ISE versie 1.3 pxGrid-integratie met IPS PxLog toepassing

Inhoud

Inleiding

Identity Services Engine (ISE) versie 1.3 ondersteunt een nieuwe API met de naam pxGrid. Dit moderne en flexibele protocol dat verificatie, encryptie en privileges (groepen) ondersteunt, maakt een makkelijke integratie met andere veiligheidsoplossingen mogelijk. In dit document wordt het gebruik van de PxLog-toepassing beschreven, die is geschreven als een conceptbewijs. PxLog kan actieve berichten van Inbraakpreventiesysteem (IPS) ontvangen en PxGrid-berichten naar ISE verzenden om de aanvaller in quarantaine te plaatsen. Als resultaat hiervan gebruikt ISE RADIUS Change of Authorization (CoA) om de vergunningsstatus van het eindpunt te wijzigen dat de netwerktoegang beperkt. Dit gebeurt allemaal op transparante wijze voor de eindgebruiker.

Bijvoorbeeld, Snort is gebruikt als IPS, maar elke andere oplossing zou kunnen worden gebruikt. Eigenlijk hoeft het geen IPS te zijn. Het enige dat vereist is, is het slogbericht naar pxLog te verzenden met het IP-adres van de aanvaller. Dit creëert een mogelijkheid voor de integratie van een groot aantal oplossingen.

Dit document presenteert ook hoe u problemen kunt oplossen en PxGrid-oplossingen kunt testen, met de standaardproblemen en -beperkingen.

Vrijwaring: De PxLog toepassing wordt niet ondersteund door Cisco. Dit artikel is geschreven als een bewijs van het concept. Het primaire doel was het te gebruiken tijdens het verbeteren van de PxGrid-implementatie op de ISE.

Voorwaarden

Vereisten

Cisco raadt u aan ervaring met de configuratie van Cisco ISE en basiskennis van deze onderwerpen te hebben:

- ISE-implementaties en configuratie van vergunningen
- CLI-configuratie van Cisco Catalyst-switches

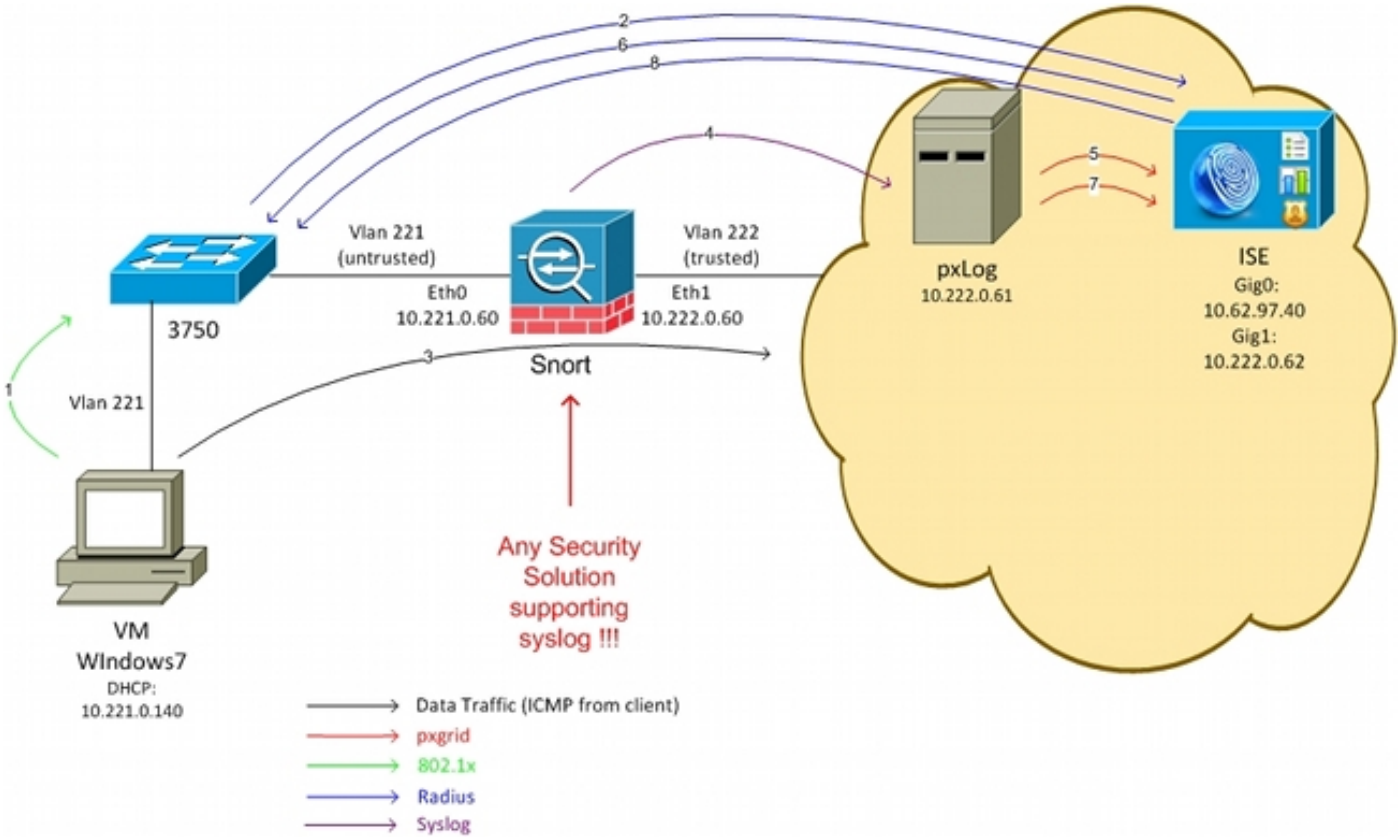
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Software voor Cisco Catalyst 3750X Series-switch, versies 15.0 en hoger

- Cisco ISE-software, versie 1.3 en hoger
- Cisco AnyConnect mobiele beveiliging met Network Access Manager (NAM), versie 3.1 en hoger
- Korte versie 2.9.6 met gegevensverzameling (DAQ)
- PPPLog toepassing geïnstalleerd op Tomcat 7 met MySQL versie 5

Netwerkdiagram en verkeersstroom



Hier is de verkeersstroom, zoals wordt geïllustreerd in het netwerkdiagram:

1. Een Microsoft Windows 7-gebruiker sluit zich aan op de switch en voert 802.1x-verificatie uit.

2. De switch gebruikt ISE als de AAA-server (Verificatie, autorisatie en accounting). De **Dot1x Full Access** autorisatieregel is aangepast en de volledige netwerktoegang wordt verleend (DACL: PERMIT_ALL).

3. De gebruiker probeert verbinding te maken met het vertrouwde netwerk en schendt de Snort-regel.

4. Als resultaat hiervan stuurt Snort een waarschuwing naar de PxLog applicatie (via syslog).

5. De toepassing pxLog voert verificatie uit tegen de lokale database. Het wordt ingesteld om syslogberichten die door Snort worden verstuurd te vangen en het IP-adres van de aanvaller te extraheren. Vervolgens gebruikt het PxGrid om een verzoek naar ISE te verzenden om het IP-adres van de aanvaller in quarantaine te plaatsen (de ISE is een PxGrid-controller).

6. De ISE herevalueert haar toelatingsbeleid. Omdat het eindpunt in quarantaine is geplaatst, is

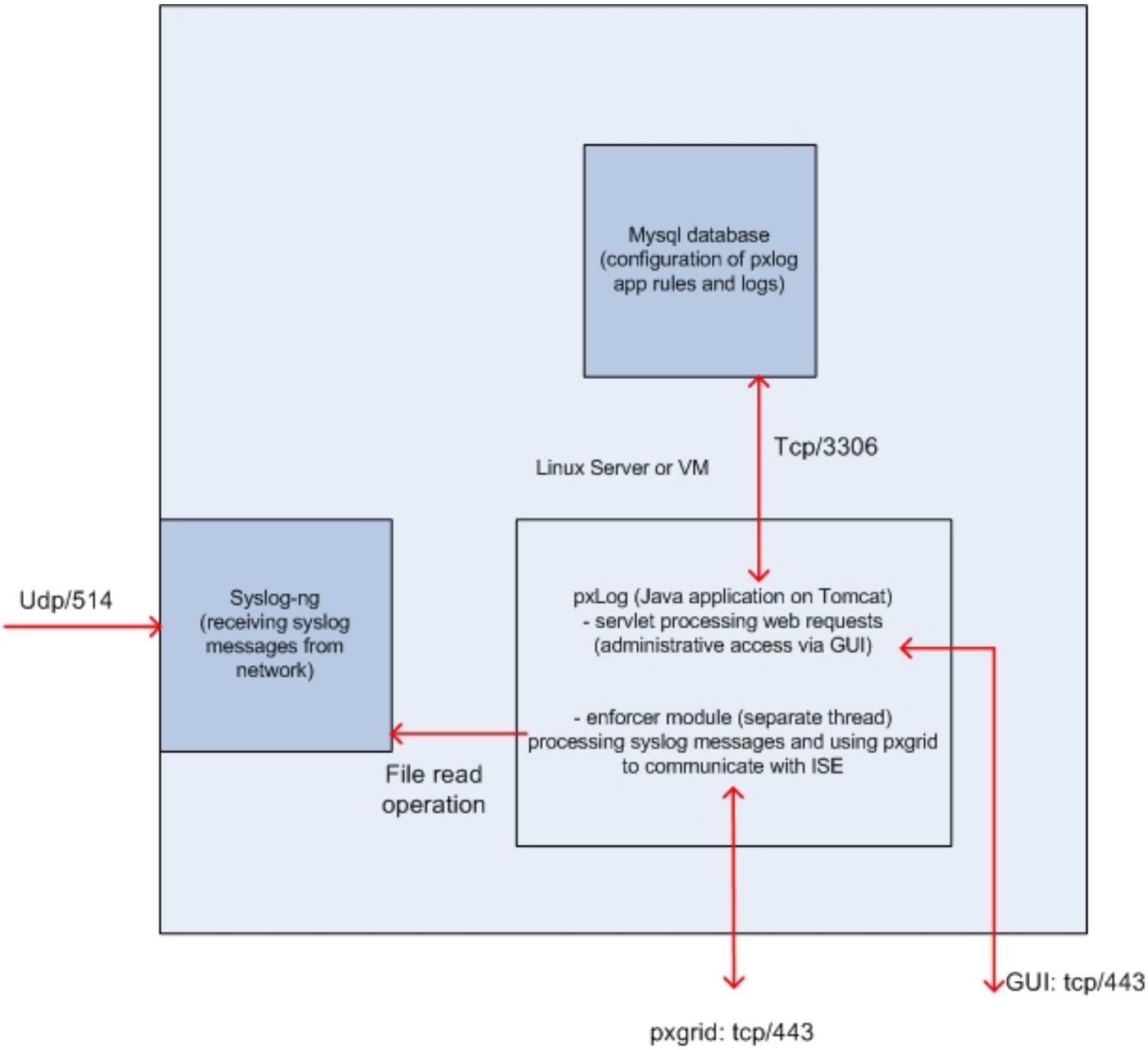
aan de **Session:EPSStatus EQUALS Quarantine** conditie voldaan en is een ander vergunningprofiel aangepast (**Dot1x Quarantine**). ISE stuurt een CoA-aansluiting naar de schakelaar om de sessie te beëindigen. Dit leidt tot herauthenticatie en een nieuwe Downloadbare ACL (DACL) (PERMIT_ICMP) wordt toegepast, wat de beperkte netwerktoegang tot de eindgebruiker verschaft.

7. In dit stadium kan de beheerder besluiten het eindpunt los te koppelen. Dit kan worden bereikt via de GUI van pxLog. Opnieuw wordt het PxGrid-bericht naar de ISE verzonden.

8. ISE voert een soortgelijke handeling uit als in Stap 6. Dit keer is het eindpunt niet langer in quarantaine geplaatst en wordt de volledige toegang geboden.

PxLog

Architectuur



De oplossing is om een reeks toepassingen te installeren op een Linux-machine:

1. De PxLog toepassing wordt in Java geschreven en op de Tomcat server ingezet. Deze aanvraag bestaat uit:

   Bezoek die webverzoeken verwerkt - Dit wordt gebruikt om toegang te krijgen tot het administratieve paneel via de webbrowser.

   Enforcer module - Thread die gestart wordt met serlet. De Enforcer leest syslog berichten uit het bestand (geoptimaliseerd), verwerkt die berichten volgens de geconfigureerde regels en voert handelingen uit (zoals quarantaine via pxGrid).

2. De MySQL database die de configuratie voor pxLog bevat (regels en loggen).

3. De syslogserver die syslogberichten van externe systemen ontvangt en schrijft ze naar een bestand.

Installatie

De toepassing pxLog gebruikt deze bibliotheken:

- jQuery (voor AJAX-ondersteuning)
- JavaServer Pages Standard Tag Library (JSTL) (Model View Controller (MVC) model, gegevens worden gescheiden van logica: De JSP-code (JavaServer) wordt gebruikt om alleen terug te geven, geen HTML-code in Java-klassen)
- Log4j als houtsubsysteem
- MySQL-connector
- toonplaatje voor het weergeven/sorteren van tabellen
- PxGrid API door Cisco (momenteel versie 14.7)

Al deze bibliotheken bevinden zich al in de lib-directory van het project, zodat het niet meer nodig is om Javachive (JAR)-bestanden te downloaden.

Zo installeert u de toepassing:

1. Pak de hele map uit naar de Tomcat Webapp-map.

2. Bewerk het **WEB-INF/web.xml-**bestand. De enige vereiste verandering is de **seriverip** variabele, die naar de ISE zou moeten wijzen. Ook de Java-KeyStores (een voor vertrouwde en een voor identiteit) kan worden gegenereerd (in plaats van de standaardinstelling). Dit wordt gebruikt door de pxGrid API die de Secure Socket Layer (SSL) sessie met zowel de client- als servercertificaten gebruikt. Beide kanten van de mededeling moeten het certificaat overleggen en elkaar vertrouwen. Raadpleeg het gedeelte PxGrid-protocolvereisten voor meer informatie.

3. Zorg ervoor dat de ISE-hostname correct is opgelost in pxLog (raadpleeg de opname in de Domain Name Server (DNS) of **/enz/hosts**). Raadpleeg het gedeelte PxGrid-

protocolvereisten voor meer informatie.

4. Configureer de MySQL-database met het **mysql/init.sql-**script. Credentials kunnen worden gewijzigd maar moeten worden weergegeven in het **WEB-INF/web.xml** bestand.

snuiven

Dit artikel is niet gericht op een specifiek IPS, wat de reden is dat er slechts een korte uitleg wordt gegeven.

Snort is inline ingesteld met DAQ-ondersteuning. Verkeer wordt omgeleid met iptafels:

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

Vervolgens wordt de injectie geïnjecteerd en doorgestuurd volgens standaard toepasbare regels.

Een paar regels van de pasklaring zijn gevormd (het **/etc/snort/rules/test.rules** dossier is inbegrepen in de mondiale configuratie).

```
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 verstuurt een syslogbericht wanneer de tijd om te leven (TTL) van het pakket gelijk is aan 6 of de grootte van de lading tussen 666 en 686 is. Het verkeer wordt niet geblokkeerd door snort.

Tevens moeten drempelwaarden worden ingesteld om te voorkomen dat de signaleringen te vaak worden geactiveerd (**/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
```

Vervolgens wijst de syslogserver op de pxLog machine (**/etc/snort/snort.conf**):

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

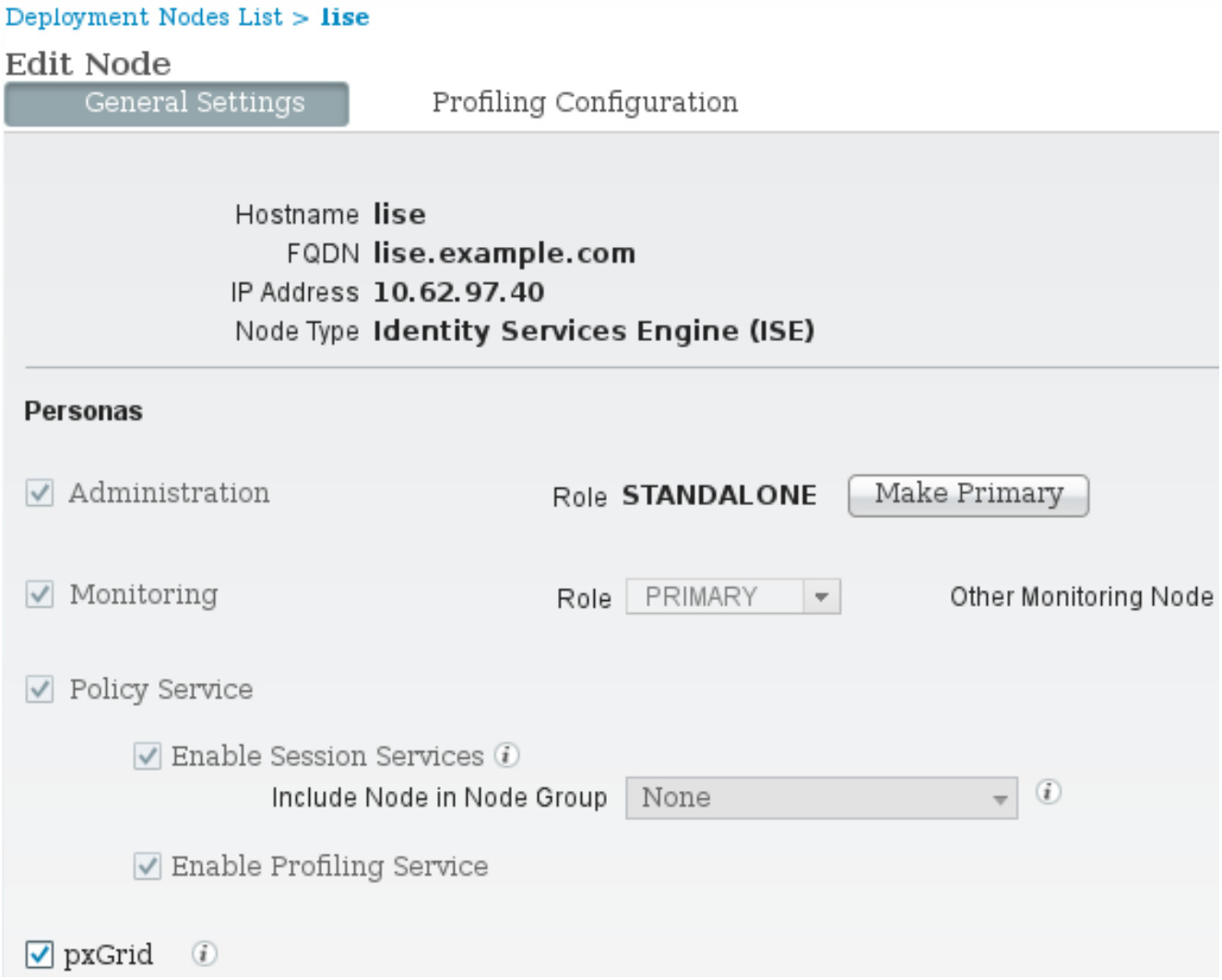
Voor sommige versies van de snort-methode zijn er insecten gerelateerd aan de syslog-configuratie, en de standaardinstellingen kunnen worden gebruikt dat punt naar de lokale host en de syslog-ng kan worden geconfigureerd om specifieke berichten naar de PxLog-host te sturen.

ISE

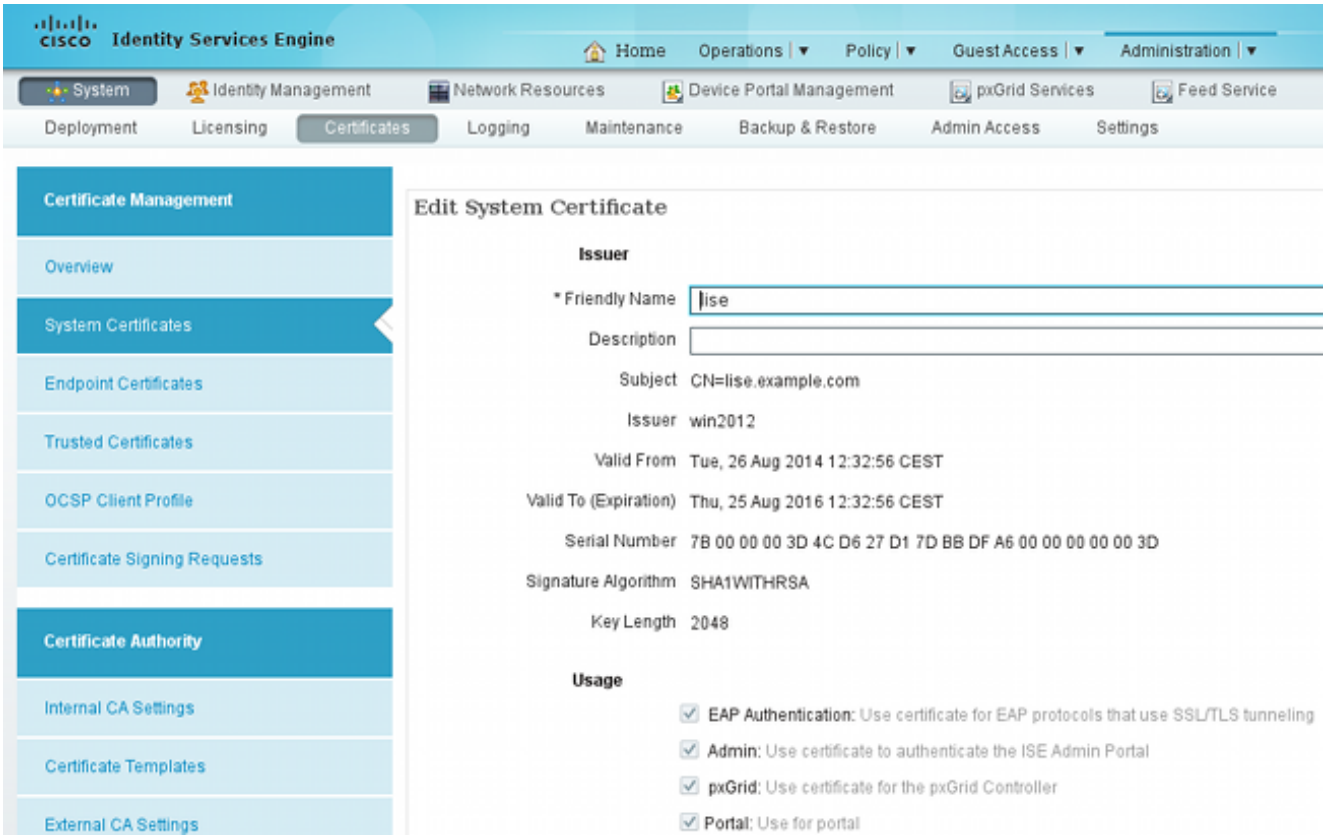
Configuratie

Persona en certificaat

1. Schakel de pxGrid-rol in, die standaard op ISE is uitgeschakeld, onder **Beheer > Plaatsing**:

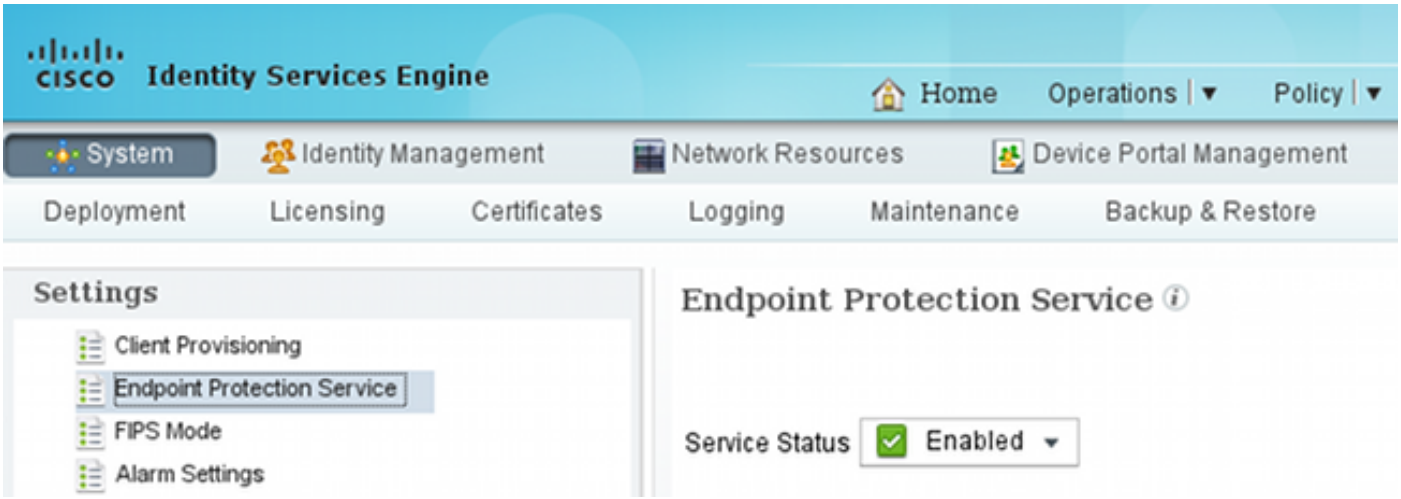


2. Controleer of de certificaten voor pxGrid zijn gebruikt onder **Beheer > Certificaten > Systeemcertificaten**:



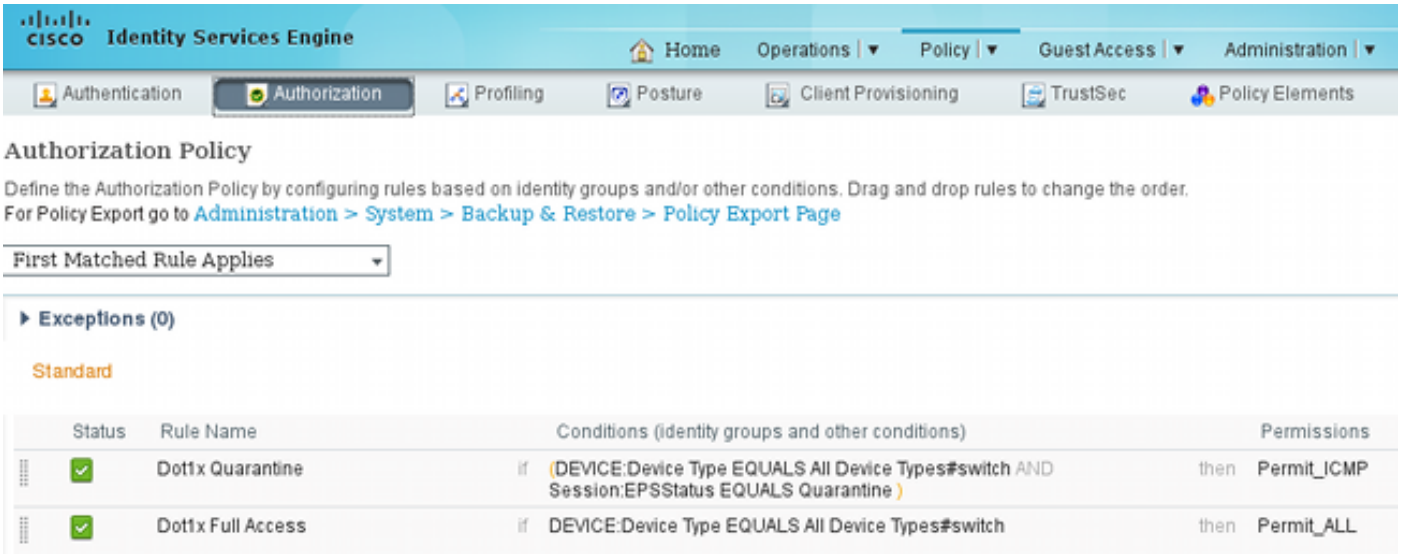
Endpoint Protection Service (EPS)

EPS moet (standaard uitgeschakeld) zijn ingeschakeld bij **Administratie > Instellingen**:



Dit stelt u in staat om de quarantaine/unquarantaine-functie te gebruiken.

machtigingsregels



De eerste regel wordt alleen aangetroffen wanneer het eindpunt in quarantaine is geplaatst. Vervolgens wordt de beperkte toegang dynamisch versterkt door RADIUS CoA. De schakelaar moet ook aan Netwerkapparaten met het juiste gedeelde geheim worden toegevoegd.

Problemen oplossen

De pxGrid-status kan met de CLI worden geverifieerd:

```
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
```

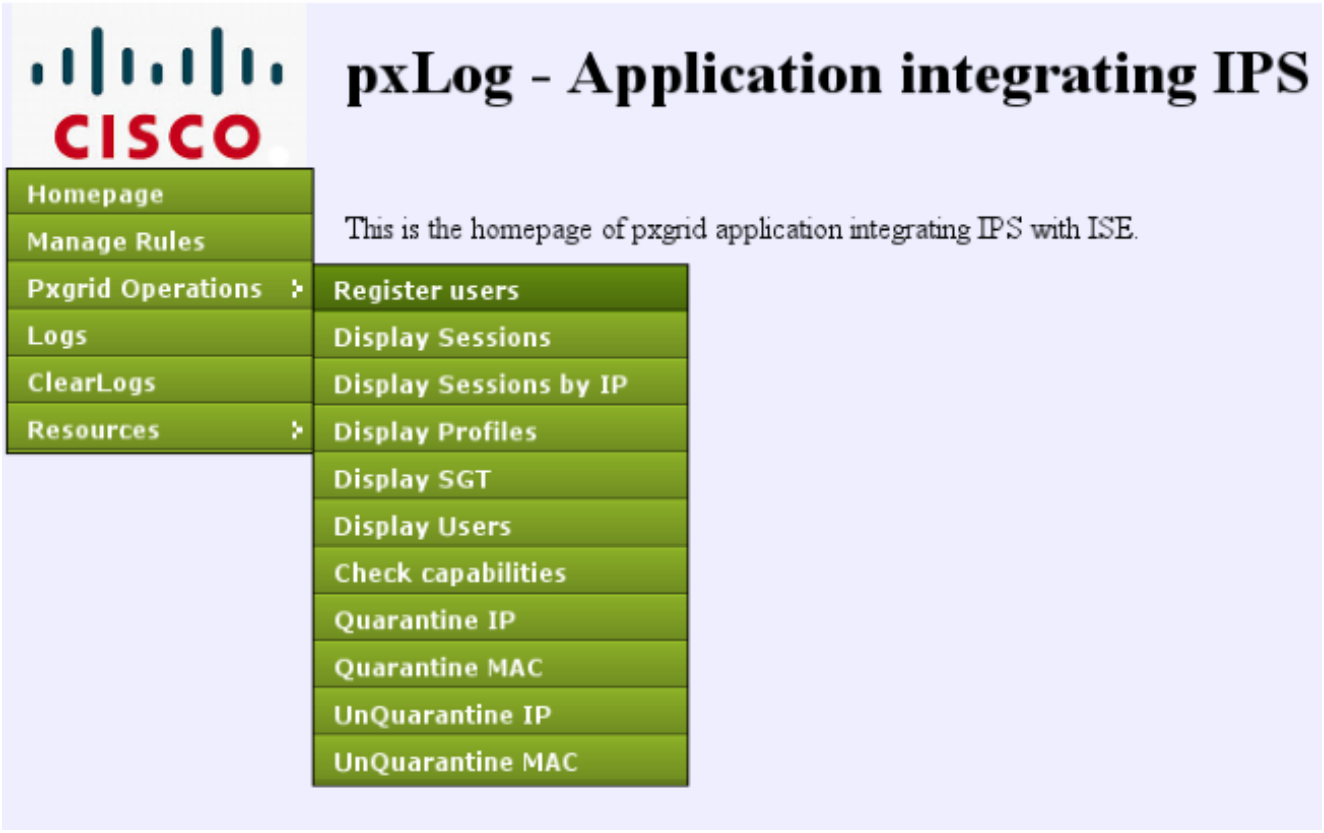
Er zijn ook afzonderlijke apparaten voor pxGrid (**Beheer > Vastlegging > Logconfiguratie > PxGrid**). Debug bestanden worden opgeslagen in de PxGrid-map. De belangrijkste gegevens zijn te vinden in **pxgrid/pxgrid-jabberd.log** en **pxgrid/pxgrid-controller.log**.

Test

Stap 1. Registratie voor PxGrid

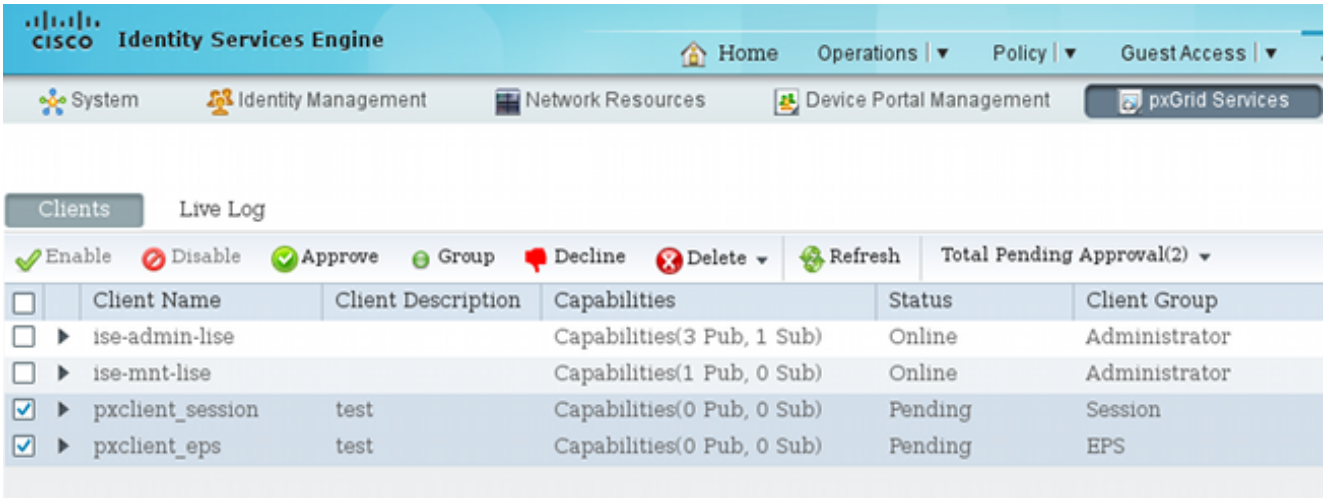
De PxLog toepassing wordt automatisch uitgevoerd wanneer Tomcat start.

1. Om pxGrid te gebruiken, registreert u twee gebruikers in de ISE (één met sessistoegang en één met quarantaine). Dit kan worden ingevuld bij **Pxgrid-bewerkingen > Gebruikers registreren**:



De registratie wordt automatisch gestart:

2. In dit stadium is het nodig om geregistreerde gebruikers op de ISE goed te keuren (de automatische goedkeuring is standaard uitgeschakeld):



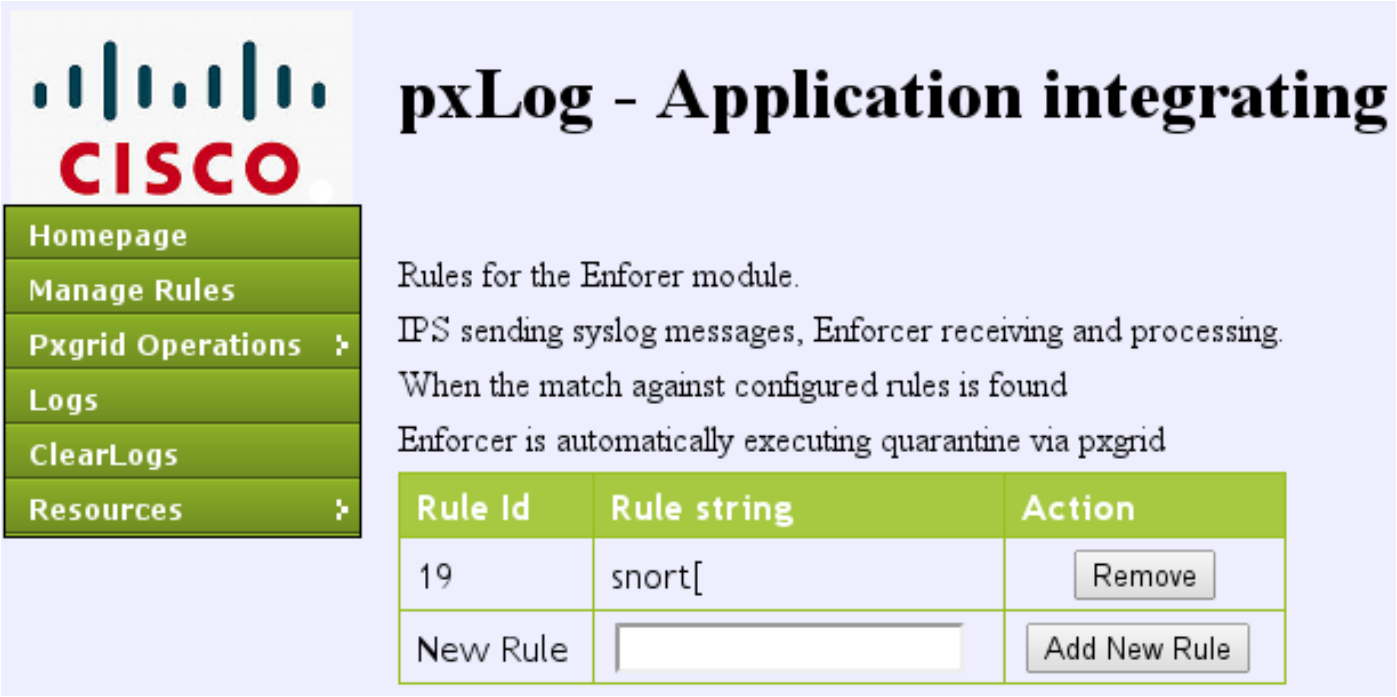
Na de goedkeuring informeert pxLog automatisch de beheerder (via een AJAX-oproep):

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

ISE toont de status voor deze twee gebruikers als online of offline (niet langer in behandeling).

Stap 2. Configuratie van pxLog regels

pxLog moet syslogberichten verwerken en acties uitvoeren die erop gebaseerd zijn. Als u een nieuwe regel wilt toevoegen, selecteert u **Regels beheren**:

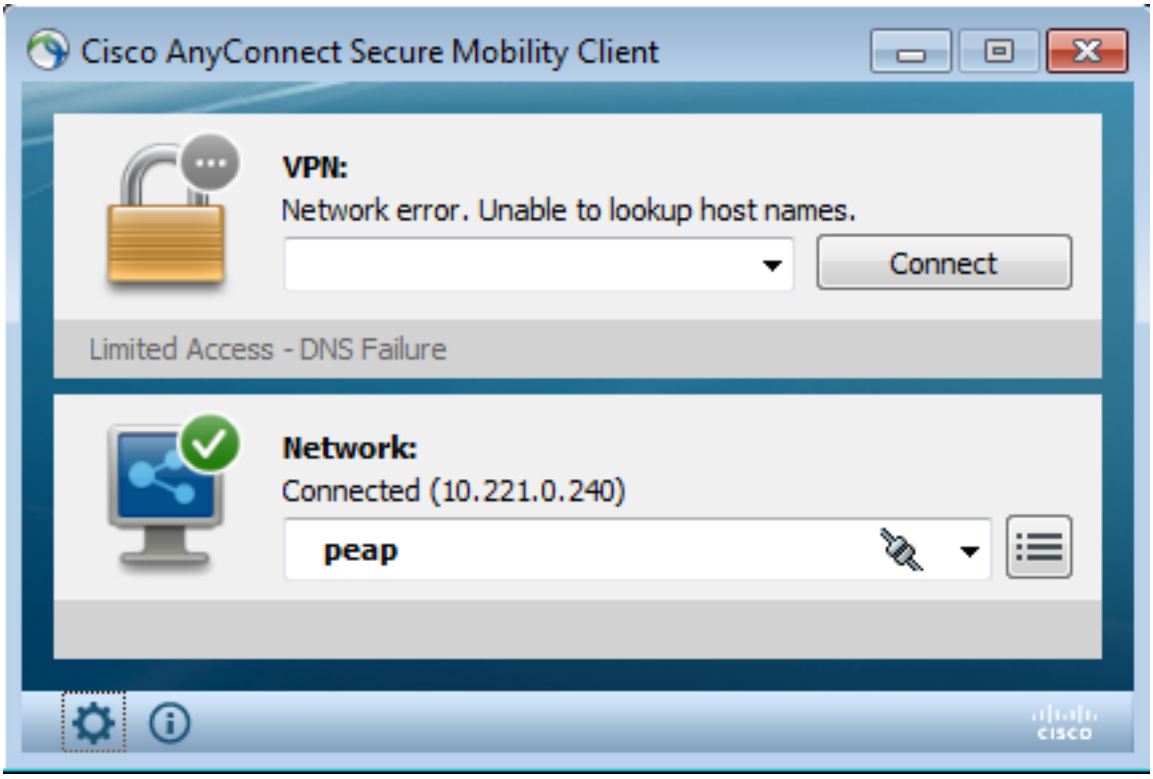


Nu zoekt de handhavingsmodule deze Regular Expression (RegExp) in het syslog-bericht: "snort[". Indien gevonden, zoekt het alle IP adressen en selecteert het één voor de laatste. Dit komt de meeste veiligheidsoplossingen aan. Raadpleeg het gedeelte Syrische gegevens voor meer informatie. Dat IP-adres (aanvaller) is in quarantaine geplaatst via pxGrid. Er zou ook een

meer gedetailleerde regel kunnen worden gebruikt (bijvoorbeeld het handtekening nummer).

Stap 3. Eerste dot1x-sessie

Het Microsoft Windows 7-station start een bekabelde dot1x-sessie. Cisco AnyConnect NAM is als leverancier gebruikt. De Extensible Authentication Protocol-Protected EAP (EAP-PEAP) methode wordt ingesteld.



Het **volledige** vergunningprofiel van ISE **Dot1x** wordt geselecteerd. De schakelaar downloads de toegangslijst om volledige toegang te verlenen:

```
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
```

Stap 4. Microsoft Windows Verstuurt het pakket dat de Alarm maakt

Dit toont wat er gebeurt als u vanuit een Microsoft Windows-pakket met TTL = 7 verzenden:

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

Die waarde wordt bij Snort in de Forwarding keten verlaagd en er wordt een alarm geslagen. Hierdoor wordt een syslogbericht naar pxLog verzonden:

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

Stap 5. PxLog

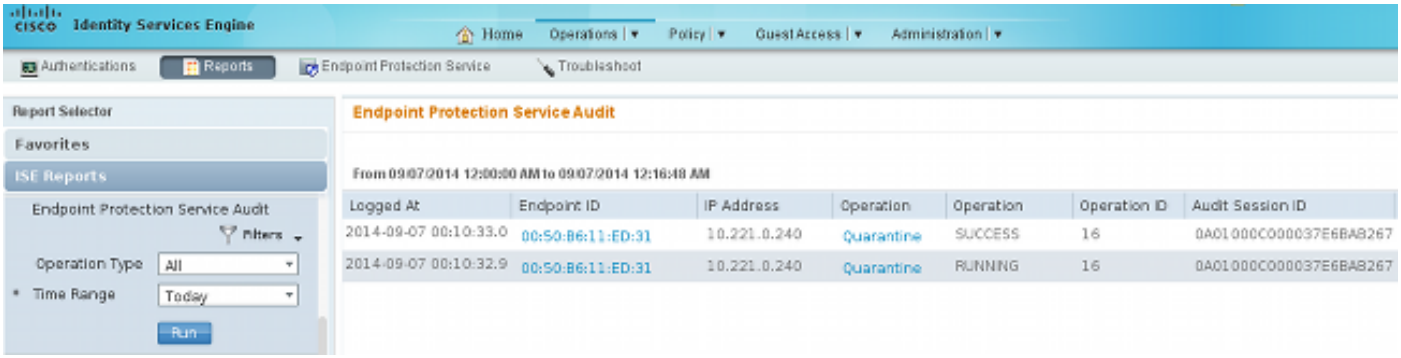
Het PxLog ontvangt het syslogbericht, verwerkt het en verzoekt om in quarantaine te plaatsen dat IP adres. Dit kan worden bevestigd als u de stammen controleert:

Logs from the actions executed by the Enforer module

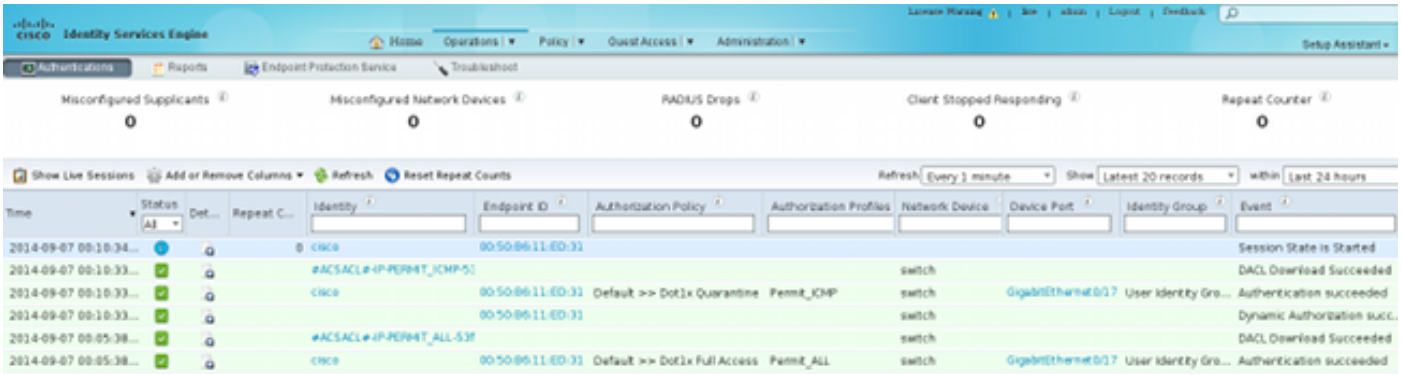
Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

Stap 6. ISE Quarantine

ISE meldt dat het IP-adres in quarantaine is geplaatst:



Als gevolg daarvan herziet zij het vergunningenbeleid, kiest zij quarantaine en stuurt zij RADIUS CoA om de vergunningsstatus op de switch voor dat specifieke eindpunt bij te werken.



Dat is het CoA-bericht dat de aanvrager dwingt om een nieuwe sessie te starten en beperkte toegang te krijgen (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)
```

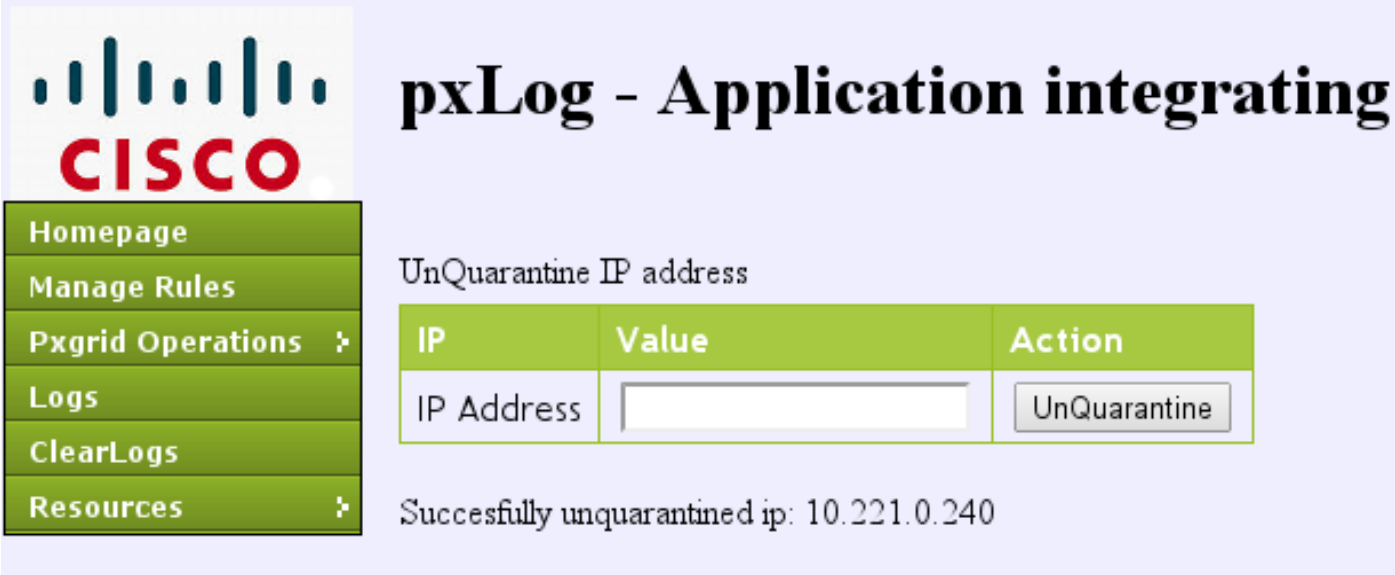
Het resultaat kan op de schakelaar (beperkte toegang voor het eindpunt) worden bevestigd:

```
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
```

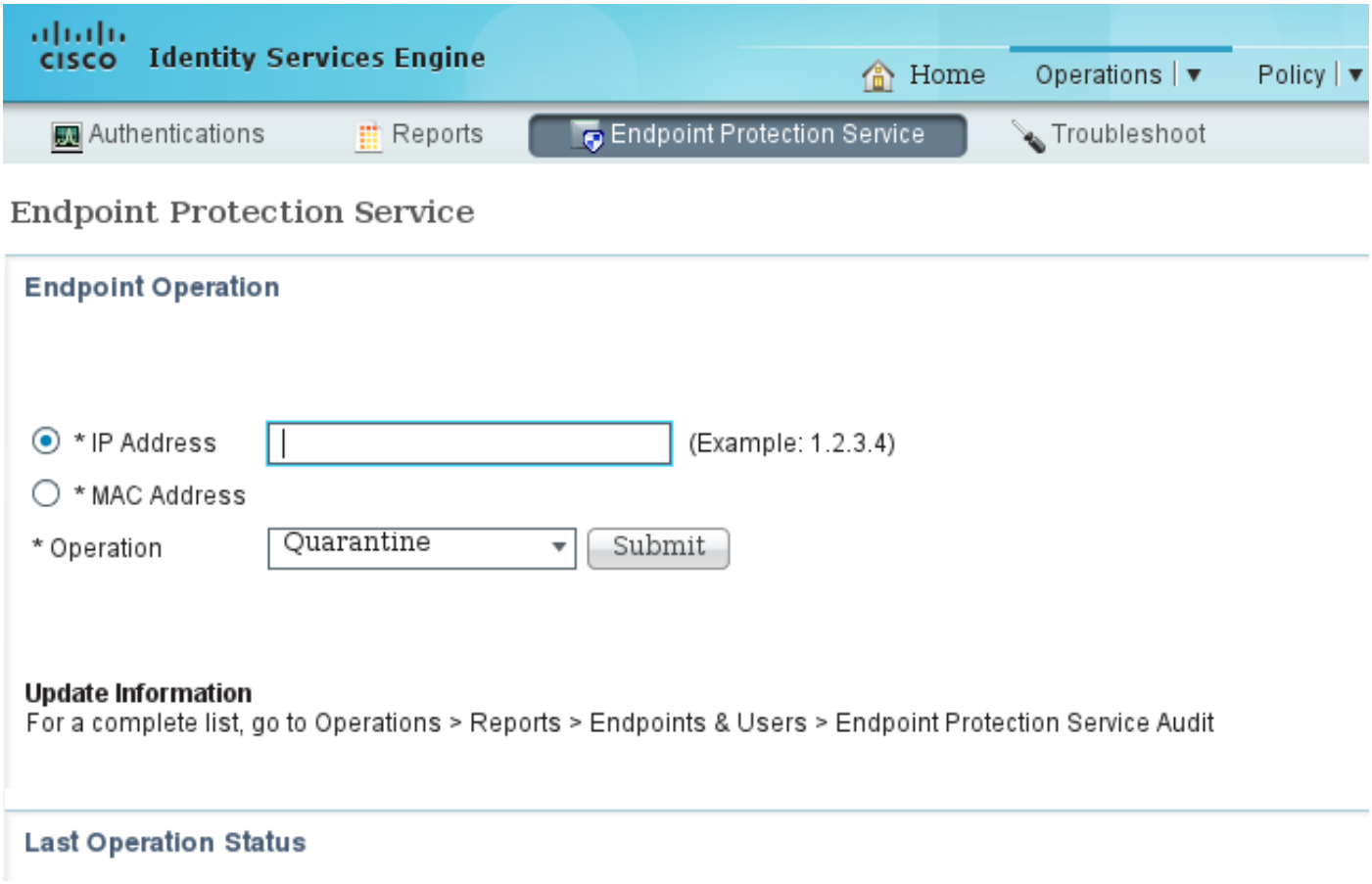
```
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

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

Stap 7. PxLog niet in quarantaine

In dit stadium besluit de beheerder om dat eindpunt in quarantaine te houden:

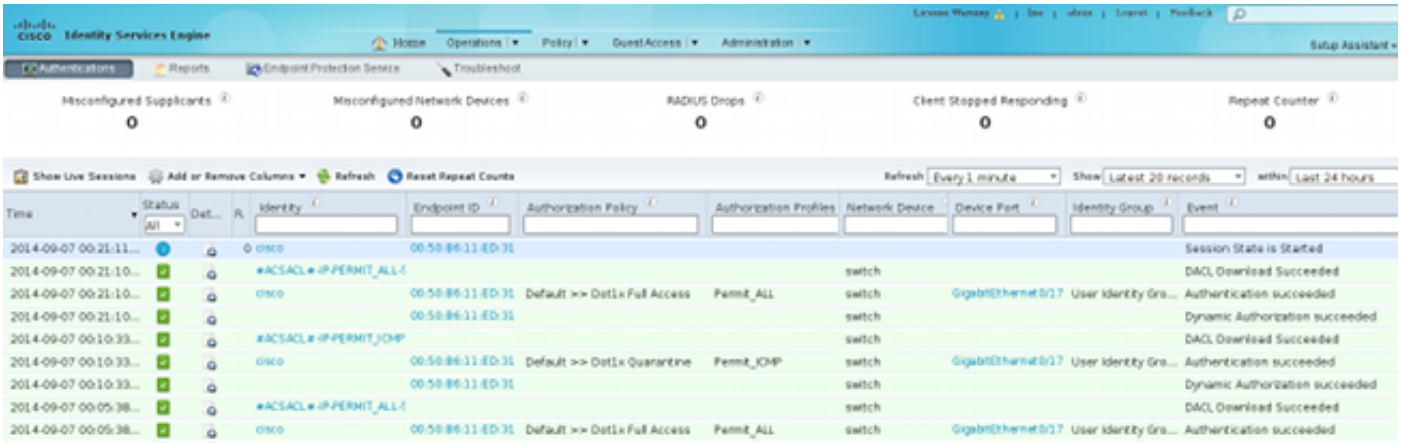


Dezelfde transactie kan rechtstreeks van de ISE worden uitgevoerd:

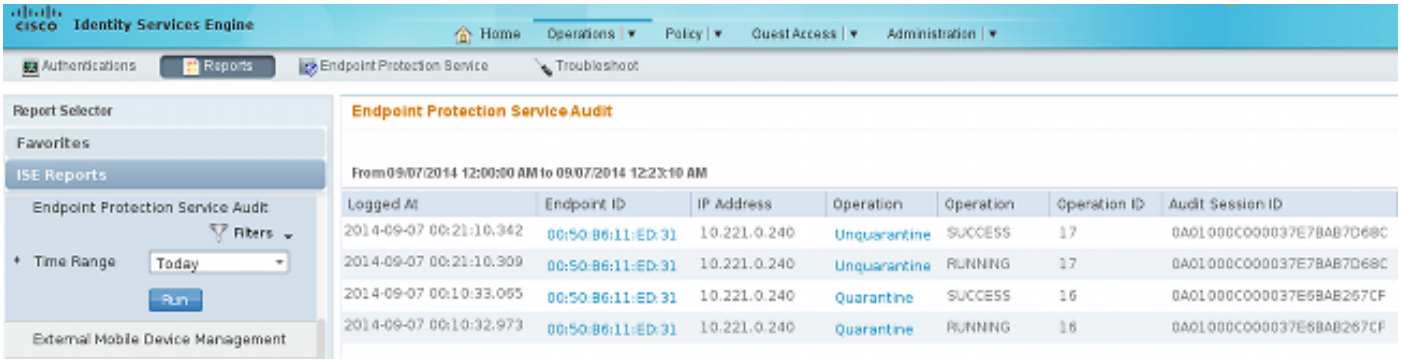


Stap 8. ISE niet in quarantaine

De ISE herziet opnieuw de regels en werkt de vergunningsstatus op de schakelaar bij (volledige netwerktoegang wordt verleend):



Het verslag bevestigt:



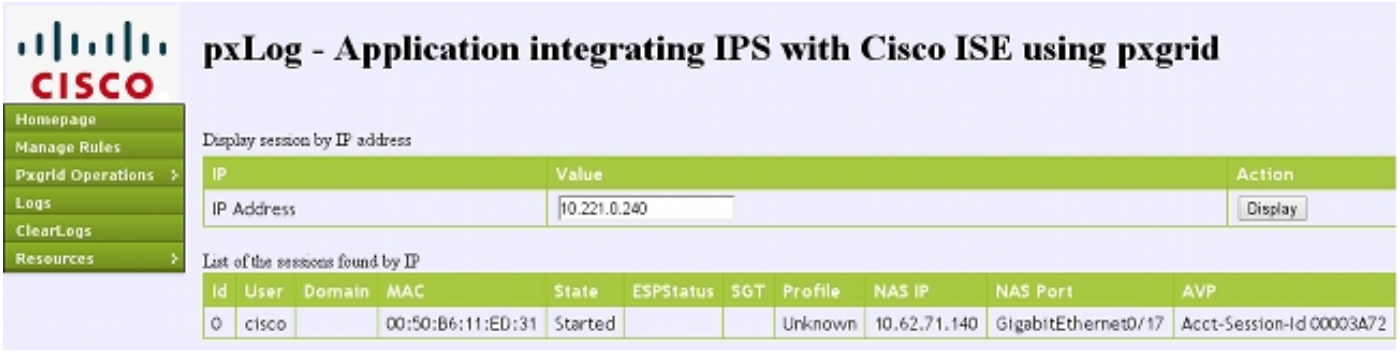
Functionaliteit voor PPPLog

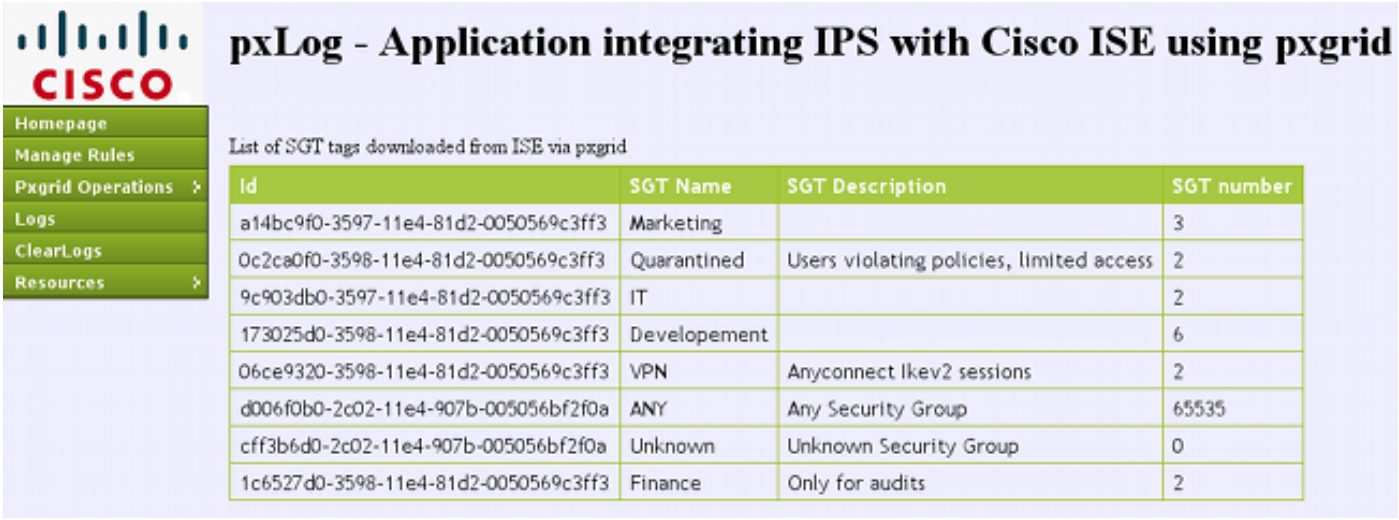
De pxLog toepassing is geschreven om de functionaliteit van de pxGrid API aan te tonen. Het stelt u in staat:

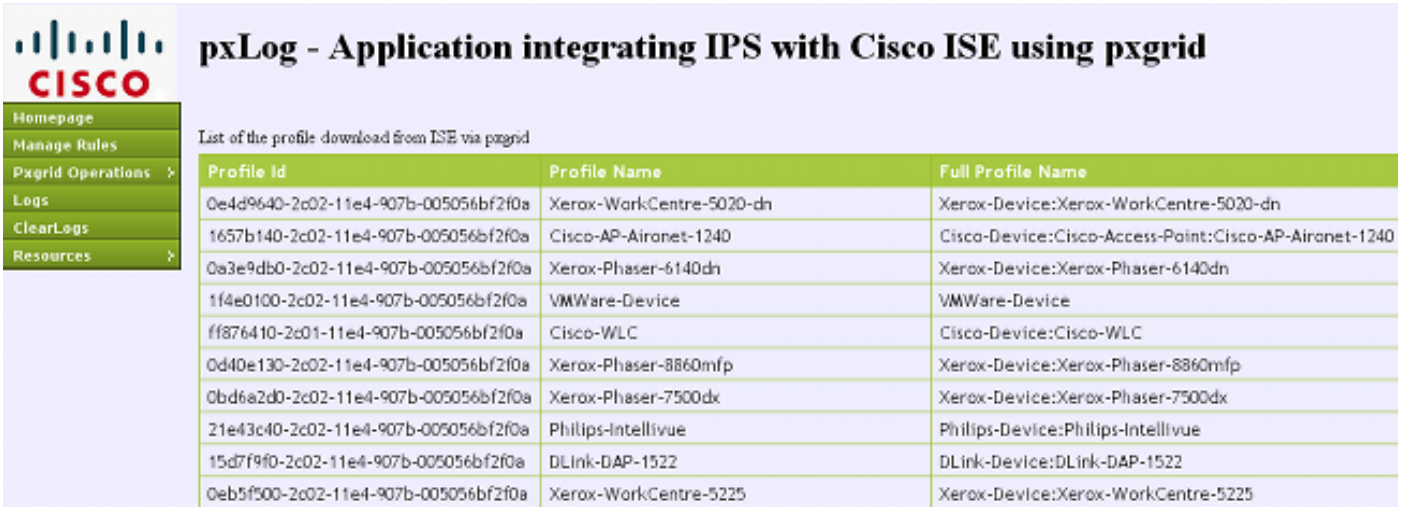
- Registreer sessie en EPS-gebruikers op ISE
- Informatie over alle sessies die actief zijn op ISE downloaden
- Informatie over een specifieke actieve sessie op ISE downloaden (via IP-adres)
- Informatie over een specifieke actieve gebruiker op de ISE downloaden (met gebruikersnaam)
- Geef de informatie over alle profielen weer (profiel)
- Toont de informatie over de TrustSec Security Group Tags (SGT's) die op ISE zijn gedefinieerd
- Versie controleren (mogelijkheden van PxGrid)
- Quarantine op basis van het IP- of het MAC-adres
- Niet-quarantaine op basis van IP of MAC-adres

In de toekomst is meer functionaliteit gepland.

Hier zijn een paar screenshots van pxLog:







PxGrid-protocolvereisten

Groepen

De cliënt (gebruiker) kan lid van één groep tegelijkertijd zijn. De twee meest gebruikte groepen zijn:

- Session - gebruikt voor informatie over sessies/profielen/SGT's om te bladeren/downloaden
- EPS - Gebruikt om quarantaine uit te voeren

Certificaten en Java KeyStore

Zoals eerder vermeld, moeten beide clienttoepassingen, pxLog en pxGrid controller (ISE), beschikken over certificaten die zijn geconfigureerd voor communicatie. De PxLog toepassing houdt de bestanden in de Java KeyStore-bestanden bij:

- **store/client.jks** - Met inbegrip van de certificaten van de klant en de certificeringsinstantie (CA)
- **store/root.jks** - Inclusief de ISE-keten: Identificatie van bewakingsknooppunt en probleemoplossing (MnT) en het CA-certificaat

Bestanden worden beveiligd met een wachtwoord (standaard: Cisco (123). De locatie van bestanden en de wachtwoorden kunnen worden gewijzigd in **WEB-INF/web.xml**.

Hier zijn de stappen om een nieuwe Java KeyStore te genereren:

1. Om een root (vertrouwde) keystore te maken, moet u het CA-certificaat importeren (**cert-ca.der** moet in DER-indeling zijn):

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

2. Wanneer u een nieuw toetsenbord maakt, kiest u een wachtwoord dat later wordt gebruikt om toegang tot het toetsenbord te krijgen.

3. Importeer het MnT-identiteitsbewijs naar het worteltoetsenbord (**cert-mnt.der** is het identiteitsbewijs dat van ISE is overgenomen en moet in DER-indeling zijn):

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

4. Voer het CA-certificaat in om de client te maken:

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

5. Maak een privé-sleutel in de client keystore:

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

6. Genereert een certificaataanvraag (CSR) in de clientsleutelwinkel:

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

7. Teken **cert-client.csr** en voer het ondertekende client-certificaat in:

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

8. Controleer dat beide toetsenborden de juiste certificaten bevatten:

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

> **Voorzichtig:** Wanneer het knooppunt ISE 1.3 is bijgewerkt, is er een optie om het identiteitsbewijs te bewaren, maar CA-ondertekening wordt verwijderd. Als resultaat hiervan gebruikt de opgewaardeerde ISE een nieuw certificaat maar voegt nooit het CA certificaat in het SSL/ServerHello bericht toe. Dit veroorzaakt de storing op de client die (volgens RFC) verwacht een volledige keten te zien.

schuilnaam

PxGrid API voor verschillende functies (zoals sessiedownload) voert een aanvullende validatie uit. De client contacteert de ISE en ontvangt de ISE hostname, die door de hostname opdracht in CLI wordt bepaald. Vervolgens probeert de client DNS-resolutie voor die hostnaam uit te voeren en probeert u gegevens van dat IP-adres te contacteren en op te halen. Als de DNS-resolutie voor de ISE-hostname mislukt, probeert de client geen gegevens te verkrijgen.

> **Voorzichtig:** Merk op dat alleen de hostname wordt gebruikt voor deze resolutie, die in dit scenario is **opgenomen**, en niet de Full Qualified Domain Name (FQDN), die in dit scenario **lise.voorbeeld.com** is.

Opmerking voor ontwikkelaars

Cisco publiceert en ondersteunt pxGrid API. Er is één pakket zo genoemd:

pxgrid-sdk-1.0.0-167

In de lijst staan:

- PxGrid JAR-bestanden met klassen, die eenvoudig kunnen worden gedecodeerd tot Java-bestanden om de code te controleren
- Steekproef van Java-KeyStores met certificaten
- Steekproef scripts die gebruik maken van voorbeeldJava beoordelen die gebruik maken van pxGrid

Syslog

Hier is de lijst van veiligheidsoplossingen die syslogberichten met het IP adres van de aanvaller

verzenden. Deze kunnen eenvoudig met pxLog worden geïntegreerd zolang u de juiste RegExp regel in de configuratie gebruikt.

snuiven

Snort verstuurt signaleringen in deze indeling:

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

Hierna volgt een voorbeeld:

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

Het IP-adres van de aanvaller is altijd het tweede vóór de laatste (bestemming). Het is eenvoudig om een granulair RegExp voor een specifieke handtekening te bouwen en het aanvaller IP-adres te halen. Hier is een voorbeeld van RegExp voor de signatuur van 100124 en bericht Internet Control Message Protocol (ICMP):

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

Cisco adaptieve security applicatie (ASA) inspectie

Wanneer de ASA is geconfigureerd voor HTTP (voorbeeld)-inspectie ziet het corresponderende syslogbericht er als volgt uit:

```
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
```

Opnieuw kon een granulair RegExp worden gebruikt om die berichten te filteren en het aanvallen IP-adres te extraheren, de tweede vóór de laatste.

Cisco Sourcefire-inbraakpreventiesystemen van de volgende generatie (NGIPS)

Hier volgt een voorbeeldbericht van de 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
```

Dus nogmaals, het is eenvoudig om het aanvaller IP-adres te halen omdat dezelfde logica van toepassing is. Ook de beleidsnaam en de handtekening worden meegeleverd, zodat de pxLog regel korrelig kan worden.

Juniper NetScreen

Hier is een voorbeeldbericht verzonden door de oudere Juniper Inbraakdetectie en -preventie (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"
```

Het IP-adres van de aanvaller kan op dezelfde manier worden afgeleid.

Juniper JunOS

JunOS is vergelijkbaar:

```
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-opdrachttabellen

Hier zijn een paar voorbeelden van Linux iptafels.

```
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
```

U kunt sysloginformatie voor elk type pakket verzenden met de geavanceerde functionaliteit die door de iptable modules wordt geboden zoals verbinding volgen, xtafels, rpfilters, patroon matching, enz.

FreeBSD-firewall (IPFW)

Hier is een voorbeeldbericht voor IPFW-blokkerende fragmenten:

```
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-leesbaarheid en CoA-verwerking

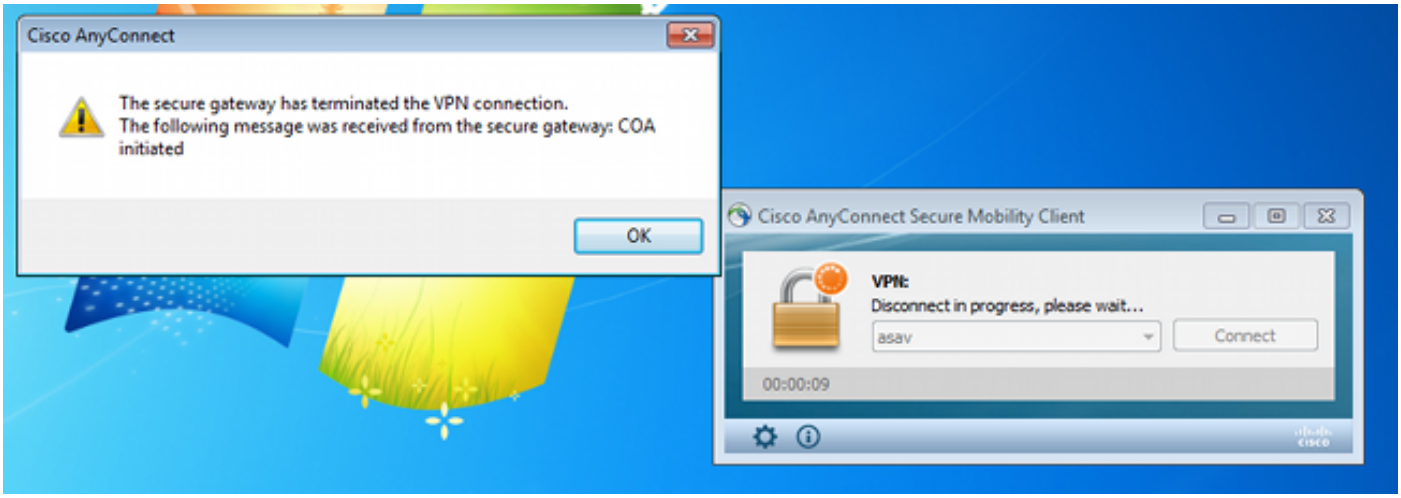
ISE kan het type sessies herkennen in termen van de CoA-behandeling.

- Voor een bekabelde 802.1x/MAC-verificatieomzeilen (MAB) stuurt ISE het CoA-reauthentiek, waardoor een tweede verificatie wordt gestart.

- Voor een draadloze 802.1x/MAB verstuurt ISE de CoA beëindiging, wat een tweede authenticatie in gang zet.

- Voor een ASA VPN stuurt ISE een CoA met een nieuwe DACL aangesloten (geen tweede authenticatie).

De EPS - module is eenvoudig. Wanneer het een quarantaine uitvoert, verstuurt het altijd een CoA-pakket. Voor bekabelde/draadloze sessies is dit geen probleem (alle 802.1x-aanvragers kunnen op transparante wijze een tweede EAP-sessie starten). Maar wanneer de ASA de CoA beëindiging ontvangt, daalt het de VPN sessie en de eindgebruiker wordt voorgesteld:



Er zijn twee mogelijke oplossingen om AnyConnect VPN automatisch opnieuw aan te sluiten (geconfigureerd in het XML-profiel):

- Autorecit, die slechts werkt wanneer u de verbinding met de VPN gateway verloor, niet voor administratieve beëindiging

- Always-on, die werkt en AnyConnect afdwingt om de sessie automatisch opnieuw in te stellen

Zelfs wanneer de nieuwe sessie wordt ingesteld, kiest de ASA de nieuwe audit-sessie-id. Vanuit het ISE-gezichtspunt is dit een nieuwe sessie en is er geen kans om de quarantaineregel te treffen. Ook voor VPN's is het niet mogelijk het MAC-adres van het eindpunt als identiteit te gebruiken, in tegenstelling tot bekabeld/draadloos punt1x.

De oplossing is de EPS te dwingen zich te gedragen als de ISE en het juiste type CoA te sturen op basis van de sessie. Deze functie wordt ingevoerd in ISE versie 1.3.1.

PxGrid-partners en -oplossingen

Hier is een lijst met PxGrid-partners en -oplossingen:

- LogRitm (Security Information and Event Management (SIEM)) - ondersteunt de REST API (Representational State Transfer)
- Splunk (SIEM) - ondersteunt REST API
- HP Arcsight (SIEM) - ondersteunt REST API
- Sentinel NetIQ (SIEM) - plannen voor ondersteuning van pxGrid
- Lancope StealthWatch (SIEM) - Plannen om pxGrid te ondersteunen

- Cisco Sourcefire - plannen voor ondersteuning van pxGrid 10000 Series
- Cisco web security applicatie (WSA) - plannen voor ondersteuning van pxGrid in april 2014

Hier zijn andere partners en oplossingen:

- Tactiveren (kwetsbaarheidsbeoordeling)
- Emulex (pakketvastlegging en forensisch)
- Bayshore Networks (Data Loss Prevention (DLP) en het IoT-beleid (Internet of Things))
- Ping Identity (Identity and Access Management (IAM)/Single Sign On (SSO))
- Qradar (SIEM)
- Logisch (SIEM)
- Symantec (SIEM en mobiel apparaatbeheer (MDM))

Raadpleeg de catalogus van marktoplossingen voor de volledige lijst met beveiligingsoplossingen.

ISE API's: REST vs EREST vs. PxGrid

Er zijn drie typen API beschikbaar op ISE versie 1.3.

Hier zie je een vergelijking:

	REST	Externe REST	PxGrid
Clientverificatie	gebruikersnaam + wachtwoord (basisHTTP-auth)	gebruikersnaam + wachtwoord (basisHTTP-auth)	attest
Afscheiding voorrecht	nee	beperkt (ERS Admin)	ja (groeper
Toegang	MnT	MnT	MnT
Vervoer	TCP/443 (HTTPS)	TCP/9060 (HTTPS)	TCP/5222 (XMPP)
HTTP-methode	KRIJGEN	KRIJG/POST/PUT	KRIJGEN/P
Standaard ingeschakeld	ja	nee	nee
Aantal verrichtingen	weinig	velen	weinig
CoA-beëindiging	ondersteund	nee	ondersteun
CoA opnieuw bevestigen	ondersteund	nee	ondersteun
Gebruikershandelingen	nee	ja	nee
Endpoint bewerkingen	nee	ja	nee
Endpoint Identity Services	nee	ja	nee
Quarantine (IP, MAC)	nee	nee	ja
Instellen zonder quarantaine (IP, MAC)	nee	nee	ja
PortBounce/shutdown	nee	nee	ja
Gebruikershandelingen controleren	nee	ja	nee
portaalbewerkingen	nee	ja	nee
Netwerkapparaatbewerkingen	nee	ja	nee
Netwerkgroepbewerkingen	nee	ja	nee

* Quarantine gebruikt Unified CoA-ondersteuning van ISE versie 1.3.1.

Downloads

PxLog kan worden gedownload van Sourceforge.

De Software Development Kit (SDK) is al inbegrepen. Voor de nieuwste SDK- en API-documentatie voor PxGrid neemt u contact op met uw partner of het Cisco-accountteam.

Gerelateerde informatie

- Cisco ISE 120 REST API
- Cisco ISE 1.2 Externe volledige API voor REST
- Cisco ISE 1.3 beheerdershandleiding
- Technische ondersteuning en documentatie – Cisco Systems