Como verificar alertas da inspeção e da assinatura do tráfego IPS

Índice

Introdução

Este documento fornece as etapas para usar-se a fim verificar a operação de opções de um sensor do Intrusion Prevention System (IPS) e do teste da assinatura em um ambiente de produção.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Versão de sistema 6.2(x)E4 da prevenção de intrusão
- Versão de sistema 7.0(x)E4 da prevenção de intrusão
- Versão de sistema 7.1(x)E4 da prevenção de intrusão

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

Comunicações internas, externos e de Gerenciamento

Use estas etapas a fim verificar o acesso e a prontidão do Gerenciamento de IPS:

- Alcance o console no IPS. Se esta é uma edição do módulo, a seguir entre:**sessão 1 do** 5500 e 5585 Series adaptável da ferramenta de segurança (ASA),**sessão IP de um** 5500x,**a sessão da /porta do entalhe do sensor de IDS do módulo de serviço em um** módulo de rede aumentou o módulo (NME),**sessionslot_number em** Cactos, e**processador 1 do module_number do entalhe da sessão nos** IO para o sistema de detecção de intrusões (IDSM) e os módulos IDSM-2 (de segunda geração).
- Entre com o nome de usuário e senha que foi configurado na instalação inicial. O nome de usuário padrão e a senha são “Cisco”. Refira o guia da instalação para a liberação apropriada para mais detalhes.
- Se a instalação está já completa, a seguir continue à conectividade IP do teste ao Gerenciamento de IPS.
- Inscreva o **comando host das estatísticas da mostra**, e tente-o sibilar e obter o acesso do Shell Seguro (ssh) ao endereço IP de Um ou Mais Servidores Cisco ICM NT do Gerenciamento de IPS. Se isto trabalha, a seguir continue à próxima etapa. Se não, pesquise defeitos então os problemas de conectividade com o manual de configuração para a liberação apropriada.
- Inscreva o **comando show version**. Verifique que a versão de software é atual, aquela uma licença é instalada, a versão da assinatura está a mais atrasada, todos os motores são operacionais, e que o certificado do host é válido.
- Se todas as etapas precedentes são validadas, a seguir alcance o endereço de gerenciamento do IPS através do HTTPS e lance o IDM. As Javas 6 devem ser instaladas. Se a Java 6 não está disponível, a seguir instale o gerente IPS expresso (IME) do página da web IPS.**Nota:** A Java 7 não é apoiada para lançar o gerenciador de dispositivo IPS (IDM) ou para alcançar neste tempo opções IPS no Security Device Manager adaptável (ASDM).
- Se a Conectividade é bem sucedida, a seguir no IDM, vá à **configuração** > ao **Gerenciamento do sensor** > **licenciando e atualize a licença do cisco.com**. Mesmo se uma licença válida existe, esta confirma a Conectividade ao Internet.
- Se bem sucedida, então vão à **configuração** > às **políticas** > a **correlação** > a **inspeção/reputação globais** e clicam sobre a **correlação global do teste** para certificar-se dos trabalhos DNS. A fim verificar isto, ir à **monitoração** > **eventos** e selecionar somente a **advertência, o erro e o fatal** e confirmar se as atualizações **globais da correlação** falham.**Nota:** A correlação global não está disponível no software IPS mais cedo do que a liberação 7.0 IPS.

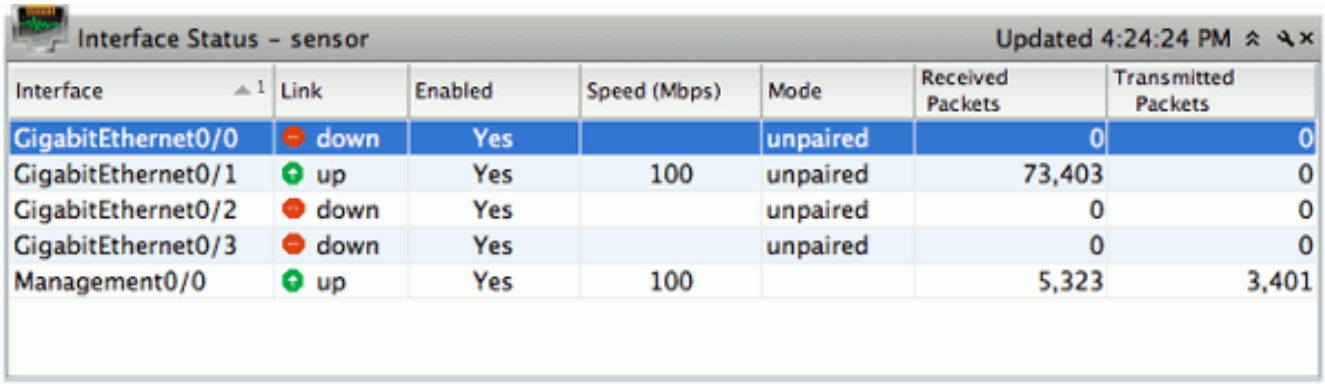
Verifique a inspeção do tráfego

Depois que você verifica comunicações com o IPS, você pode verificar a inspeção do tráfego com estas etapas.

- Verifique que o sensor que detecta o estado do link da relação é **ascendente** e recebe o tráfego. Entre à relação do sensor e incorpore estes comandos:

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.*

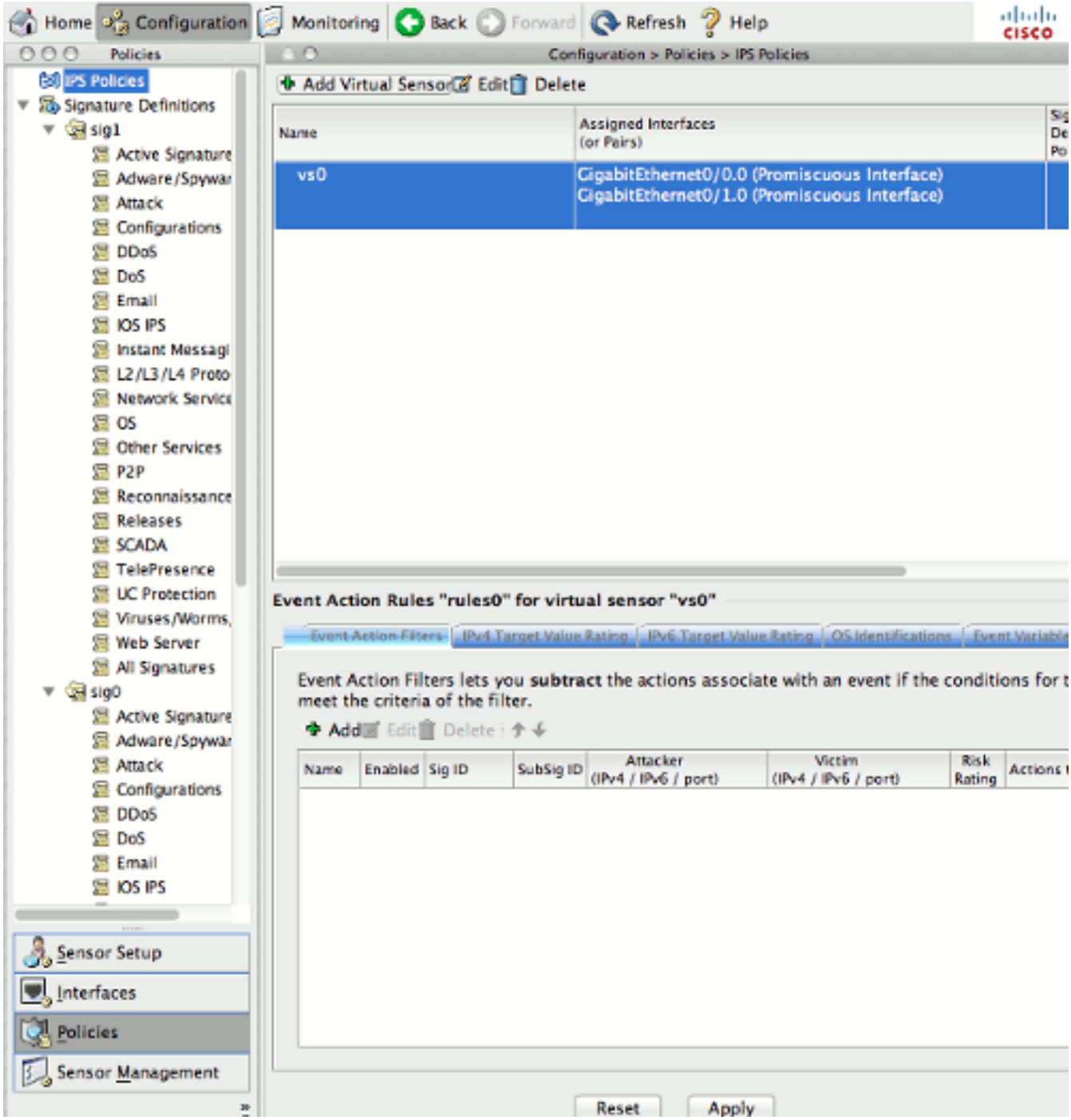
- Alternativamente no IDM, verifique que todas as relações da monitoração indicam um valor do link da **HOME** > do **status da interface** diretos **ascendentes**.



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

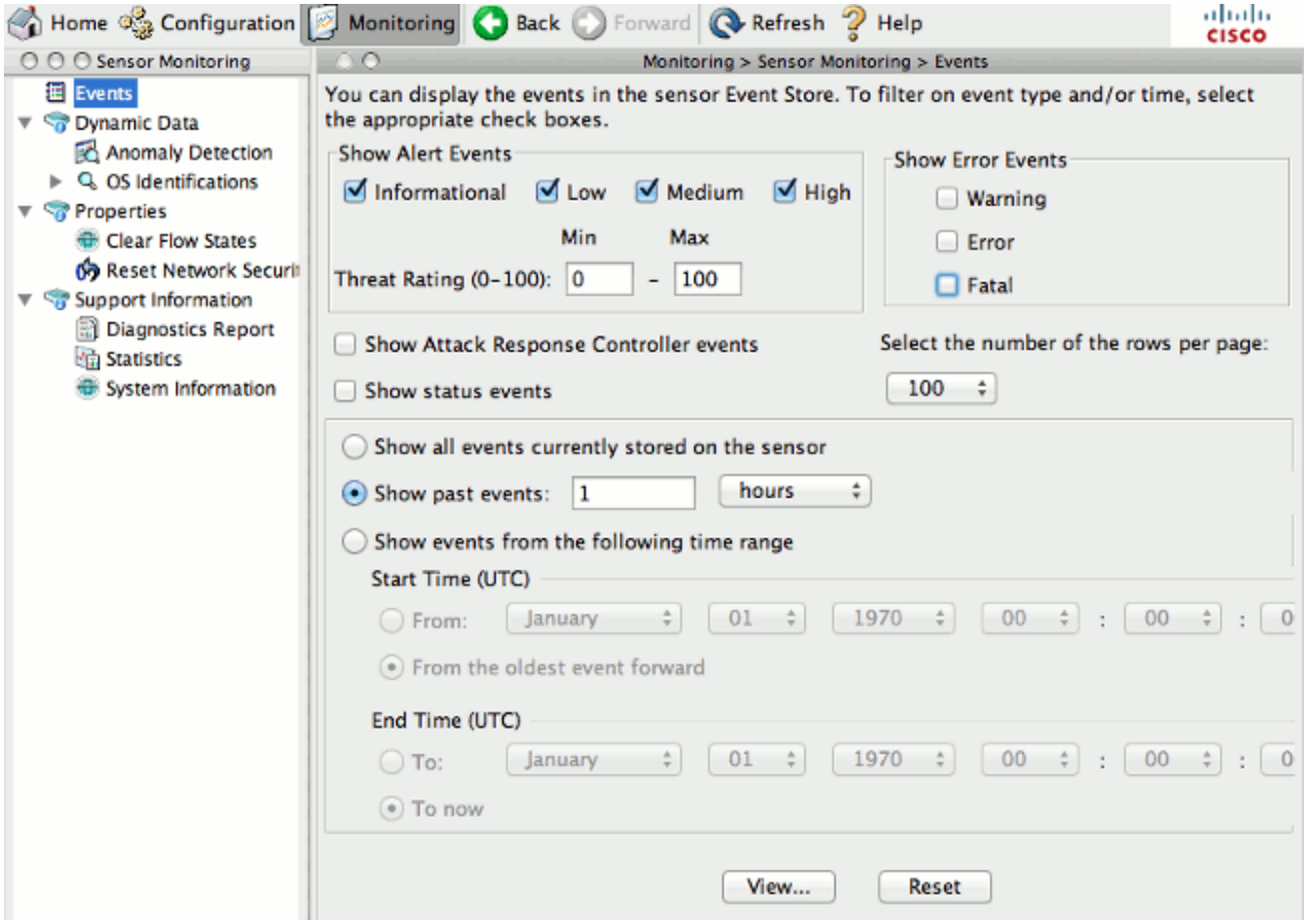
- Verifique que o sensor do sensor tem pelo menos uma relação de detecção atribuída e inspecione o tráfego. Entre ao sensor e incorpore este comando. sensor# **show stat virtual** *!! In the output, find the List of interfaces monitored by this virtual !! sensor line and confirm that at least one (1) 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.*
- Alternativamente, verifique que as relações estão atribuídas a **vs0 no** IDM sob a **configuração** > as **políticas** > as **políticas IPS**.



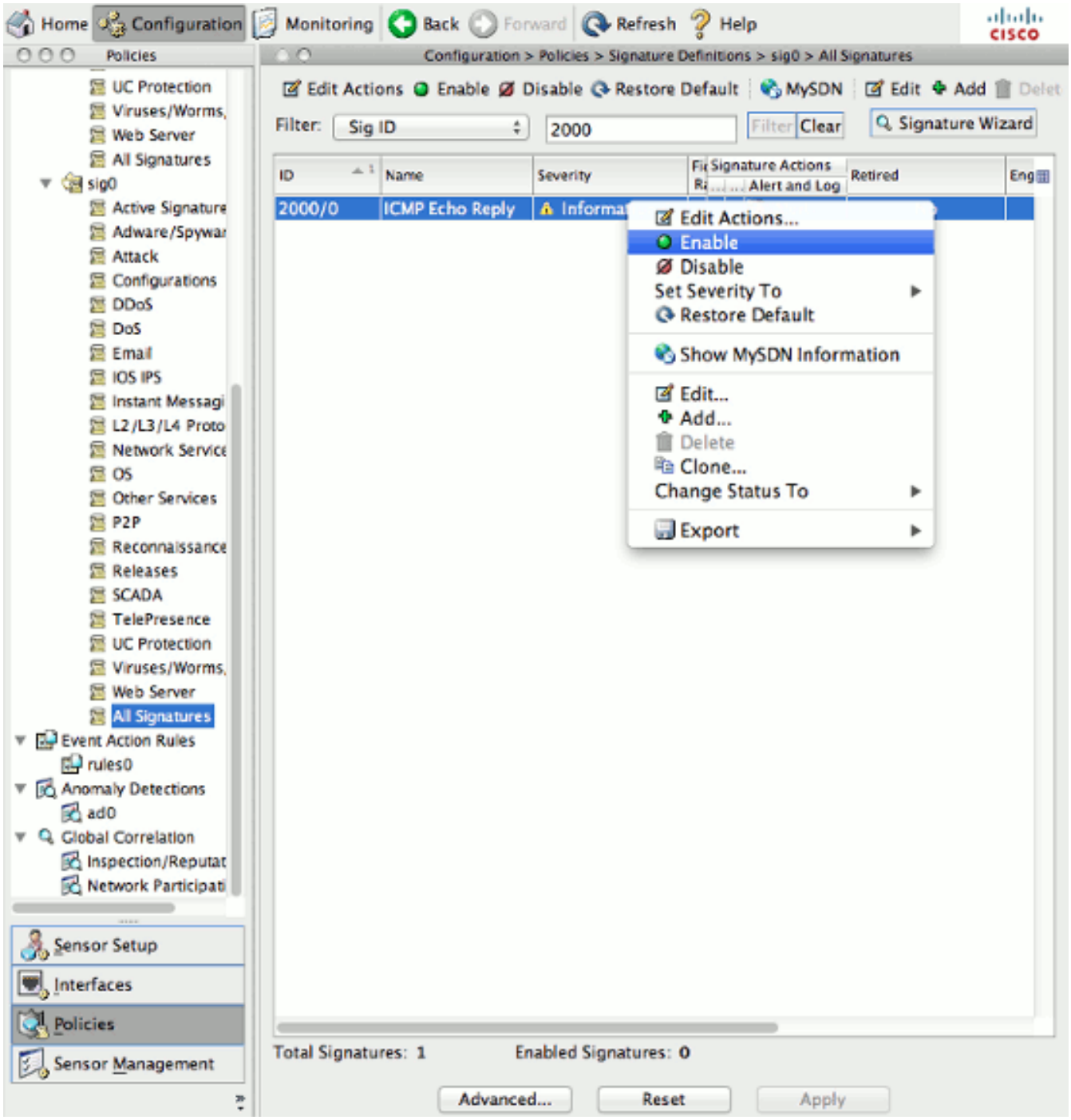
- Incorpore o SSH ao IPS e incorpore o comando da **/porta do slot de interface do indicador do pacote** e verifique-o que o tráfego está considerado na relação.**Nota:** A palavra-chave da ***expressão*** permite que o uso de expressões do **tcpdump** a fim indicar somente o tráfego que combina a expressão usada.`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`

Verifique fogos da assinatura

- Os eventos da assinatura podem ser vistos na seção da monitoração.

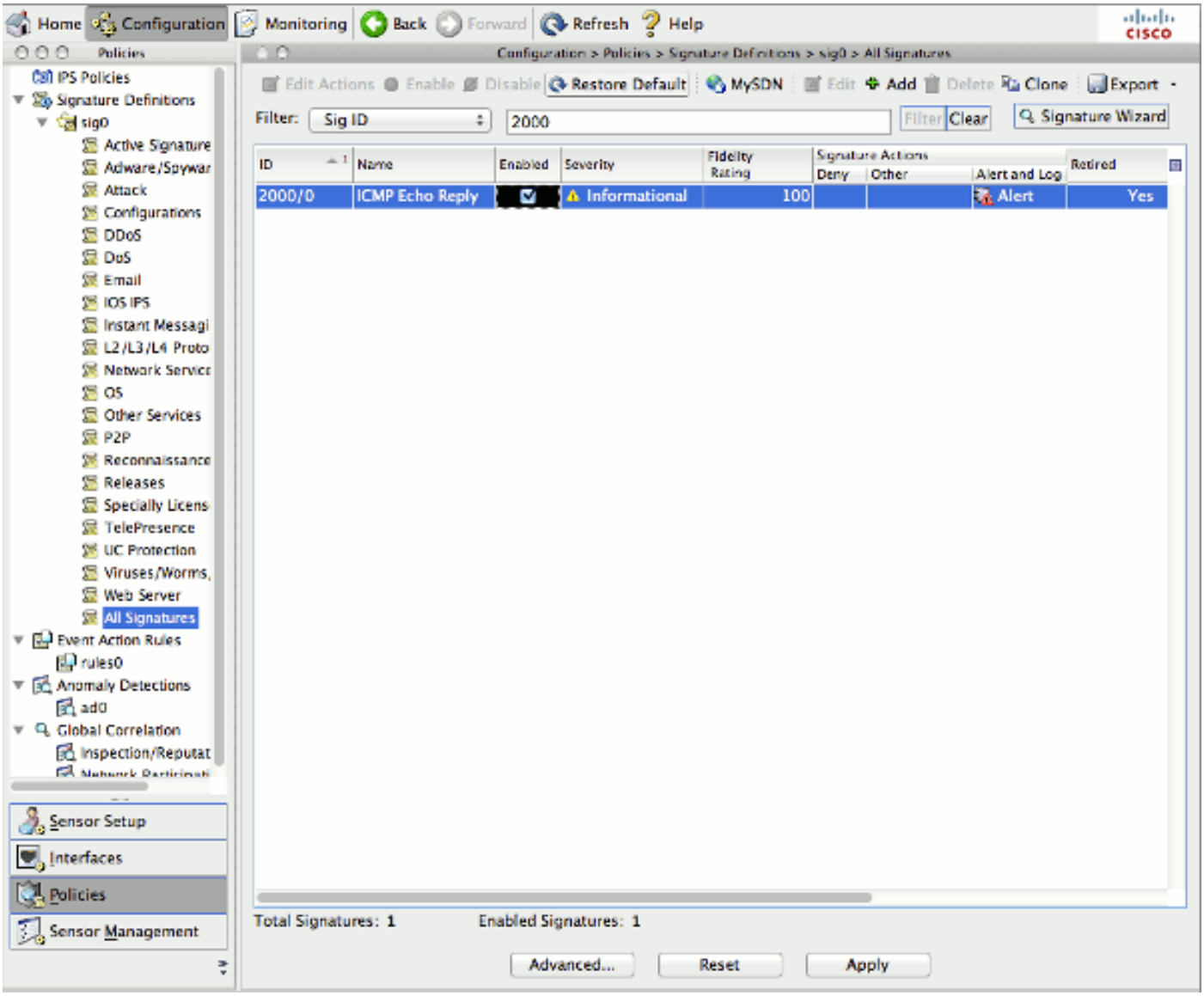


- As assinaturas podem ser alteradas sob a **configuração > todas as assinaturas**.



- Permita as assinaturas 2000/0 e 2004/0 (resposta de eco de protocolo de mensagem de controle de Internet (ICMP) e requisição de eco ICMP); inicie um sibilo através do sensor, e verifique o log de eventos na aba da monitoração.Se o ICMP é obstruído:Para 1107/0, refira o RFC1918 - *Enderece visto.*A fim provocar esta assinatura, o grupo **aposenta-se a falso** e **permite-se de retificar n**esta assinatura e de olhar o IPs nas escalas do RFC 1918 provocar as assinaturas.Estes endereços são 10.0.0.0/8, 172.16.0.0-172.31.255.255, 192.168.0.0/16.Isto não pode ser visto em um SSC-5 porque se exige para que a assinatura sido unretired.Para 3409/0, telnet à porta 80.Com instalação do servidor de Web, a porta 80 está aberta e o telnet é bem sucedido. Quando o telnet for bem sucedido, os fogos do evento no IPS.Um aperto de mão da 3-maneira TCP é exigido para que o sensor siga a conexão de TCP válida. No caso do roteamento assimétrico ou de uma repetição de uma captação do pacote parcial, o tráfego não causa um fogo da assinatura.

Depois que testar está completo, restaure os padrões a todas as assinaturas alteradas:



Informações Relacionadas

- Cenários de configuração do Gerenciamento de IPS em um módulo ips 5500x
- Guia de configuração de CLI do sensor de Sistema de prevenção de intrusões da Cisco para IPS 7.0
- Guia de configuração de CLI do sensor de Sistema de prevenção de intrusões da Cisco para IPS 7.1
- Gerente IPS expresso
- Secure Shell (SSH)
- Suporte Técnico e Documentação - Cisco Systems