如何验证IPS流量检查和签名警报

目录

简介

本文提供步骤使用为了验证入侵防御系统(IPS)传感器和签名测验选项的操作在生产环境的。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件版本：

- 入侵防御系统版本6.2(x)E4
- 入侵防御系统版本7.0(x)E4
- 入侵防御系统版本7.1(x)E4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

内部，外部和管理通讯

请使用这些步骤为了验证IPS管理访问和准备：

- 访问IPS的控制台。如果这是模块问题，则回车：从5500和5585系列可适应的安全工具(ASA)的**会话1**，从5500x的**会话ips**，**IDS传感器**网络模块增强版(NME)模块的**service-module插槽/端口会话**，在CatOS的**sessionslot_number**，和**session slot**在IOS的**module_number处理器1**入侵检测系统(IDSM)和IDSM-2 (第二代)模块的。
- 有在初始设置配置的用户名和密码的洛金。默认用户名和密码是“cisco”。欲了解更详细的信息参考适当的版本的设置指南。
- 如果设置已经完成，则请继续对测验IP连通性对IPS管理。
- 输入**host命令的show statistics**，并且设法ping和获取对IPS管理IP地址的安全壳SSH访问。如果这工作，则请继续对下一步。否则，然后请排除故障连接问题用适当的版本的配置指南。
- 输入**show version命令**。验证软件版本当前，那许可证安装，签名版本最晚，所有引擎是可操作的，并且那主机证书有效。
- 如果所有上一个步骤验证，则请通过HTTPS访问IPS的管理地址并且启动IDM。必须安装Java 6。如果Java 6不是可用的，则安装从IPS网页的IPS管理器Express (IME)。**注意：** 不支持Java 7启动IPS设备管理器(IDM)或此时访问在可适应安全设备管理器(ASDM)的IPS选项。
- 如果连接是成功的，则在IDM，请去**Configuration>从Cisco.com的Management>许可授权的传感器和Update license**。即使有效许可证存在，这确认连接到互联网。
- 如果成功，然后去**Configuration>策略>全局相关性>检查/名誉**并且单击**测验全局相关性**确保DNS工作。为了检查此，去**Monitoring>事件**和选择**警告，只错误和致命**和确认，如果**全局相关性**更新发生故障。**注意：** 全局相关性早于IPS版本7.0不是可用的在IPS软件。

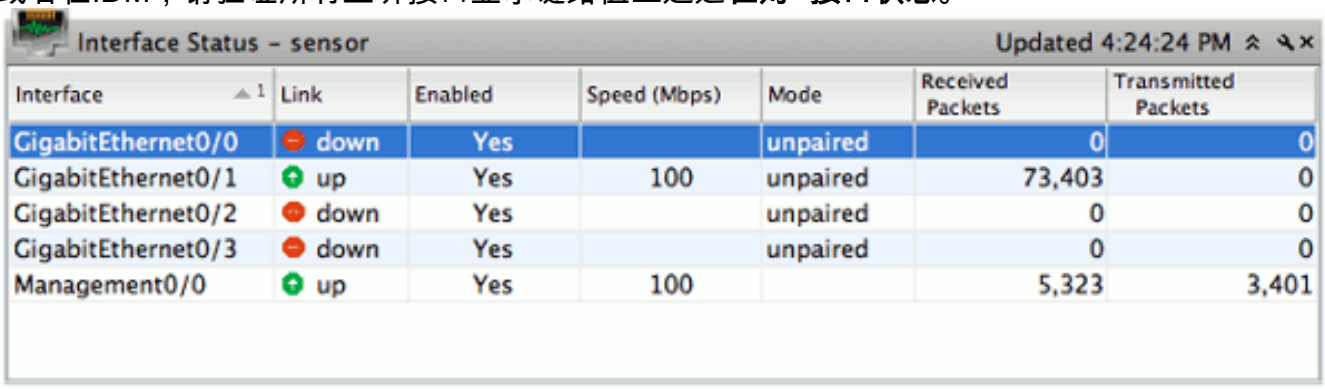
验证流量的检查

在您通过IPS后验证通信，您能验证流量的检查与这些步骤的。

- 验证感觉接口链接状态的传感器上并且收到流量。登陆对传感器接口并且输入这些命令：

```
sensor# show interface

!! In the output, find the applicable section for the sensing interface(s) in !! question and
confirm that the Link Status value is "Up". If so, note the !! value shown for the Total Packets
Received counter. After a few seconds, !! run the command again and compare the current value to
the previous. !! If the value has increased, the sensing interface(s) in-question is Up !! and
receiving traffic. Example: sensor# show interface
MAC statistics from interface GigabitEthernet0/0
   Interface function = Sensing interface
   Link Status = Up
   Total Packets Received = 100

sensor# show interface
MAC statistics from interface GigabitEthernet0/0
   Interface function = Sensing interface
   Link Status = Up
   Total Packets Received = 150

!! If a sensing interface's Link Status value is expected to be "Up", but is !! not, verify that
it is properly and physically connected to a switchport or !! other network device. If so,
verify that the switchport or other network !! device is configured properly and the remote
interface (the switchport or !! NIC on the other network device) is not administratively-
disabled !! ("shutdown"). If needed, try to swap cables with another that is known !! to be
good. !! If a sensing interface's Total Packets Received counter does not increment, !! check
the configuration of the switchport or other network device to which !! the sensing interface is
connected. If the sensing interface is supposed to !! be the destination of a SPAN/monitor
session, verify the SPAN/monitor !! configuration on the switch the sensing interface is
connected.
```

- 或者在IDM，请验证所有监听接口显示链路值上通过**霍姆>接口状态**。

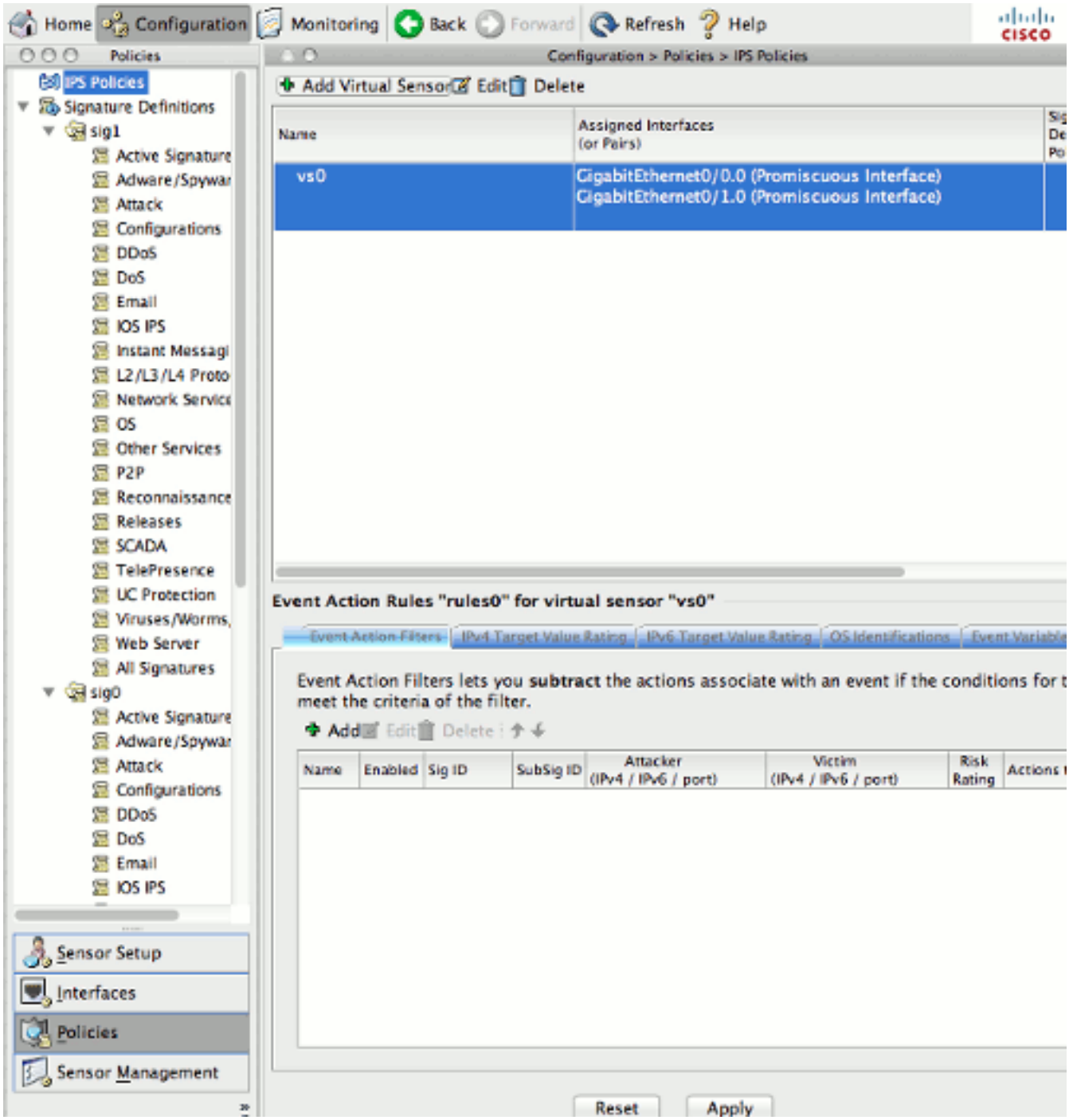


Interface	Link	Enabled	Speed (Mbps)	Mode	Received Packets	Transmitted Packets
GigabitEthernet0/0	down	Yes		unpaired	0	0
GigabitEthernet0/1	up	Yes	100	unpaired	73,403	0
GigabitEthernet0/2	down	Yes		unpaired	0	0
GigabitEthernet0/3	down	Yes		unpaired	0	0
Management0/0	up	Yes	100		5,323	3,401

- 验证传感器的虚拟传感器有分配的至少一个感觉的接口并且检查流量。登陆到传感器并且输入此命令。

```
 sensor# show stat virtual

!! In the output, find the List of interfaces monitored by this virtual !! sensor line and
confirm that at least one (1) sensing interface(s) is !! listed. Additionally, find the
Total packets processed since reset !! line/counter and confirm its value is greater-than
(>) zero (0). !! Example: sensor# show stat virtual
   Statistics for Virtual Sensor vs0
      List of interfaces monitored by this virtual sensor = GigabitEthernet0/0
      General Statistics for this Virtual Sensor
         Total packets processed since reset = 200

!! If there are no sensing interface(s) listed (or, if additional sensing !! interfaces need
to be assigned), login to the sensor using an !! administrative account and issue the
following commands !! (NOTE: In the example provided, the GigabitEthernet0/0 sensing
interface !! is assigned to virtual-sensor vs0. Replace that particular configuration !!
line accordingly with the actual sensing interface you wish to assign to !! the virtual-
sensor. If you need to assign multiple sensing interfaces, !! repeat that line (one per
sensing interface)):


sensor# conf t
sensor(config) # service analysis-engine
sensor(config-ana) # virtual-sensor vs0
sensor(config-ana-vir)# physical-interface GigabitEthernet0/0
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes?[yes]: yes

!! NOTE: The above example assigns a Promiscuous sensing interface to the vs0 !! virtual-
sensor. Inline sensing interfaces must first be "paired" together !! and then the logical
pair assigned to a virtual-sensor. Details can be !! found in the official product
configuration guide's Configuring !! Interfaces section.
```

- 或者，请验证接口分配到在IDM的vs0根据Configuration>策略> IPS策略。

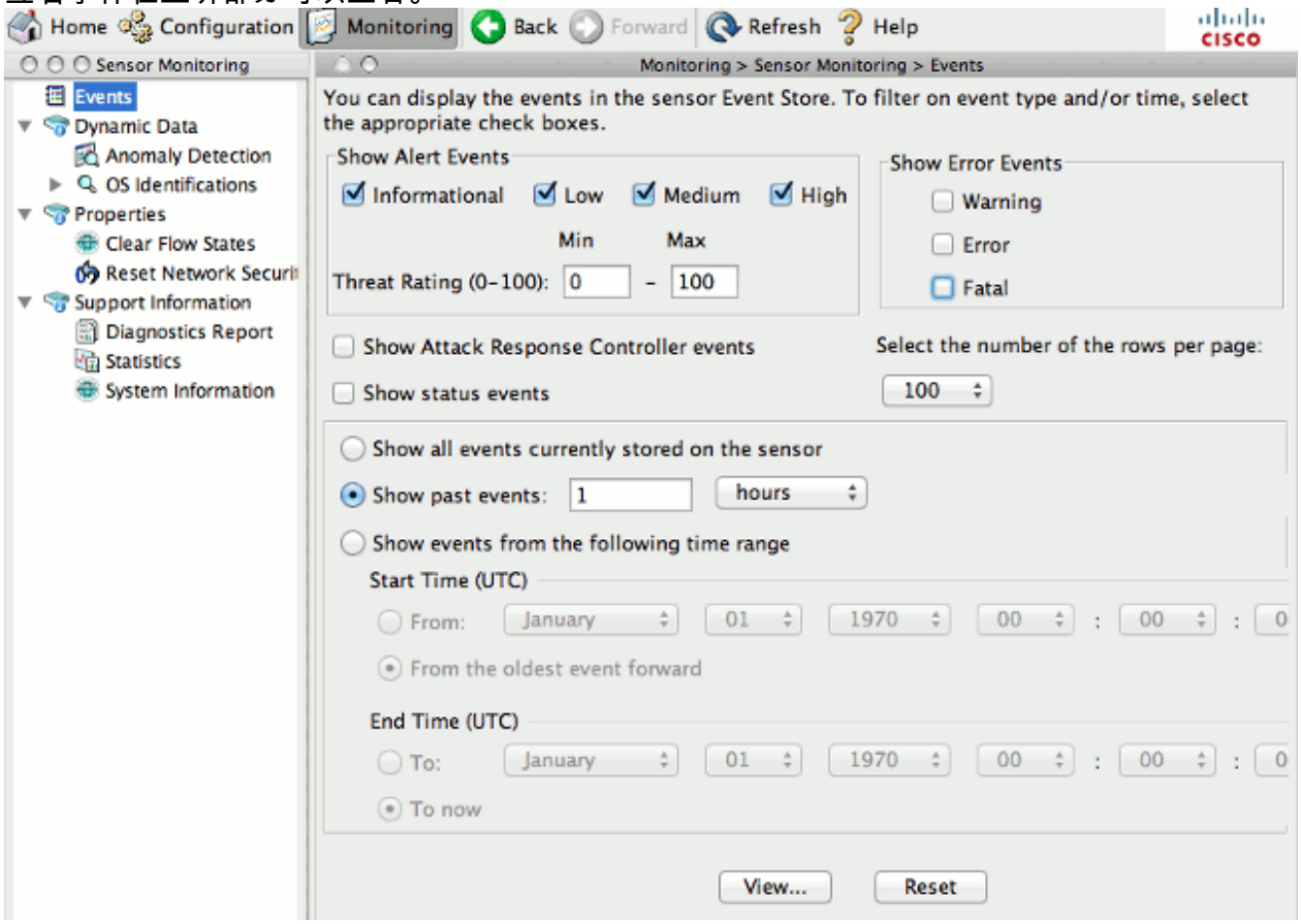


- 进入SSH对IPS并且输入**数据包显示接口插槽/端口**命令并且验证流量被看到在接口。**注意： *表达式*关键字允许使用tcpdump表达式为了显示匹配使用的表达式仅的流量。**

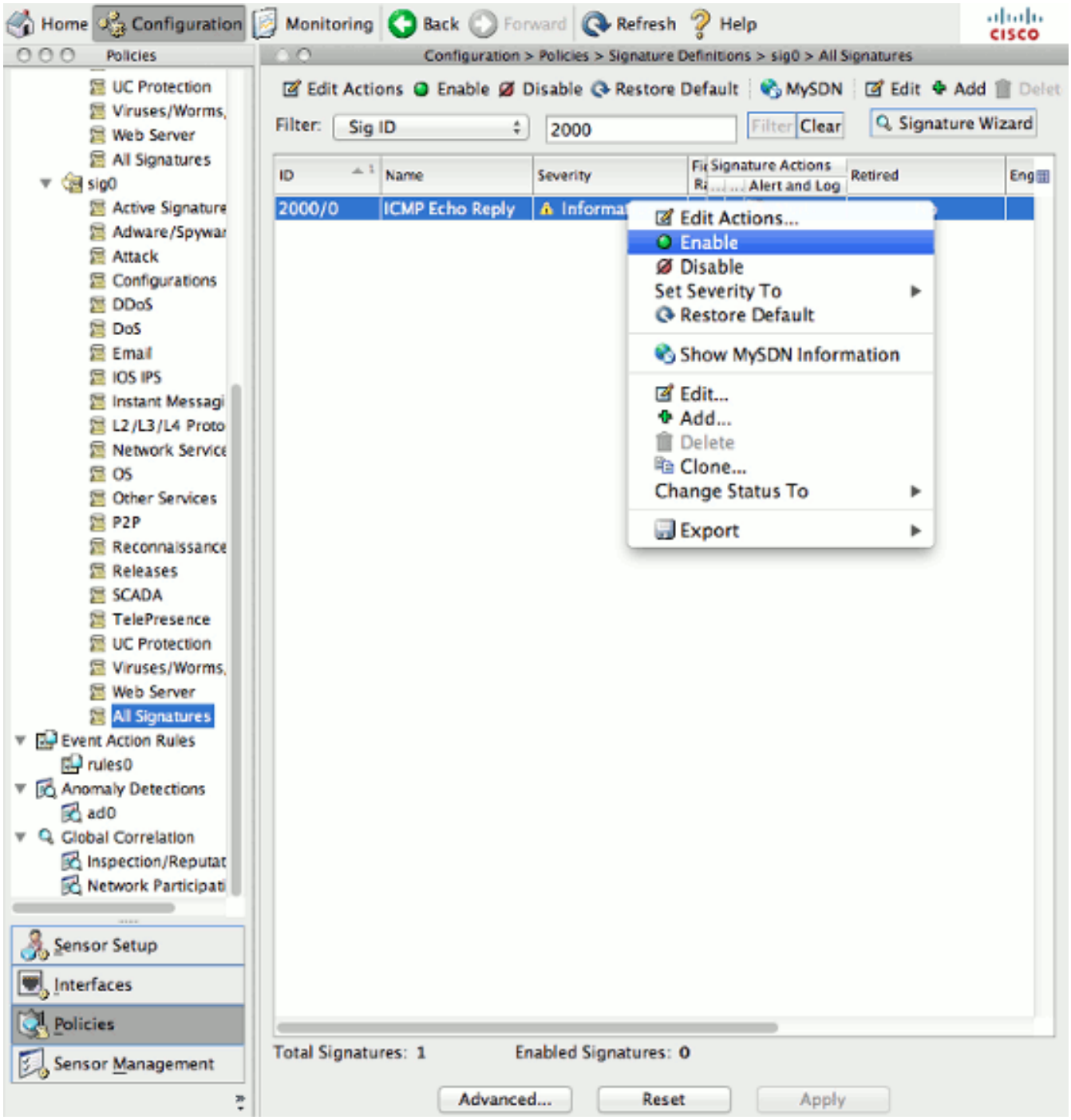
```
sensor# packet display gigabitEthernet0/1 expression ip host 198.51.100.1
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
18:32:24.247864 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172
18:32:24.247868 IP 198.51.100.1.2000 > 192.0.2.1.2000: UDP, length 172
18:32:24.257249 IP 198.51.100.1.2000 > 192.0.2.1.16384: UDP, length 172

 !! Alternatively, in the case of VLAN tagging: sensor# packet display gigabitEthernet0/1
expression vlan 20 and
    ip host 192.51.100.1
```

验证签名火

- 签名事件在监听部分可以查看。

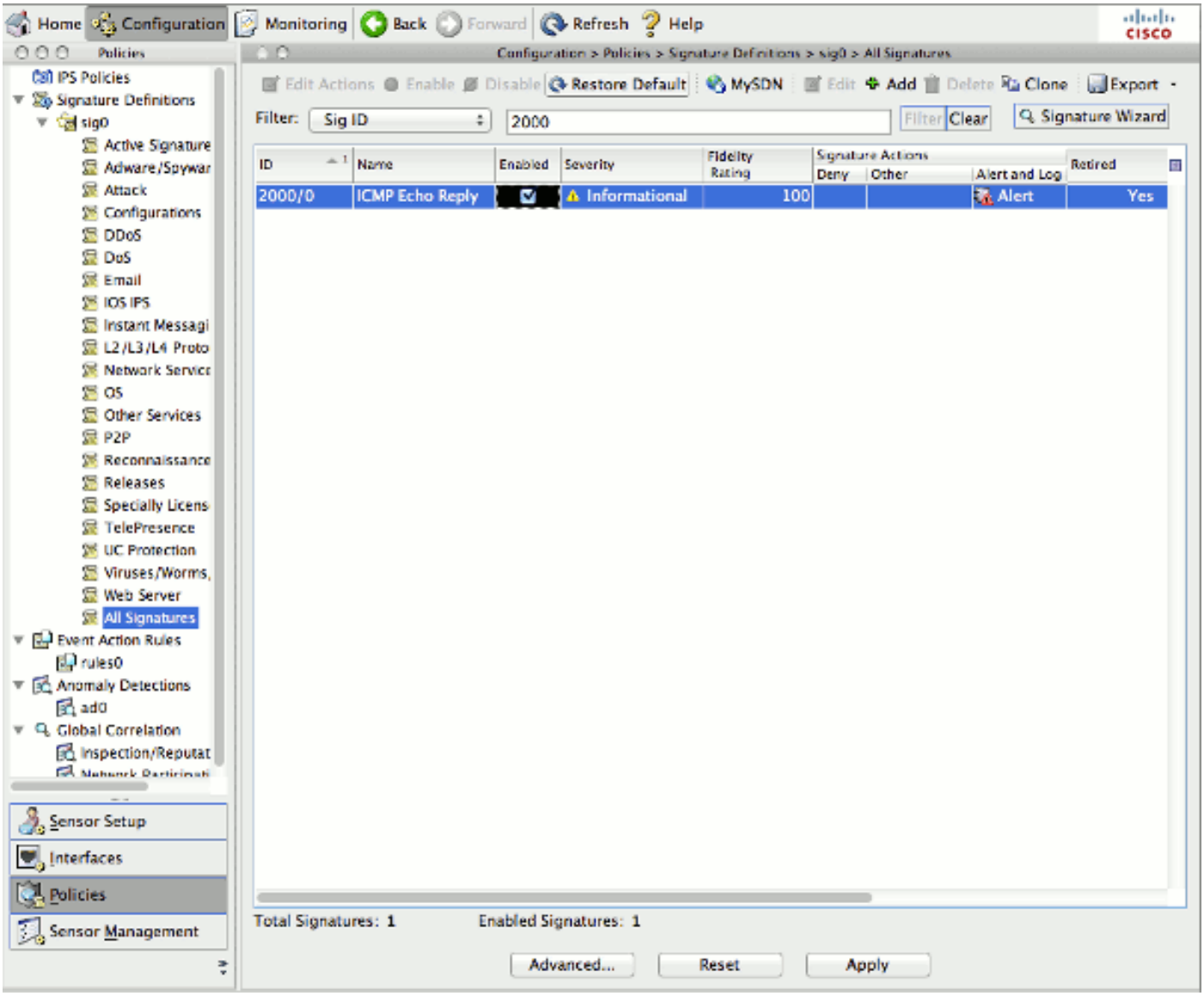


- 签名可以被修改在**Configuration>下所有签名**。



- Enable (event)签名2000/0和2004/0 (互联网消息控制协议(ICMP)ECHO应答和ICMP echo请求);通过传感器启动ping，并且检查事件日志在Monitoring选项。如果ICMP阻塞：对于1107/0，参考RFC1918 -*被看到的地址*。为了触发此签名，集**退休**对**错误**和**enable (event)**对**真**在此签名并且观看在RFC 1918范围的IP触发签名。这些地址是10.0.0.0/8， 172.16.0.0-172.31.255.255， 192.168.0.0/16。因为要求为了能unretired的签名这在SSC-5不能被看到。3409/0，对端口80的telnet。使用Web服务器设置，端口80是开放的，并且telnet是成功的。当telnet是成功的，在IPS的事件火。TCP三通的握手要求为了传感器能跟踪有效TCP连接。一旦不对称路由或一部分数据包捕获的重播，流量不导致签名的火。

在测试完成以后，请恢复默认对所有已修改签名：



相关信息

- 在5500x IPS模块的IPS管理配置情形
- 思科入侵防御系统传感器IPS的7.0 CLI配置指南
- 思科入侵防御系统传感器IPS的7.1 CLI配置指南
- IPS管理器Express
- Secure Shell (ssh)
- 技术支持和文档 - Cisco Systems