ISE 1.3版pxGrid與IPS pxLog應用的整合

目錄

簡介

身份服務引擎(ISE)版本1.3支援稱為pxGrid的新API。這種支援身份驗證、加密和許可權（組）的現代靈活協定允許與其他安全解決方案輕鬆整合。本文檔介紹作為概念驗證編寫的pxLog應用程式的用法。pxLog能夠接收來自入侵防禦系統(IPS)的系統日誌消息，並將pxGrid消息傳送到ISE以隔離攻擊者。因此，ISE使用RADIUS授權更改(CoA)來更改限制網路訪問的終端的授權狀態。所有這一切對終端使用者都是透明的。

在本例中，Snort已被用作IPS，但是可以使用任何其他解決方案。實際上它不必是IPS。只需使用攻擊者的IP地址將系統日誌消息傳送到pxLog。這為整合大量解決方案創造了可能性。

本文還提供如何對pxGrid解決方案進行故障排除和測試的方法，以及常見的問題和限制。

免責聲明：思科不支援pxLog應用程式。本文是作為概念證明而寫的。主要目的是在ISE上的pxGrid實施測試期間使用它。

必要條件

需求

思科建議您瞭解思科ISE配置和以下主題的基本知識：

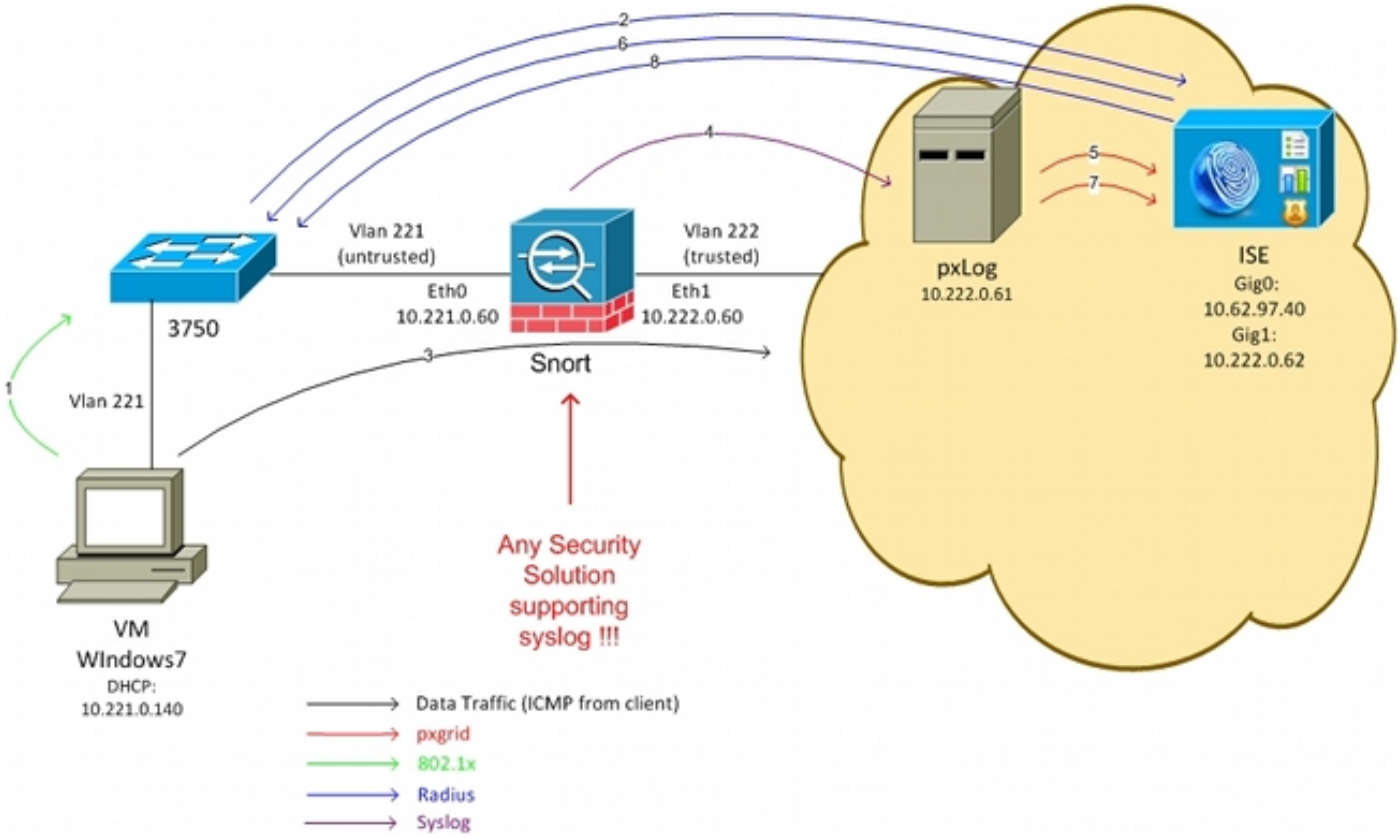
- ISE部署和授權配置
- Cisco Catalyst交換機的CLI配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7
- Cisco Catalyst 3750X系列交換器軟體版本15.0及更新版本
- Cisco ISE軟體1.3版及更高版本
- Cisco AnyConnect Mobile Security with Network Access Manager(NAM)，版本3.1及更高版本
- 含資料採集(DAQ)的Snort版本2.9.6
- pxLog應用程式安裝在MySQL版本5的Tomcat 7上

網路圖表和流量傳輸



以下是流量傳輸，如網路圖所示：

1. Microsoft Windows 7使用者連線到交換機並執行802.1x身份驗證。

2. 交換機使用ISE作為身份驗證、授權和記帳(AAA)伺服器。匹配**Dot1x Full Access**授權規則並授予完整網路訪問許可權(DACL:PERMIT_ALL)。

3. 使用者嘗試連線受信任網路並違反Snort規則。

4. 因此，Snort會向pxLog應用程式傳送警報（通過syslog）。

5. pxLog應用程式對其本地資料庫執行驗證。其配置是為了捕獲Snort傳送的系統日誌消息並提取攻擊者的IP地址。然後使用pxGrid向ISE傳送請求以隔離攻擊者IP地址（ISE是pxGrid控制器）。

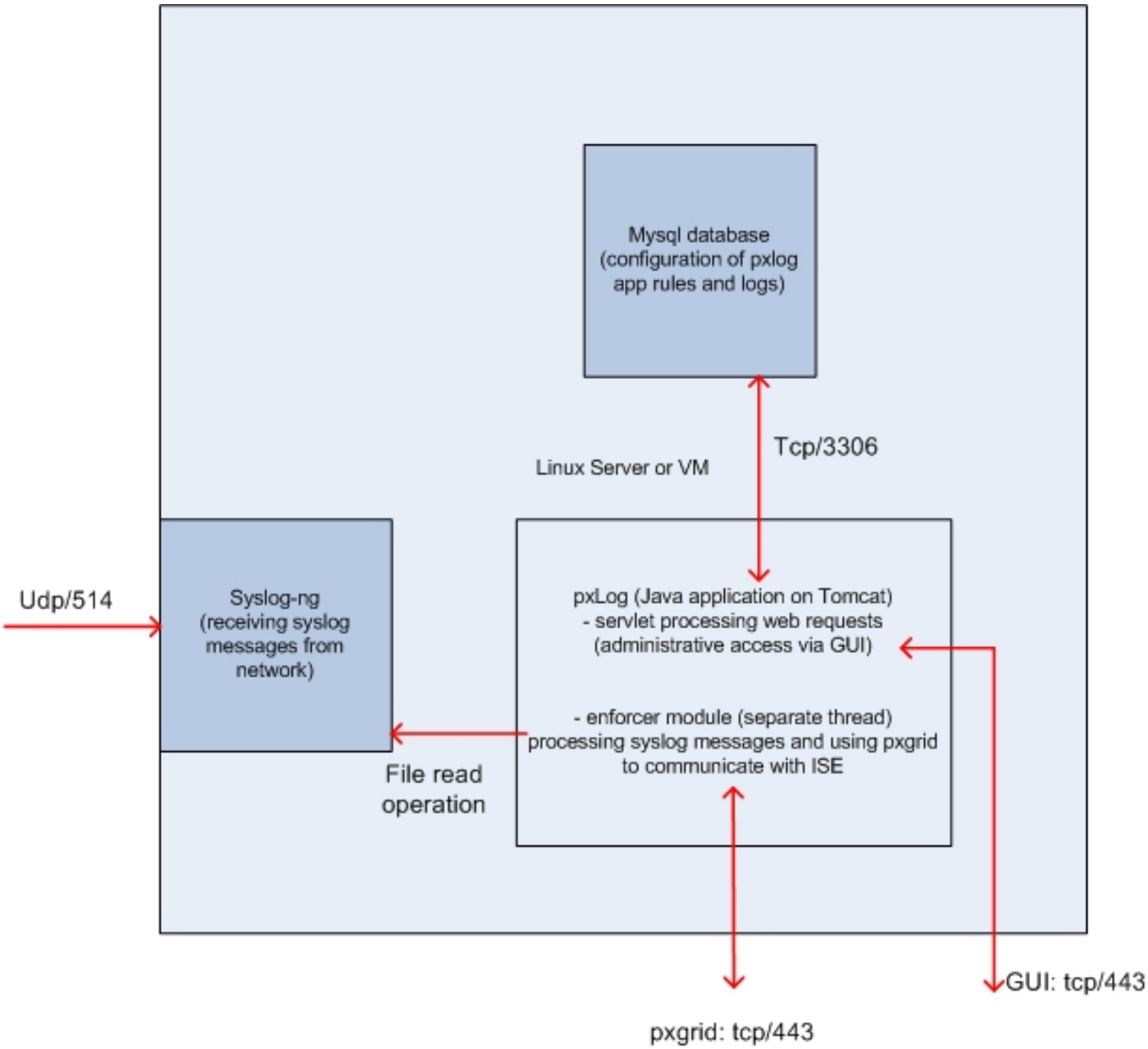
6. ISE重新評估其授權策略。由於終端已隔離，因此滿足**Session:EPSStatus EQUALS Quarantine**條件，並且匹配不同的授權配置檔案(**Dot1x Quarantine**)。 ISE向交換機傳送CoA Terminate以終止會話。這會觸發重新驗證並套用新的可下載ACL(DACL)(PERMIT_ICMP)，這為終端使用者提供有限的網路存取許可權。

7. 在這個階段，管理員可能會決定取消隔離端點。這可以通過pxLog的GUI來實現。同樣，向ISE傳送pxGrid消息。

8. ISE執行與步驟6類似的操作。這一次，終端不再被隔離，並提供完全訪問許可權。

pxLog

架構



解決方案是在Linux電腦上安裝一組應用程式：

1. 用Java編寫並部署在Tomcat伺服器上的pxLog應用程式。該應用程式套件括：

   處理Web請求的Servlet — 用於通過Web瀏覽器訪問管理面板。

   Enforcer模組 — 與servlet一起啟動的執行緒。Enforcer從檔案中讀取系統日誌消息（已最佳化），根據配置的規則處理這些消息，並執行操作（如通過pxGrid隔離）。

2. 包含pxLog（規則和日誌）配置的MySQL資料庫。

3. 從外部系統接收系統日誌消息並將其寫入檔案的系統日誌伺服器。

安裝

pxLog應用程式使用以下庫：

- jQuery（用於AJAX支援）
- JavaServer Pages標準標籤庫(JSTL)(Model View Controller， MVC)模型，資料從邏輯中分離出來：JavaServer Page(JSP)代碼僅用於呈現，在Java類中沒有HTML代碼)
- Log4j作為日誌記錄子系統
- MySQL聯結器
- 用於呈現/排序表的displaytag
- 思科的pxGrid API（當前版本alpha 147）

所有這些庫都已位於專案的lib目錄中，因此無需再下載任何其它Java ARchive(JAR)檔案。

若要安裝應用程式：

1. 將整個目錄解壓縮到Tomcat Webapp目錄。

2. 編輯**WEB-INF/web.xml**檔案。唯一需要的更改是 **serverip** 變數，該變數應指向ISE。此外，可能會生成Java Certificate KeyStores（一個用於受信任的，一個用於身份）（而不是預設值）。 pxGrid API使用安全套接字層(SSL)會話，該會話同時使用客戶端和伺服器證書。通訊的兩端需要出示憑證，並需要彼此信任。有關詳細資訊，請參閱pxGrid協定要求部分。

3. 確保在pxLog上正確解析ISE主機名(請參閱域名伺服器(DNS)或**/etc/hosts條目中的記**錄)。 有關詳細資訊，請參閱pxGrid協定要求部分。

4. 使用**mysql/init.sql**指令碼配置MySQL資料庫。可以更改憑據，但應反映在**WEB-INF/web.xml**檔案中。

Snort

本文不重點介紹任何特定IPS，因此僅提供簡要說明。

Snort設定為內嵌並支援DAQ。流量使用iptables重新導向：

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

然後，在檢查後，根據預設的可接收規則注入並轉發該資料包。

已配置了一些自定義Snort規則(全域性配置中包含**/etc/snort/rules/test.rules**檔案)。

```
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)
```

當封包的存留時間(TTL)等於6或負載大小介於666和686之間時，Snort會傳送系統日誌訊息。
Snort不會封鎖流量。

此外，還應設定閾值以確保警報觸發不頻繁(**/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
```

然後，系統日誌伺服器指向pxLog電腦(**/etc/snort/snort.conf**):

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

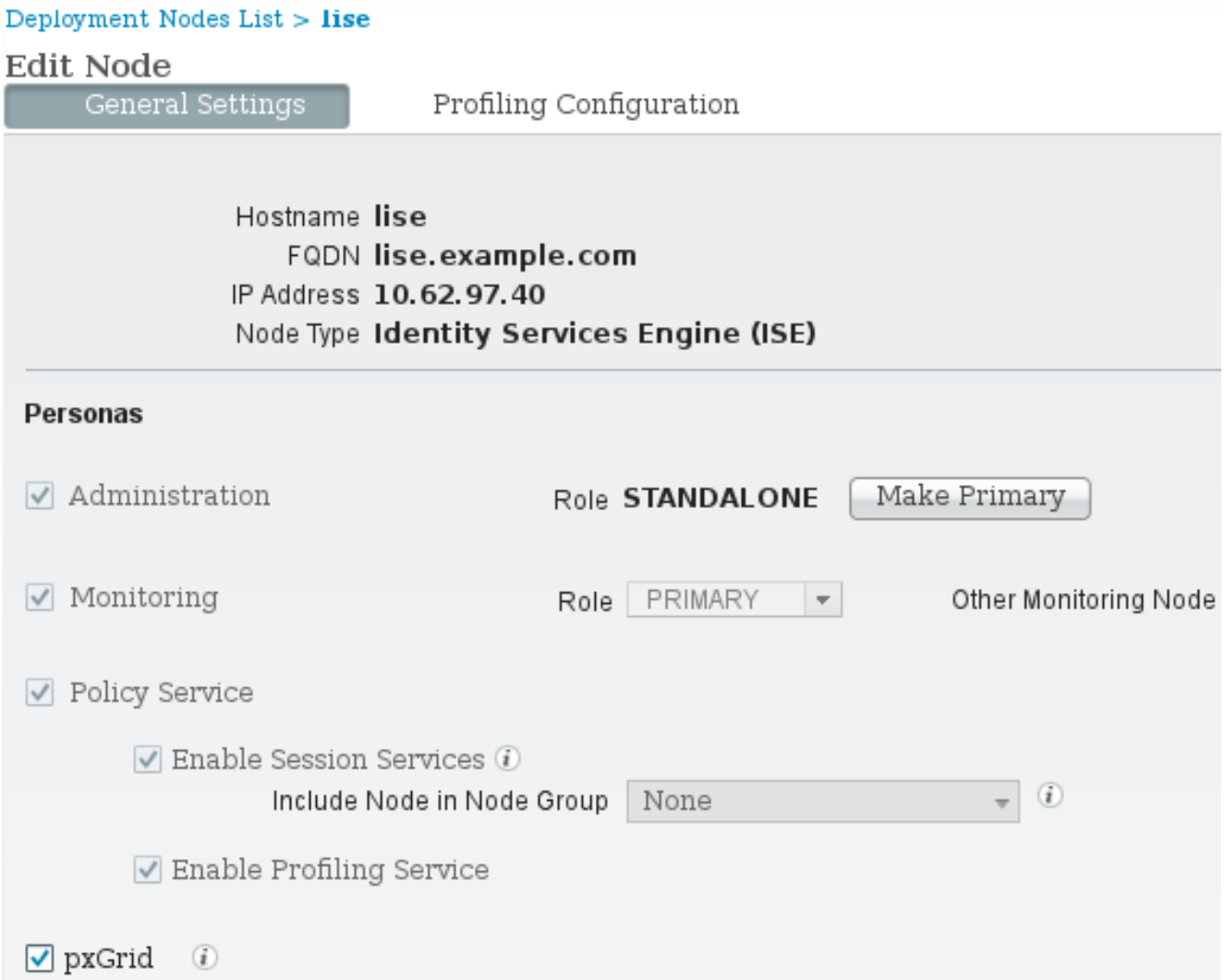
對於某些Snort版本，存在與syslog配置相關的錯誤，因此可以使用指向本地主機的預設設定，並且可以配置syslog-ng以將特定消息轉發到pxLog主機。

ISE

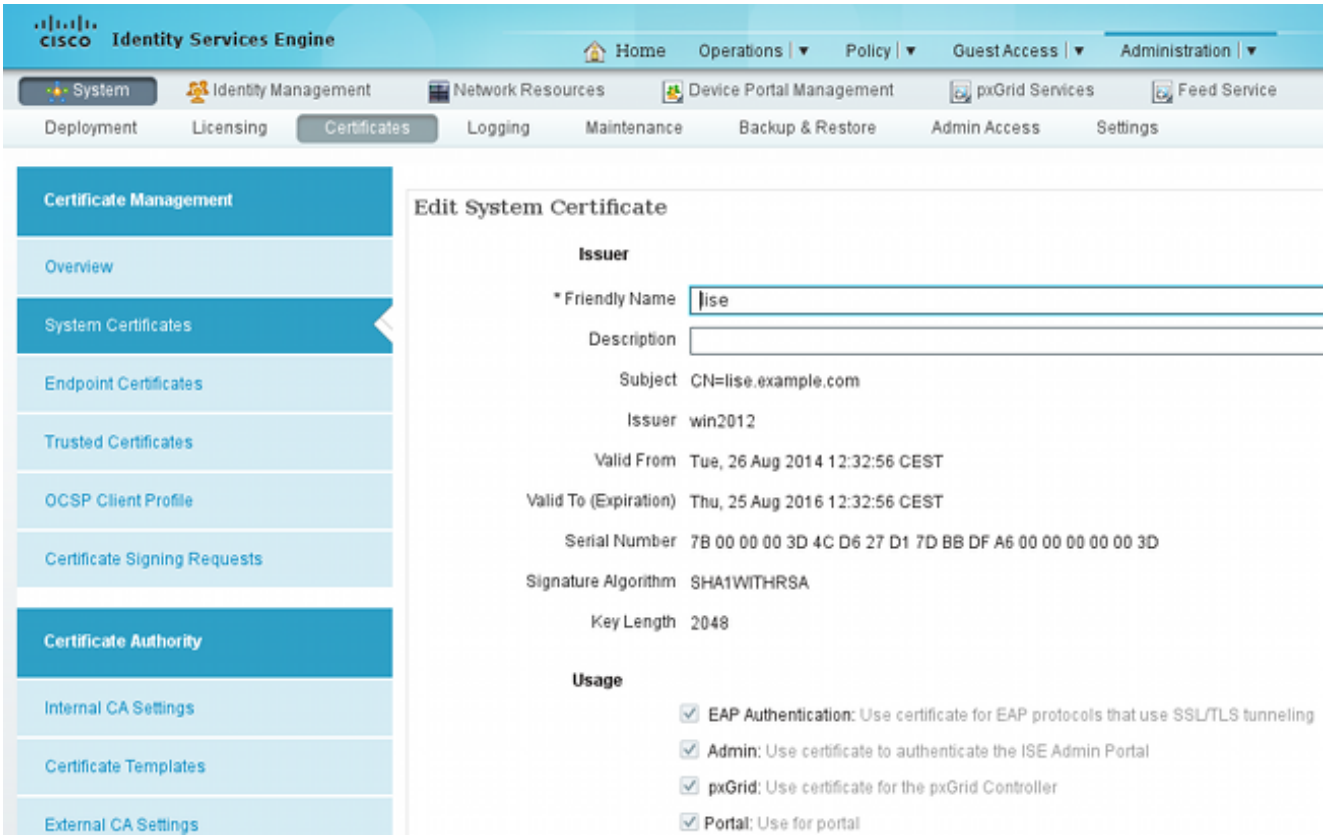
組態

角色和證書

1. 在**Administration > Deployment**下啟用pxGrid角色，該角色預設在ISE上禁用：

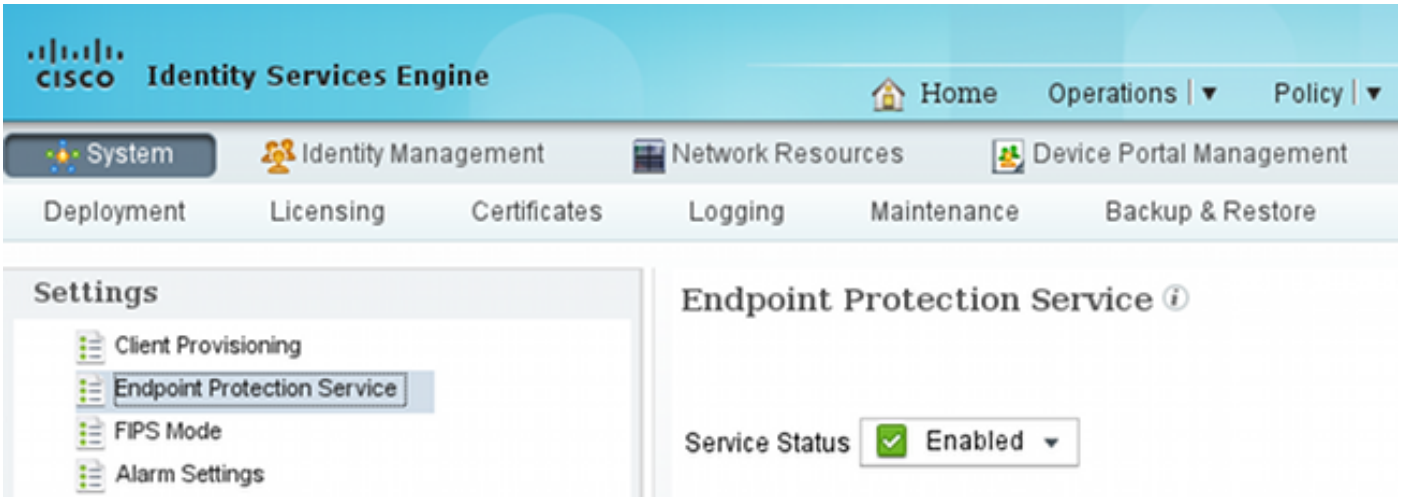


2. 驗證證書是否用於**管理>證書>系統證書**下的pxGrid:



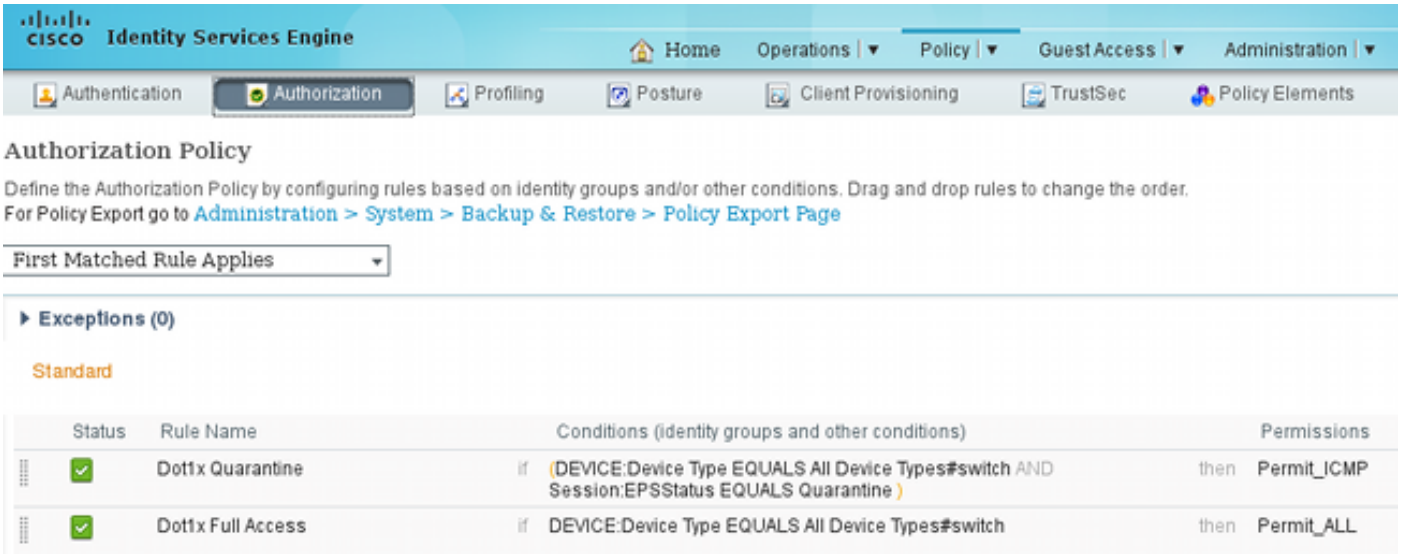
終端保護服務(EPS)

應從**Administration > Settings**啟用EPS（預設情況下禁用）：



這允許您使用隔離/取消隔離功能。

授權規則



僅當終端被隔離時，才會遇到第一個規則。接著，RADIUS CoA會動態執行限制存取。還必須將交換機以正確的共用金鑰新增到網路裝置中。

疑難排解

pxGrid狀態可以通過CLI驗證：

```
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
```

pxGrid還有單獨的調試(**管理>記錄>調試日誌配置> pxGrid**)。 調試檔案儲存在pxGrid目錄中。最重要的資料位於**pxgrid/pxgrid-jabberd.log**和**pxgrid/pxgrid-controller.log**。

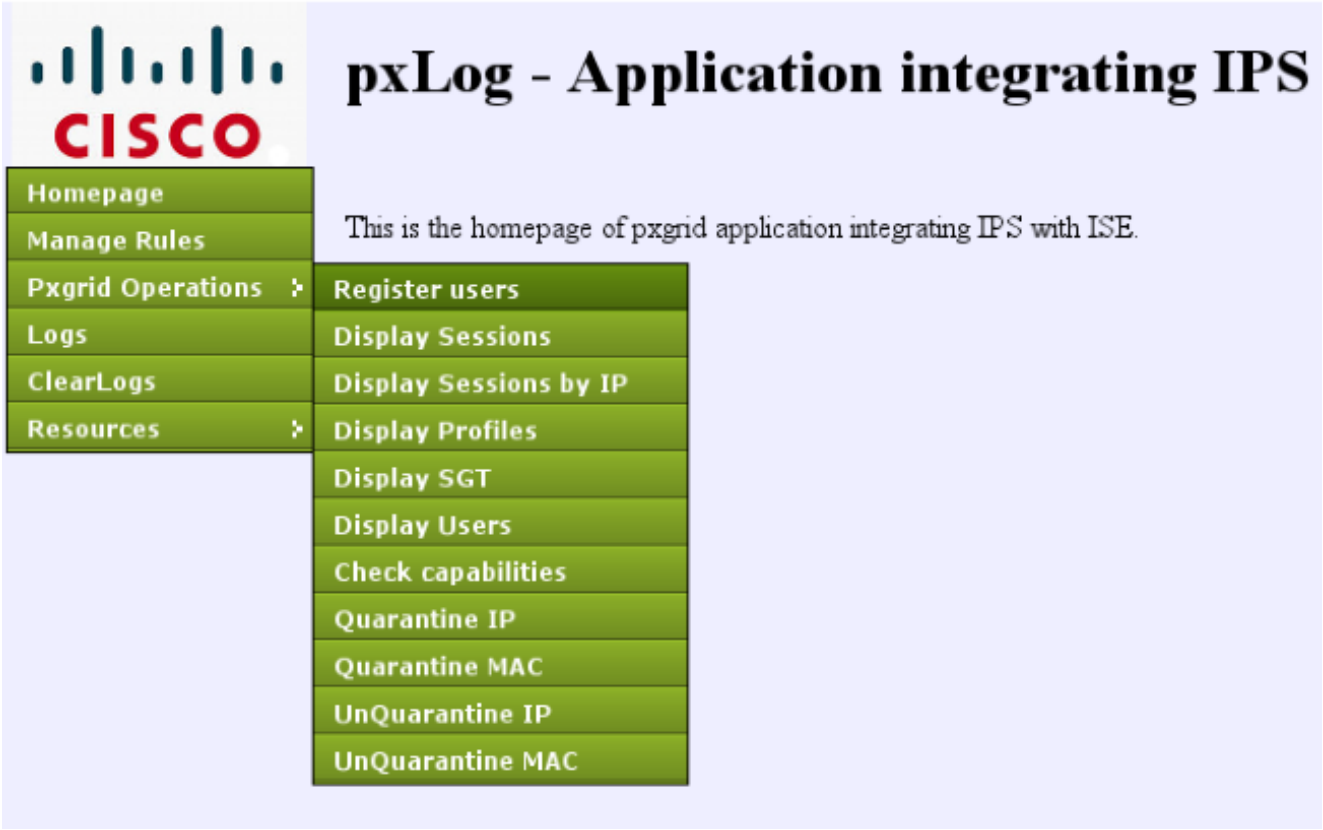
測試

步驟1.註冊pxGrid

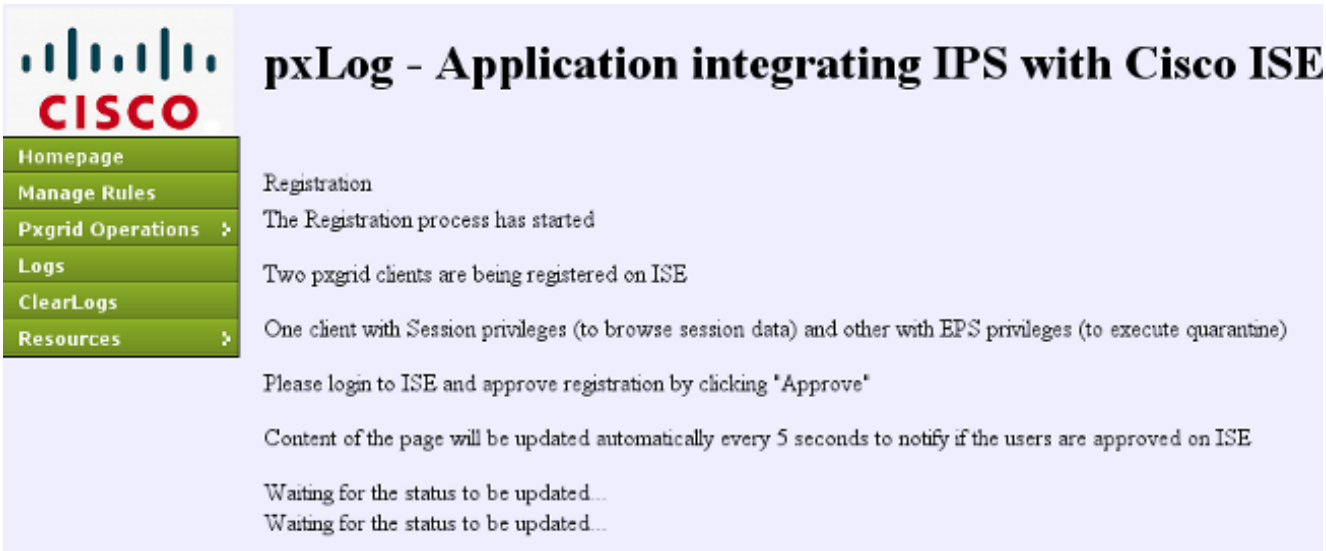
pxLog應用程式在Tomcat啟動時自動部署。

1. 要使用pxGrid，請在ISE中註冊兩個使用者（一個具有會話訪問許可權，另一個具有隔離區

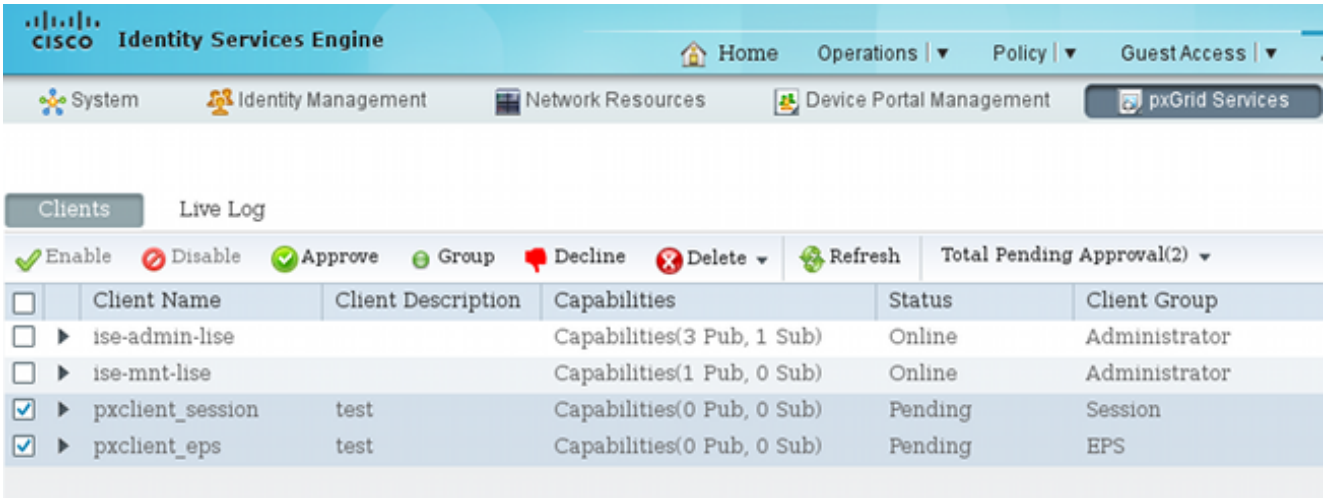
）。 可從**Pxgrid Operations > Register users**完成此操作：



註冊將自動啟動：



2. 在這個階段，需要批准ISE上的註冊使用者（預設情況下禁用自動批准）：



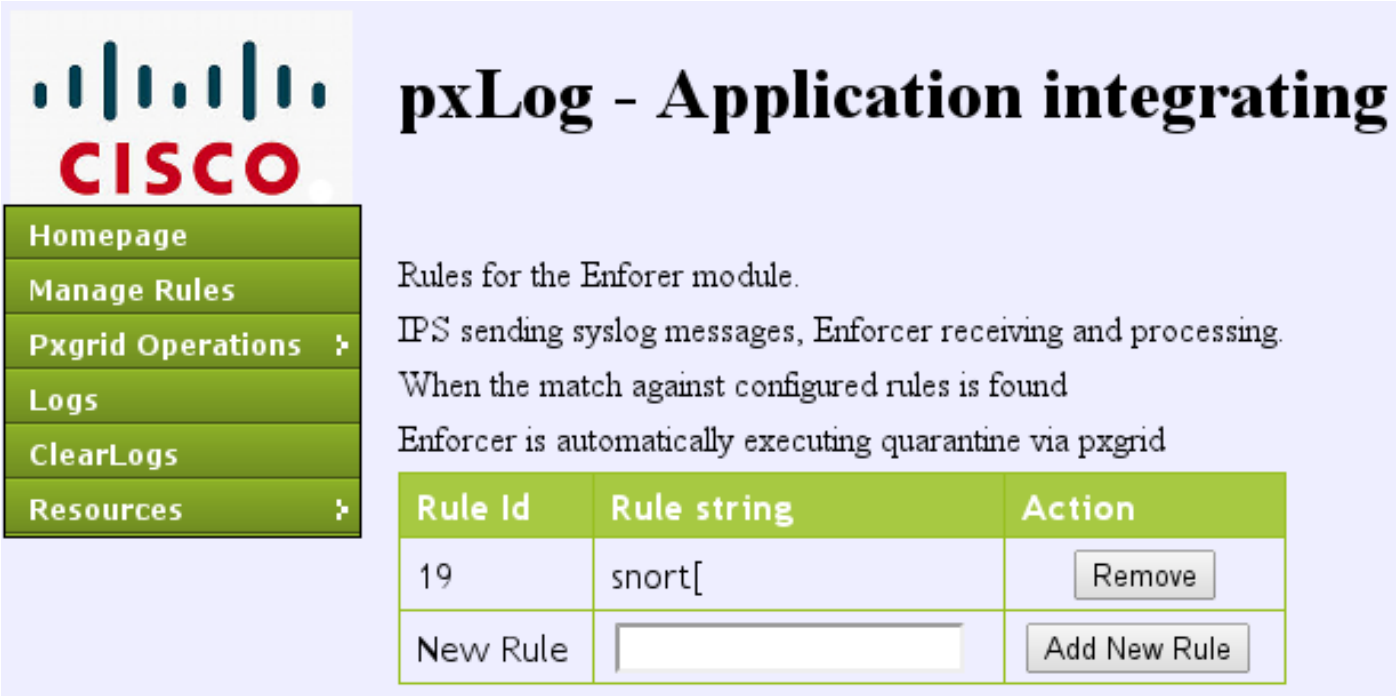
批准後，pxLog會自動通知管理員（通過AJAX呼叫）：

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

ISE將這兩個使用者的狀態顯示為Online或Offline（不再為Pending）。

步驟2.pxLog規則配置

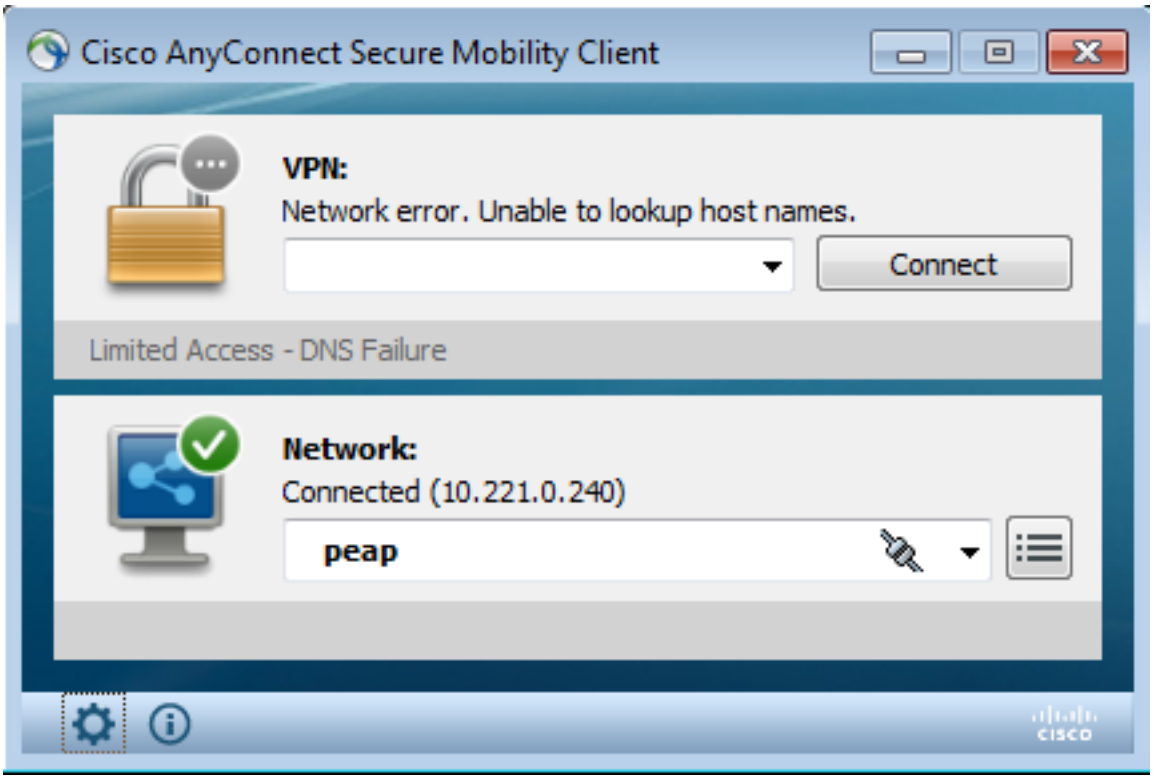
pxLog必須處理系統日誌消息，並根據消息執行操作。若要新增新規則，請選擇**Manage Rules**:



現在，Enforcer模組在系統日誌消息中查詢此正規表示式(RegExp):「snort[」。 如果找到，它會搜尋所有IP地址，並選擇最後一個地址之前的地址。這符合大多數安全解決方案。有關詳細資訊，請參閱系統日誌部分。該IP地址（攻擊者）通過pxGrid隔離。也可以使用更精細的規則（例如，可能包括簽名編號）。

步驟3.第一個Dot1x會話

Microsoft Windows 7工作站啟動有線dot1x會話。Cisco Anyconnect NAM已被用作請求方。已配置可擴展身份驗證協定保護的EAP(EAP-PEAP)方法。



ISE **Dot1x Full Access** Authorization profile被選中。交換器下載存取清單以便授予完全存取許可權：

```
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
```

步驟4. Microsoft Windows PC傳送觸發警報的資料包

這顯示如果確實從TTL = 7的Microsoft Windows資料包傳送時會發生的情況：

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

轉發鏈中的Snort會降低該值，並發出警報。因此，向pxLog傳送系統日誌消息：

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

步驟5.pxLog

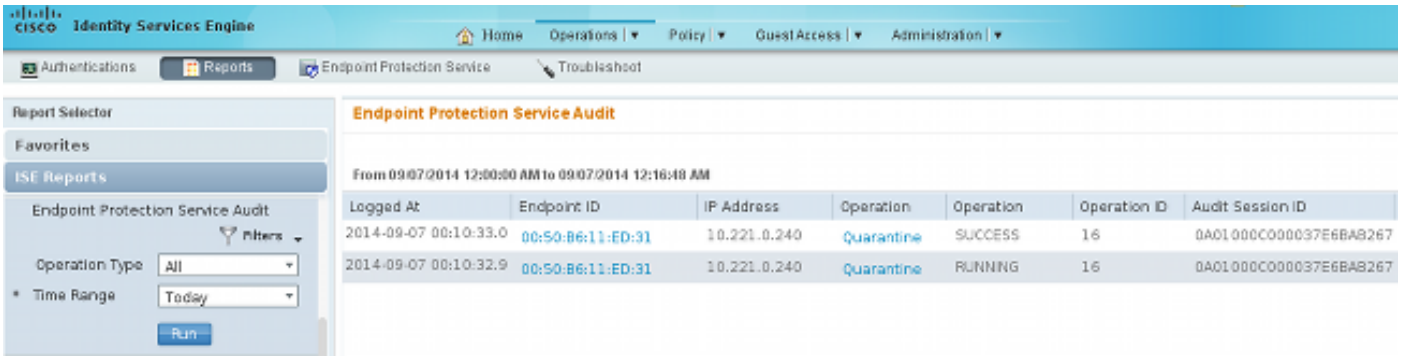
pxLog接收系統日誌消息，對其進行處理，並請求隔離該IP地址。如果檢查日誌，可以確認這一點：

Logs from the actions executed by the Enforer module

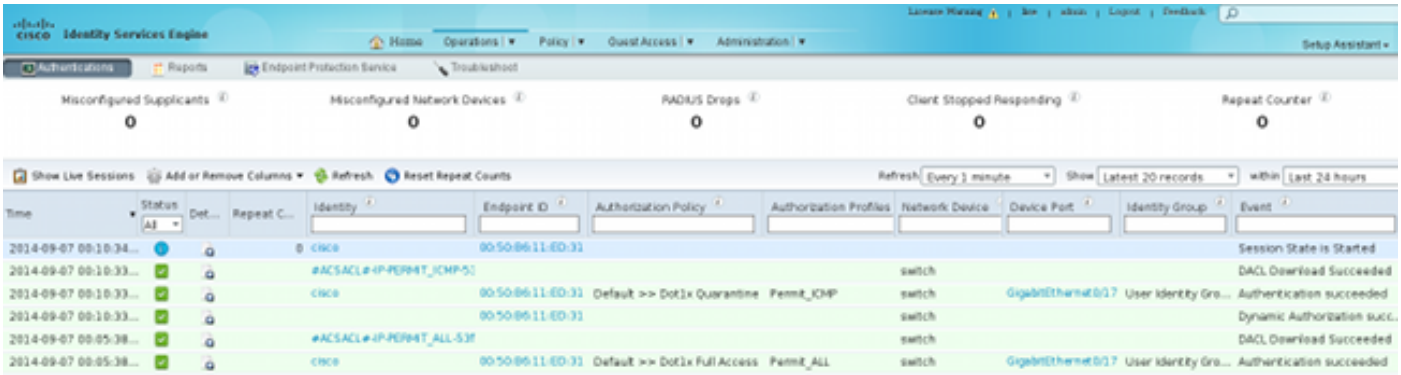
Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

步驟6. ISE隔離

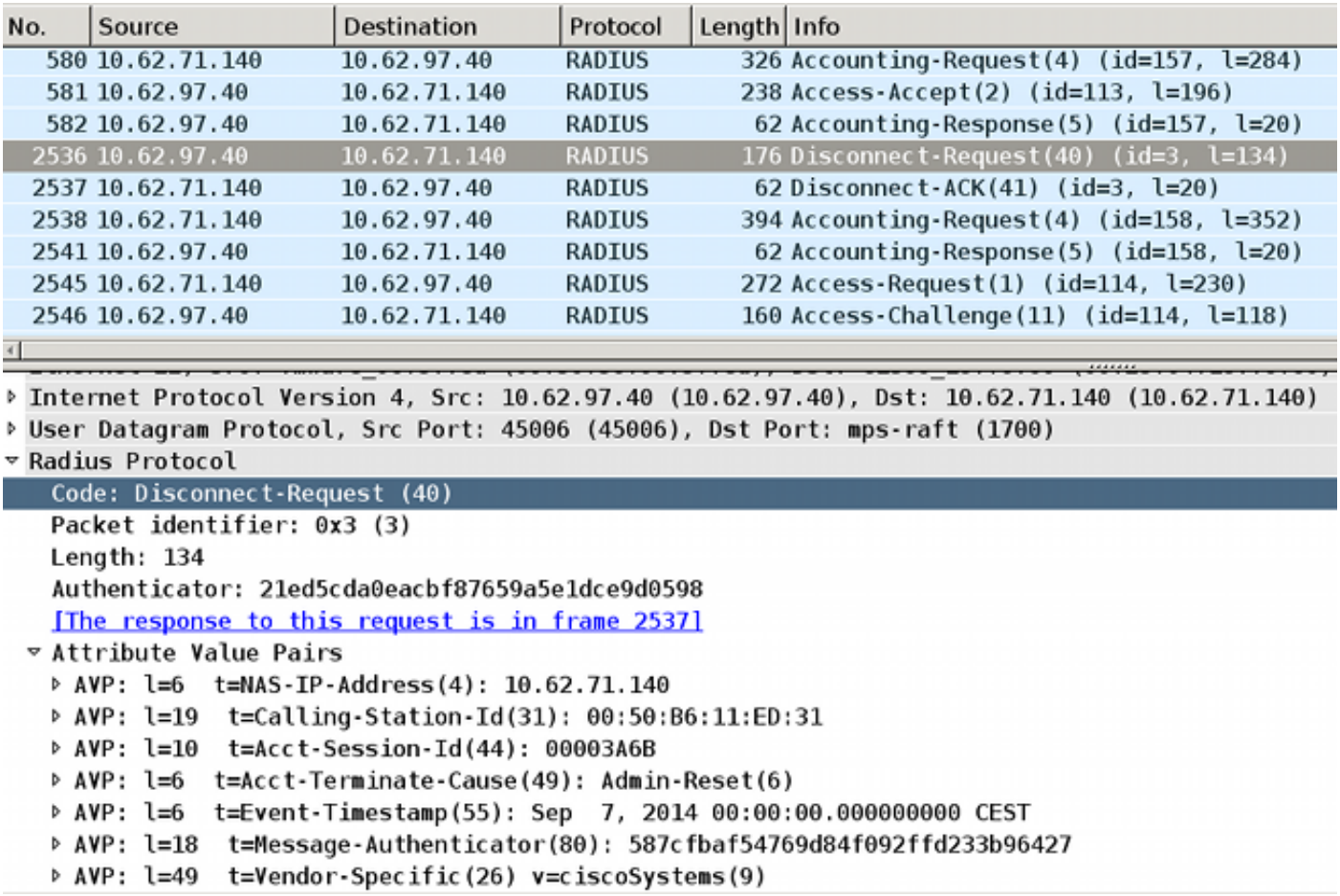
ISE報告IP地址已隔離：



因此，它會檢查授權策略、選擇隔離並傳送RADIUS CoA以更新該特定終端的交換機上的授權狀態。



這是CoA終止消息，強制請求方啟動新會話並獲得有限的訪問許可權(Permit_ICMP):



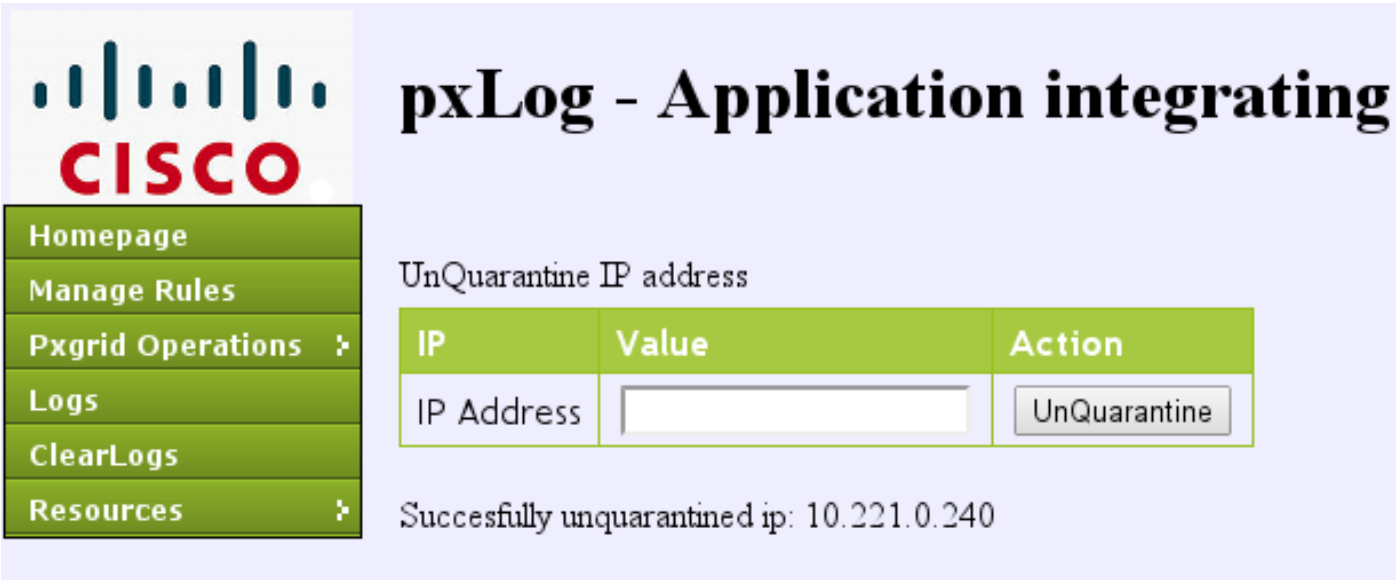
No.	Source	Destination	Protocol	Length	Info
580	10.62.71.140	10.62.97.40	RADIUS	326	Accounting-Request(4) (id=157, l=284)
581	10.62.97.40	10.62.71.140	RADIUS	238	Access-Accept(2) (id=113, l=196)
582	10.62.97.40	10.62.71.140	RADIUS	62	Accounting-Response(5) (id=157, l=20)
2536	10.62.97.40	10.62.71.140	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)

可在交換機上確認結果（終端有限訪問）：

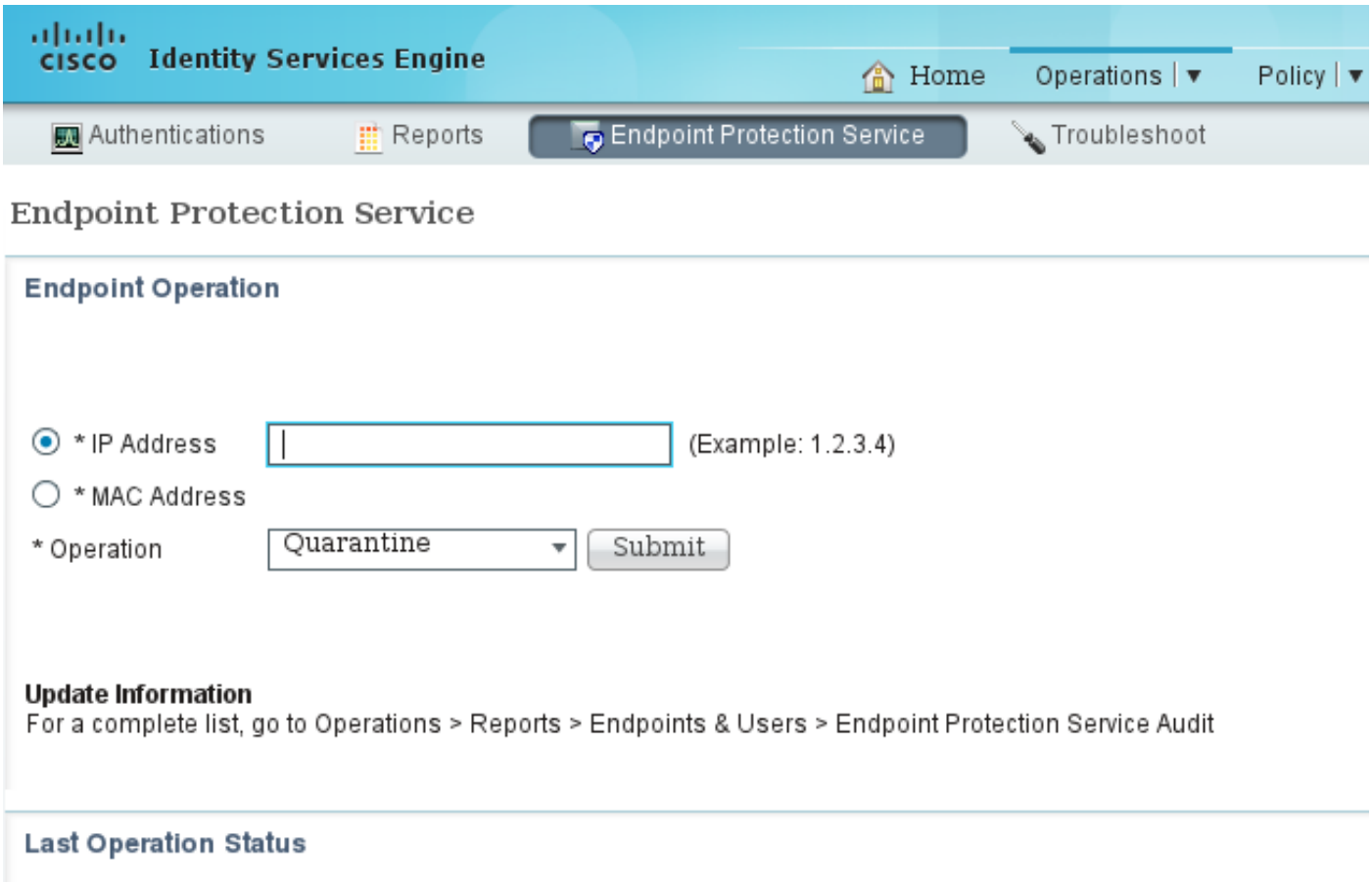
```
3750#show authentication sessions interface g0/17
           Interface:  GigabitEthernet0/17
         MAC Address:  0050.b611.ed31
          IP Address:  10.221.0.240
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure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

步驟7.pxLog取消隔離

在此階段，管理員決定取消隔離該端點：

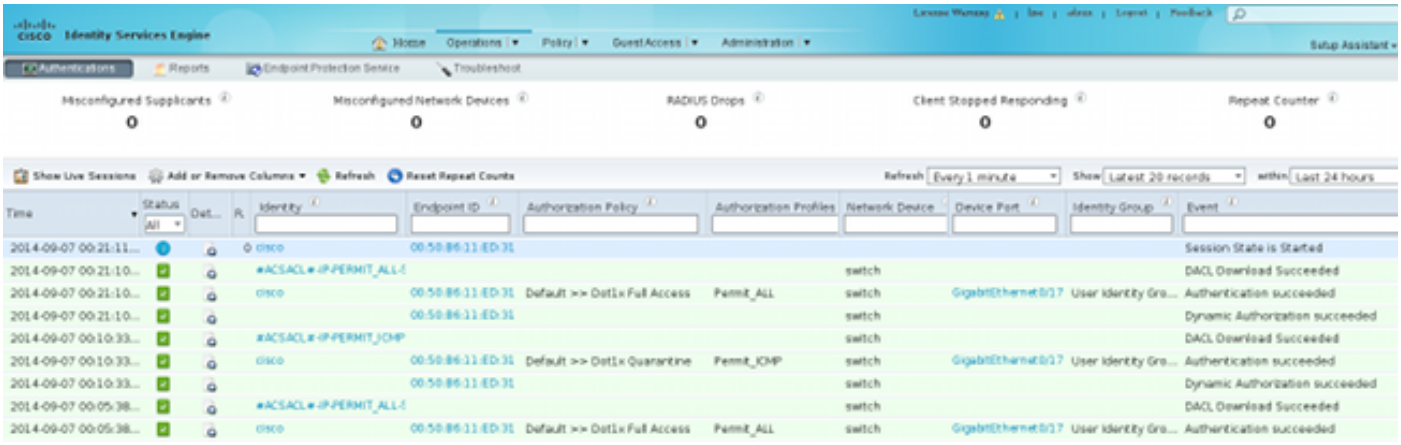


可以直接從ISE執行相同的操作：

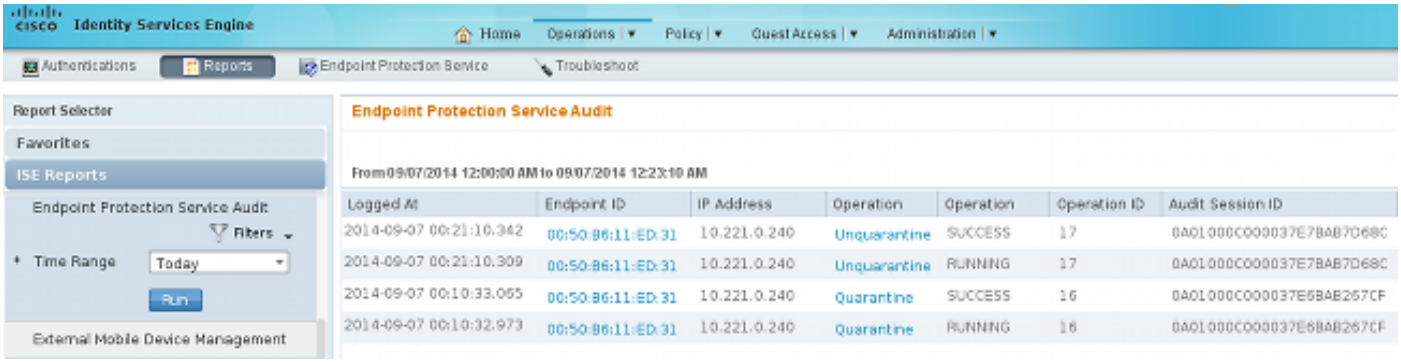


步驟8. ISE取消隔離

ISE再次檢查規則並更新交換機上的授權狀態（授予完整網路訪問許可權）：



報告確認：



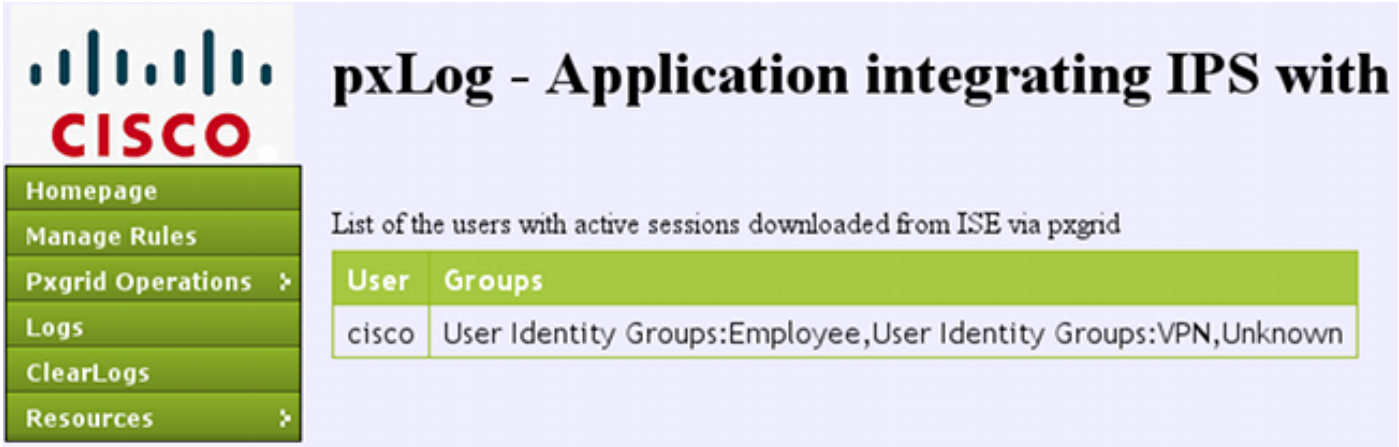
pxLog功能

編寫pxLog應用程式是為了演示pxGrid API的功能。它允許您：

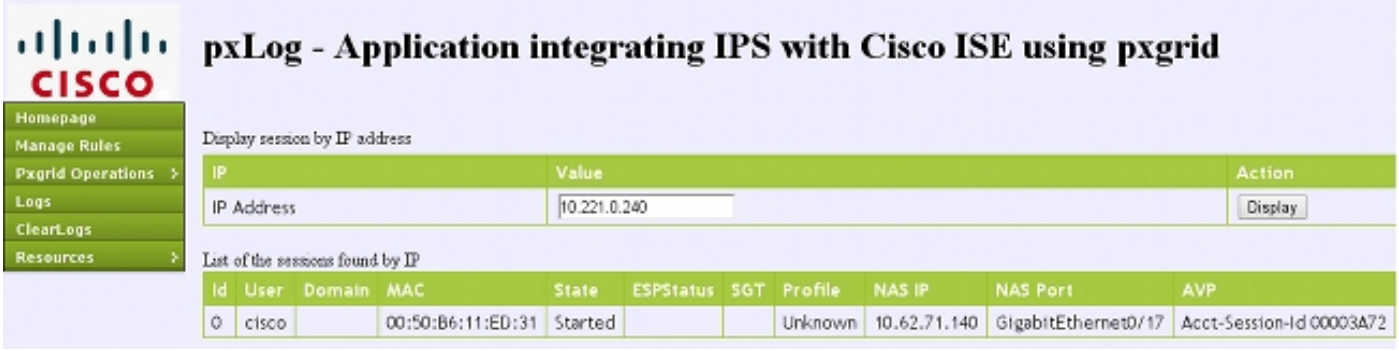
- 在ISE上註冊會話和EPS使用者
- 下載有關ISE上所有活動會話的資訊
- 下載有關ISE上特定活動會話的資訊（按IP地址）
- 下載有關ISE上特定活動使用者的資訊（按使用者名稱）
- 顯示有關所有配置檔案(Profiler)的資訊
- 顯示有關ISE上定義的TrustSec安全組標籤(SGT)的資訊
- 檢查版本（pxGrid的功能）
- 基於IP或MAC地址的隔離
- 基於IP或MAC地址取消隔離

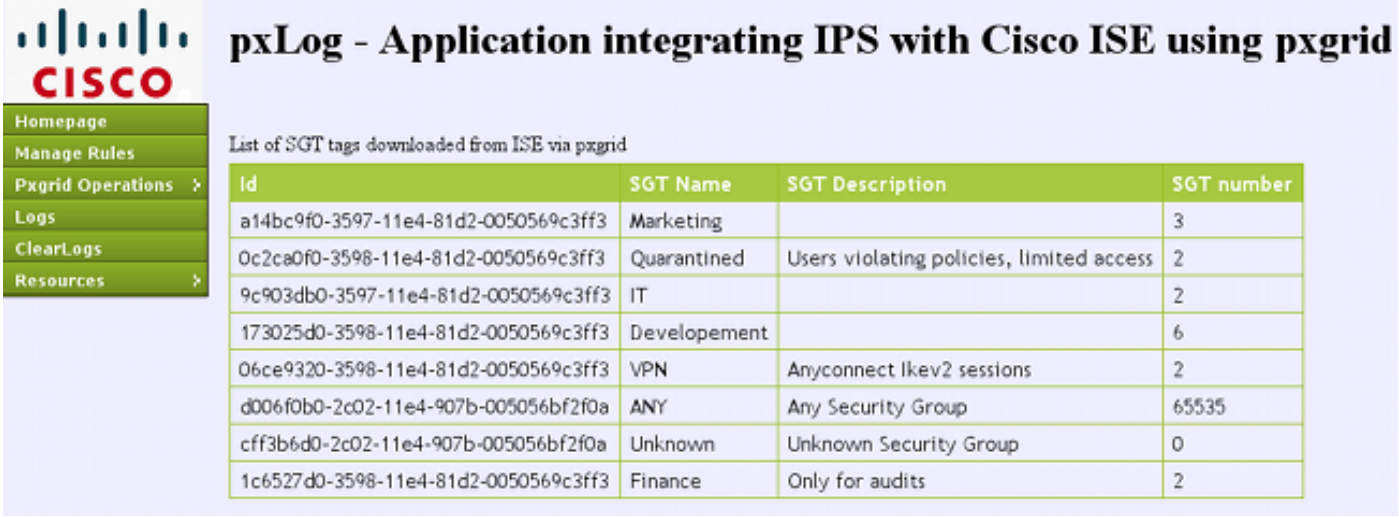
未來會規劃更多功能。

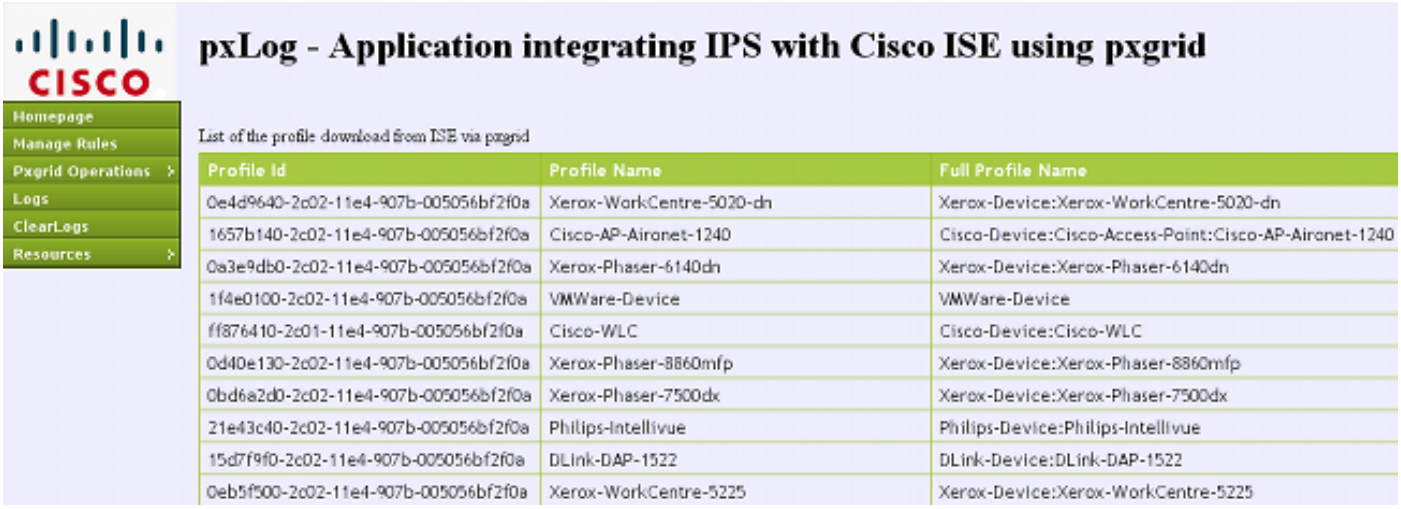
以下是pxLog的一些螢幕截圖：


pxLog - Application integrating IPS with
Homepage
Manage Rules
Pxgrid Operations
Logs
ClearLogs
Resources
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
Homepage
Manage Rules
Pxgrid Operations
Logs
ClearLogs
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
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


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 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協定要求

組

客戶端（使用者）一次可以是一個組的成員。最常用的兩個組是：

- 會話 — 用於瀏覽/下載有關會話/配置檔案/SGT的資訊
- EPS — 用於執行隔離

證書和Java KeyStore

如前所述，客戶端應用程式(pxLog和pxGrid控制器(ISE))都必須配置證書才能通訊。pxLog應用程式將這些檔案儲存在Java KeyStore檔案中：

- **store/client.jks** — 包括使用者端和憑證授權單位(CA)憑證
- **store/root.jks** — 包括ISE鏈：監控和疑難排解節點(MnT)身份和CA證書

檔案受密碼保護(預設：cisco123)。 可以在**WEB-INF/web.xml**中更改檔案位置和密碼。

以下是生成新Java KeyStore的步驟：

1. 要建立根（受信任）金鑰庫，請匯入CA證書(**cert-ca.der**應採用DER格式):

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

2. 建立新金鑰庫時，請選擇一個密碼（稍後用於訪問金鑰庫）。

3. 將MnT身份證書匯入根金鑰庫(**cert-mnt.der**是從ISE獲取的身份證書，應採用DER格式):

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

4. 要建立客戶端金鑰庫，請匯入CA證書：

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

5. 在客戶端金鑰庫中建立私鑰：

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

6. 在客戶端金鑰庫中生成證書簽名請求(CSR):

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

7. 簽署cert-client.csr並匯入簽名的客戶端證書：

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

8. 驗證兩個金鑰庫是否包含正確的證書：

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

注意：升級ISE 1.3節點後，可以選擇保留身份證書，但會刪除CA簽名。因此，升級的ISE使用新證書，但從不在SSL/ServerHello消息中附加CA證書。這會觸發預期（根據RFC）看到完整鏈的客戶端上的故障。

主機名

用於多個功能（如會話下載）的pxGrid API執行其他驗證。客戶端聯絡ISE並接收ISE主機名，該主機名由CLI中的hostname命令定義。然後，客戶端嘗試對該主機名執行DNS解析，並嘗試聯絡該IP地址並從該地址獲取資料。如果ISE主機名的DNS解析失敗，客戶端不會嘗試獲取任何資料。

注意：請注意，只有主機名用於此解析（在此情況中列出），而不是完全限定域名(FQDN)(在此情況中為lise.example.com)。

開發人員注意事項

思科發佈並支援pxGrid API。有一個這樣的包：

pxgrid-sdk-1.0.0-167

裡面有：

- 帶有類的pxGrid JAR檔案，可以輕鬆地將其解碼為Java檔案以檢查代碼
- 帶證書的Java KeyStore示例
- 使用使用pxGrid的示例Java類的示例指令碼

系統日誌

以下是使用攻擊者IP地址傳送系統日誌消息的安全解決方案清單。只要在配置中使用正確的RegExp規則，這些規則就可以輕鬆與pxLog整合。

Snort

Snort以以下格式傳送系統日誌警報：

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

以下是範例：

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

攻擊者IP地址總是最後一個地址（目標）之前的第二個地址。 為特定簽名構建粒度RegExp並提取攻擊者IP地址很簡單。以下是特徵碼和訊息網際網100124控制訊息通訊協定(ICMP)的RegExp範例：

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

Cisco Adaptive Security Appliance(ASA)檢測

當ASA配置為進行HTTP（示例）檢測時，相應的系統日誌消息如下所示：

```
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
```

同樣，可以使用精細的RegExp來過濾這些消息並提取攻擊者的IP地址，這是最後一個地址之前的第二個地址。

Cisco Sourcefire新世代入侵防禦系統(NGIPS)

以下是Sourcefire感測器傳送的示例消息：

```
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
```

同樣，提取攻擊者IP地址非常簡單，因為使用相同的邏輯。此外，還提供策略名稱和簽名，因此pxLog規則可以是精細的。

Juniper NetScreen

以下是舊版Juniper入侵檢測和預防(IDP)傳送的示例消息：

```
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"
```

攻擊者的IP地址也可以以相同方式提取。

Juniper JunOS

JunOS類似：

```
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

下面是一些Linux iptables示例。

```
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
```

您可以使用連線跟蹤、xtables、rpfilters、模式匹配等表模組提供的高級功能傳送任何型別資料包的系統日誌資訊。

FreeBSD IP防火牆(IPFW)

以下是IPFW封鎖片段的範例訊息：

```
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就緒和CoA處理

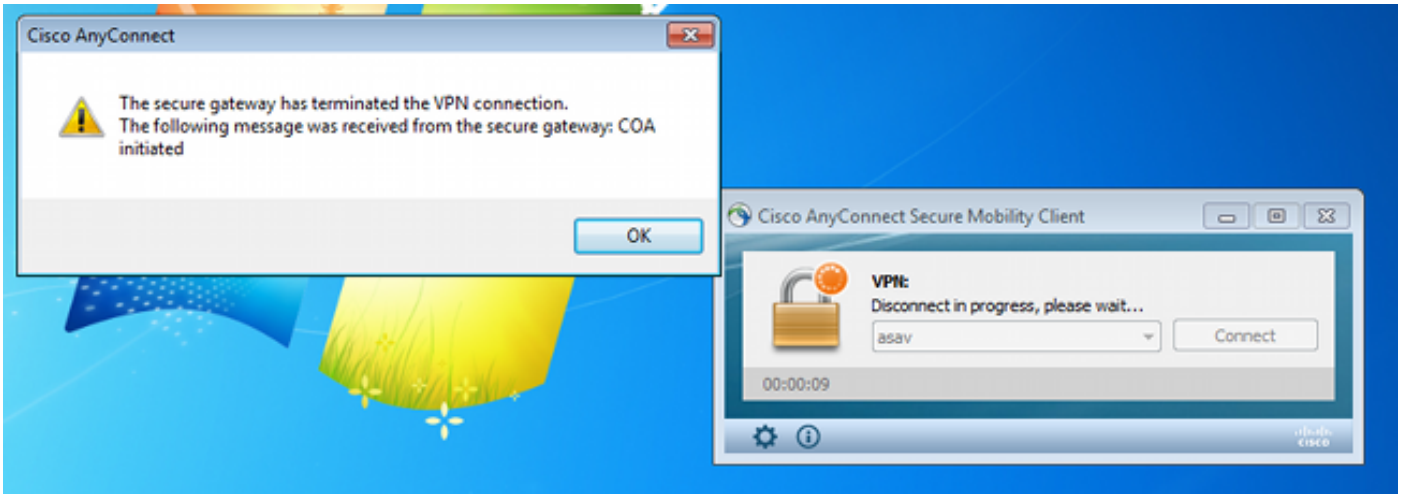
ISE能夠根據CoA處理識別會話型別。

- 對於有線802.1x/MAC身份驗證繞行(MAB),ISE傳送CoA重新身份驗證，這將觸發第二次身份驗證。

- 對於無線802.1x/MAB，ISE傳送CoA終端，後者觸發第二次身份驗證。

- 對於ASA VPN，ISE傳送附加了新DACL的CoA（無第二次身份驗證）。

EPS模組簡單。在執行隔離時，它始終傳送CoA終止資料包。對於有線/無線會話，這不是問題（所有802.1x請求方都可以透明地啟動第二個EAP會話）。 但是，當ASA收到CoA終止時，它將丟棄VPN會話，終端使用者會看到以下資訊：



有兩種可能的解決方案可以強制AnyConnect VPN自動重新連線（在XML配置檔案中配置）：

- Autoreconnect，僅在與VPN網關失去連線時起作用，而不是用於管理終止

- Always-on，工作正常並強制AnyConnect自動重新建立會話

即使建立了新會話，ASA也會選擇新的稽核會話ID。從ISE的角度來看，這是一個新會話，並且沒有機會遇到隔離規則。對於VPN，終端的MAC地址也不能用作標識，與有線/無線dot1x相反。

解決方案是強制EPS像ISE一樣運行，並根據會話傳送正確的CoA型別。此功能將在ISE版本1.3.1中引入。

pxGrid合作夥伴和解決方案

以下是pxGrid合作夥伴和解決方案的清單：

- LogRhythm（安全資訊和事件管理，SIEM） — 支援表示狀態傳輸(REST)API
- Splunk(SIEM) — 支援REST API
- HP Arcsight(SIEM) — 支援REST API
- Sentinel NetIQ(SIEM) — 計畫支援pxGrid
- Lancope StealthWatch(SIEM) — 計畫支援pxGrid
- Cisco Sourcefire — 計畫支援pxGrid 1HCY15

- 思科網路安全裝置(WSA) — 計畫在2014年4月支援pxGrid

以下是其他合作夥伴和解決方案：

- 可持續（漏洞評估）
- Emulex（資料包捕獲和調查分析）
- Bayshore網路(防資料丟失(DLP)和物聯網(IoT)策略)
- Ping身份(身份和訪問管理(IAM)/單點登入(SSO))
- Qradar(SIEM)
- LogLogic(SIEM)
- Symantec(SIEM amd流動裝置管理(MDM))

請參閱Marketplace解決方案目錄，獲取完整的安全解決方案清單。

ISE API:REST vs EREST vs pxGrid

ISE版本1.3提供三種型別的API。

以下是比較結果：

	REST	外部REST	pxGrid
客戶端身份驗證	使用者名稱+密碼（基本HTTP身份驗證）	使用者名稱+密碼（基本HTTP身份驗證）	憑證
許可權分離	否	有限（ERS管理）	是（組）
訪問	MnT	MnT	MnT
傳輸	tcp/443(HTTPS)	tcp/9060(HTTPS)	tcp/5222(XMPP)
HTTP方法	GET	GET/POST/PUT	獲取/發佈
預設啟用	是	否	否
運算元	很少	許多	很少
CoA終止	支援	否	支援
CoA重新驗證	支援	否	支援*
使用者操作	否	是	否
終端操作	否	是	否
終端身份組操作	否	是	否
隔離(IP、MAC)	否	否	是
解除隔離(IP、MAC)	否	否	是
PortBounce/Shutdown	否	否	是
訪客使用者操作	否	是	否
訪客門戶操作	否	是	否
網路裝置操作	否	是	否
網路裝置組操作	否	是	否

*隔離使用ISE版本1.3.1提供的統一CoA支援。

下載

pxLog可以從Sourceforge下載。

已包含軟體開發套件(SDK)。有關pxGrid的最新SDK和API文檔，請聯絡您的合作夥伴或思科客戶團隊。

相關資訊

- Cisco ISE 1.2 REST API
- Cisco ISE 1.2外部REST風格的API
- 思科ISE 1.3管理員指南
- 技術支援與文件 - Cisco Systems