ISE 버전 1.3 pxGrid와 IPS pxLog 애플리케이션 통합

목차

소개

ISE(Identity Services Engine) 버전 1.3은 pxGrid라는 새 API를 지원합니다.인증, 암호화 및 권한(그룹)을 지원하는 이 현대적이고 유연한 프로토콜은 다른 보안 솔루션과의 손쉬운 통합을 지원합니다.이 문서에서는 개념 증명으로 작성된 pxLog 애플리케이션의 사용에 대해 설명합니다.pxLog는 공격자를 격리하기 위해 IPS(Intrusion Prevention System)에서 syslog 메시지를 수신하고 pxGrid 메시지를 ISE로 전송할 수 있습니다.따라서 ISE는 네트워크 액세스를 제한하는 엔드포인트의 권한 부여 상태를 변경하기 위해 RADIUS CoA(Change of Authorization)를 사용합니다.이 모든 작업은 최종 사용자에게 투명하게 수행됩니다.

이 예에서는 Snort가 IPS로 사용되었지만 다른 솔루션은 사용할 수 있습니다.실제로 IPS일 필요는 없습니다.필요한 모든 것은 공격자의 IP 주소를 사용하여 syslog 메시지를 pxLog에 전송하는 것입니다.이렇게 하면 많은 수의 솔루션이 통합될 수 있습니다.

이 문서에서는 일반적인 문제 및 제한 사항과 함께 pxGrid 솔루션의 문제 해결 및 테스트 방법을 소개합니다.

면책조항:pxLog 애플리케이션은 Cisco에서 지원하지 않습니다.이 글은 발상의 증거로 쓰여졌다.주목적은 ISE에서 pxGrid 구현을 더 잘 수행하는 동안 이를 사용하는 것이었습니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco ISE 컨피그레이션 및 이러한 주제에 대한 기본 지식을 보유하고 있는 것이 좋습니다.

- ISE 구축 및 권한 부여 구성
- Cisco Catalyst 스위치의 CLI 구성

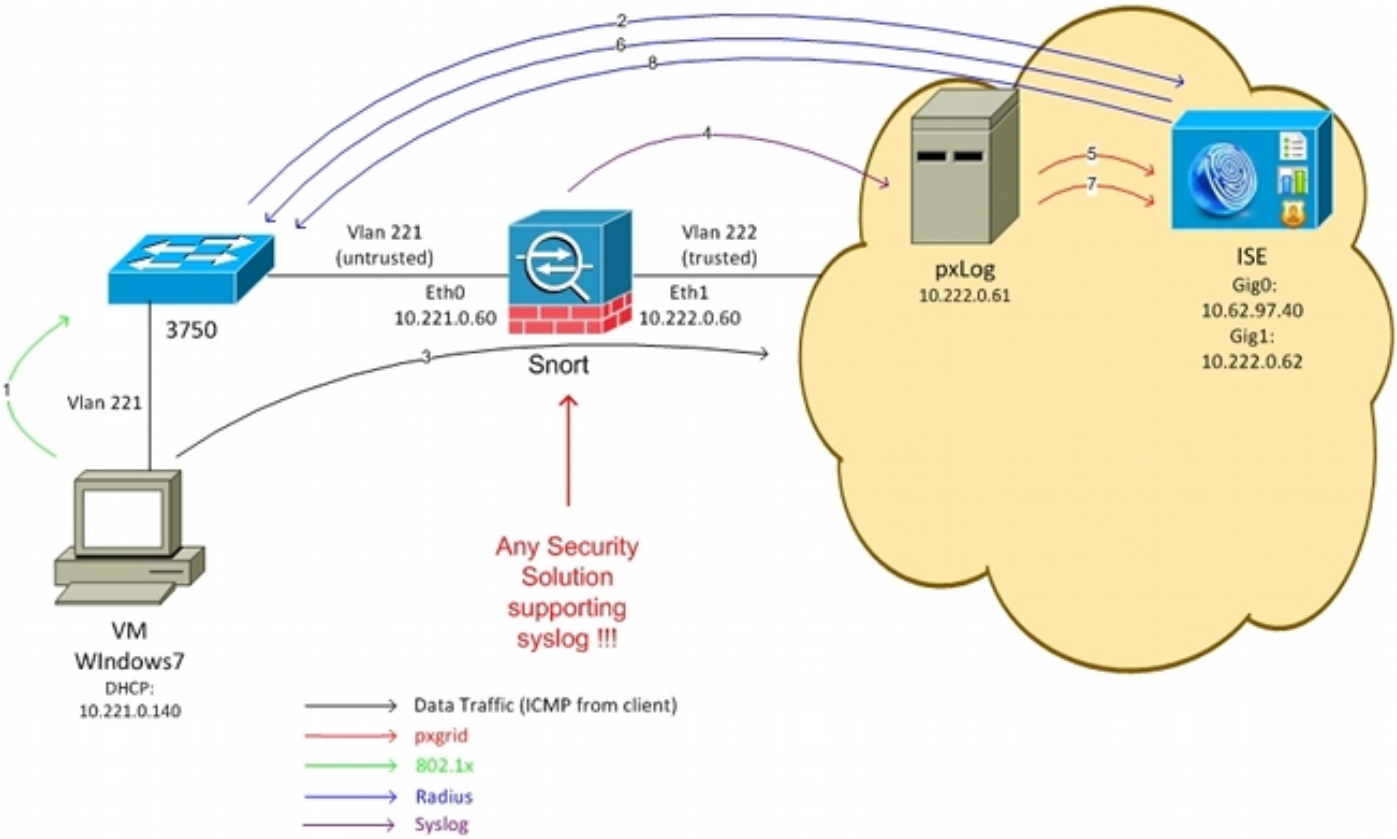
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco Catalyst 3750X Series Switch Software, 버전 15.0 이상
- Cisco ISE 소프트웨어, 버전 1.3 이상
- Cisco AnyConnect Mobile Security with Network Access Manager(NAM), 버전 3.1 이상

- Snort 버전 2.9.6 with Data Acquisition(DAQ)
- Tomcat 7에 설치된 pxLog 애플리케이션(MySQL 버전 5 포함)

네트워크 다이어그램 및 트래픽 흐름



다음은 네트워크 다이어그램에 표시된 트래픽 흐름입니다.

1. Microsoft Windows 7 사용자는 스위치에 연결하여 802.1x 인증을 수행합니다.

2. 스위치는 ISE를 AAA(Authentication, Authorization, and Accounting) 서버로 사용합니다 .Dot**1x 전체 액세스** 권한 부여 규칙이 일치하고 전체 네트워크 액세스가 부여됩니다(DACL:모두 허용(PERMIT_ALL).

3. 사용자는 신뢰할 수 있는 네트워크에 연결하려고 시도하고 Snort 규칙을 위반합니다.

4. 따라서 Snort는 syslog를 통해 pxLog 애플리케이션에 알림을 전송합니다.

5. pxLog 애플리케이션은 로컬 데이터베이스에 대해 확인을 수행합니다.Snort에서 보낸 syslog 메시지를 포착하고 공격자의 IP 주소를 추출하기 위해 구성됩니다.그런 다음 pxGrid를 사용하여 공격자 IP 주소를 격리하기 위해 ISE로 요청을 전송합니다(ISE는 pxGrid 컨트롤러임).

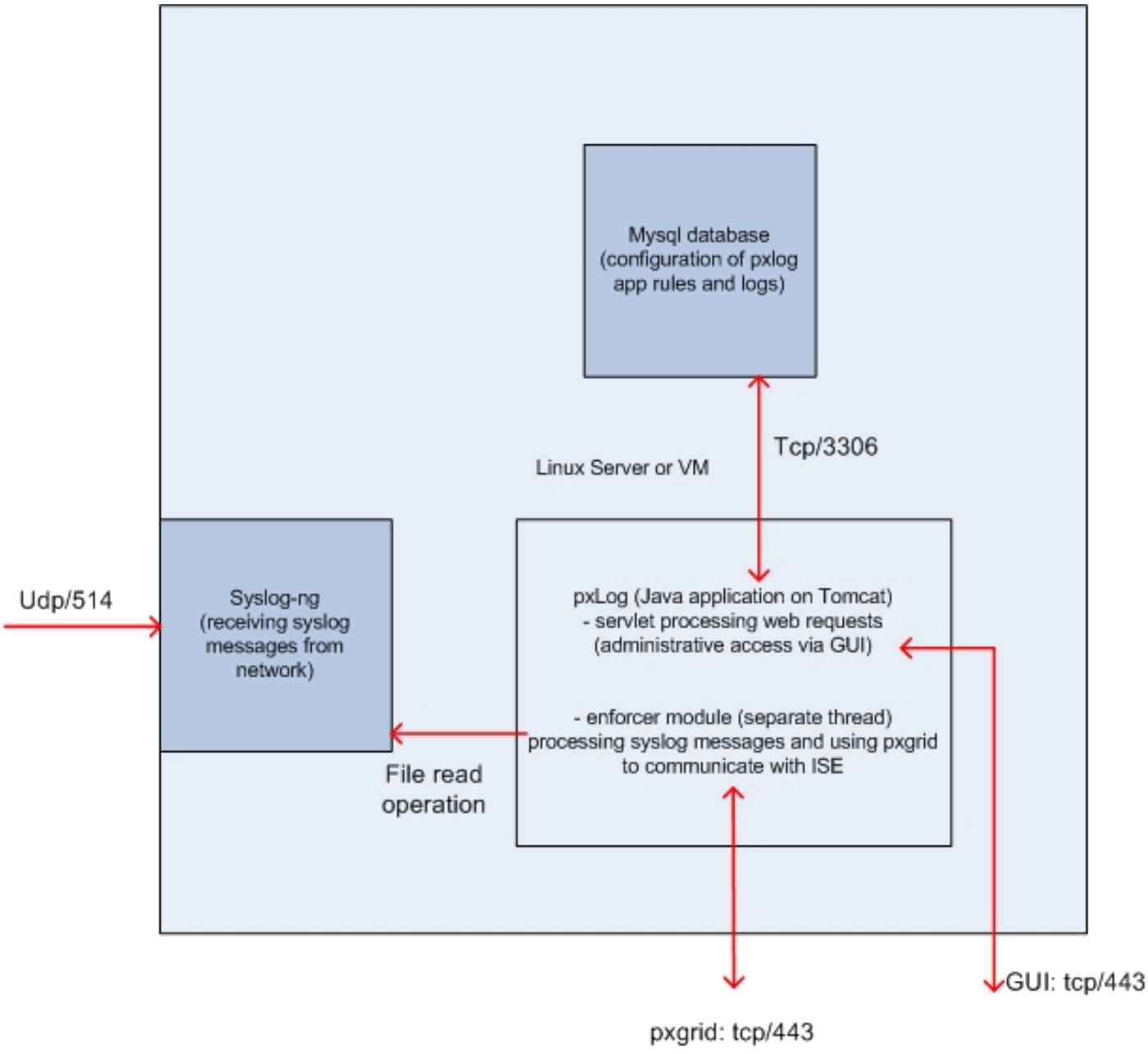
6. ISE는 권한 부여 정책을 다시 평가합니다.엔드포인트가 격리되므로 **Session:EPSStatus EQUALS Quarantine** 조건이 충족되고 다른 권한 부여 프로파일이 일치됩니다(**Dot1x Quarantine**). ISE는 세션을 종료하기 위해 스위치에 CoA 종료를 보냅니다.이렇게 하면 재인증이 트리거되고 최종 사용자에게 제한된 네트워크 액세스를 제공하는 새로운 DACL(Downloadable ACL)(PERMIT_ICMP)이 적용됩니다.

7. 이 단계에서 관리자는 엔드포인트의 격리 해제를 결정할 수 있습니다.이는 pxLog의 GUI를 통해 수행할 수 있습니다.다시, ISE에 대한 pxGrid 메시지가 전송됩니다.

8. ISE는 6단계와 유사한 작업을 수행합니다. 이번에는 엔드포인트가 더 이상 격리되지 않고 전체 액세스가 제공됩니다.

pxLog

아키텍처



이 솔루션은 Linux 시스템에 애플리케이션 세트를 설치하는 것입니다.

1. Java로 작성되고 Tomcat 서버에 구축된 pxLog 애플리케이션.이 애플리케이션은 다음과 같이 구성됩니다.

   웹 요청을 처리하는 서블릿 - 웹 브라우저를 통해 관리 패널에 액세스하기 위해 사용됩니다.

Enforcer module - 서블릿과 함께 시작되는 스레드입니다.Enforcer는 파일에서 syslog 메시지를 읽고(최적화됨), 구성된 규칙에 따라 해당 메시지를 처리하고, 작업(예: pxGrid를 통한 격리)을 실행합니다.

2. pxLog에 대한 컨피그레이션이 포함된 MySQL 데이터베이스(규칙 및 로그).

3. 외부 시스템에서 syslog 메시지를 수신하여 파일에 쓰는 syslog 서버입니다.

설치

pxLog 애플리케이션은 다음 라이브러리를 사용합니다.

- jQuery(AJAX 지원용)
- JSTL(JavaServer Pages Standard Tag Library) 모델(MVC(Model View Controller) 모델, 데이터는 로직과 구분됩니다.JSP(JavaServer Page) 코드는 렌더링에만 사용되며 Java 클래스에 HTML 코드가 없습니다.
- 로깅 하위 시스템으로 Log4j
- MySQL 커넥터
- 테이블 렌더링/정렬에 대한 displaytag
- Cisco의 pxGrid API(현재 버전 alpha 147)

이러한 모든 라이브러리는 프로젝트의 lib 디렉토리에 이미 있으므로 더 이상 JAR(Java ARchive) 파일을 다운로드할 필요가 없습니다.

응용 프로그램을 설치하려면 다음을 수행합니다.

1. Tomcat Webapp 디렉터리에 대한 전체 디렉터리의 압축을 해제합니다.

2. WEB-INF/web.xml 파일을 편집합니다.유일하게 필요한 변경 사항은 **serverip** 변수인 ISE를 가리킵니다.또한 Java Certificate KeyStores(신뢰할 수 있는 하나 및 ID용 하나)가 기본값 대신 생성될 수 있습니다. 이는 클라이언트 및 서버 인증서와 함께 SSL(Secure Sockets Layer) 세션을 사용하는 pxGrid API에서 사용됩니다.통신의 양쪽은 인증서를 제공해야 하며 서로를 신뢰해야 합니다.자세한 내용은 pxGrid 프로토콜 요구 사항 섹션을 참조하십시오.

3. ISE 호스트 이름이 pxLog에서 올바르게 확인되었는지 확인합니다(DNS(Domain Name Server) 또는 **/etc/hosts 항목**의 레코드 참조). 자세한 내용은 pxGrid 프로토콜 요구 사항 섹션을 참조하십시오.

4. mysql/init.sql 스크립트로 MySQL 데이터베이스를 **구성합니다**.자격 증명은 변경할 수 있지만 WEB-INF/web.xml 파일에 반영해야 합니다.

Snort

이 문서에서는 특정 IPS에 초점을 두지 않으므로 간단한 설명만 제공됩니다.

Snort는 DAQ 지원과 함께 인라인으로 구성됩니다.트래픽은 iptables로 리디렉션됩니다.

```
iptables -I FORWARD -j ACCEPT
iptables -I FORWARD -j NFQUEUE --queue-num 1
```
그런 다음 검사 후 기본 iptable 규칙에 따라 삽입되고 전달됩니다.

몇 가지 사용자 지정 Snort 규칙이 구성되었습니다(**/etc/snort/rules/test.rules** 파일이 전역 컨피그레이션에 포함되어 있음).

```
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)
```
패킷의 TTL(Time To Live)이 6이거나 페이로드의 크기가 666에서 686 사이인 경우 Snort는 syslog 메시지를 전송합니다. 트래픽은 Snort에 의해 차단되지 않습니다.

또한 경고가 너무 자주 트리거되지 않도록 임계값을 설정해야 합니다(/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
```
그런 다음 syslog 서버가 pxLog 시스템(/etc/snort/snort.conf)을 가리킵니다.

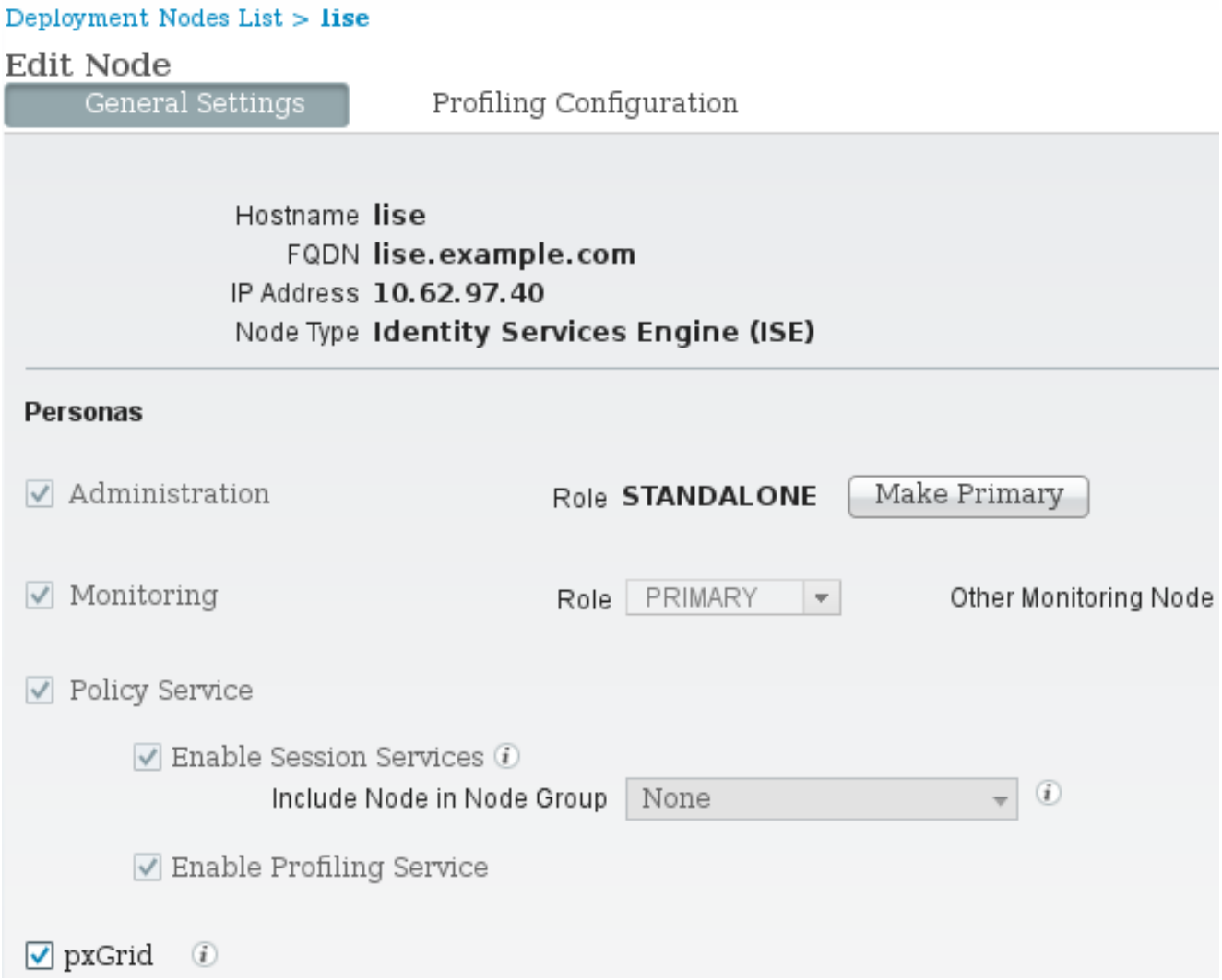
```
output alert_syslog: host=10.222.0.61:514, LOG_AUTH LOG_ALER
```
일부 버전의 Snort에서는 syslog 컨피그레이션과 관련된 버그가 있습니다. 그런 다음, 특정 메시지를 pxLog 호스트로 전달하기 위해 localhost 및 syslog-ng를 가리키도록 기본 설정을 사용할 수 있습니다.

ISE

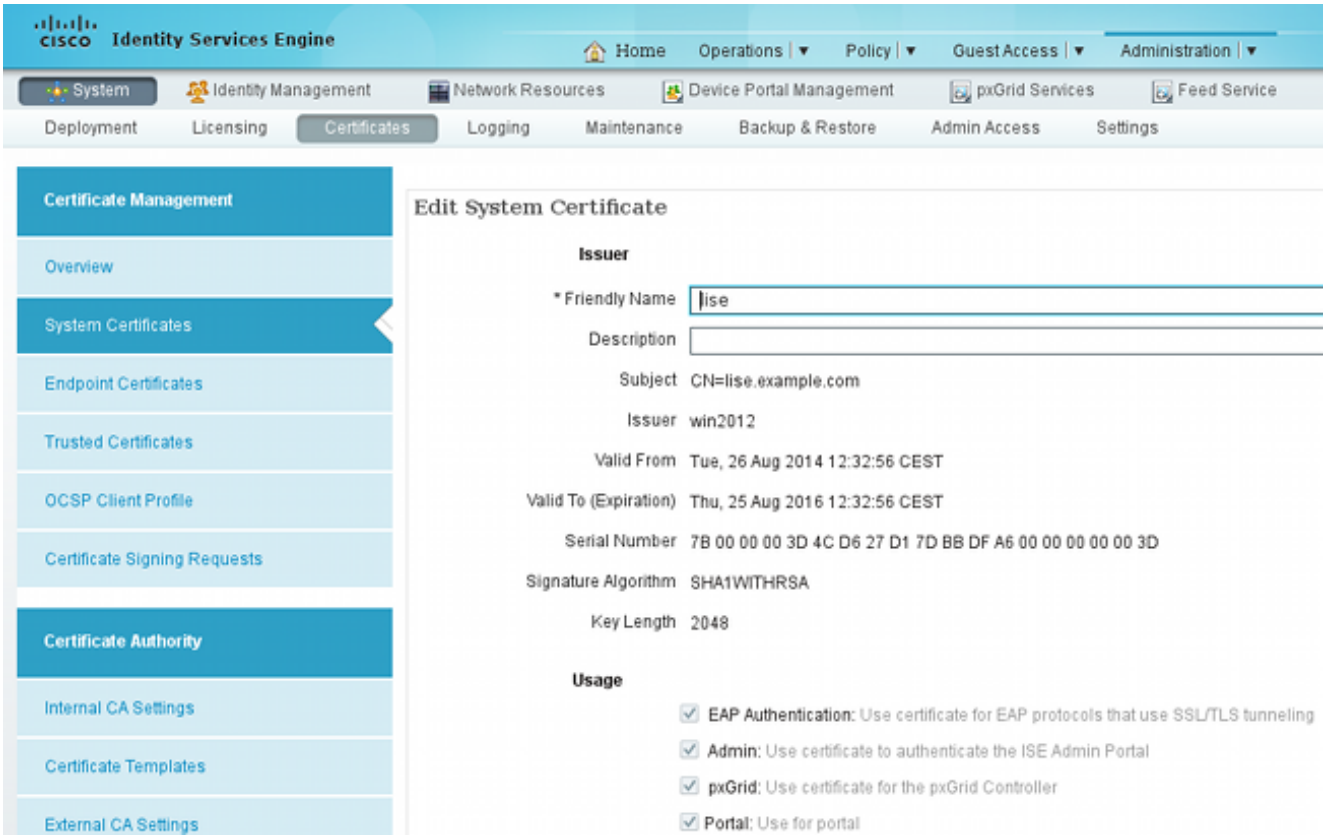
구성

개인 및 인증서

1. ISE에서 기본적으로 비활성화된 pxGrid 역할을 Administration(관리) > Deployment(구축)에서 **활성화합니다**.

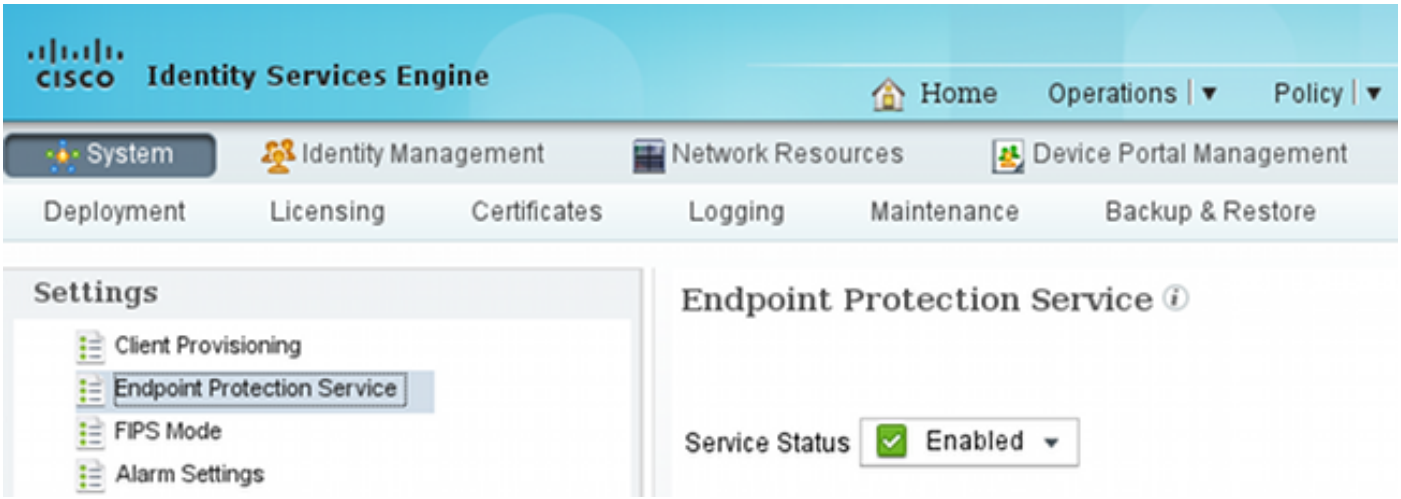


2. Administration(관리) > Certificates(인증서) > System Certificates(시스템 인증서)에서 pxGrid에 인증서가 사용되는지 **확인합니다**.



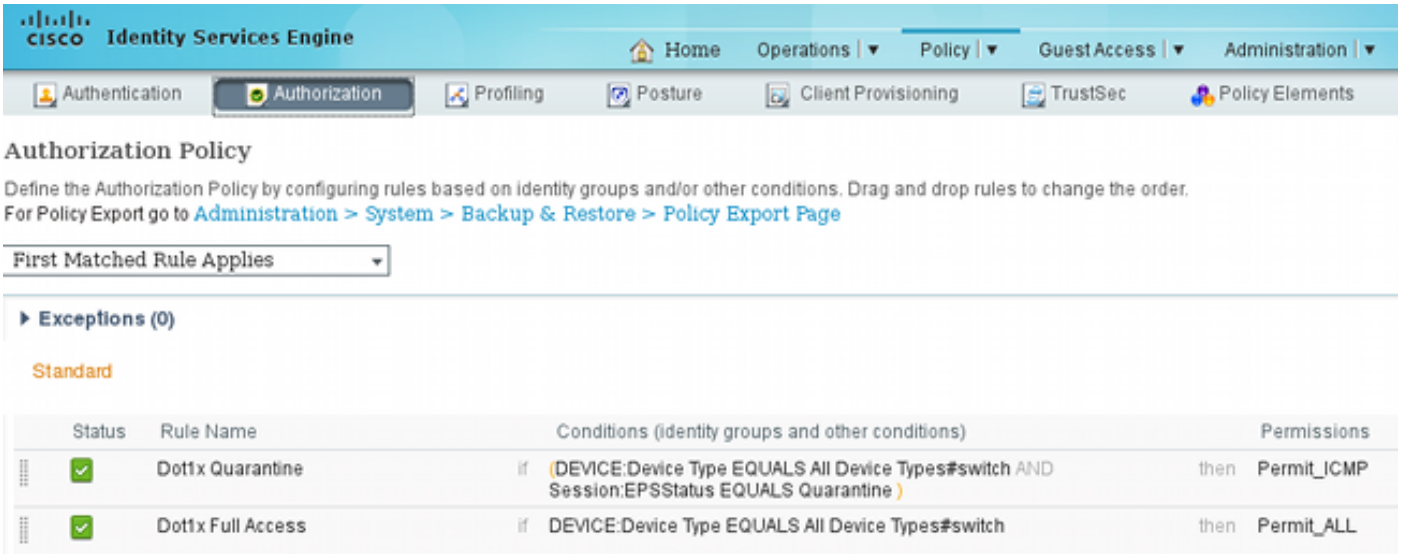
EPS(Endpoint Protection Service)

EPS는 Administration(관리) > **Settings(설정)**에서 활성화(기본적으로 비활성화)해야 합니다.



이를 통해 격리/격리 해제 기능을 사용할 수 있습니다.

권한 부여 규칙



첫 번째 규칙은 엔드포인트가 격리된 경우에만 발생합니다.그러면 제한된 액세스는 RADIUS CoA에 의해 동적으로 시행됩니다.또한 스위치를 올바른 공유 암호로 네트워크 장치에 추가해야 합니다.

문제 해결

pxGrid 상태는 CLI에서 확인할 수 있습니다.

```
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
```

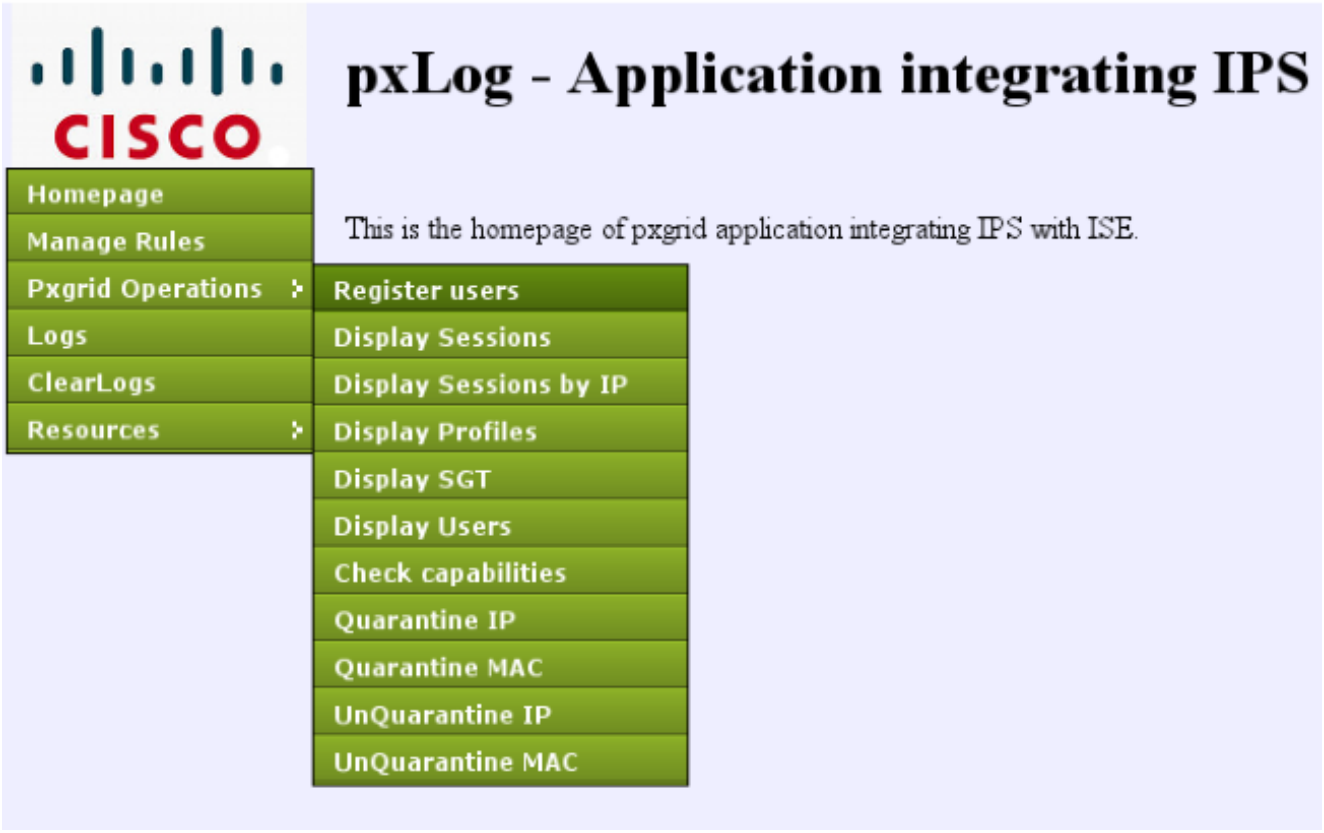
pxGrid에 대한 별도의 디버그도 있습니다(**Administration > Logging > Debug Log Configuration > pxGrid**). 디버그 파일은 pxGrid 디렉토리에 저장됩니다.가장 중요한 데이터는 pxgrid/pxgrid-jabberd.log 및 **pxgrid/pxgrid-controller.log**에 **있습니다**.

테스트

1단계. pxGrid 등록

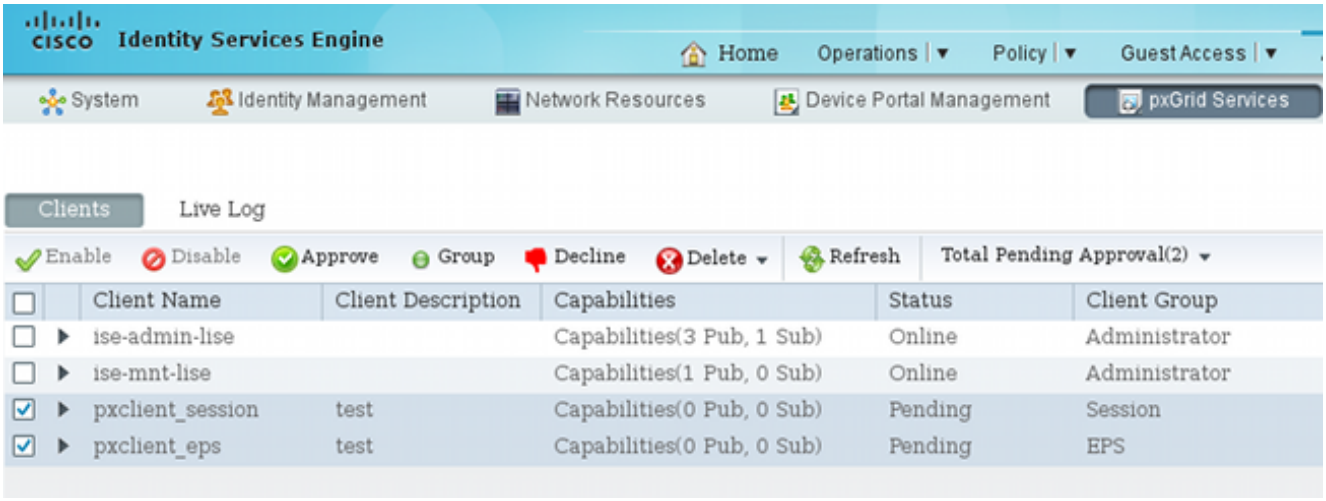
Tomcat이 시작되면 pxLog 애플리케이션이 자동으로 구축됩니다.

1. pxGrid를 사용하려면 ISE에 사용자 2명을 등록합니다(세션 액세스 권한이 있는 사용자 1명, 격리 포함). 이 작업은 Pxgrid Operations(Pxgrid 작업) **> Register users(사용자 등록)**에서 완료할 수 있습니다.

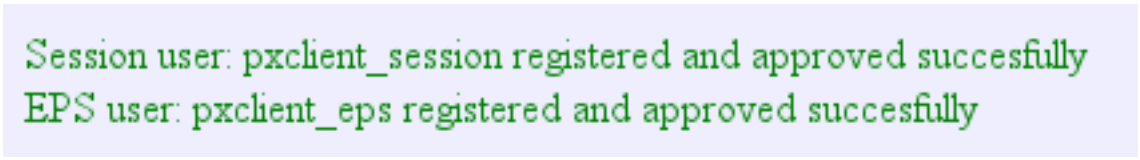


등록이 자동으로 시작됩니다.

2. 이 단계에서는 ISE에서 등록된 사용자를 승인해야 합니다(자동 승인이 기본적으로 비활성화됨).



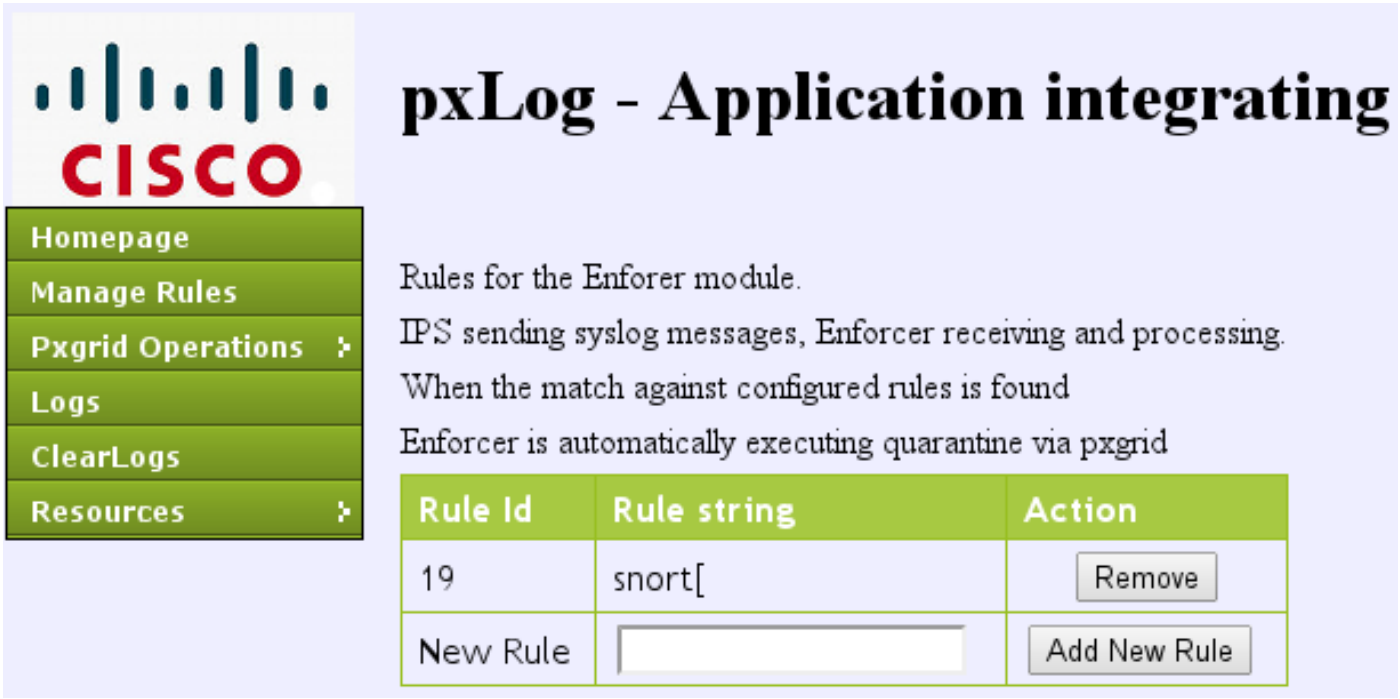
승인 후 pxLog는 AJAX 호출을 통해 관리자에게 자동으로 알립니다.



ISE는 해당 두 사용자의 상태를 Online(온라인) 또는 Offline(오프라인)(더 이상 Pending(보류 중)이 아님)으로 표시합니다.

2단계.pxLog 규칙 컨피그레이션

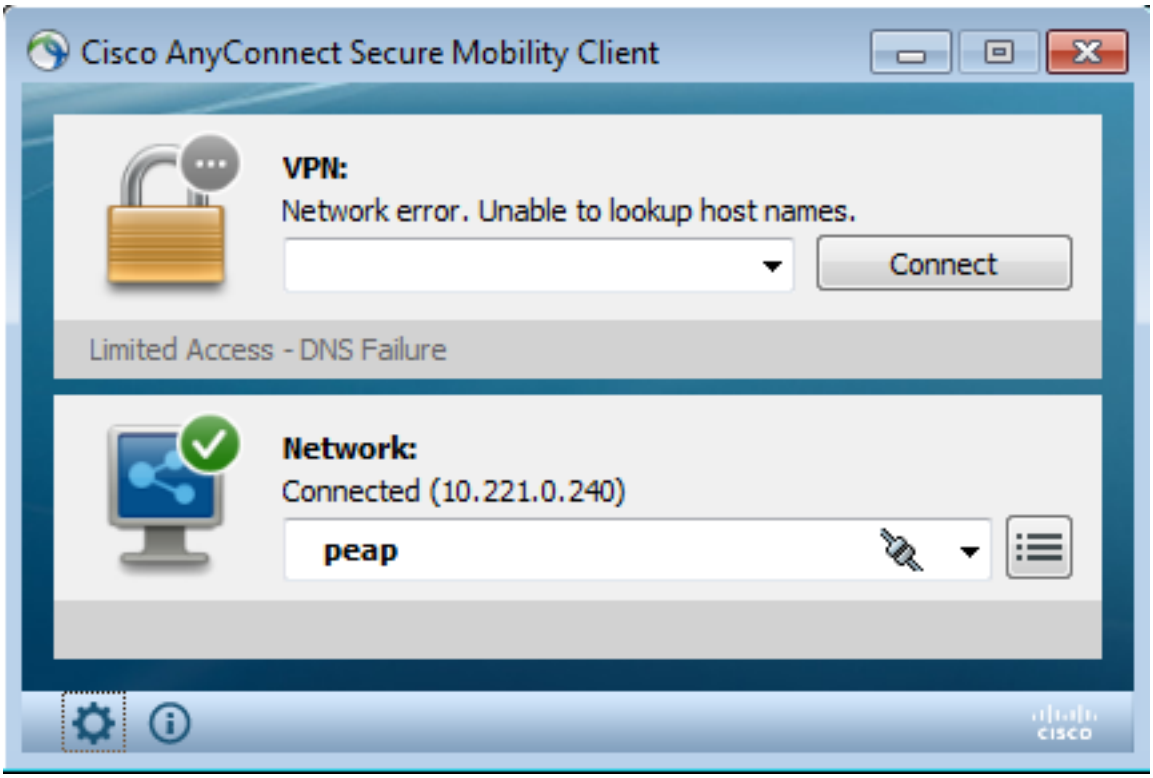
pxLog는 syslog 메시지를 처리하고 이에 따라 작업을 실행해야 합니다.새 규칙을 추가하려면 Manage **Rules**(규칙 관리)를 선택합니다.



이제 enforcer 모듈은 syslog 메시지에서 이 정규식(RegExp)을 찾습니다."snort[". 검색되면 모든 IP 주소를 검색하고 마지막 주소 앞에 있는 주소를 선택합니다.대부분의 보안 솔루션과 일치합니다.자세한 내용은 Syslog 섹션을 참조하십시오.해당 IP 주소(공격자)는 pxGrid를 통해 격리됩니다.또한 더 세분화된 규칙을 사용할 수도 있습니다(예: 시그니처 번호가 포함될 수 있음).

3단계. 첫 번째 Dot1x 세션

Microsoft Windows 7 스테이션은 유선 dot1x 세션을 시작합니다.Cisco Anyconnect NAM은 신청자로 사용되었습니다.EAP-PEAP(Extensible Authentication Protocol-Protected EAP) 방법이 구성됩니다.



ISE **Dot1x Full Access** 권한 부여 프로파일이 선택됩니다.스위치는 전체 액세스 권한을 부여하기 위해 액세스 목록을 다운로드합니다.

```
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
```

4단계. Microsoft Windows PC에서 경보를 트리거하는 패킷을 보냅니다.

이것은 TTL = 7인 Microsoft Windows 패킷에서 보내는 경우 발생하는 상황을 보여줍니다.

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

이 값은 전달 체인의 Snort에서 감소하며 경보가 발생합니다.따라서 pxLog에 대한 syslog 메시지가 전송됩니다.

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

5단계.pxLog

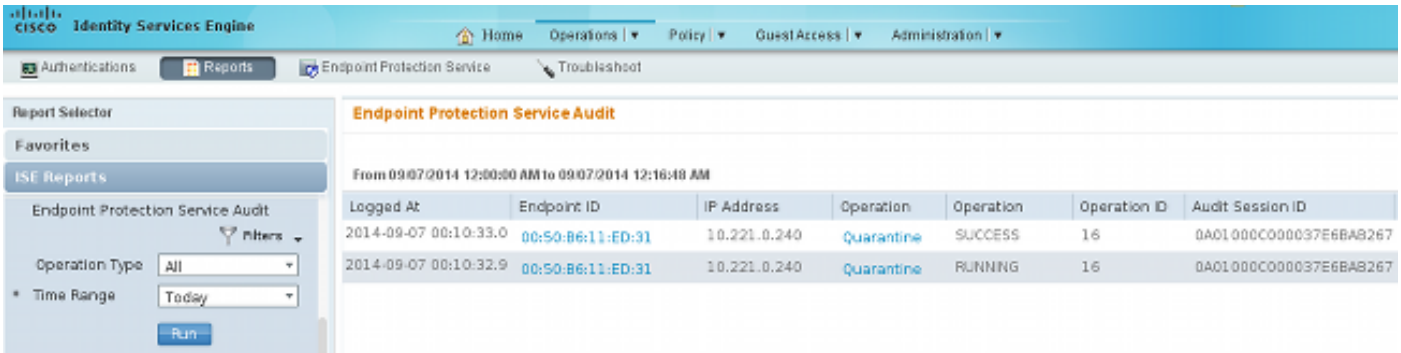
pxLog는 syslog 메시지를 수신하여 처리하고 해당 IP 주소를 격리하도록 요청합니다.다음 로그를 확인할 경우 확인할 수 있습니다.

Logs from the actions executed by the Enforer module

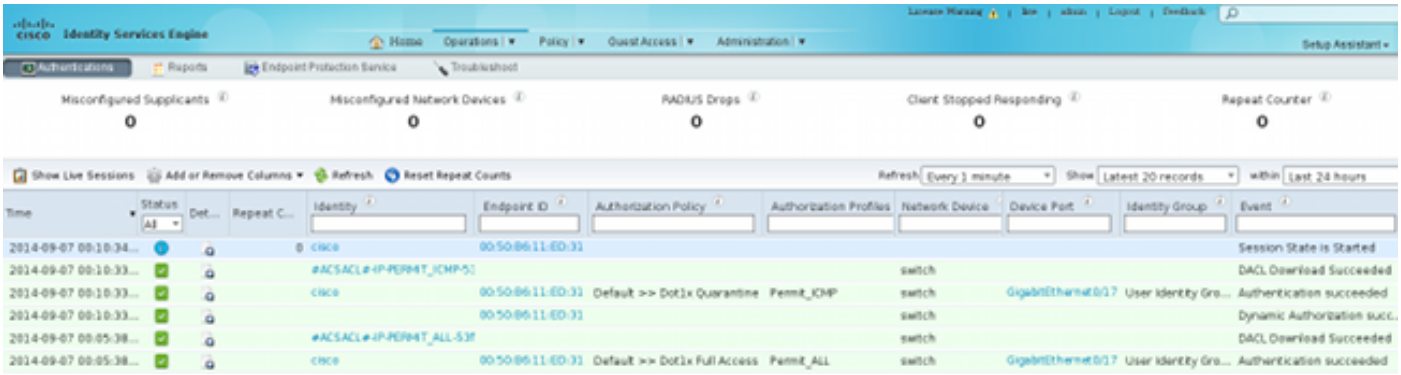
Id	Type	Action	Syslog message	IP
66	SYSLOG	QUARANTINE	Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61	10.221.0.240

6단계. ISE 격리

ISE는 IP 주소가 격리되었음을 보고합니다.



그 결과, 특정 엔드포인트의 스위치에서 권한 부여 상태를 업데이트하기 위해 권한 부여 정책을 검토하고, 격리를 선택하고, RADIUS CoA를 전송합니다.



이는 신청자가 새 세션을 시작하고 제한된 액세스(Permit_ICMP)를 받도록 강제하는 CoA 종료 메시지입니다.

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)
```

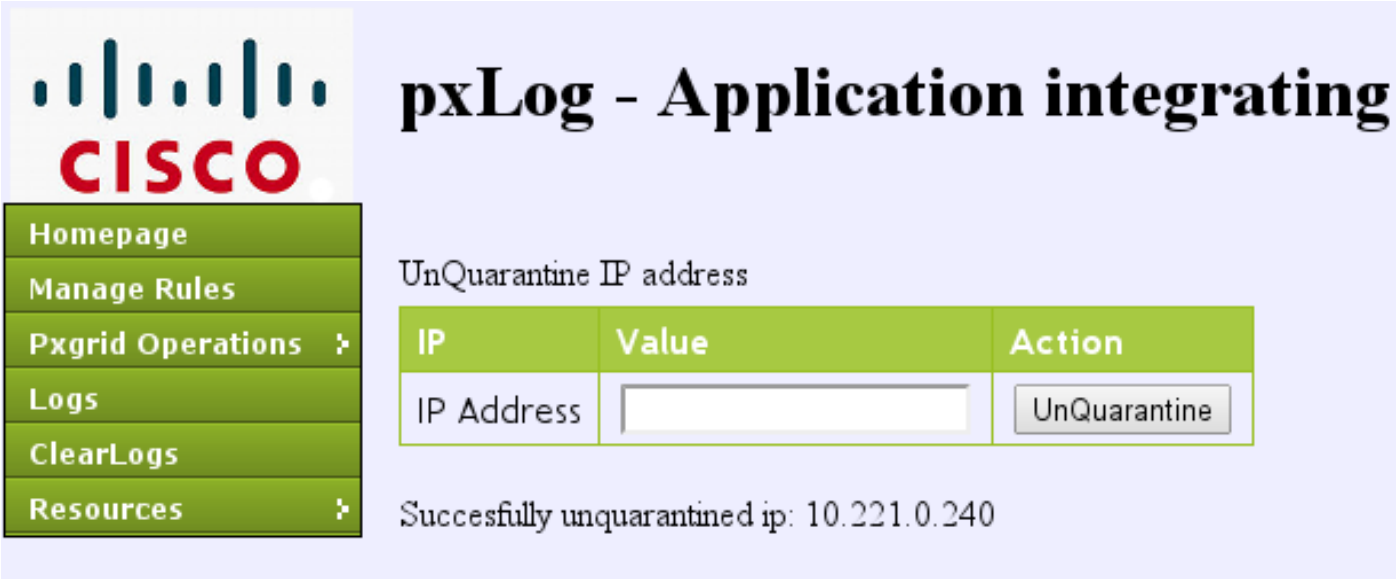
스위치에서 결과를 확인할 수 있습니다(엔드포인트에 대한 제한된 액세스).

```
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
```

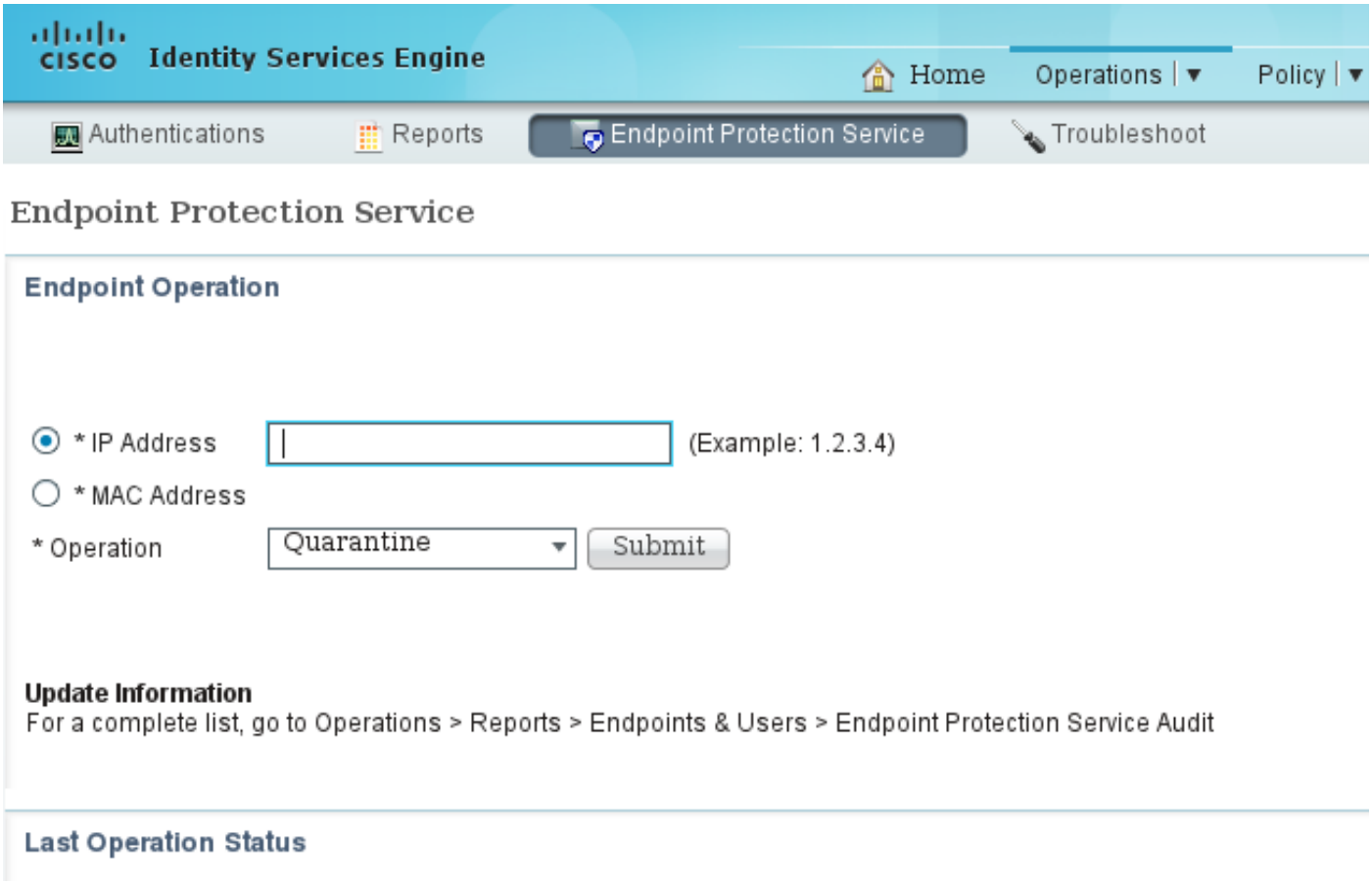
```
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A01000C000037E7BAB7D68C
     Acct Session ID:  0x00003A71
              Handle:  0xE000080F

Runnable methods list:
      Method   State
      dot1x    Authc Success

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

7단계.pxLog 격리 해제

이 단계에서는 관리자가 해당 엔드포인트의 격리 해제를 결정합니다.

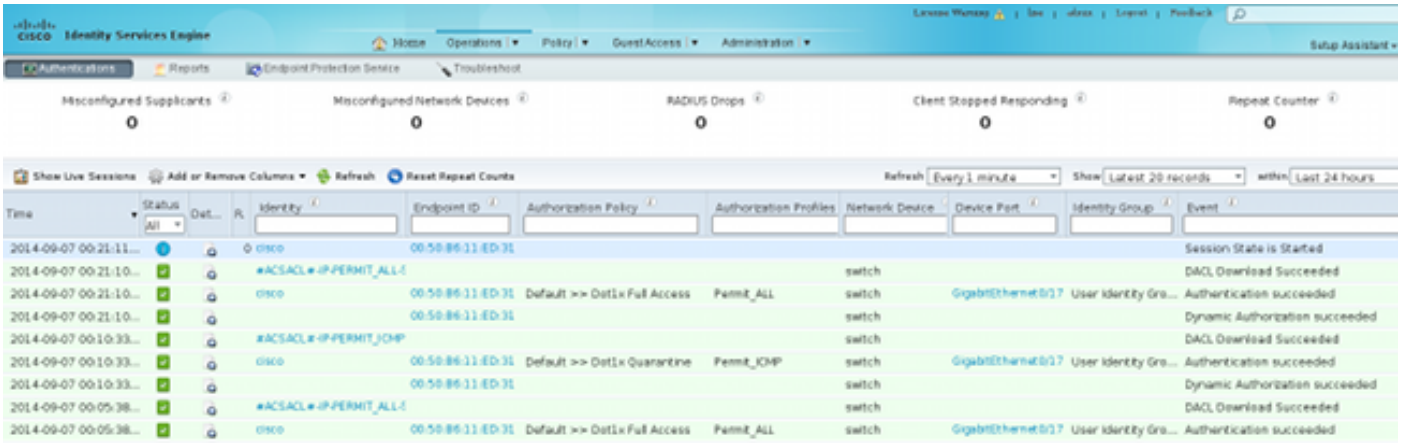


동일한 작업을 ISE에서 직접 실행할 수 있습니다.

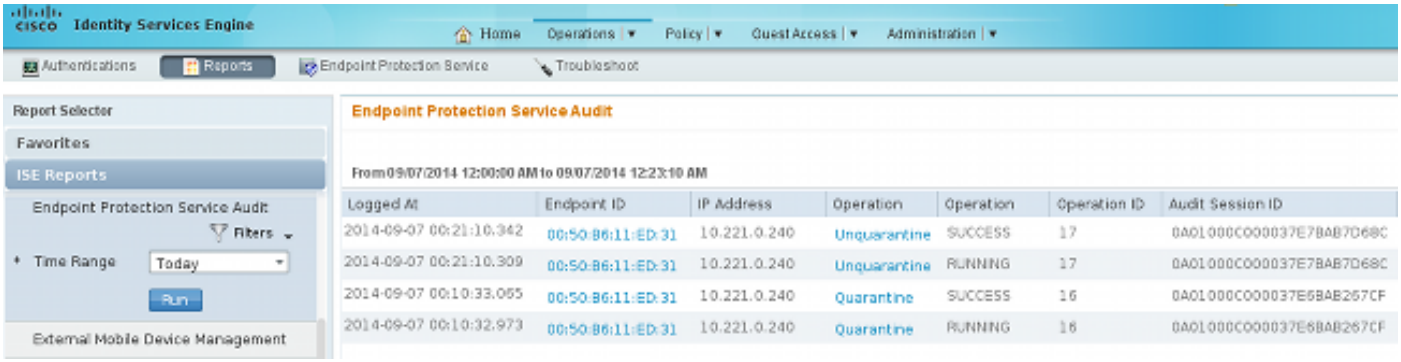


8단계. ISE 격리 해제

ISE는 다시 규칙을 검토하고 스위치에서 권한 부여 상태를 업데이트합니다(전체 네트워크 액세스가 부여됨).



보고서는 다음을 확인합니다.



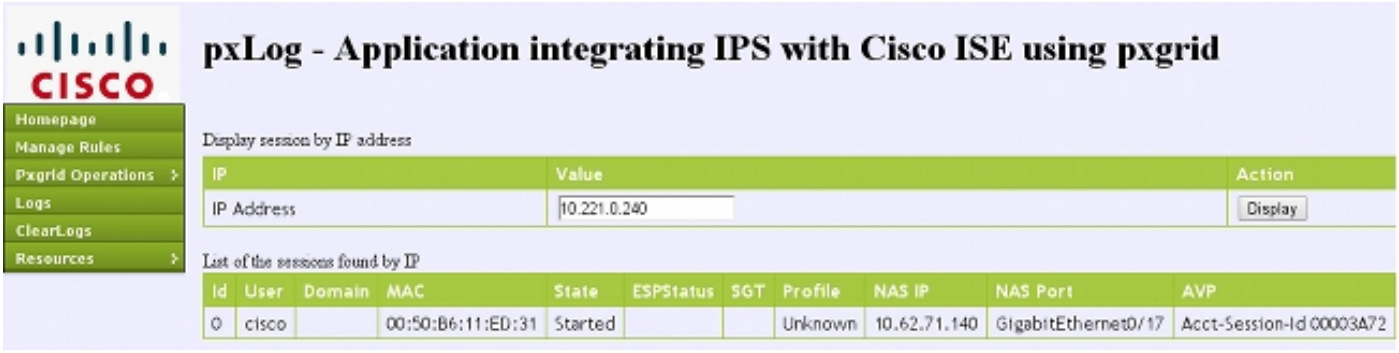
pxLog 기능

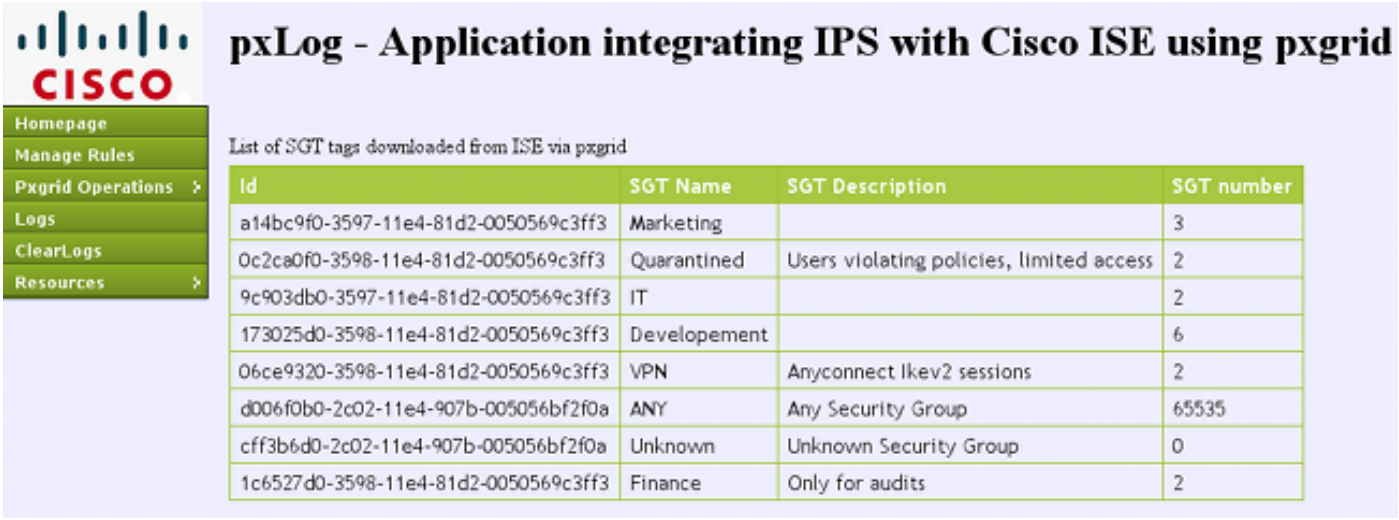
pxLog 애플리케이션은 pxGrid API의 기능을 보여주기 위해 작성되었습니다.이를 통해 다음을 수행할 수 있습니다.

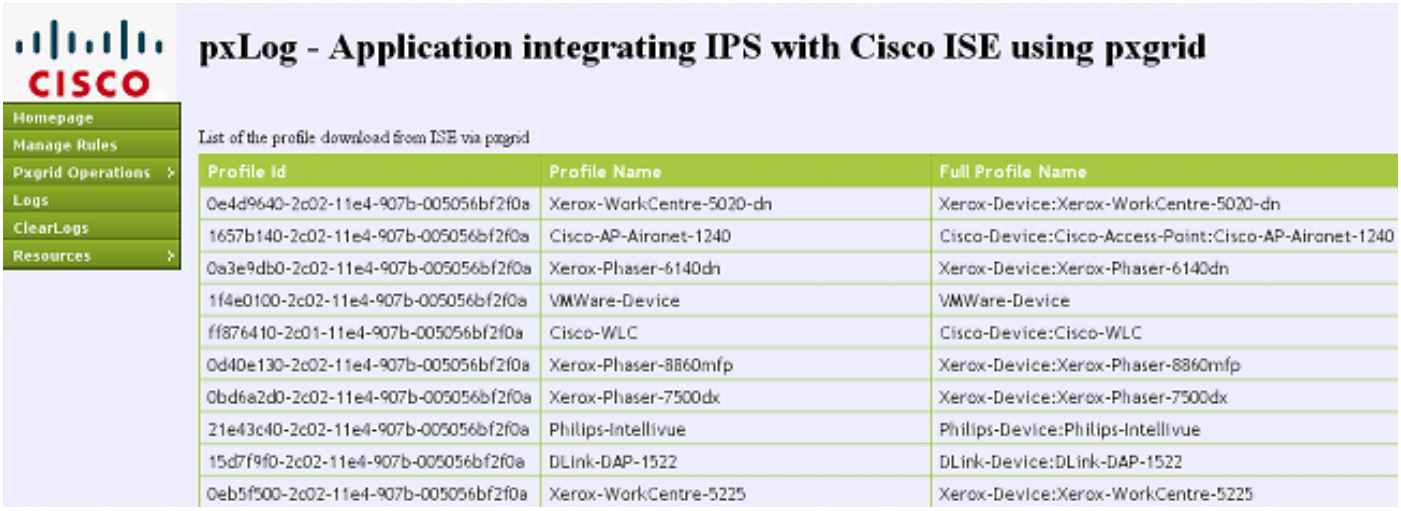
- ISE에서 세션 및 EPS 사용자 등록
- ISE에서 활성화된 모든 세션에 대한 정보 다운로드
- ISE의 특정 활성 세션에 대한 정보 다운로드(IP 주소별)
- ISE의 특정 활성 사용자에 대한 정보 다운로드(사용자 이름 기준)
- 모든 프로파일(프로파일러)에 대한 정보 표시
- ISE에 정의된 TrustSec SGT(Security Group Tag)에 대한 정보를 표시합니다.
- 버전 확인(pxGrid 기능)
- IP 또는 MAC 주소를 기반으로 격리
- IP 또는 MAC 주소를 기반으로 격리 해제

향후 더 많은 기능이 계획됩니다.

다음은 pxLog의 몇 가지 스크린샷입니다.







pxGrid 프로토콜 요구 사항

그룹

클라이언트(사용자)는 한 번에 하나의 그룹의 구성원이 될 수 있습니다.가장 일반적으로 사용되는 두 그룹은 다음과 같습니다.

- 세션 - 세션/프로필/SGT에 대한 정보를 검색/다운로드하는 데 사용됩니다.
- EPS - 격리를 실행하는 데 사용됩니다.

인증서 및 Java KeyStore

앞서 언급한 대로, 클라이언트 애플리케이션인 pxLog 및 pxGrid 컨트롤러(ISE)에 통신을 위해 구성된 인증서가 있어야 합니다.pxLog 애플리케이션은 Java KeyStore 파일에 보관합니다.

- **store/client.jks** - 클라이언트 및 CA(Certificate Authority) 인증서를 포함합니다.
- **store/root.jks** - ISE 체인을 포함합니다.MnT(Monitoring and Troubleshooting Node) ID 및 CA 인증서

파일은 암호로 보호됩니다(기본값:cisco123). 파일 위치 및 비밀번호는 WEB-INF/web.xml에서 변경할 수 **있습니다**.

다음은 새 Java KeyStore를 생성하는 단계입니다.

1. 루트(신뢰할 수 있는) 키 저장소를 생성하려면 CA 인증서(cert-**ca.der**는 DER 형식이어야 함)를 가져옵니다.

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

2. 새 키 저장소를 만들 때 나중에 키 저장소에 액세스하기 위해 사용되는 암호를 선택합니다.

3. MnT ID 인증서를 루트 키 저장소로 가져옵니다(**cert-mnt.der**는 ISE에서 가져온 ID 인증서이며 DER 형식이어야 함).

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

4. 클라이언트 키 저장소를 생성하려면 CA 인증서를 가져옵니다.

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

5. 클라이언트 키 저장소에 개인 키를 만듭니다.

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

6. 클라이언트 키 저장소에서 CSR(Certificate Signing Request)을 생성합니다.

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

7. cert-**client.csr**에 서명하고 서명된 클라이언트 인증서를 가져옵니다.

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

8. 두 키 저장소에 올바른 인증서가 포함되어 있는지 확인합니다.

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

주의:ISE 1.3 노드가 업그레이드되면 ID 인증서를 유지할 수 있는 옵션이 있지만 CA 서명은 제거됩니다.따라서 업그레이드된 ISE는 새 인증서를 사용하지만 SSL/ServerHello 메시지에 CA 인증서를 첨부하지 않습니다.이렇게 하면 (RFC에 따라) 전체 체인을 볼 것으로 예상되는 클라이언트에서 오류가 트리거됩니다.

호스트 이름

세션 다운로드와 같은 여러 기능을 위한 pxGrid API는 추가 검증을 수행합니다.클라이언트는 ISE에 연결하고 CLI의 hostname 명령으로 정의된 ISE 호스트 이름을 수신합니다.그런 다음 클라이언트는 해당 호스트 이름에 대해 DNS 확인을 시도하고 해당 IP 주소에서 데이터를 연결하고 가져오려고 시도합니다.ISE 호스트 이름에 대한 DNS 확인에 실패하면 클라이언트는 데이터를 가져오려고 시도하지 않습니다.

주의:이 시나리오에서 lise.example.com인 FQDN(Fully Qualified Domain Name)이 아니라 이 시나리오에서는 호스트 이름만 이 확인에 사용됩니다.

개발자 참고 사항

Cisco는 pxGrid API를 게시하고 지원합니다.다음과 같은 패키지가 있습니다.

pxgrid-sdk-1.0.0-167

내부에는 다음이 포함됩니다.

- pxGrid JAR 파일과 클래스 포함. 코드를 확인하기 위해 Java 파일로 쉽게 디코딩할 수 있습니다.
- 인증서가 있는 샘플 Java 키 저장소
- pxGrid를 사용하는 샘플 Java 클래스를 사용하는 샘플 스크립트

Syslog

다음은 공격자 IP 주소로 syslog 메시지를 전송하는 보안 솔루션의 목록입니다.컨피그레이션에서 올바른 RegExp 규칙을 사용하는 경우 이러한 규칙을 pxLog에 쉽게 통합할 수 있습니다.

Snort

Snort는 다음 형식으로 syslog 알림을 전송합니다.

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

예를 들면 다음과 같습니다.

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

공격자 IP 주소는 항상 마지막 IP 주소(대상)보다 두 번째입니다. 특정 서명에 대한 세분화된 RegExp를 구축하고 공격자 IP 주소를 추출하는 것은 간단합니다.다음은 서명 100124 및 메시지 ICMP(Internet Control Message Protocol)에 대한 RegExp 예입니다.

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

Cisco ASA(Adaptive Security Appliance) 검사

ASA가 HTTP(예) 검사를 위해 구성된 경우 해당 syslog 메시지는 다음과 같습니다.

```
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
```

다시 세분화된 RegExp를 사용하여 이러한 메시지를 필터링하고 공격자 IP 주소를 추출할 수 있습니다(마지막 IP 주소 앞에 두 번째).

Cisco Sourcefire NGIPS(Next Generation Intrusion Prevention System)

다음은 Sourcefire 센서에서 보낸 메시지의 예입니다.

```
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
```

따라서 동일한 논리가 적용되기 때문에 공격자 IP 주소를 추출하는 것이 간단합니다.또한 정책 이름과 서명이 제공되므로 pxLog 규칙이 세분화될 수 있습니다.

Juniper NetScreen

다음은 이전 Juniper IDP(Intrusion Detection & Prevention)에서 보낸 메시지의 예입니다.

```
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"
```
공격자의 IP 주소는 동일한 방법으로 추출할 수 있습니다.

Juniper JunOS

JunOS는 다음과 유사합니다.

```
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

다음은 Linux iptables의 예입니다.

```
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
```
연결 추적, xtables, rpfilters, pattern matching 등과 같은 iptable 모듈에서 제공하는 고급 기능을 사용하여 모든 유형의 패킷에 대한 syslog 정보를 전송할 수 있습니다.

FreeBSD IPFirewall(IPFW)

다음은 IPFW 차단 프래그먼트의 예입니다.

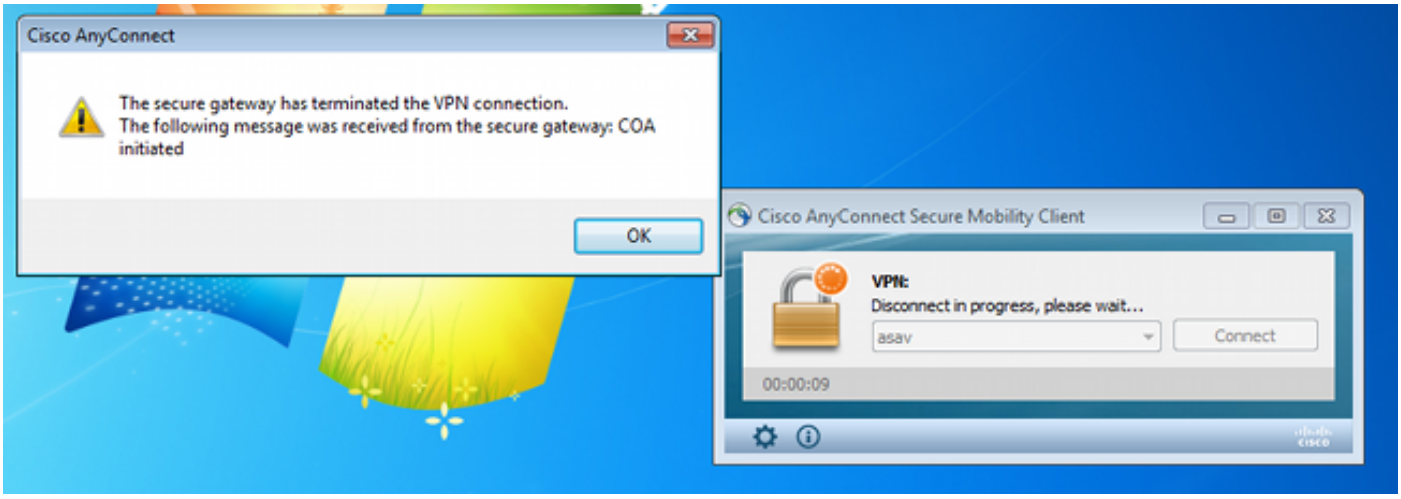
```
Sep  7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0
(frag 52639:519@1480)
```

VPN 준비 상태 및 CoA 처리

ISE는 CoA 처리 측면에서 세션 유형을 인식할 수 있습니다.

- 유선 802.1x/MAB(MAC Authentication Bypass)의 경우 ISE는 CoA 재인증을 전송하며, 이 재인증은 두 번째 인증을 트리거합니다.
- 무선 802.1x/MAB의 경우 ISE는 CoA 종료를 전송하여 두 번째 인증을 트리거합니다.
- ASA VPN의 경우 ISE는 새 DACL이 연결된 CoA(두 번째 인증 없음)를 전송합니다.

EPS 모듈은 간단합니다.쿼런틴을 실행하면 항상 CoA 종료 패킷을 전송합니다.유선/무선 세션의 경우 문제가 되지 않습니다(모든 802.1x 신청자는 투명하게 두 번째 EAP 세션을 시작할 수 있음). 그러나 ASA가 CoA 종료를 수신하면 VPN 세션이 삭제되고 최종 사용자에게 다음과 같은 메시지가 표시됩니다.



AnyConnect VPN이 자동으로 다시 연결되도록(XML 프로필에 구성됨)하는 두 가지 가능한 솔루션이 있습니다.

- 자동 연결 - VPN 게이트웨이와의 연결이 끊길 때만 작동하며, 관리 종료에는 적용되지 않습니다.

- Always-on - AnyConnect가 자동으로 세션을 다시 설정하도록 강제하고 작동

새 세션이 설정되더라도 ASA는 새 audit-session-id를 선택합니다. ISE 관점에서 이 세션은 새 세션이며 격리 규칙을 발견할 가능성이 없습니다.또한 VPN에서는 유선/무선 dot1x와 달리 엔드포인트의 MAC 주소를 ID로 사용할 수 없습니다.

이 솔루션은 EPS가 ISE처럼 동작하도록 하고 세션을 기반으로 올바른 유형의 CoA를 전송하도록 하는 것입니다.이 기능은 ISE 버전 1.3.1에 도입됩니다.

pxGrid 파트너 및 솔루션

다음은 pxGrid 파트너 및 솔루션의 목록입니다.

- LogRhel(Security Information and Event Management) - REST(Representational State Transfer) API 지원
- Splunk(SIEM) - REST API 지원
- HP SIEM(Arcsight) - REST API 지원
- SIEM(Sentinel NetIQ) - pxGrid 지원 계획
- SIEM(Lancope StealthWatch) - pxGrid 지원 계획
- Cisco Sourcefire - pxGrid 1HCY15를 지원할 계획
- Cisco WSA(Web Security Appliance) - 2014년 4월 pxGrid 지원 계획

다른 파트너 및 솔루션은 다음과 같습니다.

- Potended(취약성 평가)
- Emulex(패킷 캡처 및 포렌식)
- Bayshore Networks(DLP) 및 IoT(Internet of Things) 정책)
- Ping Identity(IAM)/Single Sign On(SSO)
- Qradar(SIEM)
- LogLogic(SIEM)
- Symantec(SIEM MDM(Mobile Device Management))

보안 솔루션 전체 목록은 Marketplace Solutions Catalog를 참조하십시오.

ISE API:REST와 EREST와 pxGrid 비교

ISE 버전 1.3에서는 3가지 유형의 API를 사용할 수 있습니다.

비교 내용은 다음과 같습니다.

	REST	외부 RESTful	pxGrid
클라이언트 인증	사용자 이름 + 암호 (기본 HTTP 인증)	사용자 이름 + 암호 (기본 HTTP 인증)	인증서
권한 분리	아니요	제한(ERS 관리자)	예(그룹)
액세스	MnT	MnT	MnT
전송	tcp/443(HTTPS)	tcp/9060(HTTPS)	tcp/5222(XMPP)
HTTP 메서드	다운로드	가져오기/게시/넣기	가져오기/게시
기본적으로 활성화됨	예	아니요	아니요
작업 수	몇 분	많은	몇 분
CoA 종료	지원	아니요	지원
CoA 재인증	지원	아니요	지원되는 *
사용자 작업	아니요	예	아니요
엔드포인트 작업	아니요	예	아니요
엔드포인트 ID 그룹 작업	아니요	예	아니요
격리(IP, MAC)	아니요	아니요	예
격리 해제(IP, MAC)	아니요	아니요	예
포트 바운스/종료	아니요	아니요	예
게스트 사용자 작업	아니요	예	아니요
게스트 포털 작업	아니요	예	아니요
네트워크 장치 작업	아니요	예	아니요
네트워크 장치 그룹 작업	아니요	예	아니요

* 격리는 ISE 버전 1.3.1의 Unified CoA 지원을 사용합니다.

다운로드

pxLog는 Sourceforge에서 다운로드할 수 있습니다.

SDK(소프트웨어 개발 키트)가 이미 포함되어 있습니다.pxGrid에 대한 최신 SDK 및 API 문서는 파트너 또는 Cisco 어카운트 팀에 문의하십시오.

관련 정보

- Cisco ISE 1.2 REST API
- Cisco ISE 1.2 외부 RESTful API
- Cisco ISE 1.3 관리자 가이드
- 기술 지원 및 문서 – Cisco Systems