

ISE Version 1.3 pxGrid-Integration mit IPS pxLog-Anwendung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm und Datenverkehrsfluss](#)

[pxLog](#)

[Architektur](#)

[Installation](#)

[Snort](#)

[ISE](#)

[Konfiguration](#)

[Personal und Zertifikat](#)

[Endpoint Protection Service \(EPS\)](#)

[Autorisierungsregeln](#)

[Fehlerbehebung](#)

[Test](#)

[Schritt 1: Registrierung für pxGrid](#)

[Schritt 2: Konfiguration der pxLog-Regeln](#)

[Schritt 3: Erste Dot1x-Sitzung](#)

[Schritt 4: Microsoft Windows PC sendet das Paket, das den Alarm auslöst.](#)

[Schritt 5: pxLog](#)

[Schritt 6: ISE-Quarantäne](#)

[Schritt 7: pxLog Unquarantine](#)

[Schritt 8: ISE Unquarantäne.](#)

[pxLog-Funktionalität](#)

[Anforderungen an das pxGrid-Protokoll](#)

[Gruppen](#)

[Zertifikate und Java KeyStore](#)

[Hostname](#)

[Hinweis für Entwickler](#)

[Syslog](#)

[Snort](#)

[Cisco Adaptive Security Appliance \(ASA\)-Inspektion](#)

[Cisco Sourcefire Next-Generation Intrusion Prevention-Systeme \(NGIPS\)](#)

[Juniper NetScreen](#)

[Juniper JunOS](#)

[Linux-IPs](#)

[FreeBSD IPFW \(IPFW\)](#)

[VPN-Bereitschaft und CoA-Verarbeitung](#)

[pxGrid-Partner und -Lösungen](#)

[ISE-APIs: REST vs. EREST vs. pxGrid](#)

[Downloads](#)

[Zugehörige Informationen](#)

Einführung

Die Identity Services Engine (ISE) Version 1.3 unterstützt die neue API pxGrid. Dieses moderne und flexible Protokoll, das Authentifizierung, Verschlüsselung und Privilegien (Gruppen) unterstützt, ermöglicht eine einfache Integration mit anderen Sicherheitslösungen. Dieses Dokument beschreibt die Verwendung der pxLog-Anwendung, die als Machbarkeitsstudie geschrieben wurde. pxLog kann Syslog-Meldungen von Intrusion Prevention System (IPS) empfangen und pxGrid-Nachrichten an die ISE senden, um den Angreifer unter Quarantäne zu stellen. Daher verwendet die ISE RADIUS Change of Authorization (CoA), um den Autorisierungsstatus des Endpunkts zu ändern, der den Netzwerkzugriff einschränkt. All dies geschieht für den Endbenutzer transparent.

In diesem Beispiel wurde Snort als IPS verwendet, aber jede andere Lösung kann verwendet werden. Es muss kein IPS sein. Sie müssen lediglich die Syslog-Meldung an pxLog mit der IP-Adresse des Angreifers senden. Dies schafft die Möglichkeit der Integration einer großen Anzahl von Lösungen.

In diesem Dokument wird auch erläutert, wie Sie pxGrid-Lösungen mit den typischen Problemen und Einschränkungen beheben und testen können.

Haftungsausschluss: Die Anwendung pxLog wird von Cisco nicht unterstützt. Dieser Artikel wurde als Machbarkeitsstudie geschrieben. Der Hauptzweck bestand darin, diese während der optimalen pxGrid-Implementierung auf der ISE zu verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Erfahrungen mit der Cisco ISE-Konfiguration und grundlegende Kenntnisse zu folgenden Themen zu verfügen:

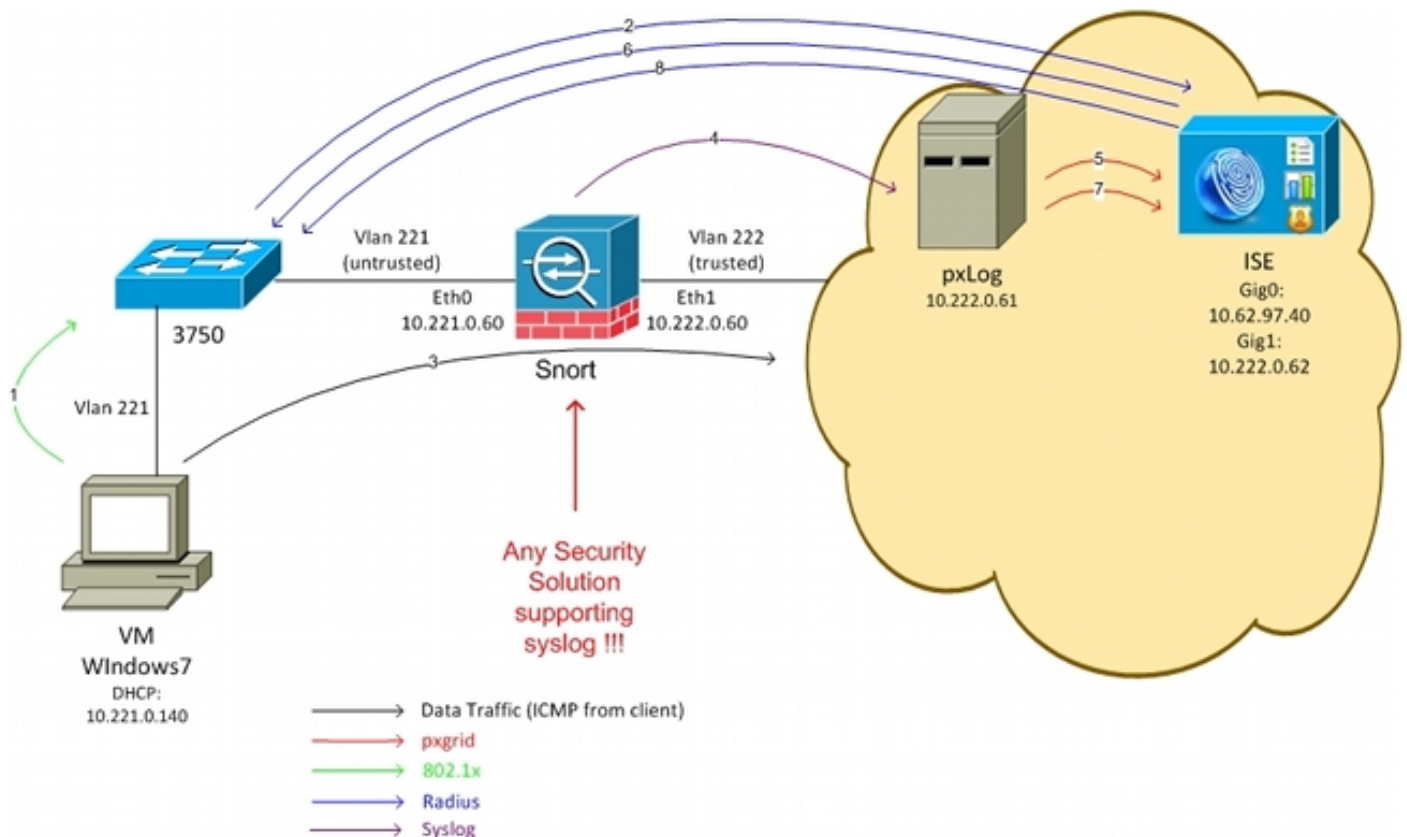
- ISE-Bereitstellungen und Autorisierungskonfiguration
- CLI-Konfiguration von Cisco Catalyst Switches

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco Catalyst Switches der Serie 3750X, Versionen 15.0 und höher
- Cisco ISE Software, Versionen 1.3 und höher
- Cisco AnyConnect Mobile Security mit Network Access Manager (NAM), Version 3.1 und höher
- Snort Version 2.9.6 mit Datenerfassung (DAQ)
- pxLog-Anwendung installiert auf Tomcat 7 mit MySQL Version 5

Netzwerkdiagramm und Datenverkehrsfluss



Hier ist der Datenverkehrsfluss, wie im Netzwerkdiagramm veranschaulicht:

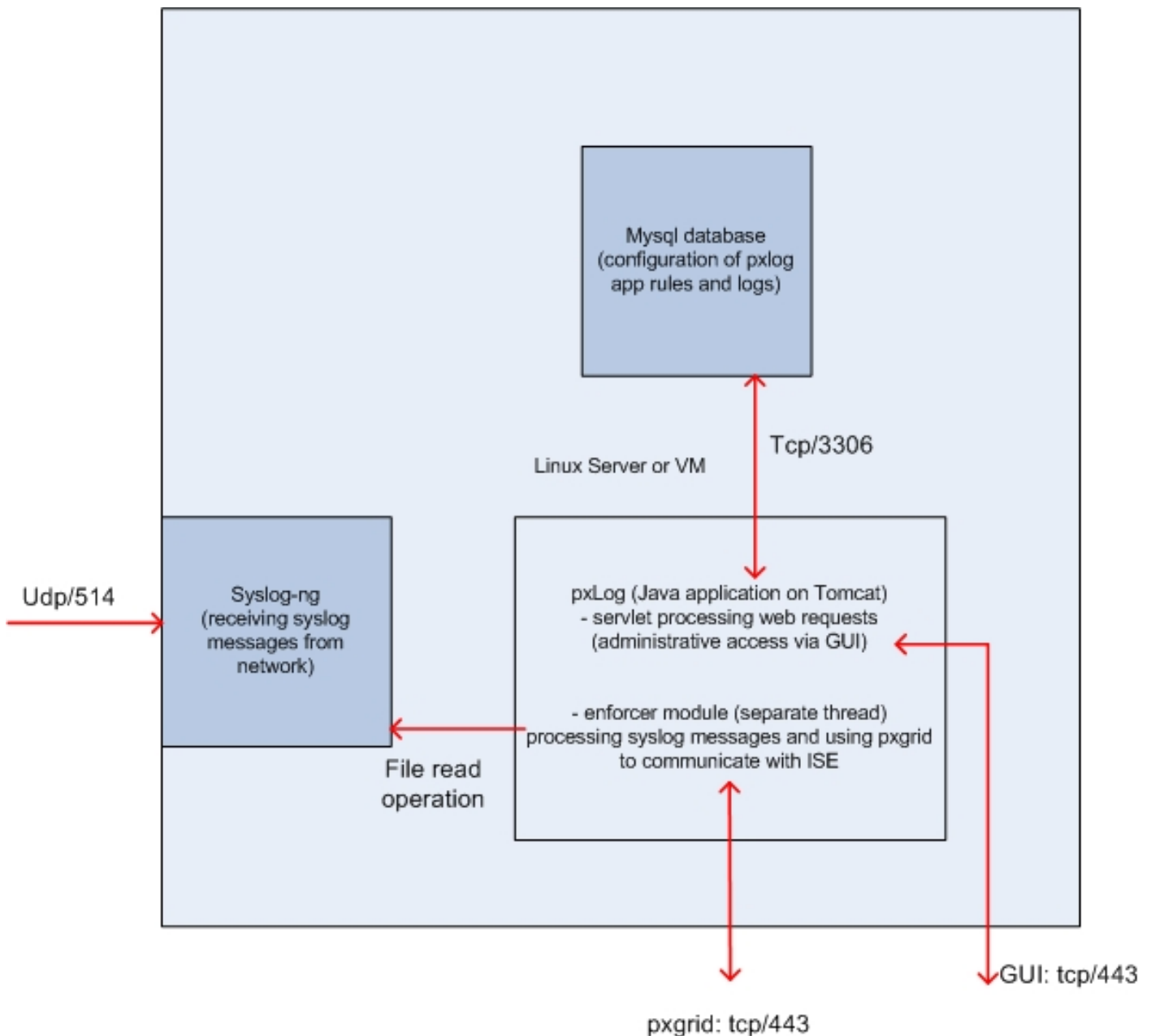
1. Ein Microsoft Windows 7-Benutzer stellt eine Verbindung zum Switch her und führt eine 802.1x-Authentifizierung durch.
2. Der Switch verwendet die ISE als AAA-Server (Authentication, Authorization, and Accounting). Die **Dot1x-Regel für die vollständige** Zugriffsberechtigung wird zugeordnet, und der vollständige Netzwerkzugriff wird gewährt (DACL: PERMIT_ALL).
3. Der Benutzer versucht, eine Verbindung zum vertrauenswürdigen Netzwerk herzustellen und verletzt die Snort-Regel.
4. Daher sendet Snort eine Warnung an die pxLog-Anwendung (über Syslog).
5. Die pxLog-Anwendung führt eine Überprüfung anhand ihrer lokalen Datenbank durch. Sie wird so konfiguriert, dass sie Syslog-Meldungen abfängt, die von Snort gesendet wurden, und die IP-Adresse des Angreifers extrahiert. Anschließend wird pxGrid verwendet, um eine

Anfrage an die ISE zu senden, um die IP-Adresse des Angreifers zu isolieren (die ISE ist ein pxGrid-Controller).

6. Die ISE bewertet ihre Autorisierungsrichtlinie neu. Da der Endpunkt unter Quarantäne gestellt wird, wird die Bedingung **Session:EPSSStatus EQUALS Quarantine** erfüllt, und es wird ein anderes Autorisierungsprofil zugeordnet (**Dot1x Quarantine**). Die ISE sendet einen CoA-Abschlussstecker an den Switch, um die Sitzung zu beenden. Dies löst eine erneute Authentifizierung aus, und es wird eine neue herunterladbare ACL (PERMIT_ICMP) angewendet, die den Endbenutzer den eingeschränkten Netzwerkzugriff bereitstellt.
7. In dieser Phase kann der Administrator beschließen, den Endpunkt aus der Quarantäne zu entfernen. Dies kann über die GUI von pxLog erreicht werden. Auch hier wird die pxGrid-Nachricht an die ISE gesendet.
8. Die ISE führt eine ähnliche Operation wie in Schritt 6 durch. Diesmal ist der Endpunkt nicht mehr unter Quarantäne gestellt, und es wird umfassender Zugriff bereitgestellt.

pxLog

Architektur



Die Lösung besteht darin, eine Reihe von Anwendungen auf einem Linux-Computer zu installieren:

1. Die in Java geschriebene und auf dem Tomcat-Server bereitgestellte Anwendung pxLog. Diese Anwendung besteht aus:

Servlet, der Webanfragen verarbeitet - Dieser Dienst wird verwendet, um über den Webbrowser auf die Verwaltungsanzeige zuzugreifen.

Enforcer-Modul - Thread, der zusammen mit Servlet gestartet wird. Der Forcer liest Syslog-Meldungen aus der Datei (optimiert), verarbeitet diese Meldungen gemäß den konfigurierten Regeln und führt Aktionen aus (z. B. Quarantäne über pxGrid).

2. Die MySQL-Datenbank, die die Konfiguration für pxLog enthält (Regeln und Protokolle).

3. Der Syslog-Server, der Syslog-Meldungen von externen Systemen empfängt und in eine Datei schreibt.

Installation

Die pxLog-Anwendung verwendet folgende Bibliotheken:

- jQuery (für AJAX-Unterstützung)
- JavaServer Pages Standard Tag Library (JSTL) (Model View Controller (MVC)-Modell, Daten werden von der Logik getrennt: JavaServer Page (JSP)-Code wird nur für die Wiedergabe verwendet, kein HTML-Code in Java-Klassen.
- Log4j als Protokollierungs-Subsystem
- MySQL-Anschluss
- Anzeigetag für das Rendern/Sortieren von Tabellen
- pxGrid API von Cisco (derzeit Version 147)

Alle diese Bibliotheken befinden sich bereits im lib-Verzeichnis des Projekts, sodass es nicht mehr notwendig ist, Java ARchive (JAR)-Dateien herunterzuladen.

So installieren Sie die Anwendung:

1. Entpacken Sie das gesamte Verzeichnis in das Tomcat Webapp-Verzeichnis.
2. Bearbeiten Sie die **WEB-INF/web.xml**-Datei. Die einzige erforderliche Änderung ist die **serverip**-Variable, die auf die ISE verweisen sollte. Außerdem können Java Certificate KeyStores (eine für vertrauenswürdige und eine für identitätsbasierte Gruppen) generiert werden (anstelle der Standardwerte). Diese wird von der pxGrid-API verwendet, die die SSL-Sitzung (Secure Sockets Layer) sowohl mit den Client- als auch mit den Serverzertifikaten verwendet. Beide Seiten der Kommunikation müssen sich mit dem Zertifikat präsentieren und einander vertrauen. Weitere Informationen finden Sie im Abschnitt mit den Anforderungen des pxGrid-Protokolls.
3. Stellen Sie sicher, dass der ISE-Hostname in pxLog korrekt aufgelöst wird (siehe Eintrag im Domain Name Server (DNS) oder **/etc/hosts Eintrag**). Weitere Informationen finden Sie im Abschnitt mit den Anforderungen des pxGrid-Protokolls.
4. Konfigurieren Sie die MySQL-Datenbank mit dem Skript **mysql/init.sql**. Anmeldeinformationen können geändert werden, sollten sich jedoch in der Datei **WEB-INF/web.xml** wiederfinden.

Snort

Dieser Artikel konzentriert sich nicht auf ein bestimmtes IPS, weshalb nur eine kurze Erläuterung gegeben wird.

Snort wird als Inline mit DAQ-Unterstützung konfiguriert. Datenverkehr wird mit iPables umgeleitet:

```
iptables -I FORWARD -j ACCEPT
```

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

Anschließend wird sie nach der Prüfung eingesteckt und gemäß den standardmäßig gültigen Regeln weitergeleitet.

Es wurden einige benutzerdefinierte Snort-Regeln konfiguriert (die `/etc/snort/rules/test.rules`-Datei ist in der globalen Konfiguration enthalten).

```
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 sendet eine Syslog-Meldung, wenn die Time To Live (TTL) des Pakets 6 oder die Payload zwischen 666 und 686 beträgt. Der Datenverkehr wird nicht von Snort blockiert.

Außerdem sollten Schwellenwerte eingerichtet werden, um sicherzustellen, dass die Warnungen nicht zu oft ausgelöst werden (`/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
```

Anschließend verweist der Syslog-Server auf den pxLog-Computer (`/etc/snort/snort.conf`):

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

Bei einigen Versionen von Snort gibt es Bugs, die sich auf die Syslog-Konfiguration beziehen. Anschließend können die Standardeinstellungen verwendet werden, die auf den localhost und syslog-ng verweisen, um bestimmte Meldungen an den pxLog-Host weiterzuleiten.

ISE

Konfiguration

Personal und Zertifikat

1. Aktivieren Sie die pxGrid-Rolle, die auf der ISE standardmäßig deaktiviert ist, unter **Administration > Deployment**:

Edit Node

General Settings

Profiling Configuration

Hostname **lise**
FQDN **lise.example.com**
IP Address **10.62.97.40**
Node Type **Identity Services Engine (ISE)**

Personas

- Administration Role **STANDALONE**

- Monitoring Role Other Monitoring Node

- Policy Service
 - Enable Session Services ⓘ
 Include Node in Node Group ⓘ

 - Enable Profiling Service

- pxGrid ⓘ

2. Überprüfen Sie, ob die Zertifikate für pxGrid unter **Administration > Certificates > System Certificates** verwendet werden:

Certificate Management

- Overview
- System Certificates**
- Endpoint Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests

Certificate Authority

- Internal CA Settings
- Certificate Templates
- External CA Settings

Edit System Certificate

Issuer

* Friendly Name

Description

Subject CN=Iise.example.com

Issuer win2012

Valid From Tue, 26 Aug 2014 12:32:56 CEST

Valid To (Expiration) Thu, 25 Aug 2016 12:32:56 CEST

Serial Number 7B 00 00 00 3D 4C D6 27 D1 7D BB DF A6 00 00 00 00 00 3D

Signature Algorithm SHA1WITHRSA

Key Length 2048

Usage

- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- Admin: Use certificate to authenticate the ISE Admin Portal
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

Endpoint Protection Service (EPS)

EPS sollte in **Administration > Settings (Administration > Einstellungen)** aktiviert (standardmäßig deaktiviert) werden:

Settings

- Client Provisioning
- Endpoint Protection Service**
- FIPS Mode
- Alarm Settings

Endpoint Protection Service ⓘ

Service Status Enabled ▾

Dadurch können Sie die Quarantäne-/Quarantänefunktion verwenden.

Autorisierungsregeln

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|--------|-------------------|--|------------------|
| ✓ | Dottx Quarantine | if (DEVICE:Device Type EQUALS All Device Types#switch AND Session:EPStatus EQUALS Quarantine) | then Permit_ICMP |
| ✓ | Dottx Full Access | if DEVICE:Device Type EQUALS All Device Types#switch | then Permit_ALL |

Die erste Regel wird nur angetroffen, wenn der Endpunkt unter Quarantäne gestellt wird. Der beschränkte Zugriff wird dann dynamisch vom RADIUS CoA durchgesetzt. Der Switch muss Netzwerkgeräten mit dem richtigen gemeinsamen geheimen Schlüssel hinzugefügt werden.

Fehlerbehebung

Der pxGrid-Status kann mit der CLI überprüft werden:

```
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 |

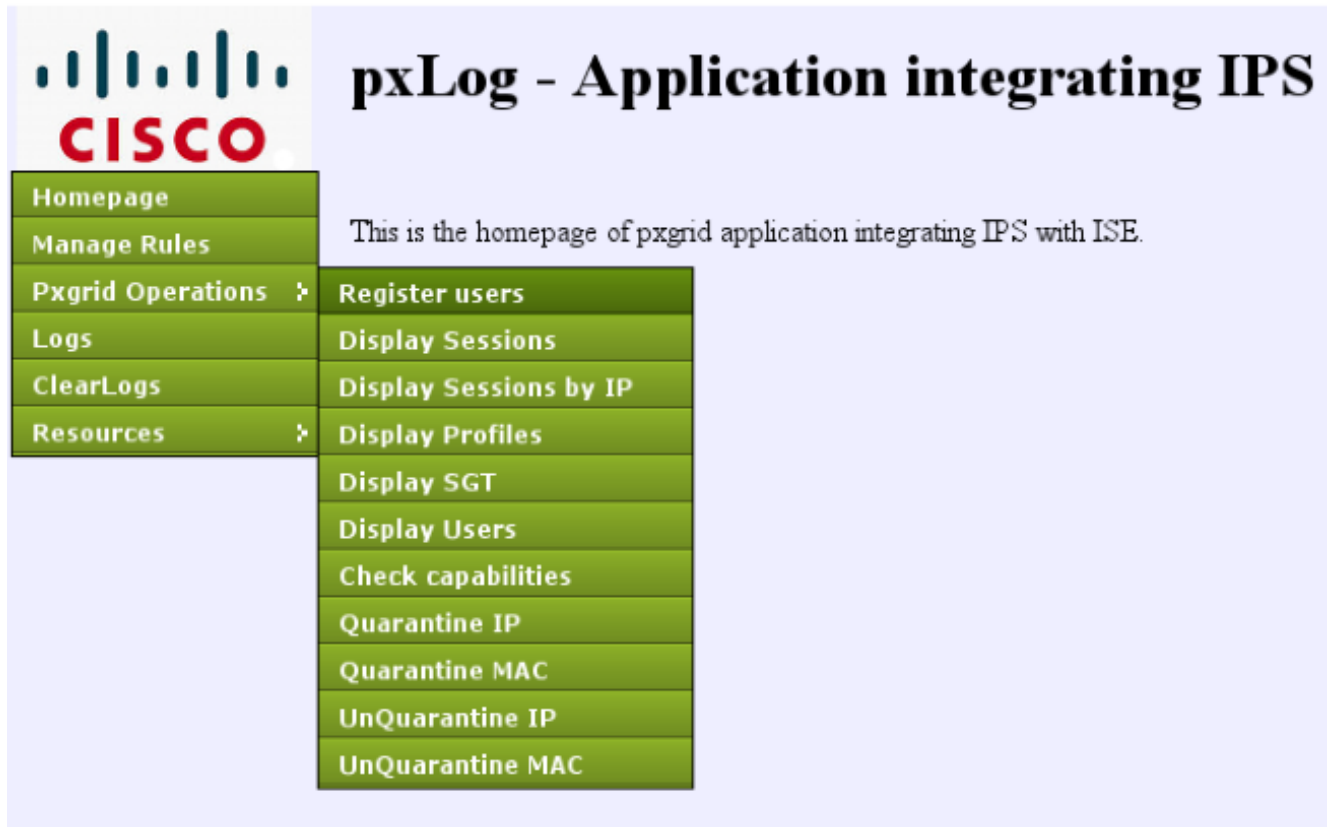
Es gibt auch separate Debuggen für pxGrid (**Administration > Logging > Debug Log Configuration > pxGrid**). Debugdateien werden im pxGrid-Verzeichnis gespeichert. Die wichtigsten Daten sind die `pxgrid/pxgrid-jabberd.log` und die `pxgrid/pxgrid-controller.log`.

Test

Schritt 1: Registrierung für pxGrid

Die pxLog-Anwendung wird beim Start von Tomcat automatisch bereitgestellt.

1. Um pxGrid verwenden zu können, registrieren Sie zwei Benutzer in der ISE (einer mit Sitzungszugriff und einer mit Quarantäne). Dies kann über **Pxgrid Operations > Register users** abgeschlossen werden:



The screenshot shows the pxLog application interface. On the left is a navigation menu with the following items: Homepage, Manage Rules, Pxgrid Operations (with a dropdown arrow), Logs, ClearLogs, and Resources (with a dropdown arrow). The main content area displays the title "pxLog - Application integrating IPS" and a sub-header "This is the homepage of pxgrid application integrating IPS with ISE." Below the sub-header is a list of options: Register users, Display Sessions, Display Sessions by IP, Display Profiles, Display SGT, Display Users, Check capabilities, Quarantine IP, Quarantine MAC, UnQuarantine IP, and UnQuarantine MAC.

Die Registrierung beginnt automatisch:



The screenshot shows the pxLog application interface during the registration process. The navigation menu is the same as in the previous screenshot. The main content area displays the title "pxLog - Application integrating IPS with Cisco ISE" and the following text: "Registration", "The Registration process has started", "Two pxgrid clients are being registered on ISE", "One client with Session privileges (to browse session data) and other with EPS privileges (to execute quarantine)", "Please login to ISE and approve registration by clicking 'Approve'", "Content of the page will be updated automatically every 5 seconds to notify if the users are approved on ISE", "Waiting for the status to be updated...", and "Waiting for the status to be updated..."

2. In dieser Phase müssen registrierte Benutzer auf der ISE genehmigt werden (die automatische Genehmigung ist standardmäßig deaktiviert):

| Client Name | Client Description | Capabilities | Status | Client Group |
|------------------|--------------------|----------------------------|---------|---------------|
| ise-admin-lise | | Capabilities(3 Pub, 1 Sub) | Online | Administrator |
| ise-mnt-lise | | Capabilities(1 Pub, 0 Sub) | Online | Administrator |
| pxclient_session | test | Capabilities(0 Pub, 0 Sub) | Pending | Session |
| pxclient_eps | test | Capabilities(0 Pub, 0 Sub) | Pending | EPS |

Nach der Genehmigung benachrichtigt pxLog den Administrator automatisch (über einen AJAX-Aufruf):

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

Die ISE zeigt den Status dieser beiden Benutzer als Online oder Offline (nicht mehr ausstehend) an.

Schritt 2: Konfiguration der pxLog-Regeln

pxLog muss Syslog-Meldungen verarbeiten und entsprechende Aktionen ausführen. Um eine neue Regel hinzuzufügen, wählen Sie **Regeln verwalten**:

pxLog - Application integrating

Rules for the Enforcer module.
 IPS sending syslog messages, Enforcer receiving and processing.
 When the match against configured rules is found
 Enforcer is automatically executing quarantine via pxgrid

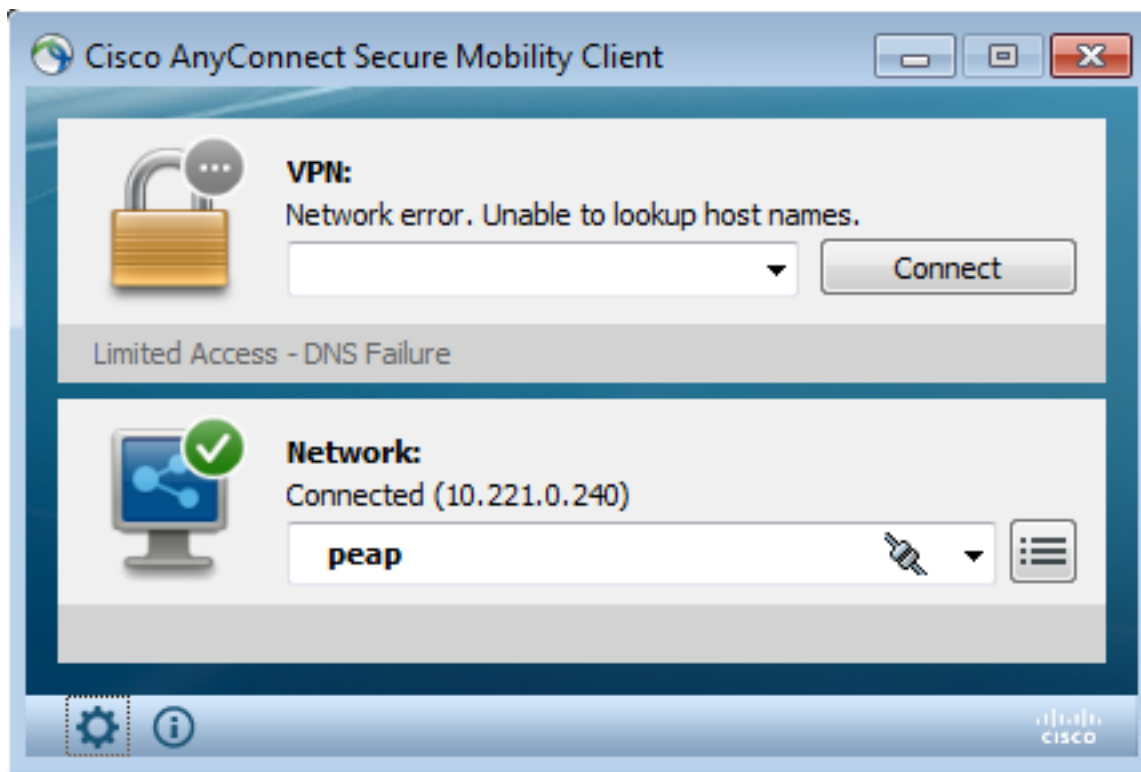
| Rule Id | Rule string | Action |
|----------|----------------------|--------------|
| 19 | snort[| Remove |
| New Rule | <input type="text"/> | Add New Rule |

Das Erzwingermodul sucht nun in der Syslog-Meldung nach diesem regulären Ausdruck (RegExp): "snort[". Wird diese gefunden, werden alle IP-Adressen durchsucht und die vor der letzten Adresse ausgewählte Adresse ausgewählt. Dies entspricht den meisten

Sicherheitslösungen. Weitere Informationen finden Sie im Abschnitt Syslog. Diese IP-Adresse (Angreifer) wird über pxGrid unter Quarantäne gestellt. Es kann auch eine präzisere Regel verwendet werden (z. B. die Signaturnummer).

Schritt 3: Erste Dot1x-Sitzung

Die Microsoft Windows 7-Station initiiert eine Wired dot1x-Sitzung. Cisco AnyConnect NAM wurde als Komponente verwendet. Die Extensible Authentication Protocol-Protected EAP (EAP-PEAP)-Methode wird konfiguriert.



Das ISE **Dot1x Full Access**-Autorisierungsprofil wird ausgewählt. Der Switch lädt die Zugriffsliste herunter, um vollständigen Zugriff zu gewähren:

```
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
```

Schritt 4: Microsoft Windows PC sendet das Paket, das den Alarm auslöst.

Dies zeigt, was passiert, wenn Sie von einem Microsoft Windows-Paket mit TTL = 7 senden:

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

Dieser Wert wird auf Snort in der Weiterleitungskette reduziert, und es wird ein Alarm ausgelöst. Als Ergebnis wird eine Syslog-Meldung an pxLog gesendet:

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

Schritt 5: pxLog

Das pxLog empfängt die Syslog-Meldung, verarbeitet sie und fordert dazu auf, diese IP-Adresse unter Quarantäne zu stellen. Dies kann durch Überprüfen der Protokolle bestätigt werden:

Logs from the actions executed by the Enforcer module

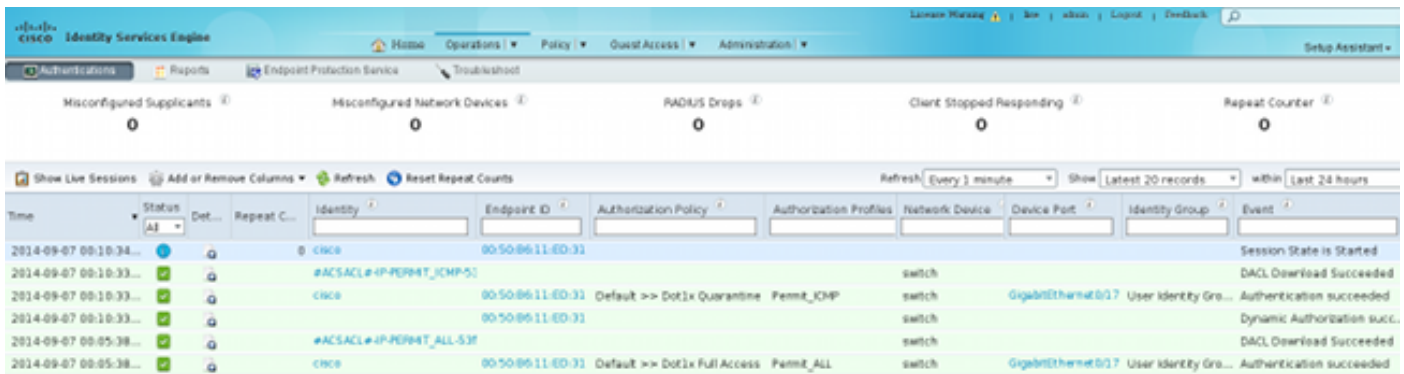
| Id | Type | Action | Syslog message | IP |
|----|--------|------------|---|--------------|
| 66 | SYSLOG | QUARANTINE | Sep 6 22:10:31 snort snort[6310]: [1:100124:0] ALERT {ICMP} 10.221.0.240 -> 10.222.0.61 | 10.221.0.240 |

Schritt 6: ISE-Quarantäne

Die ISE meldet, dass die IP-Adresse unter Quarantäne gestellt wurde:

| Logged At | Endpoint ID | IP Address | Operation | Operation | Operation ID | Audit Session ID |
|-----------------------|-------------------|--------------|------------|-----------|--------------|-----------------------|
| 2014-09-07 00:10:33.0 | 00:50:B6:11:ED:31 | 10.221.0.240 | Quarantine | SUCCESS | 16 | 0A01000C000037E6B8267 |
| 2014-09-07 00:10:32.9 | 00:50:B6:11:ED:31 | 10.221.0.240 | Quarantine | RUNNING | 16 | 0A01000C000037E6B8267 |

Als Ergebnis überprüft sie die Autorisierungsrichtlinie, wählt Quarantäne aus und sendet RADIUS CoA, um den Autorisierungsstatus für diesen bestimmten Endpunkt auf dem Switch zu aktualisieren.



Dies ist die CoA-Abschlussmeldung, die den Supplicant zwingt, eine neue Sitzung zu starten und begrenzten Zugriff zu erhalten (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)

```

Das Ergebnis kann auf dem Switch bestätigt werden (begrenzter Zugriff für den Endpunkt):

```

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
```

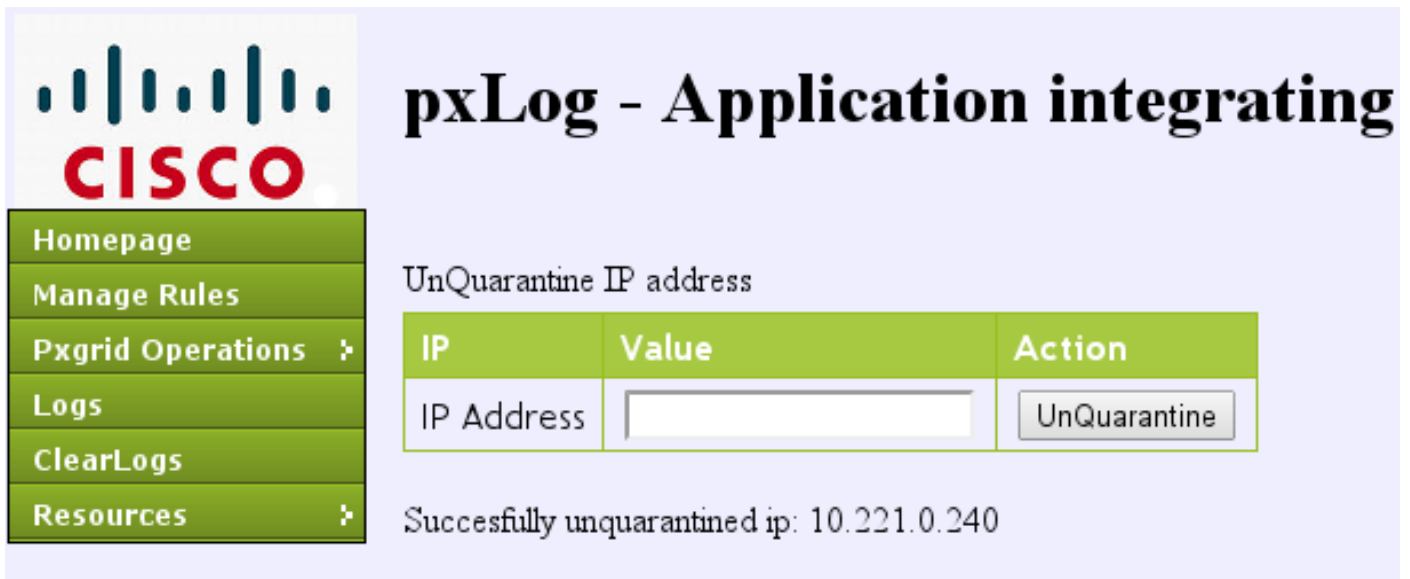
Runnable methods list:

```
Method State
dot1x Authc Success
```

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

Schritt 7: pxLog Unquarantine

In dieser Phase beschließt der Administrator, die Quarantäne für diesen Endpunkt aufzuheben:



The screenshot shows the Cisco pxLog - Application integrating interface. On the left is a navigation menu with the following items: Homepage, Manage Rules, Pxgrid Operations (with a dropdown arrow), Logs, ClearLogs, and Resources (with a dropdown arrow). The main content area has the title "pxLog - Application integrating" and a sub-header "UnQuarantine IP address". Below this is a table with three columns: IP, Value, and Action. The first row contains "IP Address", an empty input field, and a button labeled "UnQuarantine". Below the table, a message states "Successfully unquarantined ip: 10.221.0.240".

| IP | Value | Action |
|------------|----------------------|--------------|
| IP Address | <input type="text"/> | UnQuarantine |

Successfully unquarantined ip: 10.221.0.240

Ein und derselbe Vorgang kann direkt über die ISE ausgeführt werden:

Endpoint Protection Service

Endpoint Operation

* IP Address (Example: 1.2.3.4)
 * MAC Address
 * Operation

Update Information

For a complete list, go to Operations > Reports > Endpoints & Users > Endpoint Protection Service Audit

Last Operation Status

Schritt 8: ISE Unquarantäne.

Die ISE überprüft erneut die Regeln und aktualisiert den Autorisierungsstatus auf dem Switch (vollständiger Netzwerkzugriff wird gewährt):

| Time | Status | Det... | R | Identity | Endpoint ID | Authorization Policy | Authorization Profiles | Network Device | Device Port | Identity Group | Event |
|------------------------|--------|--------|---|--------------------------|-------------------|------------------------------|------------------------|----------------|---------------------|----------------------|---------------------------------|
| 2014-09-07 00:21:11... | | | | osco | 00:50:86:11:ED:31 | | | | | | Session State is Started |
| 2014-09-07 00:21:10... | | | | #ACSACL# IP/PERMIT_ALL-1 | | | | switch | | | DACL Download Succeeded |
| 2014-09-07 00:21:10... | | | | osco | 00:50:86:11:ED:31 | Default => Dat1x Full Access | Permit_ALL | switch | GigabitEthernet0/17 | User Identity Gro... | Authentication succeeded |
| 2014-09-07 00:21:10... | | | | osco | 00:50:86:11:ED:31 | | | switch | | | Dynamic Authorization succeeded |
| 2014-09-07 00:10:33... | | | | #ACSACL# IP/PERMIT_CHP | | | | switch | | | DACL Download Succeeded |
| 2014-09-07 00:10:33... | | | | osco | 00:50:86:11:ED:31 | Default => Dat1x Quarantine | Permit_CHP | switch | GigabitEthernet0/17 | User Identity Gro... | Authentication succeeded |
| 2014-09-07 00:10:33... | | | | osco | 00:50:86:11:ED:31 | | | switch | | | Dynamic Authorization succeeded |
| 2014-09-07 00:05:38... | | | | #ACSACL# IP/PERMIT_ALL-1 | | | | switch | | | DACL Download Succeeded |
| 2014-09-07 00:05:38... | | | | osco | 00:50:86:11:ED:31 | Default => Dat1x Full Access | Permit_ALL | switch | GigabitEthernet0/17 | User Identity Gro... | Authentication succeeded |

Der Bericht bestätigt Folgendes:

The screenshot shows the Cisco ISE Reports interface. The main content area displays the 'Endpoint Protection Service Audit' report for the time range 'Today'. The report includes a table with the following data:

| Logged At | Endpoint ID | IP Address | Operation | Operation | Operation ID | Audit Session ID |
|-------------------------|-------------------|--------------|--------------|-----------|--------------|--------------------------|
| 2014-09-07 00:21:10.342 | 00:50:B6:11:ED:31 | 10.221.0.240 | Unquarantine | SUCCESS | 17 | 0A01000C000037E7B8B7D68C |
| 2014-09-07 00:21:10.309 | 00:50:B6:11:ED:31 | 10.221.0.240 | Unquarantine | RUNNING | 17 | 0A01000C000037E7B8B7D68C |
| 2014-09-07 00:10:33.055 | 00:50:B6:11:ED:31 | 10.221.0.240 | Quarantine | SUCCESS | 16 | 0A01000C000037E6B8E267CF |
| 2014-09-07 00:10:32.973 | 00:50:B6:11:ED:31 | 10.221.0.240 | Quarantine | RUNNING | 16 | 0A01000C000037E6B8E267CF |

pxLog-Funktionalität

Die pxLog-Anwendung wurde geschrieben, um die Funktionalität der pxGrid-API zu demonstrieren. Sie profitieren von folgenden Vorteilen:

- Registrierung von Sitzungen und EPS-Benutzern auf der ISE
- Herunterladen von Informationen zu allen auf der ISE aktiven Sitzungen
- Herunterladen von Informationen zu einer bestimmten aktiven Sitzung auf der ISE (nach IP-Adresse)
- Herunterladen von Informationen zu einem bestimmten aktiven Benutzer auf der ISE (nach Benutzername)
- Anzeigen der Informationen zu allen Profilen (Profiler)
- Anzeigen der Informationen zu den auf der ISE definierten TrustSec Security Group Tags (SGTs)
- Version überprüfen (Funktionen von pxGrid)
- Quarantäne basierend auf der IP- oder MAC-Adresse
- Aufhebung der Quarantäne basierend auf IP- oder MAC-Adresse

Weitere Funktionen sind in Zukunft geplant.

Hier sind einige Beispiel-Screenshots von pxLog:

The screenshot shows the pxLog application interface. The main content area displays the title 'pxLog - Application integrating IPS with' and a table with the following data:

| User | Groups |
|-------|--|
| cisco | User Identity Groups:Employee,User Identity Groups:VPN,Unknown |

The screenshot shows the pxLog application interface. The main content area displays the title 'pxLog - Application integrating IPS with Cisco ISE using pxgrid' and a table with the following data:

| Id | User | Domain | MAC | State | ESPStatus | SGT | Profile | NAS IP | NAS Port | AVP |
|----|-------|--------|-------------------|---------|-----------|-----|---------|--------------|---------------------|--------------------------|
| 0 | cisco | | 00:50:B6:11:ED:31 | Started | | | Unknown | 10.62.71.140 | GigabitEthernet0/17 | Acct-Session-Id 00003A72 |



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

Display session by IP address

| IP | Value | Action |
|------------|---|--|
| IP Address | <input type="text" value="10.221.0.240"/> | <input type="button" value="Display"/> |

List of the sessions found by IP

| Id | User | Domain | MAC | State | ESPStatus | SGT | Profile | NAS IP | NAS Port | AVP |
|----|-------|--------|-------------------|---------|-----------|-----|---------|--------------|---------------------|--------------------------|
| 0 | cisco | | 00:50:B6:11:ED:31 | Started | | | Unknown | 10.62.71.140 | GigabitEthernet0/17 | Acct-Session-Id 00003A72 |



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

List of SGT tags downloaded from ISE via pxgrid

| Id | SGT Name | SGT Description | SGT number |
|--------------------------------------|-------------|--|------------|
| a14bc9f0-3597-11e4-81d2-0050569c3ff3 | Marketing | | 3 |
| 0c2ca0f0-3598-11e4-81d2-0050569c3ff3 | Quarantined | Users violating policies, limited access | 2 |
| 9c903db0-3597-11e4-81d2-0050569c3ff3 | IT | | 2 |
| 173025d0-3598-11e4-81d2-0050569c3ff3 | Development | | 6 |
| 06ce9320-3598-11e4-81d2-0050569c3ff3 | VPN | Anyconnect Ikev2 sessions | 2 |
| d006f0b0-2c02-11e4-907b-005056bf2f0a | ANY | Any Security Group | 65535 |
| cff3b6d0-2c02-11e4-907b-005056bf2f0a | Unknown | Unknown Security Group | 0 |
| 1c6527d0-3598-11e4-81d2-0050569c3ff3 | Finance | Only for audits | 2 |



pxLog - Application integrating IPS with Cisco ISE using pxgrid

- Homepage
- Manage Rules
- Pxgrid Operations >
- Logs
- ClearLogs
- Resources >

List of the profile download from ISE via pxgrid

| Profile Id | Profile Name | Full Profile Name |
|--------------------------------------|--------------------------|---|
| 0e4d9640-2c02-11e4-907b-005056bf2f0a | Xerox-WorkCentre-5020-dn | Xerox-Device:Xerox-WorkCentre-5020-dn |
| 1657b140-2c02-11e4-907b-005056bf2f0a | Cisco-AP-Aironet-1240 | Cisco-Device:Cisco-Access-Point:Cisco-AP-Aironet-1240 |
| 0a3e9db0-2c02-11e4-907b-005056bf2f0a | Xerox-Phaser-6140dn | Xerox-Device:Xerox-Phaser-6140dn |
| 1f4e0100-2c02-11e4-907b-005056bf2f0a | VMWare-Device | VMWare-Device |
| ff876410-2c01-11e4-907b-005056bf2f0a | Cisco-WLC | Cisco-Device:Cisco-WLC |
| 0d40e130-2c02-11e4-907b-005056bf2f0a | Xerox-Phaser-8860mfp | Xerox-Device:Xerox-Phaser-8860mfp |
| 0bd6a2d0-2c02-11e4-907b-005056bf2f0a | Xerox-Phaser-7500dx | Xerox-Device:Xerox-Phaser-7500dx |
| 21e43c40-2c02-11e4-907b-005056bf2f0a | Philips-Intellivue | Philips-Device:Philips-Intellivue |
| 15d7f9f0-2c02-11e4-907b-005056bf2f0a | DLink-DAP-1522 | DLink-Device:DLink-DAP-1522 |
| 0eb5f500-2c02-11e4-907b-005056bf2f0a | Xerox-WorkCentre-5225 | Xerox-Device:Xerox-WorkCentre-5225 |

Anforderungen an das pxGrid-Protokoll

Gruppen

Der Client (Benutzer) kann gleichzeitig Mitglied einer Gruppe sein. Die beiden am häufigsten verwendeten Gruppen sind:

- Sitzung - Dient zum Durchsuchen/Herunterladen von Informationen zu Sitzungen/Profilen/SGTs.
- EPS - Wird zur Ausführung der Quarantäne verwendet

Zertifikate und Java KeyStore

Wie bereits erwähnt, müssen für die Kommunikation bei beiden Clientanwendungen, pxLog und pxGrid Controller (ISE), Zertifikate konfiguriert sein. Die pxLog-Anwendung speichert diese in den Java KeyStore-Dateien:

- **store/client.jks** - Enthält die Zertifikate des Clients und der Zertifizierungsstelle (Certificate Authority, CA)
- **store/root.jks** - Umfasst die ISE-Kette: MnT-Identität (Monitoring and Troubleshooting Node) und Zertifizierungsstellen-Zertifikat

Dateien sind kennwortgeschützt (Standard: cisco123). Dateipfad und Kennwörter können unter **WEB-INF/web.xml** geändert werden.

So erstellen Sie einen neuen Java KeyStore:

1. Um einen Stamm-Keystore (vertrauenswürdigen) zu erstellen, importieren Sie das Zertifizierungsstellenzertifikat (**cert-ca.der** sollte im DER-Format vorliegen):

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

2. Wenn Sie einen neuen Keystore erstellen, wählen Sie ein Kennwort aus, das später verwendet wird, um auf den Keystore zuzugreifen.

3. Importieren Sie das MnT-Identitätszertifikat in den Stamm-Keystore (**cert-mnt.der** ist das Identitätszertifikat der ISE und sollte im DER-Format vorliegen):

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

4. Um den Client-Keystore zu erstellen, importieren Sie das Zertifizierungsstellenzertifikat:

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

5. Erstellen Sie einen privaten Schlüssel im Clientschlüssel:

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

6. Erstellen einer CSR-Anfrage (Certificate Signing Request) im Clientschlüssel:

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

7. Signieren Sie **cert-client.csr**, und importieren Sie das signierte Clientzertifikat:

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

8. Stellen Sie sicher, dass beide Tastenanschläge die richtigen Zertifikate enthalten:

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

Vorsicht: Wenn der ISE 1.3-Knoten aktualisiert wird, besteht die Möglichkeit, das Identitätszertifikat beizubehalten. Die CA-Signierung wird jedoch entfernt. Daher verwendet die aktualisierte ISE ein neues Zertifikat, fügt das Zertifizierungsstellenzertifikat jedoch nie in die SSL/ServerHello-Nachricht ein. Dies löst den Ausfall auf dem Client aus, der (gemäß RFC) eine vollständige Kette erwartet.

Hostname

Die pxGrid-API für mehrere Funktionen (z. B. Sitzungs-Download) führt eine zusätzliche Validierung durch. Der Client kontaktiert die ISE und empfängt den ISE-Hostnamen, der durch den Befehl `hostname` in der CLI definiert wird. Anschließend versucht der Client, die DNS-Auflösung für diesen Hostnamen auszuführen und versucht, Daten aus dieser IP-Adresse zu kontaktieren und abzurufen. Wenn die DNS-Auflösung für den ISE-Hostnamen fehlschlägt, versucht der Client nicht, Daten abzurufen.

Vorsicht: Beachten Sie, dass für diese Auflösung nur der Hostname verwendet wird, was in diesem Szenario **auch** der **ist**, nicht der vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN), der in diesem Szenario **lise.example.com** ist.

Hinweis für Entwickler

Cisco veröffentlicht und unterstützt die pxGrid-API. Es gibt ein Paket mit dem Namen:

```
pxgrid-sdk-1.0.0-167
```

Im Inneren gibt es:

- pxGrid JAR-Dateien mit Klassen, die einfach in Java-Dateien decodiert werden können, um den Code zu überprüfen
- Beispiel für Java KeyStores mit Zertifikaten
- Beispielskripts, die Beispiel-Java-Klassen verwenden, die pxGrid verwenden

Syslog

Im Folgenden finden Sie eine Liste von Sicherheitslösungen, die Syslog-Meldungen mit der IP-Adresse des Angreifers senden. Diese können problemlos in pxLog integriert werden, solange Sie die richtige RegExp-Regel in der Konfiguration verwenden.

Snort

Snort sendet Syslog-Warnungen in diesem Format:

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

Hier ein Beispiel:

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

Die IP-Adresse des Angreifers ist immer die zweite vor der letzten (Ziel). Es ist einfach, eine granulare RegExp für eine bestimmte Signatur zu erstellen und die IP-Adresse des Angreifers zu extrahieren. Hier sehen Sie ein Beispiel für RegExp für die Signatur 100124 und die Meldung Internet Control Message Protocol (ICMP):

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

Cisco Adaptive Security Appliance (ASA)-Inspektion

Wenn die ASA für die HTTP-Überprüfung (z. B.) konfiguriert ist, sieht die entsprechende Syslog-Meldung wie folgt aus:

```
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
```

Auch hier könnte eine granulare RegExp verwendet werden, um diese Nachrichten zu filtern und die IP-Adresse des Angreifers zu extrahieren, die zweite vor der letzten.

Cisco Sourcefire Next-Generation Intrusion Prevention-Systeme (NGIPS)

Hier eine Beispielmeldung, die vom Sourcefire-Sensor gesendet wird:

```
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
```

Auch hier ist es einfach, die IP-Adresse des Angreifers zu extrahieren, da dieselbe Logik gilt. Außerdem werden der Richtlinienname und die Signatur bereitgestellt, sodass die pxLog-Regel granular sein kann.

Juniper NetScreen

Hier sehen Sie eine Beispielnachricht, die von Juniper Intrusion Detection & Prevention (IDP) gesendet wurde:

```
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" elapsedTime="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"
```

Die IP-Adresse des Angreifers kann auf die gleiche Weise extrahiert werden.

Juniper JunOS

JunOS ist ähnlich:

```
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-IPs

Hier sind einige Beispiele für Linux iptables.

```
Jun 15 23:37:33 netfilter kernel: Inbound IN=lo OUT=
MAC=00:13:d3:38:b6:e4:00:01:5c:22:9b:c2:08:00 src=10.0.0.1 DST=10.0.0.100 LEN=60
TOS=0x10 PREC=0x00 TTL=64 ID=47312 DF PROTO=TCP SPT=40945 DPT=3003 WINDOW=32767
RES=0x00 SYN URGP=0
```

Sie können Syslog-Informationen für jeden Pakettyp mit den erweiterten Funktionen der iptable-Module wie z. B. Verbindungsverfolgung, xtables, rpfilter, Musterabgleich usw. senden.

FreeBSD IPFW (IPFW)

Hier ist eine Beispielmeldung für IPFW-Blockierungsfragmente:

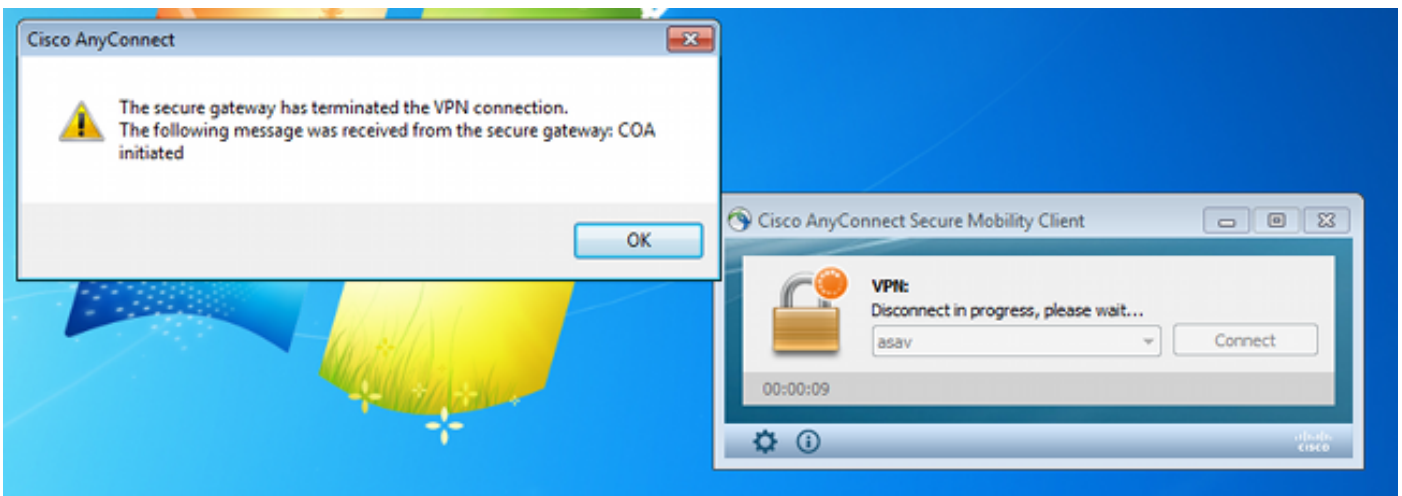
```
Sep 7 15:03:14 delta ipfw: 11400 Deny UDP 10.61.216.50 10.81.199.2 in via fxp0
(frag 52639:519@1480)
```

VPN-Bereitschaft und CoA-Verarbeitung

Die ISE kann die Art der Sitzungen hinsichtlich der CoA-Verarbeitung erkennen.

- Bei einem kabelgebundenen 802.1x/MAC Authentication Bypass (MAB) sendet die ISE die CoA-Neuauthentifizierung, die eine zweite Authentifizierung auslöst.
- Bei einem Wireless-802.1x/MAB sendet die ISE das CoA-Abschlusszertifikat, das eine zweite Authentifizierung auslöst.
- Bei einem ASA VPN sendet die ISE ein CoA mit einer neuen DACL (keine zweite Authentifizierung).

Das EPS-Modul ist einfach. Wenn eine Quarantäne ausgeführt wird, wird immer ein CoA-Terminierungspaket gesendet. Bei kabelgebundenen/Wireless-Sitzungen ist dies kein Problem (alle 802.1x-Komponenten können transparent eine zweite EAP-Sitzung starten). Wenn die ASA das CoA-Abschlussdatum erhält, verwirft sie die VPN-Sitzung und dem Endbenutzer wird Folgendes angezeigt:



Es gibt zwei Möglichkeiten, das AnyConnect VPN zu zwingen, automatisch eine Verbindung herzustellen (konfiguriert im XML-Profil):

- AutoConnect funktioniert nur, wenn die Verbindung zum VPN-Gateway unterbrochen wird, nicht, wenn die Verbindung durch den Administrator beendet wird.
- Stets verfügbar, was funktioniert und AnyConnect dazu zwingt, die Sitzung automatisch wiederherzustellen

Selbst wenn die neue Sitzung eingerichtet ist, wählt die ASA die neue Audit-Session-ID. Aus der ISE-Sicht ist dies eine neue Sitzung, und es besteht keine Möglichkeit, auf die Quarantäneregeln zu stoßen. Auch für die VPNs ist es nicht möglich, die MAC-Adresse des Endpunkts als Identität anstelle des kabelgebundenen/Wireless dot1x zu verwenden.

Die Lösung besteht darin, das EPS zu zwingen, sich wie die ISE zu verhalten, und den richtigen CoA-Typ basierend auf der Sitzung zu senden. Diese Funktion wird in ISE Version 1.3.1 eingeführt.

pxGrid-Partner und -Lösungen

Hier finden Sie eine Liste der pxGrid-Partner und -Lösungen:

- LogRhythm (Security Information and Event Management (SIEM)) - Unterstützt die REST-API

(Representational State Transfer)

- Splunk (SIEM) - Unterstützt die REST-API
- HP Arcsight (SIEM) - Unterstützt REST-API
- Sentinel NetIQ (SIEM) - Pläne zur Unterstützung von pxGrid
- Lancope StealthWatch (SIEM) - Pläne zur Unterstützung von pxGrid
- Cisco Sourcefire - Pläne zur Unterstützung von pxGrid, 1. Halbjahr 2015
- Cisco Web Security Appliance (WSA) - Geplante Unterstützung für pxGrid im April 2014

Hier finden Sie weitere Partner und Lösungen:

- Tenable (Schwachstellenbewertung)
- Emulex (Paketerfassung und Forensik)
- Bayshore Networks (Data Loss Prevention, DLP) und Internet of Things (IoT)
- Ping-Identität (Identity and Access Management (IAM)/Single Sign On (SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (SIEM AMD Mobile Device Management (MDM))

Eine vollständige Liste aller Sicherheitslösungen finden Sie im [Marketplace-Lösungskatalog](#).

ISE-APIs: REST vs. EREST vs. pxGrid

ISE Version 1.3 bietet drei Arten von APIs.

Hier ein Vergleich:

| | ZURÜCKSETZEN | Externer RESTful | pxGrid |
|---------------------------------------|---|--|--------------------|
| Client-Authentifizierung | Benutzername + Kennwort (einfache HTTP- Authentifizierung) | Benutzername + Kennwort (einfache HTTP- Authentifizierung) | Zertifikat |
| Privilegienseparierung Zugriff | Nein MnT | begrenzt (ERS-Administrator) MnT | Ja (Grup MnT |
| Transport | tcp/443 (HTTPS) | tcp/9060 (HTTPS) | tcp/5222 (XMPP) |
| HTTP-Methode | ERHALTEN | GET/POST/PUT | GET/PO |
| Standardmäßig aktiviert | Ja | Nein | Nein |
| Anzahl der Vorgänge | Wenig | viele | Wenig |
| CoA-Terminierung | unterstützt | Nein | unterstüt |
| CoA-Reauthentifizierung | unterstützt | Nein | unterstüt |
| Benutzervorgänge | Nein | Ja | Nein |
| Endpunkterstellung | Nein | Ja | Nein |
| Endpunkt-Identitätsgruppenoperationen | Nein | Ja | Nein |
| Quarantäne (IP, MAC) | Nein | Nein | Ja |
| UnQuarantine (IP, MAC) | Nein | Nein | Ja |
| PortBounce/Herunterfahren | Nein | Nein | Ja |
| Gastbenutzerbetrieb | Nein | Ja | Nein |
| Gastportal-Betrieb | Nein | Ja | Nein |
| Betrieb von Netzwerkgeräten | Nein | Ja | Nein |
| Netzwerkgerätegruppenbetrieb | Nein | Ja | Nein |

* Quarantäne verwendet Unified CoA-Unterstützung von ISE Version 1.3.1.

Downloads

pxLog kann von [Sourceforge](#) heruntergeladen werden.

Das Software Development Kit (SDK) ist bereits enthalten. Die aktuellste SDK- und API-Dokumentation für pxGrid erhalten Sie von Ihrem Partner oder vom Cisco Account Team.

Zugehörige Informationen

- [Cisco ISE 1.2 REST-API](#)
- [Cisco ISE 1.2 Externe RESTful-API](#)
- [Cisco ISE 1.3 Administratorhandbuch](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)