ISE Version 1.3 pxGrid Integration with IPS pxLog Application

Document ID: 118688

Contributed by Michal Garcarz, Cisco TAC Engineer.
Dec 23, 2014

Contents

Related Information

Introduction

The Identity Services Engine (ISE) Version 1.3 supports a new API called pxGrid. This modern and flexible protocol that supports authentication, encryption, and privileges (groups) allows for easy integration with other security solutions. This document describes the usage of pxLog application which has been written as a proof of concept. pxLog is able to receive syslog messages from Intrusion Prevention System (IPS) and send pxGrid messages to the ISE in order to quarantine the attacker. As a result, ISE uses RADIUS Change of Authorization (CoA) in order to change the authorization status of the endpoint that limits the network access. All of this happens transparently to the end user.

For this example, Snort has been used as the IPS, but any other solution could be used. Actually it does not have to be an IPS. All that is required is to send the syslog message to pxLog with the IP address of the attacker. This creates a possibility for the integration of a large number of solutions.

This document also presents how to troubleshoot and test pxGrid solutions, with the typical problems and limitations.

Disclaimer: The pxLog application is not supported by Cisco. This article has been written as a proof of concept. The primary purpose was to use it during the betatesting of pxGrid implementation on the ISE.

Prerequisites

Requirements

Cisco recommends that you have experience with Cisco ISE configuration and basic knowledge of these topics:

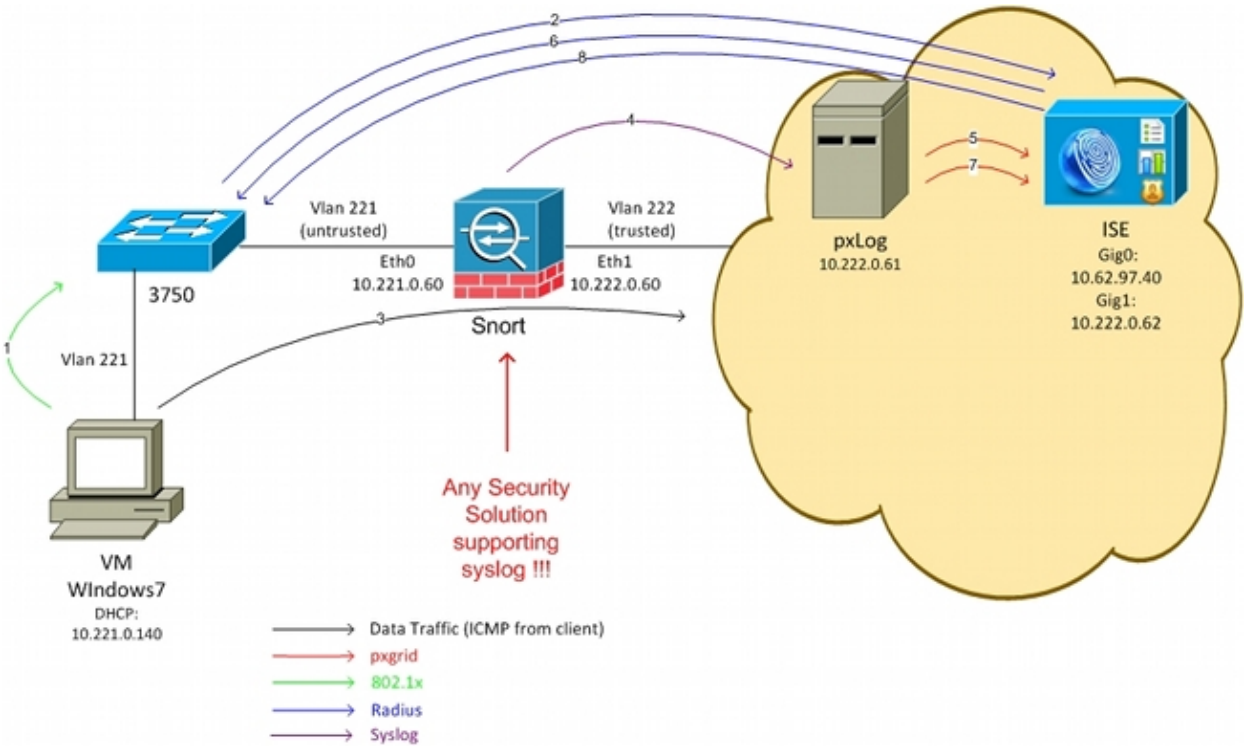
- ISE deployments and authorization configuration
- CLI configuration of Cisco Catalyst Switches

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco Catalyst 3750X Series Switch Software, Versions 15.0 and Later
- Cisco ISE Software, Versions 1.3 and Later
- Cisco AnyConnect Mobile Security with Network Access Manager (NAM), Version 3.1 and Later
- Snort Version 2.9.6 with Data Acquisition (DAQ)
- pxLog Application Installed on Tomcat 7 with MySQL Version 5

Network Diagram and Traffic Flow



Here is the traffic flow, as illustrated in the network diagram:

1. A Microsoft Windows 7 user connects to the switch and performs 802.1x authentication.

2. The switch uses the ISE as the Authentication, Authorization, and Accounting (AAA) server. The ***Dot1x Full Access*** authorization rule is matched and full network access is granted (DACL: PERMIT_ALL).

3. The user tries to connect with the trusted network and violates the Snort rule.

4. As a result, Snort sends an alert to the pxLog application (via syslog).

5. The pxLog application performs verification against its local database. It is configured in order to catch syslog messages sent by Snort and extract the IP address of the attacker. Then it uses pxGrid to send a request towards the ISE in order to quarantine the attacker IP address (the ISE is a pxGrid controller).

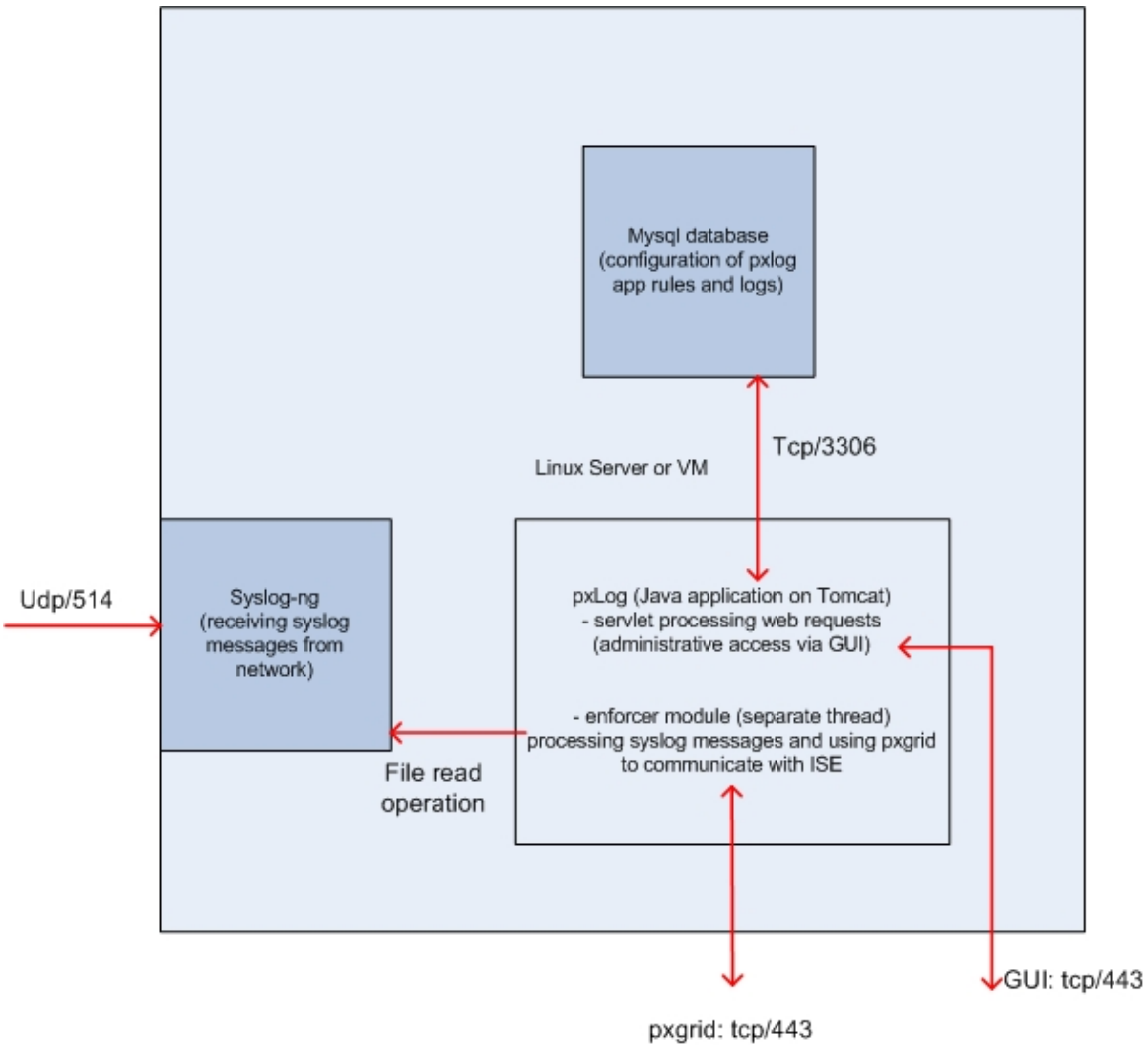
6. The ISE re−evaluates its authorization policy. Because the endpoint is quarantined, the ***Session:EPSStatus EQUALS Quarantine*** condition is met and a different authorization profile is matched (***Dot1x Quarantine***). The ISE sends a CoA Terminate to the switch in order to terminate the session. This triggers the re−authentication and a new Downloadable ACL (DACL) (PERMIT_ICMP) is applied, which provides the limited network access to the end user.

7. At this stage, the administrator might decide to unquarantine the endpoint. This can be achieved via the GUI of pxLog. Again, the pxGrid message towards the ISE is sent.

8. The ISE performs a similar operation as in Step 6. This time, the endpoint is no longer quarantined and full access is provided.

pxLog

Architecture



The solution is to install a set of applications on a Linux machine:

1. The pxLog application written in Java and deployed on the Tomcat server. That application consists of:

    - ♦ Servlet that processes web requests − This is used in order to access the administrative panel via the web browser.

    - ♦ Enforcer module − Thread that is started together with servlet. The Enforcer reads syslog messages from the file (optimized), processes those messages as per the configured rules, and executes actions (like quarantine via pxGrid).

2. The MySQL database that contains the configuration for pxLog (rules and logs).

3. The syslog server that receives syslog messages from external systems and writes them to a file.

Installation

The pxLog application uses these libraries:

- jQuery (for AJAX support)
- JavaServer Pages Standard Tag Library (JSTL) (Model View Controller (MVC) model, data is separated from logic: JavaServer Page (JSP) code is used to render only, no HTML code in Java classes)
- Log4j as a logging subsystem
- MySQL connector
- displaytag for rendering/sorting tables
- pxGrid API by Cisco (currently Version alpha 147)

All of those libraries are already in the lib directory of the project so there is no need to download any more Java ARchive (JAR) files.

In order to install the application:

1. Unpack the whole directory to the Tomcat Webapp directory.

2. Edit the ***WEB−INF/web.xml*** file. The only required change is the ***serverip*** variable, which should point to the ISE. Also the Java Certificate KeyStores (one for trusted and one for identity) might be generated (instead of the default). This is used by the pxGrid API that uses the Secure Sockets Layer (SSL) session with both the client and server certificates. Both sides of the communication need to present with the certificate and need to trust each other. Refer to the pxGrid Protocol Requirements section for more information.

3. Make sure the ISE hostname is resolved correctly on pxLog (refer to the record in the Domain Name Server (DNS) or ***/etc/hosts entry***). Refer to the pxGrid Protocol Requirements section for more information.

4. Configure the MySQL database with the ***mysql/init.sql*** script. Credentials can be changed but should be reflected in the ***WEB−INF/web.xml*** file.

Snort

This article does not focus on any specific IPS, which is why only a brief explanation is provided.

Snort is configured as inline with DAQ support. Traffic is redirected with iptables:

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

Then, after inspection, it is injected and forwarded as per default iptable rules.

A few custom Snort rules have been configured (the ***/etc/snort/rules/test.rules*** file is included in the global configuration).

```
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)
```

Snort sends a syslog message when the Time To Live (TTL) of the packet is equal to 6 or the size of the payload is between 666 and 686. Traffic is not blocked by Snort.

Also thresholds should be set up to make sure the alerts are not triggered too often (***/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
```

Then the syslog server points to the pxLog machine (***/etc/snort/snort.conf***):

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

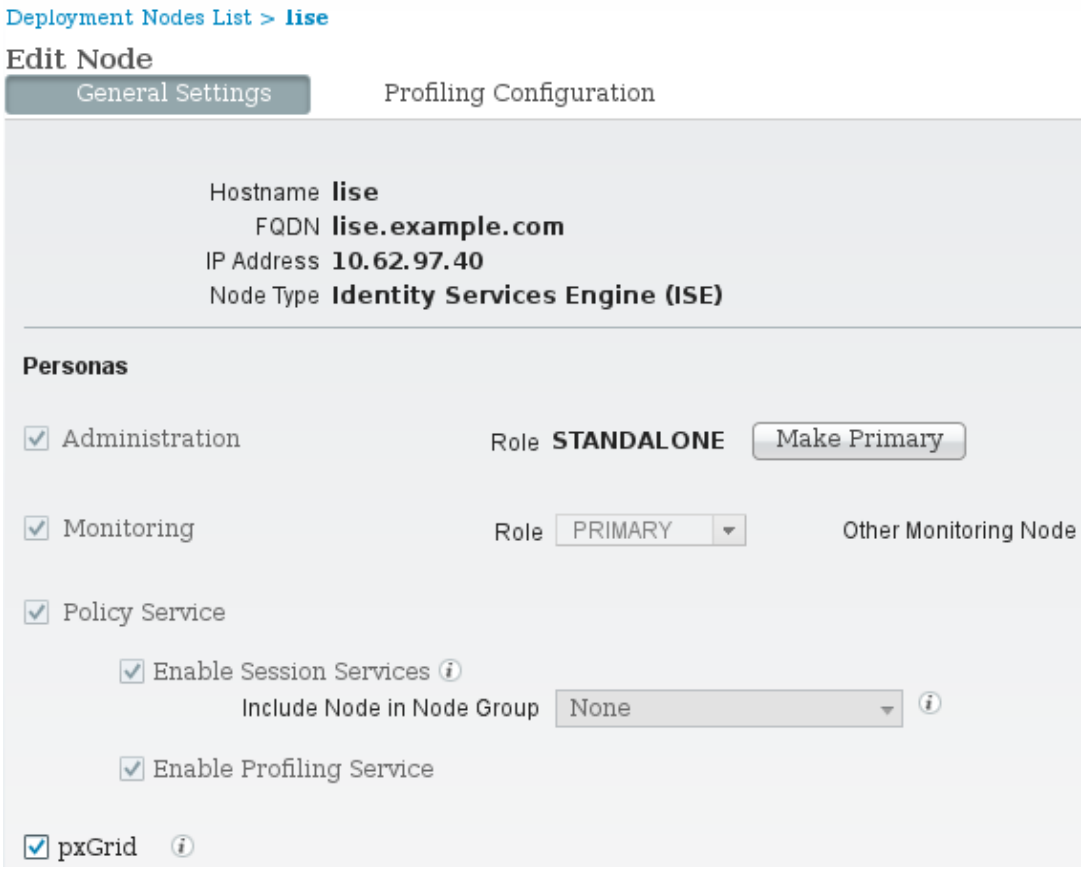
For some versions of Snort, there are bugs related to the syslog configuration, and then the default settings could be used that point to the localhost and syslog−ng could be configured in order to forward specific messages to the pxLog host.

ISE

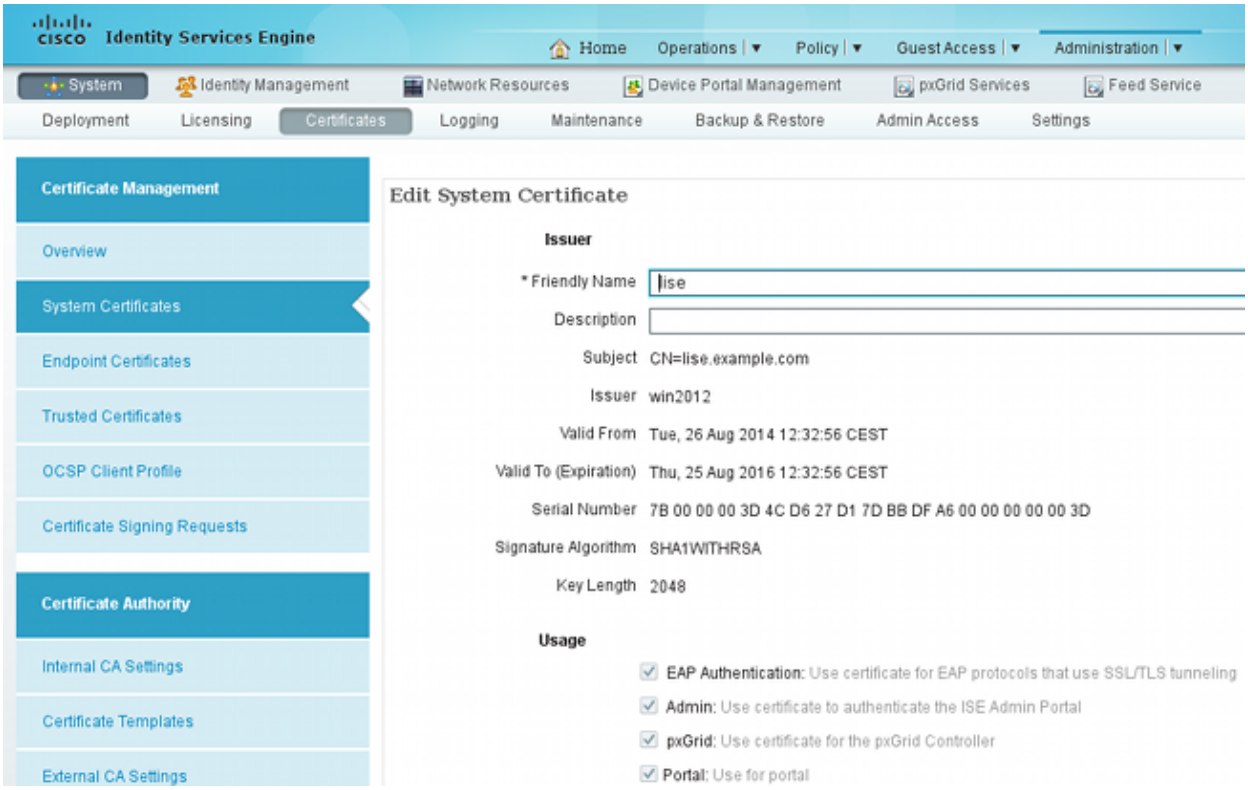
Configuration

Persona and Certificate

1. Enable the pxGrid role, which is disabled on the ISE by default, under ***Administration*** > ***Deployment***:

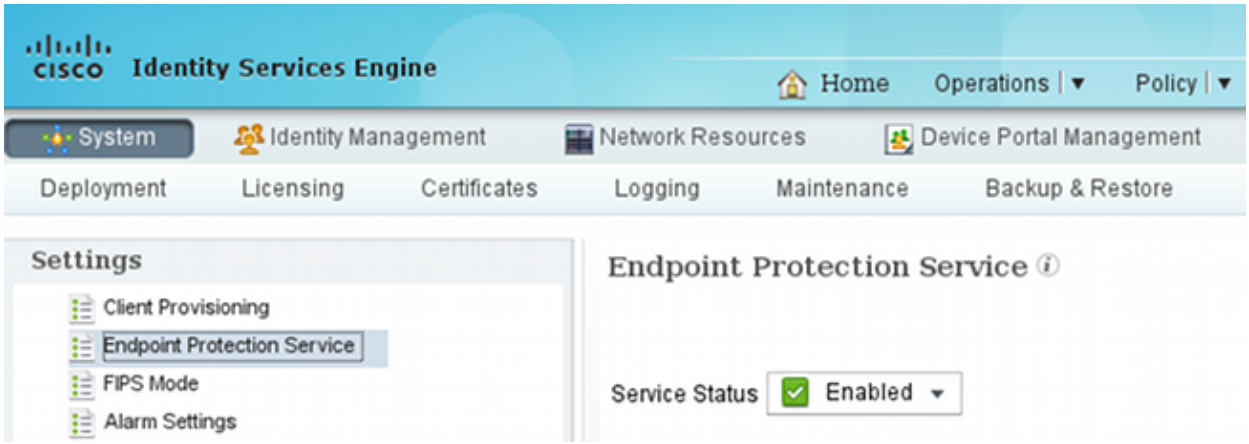


2. Verify if the certificates are used for pxGrid under ***Administration*** > ***Certificates*** > ***System Certificates***:



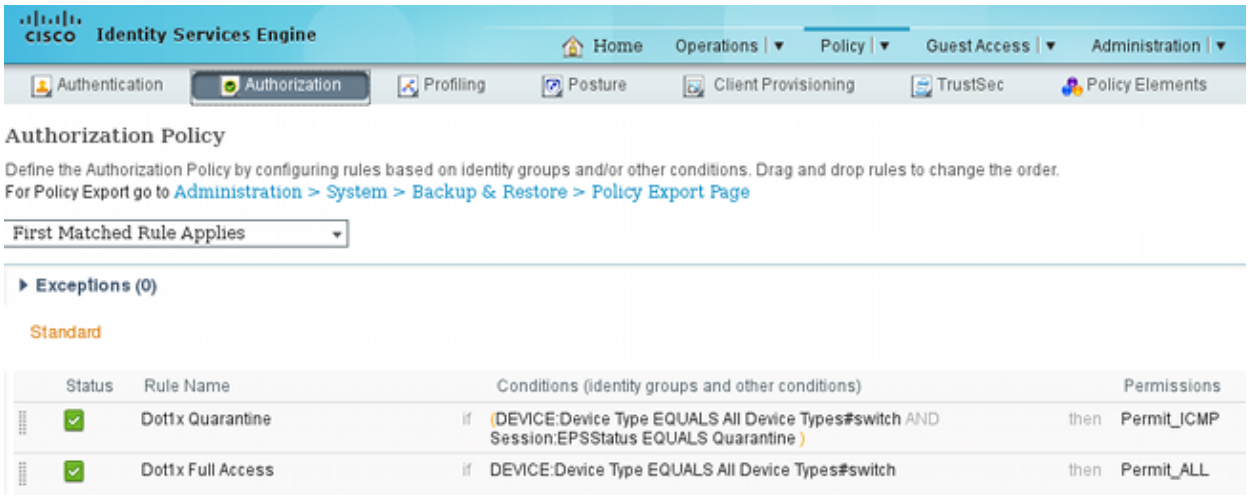
Endpoint Protection Service (EPS)

EPS should be enabled (disabled by default) from ***Administration*** > ***Settings***:



This allows you to use the quarantine/unquarantine functionality.

Authorization Rules



The first rule is encountered only when the endpoint is quarantined. Then limited access is dynamically enforced by the RADIUS CoA. The switch also must be added to Network Devices with the correct shared secret.

Troubleshoot

The pxGrid status can be verified with the 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
```

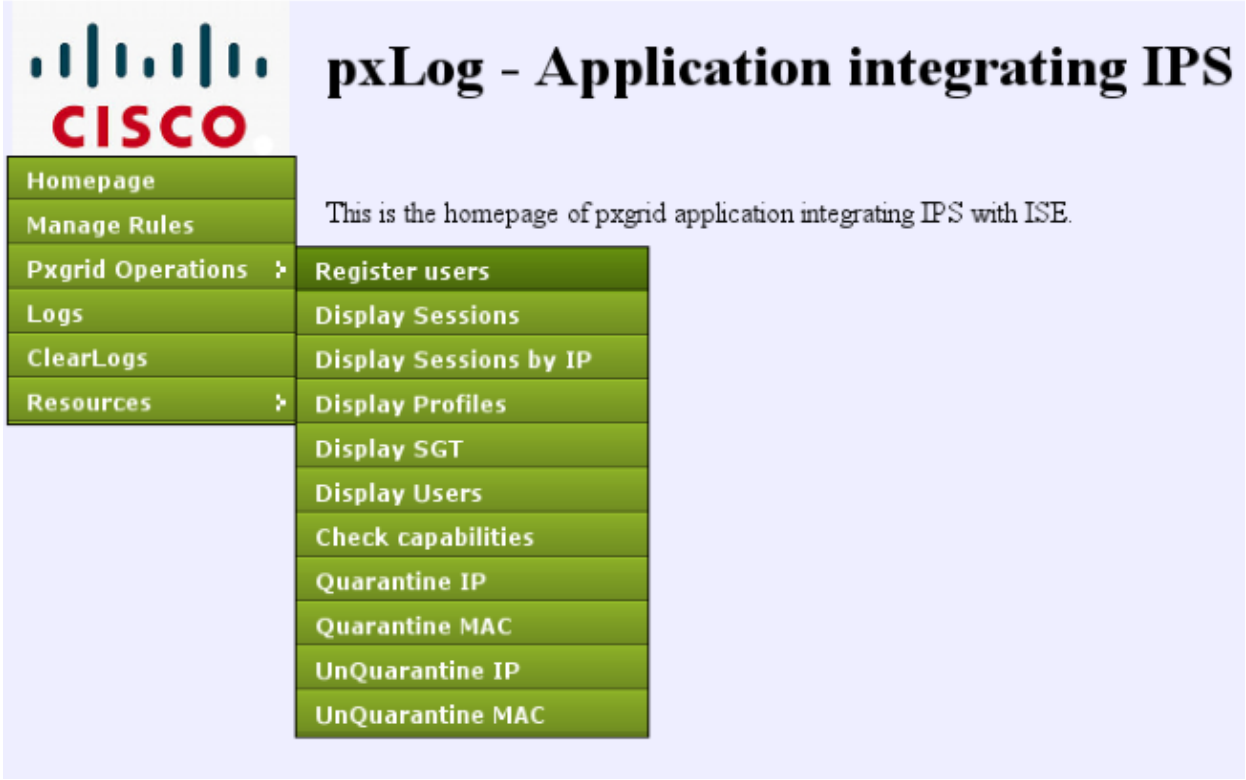
There are also separate debugs for pxGrid (***Administration*** > ***Logging*** > ***Debug Log Configuration*** > ***pxGrid***). Debug files are stored in the pxGrid directory. The most important data is in the ***pxgrid/pxgrid−jabberd.log*** and the ***pxgrid/pxgrid−controller.log***.

Test

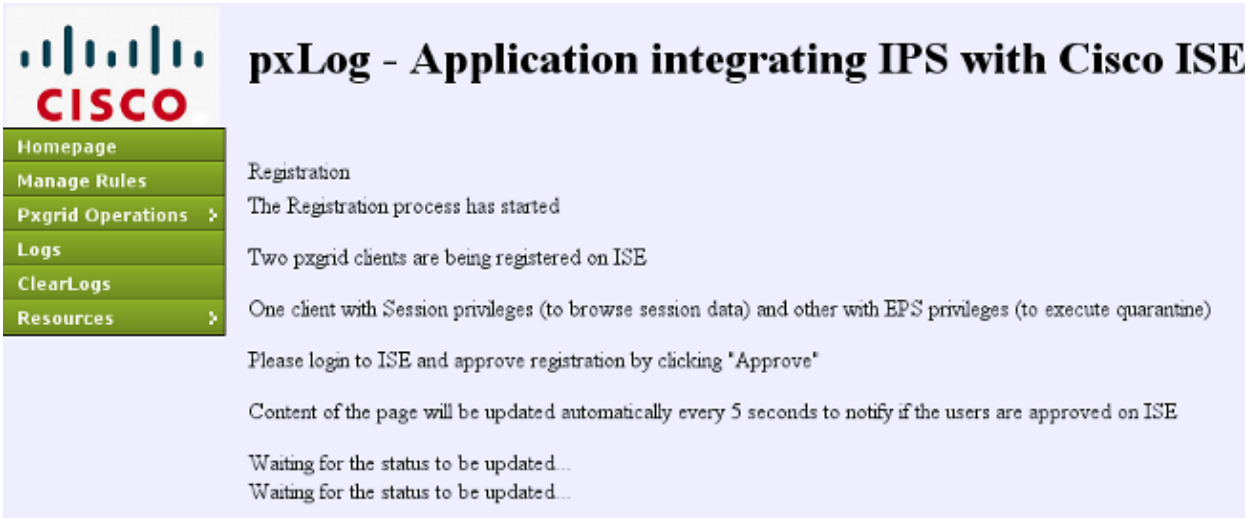
Step1. Registration for pxGrid

The pxLog application is automatically deployed when Tomcat starts.

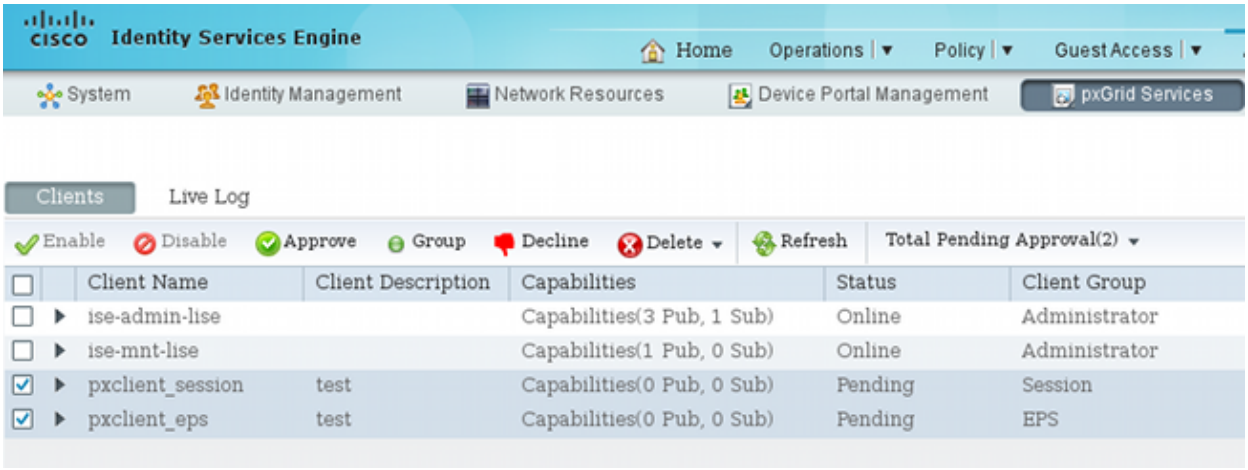
1. In order to use pxGrid, register two users in the ISE (one with session access, and one with quarantine). This can be completed from ***Pxgrid Operations*** > ***Register users***:



Registration starts automatically:



2. At this stage, it is necessary to approve registered users on the ISE (auto approval is disabled by default):



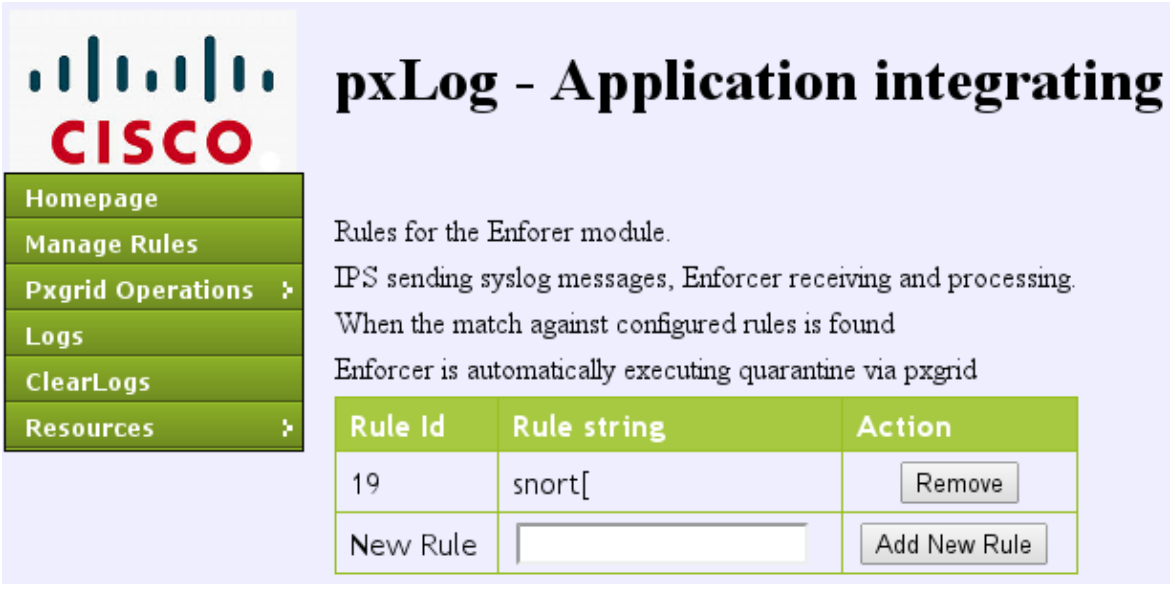
After the approval, pxLog automatically notifies the administrator (via an AJAX call):

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

ISE shows the status for those two users as Online or Offline (not Pending anymore).

Step2. pxLog Rules Configuration

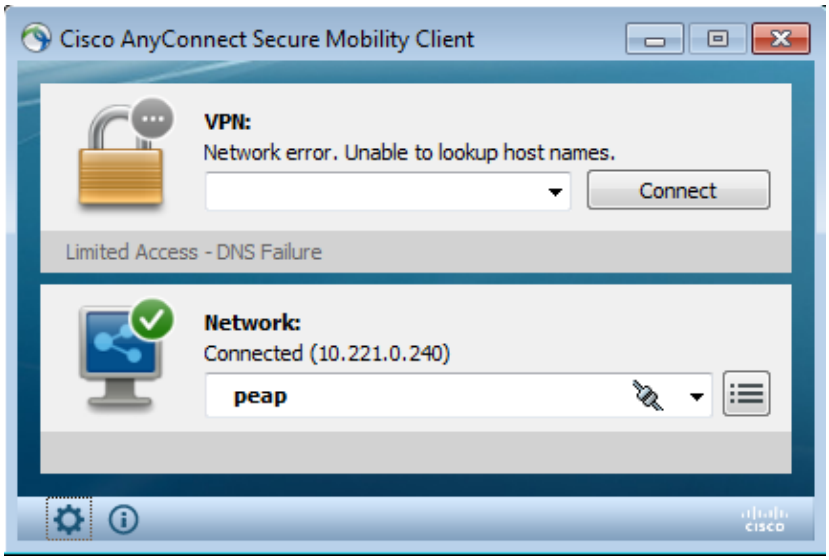
pxLog must process syslog messages and execute actions based on it. In order to add a new rule, select ***Manage Rules***:



Now the enforcer module looks for this Regular Expression (RegExp) in the syslog message: "snort[". If found, it searches all IP addresses and selects the one before the last one. This matches most security solutions. Refer to the Syslog section for more information. That IP address (attacker) is quarantined via pxGrid. Also a more granular rule might be used (for example, it might include the signature number).

Step3. First Dot1x Session

The Microsoft Windows 7 station initiates a wired dot1x session. Cisco Anyconnect NAM has been used as a supplicant. The Extensible Authentication Protocol−Protected EAP (EAP−PEAP) method is configured.



The ISE ***Dot1x Full Access*** authorization profile is selected. The switch downloads the access list in order to grant full access:

```
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 Sends the Packet that Triggers the Alarm

This shows what happens if you do send from a Microsoft Windows packet with TTL = 7:

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

That value is decremented on Snort in the Forwarding chain and an alarm is raised. As a result, a syslog message towards pxLog is sent:

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

Step5. pxLog

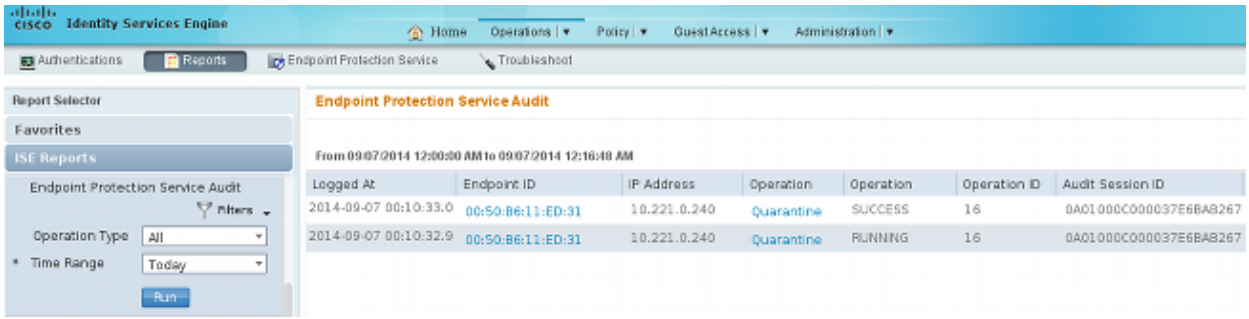
The pxLog receives the syslog message, processes it, and requests to quarantine that IP address. This can be confirmed if you check the logs:

Logs from the actions executed by the Enforer module

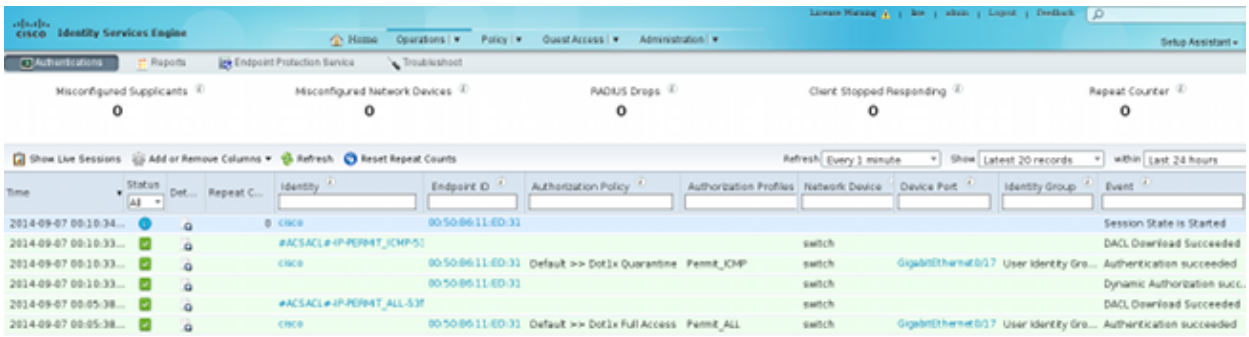
Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

Step6. ISE Quarantine

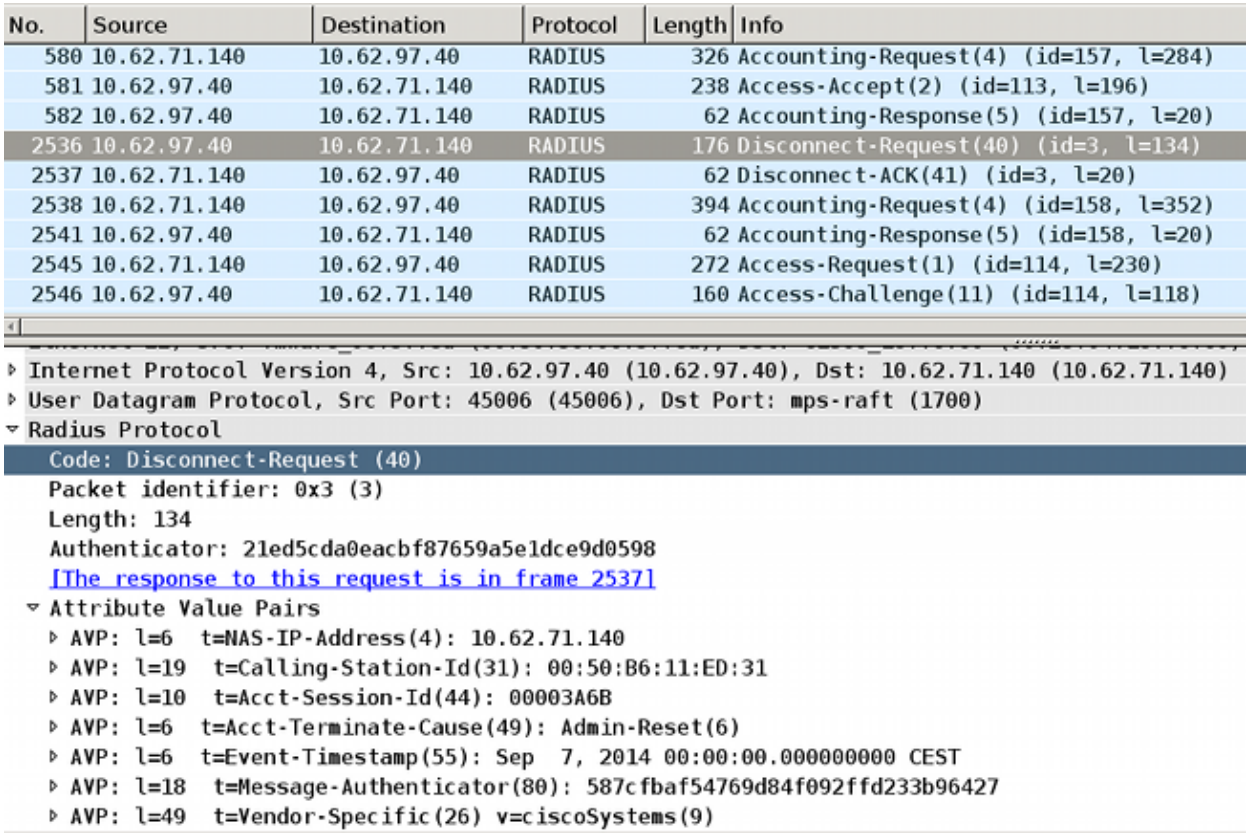
The ISE reports that the IP address has been quarantined:



As a result, it reviews the authorization policy, chooses quarantine, and sends RADIUS CoA in order to update the authorization status on the switch for that specific endpoint.



That is the CoA terminate message that forces the supplicant to initiate a new session and get limited access (Permit_ICMP):

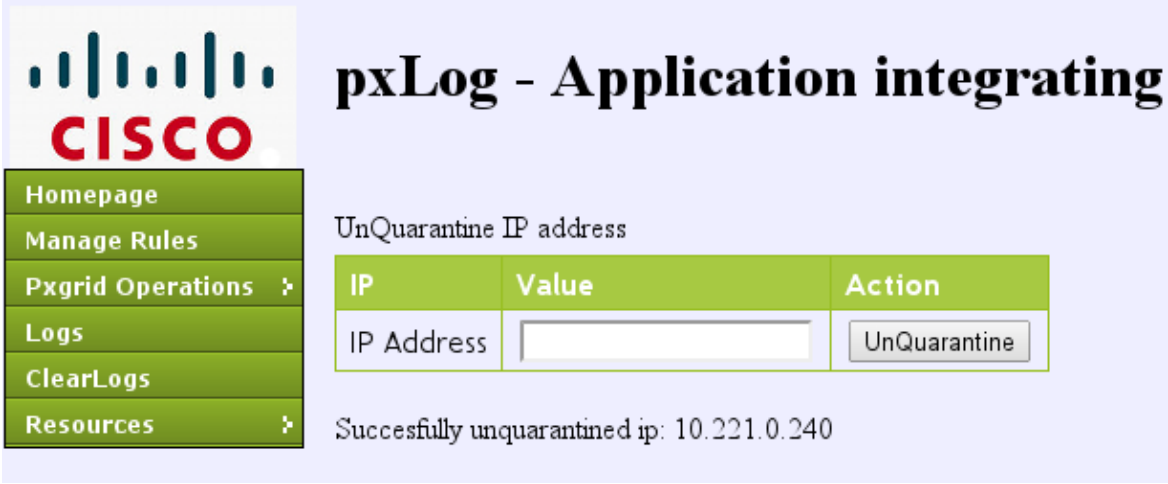


The result can be confirmed on the switch (limited access for the endpoint):

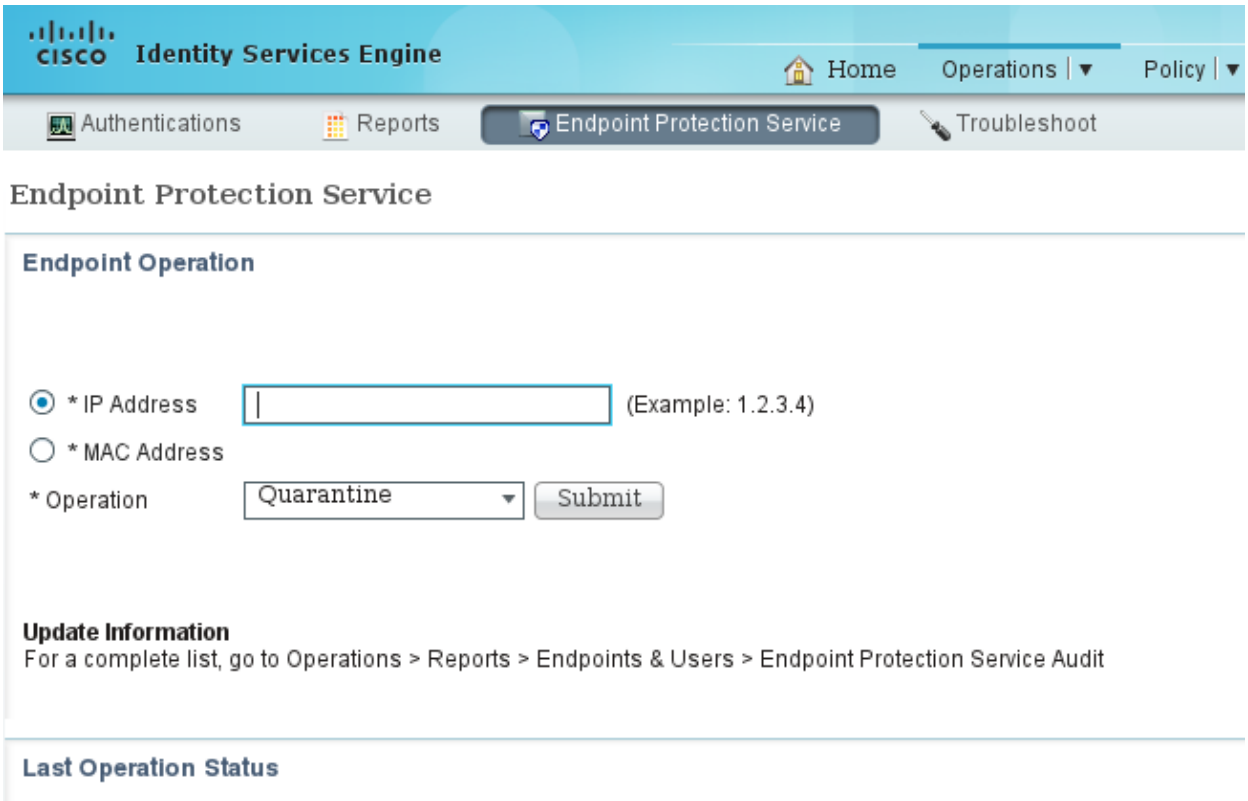
```
3750#show authentication sessions interface g0/17
            Interface:  GigabitEthernet0/17
          MAC Address:  0050.b611.ed31
           IP Address:  10.221.0.240
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should 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

At this stage, the administrator decides to unquarantine that endpoint:

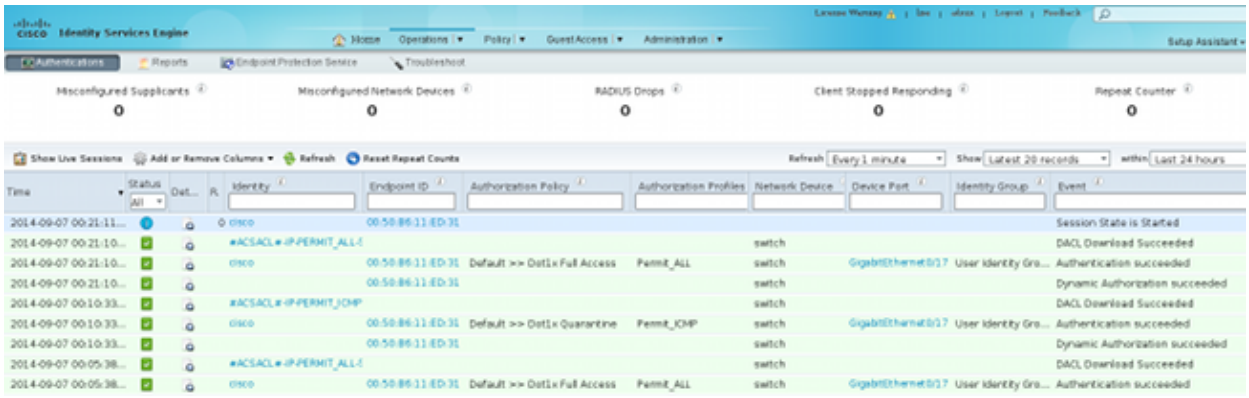


The same operation can be executed directly from the ISE:

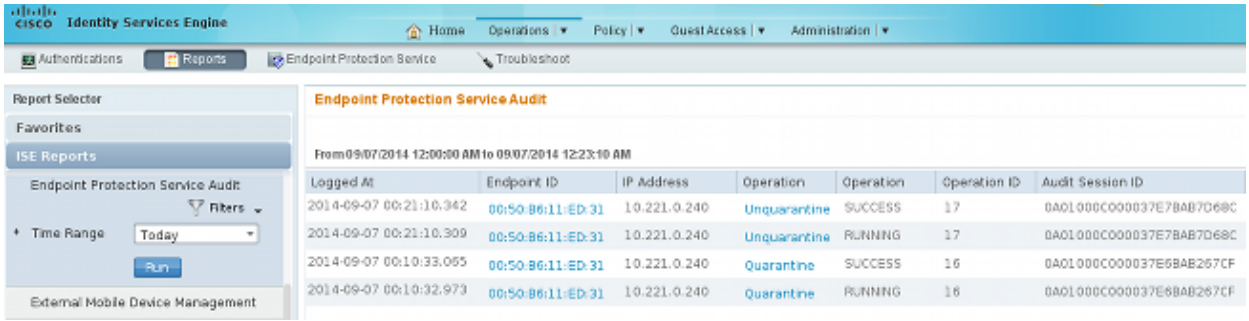


Step8. ISE Unquarantine

The ISE again reviews the rules and updates the authorization status on the switch (full network access is granted):



The report confirms:



pxLog Functionality

The pxLog application has been written in order to demonstrate the functionality of the pxGrid API. It allows you to:

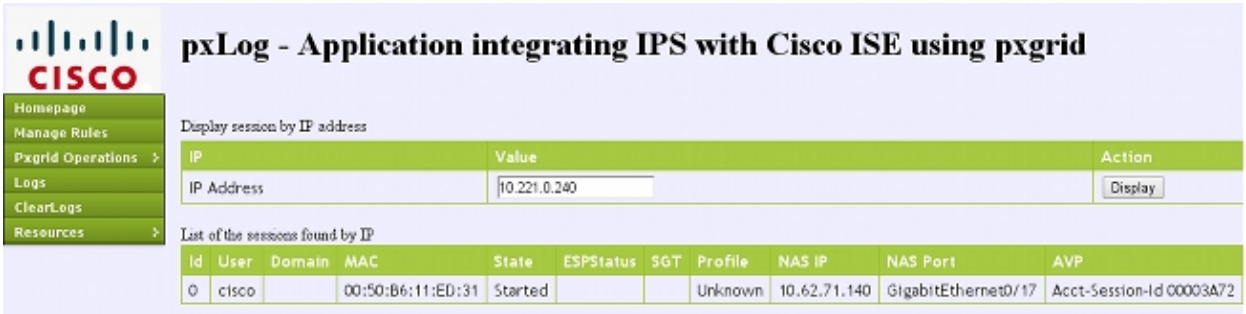
- Register session and EPS users on the ISE
- Download information about all sessions active on the ISE
- Download information about a specific active session on the ISE (by IP address)
- Download information about a specific active user on the ISE (by username)
- Display the information about all profiles (profiler)
- Display the information about the TrustSec Security Group Tags (SGTs) defined on the ISE
- Check version (capabilities of pxGrid)
- Quarantine based on the IP or MAC address
- Unquarantine based on IP or MAC address

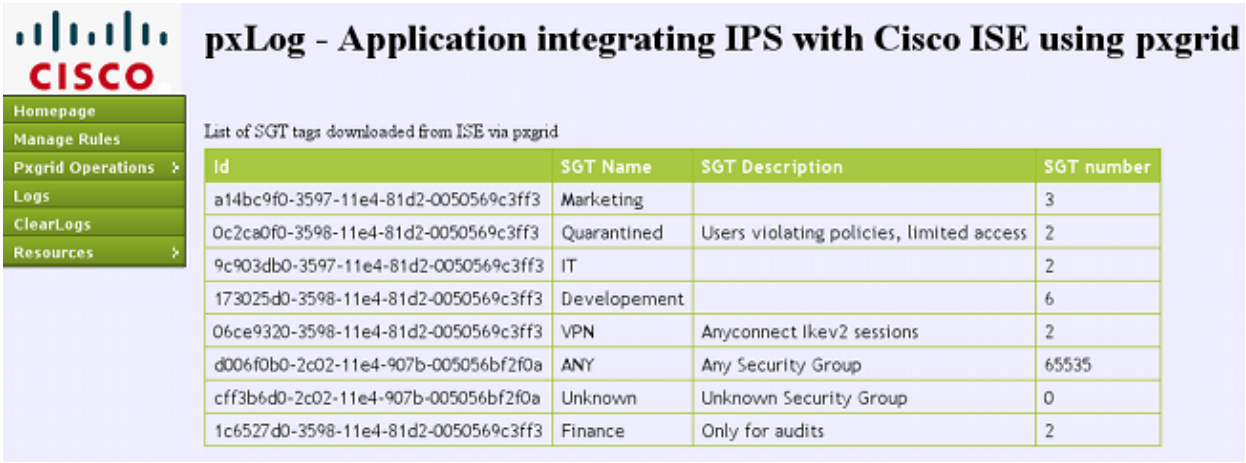
More functionality is planned in the future.

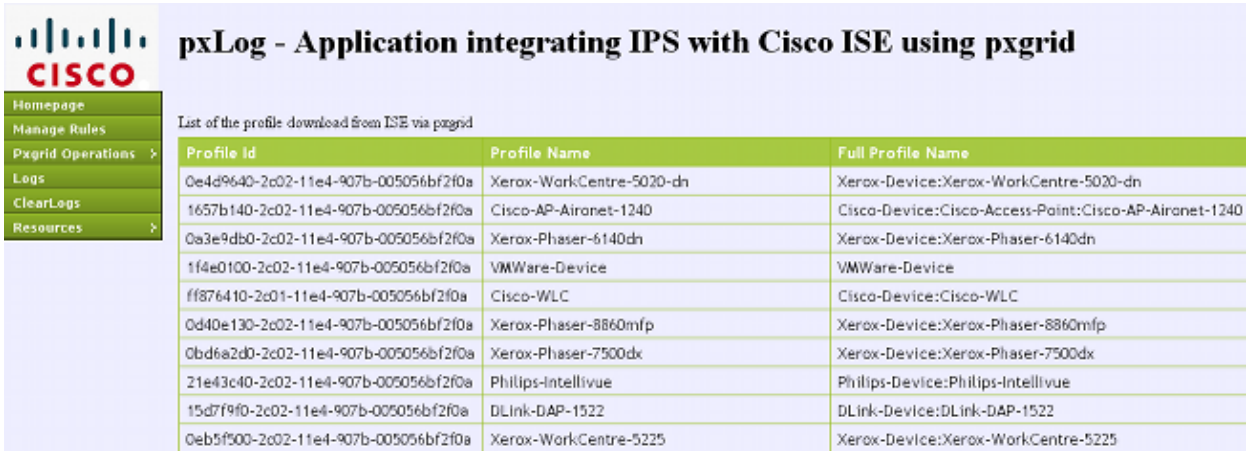
Here are some example screenshots from pxLog:


CISCO
Homepage
Manage Rules
Pxgrid Operations
Logs
ClearLogs
Resources
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


CISCO
Homepage
Manage Rules
Pxgrid Operations
Logs
ClearLogs
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


CISCO
Homepage
Manage Rules
Pxgrid Operations
Logs
ClearLogs
Resources
pxLog - Application integrating IPS with Cisco ISE using pxgrid
Display session by IP address
IP
Value
Action
IP Address
10.221.0.240
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


CISCO
Homepage
Manage Rules
Pxgrid Operations
Logs
ClearLogs
Resources
pxLog - Application integrating IPS with Cisco ISE using pxgrid
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 Developement 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



pxGrid Protocol Requirements

Groups

The client (user) can be a member of one group at a time. The two most commonly used groups are:

- Session − Used in order to browse/download information about sessions/profiles/SGTs
- EPS − Used in order to execute quarantine

Certificates and Java KeyStore

As mentioned previously, both client applications, pxLog and pxGrid controller (ISE), must have certificates configured in order to communicate. The pxLog application keeps those in the Java KeyStore files:

- ***store/client.jks*** − Includes the client and the Certificate Authority (CA) certificates
- ***store/root.jks*** − Includes the ISE chain: Monitoring and Troubleshooting Node (MnT) identity and the CA certificate

Files are protected by password (default: cisco123). File location and passwords can be changed in ***WEB−INF/web.xml***.

Here are the steps to generate a new Java KeyStore:

1. In order to create a root (trusted) keystore, import the CA certificate (***cert−ca.der*** should be in DER format):

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

2. When you create a new keystore, choose a password, which is used later in order to access the keystore.

3. Import the MnT identity certificate to the root keystore (***cert−mnt.der*** is the identity certificate taken from ISE and should be in DER format):

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

4. In order to create the client keystore, import the CA certificate:

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

5. Create a private key in the client keystore:

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

6. Generate a Certificate Signing Request (CSR) in the client keystore:

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

7. Sign the ***cert−client.csr*** and import the signed client certificate:

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

8. Verify that both keystores contain the correct certificates:

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

Caution: When the ISE 1.3 node is upgraded, there is an option to keep the identity certificate, but CA signing is removed. As a result, the upgraded ISE uses a new certificate but never attaches the CA certificate in the SSL/ServerHello message. This triggers the failure on the client that expects (as per RFC) to see a full chain.

Hostname

The pxGrid API for several functions (like session download) performs additional validation. The client contacts the ISE and receives the ISE hostname, which is defined by the hostname command in the CLI. Then, the client tries to perform DNS resolution for that hostname and tries to contact and fetch data from that IP address. If the DNS resolution for the ISE hostname fails, the client does not try to get any data.

Caution: Notice that only the hostname is used for this resolution, which is ***lise*** in this scenario, not the Fully

Qualified Domain Name (FQDN), which is ***lise.example.com*** in this scenario.

Note for Developers

Cisco publishes and supports the pxGrid API. There is one package named like this:

pxgrid−sdk−1.0.0−167

Inside there are:

- pxGrid JAR files with classes, which can be easily decoded to Java files to check the code
- Sample Java KeyStores with certificates
- Sample scripts that use sample Java classess that use pxGrid

Syslog

Here is the list of security solutions that send syslog messages with the attacker IP address. These can be easily integrated with pxLog as long as you use the correct RegExp rule in the configuration.

Snort

Snort sends syslog alerts in this format:

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

Here is an example:

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

The attacker IP address is always the second before the last one (destination). It is simple to build a granular RegExp for a specific signature and extract the attacker IP address. Here is an example RegExp for the signature 100124 and message Internet Control Message Protocol (ICMP):

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

Cisco Adaptive Security Appliance (ASA) Inspection

When the ASA is configured for HTTP (example) inspection, the corresponding syslog message looks like this:

```
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
```

Again a granular RegExp could be used in order to filter those messages and extract the attacker IP address, the second before the last one.

Cisco Sourcefire Next Generation Intrusion Prevention Systems (NGIPS)

Here is an example message sent by the Sourcefire sensor:

```
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
```

So again, it is simple to extract the attacker IP address because the same logic applies. Also the policy name and the signature is provided, so the pxLog rule can be granular.

Juniper NetScreen

Here is an example message sent by the older Juniper Intrusion Detection & Prevention (IDP):

```
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" 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"
```

The IP address of the attacker can be extracted in the same way.

Juniper JunOS

JunOS is 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
```

Linux iptables

Here are some example Linux iptables.

```
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
```

You can send syslog information for any type of packet with the advanced functionality provided by the iptable modules like connection tracking, xtables, rpfilters, pattern matching, and so on.

FreeBSD IPFirewall (IPFW)

Here is an example message for IPFW blocking fragments:

```
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)
```

VPN Readiness and CoA Handling

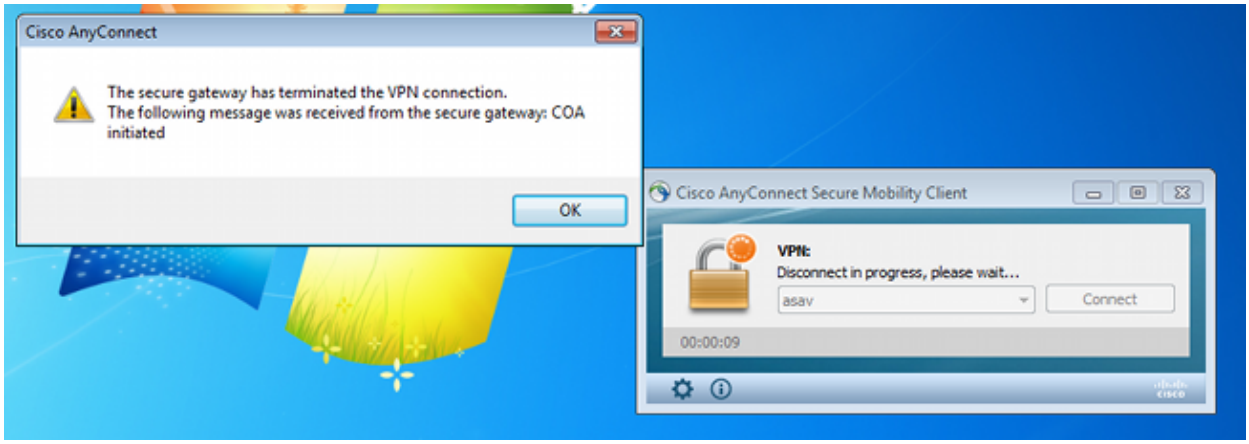
The ISE is able to recognize the type of sessions in terms of the CoA handling.

- For a wired 802.1x/MAC Authentication Bypass (MAB), the ISE sends the CoA reauthenticate,

which triggers a second authentication.

- For a wireless 802.1x/MAB, the ISE sends the CoA terminate, which triggers a second authentication.
- For an ASA VPN, the ISE sends a CoA with a new DACL attached (no second authentication).

The EPS module is simple. When it executes a quarantine, it always sends a CoA terminate packet. For wired/wireless sessions, it is not a problem (all 802.1x supplicants are able to transparently initiate a second EAP session). But when the ASA receives the CoA terminate, it drops the VPN session and the end user is presented with this:



There are two possible solutions to force the AnyConnect VPN to automatically reconnect (configured in the XML profile):

- Autoreconnect, which works only when you lose the connection with the VPN gateway, not for administrative termination
- Always−on, which works and forces AnyConnect to automatically re−establish the session

Even when the new session is established, the ASA chooses the new audit−session−id. From the ISE point−of−view, this is a new session and there is no chance to encounter the quarantine rule. Also for the VPNs, it is not possible to use the MAC address of the endpoint as the identity, as opposed to wired/wireless dot1x.

The solution is to force the EPS to behave like the ISE and send the correct type of CoA based on the session. This functionality will be introduced in ISE Version 1.3.1.

pxGrid Partners and Solutions

Here is a list of pxGrid partners and solutions:

- LogRhythm (Security Information and Event Management (SIEM)) − Supports the Representational State Transfer (REST) API
- Splunk (SIEM) − Supports the REST API
- HP Arcsight (SIEM) − Supports the REST API
- Sentinel NetIQ (SIEM) − Plans to support pxGrid
- Lancope StealthWatch (SIEM) − Plans to support pxGrid
- Cisco Sourcefire − Plans to support pxGrid 1HCY15
- Cisco Web Security Appliance (WSA) − Plans to support pxGrid in April 2014

Here are other partners and solutions:

- Tenable (vulnerability assessment)
- Emulex (packet capture and forensics)
- Bayshore Networks (Data Loss Prevention (DLP) and Internet of Things (IoT) policy)
- Ping Identity (Identity and Access Management (IAM)/Single Sign On (SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (SIEM amd Mobile Device Management (MDM))

Refer to the Marketplace Solutions Catalog for the full list of security solutions.

ISE APIs: REST vs EREST vs pxGrid

There are three types of API available on ISE Version 1.3.

Here is a comparison:

	REST	External RESTful	pxGrid
Client authentication	username + password (basic HTTP auth)	username + password (basic HTTP auth)	certificate
Privilege separation	no	limited (ERS Admin)	yes (Groups)
Accessing	MnT	MnT	MnT
Transport	tcp/443 (HTTPS)	tcp/9060 (HTTPS)	tcp/5222 (XMPP)
HTTP method	GET	GET/POST/PUT	GET/POST
Enabled by default	yes	no	no
Number of operations	few	many	few
CoA Terminate	supported	no	supported
CoA Reauthenticate	supported	no	supported *
User operations	no	yes	no
Endpoint operations	no	yes	no
Endpoint Identity group operations	no	yes	no
Quarantine (IP, MAC)	no	no	yes
UnQuarantine (IP, MAC)	no	no	yes
PortBounce/Shutdown	no	no	yes
Guest user operations	no	yes	no
Guest portal operations	no	yes	no
Network device operations	no	yes	no
Network device group operations	no	yes	no

* Quarantine uses unified CoA support from ISE Version 1.3.1.

Downloads

pxLog can be downloaded from Sourceforge .

The Software Development Kit (SDK) is already included. For the latest SDK and API documentation for pxGrid, contact your Partner or the Cisco Account team.

Related Information

- ***Cisco ISE 1.2 REST API***
- ***Cisco ISE 1.2 External RESTful API***
- ***Cisco ISE 1.3 Administrators Guide***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Dec 23, 2014 Document ID: 118688