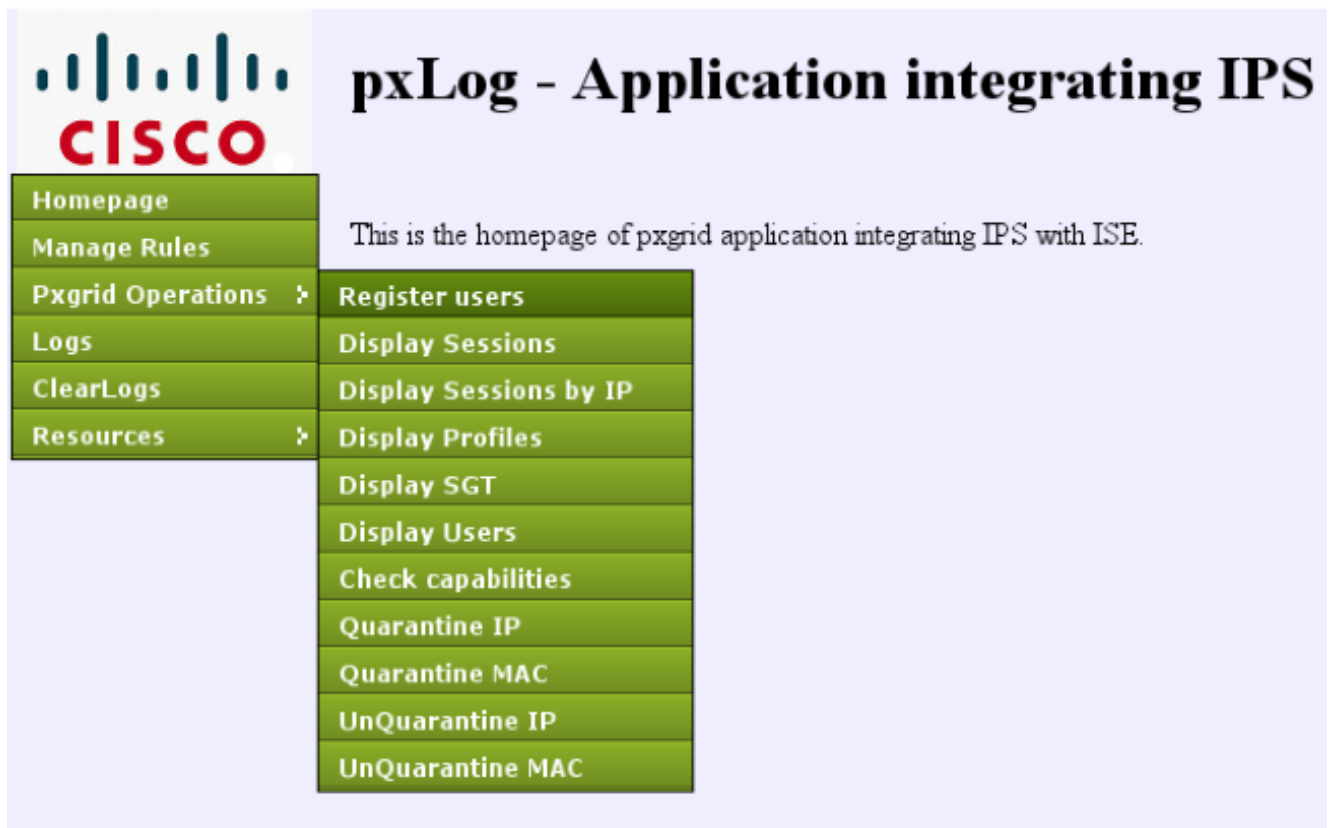
Hay también debugs separados para el pxGrid (la **administración > configuración > pxGrid del registro del registro > del debug**). Los archivos del debug se salvan en el directorio del pxGrid. Los datos más importantes están en el **pxgrid/pxgrid-jabberd.log** y el **pxgrid/pxgrid-controller.log**.

Prueba

Step1. Registro para el pxGrid

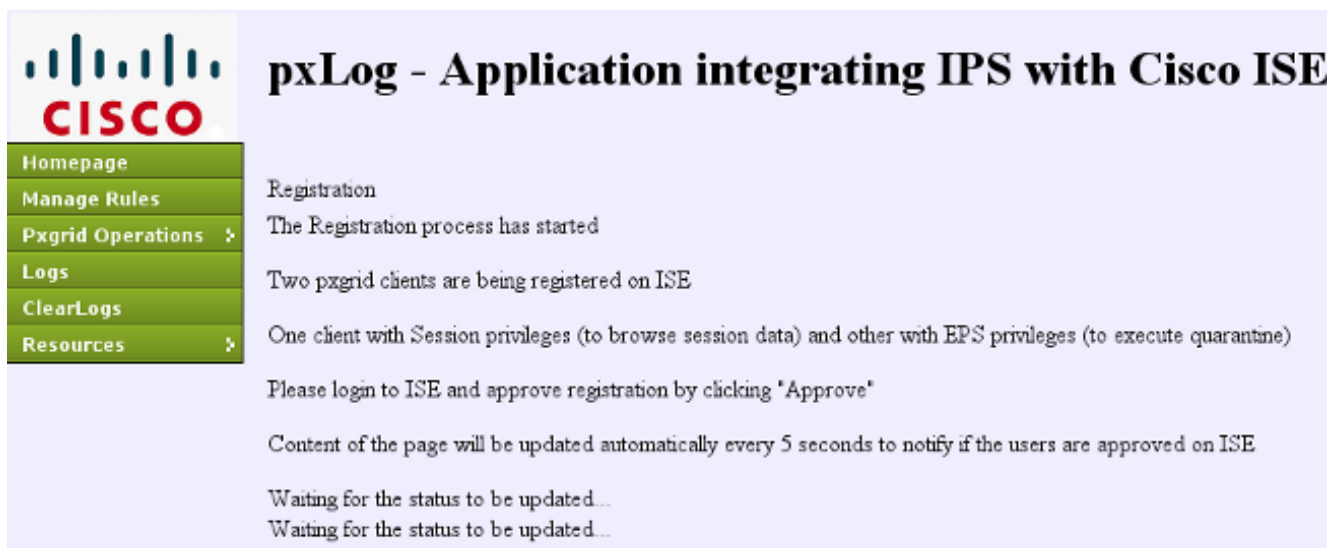
La aplicación del pxLog se despliega automáticamente cuando Tomcat comienza.

1. Para utilizar el pxGrid, registre a dos usuarios en el ISE (uno con el acceso de la sesión, y uno con la cuarentena). Esto se puede completar de los **usuarios de las operaciones >** del registro de Pxgrid:



The screenshot shows the pxLog application interface. On the left is a navigation menu with the following items: Homepage, Manage Rules, Pxgrid Operations (with a dropdown arrow), Logs, ClearLogs, and Resources (with a dropdown arrow). The main content area is titled "pxLog - Application integrating IPS" and contains the text "This is the homepage of pxgrid application integrating IPS with ISE." Below this text is a dropdown menu for "Pxgrid Operations" with 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.

El registro comienza automáticamente:



The screenshot shows the pxLog application interface during the registration process. The title is "pxLog - Application integrating IPS with Cisco ISE". The navigation menu is the same as in the previous screenshot. The main content area displays the following information: "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", and two instances of "Waiting for the status to be updated...".

2. En esta etapa, es necesario aprobar a los usuarios registrados en el ISE (la aprobación auto se inhabilita por abandono):

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
<input checked="" type="checkbox"/> pxclient_session	test	Capabilities(0 Pub, 0 Sub)	Pending	Session
<input checked="" type="checkbox"/> pxclient_eps	test	Capabilities(0 Pub, 0 Sub)	Pending	EPS

Después de la aprobación, el pxLog notifica automáticamente al administrador (vía una llamada de AJAX):

```
Session user: pxclient_session registered and approved succesfully
EPS user: pxclient_eps registered and approved succesfully
```

El ISE muestra el estatus para esos dos usuarios como en línea u off-liné (no pendiente más).

Step2. el pxLog gobierna la configuración

el pxLog debe procesar los mensajes de Syslog y ejecutar las acciones basadas en él. Para agregar una nueva regla, selecta **maneje las reglas**:

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

pxLog - Application integrating

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

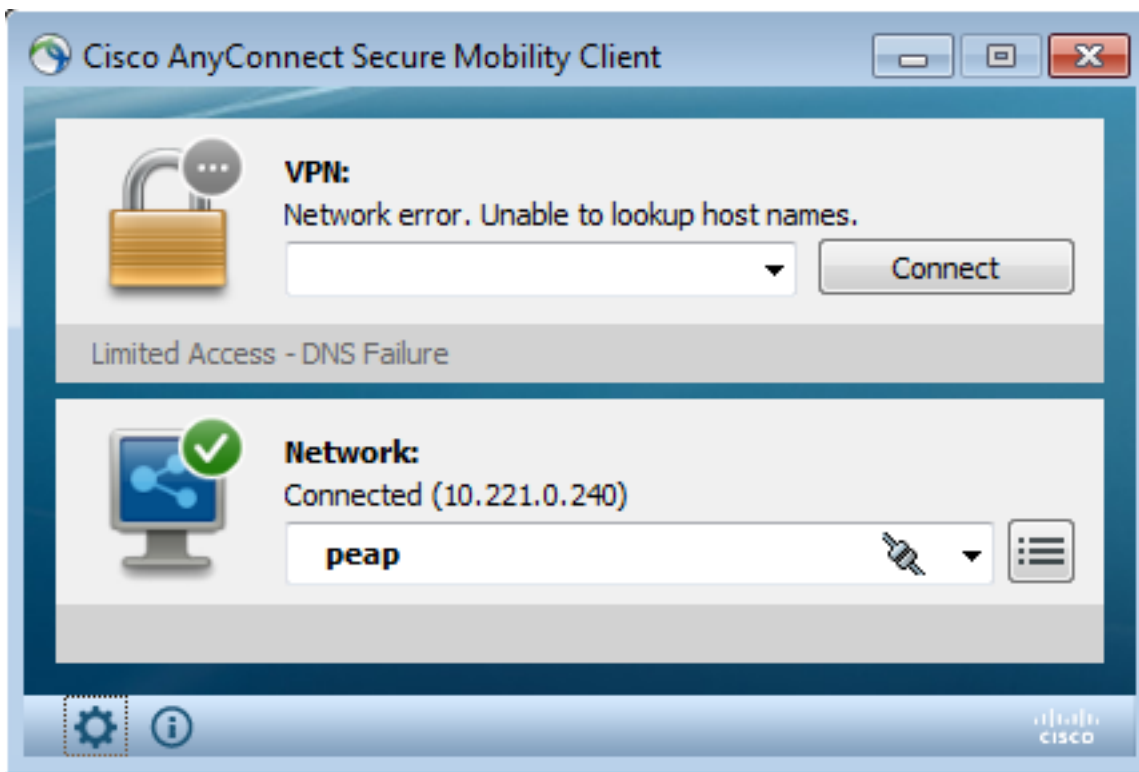
Rule Id	Rule string	Action
19	snort[<input type="button" value="Remove"/>
New Rule	<input type="text"/>	<input type="button" value="Add New Rule"/>

Ahora el módulo del guardián busca esta expresión normal (regexp) en el mensaje de Syslog: "snort [". Si está encontrado, busca todos los IP Addresses y selecciona el que está antes el más reciente. Esto hace juego la mayoría de las soluciones acerca de la seguridad. Refiera a la

sección del Syslog para más información. Esa dirección IP (atacante) quarantined vía el pxGrid. También una regla más granular pudo ser utilizada (por ejemplo, puede ser que incluya el número de la firma).

Step3. Primera sesión del dot1x

La estación de Microsoft Windows 7 inicia una sesión atada con alambre del dot1x. Cisco Anyconnect NAM se ha utilizado como supplicant. Se configura el método Protocolo-prottegido autenticación ampliable EAP (EAP-PEAP).



Se selecciona el perfil **de total acceso de la** autorización del dot1x ISE. El Switch descarga la lista de acceso para conceder el acceso total:

```
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
```

Step4. Microsoft Windows PC envía el paquete que acciona la alarma

Esto muestra qué sucede si usted envía de un paquete de Microsoft Windows con TTL = 7:

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

Que el valor decremented en el Snort en el encadenamiento de la expedición y una alarma se aumenta. Como consecuencia, un mensaje de Syslog hacia el pxLog se envía:

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

Step5. pxLog

El pxLog recibe el mensaje de Syslog, lo procesa, y lo pide para quarantine esa dirección IP. Esto puede ser confirmada si usted marca los registros:

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

Step6. Cuarentena ISE

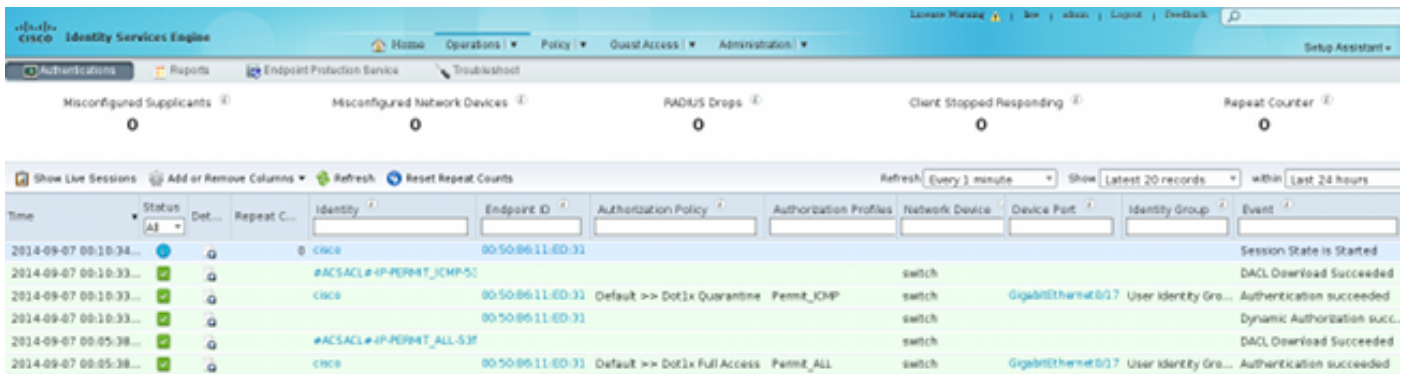
El ISE señala que la dirección IP quarantined:

Endpoint Protection Service Audit

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	0A01000C00037E6B8267
2014-09-07 00:10:32.9	00:50:B6:11:ED:31	10.221.0.240	Quarantine	RUNNING	16	0A01000C00037E6B8267

Como consecuencia, revisa la directiva de la autorización, elige la cuarentena, y envía el CoA RADIUS para poner al día el estatus de autorización en el Switch para ese punto final específico.



Ése es el CoA termina el mensaje que fuerza el supplicant para iniciar una nueva sesión y para conseguir el acceso limitado (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)
  
```

El resultado se puede confirmar en el Switch (acceso limitado para el punto final):

```

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
```

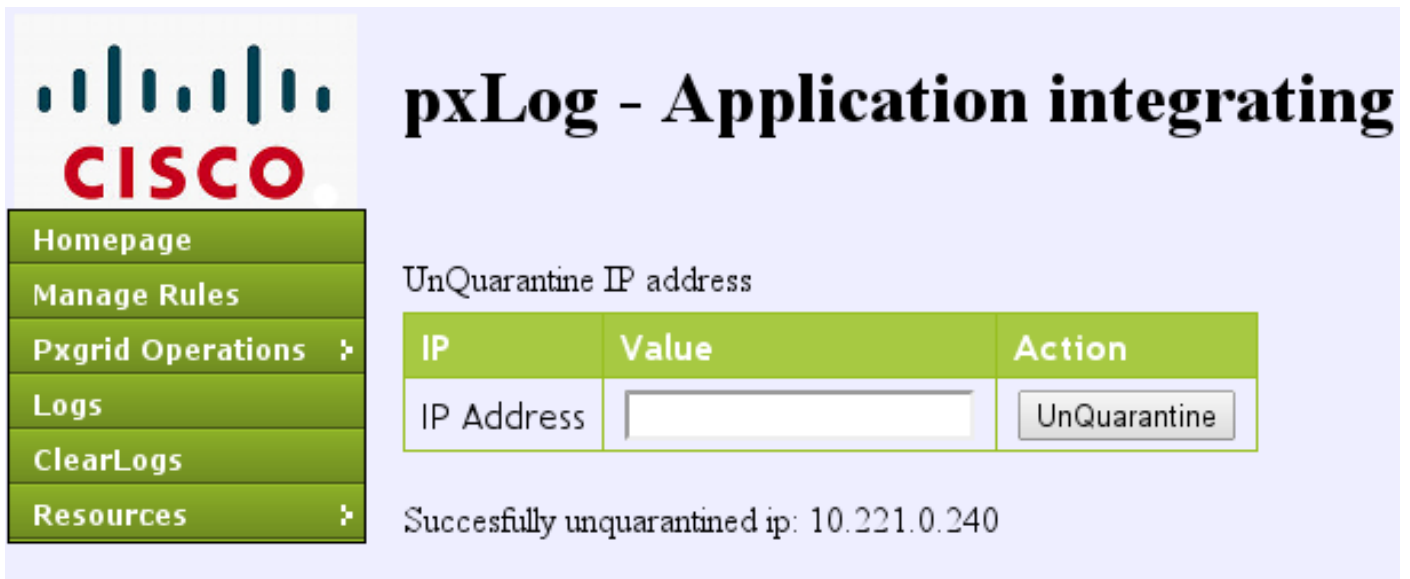
Runnable methods list:

```
Method State
dot1x Authc Success
```

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

Step7. pxLog Unquarantine

En esta etapa, el administrador decide al unquarantine que punto final:



The screenshot displays the Cisco pxLog interface for application integration. On the left is a navigation menu with the following items: Homepage, Manage Rules, Pxgrid Operations (with a dropdown arrow), Logs, ClearLogs, and Resources (with a dropdown arrow). The main content area is titled "pxLog - Application integrating" and features a section for "UnQuarantine IP address". This section contains a table with three columns: "IP", "Value", and "Action". The "IP" column contains the text "IP Address". The "Value" column contains an empty text input field. The "Action" column contains a button labeled "UnQuarantine". Below the table, a status message reads "Successfully unquarantined ip: 10.221.0.240".

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

Successfully unquarantined ip: 10.221.0.240

La misma operación se puede ejecutar directamente del ISE:

Endpoint Protection Service

Endpoint Operation

* IP Address (Example: 1.2.3.4)
 * MAC Address
 * Operation Quarantine

Update Information

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

Last Operation Status

Step8. ISE Unquarantine

El ISE revisa las reglas y pone al día otra vez el estatus de autorización en el Switch (se concede el acceso a la red completo):

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-1				switch			DACL Download Succeeded
2014-09-07 00:21:10...	●			osco	00:50:86:11:ED:31	Default => Dat1x 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_CHP				switch			DACL Download Succeeded
2014-09-07 00:10:33...	●			osco	00:50:86:11:ED:31	Default => Dat1x Quarantine	Permit_CHP	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-1				switch			DACL Download Succeeded
2014-09-07 00:05:38...	●			osco	00:50:86:11:ED:31	Default => Dat1x Full Access	Permit_ALL	switch	GigabitEthernet0/17	User Identity Gro...	Authentication succeeded

El informe confirma:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. The main content area is titled "Endpoint Protection Service Audit" and displays a table of logs from 09/07/2014 12:00:00 AM to 09/07/2014 12:23:10 AM. The table has columns for Logged At, Endpoint ID, IP Address, Operation, Operation Status, Operation ID, and Audit Session ID.

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

funciones del pxLog

La aplicación del pxLog se ha escrito para demostrar las funciones del pxGrid API. Le permite a:

- Registre la sesión y a los usuarios EP en el ISE
- Descargue la información sobre todas las sesiones activas en el ISE
- Descargue la información sobre una sesión activa específica en el ISE (por la dirección IP)
- Descargue la información sobre un usuario activo específico en el ISE (por el nombre de usuario)
- Visualice la información sobre todos los perfiles (el profiler)
- Visualice la información sobre las etiquetas del grupo de seguridad de TrustSec (SGTs) definidas en el ISE
- Marque la versión (las capacidades del pxGrid)
- Quarantine basado en el IP o la dirección MAC
- Unquarantine basó en el IP o la dirección MAC

Más funciones se planean en el futuro.

Aquí está algún screenshots del ejemplo del pxLog:

The screenshot shows the pxLog application interface. The title is "pxLog - Application integrating IPS with". Below the title, there is a list of users with active sessions downloaded from ISE via pxgrid. The table has columns for User and Groups.

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

The screenshot shows the pxLog application interface. The title is "pxLog - Application integrating IPS with Cisco ISE using pxgrid". Below the title, there is a list of active sessions on ISE. The table has columns for Id, User, Domain, MAC, State, ESPStatus, SGT, Profile, NAS IP, NAS Port, and AVP.

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

requerimientos del protocolo del pxGrid

Grupos

El cliente (usuario) puede ser un miembro de un en un momento del grupo. Los dos grupos más de uso general son:

- Sesión - Utilizado para hojear/información de la descarga sobre las sesiones/los perfiles/SGTs
- EP - Utilizado para ejecutar la cuarentena

Certificados y Javas KeyStore

Según lo mencionado previamente, el regulador de ambas aplicaciones de cliente, del pxLog y del pxGrid (ISE), debe tener Certificados configurados para comunicar. La aplicación del pxLog mantiene éstos los archivos de KeyStore de las Javas:

- **almacén/client.jks** - Incluye el cliente y los Certificados del Certificate Authority (CA)
- **almacén/root.jks** - Incluye el encadenamiento ISE: Identidad del nodo de la supervisión y del troubleshooting (MNT) y el certificado de CA

Los archivos son protegidos por la contraseña (valor por defecto: cisco123). La ubicación del archivo y las contraseñas se pueden cambiar en **WEB-INF/web.xml**.

Aquí están los pasos para generar una nueva Java KeyStore:

1. Para crear un keystore (de confianza) de la raíz, importe el certificado de CA (**cert-ca.der debe estar en el formato DER**):

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

2. Cuando usted crea un nuevo keystore, elija una contraseña, que se utiliza más adelante para acceder el keystore.
3. Importe el certificado de identidad MNT al keystore de la raíz (**cert-mnt.der es el certificado de identidad tomado del ISE y debe estar en el formato DER**):

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

4. Para crear el keystore del cliente, importe el certificado de CA:

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

5. Cree una clave privada en el keystore del cliente:

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

6. Genere un pedido de firma de certificado (CSR) en el keystore del cliente:

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

7. Firme el **cert-client.csr** e importe el certificado del cliente firmado:

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

8. Verifique que ambos keystores contengan los Certificados correctos:

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

Caution: Cuando el nodo ISE 1.3 se actualiza, hay una opción para guardar el certificado de identidad, pero se quita la firma de CA. Como consecuencia, el ISE actualizado utiliza un nuevo certificado pero nunca asocia el certificado de CA en el mensaje SSL/ServerHello. Esto acciona el error en el cliente que espera (según el RFC) ver un encadenamiento lleno.

Hostname

El pxGrid API para varias funciones (como la descarga de la sesión) realiza la validación adicional. El cliente entra en contacto el ISE y recibe el nombre de host ISE, que es definido por el comando hostname en el CLI. Entonces, el cliente intenta realizar la resolución de DNS para ese nombre de host e intenta entrar en contacto y traer los datos de esa dirección IP. Si la resolución de DNS para el nombre de host ISE falla, el cliente no intenta conseguir ningunos datos.

Caution: Note que solamente el nombre de host está utilizado para esta resolución, que es **lise** en este escenario, no el nombre de dominio completo (FQDN), que es **lise.example.com** en este escenario.

Observe para los desarrolladores

Cisco publica y soporta el pxGrid API. Hay un paquete nombrado como esto:

```
pxgrid-sdk-1.0.0-167
```

Dentro de hay:

- archivos JAR del pxGrid con las clases, que se pueden decodificar fácilmente a los archivos de las Javas para marcar el código
- Javas KeyStores de la muestra con los Certificados
- Secuencias de comandos de ejemplo que utilizan los classess de las Javas de la muestra que utilizan el pxGrid

Syslog

Aquí está la lista de soluciones acerca de la seguridad que envíen los mensajes de Syslog con la dirección IP del atacante. Éstos se pueden integrar fácilmente con el pxLog mientras usted utilice la regla correcta del regexp en la configuración.

Snort

El Snort envía las alertas del Syslog en este formato:

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

Aquí tiene un ejemplo:

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

La dirección IP del atacante es siempre la segunda antes la más reciente (destino). Es simple construir un regexp granular para una firma específica y extraer la dirección IP del atacante. Aquí está un regexp del ejemplo para la firma 100124 y el Internet Control Message Protocol (ICMP) del mensaje:

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

Examen adaptante del dispositivo de seguridad de Cisco (ASA)

Cuando el ASA se configura para el examen HTTP (ejemplo), el mensaje de Syslog correspondiente parece esto:

```
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
```

Un regexp granular se podía utilizar otra vez para filtrar esos mensajes y extraer la dirección IP del atacante, el segundo antes la más reciente.

Sistemas de prevención de intrusiones de la última generación de Cisco Sourcefire (NGIPS)

Aquí está un mensaje de ejemplo enviado por el sensor de 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
```

Tan otra vez, es simple extraer la dirección IP del atacante porque la misma lógica se aplica. También se proporciona el nombre de la directiva y la firma, así que la regla del pxLog puede ser granular.

NetScreen del enebro

Aquí está un mensaje de ejemplo enviado por la más viejas detección de intrusos y prevención (IDP) del enebro:

```
dayId="20061012" recordId="0" timeRecv="2006/10/12
21:52:21" timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0"
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"
```

La dirección IP del atacante se puede extraer de la misma manera.

Enebro JunOS

JunOS es similar:

```
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
```

Iptables de Linux

Aquí están algunos iptables de Linux del ejemplo.

```
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
```

Usted puede enviar la Información de syslog para cualquier tipo de paquete con las funciones avanzadas proporcionadas por los módulos iptable como la conexión que sigue, los xtables, los rpfilters, coincidencia de patrones, y así sucesivamente.

FreeBSD IPFirewall (IPFW)

Aquí está un mensaje de ejemplo para IPFW que bloquea los fragmentos:

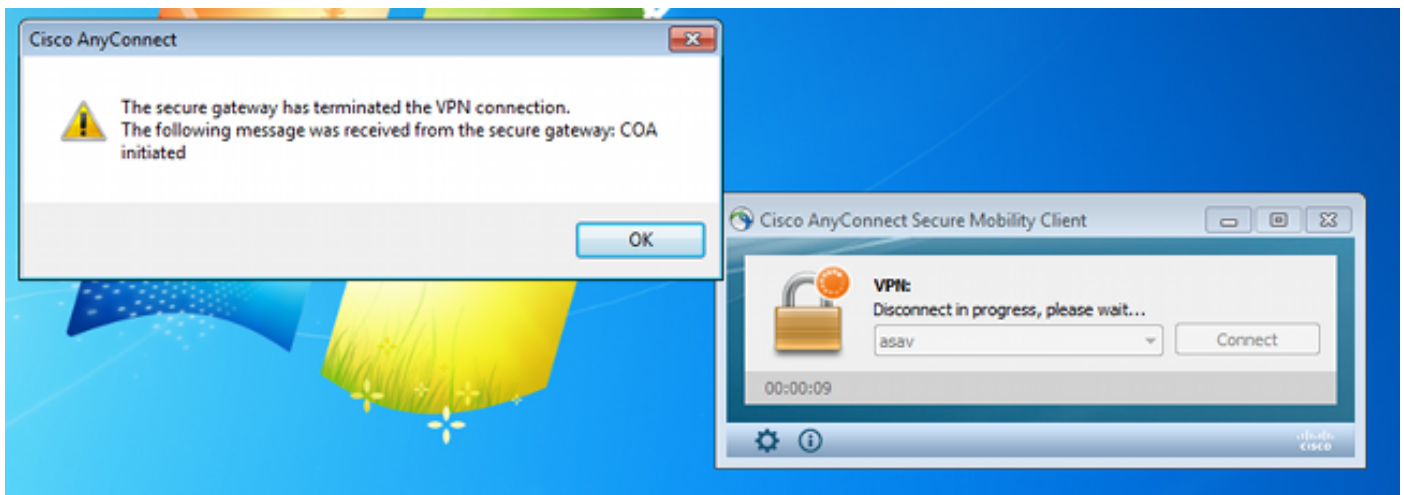
```
Sep 7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0
(frag 52639:519@1480)
```

Disposición VPN y dirección CoA

El ISE puede reconocer el tipo de sesiones en términos de dirección CoA.

- Para puente atado con alambre de la autenticación 802.1x/MAC (MAB), el ISE envía el CoA reauthenticate, que acciona una segunda autenticación.
- Para una Tecnología inalámbrica 802.1x/MAB, el ISE envía el CoA termina, que acciona una segunda autenticación.
- Para un ASA VPN, el ISE envía un CoA con un nuevo DACL asociado (ninguna segunda autenticación).

El módulo EP es simple. Cuando ejecuta una cuarentena, envía siempre un CoA termina el paquete. Para las sesiones atadas con alambre/inalámbricas, no es un problema (todos los suplicantes del 802.1x pueden transparente iniciar una segunda sesión EAP). Pero cuando el ASA recibe el CoA termine, él cae a la sesión de VPN y presentan el usuario final con esto:



Hay dos Soluciones posibles para forzar el AnyConnect VPN para volver a conectar automáticamente (configurado en el perfil XML):

- Autoreconnect, que trabaja solamente cuando usted pierde la conexión con el gateway de VPN, no para la terminación administrativa
- Siempre-en, que trabaja y las fuerzas AnyConnect para restablecer automáticamente la sesión

Incluso cuando se establece la nueva sesión, el ASA elige la nueva auditoría-sesión-identificación. Desde el punto de vista ISE, esto es una nueva sesión y no hay ocasión de encontrar la regla de la cuarentena. También para los VPN, no es posible utilizar la dirección MAC del punto final como la identidad, en comparación con el dot1x atado con alambre/inalámbrico.

La solución es forzar los EP para comportarse como el ISE y para enviar el tipo correcto de CoA basado en la sesión. Estas funciones serán introducidas en la versión 1.3.1 ISE.

Partners y soluciones del pxGrid

Aquí está una lista de Partners y de soluciones del pxGrid:

- LogRhythm (información sobre seguridad y administración de eventos (SIEM)) - Soporta la transferencia representativa del estado (RESTO) API

- Splunk (SIEM) - Soporta el RESTO API
- HP Arcsight (SIEM) - Soporta el RESTO API
- Centinela NetIQ (SIEM) - Planes para soportar el pxGrid
- Lancope StealthWatch (SIEM) - Planes para soportar el pxGrid
- Cisco Sourcefire - Planes para soportar el pxGrid 1HCY15
- Dispositivo de seguridad de la red de Cisco (WSA) - Planes para soportar el pxGrid en abril de 2014

Aquí están otros Partners y soluciones:

- Sostenible (evaluación de vulnerabilidades)
- Emulex (captura de paquetes y medicina legal)
- Redes de Bayshore (Data Loss Prevention (DLP) y Internet de la directiva de las cosas (IoT))
- Identidad del ping muestra (de la identidad y de la Administración de acceso (soy) /Single encendido (SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (Administración de dispositivo móvil del amd SIEM (MDM))

Refiera al [catálogo de las soluciones del mercado](#) para la lista completa de soluciones acerca de la seguridad.

ISE API: RESTO contra EREST contra el pxGrid

Hay tres tipos de API disponibles en la versión 1.3 ISE.

Aquí está una comparación:

	RESTO	Externo relajante	pxGrid
Autenticación de cliente	nombre de usuario + contraseña (auth básico HTTP)	nombre de usuario + contraseña (auth básico HTTP)	certifica
Separación del privilegio	no	limitado (ERS Admin)	sí (grup
El acceder	MNT	MNT	MNT
Transporte	tcp/443 (HTTPS)	tcp/9060 (HTTPS)	tcp/522
Método HTTP	GET	GET/POST/PUT	(XMPP) GET/PC
Habilitado por abandono	sí	no	no
Número de operaciones	pocos	muchos	pocos
El CoA termina	soportado	no	soporta
El CoA Reauthenticate	soportado	no	soporta
Operaciones de usuario	no	sí	no
Operaciones del punto final	no	sí	no
Operaciones del grupo de la identidad del punto final	no	sí	no
Cuarentena (IP, MAC)	no	no	sí
UnQuarantine (IP, MAC)	no	no	sí
PortBounce/apaga	no	no	sí
Operaciones de Usuario invitado	no	sí	no
Operaciones del portal del invitado	no	sí	no
Operaciones del dispositivo de red	no	sí	no

Operaciones del grupo de dispositivos de red no sí no

* Las aplicaciones de la cuarentena unificaron el soporte CoA de la versión 1.3.1 ISE.

Descargas

el pxLog se puede descargar de [Sourceforge](#).

El Software Development Kit (SDK) es ya incluido. Para la última documentación SDK y API para el pxGrid, entre en contacto su partner o al equipo de cuenta de Cisco.

Información Relacionada

- [RESTO API de Cisco ISE 1.2](#)
- [Cisco ISE 1.2 API relajante externo](#)
- [Guía de administradores de Cisco ISE 1.3](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)