Integrazione di ISE versione 1.3 pxGrid con l'applicazione IPS pxLog

Sommario

Introduzione

Identity Services Engine (ISE) versione 1.3 supporta una nuova API chiamata pxGrid. Questo protocollo moderno e flessibile che supporta l'autenticazione, la crittografia e i privilegi (gruppi) consente una facile integrazione con altre soluzioni di sicurezza. Questo documento descrive l'utilizzo dell'applicazione pxLog scritta come prova di concetto. pxLog è in grado di ricevere messaggi syslog da IPS (Intrusion Prevention System) e inviare messaggi pxGrid ad ISE per mettere in quarantena l'autore dell'attacco. Di conseguenza, ISE utilizza RADIUS Change of Authorization (CoA) per modificare lo stato di autorizzazione dell'endpoint che limita l'accesso alla rete. Tutto questo avviene in modo trasparente per l'utente finale.

Per questo esempio, come IPS è stato utilizzato Snort, ma è possibile utilizzare qualsiasi altra soluzione. In realtà non deve essere un IPS. è sufficiente inviare il messaggio syslog a pxLog con l'indirizzo IP dell'autore dell'attacco. Questo crea la possibilità di integrare un gran numero di soluzioni.

Questo documento illustra anche come risolvere i problemi e testare le soluzioni pxGrid, con i problemi e le limitazioni tipici.

Avvertenza: L'applicazione pxLog non è supportata da Cisco. Questo articolo è stato scritto come prova di concetto. Lo scopo principale era quello di usarlo durante il test migliore dell'implementazione di pxGrid sull'ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione di Cisco ISE e delle conoscenze base su questi argomenti:

- Implementazioni ISE e configurazione dell'autorizzazione
- Configurazione CLI degli switch Cisco Catalyst

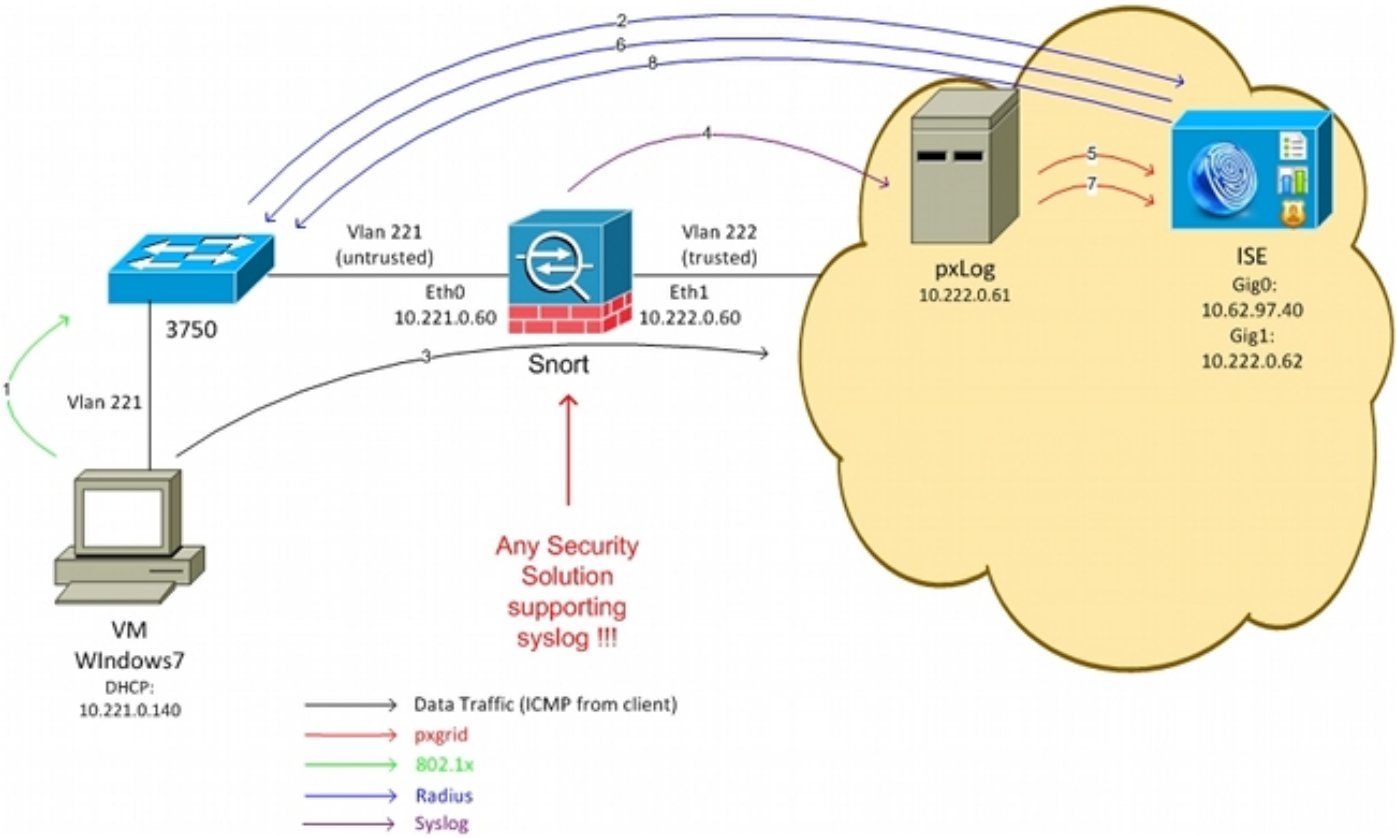
Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7

- Software Cisco Catalyst serie 3750X Switch, versioni 15.0 e successive
- Software Cisco ISE, versione 1.3 e successive
- Cisco AnyConnect Mobile Security con Network Access Manager (NAM), versione 3.1 e successive
- Snort versione 2.9.6 con acquisizione dati (DAQ)
- Applicazione pxLog installata su Tomcat 7 con MySQL versione 5

Esempio di rete e flusso del traffico



Di seguito è riportato il flusso del traffico, come mostrato nello schema della rete:

1. Un utente di Microsoft Windows 7 si connette allo switch ed esegue l'autenticazione 802.1x.

2. Lo switch usa l'ISE come server di autenticazione, autorizzazione e accounting (AAA). La regola di autorizzazione **Accesso completo Dot1x** corrisponde e viene concesso l'accesso completo alla rete (DACL: PERMIT_ALL).

3. L'utente tenta di connettersi alla rete attendibile e viola la regola Snort.

4. Di conseguenza, Snort invia un avviso all'applicazione pxLog (tramite syslog).

5. L'applicazione pxLog esegue la verifica rispetto al proprio database locale. È configurato per intercettare i messaggi syslog inviati da Snort ed estrarre l'indirizzo IP dell'autore dell'attacco. Quindi usa pxGrid per inviare una richiesta all'ISE in modo da mettere in quarantena l'indirizzo IP dell'utente malintenzionato (l'ISE è un controller pxGrid).

6. L'ISE riesamina la sua politica di autorizzazione. Poiché l'endpoint è in quarantena, viene

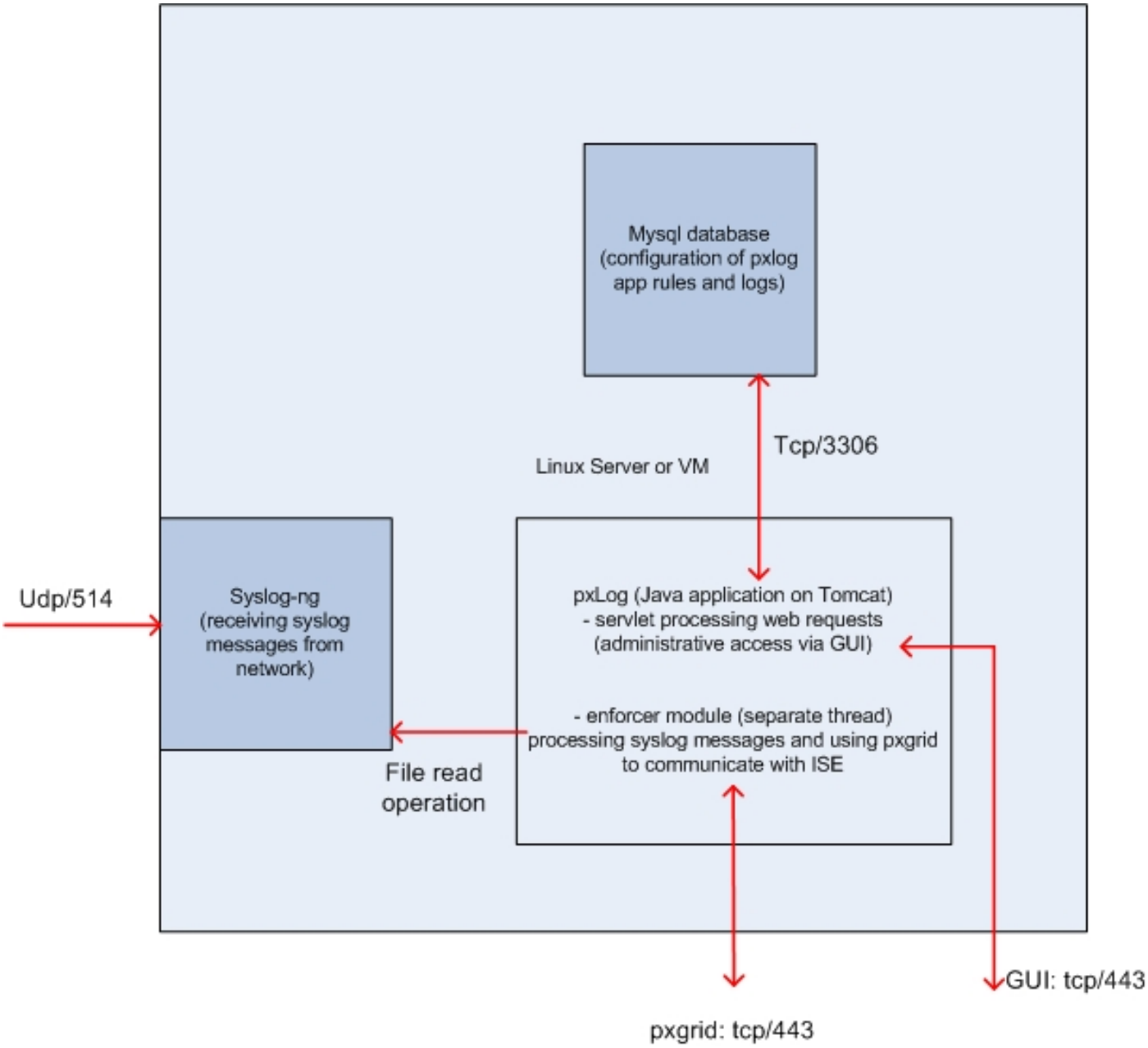
soddisfatta la condizione **Session:EPSStatus EQUALS Quarantine** e viene confrontato un profilo di autorizzazione diverso (**Dot1x Quarantine**). L'ISE invia un messaggio CoA Terminate allo switch per terminare la sessione. In questo modo viene attivata la riautenticazione e viene applicato un nuovo ACL scaricabile (DACL) (PERMIT_ICMP), che fornisce all'utente finale un accesso di rete limitato.

7. In questa fase, l'amministratore può decidere di riattivare la quarantena per l'endpoint. Ciò è possibile tramite la GUI di pxLog. Anche in questo caso, viene inviato il messaggio pxGrid verso l'ISE.

8. L'ISE esegue un'operazione simile a quella della fase 6. Questa volta, l'endpoint non è più in quarantena e viene fornito l'accesso completo.

pxLog

Architettura



La soluzione consiste nell'installare un set di applicazioni su un computer Linux:

1. Applicazione pxLog scritta in Java e distribuita sul server Tomcat. La domanda è composta da:

   Servlet che elabora le richieste Web: utilizzato per accedere al pannello di amministrazione tramite il browser Web.

   Modulo Enforcer: thread avviato insieme al servlet. Enforcer legge i messaggi syslog dal file (ottimizzato), li elabora secondo le regole configurate ed esegue azioni (come la quarantena tramite pxGrid).

2. Il database MySQL che contiene la configurazione per pxLog (regole e registri).

3. Il server syslog che riceve i messaggi syslog dai sistemi esterni e li scrive in un file.

Installazione

L'applicazione pxLog utilizza le seguenti librerie:

- jQuery (per supporto AJAX)
- JSTL (JavaServer Pages Standard Tag Library) (modello MVC (Model View Controller). I dati sono separati dalla logica: Il codice JavaServer Page (JSP) viene utilizzato solo per il rendering, non per il codice HTML nelle classi Java
- Log4j come sottosistema di log
- Connettore MySQL
- displaytag per rendering/ordinamento di tabelle
- API pxGrid di Cisco (attualmente versione alpha 147)

Tutte queste librerie si trovano già nella directory lib del progetto, quindi non è necessario scaricare altri file Java ARchive (JAR).

Per installare l'applicazione:

1. Decomprimere l'intera directory nella directory Tomcat Webapp.

2. Modificare il file **WEB-INF/web.xml**. L'unica modifica richiesta è la variabile **serverip**, che deve puntare all'ISE. È inoltre possibile che vengano generati gli archivi chiavi dei certificati Java (uno per l'attendibilità e uno per l'identità) anziché quelli predefiniti. Viene utilizzata dall'API pxGrid che utilizza la sessione SSL (Secure Sockets Layer) con i certificati client e server. Entrambe le parti della comunicazione devono presentare il certificato e devono fidarsi a vicenda. Per ulteriori informazioni, consultare la sezione Requisiti del protocollo pxGrid.

3. Verificare che il nome host ISE sia risolto correttamente in pxLog (fare riferimento al record nella **voce** DNS (Domain Name Server) o**/etc/hosts**). Per ulteriori informazioni, consultare la sezione Requisiti del protocollo pxGrid.

4. Configurare il database MySQL con lo script **mysql/init.sql**. Le credenziali possono essere modificate ma devono essere riportate nel file **WEB-INF/web.xml**.

Snort

Questo articolo non si concentra su alcun IPS specifico, e per questo motivo viene fornita solo una breve spiegazione.

Lo snort è configurato in linea con il supporto DAQ. Il traffico viene reindirizzato con iptables:

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

Quindi, dopo l'ispezione, viene iniettato e inoltrato secondo le regole predefinite.

Sono state configurate alcune regole di snort personalizzate (il file **/etc/snort/rules/test.rules** è incluso nella configurazione globale).

```
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 invia un messaggio syslog quando il valore TTL (Time To Live) del pacchetto è uguale a 6 o le dimensioni del payload sono comprese tra 66 e 686. Il traffico non viene bloccato da Snort.

Èinoltre necessario impostare delle soglie per garantire che gli allarmi non siano attivati troppo spesso (**/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
```

Il server syslog punta quindi al computer pxLog (**/etc/snort/snort.conf**):

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

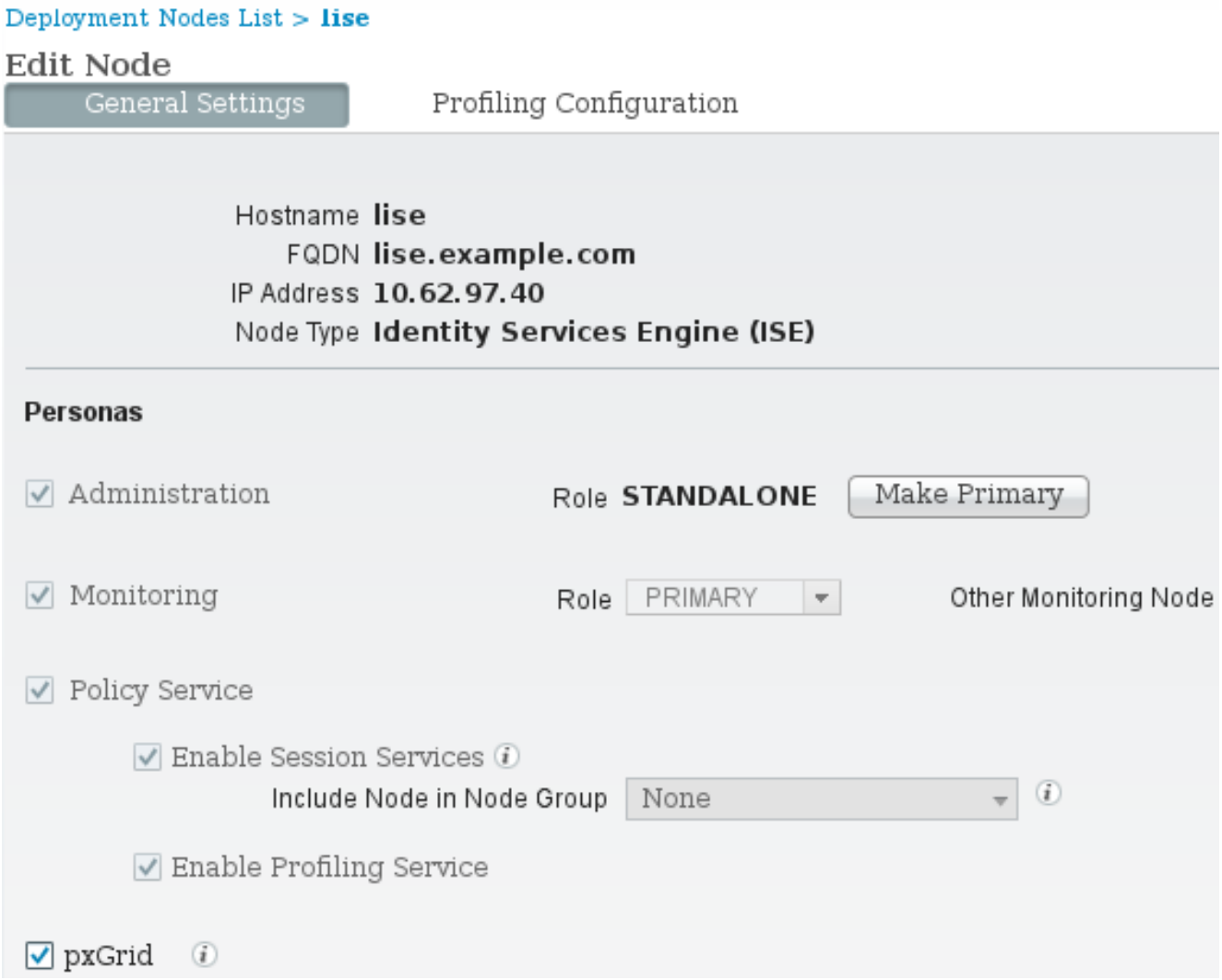
Per alcune versioni di Snort, ci sono bug relativi alla configurazione syslog, quindi è possibile usare le impostazioni predefinite che puntano a localhost e syslog-ng può essere configurato per inoltrare messaggi specifici all'host pxLog.

ISE

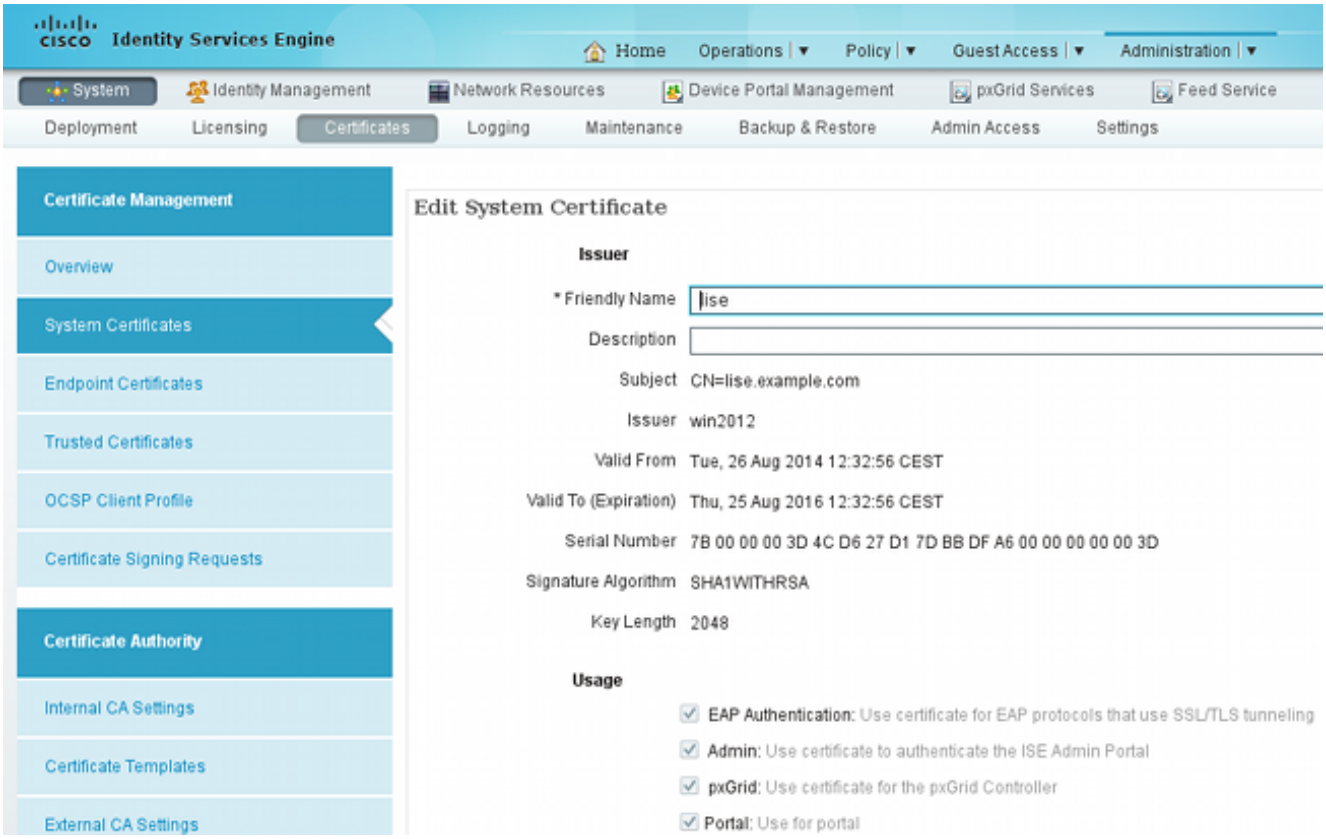
Configurazione

Persona e certificato

1. Abilitare il ruolo pxGrid, disabilitato per impostazione predefinita in ISE, in **Amministrazione > Distribuzione**:

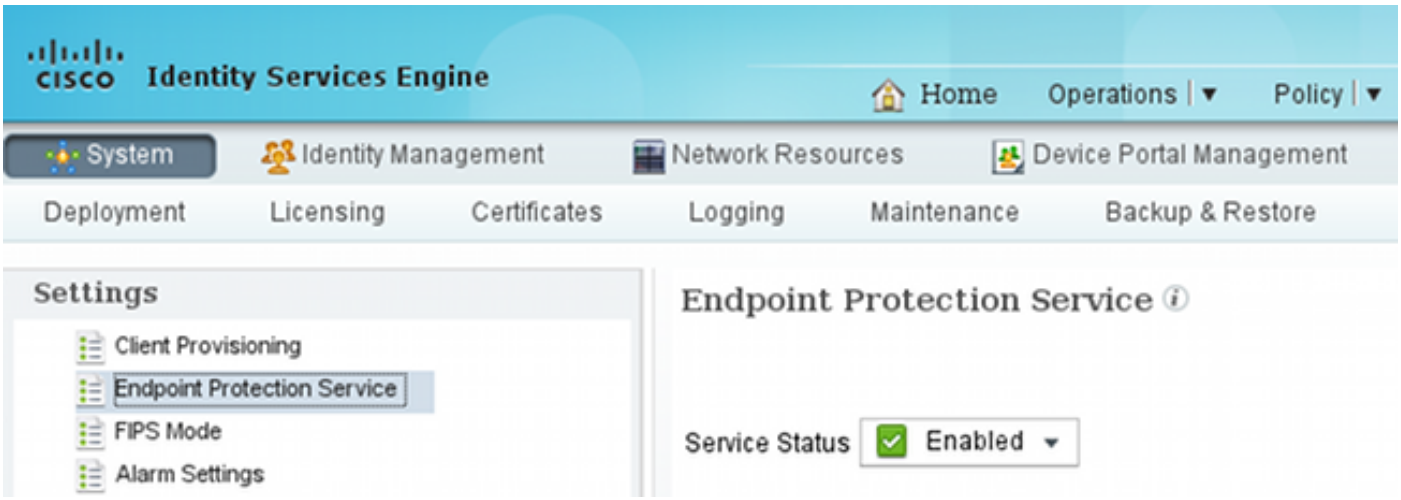


2. Verificare se i certificati sono utilizzati per pxGrid in **Amministrazione > Certificati > Certificati di sistema**:



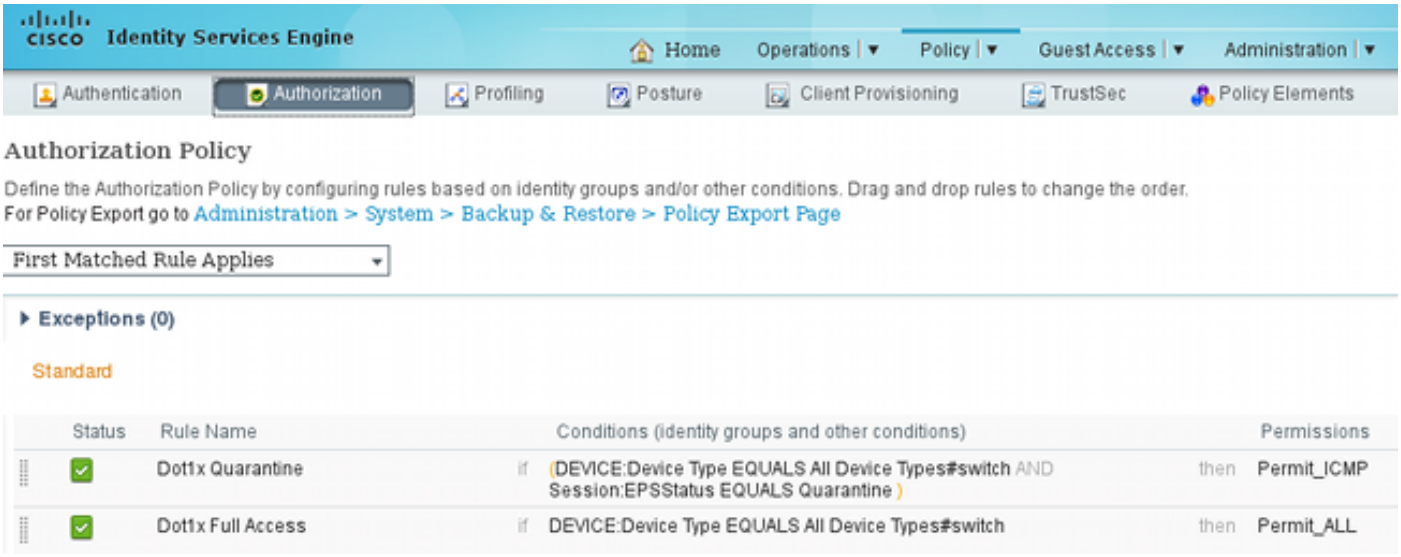
Servizio Endpoint Protection

EPS deve essere abilitato (disabilitato per impostazione predefinita) da **Amministrazione > Impostazioni**:



In questo modo è possibile utilizzare la funzionalità di quarantena/rimozione della quarantena.

Regole di autorizzazione



La prima regola viene rilevata solo quando l'endpoint viene messo in quarantena. L'accesso limitato viene quindi applicato in modo dinamico dalla CoA RADIUS. Inoltre, lo switch deve essere aggiunto ai dispositivi di rete con il segreto condiviso corretto.

Risoluzione dei problemi

Lo stato di pxGrid può essere verificato dalla 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
```

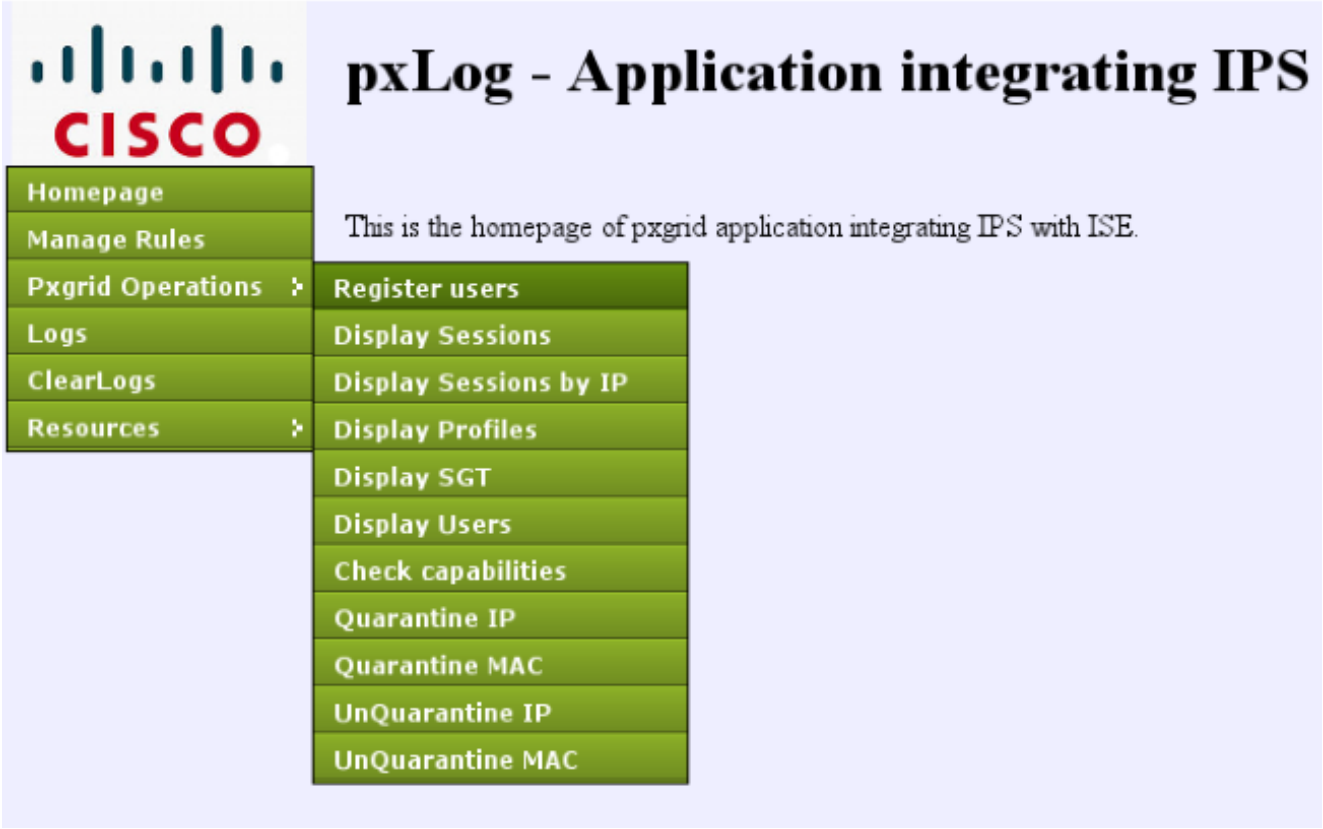
Sono inoltre disponibili debug separati per pxGrid (**Amministrazione > Registrazione > Configurazione registro di debug > pxGrid**). I file di debug sono memorizzati nella directory pxGrid. I dati più importanti si trovano nei siti **pxgrid/pxgrid-jabberd.log** e **pxgrid/pxgrid-controller.log**.

Test

Passaggio 1. Registrazione per pxGrid

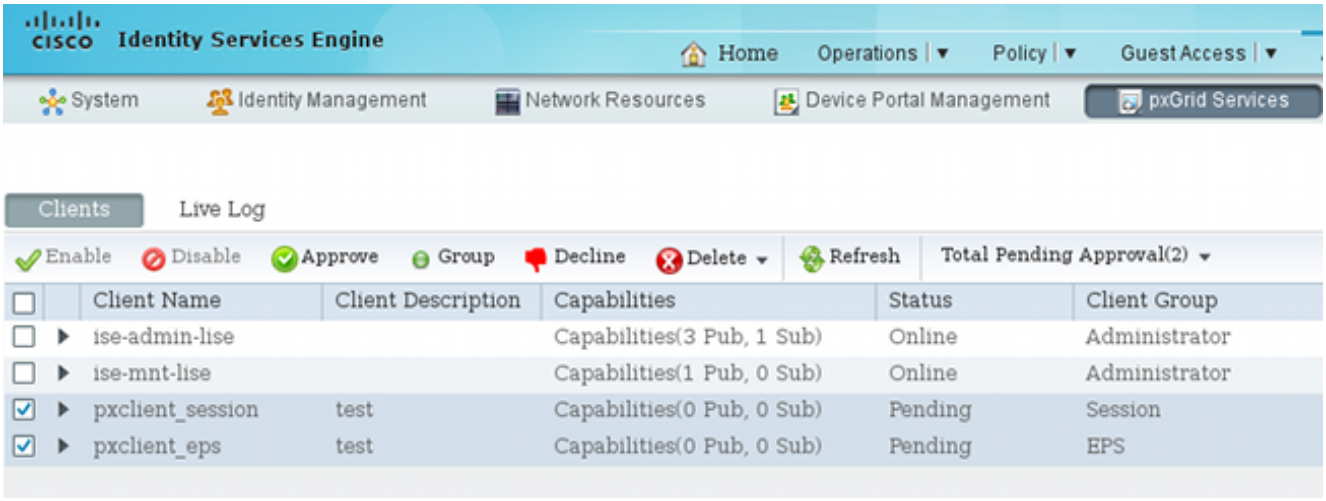
L'applicazione pxLog viene distribuita automaticamente all'avvio di Tomcat.

1. Per utilizzare pxGrid, registrare due utenti nell'ISE (uno con accesso alla sessione e uno con quarantena). È possibile completare questa operazione da **Operazioni Pxgrid > Registra utenti**:



La registrazione viene avviata automaticamente:

2. In questa fase, è necessario approvare gli utenti registrati sull'ISE (l'approvazione automatica è disabilitata per impostazione predefinita):



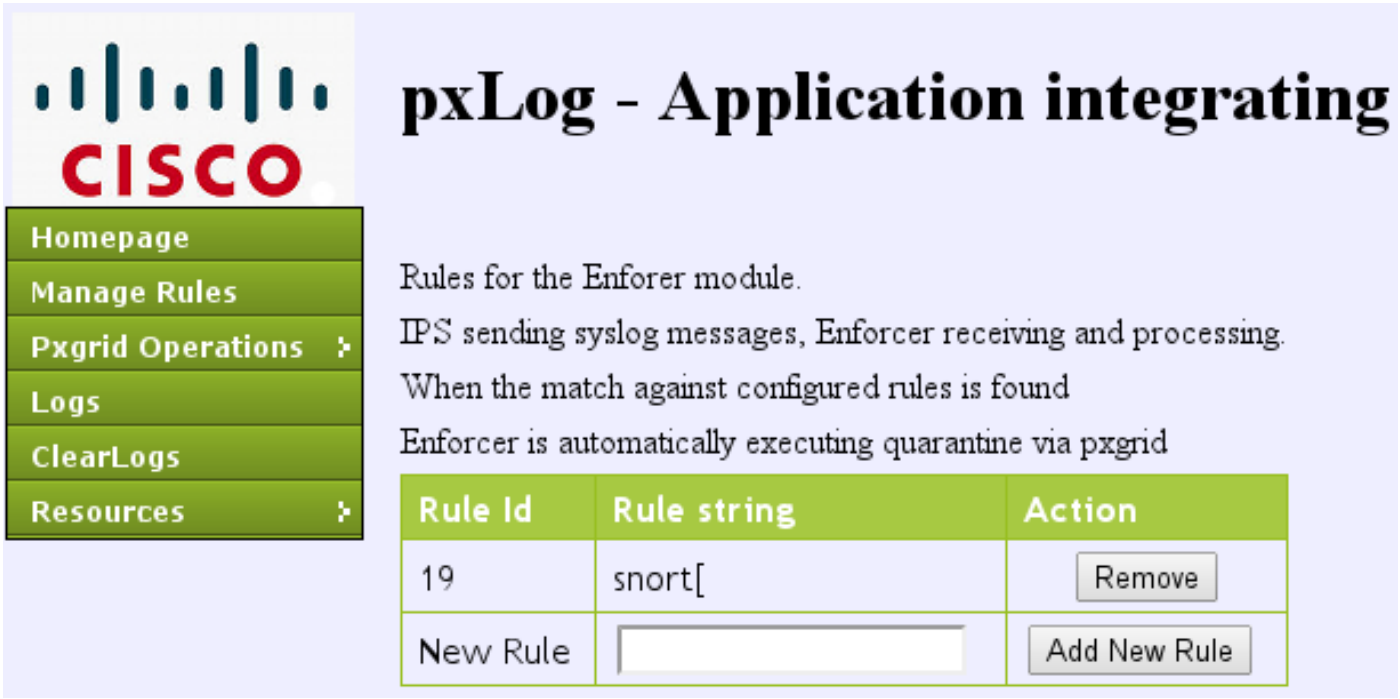
Dopo l'approvazione, pxLog avvisa automaticamente l'amministratore (tramite una chiamata AJAX):

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

ISE mostra lo stato di questi due utenti come Online o Offline (non più In sospeso).

Passaggio 2. Configurazione regole pxLog

pxLog deve elaborare i messaggi syslog ed eseguire le azioni in base ad essi. Per aggiungere una nuova regola, selezionare **Gestisci regole**:

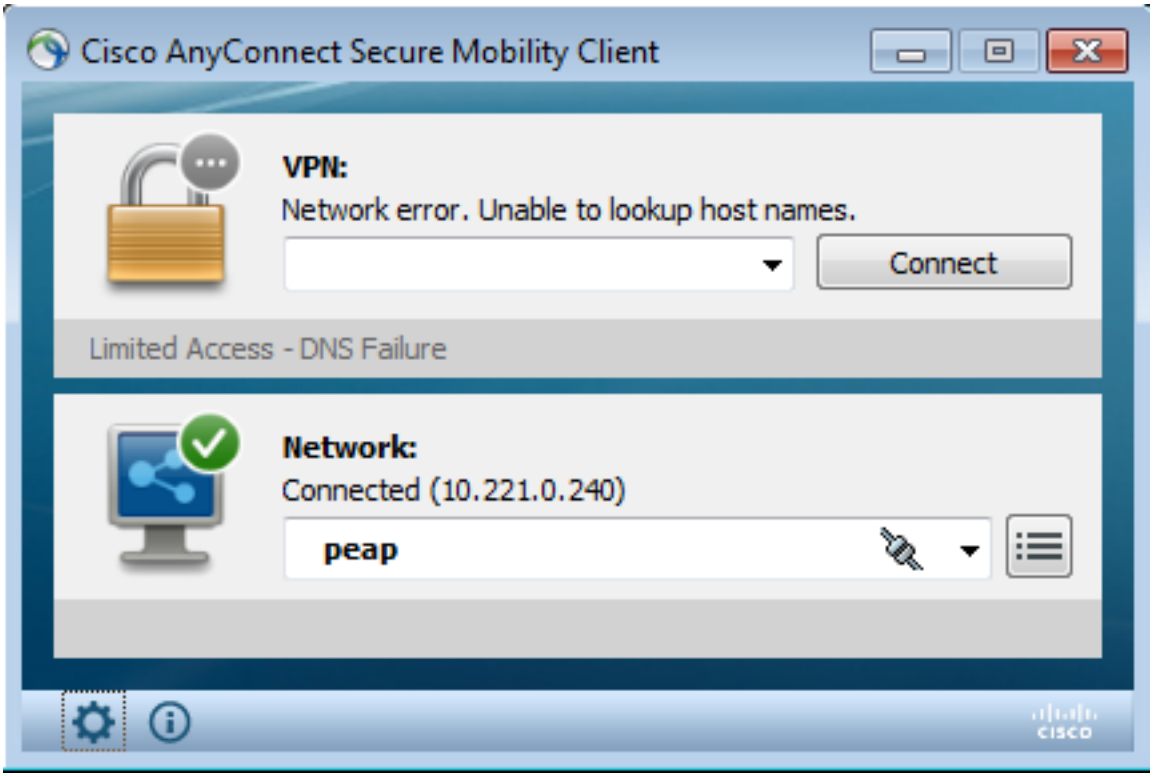


A questo punto, il modulo enforcer cerca l'espressione regolare (RegExp) nel messaggio syslog: "snort[". Se individuato, esegue la ricerca in tutti gli indirizzi IP e seleziona quello precedente all'ultimo. Questa soluzione è adatta alla maggior parte delle soluzioni di sicurezza. Per ulteriori informazioni, consultare la sezione Syslog. L'indirizzo IP (utente non autorizzato) è stato messo in

quarantena tramite pxGrid. È inoltre possibile utilizzare una regola più granulare, ad esempio il numero della firma.

Passaggio 3. Prima sessione Dot1x

La stazione di Microsoft Windows 7 avvia una sessione dot1x cablata. Cisco Anyconnect NAM è stato usato come supplicant. Il metodo EAP (Extensible Authentication Protocol-Protected EAP) è configurato.



Viene selezionato il profilo di autorizzazione ISE **Dot1x Full Access**. Lo switch scarica l'elenco degli accessi per concedere l'accesso completo:

```
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
```

Passaggio 4. Microsoft Windows PC invia il pacchetto che attiva l'allarme

Questo comando mostra ciò che accade se si invia da un pacchetto Microsoft Windows con TTL = 7:

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

Tale valore viene diminuito su Snort nella catena di inoltro e viene generato un allarme. Di conseguenza, viene inviato un messaggio syslog verso pxLog:

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

Passaggio 5. pxLog

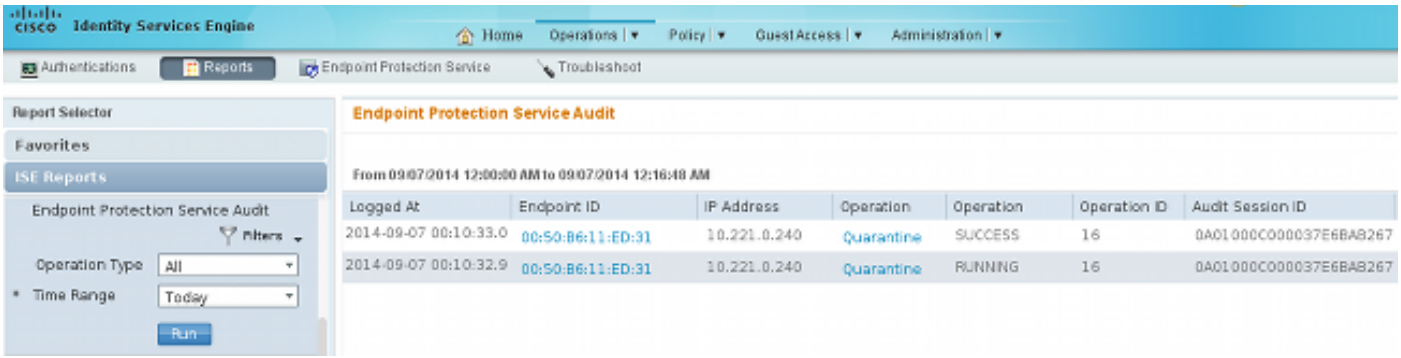
Il pxLog riceve il messaggio syslog, lo elabora e richiede di mettere in quarantena l'indirizzo IP. È possibile verificare questa condizione controllando i registri:

Logs from the actions executed by the Enforer module

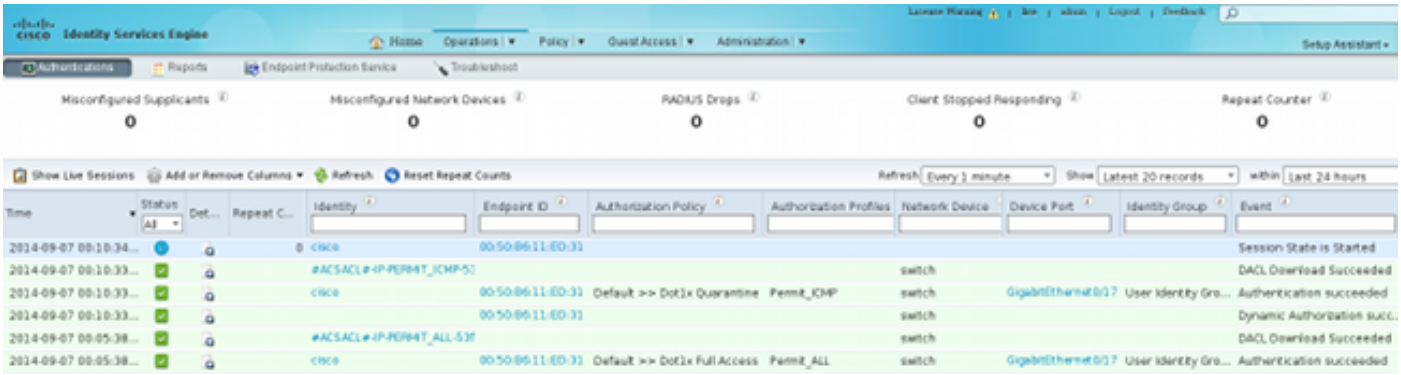
Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

Fase 6. Messa in quarantena di ISE

L'ISE riporta che l'indirizzo IP è stato messo in quarantena:



Di conseguenza, rivede il criterio di autorizzazione, sceglie la quarantena e invia RADIUS CoA per aggiornare lo stato di autorizzazione sullo switch per l'endpoint specifico.



Questo è il messaggio di terminazione CoA che forza il supplicant ad avviare una nuova sessione e ottenere un accesso limitato (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)
```

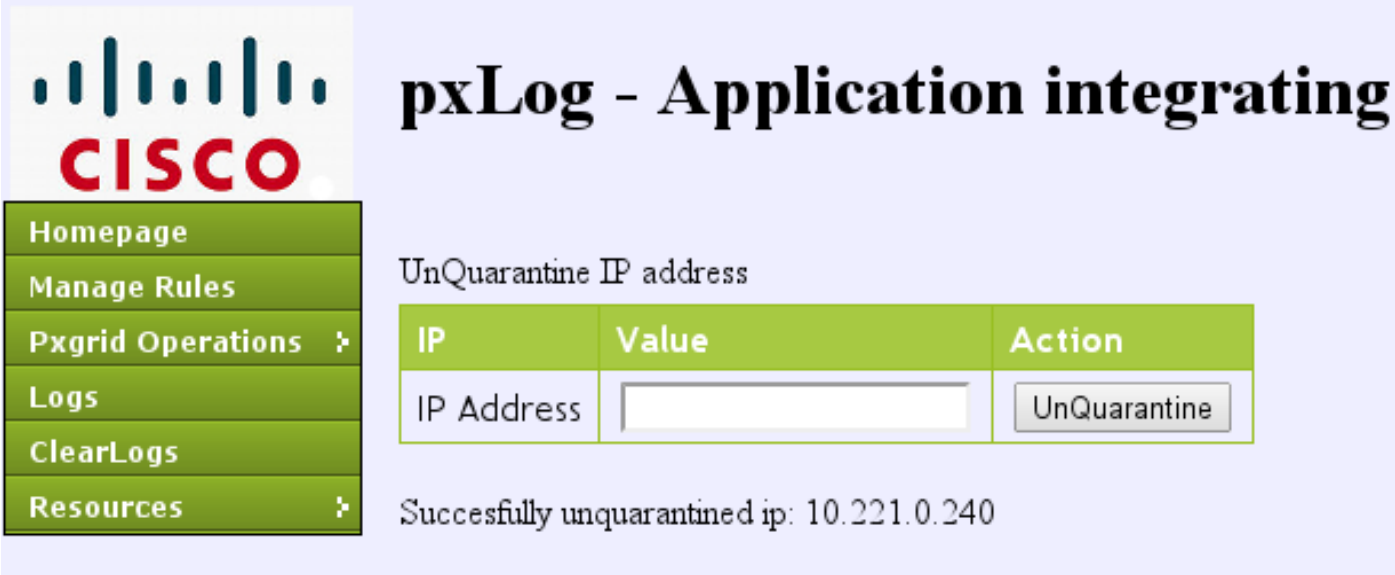
Il risultato può essere confermato sullo switch (accesso limitato per l'endpoint):

```
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
```

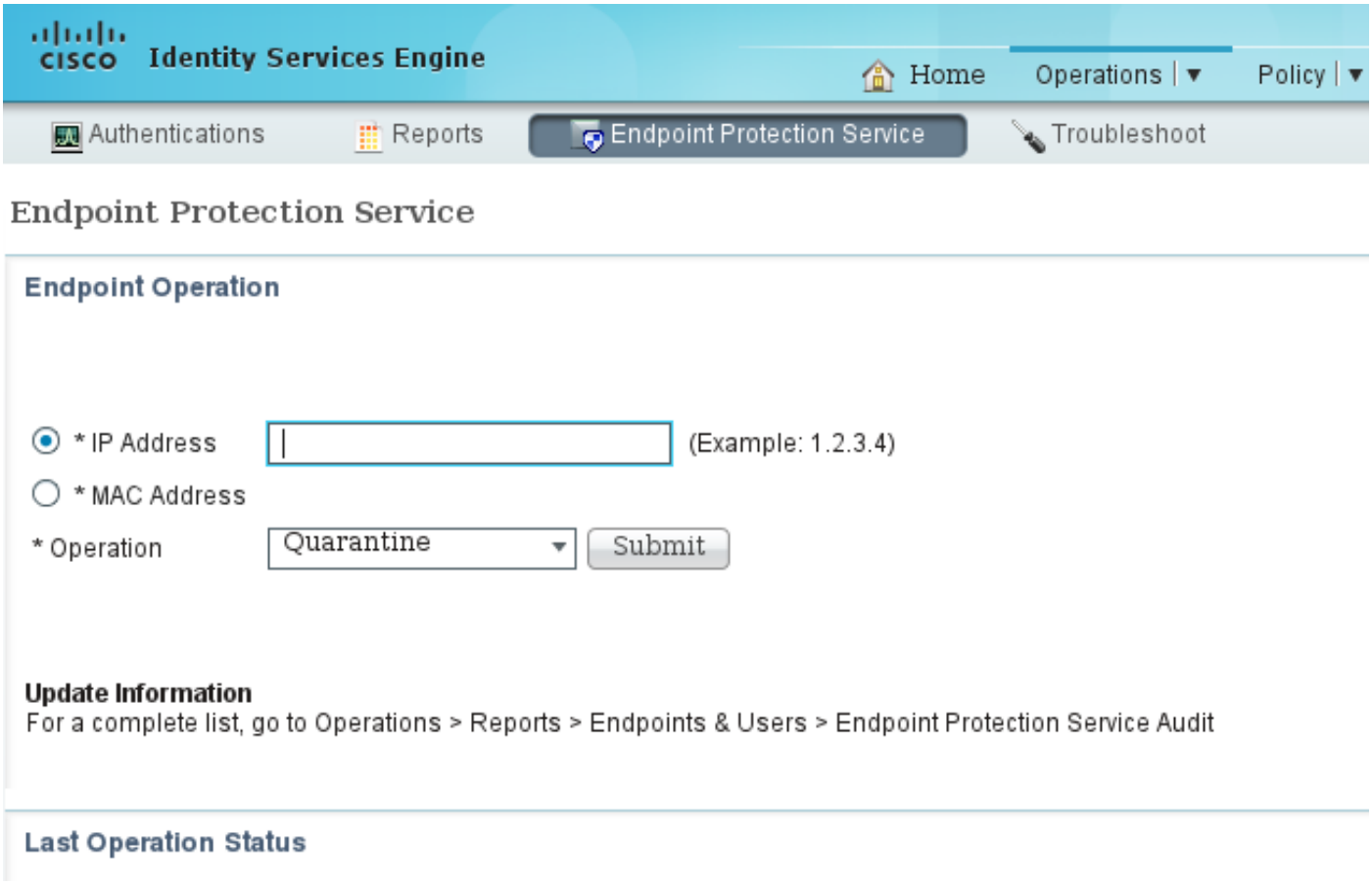
```
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

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

Passaggio 7. pxLog Unquarantine

In questa fase, l'amministratore decide di riattivare la quarantena per l'endpoint:

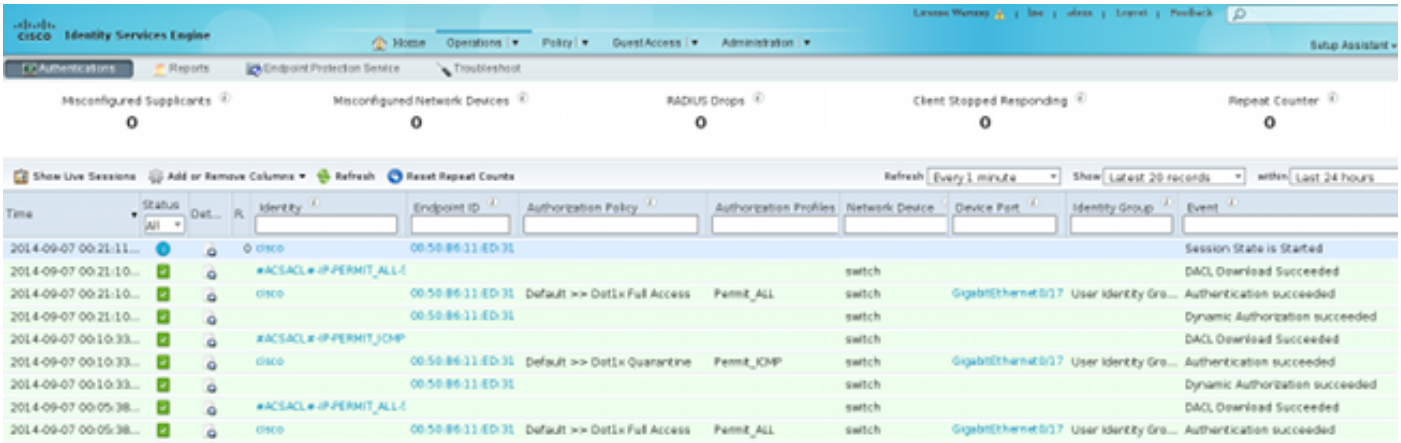


La stessa operazione può essere eseguita direttamente dall'ISE:

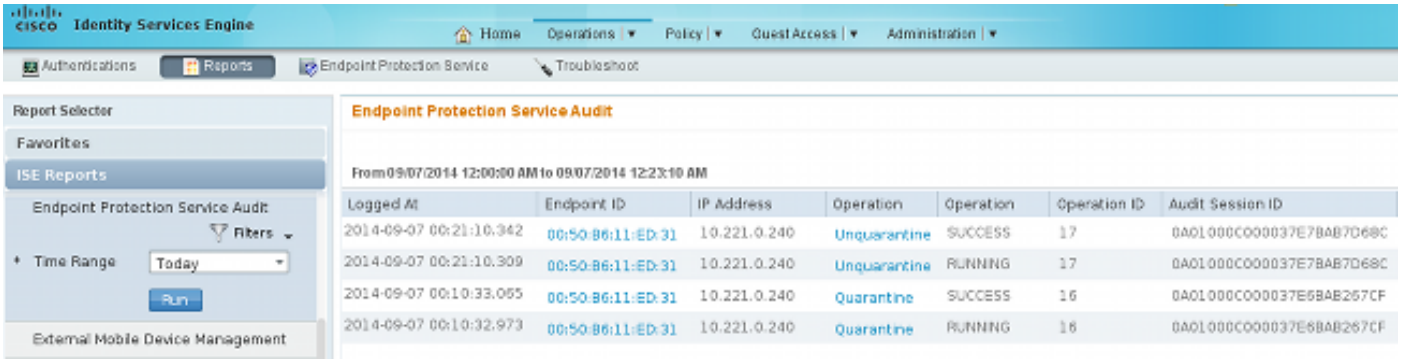


Passaggio 8. Annullamento della quarantena ISE

L'ISE riesamina le regole e aggiorna lo stato di autorizzazione sullo switch (viene concesso l'accesso completo alla rete):



La relazione conferma:



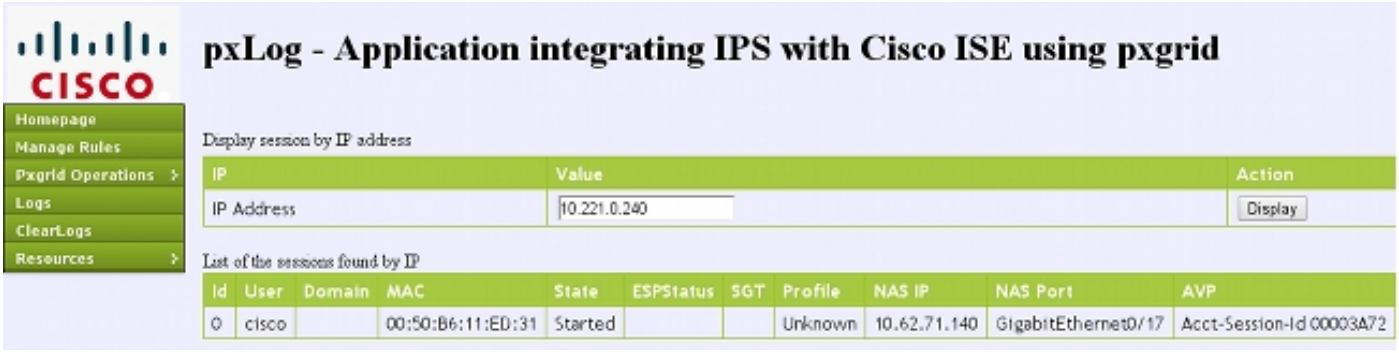
Funzionalità pxLog

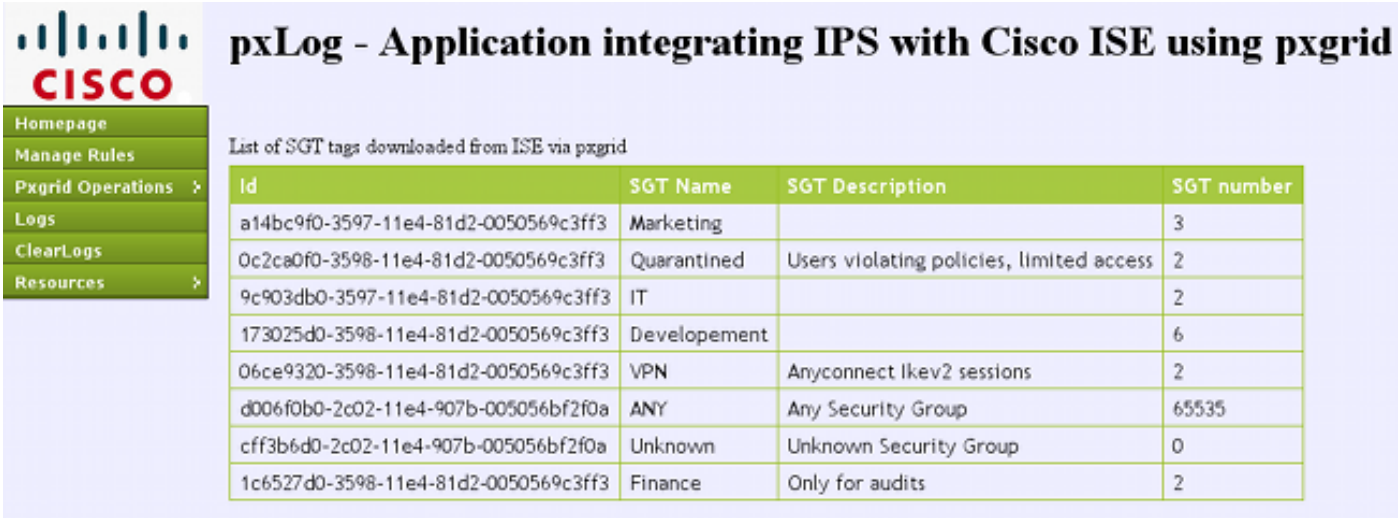
L'applicazione pxLog è stata scritta per dimostrare la funzionalità dell'API pxGrid. Consente di:

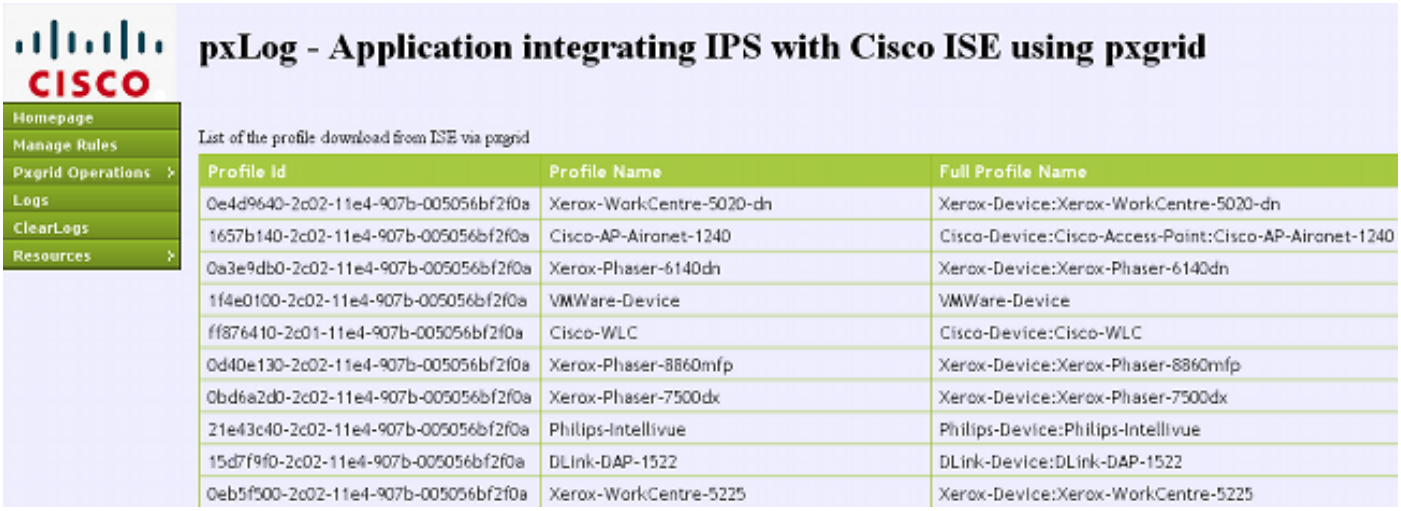
- Registrare la sessione e gli utenti EPS sull'ISE
- Scarica le informazioni su tutte le sessioni attive sull'ISE
- Scarica le informazioni su una sessione attiva specifica sull'ISE (tramite indirizzo IP)
- Scarica le informazioni su un utente attivo specifico sull'ISE (per nome utente)
- Visualizza le informazioni su tutti i profili (profiler)
- Visualizza le informazioni sui tag del gruppo di sicurezza TrustSec (SGT) definiti nell'ISE
- Verifica versione (funzionalità di pxGrid)
- Quarantena basata sull'indirizzo IP o MAC
- Rimuovi quarantena basata su indirizzo IP o MAC

Nuove funzionalità sono previste per il futuro.

Ecco alcuni screenshot di esempio da pxLog:







Requisiti del protocollo pxGrid

Gruppi

Il client (utente) può essere membro di un gruppo alla volta. I due gruppi più utilizzati sono:

- Sessione: utilizzata per sfogliare/scaricare informazioni su sessioni/profili/SGT
- EPS - Utilizzato per eseguire la quarantena

Certificati e Java KeyStore

Come accennato in precedenza, entrambe le applicazioni client, pxLog e pxGrid Controller (ISE), devono avere certificati configurati per comunicare. L'applicazione pxLog conserva quelle nei file Java KeyStore:

- **store/client.jks** - Include il client e i certificati CA (Certification Authority)
- **store/root.jks** - Include la catena ISE: Identità del nodo di monitoraggio e risoluzione dei problemi (MnT) e certificato CA

I file sono protetti da password (impostazione predefinita: cisco123). La posizione e le password dei file possono essere modificate in **WEB-INF/web.xml**.

Ecco i passaggi per generare un nuovo Java KeyStore:

1. Per creare un keystore radice (attendibile), importare il certificato CA (**cert-ca.der** deve essere in formato DER):

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

2. Quando si crea un nuovo keystore, scegliere una password, che verrà utilizzata successivamente per accedere al keystore.

3. Importare il certificato di identità MnT nel keystore radice (**cert-mnt.der** è il certificato di identità preso da ISE e deve essere in formato DER):

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

4. Per creare il keystore del client, importare il certificato CA:

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

5. Crea una chiave privata nel keystore client:

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

6. Generare una richiesta di firma del certificato (CSR) nell'archivio chiavi del client:

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

7. Firmare il file **cert-client.csr** e importare il certificato client firmato:

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

8. Verificare che entrambi i keystore contengano i certificati corretti:

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

Attenzione: Quando il nodo ISE 1.3 viene aggiornato, è disponibile un'opzione per mantenere il certificato di identità, ma la firma dell'autorità di certificazione viene rimossa. Di conseguenza, l'ISE aggiornato utilizza un nuovo certificato ma non allega mai il certificato CA nel messaggio SSL/ServerHello. In questo modo viene attivato il guasto sul client che si aspetta (in base alla RFC) di vedere una catena completa.

Nome host

L'API pxGrid per diverse funzioni (come il download della sessione) esegue una convalida aggiuntiva. Il client contatta l'ISE e riceve il nome host ISE, definito dal comando hostname nella CLI. Il client tenta quindi di eseguire la risoluzione DNS per il nome host e di contattare e recuperare i dati da tale indirizzo IP. Se la risoluzione DNS per il nome host ISE ha esito negativo, il client non tenterà di ottenere dati.

Attenzione: Si noti che per questa risoluzione viene utilizzato solo il nome host, **indicato** in questo scenario, e non il nome di dominio completo (FQDN), che in questo scenario è **lise.example.com**.

Nota per gli sviluppatori

Cisco pubblica e supporta l'API pxGrid. Esiste un pacchetto con il nome seguente:

pxgrid-sdk-1.0.0-167

All'interno ci sono:

- pxGrid file JAR con classi, che possono essere facilmente decodificati in file Java per controllare il codice
- KeyStore Java di esempio con certificati
- Script di esempio che utilizzano classi Java di esempio che utilizzano pxGrid

Syslog

Di seguito è riportato l'elenco delle soluzioni di sicurezza che inviano messaggi syslog con l'indirizzo IP dell'autore dell'attacco. Questi possono essere facilmente integrati con pxLog a

condizione che si utilizzi la regola RegExp corretta nella configurazione.

Snort

Snort invia gli allarmi syslog nel seguente formato:

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

Di seguito è riportato un esempio:

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

L'indirizzo IP dell'autore dell'attacco è sempre il secondo prima dell'ultimo (destinazione). È semplice creare un RegExp granulare per una firma specifica ed estrarre l'indirizzo IP dell'autore dell'attacco. Di seguito è riportato un esempio di RegExp per la firma 100124 e il messaggio ICMP (Internet Control Message Protocol):

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

Ispezione Cisco Adaptive Security Appliance (ASA)

Quando l'ASA è configurata per l'ispezione HTTP (esempio), il messaggio syslog corrispondente ha il seguente aspetto:

```
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
```

Anche in questo caso si potrebbe usare un RegExp granulare per filtrare questi messaggi ed estrarre l'indirizzo IP dell'utente malintenzionato, il secondo prima dell'ultimo.

Cisco Sourcefire Next-Generation Intrusion Prevention Systems (NGIPS)

Di seguito è riportato un esempio di messaggio inviato dal sensore 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
```

Di nuovo, è semplice estrarre l'indirizzo IP dell'utente malintenzionato perché vale la stessa logica. Vengono inoltre forniti il nome del criterio e la firma, in modo che la regola pxLog possa essere granulare.

Juniper NetScreen

Di seguito è riportato un messaggio di esempio inviato dal precedente 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"
```

L'indirizzo IP dell'autore dell'attacco può essere estratto allo stesso modo.

Juniper JunOS

JunOS è simile:

```
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
```

iptable Linux

Di seguito sono riportati alcuni esempi di iptable Linux.

```
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
```

Èpossibile inviare informazioni syslog per qualsiasi tipo di pacchetto con le funzionalità avanzate fornite dai moduli iptable, quali il rilevamento delle connessioni, xtables, rpfilters, il pattern matching e così via.

IPFirewall (IPFW) FreeBSD

Di seguito è riportato un messaggio di esempio per bloccare i frammenti IPFW:

```
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)
```

Preparazione VPN e gestione CoA

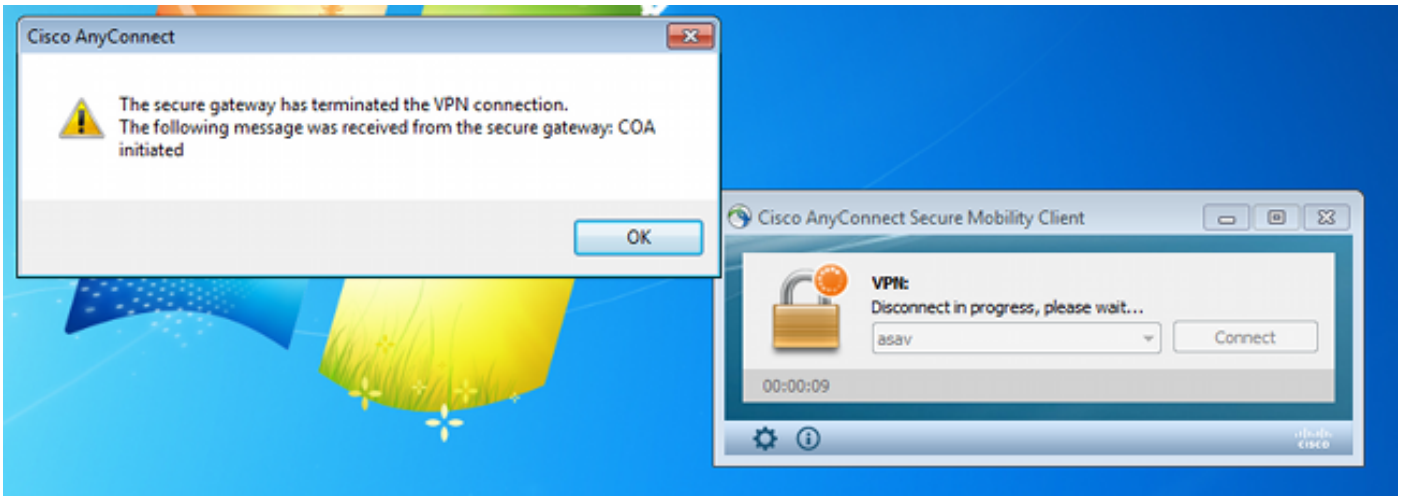
L'ISE è in grado di riconoscere il tipo di sessioni in termini di gestione del CoA.

- Per un cavo 802.1x/MAC Authentication Bypass (MAB), l'ISE invia la nuova autenticazione CoA, che attiva una seconda autenticazione.

- Per un dispositivo wireless 802.1x/MAB, l'ISE invia il terminale CoA, che attiva una seconda autenticazione.

- Per una VPN ASA, l'ISE invia una CoA con un nuovo DACL collegato (senza seconda autenticazione).

Il modulo EPS è semplice. Quando esegue una quarantena, invia sempre un pacchetto di terminazione CoA. Per le sessioni cablate/wireless, non è un problema (tutti i supplicant 802.1x sono in grado di avviare in modo trasparente una seconda sessione EAP). Tuttavia, quando l'ASA riceve il messaggio di terminazione del CoA, interrompe la sessione VPN e l'utente finale riceve questa notifica:



Per forzare la riconnessione automatica della VPN AnyConnect (configurata nel profilo XML), sono disponibili due soluzioni:

- Autoreconnect, che funziona solo quando si perde la connessione con il gateway VPN, non per terminazione amministrativa

- Always-on, che funziona e forza AnyConnect a ristabilire automaticamente la sessione

Anche quando la nuova sessione è stabilita, l'ASA sceglie il nuovo ID della sessione di revisione. Dal punto di vista di ISE, questa è una nuova sessione e non c'è alcuna possibilità di rilevare la regola di quarantena. Anche per le VPN, non è possibile usare l'indirizzo MAC dell'endpoint come identità, a differenza del punto1x cablato/wireless.

La soluzione è costringere l'EPS a comportarsi come l'ISE e inviare il corretto tipo di CoA in base alla sessione. Questa funzionalità sarà introdotta in ISE versione 1.3.1.

Partner e soluzioni pxGrid

Ecco un elenco di partner e soluzioni pxGrid:

- LogRhythm (Security Information and Event Management (SIEM)) - Supporta l'API REST (Representative State Transfer)
- Splunk (SIEM) - Supporta l'API REST
- HP Arcsight (SIEM) - Supporta l'API REST
- Sentinel NetIQ (SIEM) - Piani per il supporto di pxGrid
- Lancope Stealth Watch (SIEM) - Piani per supportare pxGrid

- Cisco Sourcefire - Prevede di supportare pxGrid 1HCY15
- Cisco Web Security Appliance (WSA) - Prevede di supportare pxGrid ad aprile 2014

Ecco altri partner e soluzioni:

- Tenable (valutazione della vulnerabilità)
- Emulex (acquisizione pacchetti e analisi legale)
- Reti Bayshore (prevenzione delle perdite di dati (DLP) e Internet of Things (IoT))
- Ping Identity (Gestione identità e accesso (IAM)/Single Sign-On (SSO))
- Qradar (SIEM)
- SIEM (LogLogic)
- Symantec (SIEM amd Mobile Device Management (MDM))

Per l'elenco completo delle soluzioni di sicurezza, consultare il Catalogo delle soluzioni Marketplace.

API ISE: Confronto tra REST e EREST e pxGrid

ISE versione 1.3 offre tre tipi di API.

Ecco un confronto:

	RIPOSO	**Riposo esterno**	**pxGrid**
Autenticazione client	username + password (autenticazione HTTP di base)	username + password (autenticazione HTTP di base)	certificato
Separazione privilegi	no	limitato (Amministratore ERS)	yes (Grup
Accesso	MnT	MnT	MnT
Trasporto	tcp/443 (HTTPS)	tcp/9060 (HTTPS)	tcp/5222 (XMPP)
Metodo HTTP	OTTIENI	GET/POST/PUT	GET/POS
Attivato per impostazione predefinita	sì	no	no
Numero di operazioni	pochi	molti	pochi
Terminazione CoA	supportato	no	supportato
Riautenticazione CoA	supportato	no	supportato
Operazioni utente	no	sì	no
Operazioni sugli endpoint	no	sì	no
Operazioni gruppo di identità endpoint	no	sì	no
Quarantena (IP, MAC)	no	no	sì
Rimuovi quarantena (IP, MAC)	no	no	sì
PortBounce/Shutdown	no	no	sì
Operazioni utente guest	no	sì	no
Operazioni del portale guest	no	sì	no
Operazioni con i dispositivi di rete	no	sì	no
Operazioni gruppo dispositivi di rete	no	sì	no

* Quarantine utilizza il supporto CoA unificato di ISE versione 1.3.1.

Download

pxLog può essere scaricato da Sourceforge.

Software Development Kit (SDK) già incluso. Per la documentazione più recente su SDK e API per pxGrid, contattare il partner o il team Cisco che gestisce gli account.

Informazioni correlate

- Cisco ISE 1.2 REST API
- Cisco ISE 1.2 External RESTful API
- Guida per l'amministratore di Cisco ISE 1.3
- Documentazione e supporto tecnico – Cisco Systems