ISE版本1.3与IPS pxLog应用程序的pxGrid集成

目录

简介

身份服务引擎(ISE)版本1.3支持一新的API呼叫的pxGrid。支持验证的此现代和灵活协议，加密和权限(组)允许与其他安全问题解决方案的容易集成。本文描述的pxLog应用程序使用情况写入作为概念证明。pxLog能收到从入侵防御系统(IPS)的系统消息和传送pxGrid信息到ISE为了检疫攻击者。结果，ISE用途RADIUS崔凡吉莱授权(CoA)为了更改限制网络访问终端的授权状态。所有此发生透明地在最终用户身上。

对于此示例，喷鼻息使用了作为IPS，但是可能使用所有其他解决方案。实际上它不必须是IPS。要求的所有是传送系统消息对pxLog用攻击者的IP地址。这创建很大数量的解决方案的集成的一种可能性。

本文也提交如何排除故障和测试pxGrid解决方案，与典型的问题和限制。

免责声明：思科不支持pxLog应用程序。此条款写入作为概念证明。主要目的将使用它在betatesting在ISE的pxGrid实施期间。

先决条件

要求

思科建议您有与思科ISE这些主题配置和基础知识的体验：

- ISE部署和授权配置
- 思科Catalyst交换机的CLI配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco Catalyst 3750X系列交换机软件，版本15.0和以上
- Cisco ISE软件，版本1.3和以上
- Cisco AnyConnect移动安全以网络访问管理器(NAM)，版本3.1和以上
- 与数据采集(DAQ)的喷鼻息版本2.9.6
- 在与MySQL版本5的Tomcat安装的pxLog应用程序7

网络图和通信流

这是通信流，如网络图所示：

1. Microsoft Windows 7用户连接到交换机并且执行802.1x验证。

2. 交换机使用ISE作为验证、授权和统计(AAA)服务器。**Dot1x全部存取的**授权规则匹配，并且全双工网络访问授权(DACL ：PERMIT_ALL)。

3. 用户设法连接可靠网络并且违反喷鼻息规则。

4. 结果，喷鼻息发送警报对pxLog应用程序(通过Syslog)。

5. pxLog应用程序进行验证其本地数据库。它配置为了捉住喷鼻息传送的系统消息和解压缩攻击者的IP地址。然后它使用pxGrid发送往ISE的一请求为了检疫攻击者IP地址(ISE是pxGrid控制器)。

6. ISE复评其授权策略。由于终端被检疫，**会话：EPSStatus等于检疫**情况满足，并且一不同的授权配置文件匹配(**Dot1x检疫**)。ISE发送CoA终止到交换机为了终止会话。这触发再验证，并且一个新的可下载的ACLs (DACL) (PERMIT_ICMP)应用，提供对最终用户的有限的网络访问。

7. 在此阶段，管理员也许决定到unquarantine终端。这可以通过pxLog GUI达到。再次，往ISE的pxGrid信息传送。

8. ISE在步骤6.执行一相似的操作正如。这时，终端不再被检疫，并且提供完全权限。

pxLog

体系结构

解决方案将安装一套在Linux计算机的应用程序：

1. 在Tomcat服务器写入在Java和实施的pxLog应用程序。该应用程序包括：

   处理Web请求-的Servlet这用于为了通过Web浏览器访问管理面板。

   实施者模块-与Servlet一起开始的线索。实施者读取系统消息从文件(优化)，根据配置的规则处理那些消息，并且执行操作(类似检疫通过pxGrid)。

2. 包含pxLog的配置的MySQL数据库(规则和日志)。

3. 收到从外部系统的系统消息并且写他们到文件的系统日志服务器。

安装

pxLog应用程序使用这些库：

- jQuery (阿贾克斯支持)
- JavaServer页标准的标记库(JSTL) (式样视图控制器(MVC)型号，数据从逻辑被分离：JavaServer页(JSP)代码没有用于只回报，在Java类的HTML代码)
- Log4j作为记录日志子系统
- MySQL连接器
- 表的回报的/排序displaytag
- pxGrid API用思科(当前版本阿尔法147)

所有那些库已经在项目的解放目录那么那里是没有需要下载Java Archive文件(JAR)文件。

为了安装应用程序：

1. 打开全部的目录对Tomcat Webapp目录。

2. 编辑**WebINF/web.xml文件**。唯一的必需更改serveripvariable，应该指向ISE。并且Java证书KeyStores (一委托的和一标识的)也许生成(而不是默认)。以两客户端和服务器证书使用安全套接字协议层(SSL)会话pxGrid API使用的这。通信需要的两边提交与证书和需要互相委托。参考pxGrid协议需求部分欲知更多信息。

3. 确保ISE主机名正确地被解决在pxLog (参考在域名服务器(DNS)或**/etc/hosts条目的**)记录。参考pxGrid协议需求部分欲知更多信息。

4. 配置与**mysql/init.sql脚本的**MySQL数据库。凭证在**WebINF/web.xml文件**更改，但是应该反射。

喷鼻息

此条款不着重任何特定IPS，是为什么提供仅简要说明。

喷鼻息配置作为线型与DAQ支持。流量重定向与iptables ：

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

然后，在检查以后，它根据默认iptable规则被注入并且转发。

一些个自定义喷鼻息规则配置(**/etc/snort/rules/test.rules**文件在全局配置里包括)。

```
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)
```

喷鼻息传送系统消息，当数据包的存活时间(TTL)是相等的到6时或有效负载的大小在666和686之间。流量没有由喷鼻息阻塞。

并且应该设置阈值确保警报太经常没有被触发(**/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
```

然后系统日志服务器指向pxLog计算机(**/etc/snort/snort.conf**) ：

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

对于喷鼻息一些版本，有与Syslog配置涉及的Bug的默认设置指向localhost，并且Syslog NG可能配置为了转发特定消息到pxLog主机可能然后使用。

ISE

配置

角色和证书

1. 启用pxGrid角色，默认情况下在ISE禁用，在**Administration >部署下**：

2. 如果证书使用在**Administration >证书>System下的**pxGrid**证书，请**验证：

终端保护业务(EPS)

应该从**Administration >设置**启用EPS (默认情况下禁用)：

这允许您使用检疫/unquarantine功能。

授权规则

只有当终端被检疫时，第一个规则遇到。然后有限访问由RADIUS CoA动态地强制执行。必须也添加交换机到有正确共享机密的网络设备。

故障排除

pxGrid状态可以验证与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
```

也有pxGrid的(**Administration >记录日志>调试日志Configuration> pxGrid**)独立的调试。调试文件在pxGrid目录存储。多数重的数据在**pxgrid/pxgrid-jabberd.log和**pxgrid/pxgrid-controller.log**。**

测验

Step1。pxGrid的注册

当Tomcat开始时， pxLog应用程序自动地被实施。

1. 为了使用pxGrid，请注册ISE的(一与会话访问，和一两个用户以检疫)。这可以从**Pxgrid操作>寄存器用户**完成：

   注册自动地开始：

2. 在此阶段，是必要的审批ISE的注册用户默认情况下(自动批准禁用) ：

   在批准以后， pxLog自动地通知管理员(通过阿贾克斯呼叫) ：

   ISE显示那两个用户的状态如联机或脱机(不等待再)。

Step2.pxLog规定配置

pxLog必须处理系统消息和执行根据它的操作。为了添加新规则，请选择**管理规则**：

现在实施者模块寻找此常规表示(Regexp)在系统消息：“喷鼻息[”。如果找到，它搜索所有IP地址并且在最后一个前选择那个。这匹配多数安全问题解决方案。参考Syslog部分欲知更多信息。该IP地址(攻击者)通过pxGrid被检疫。并且也许使用一个更加粒状的规则(例如，也许包括签名编号)。

Step3.第一Dot1x会话

Microsoft Windows 7站点启动一有线的dot1x会话。思科Anyconnect NAM使用了作为请求方。扩展验证协议保护的EAP (EAP-PEAP)方法配置。

ISE **Dot1x全部存取的**授权配置文件选择。交换机下载访问列表为了授权完全权限：

```
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
```

Step4.Microsoft Windows PC发送触发报警的数据包

这显示发生了什么，如果从一Microsoft Windows数据包发送与TTL = 7 ：

```
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
```

值在转发一系列和报警的喷鼻息消耗被上升。结果，往pxLog的一系统消息传送：

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

Step5.pxLog

pxLog收到系统消息，处理它和请求检疫该IP地址。这可以被确认是否检查日志：

Step6.ISE检疫

ISE报道IP地址被检疫：

结果，它查看授权策略，选择检疫，并且发送RADIUS CoA为了更新在交换机的授权状态该特定终端的。

那是CoA终止强制请求方启动个新会话和获得有限访问的消息(Permit_ICMP) ：

结果在交换机(终端的有限访问可以证实) ：

```
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
```

Step7.pxLog Unquarantine

在此阶段，管理员决定对终端的unquarantine ：

同一操作可以直接地从ISE被执行：

Step8.ISE Unquarantine

ISE再查看规则并且更新在交换机的授权状态(全双工网络访问授权) ：

报告确认：

pxLog功能

pxLog应用程序写入为了展示pxGrid API的功能。您可以通过它执行以下操作：

- 注册会话和EPS用户ISE的
- 下载关于所有会话的信息活动在ISE
- 下载关于特定激活的会话的信息ISE的(由IP地址)
- 下载关于一特定活动用户的信息ISE的(由用户名)
- 显示关于所有配置文件(仿形铣床)的信息
- 显示关于在ISE (SGTs)的信息定义的TrustSec安全组标记
- 检查版本(pxGrid的功能)
- 检疫基于IP或MAC地址
- Unquarantine根据IP或MAC地址

更多功能在将来计划。

这是从pxLog的一些示例屏幕画面：

pxGrid协议需求

组

客户端(用户)可以每次是一组的成员。两最常用的组是：

- 会话-用于为了浏览/关于会话/配置文件/SGTs的下载信息
- EPS -用于为了执行检疫

证书和Java KeyStore

如被提及以前，两个客户端应用、pxLog和pxGrid控制器(ISE)，必须有配置的证书为了通信。pxLog应用程序在Java KeyStore文件保留那些：

- **存储/client.jks -**包括客户端和Certificate Authority (CA)证书
- **存储/root.jks -**包括ISE一系列：监听和故障排除节点(MnT)标识和CA证书

文件由密码(默认保护：cisco123)。文件位置和密码在**WebINF/web.xml**可以更改。

这是生成一新的Java的步骤KeyStore ：

1. 为了创建根(委托) keystore，请导入CA证书(**CERTca.der应该**在DER格式) ：

```
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
```

2. 当您创建一新的keystore时，请选择密码，使用的以后为了访问keystore。

3. 导入MnT身份证书对根keystore (**CERTmnt.der是**从ISE采取的身份证书，并且应该在DER格式)：

```
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
```

4. 为了创建客户端keystore，请导入CA证书：

```
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
```

5. 创建在客户端keystore的一专用密钥：

```
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
```

6. 生成一证书签名请求(CSR)在客户端keystore ：

```
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
```

7. 签署CERTclient.csr并且导入签字的客户端证书：

```
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
```

8. 验证两keystores包含正确证书：

```
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
```

警告：当ISE 1.3节点升级时，有选项保持身份证书，但是CA签字删除。结果，升级的ISE使用一新证书，但是从未附加在SSL/ServerHello消息的CA证书。这触发期望的客户端的失败(根据RFC)发现全双工一系列。

主机名

几个功能的pxGrid API (类似会话下载)执行另外的验证。客户端与ISE联系并且接收ISE主机名，由hostname命令定义在CLI。然后，客户端设法执行该主机名的DNS解析并且设法与和拿来从该IP地址的数据联系。如果ISE主机名的DNS解析发生故障，客户端不设法得到任何数据。

警告：注意仅主机名使用此解决方法，是在此方案的**lise**，不是完全合格的域名(FQDN)，是在此方案的**lise.example.com**。

开发员的注意

思科发布并且支持pxGrid API。有象这样被命名的一个包：

pxgrid-sdk-1.0.0-167

在里面有：

- 有类的pxGrid JAR文件，可以容易地解码到Java文件检查代码
- 与证书的示例Java KeyStores
- 使用示例Java classess使用pxGrid的示例脚本

Syslog

这是传送系统消息用攻击者IP地址安全问题解决方案的列表。只要您在配置里，使用正确Regexp规则这些可以容易地集成与pxLog。

喷鼻息

喷鼻息发送在此格式的Syslog警报：

```
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
```

示例如下：

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

攻击者IP地址总是第二在最后一个前(目的地)。简单构件一个特定签名的一粒状Regexp和解压缩攻击者IP地址。这是签名100124和消息互联网控制消息协议(ICMP)的一示例Regexp ：

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

思科可适应安全工具(ASA)检查

当ASA为HTTP (示例)时检查配置，相应的SYSLOG消息如下所示:

```
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
```

再次一粒状Regexp能用于为了过滤那些消息和在最后一个前解压缩攻击者IP地址，第二。

思科Sourcefire下一代入侵防御系统(NGIPS)

这是Sourcefire传感器传送的示例消息：

```
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
```

那么，因为同样逻辑应用，再，简单解压缩攻击者IP地址。并且提供策略名称和签名，因此pxLog规则可以是粒状。

Juniper NetScreen

这是更旧的Juniper入侵检测&预防传送的示例消息(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"
```

攻击者的IP地址可以相似地解压缩。

Juniper JunOS

JunOS是类似的：

```
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

这是一些示例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
```

您能发送任一种数据包的系统日志信息有iptable模块提供的先进的功能的类似连接跟踪， xtables，rpfilters，模式匹配，等等。

FreeBSD IPFirewall (IPFW)

这是IPFW阻塞片段的一个示例消息：

```
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准备和CoA处理

ISE能识别会话种类根据CoA处理。

- 对于一条有线的802.1x/MAC验证旁路(MAB)， ISE发送CoA重新鉴别，触发秒钟验证。
- 对于无线802.1x/MAB， ISE发送CoA终止，触发秒钟验证。
- 对于ASA VPN， ISE发送与附加的新的DACL的CoA (没有第二验证)。

EPS模块简单。当它执行一检疫时，总是发送CoA终止数据包。对于有线的/无线会话，它不是问题(所有802.1x恳求者能透明地启动秒钟EAP会话)。但是，当ASA接收CoA时请终止，它丢弃VPN会话，并且最终用户提交与此：

有强制AnyConnect的两个可能的解决方案VPN自动地重新连接(配置在XML配置文件)：

- Autoreconnect，工作，只有当您丢失连接用VPN网关，不管理终端的

- 不间断工作的，工作和强制AnyConnect自动地重建会话

既使当个新会话设立， ASA选择新的审计会话id。从观点的ISE，这是个新会话，并且没有机会遇到检疫规则。并且对于VPN，使用终端的MAC地址作为标识，与有线的/无线dot1x相对是不可能的。

解决方案将强制EPS正常运行类似ISE和发送根据会话的CoA的正确类型。此功能在ISE版本1.3.1将介绍。

pxGrid合作伙伴和解决方案

这是pxGrid合作伙伴和解决方案列表：

- LogRhythm (安全信息和事件管理(SIEM))-支持代表状态转移(其余) API
- Splunk (SIEM) -支持其余API
- HP Arcsight (SIEM) -支持其余API
- 稍兵NetIQ (SIEM) -规划支持pxGrid
- Lancope StealthWatch (SIEM) -规划支持pxGrid
- 思科Sourcefire -规划支持pxGrid 1HCY15
- 思科Web安全工具(WSA) -规划支持在April 2014的pxGrid

这是其他合作伙伴和解决方案：

- 站得住脚(漏洞评估)
- Emulex (数据包捕获和辩论术)
- Bayshore网络(数据丢失事(IoT)策略)预防(DLP)和互联网
- Ping标识(标识和访问管理(IAM) /Single符号(SSO))
- Qradar (SIEM)
- LogLogic (SIEM)
- Symantec (SIEM amd移动设备管理(MDM))

参考安全问题解决方案详尽列表的市场解决方案目录。

ISE API ：其余与EREST与pxGrid

有API联机的三种类型在ISE版本1.3的。

这是比较：

	其余	**宁静的外部**	**pxGrid**
客户端验证	用户名+密码(基本HTTP验证)	用户名+密码(基本HTTP验证)	证书
权限分离	否	有限(ERS Admin)	是(组)
访问	MnT	MnT	MnT
传输	tcp/443 (HTTPS)	tcp/9060 (HTTPS)	tcp/5222 (XMPP)
HTTP方法	GET	GET/POST/PUT	GET/POST
默认情况下启用	是	否	否
操作编号	少量	许多	少量
CoA终止	支持的	否	支持的

CoA再次验证	支持的	否	支持的*
用户操作	否	是	否
终端操作	否	是	否
终端标识组操作	否	是	否
检疫(IP ， MAC)	否	否	是
UnQuarantine (IP ， MAC)	否	否	是
PortBounce/关闭	否	否	是
来宾用户操作	否	是	否
访客门户操作	否	是	否
网络设备操作	否	是	否
网络设备组操作	否	是	否

*检疫用途统一从ISE版本1.3.1的CoA支持。

下载

pxLog可以从Sourceforge下载。

软件开发工具(SDK)已经包括。对于pxGrid的最新的SDK和API文档，与您的合作伙伴或思科客户团队联系。

相关信息

- 思科ISE 1.2其余API
- 思科ISE 1.2外部宁静的API
- 思科ISE 1.3管理员指南
- 技术支持和文档 - Cisco Systems