Как проверить предупреждения контроля и подписи трафика IPS

Содержание

Введение

Этот документ предоставляет шаги в использование для проверки использования датчика Системы предотвращения вторжений (IPS) и тестовых опций подписи в производственной среде.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Выпуск 6.2 (x) E4 системы предотвращения вторжений
- Выпуск 7.0 (x) E4 системы предотвращения вторжений
- Выпуск 7.1 (x) E4 системы предотвращения вторжений

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Внутренний, внешний и связь менеджмента

Используйте эти шаги для проверки доступа управления IPS и готовности:

- Обратитесь к консоли в IPS. Если это - проблема модуля, то войдите:**откройте сеанс 1** от Устройства адаптивной защиты (ASA) 5500 и 5585 серий,**ips сеанса** от 5500x,**слот/сеанс порта service-module ids-sensor на** модуле Расширенного сетевого модуля (NME),**sessionslot_number** в CatOS, и**процессор 1 module_number session slot** в IOS для Системы обнаружения проникновения (IDSM) и IDSM-2 (второе поколение) модули.
- Вход в систему с именем пользователя и паролем, которое было настроено в начальной настройке. Имя пользователя по умолчанию и пароль являются "Cisco". См. руководство по установке для соответствующего выпуска для получения дополнительной информации.
- Если настройка уже завершена, то продолжите тестировать возможность подключения с помощью IP-адреса к управлению IPS.
- Введите **команду show statistics host** и попытайтесь пропинговать и получить доступ Secure Shell (SSH) к IP-адресу управления IPS. Если это работает, то продолжите к следующему шагу. В противном случае тогда устраните неполадки неполадок подключения с руководством по конфигурации для соответствующего выпуска.
- Введите **команду Show version**. Проверьте, что версия программного обеспечения является текущей, что лицензия установлена, версия подписи последняя, все механизмы в рабочем состоянии, и что сертификат хоста допустим.
- Если все предыдущие шаги проверены, то обращаются к адресу управления IPS через HTTPS и запускают IDM. Java 6 должен быть установлен. Если Java 6 не доступен, то установите IPS Manager Express (IME) от веб-страницы IPS.**Примечание: Java 7** не поддерживается, чтобы запустить диспетчера устройств IPS (IDM) или обратиться к опциям IPS в Менеджере устройств адаптивной безопасности (ASDM) (ASDM) в это время.
- Если подключение успешно, то в IDM, перейдите **к Конфигурации> менеджмент Датчика> Лицензирование и Update License от Cisco.com**. Даже если действующая лицензия существует, это подтверждает подключение к Интернету.
- Если успешный, то перейдите **к Конфигурации> Политика> Глобальная Корреляция> Контроль/Репутация** и щелкните **по Test Global Correlation**, чтобы удостовериться, что работает DNS. Для проверки этого перейдите **к Контролирующему> Events (sentence)** и выберите только **Предупреждение, Ошибку и Фатальный** и подтвердите, отказывают ли **Обновления глобальной взаимосвязи**.**Примечание:** Глобальная Корреляция не доступна на программном обеспечении IPS ранее, чем Выпуск 7.0 IPS.

Проверьте контроль трафика

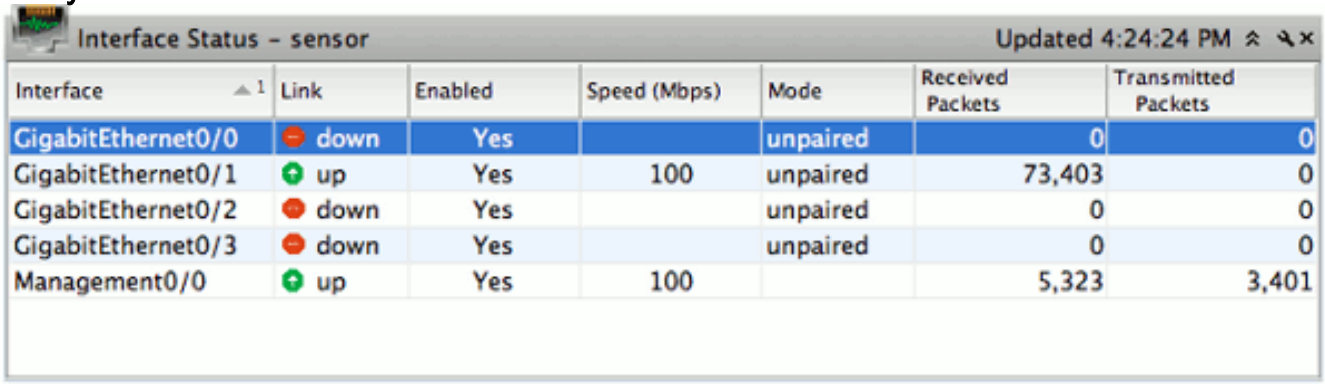
После проверки связи через IPS можно проверить контроль трафика с этими шагами.

- Проверьте, что датчик, снимающий показания интерфейсный Статус соединения,

подключен и получает трафик. Вход в систему к датчику взаимодействует и вводит эти команды:

```
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.
```

- Альтернативно в IDM, проверьте, что все интерфейсы мониторинга отображают значение ссылки через **Дом> Интерфейсный Статус**.



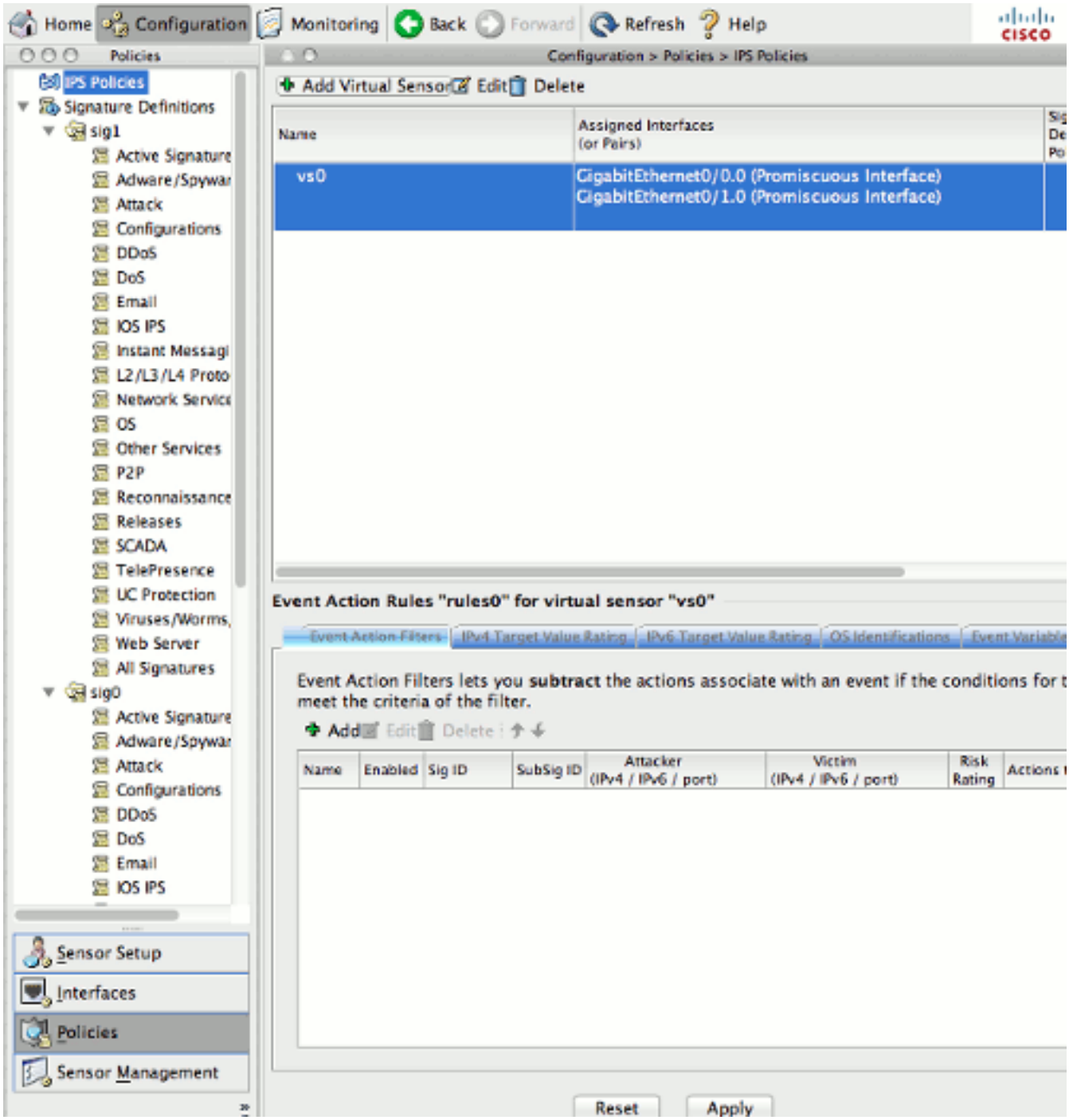
Interface Status – sensor — Updated 4:24:24 PM

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

- Проверьте, что действительный датчик (датчики) датчика имеет по крайней мере один назначенный интерфейс считывания и осматривает трафик. Вход в систему к датчику и вводит эту команду.

```
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.
```

- Также проверьте, что интерфейсы назначены на **vs0** в IDM под **Конфигурацией> Политика> Политика IPS**.

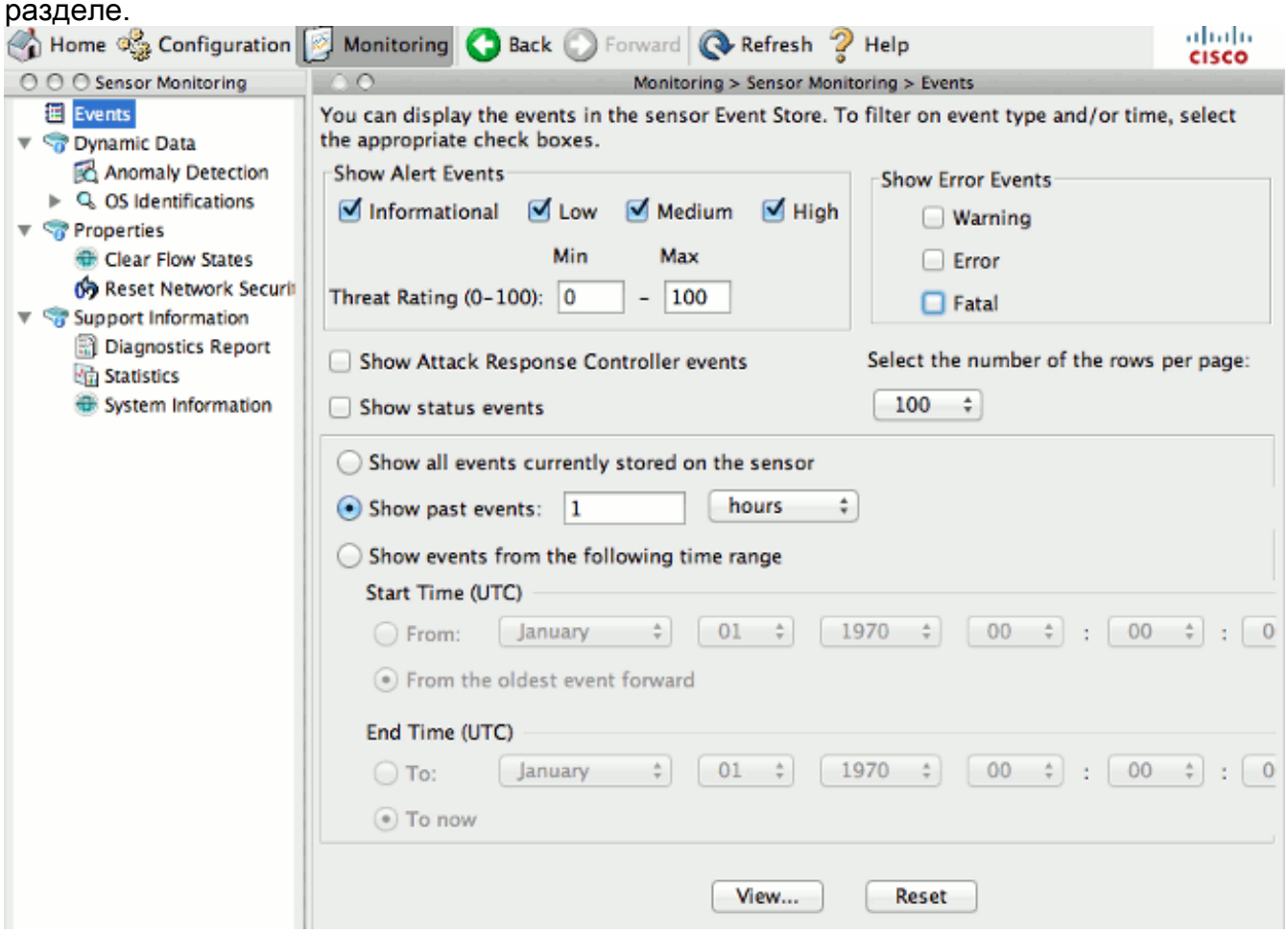


- Введите SSH в IPS и введите **команду packet display interface slot/port** и проверьте, что трафик замечен на интерфейсе.**Примечание:** Ключевое слово ***выражения*** позволяет использование выражений **tcpdump** для отображения только трафика, который совпадает с используемым выражением.`sensor# 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`

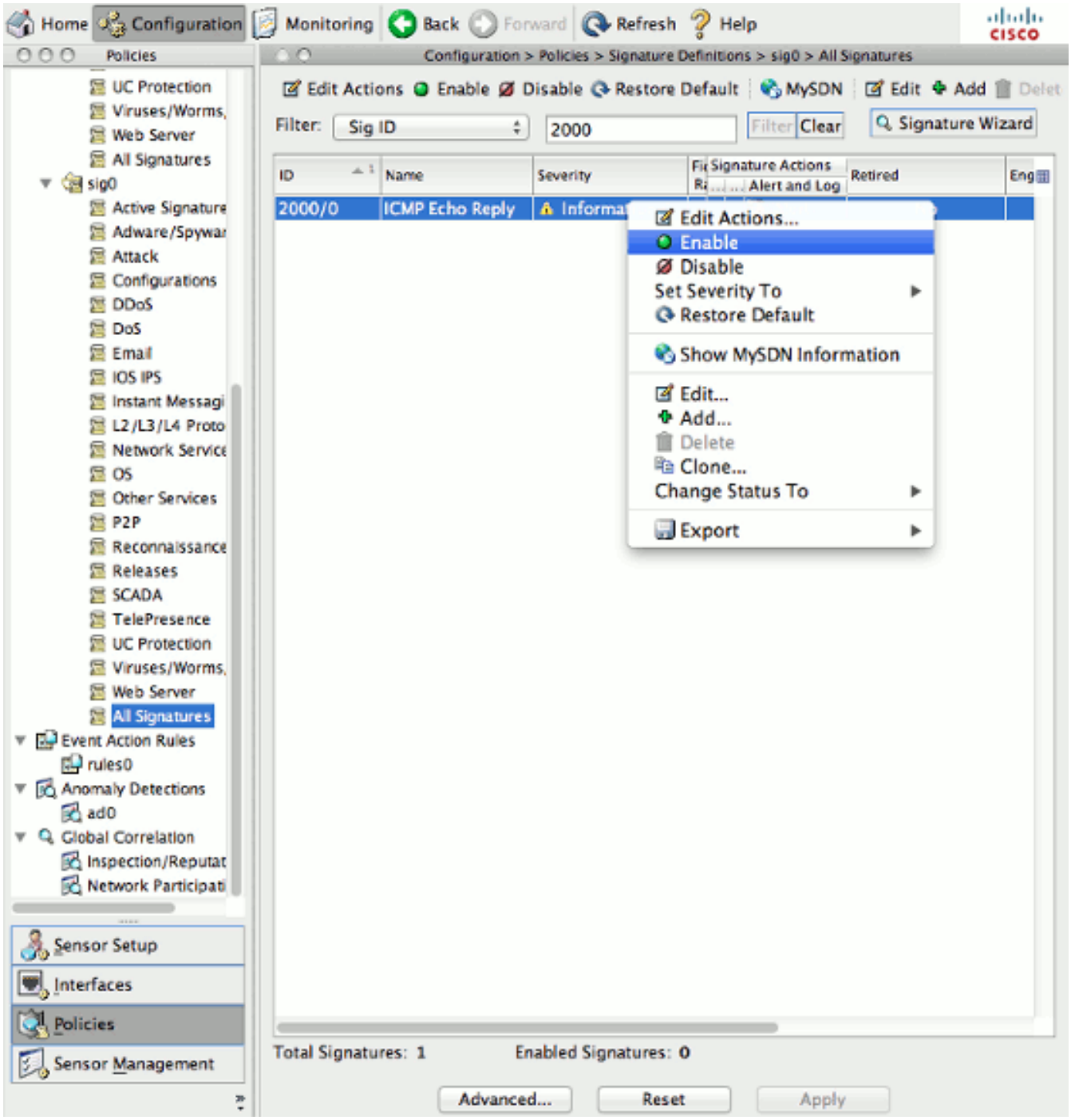
Проверьте огни подписи

- События подписи могут быть просмотрены в Контролирующем

разделе.

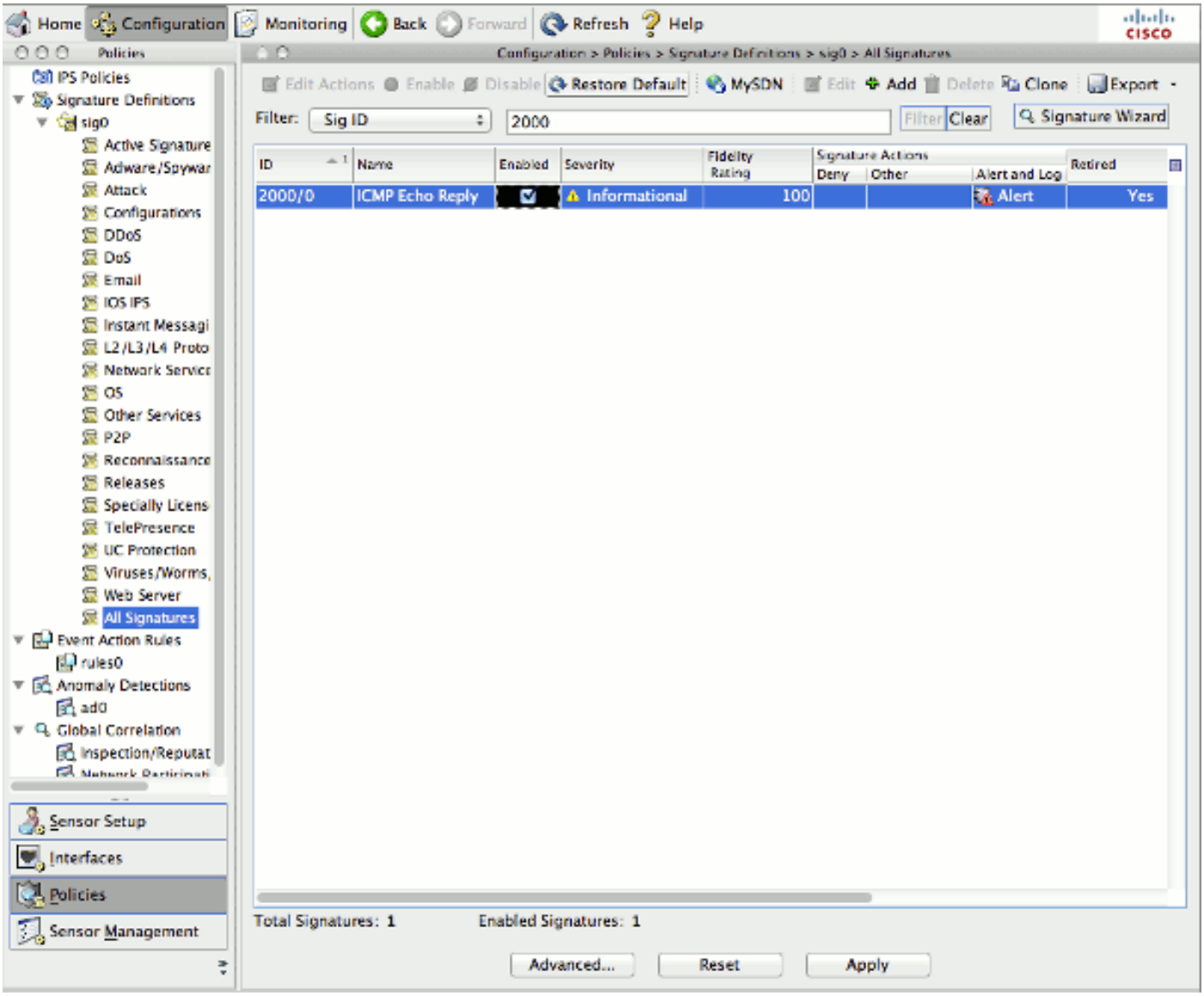


- Подписи могут модифицироваться под **Конфигурацией> Все Подписи**.



- Включите подписи 2000/0 и 2004/0 (Эхо - ответ Протокола ICMP и Эхо-запрос протокола ICMP); инициируйте эхо-запрос через датчик и проверьте журнал событий во вкладке Monitoring.Если заблокирован ICMP:Для 1107/0 обратитесь к RFC1918 - *Замеченный Адрес.*Для инициирования этой подписи установите**, удаляются** ко **лжи** и **включают** к **истине** на этой подписи и наблюдают, что IPs в диапазонах RFC 1918 инициирует подписи.Эти адреса являются 10.0.0.0/8, 172.16.0.0-172.31.255.255, 192.168.0.0/16.Это не может быть замечено на SSC-5, потому что он требуется для подписи быть неисключенным.Для 3409/0, telnet к порту 80.С настройкой Web-сервера порт 80 открыт, и telnet успешна. Когда telnet успешна, событие стреляет в IPS.Трехстороннее квитирование TCP требуется для датчика отследить допустимый TCP - подключение. В случае асимметричной маршрутизации или воспроизведения перехвата частичного пакета, трафик не вызывает огонь подписи.

После того, как тестирование завершено, восстановите настройки по умолчанию к любым модифицированным подписям:



Дополнительные сведения

- Сценарии конфигурации управления IPS на 5500x модуль ips
- Руководство конфигурации интерфейса командой строки датчика системы предотвращения вторжений Cisco (IPS) для IPS 7.0
- Руководство конфигурации интерфейса командой строки датчика системы предотвращения вторжений Cisco (IPS) для IPS 7.1
- IPS Manager Express
- Secure Shell (SSH)
- Cisco Systems – техническая поддержка и документация