Версия 1.3 ISE pxGrid Интеграция с IPS pxLog Приложение

Содержание

Введение

Версия 1.3 платформы Identity Services Engine (ISE) поддерживает новый API, названный pxGrid. Этот современный и гибкий протокол, который поддерживает аутентификацию, шифрование и привилегии (группы), обеспечивает простую интеграцию с другими решениями по обеспечению безопасности. Этот документ описывает использование pxLog приложения, которое было записано как подтверждение концепции. pxLog в состоянии получить сообщения системного журнала от Системы предотвращения вторжений (IPS) и передать сообщения pxGrid к ISE для изоляции атакующего. В результате ISE использует изменение авторизации RADIUS (CoA) для изменения статуса авторизации оконечной точки, которая ограничивает доступ к сети. Все это происходит прозрачно конечному пользователю.

Для данного примера Фырканье использовалось в качестве IPS, но могло использоваться любое другое решение. Фактически это не должен быть IPS. Все, что требуется, должно передать сообщение системного журнала к pxLog с IP-адресом атакующего. Это создает возможность для интеграции большого числа решений.

Этот документ также представляет, как устранить неполадки и протестировать pxGrid решения с типичными проблемами и ограничениями.

Правовая оговорка: pxLog приложение не поддерживается Cisco. Эта статья была написана как подтверждение концепции. Первичная цель должна была использовать его во время проведения бета-тестирование pxGrid реализации на ISE.

Предварительные условия

Требования

Cisco рекомендует иметь опыт с конфигурацией Cisco ISE и базовыми знаниями об этих темах:

- Развертывания ISE и Конфигурация авторизации
- Конфигурация интерфейса командой строки коммутаторов Cisco Catalyst

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Microsoft Windows 7
- Cisco Catalyst программное обеспечение коммутатора серии 3750X, версии 15.0 и позже
- Программное обеспечение Cisco ISE, версии 1.3 и позже
- Cisco AnyConnect Mobile Security с Network Access Manager (NAM) версии 3.1 или более поздней версии
- Версия 2.9.6 фырканья со сбором данных (DAQ)
- Приложение pxLog, установленное на Tomcat 7 с Версией 5 MySQL

Диаграмма сети и поток трафика

Вот трафик, как проиллюстрировано в схеме сети:

1. Microsoft Windows 7 пользовательских подключений к коммутатору и выполняет аутентификацию 802.1x.

2. Коммутатор использует ISE в качестве аутентификации, авторизации и учета (AAA). С правилом авторизации **Полного доступа Dot1x** совпадают, и полный доступ к сети предоставляют (DACL: PERMIT_ALL).

3. Пользователь пытается соединиться с надежной сетью и нарушает правило Фырканья.

4. В результате Фырканье передает предупреждение к pxLog приложению (через системный журнал).

5. pxLog приложение выполняет проверку против своей локальной базы данных. Это настроено, чтобы поймать сообщения системного журнала, передаваемые Фырканьем, и извлечь IP-адрес атакующего. Затем это использует pxGrid для отправления запроса к ISE для изоляции IP-адреса атакующего (ISE является pxGrid контроллером).

6. ISE переоценивает свою политику авторизации. Поскольку оконечная точка изолирована, **Карантинное** условие **EQUALS Session:EPSStatus** соблюдают, и с другим профилем авторизации совпадают (**Карантин Dot1x**). ISE передает CoA, Оконечный к коммутатору для завершения сеанса. Это инициирует повторную проверку подлинности, и новый Загружаемый список ACL (DACL) (PERMIT_ICMP) применен, который предоставляет ограниченный доступ к сети конечному пользователю.

7. На данном этапе администратор мог бы решить не изолировать оконечную точку. Это может быть достигнуто через GUI pxLog. Снова, сообщение pxGrid к ISE передается.

8. ISE выполняет подобную операцию как в Шаге 6. На этот раз оконечная точка больше не изолируется, и полный доступ предоставлен.

pxLog

Архитектура

Решение состоит в том, чтобы установить ряд приложений на машине Linux:

1. pxLog приложение, записанное в Java и развернутое на сервере Tomcat. То приложение состоит из:

   Servlet, который обрабатывает веб-запросы - Это используется для доступа к административной панели через web-браузер.

   Модуль средства обеспечения выполнения - Поток, который запущен вместе с servlet. Сообщения системного журнала чтений Средства обеспечения выполнения от (оптимизированного) файла, обрабатывают те сообщения согласно настроенным правилам и выполняют действия (как карантин через pxGrid).

2. База данных MySQL, которая содержит конфигурацию для pxLog (правила и журналы).

3. Сервер системного журнала, который получает сообщения системного журнала от внешних систем и пишет их в файл.

Установка

pxLog приложение пользуется этими библиотеками:

- jQuery (для поддержки Ajax)
- Библиотека тегов Стандарта Страниц JavaServer (JSTL) (модель Контроллера представления модели (MVC), данные разделены от логики: Страница JavaServer (JSP) код используется для рендеринга только, никакой код HTML в Классах Java),
- Log4j как подсистема регистрации
- Разъём MySQL
- displaytag для рендеринга/сортировки таблиц
- pxGrid API Cisco (в настоящее время альфа Версии 147)

Все те библиотеки уже находятся в каталоге библиотеки проекта, таким образом, нет никакой потребности больше загружать Java Archive (JAR) файлы.

Для устанавливания приложения:

1. Распакуйте целый каталог к каталогу Tomcat Webapp.

2. Отредактируйте файл **WEB-INF/web.xml**. Единственное необходимое изменение является **serverip** переменной, которая должна указать к ISE. Также Сертификат Java KeyStores (один для доверяемого и один для идентичности) мог бы генерироваться (вместо по умолчанию). Это используется pxGrid API, который использует сеанс Уровня защищенных сокетов (SSL) с обоими сертификаты клиента и сервера. Обе стороны связи должны предоставить сертификат и должны доверять друг другу. См. pxGrid Требования к протоколу разделяют для получения дополнительной информации.

3. Удостоверьтесь, что имя хоста ISE решено правильно на pxLog (обратитесь к записи в Сервере доменных имен (DNS) или**/etc/hosts записи**). См. pxGrid Требования к протоколу разделяют для получения дополнительной информации.

4. Настройте базу данных MySQL с **mysql/init.sql** сценарием. Учетные данные могут быть изменены, но должны быть отражены в файле **WEB-INF/web.xml**.

Фырканье

Эта статья не фокусируется ни на каком определенном IPS, который является, почему предоставлено только краткое объяснение.

Фырканье настроено как встроенное с поддержкой DAQ. Трафик перенаправлен с iptables:

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

Затем после контроля это введено и передано согласно iptable правилам по умолчанию.

Несколько пользовательских правил Фырканья были настроены (**/etc/snort/rules/test.rules** файл включен в глобальную конфигурацию).

```
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)
```

Фырканье передает сообщение системного журнала, когда Время жизни (TTL) пакета равно 6, или размер информационного наполнения между 666 и 686. Трафик не заблокирован Фырканьем.

Также пороги должны быть установлены, чтобы удостовериться, что предупреждения не инициируются слишком часто **(/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
```

Затем сервер системного журнала указывает к pxLog машине **(/etc/snort/snort.conf)**:

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

Для некоторых версий Фырканья существуют дефекты, отнесенные к конфигурации системного журнала, и затем настройки по умолчанию могли использоваться, что точка к локальному узлу и нанограмму системного журнала могла быть настроена для передачи определенных сообщений к хосту pxLog.

ISE

!--- конфигурацию

Персона и сертификат

1. Включите pxGrid роль, которая отключена на ISE по умолчанию при

администрировании> Развертывания:

2. Проверьте, используются ли сертификаты для pxGrid при **администрировании> Сертификаты> Системные Сертификаты**:

Служба защиты оконечной точки (EPS)

EPS должен быть включен (отключенный по умолчанию) от **администрирования> Параметры настройки**:

Это позволяет вам использовать функциональность карантина/некарантина.

Правила авторизации

С первым правилом встречаются только, когда изолирована оконечная точка. Затем ограниченный доступ динамично принужден RADIUS CoA. Коммутатор также должен быть добавлен к Сетевым устройствам с корректным общим секретным ключом.

Устранение неполадок

pxGrid статус может быть проверен с CLI:

```
lise/admin# show application status ise

ISE PROCESS NAME                       STATE           PROCESS ID
--------------------------------------------------------------------
Database Listener                      running         6717
Database Server                        running         51 PROCESSES
Application Server                     running         9486
Profiler Database                      running         7804
AD Connector                           running         10058
M&T Session Database                   running         7718
M&T Log Collector                      running         9752
M&T Log Processor                      running         9712
Certificate Authority Service          running         9663
pxGrid Infrastructure Service          running         14979
pxGrid Publisher Subscriber Service    running         15281
pxGrid Connection Manager              running         15248
pxGrid Controller                      running         15089
Identity Mapping Service               running         9962
```

Существуют также отдельные отладки для pxGrid (**администрирование> Регистрация> Конфигурация Журнала Отладки> pxGrid**). Файлы отладки хранятся в pxGrid каталоге. Самые важные данные находятся в **pxgrid/pxgrid-jabberd.log** и **pxgrid/pxgrid-controller.log**.

Тест

Шаг 1. Регистрация для pxGrid

Когда Tomcat запускается, pxLog приложение автоматически развернуто.

1. Для использования pxGrid зарегистрируйте двух пользователей в ISE (один с доступом в сеансе, и один с карантином). Это может быть завершено от **Операций Pxgrid> пользователи Регистра**:

   Регистрация запускается автоматически:

2. На данном этапе необходимо утвердить зарегистрированных пользователей на ISE (автоматическое утверждение отключено по умолчанию):

   После утверждения, pxLog автоматически уведомляет администратора (через вызов Ajax):

   ISE показывает статус для тех двух пользователей как Онлайн или Оффлайн (Не ожидающий больше).

Конфигурация Правил Шаг 2. pxLog

pxLog должен обработать сообщения системного журнала и выполнить действия на основе его. Для добавления нового правила выберите **Manage Rules**:

Теперь модуль средства обеспечения выполнения ищет это Регулярное выражение (RegExp) в сообщении системного журнала: "фырканье [". Если найдено, это ищет все IP-адреса и выбирает тот перед последним. Это совпадает с большинством решений по обеспечению безопасности. См. Системный журнал разделяют для получения дополнительной информации. Тот IP-адрес (атакующий) изолирован через pxGrid. Также более гранулированное правило могло бы использоваться (например, оно могло бы включать номер подписи).

Шаг 3. Первый сеанс Dot1x

Microsoft Windows 7 станций инициирует проводной сеанс dot1x. NAM Cisco Anyconnect использовался в качестве соискателя. Защищенный от расширяемого протокола аутентификации EAP (PEAP EAP) метод настроен.

Профиль авторизации **Полного доступа Dot1x** ISE выбран. Коммутатор загружает список доступа для предоставления полного доступа:

```
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
```

Шаг 4. . Microsoft Windows PC Передает Пакет который Триггеры Сигнал тревоги

Это показывает то, что происходит, если вы действительно передаете от пакета Microsoft Windows c TTL = 7:

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

То значение постепенно уменьшено на Фырканье в Передающей цепочке, и аварийный сигнал выдан. В результате сообщение системного журнала к pxLog передается:

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

Шаг 5. . pxLog

pxLog получает сообщение системного журнала, обрабатывает его и запрашивает изолировать тот IP-адрес. Это может быть подтверждено при проверке журналов:

Шаг 6. Карантин ISE

ISE сообщает, что был изолирован IP-адрес:

В результате это рассматривает политику авторизации, выбирает карантин и передает RADIUS CoA для обновления статуса авторизации на коммутаторе для той определенной оконечной точки.

Это - CoA оконечное сообщение, которое вынуждает соискателя инициировать новый сеанс и получить ограниченный доступ (Permit_ICMP):

Результат может быть подтвержден на коммутаторе (ограниченный доступ для оконечной точки):

```
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
```

Некарантин Шаг 7. pxLog

На данном этапе администратор решает не изолировать ту оконечную точку:

Та же операция может быть выполнена непосредственно от ISE:

Шаг 8. Некарантин ISE

ISE снова рассматривает правила и обновляет статус авторизации на коммутаторе (полный доступ к сети предоставляют):

Отчёт подтверждает:

Функциональность pxLog

pxLog приложение было записано для демонстрации функциональности pxGrid API. Это позволяет вам:

- Сеанс регистра и пользователи EPS на ISE
- Информация о загрузке обо всех сеансах, активных на ISE
- Информация о загрузке об определенном активном сеансе на ISE (IP-адресом)
- Информация о загрузке об определенном активном пользователе на ISE (именем пользователя)

- Отобразите информацию обо всех профилях (профилировщик)
- Отобразите информацию о Метках Группы безопасности TrustSec (SGTs), определенный на ISE
- Проверьте версию (возможности pxGrid)
- Карантин на основе IP или MAC-адреса
- Некарантин на основе IP или MAC-адреса

Большая функциональность запланирована в будущем.

Вот некоторые снимки экрана в качестве примера от pxLog:

Требования к протоколу pxGrid

Группы

Клиент (пользователь) может быть участником одной группы за один раз. Две обычно используемых группы:

- Сеанс - Используемый для просмотра информации о sessions/profiles/SGTs
- EPS - Используемый для выполнения карантина

Сертификаты и Java KeyStore

Как упомянуто ранее, обоим клиентским приложениям, pxLog и pxGrid контроллеру (ISE), нужно было настроить сертификаты для передачи. pxLog приложение поддерживает тех в файлах Java KeyStore:

- **store/client.jks** - Включает клиента и сертификаты Центра сертификации (CA)
- **store/root.jks** - Включает цепочку ISE: Мониторинг и Устранение проблем Узла (MnT) идентичность и сертификат CA

Файлы защищены паролем (по умолчанию: cisco123). Расположение файла и пароли могут быть изменены в **WEB-INF/web.xml**.

Вот шаги для генерации нового Java KeyStore:

1. Для создания keystore root которому (доверяют) импортируйте сертификат CA (**свидетельство-ca.der** должно быть в формате DER):

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

2. Когда вы создаете новый keystore, выбираете пароль, который используется позже для доступа к keystore.

3. Импортируйте сертификат идентификации MnT к root keystore (**свидетельство-mnt.der** является сертификатом идентификации, взятым от ISE, и должно быть в формате DER):

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

4. Для создания клиентского keystore импортируйте сертификат CA:

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

5. Создайте секретный ключ в клиентском keystore:

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

6. Генерируйте Запрос подписи сертификата (CSR) в клиентском keystore:

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

7. Подпишите **свидетельство-client.csr** и импортируйте сертификат клиента со знаком:

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

8. Проверьте, что оба keystores содержат корректные сертификаты:

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

Внимание. : Когда узел ISE 1.3 обновлен, существует опция для хранения сертификата идентификации, но удалено CA подписание. В результате обновленный ISE использует новый сертификат, но никогда не подключает сертификат CA в сообщении SSL/ServerHello. Это инициирует сбой на клиенте, который ожидает (согласно RFC) видеть полную цепочку.

Host name

pxGrid API для нескольких функций (как загрузка сеанса) выполняет дополнительную проверку. Клиент связывается с ISE и получает имя хоста ISE, которое определено командой hostname в CLI. Затем клиент пытается выполнить Разрешение DNS для того имени хоста и попыток связаться и выбрать данные от того IP-адреса. Если Разрешение DNS для сбоев имени хоста ISE, клиент не пытается получить какие-либо данные.

Внимание. : Заметьте, что только имя хоста используется для этого разрешения, которое является **lise** в этом сценарии, не Полным доменным именем (FQDN), которое является **lise. пример. com** в этом сценарии.

Обратите внимание для разработчиков

Cisco публикует и поддерживает pxGrid API. Существует один пакет, названный как это:

pxgrid-sdk-1.0.0-167

Внутри существуют:

- Файлы JAR pxGrid с классами, которые могут легко декодироваться к файлам Java для проверки кода
- Типовой Java KeyStores с сертификатами
- Образцы сценария, которые используют типовые классы Java то использование pxGrid

Системный журнал

Вот список решений по обеспечению безопасности, которые передают сообщения системного журнала с IP-адресом атакующего. Они могут быть легко интегрированы с pxLog, пока вы используете корректное правило RegExp в конфигурации.

Фырканье

Фырканье передает предупреждения системного журнала в этом формате:

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

Например:

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

IP-адрес атакующего является всегда вторым перед последним (назначение). Просто создать гранулированный RegExp для определенной подписи и извлечь IP-адрес атакующего. Вот является пример RegExp для подписи 100124 и сообщения Протокол ICMP:

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

Устройство адаптивной защиты Cisco (ASA) контроль

Когда ASA настроен для HTTP (пример) контроль, соответствующее сообщение системного журнала похоже на это:

```
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
```

Снова гранулированный RegExp мог использоваться, чтобы фильтровать те сообщения и извлечь IP-адрес атакующего, второе перед последним.

Cisco Системы предотвращения вторжений следующего поколения (NGIPS) Sourcefire

Вот пример сообщения, передаваемый датчиком Sourcefire:

```
Jan 28 19:46:19 IDS01 SFIMS: [CA IDS][Policy1][119:15:1] http_inspect: OVERSIZE
REQUEST-URI DIRECTORY [Classification: Potentially Bad Traffic] [Priority: 2]
{TCP} 10.12.253.47:55504 -> 10.15.224.60:80
```

Таким образом, снова просто извлечь IP-адрес атакующего, потому что применяется та же

логика. Также название политики и подпись предоставлены, таким образом, правило pxLog может быть гранулировано.

NetScreen Juniper

Вот пример сообщения, передаваемый более старой Juniper Intrusion Detection & Prevention (IDP):

```
dayId="20061012" recordId="0" timeRecv="2006/10/12
21:52:21" timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0"
device_ip="10.209.83.4" cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN"
srcZn="NULL" srcIntf="NULL" srcAddr="192.168.170.20" srcPort="63396"
natSrcAddr="NULL" natSrcPort="0" dstZn="NULL" dstIntf="NULL"
dstAddr="192.168.170.10" dstPort="27374" natDstAddr="NULL" natDstPort="0"
protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS"
ruleNo="4" action="NONE" severity="LOW" alert="no" elaspedTime="0" inbytes="0"
outbytes="0" totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0"
packetData="no" varEnum="31" misc="<017>'interface=eth2" user="NULL"
app="NULL" uri="NULL"
```

IP-адрес атакующего может быть извлечен таким же образом.

Juniper JunOS

JunOS подобен:

```
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

Вот является некоторый пример 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
```

Можно передать сведения системного журнала за любым типом пакета с передовой функциональностью, предоставленной iptable модулями как отслеживание соединения, xtables, rpfilters, совпадение с образцом, и так далее.

FreeBSD IPFirewall (IPFW)

Вот является пример сообщения для IPFW блокирующимися фрагментами:

```
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)
```

Готовность VPN и обработка CoA

ISE в состоянии распознать тип сеансов с точки зрения обработки CoA.

- Для проводного Обхода 802.1X/ПРОРЕРКИ ПОЕЛИННОСТИ MAC (MAB) ISE передает CoA, повторно аутентифицируются, который инициирует вторую аутентификацию.
- Для беспроводного 802.1x/MAB ISE передает оконечный CoA, который инициирует вторую аутентификацию.
- Для VPN ASA ISE передает CoA с новым подключенным DACL (никакая вторая аутентификация).

Модуль EPS прост. Когда это выполняет карантин, это всегда передает CoA оконечный пакет. Для проводных/беспроводных сеансов это не проблема (все соискатели 802.1x в состоянии прозрачно инициировать второй сеанс EAP). Но когда ASA получает оконечный CoA, это отбрасывает сеанс VPN, и конечному пользователю предоставляют это:

Существует два возможных решения, чтобы вынудить VPN AnyConnect автоматически повторно соединиться (настроенный в профиле XML):

- Автовоссоединитесь, который работает только, когда вы теряете соединение со Шлюзом VPN, не для административного завершения
- Постоянный, который работает и вынуждает AnyConnect автоматически восстановить сеанс

Даже когда новый сеанс установлен, ASA выбирает новый контрольный идентификатор сеанса. С точки зрения ISE это - новый сеанс и нет никакого шанса встретиться с карантинным правилом. Также для VPN, не возможно использовать MAC-адрес оконечной точки как идентичность, в противоположность проводному/беспроводному dot1x.

Решение состоит в том, чтобы вынудить EPS вести себя как ISE и передать корректный тип CoA на основе сеанса. Эта функциональность будет представлена в Версии 1.3.1 ISE.

Партнеры pxGrid и Решения

Вот список партнеров pxGrid и решений:

- LogRhythm (Сведения о безопасности и управление событиями (SIEM)) - поддерживает представительную государственную передачу (REST) API
- Splunk (SIEM) - Поддерживает остальных API
- HP Arcsight (SIEM) - поддерживает остальных API
- Сигнальная метка NetIQ (SIEM) - Планирует поддержать pxGrid
- Lancope StealthWatch (SIEM) - Планирует поддержать pxGrid
- Cisco Sourcefire - Планирует поддержать pxGrid 1HCY15
- Cisco Web Security Appliance (WSA) - Планирует поддержать pxGrid в апреле 2014

Вот другие партнеры и решения:

- Надежный (оценка уязвимости)
- Emulex (захват пакета и судебная экспертиза)
- Сети Bayshore (Предотвращение потери данных (DLP) и политика Интернета вещей

(IoT))
- Идентичность эхо-запроса (Идентичность и Управление доступом (IAM) / Единая точка входа (SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (AMD SIEM Управление мобильными устройствами (MDM))

См. Каталог Решений для Рынка для полного списка решений по обеспечению безопасности.

API ISE: REST по сравнению с EREST по сравнению с pxGrid

Существует три типа API, доступного на Версии 1.3 ISE.

Вот сравнение:

	REST
Аутентификация клиента	имя пользователя + пароль (основная аутентификация HTTP)
Разделение привилегии	нет
Доступ	MnT
Транспорт	tcp/443 (HTTPS)
Метод HTTP	Get
Включенный по умолчанию	да
Количество операций	немногие
Оконечный CoA	поддерживаемый
CoA повторно аутентифицируются	поддерживаемый
Пользовательские операции	нет
Операции оконечной точки	нет
Идентификационные операции группы оконечной точки	нет
Карантин (IP, MAC)	нет
UnQuarantine (IP, MAC)	нет
PortBounce/Shutdown	нет
Операции гостя	нет
Гостевые операции портала	нет
Операции сетевого устройства	нет
Операции группы сетевых устройств	нет

* Карантинное использование объединило поддержку CoA от Версии 1.3.1 ISE.

Загрузки

pxLog может быть загружен из SourceForge .

Software Development Kit (SDK) уже включен. Для последнего SDK и документации API для pxGrid, свяжитесь со своим Партнером или Группой Cisco Account.

Дополнительные сведения

- Cisco ISE 1.2 API REST
- Cisco ISE 1.2 внешних API RESTful
- Cisco ISE 1.3 руководства администратора
- Cisco Systems – техническая поддержка и документация