Configurando um Cisco Secure IDS Sensor em CSPM

Índice

Introdução

Este documento explica o procedimento usado para configurar um sensor do Cisco Secure Intrusion Detection System (IDS) no Cisco Secure Policy Manager (CSPM). Este documento pressupõe que você instalou o CSPM versão 2.3.1 no seu computador. Versão “eu” permito o gerenciamento de dispositivos IDS (sensors de ferramenta, de ® do Cisco IOS Roteadores, ou IDS blade) em um 6000 Switch do ® do Cisco catalyst. Este documento igualmente supõe que os parâmetros postoffice do IDS estão definidos corretamente. Estes incluem o HOSTID, o ORGID, o HOSTNAME, e o ORGNAME. Observe que, para o host CSPM se comunicar com um Sensor, o ORGID e o ORGNAME devem corresponder ao que está definido no Sensor.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em CSPM 2.3.I e mais tarde.

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.

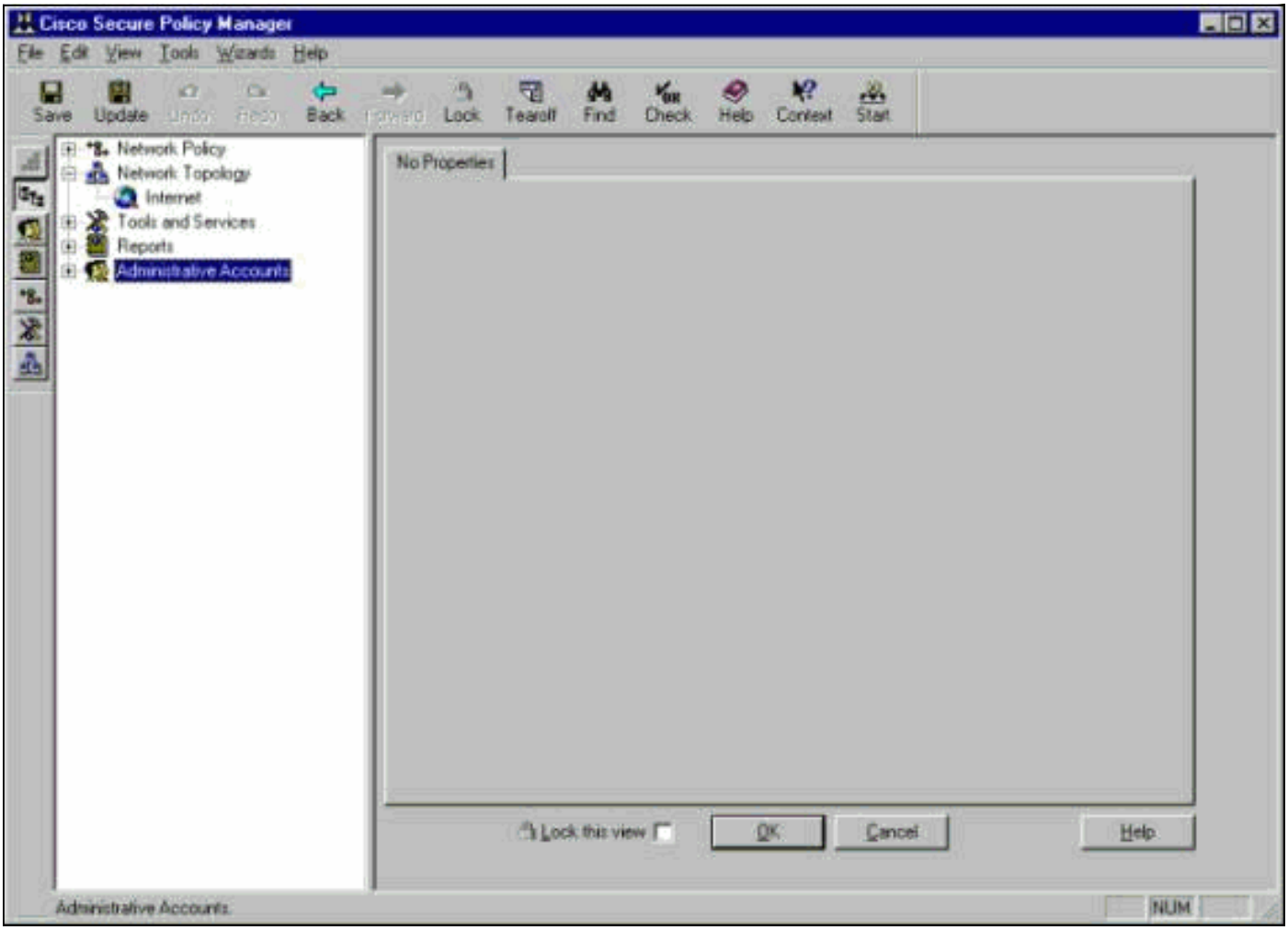
Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configuração

Estas seções explicam o processo usado para configurar um sensor de IDS no CSPM.

Lançamento CSPM e início de uma sessão. Um molde em branco aparece (primeira inicialização) permitindo definir sua rede.



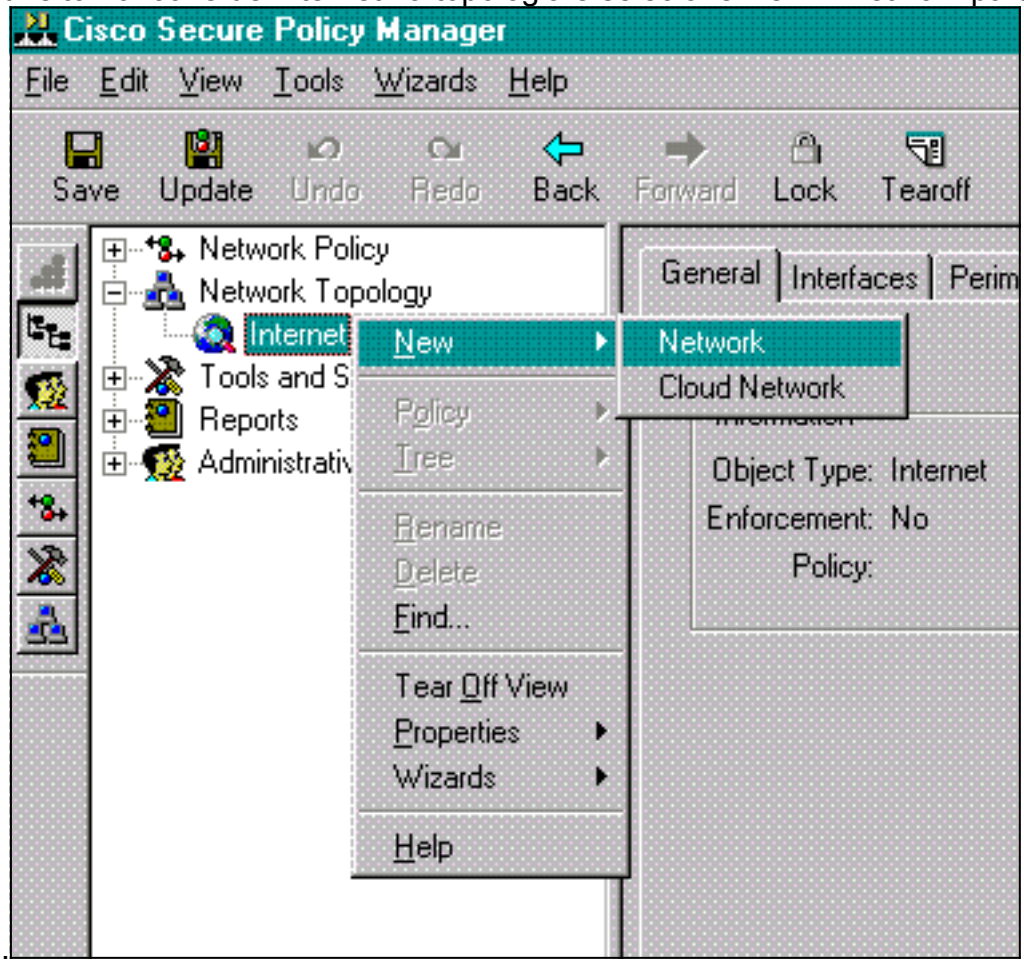
Estas três definições são exigidas na topologia CSPM para IDS.

1. Defina a rede em que a interface de controle do Sensor reside e a rede em que o host de CSPM reside. Se estão na mesma sub-rede, a seguir somente uma rede precisa de ser definida. Defina essa rede primeiro.
2. Defina o host CSPM em sua rede. Sem a definição de host do CSPM, o Sensor não pode ser gerenciado.
3. Defina o Sensor na sua respectiva rede.

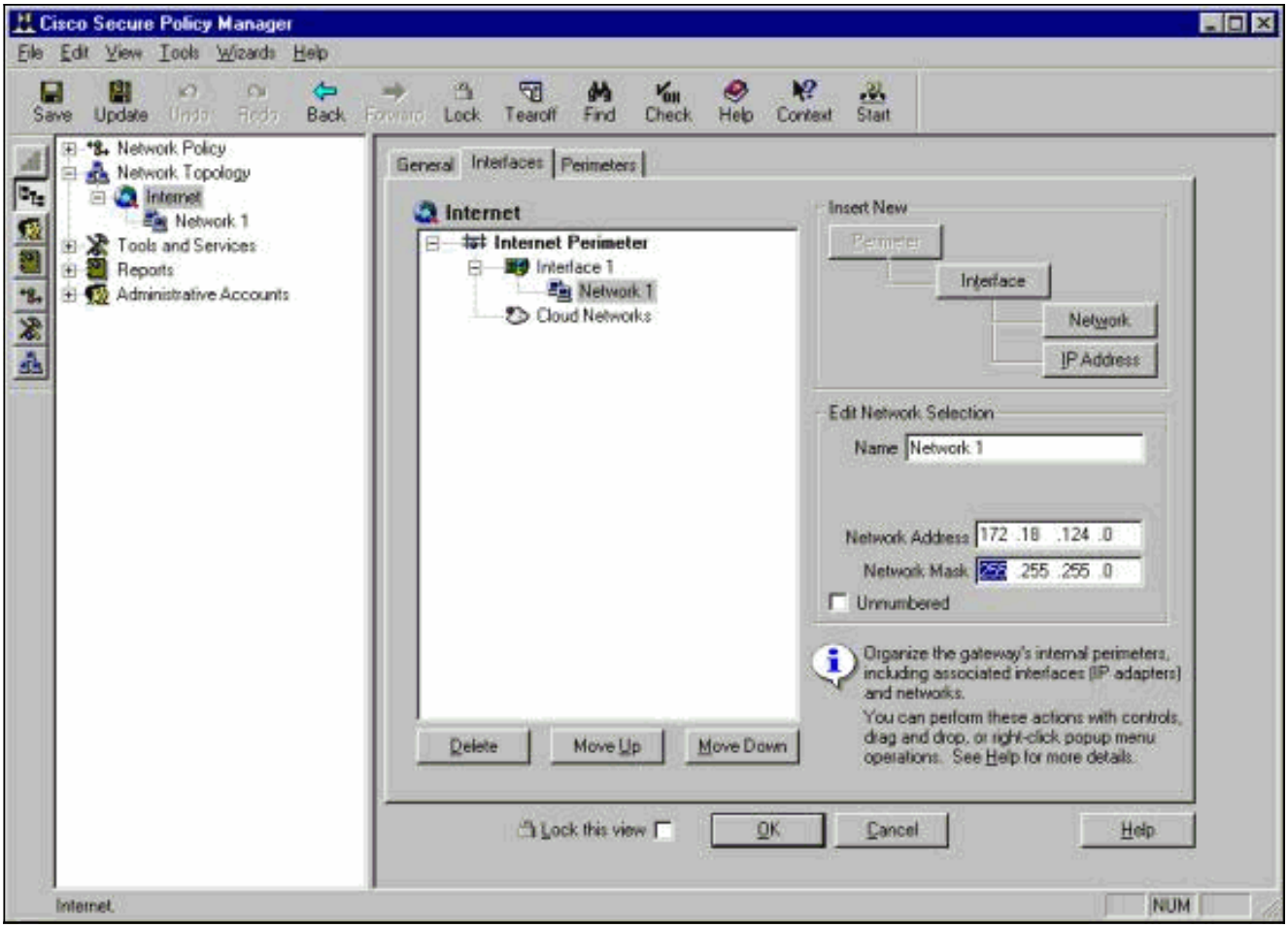
Definir a rede na qual o host CSPM reside

Conclua estes passos:

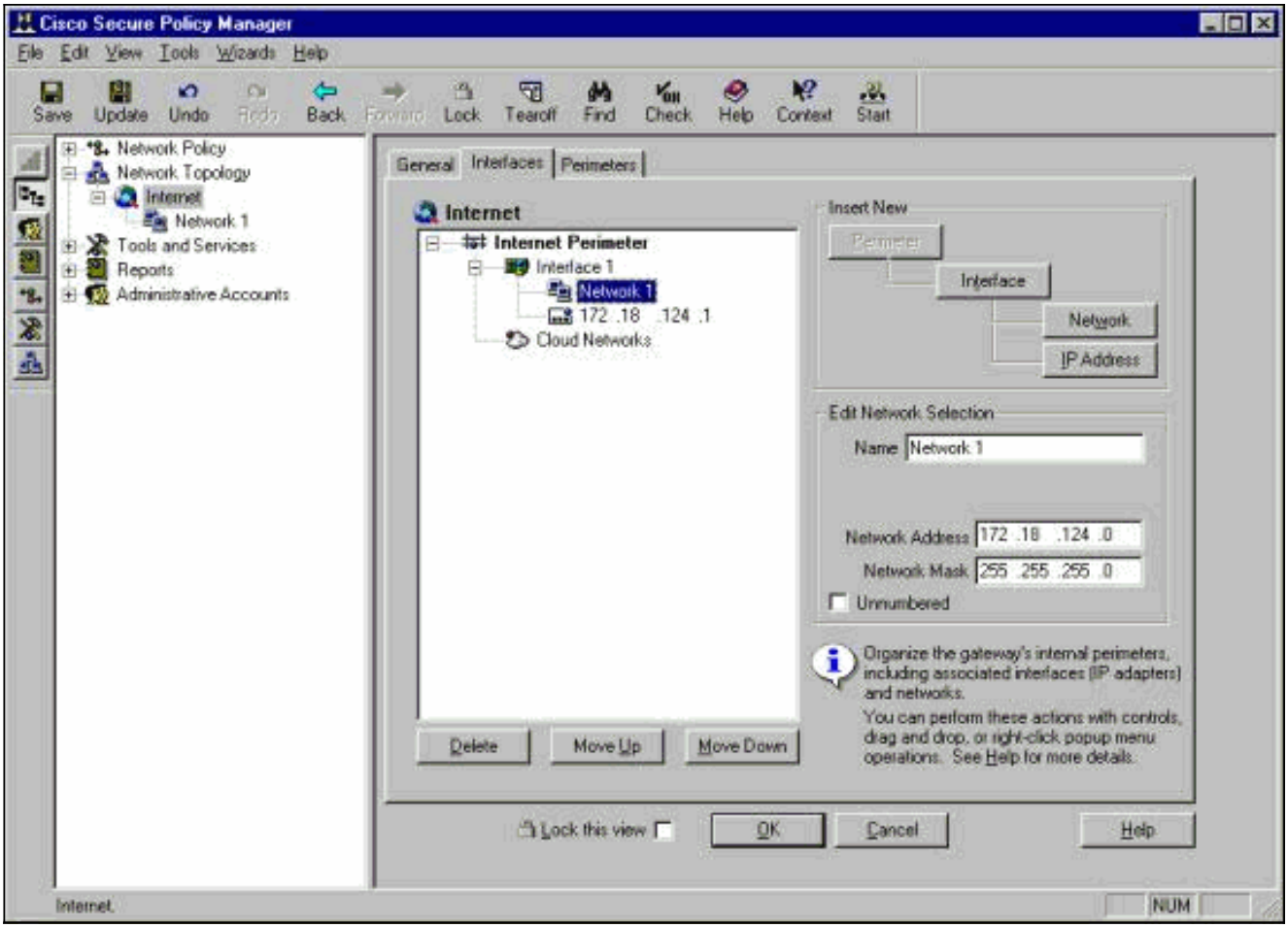
1. Clique com o botão direito no ícone de Internet na topologia e selecione New > Network para criar uma nova rede.



2. No lado direito do painel Network, adicione o nome da nova rede, o endereço da rede e a máscara de rede que será
usada.



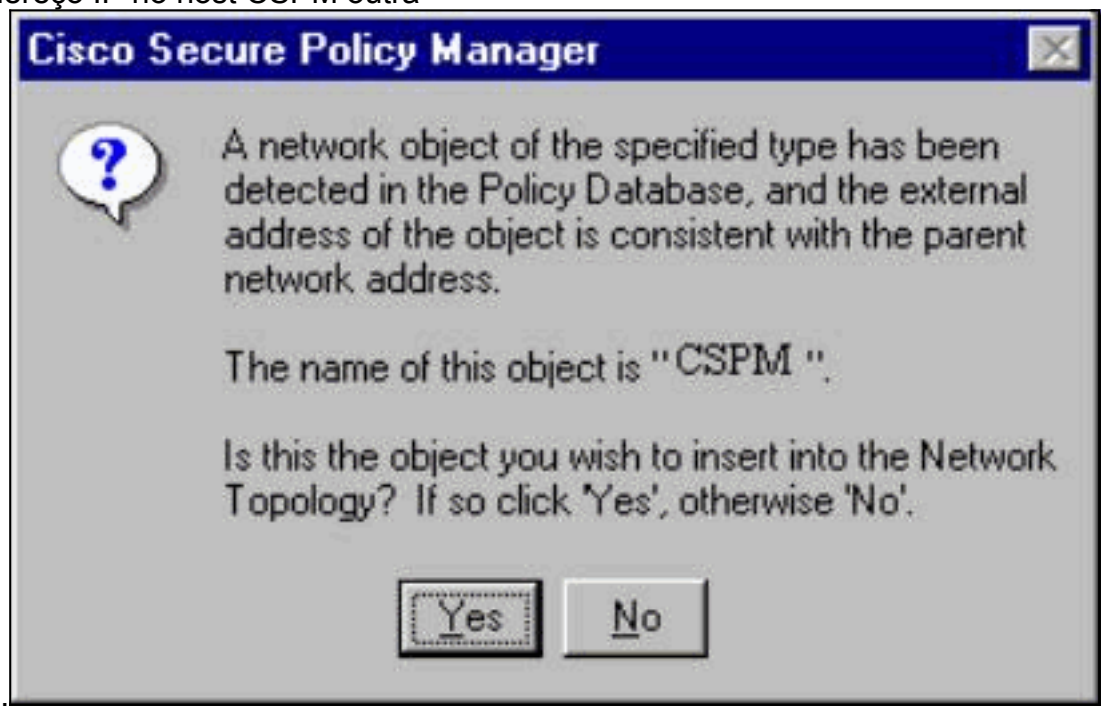
3. Clique no botão IP Address e digite o endereço IP usado pela rede para alcançar a Internet.Normalmente é o gateway padrão para a rede.**Nota:** Quando você controla sensores, o endereço de gateway não tem que necessariamente estar correto desde que o sensor não é enviado a esta informação de gateway padrão. Deve já ser definido no sensor.
4. Clique em **OK**. A rede é adicionada ao mapa de topologia sem nenhuns erros.



Adicionar o host de CSMP

Use este procedimento para adicionar o host CSPM.

1. Na topologia de rede, clicar com o botão direito na rede que você apenas adicionou e **novo** seleto **> host**.O CSPM traz acima uma tela similar a esta. Em caso negativo, a rede que você acabou de definir não será a rede na qual o host CSPM está localizado. Verifique o endereço IP no host CSPM outra vez.

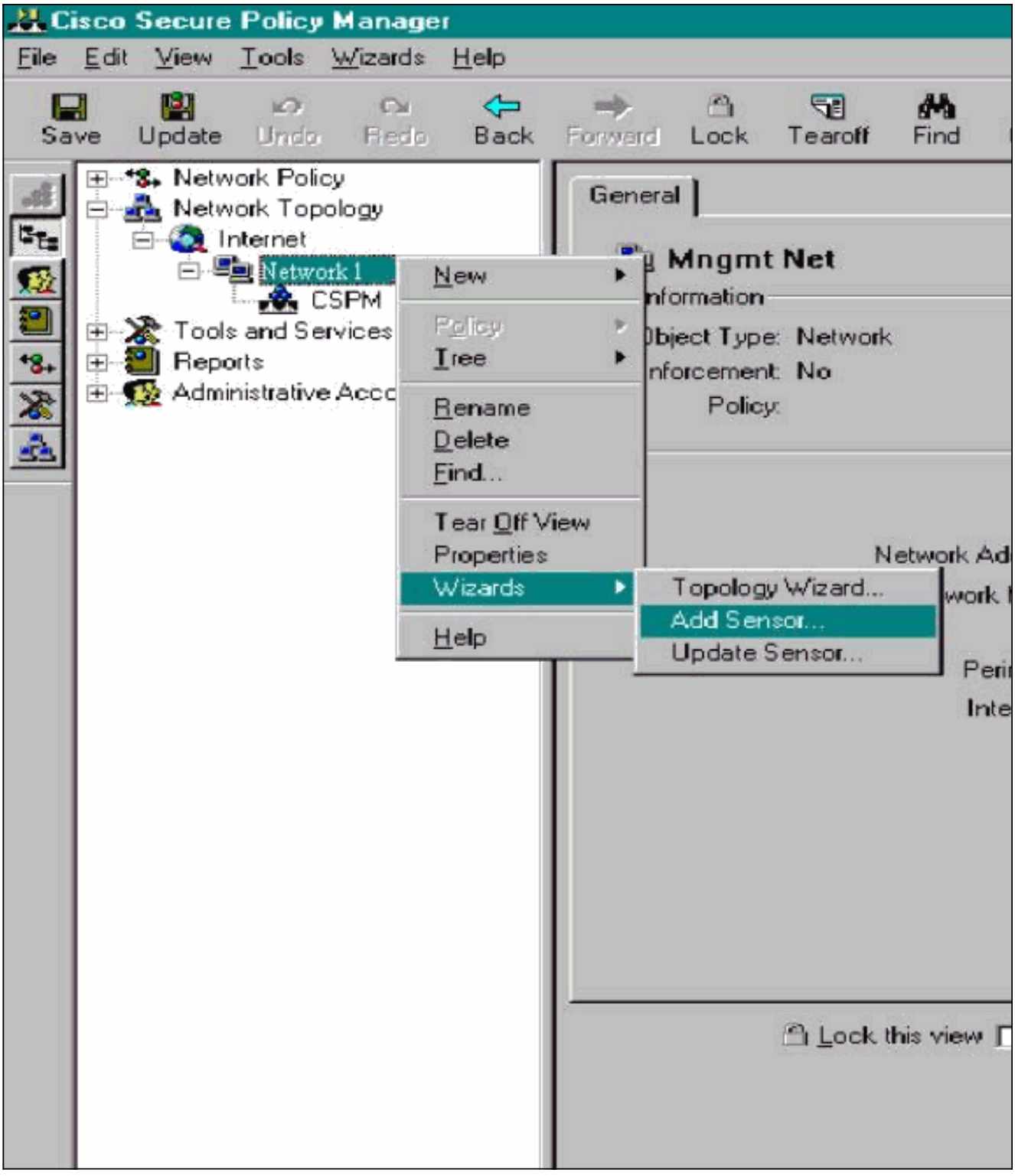


2. Clique em Sim para instalar o host CSPM na topologia.
3. Verifique se as informações na tela Geral para o host CSPM estão ok.
4. Clique em OK na tela General do host CSPM.

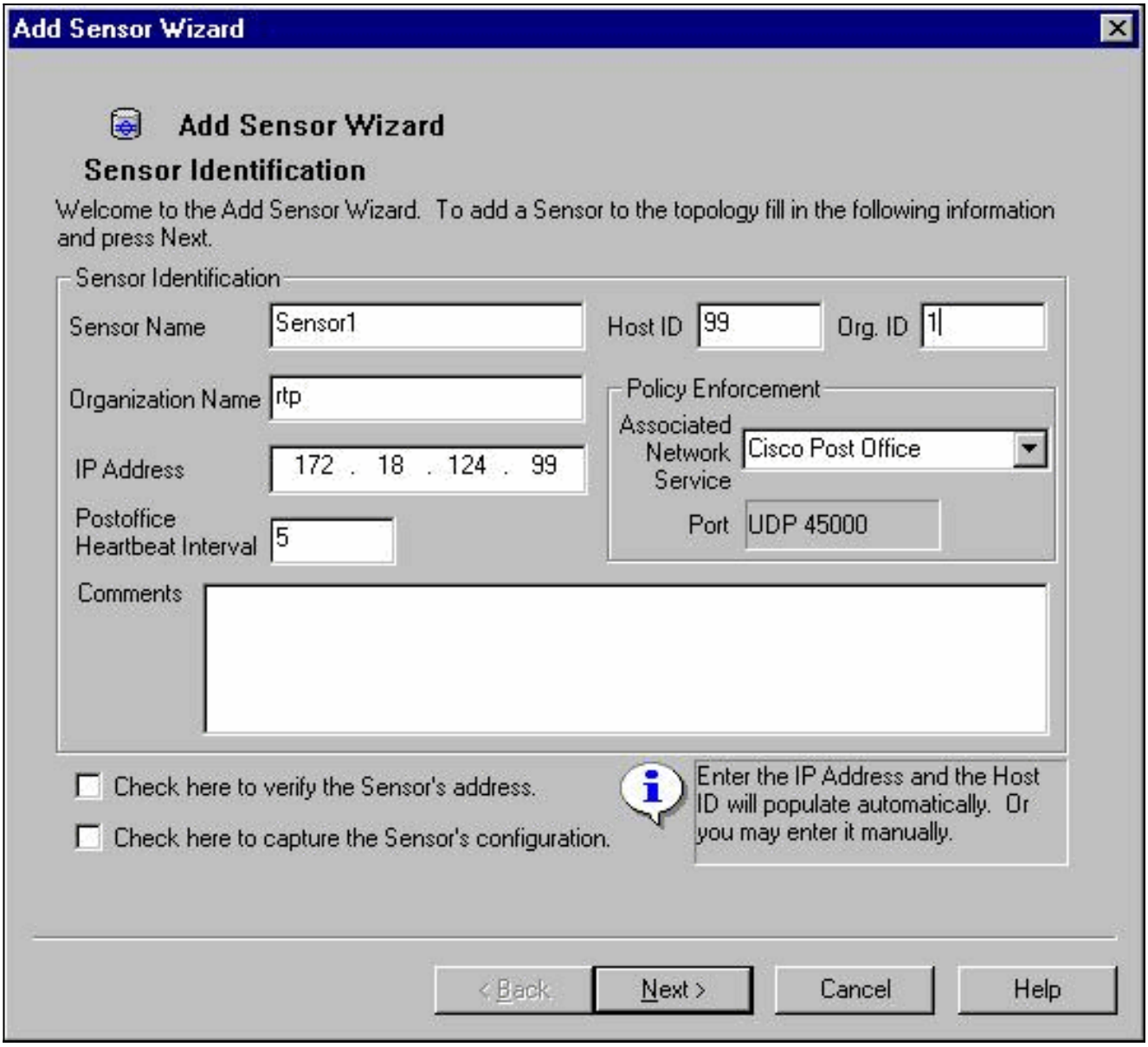
Adicione o dispositivo sensor

Use este procedimento para adicionar o dispositivo de sensor.

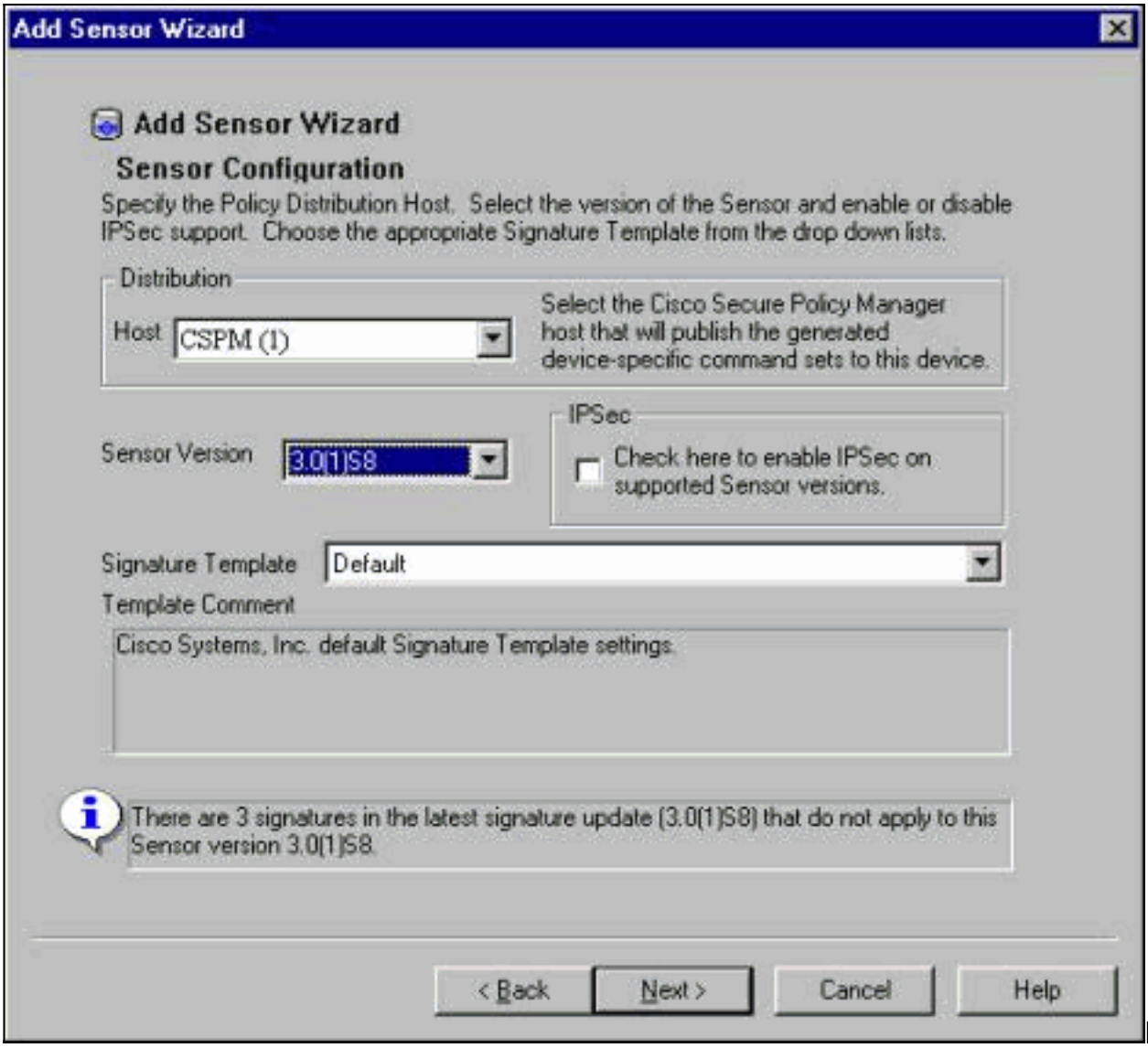
1. Clicar com o botão direito na rede em que seu sensor reside e **sensor** seleto do > Add dos **assistentes**.**Nota:** Se o host CSPM e a interface de controle de seu sensor não estão na mesma rede, defina a rede em que seu sensor
reside.



2. Digite os parâmetros corretos de postoffice para o Sensor.



3. Clique em Check here (Verificar aqui) para verificar a caixa de endereço do Sensor.**Nota:** Se isto é a primeira vez você está estabelecendo este sensor, você não quer capturar a configuração do sensor. Se você configurou previamente este sensor em outra parte através de um UNIX Diretor ou de um outro host CSPM e fez alterações de configuração às assinaturas de sensores, a seguir você quer capturar a configuração do sensor.
4. Clique em Next (Avançar) para definir as versões de assinatura do Sensor. Você pode igualmente emitir o **comando nrvers** verificar isto no sensor.



Nota: Se o CSPM não tem a versão do sensor correta que você está executando em seu sensor, atualize as assinaturas em seu host CSPM. Consulte Download do software (somente para clientes registrados) para obter atualizações.

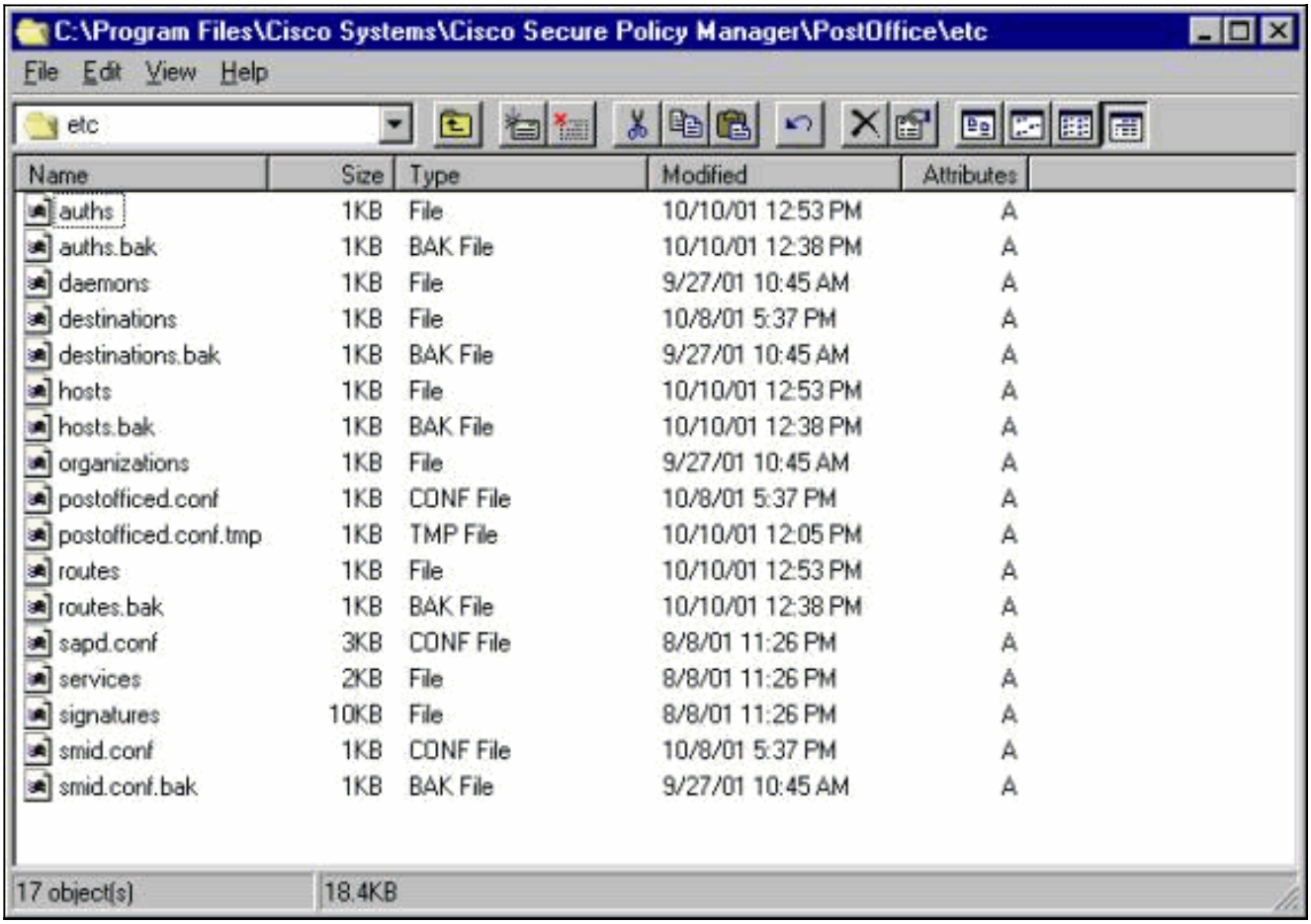
5. Clique o **botão Next Button** para continuar.
6. Clique o **revestimento** para terminar a instalação do sensor na topologia.
7. A partir do menu principal do CSPM, selecione File > Save and Update para compilar as informações digitadas na topologia no CSPM. Observe que essa etapa é necessária para iniciar o protocolo postoffice no host CSPM.
8. Verifique que tudo trabalha registrando em seu sensor como o usuário do netrangr.
9. Execute o comando nrconns.`>nrconns Connection Status for gacy.rtp cspm.rtp Connection 1: 172.18.124.106 45000 1 [Established] sto:0004 with Version 1 netrangr@gacy:/usr/nr >`

   Nota: Se o sensor e o host CSPM não se estão comunicando, a saída similar a esta aparece pelo contrário:`netrangr@gacy:/usr/nr`

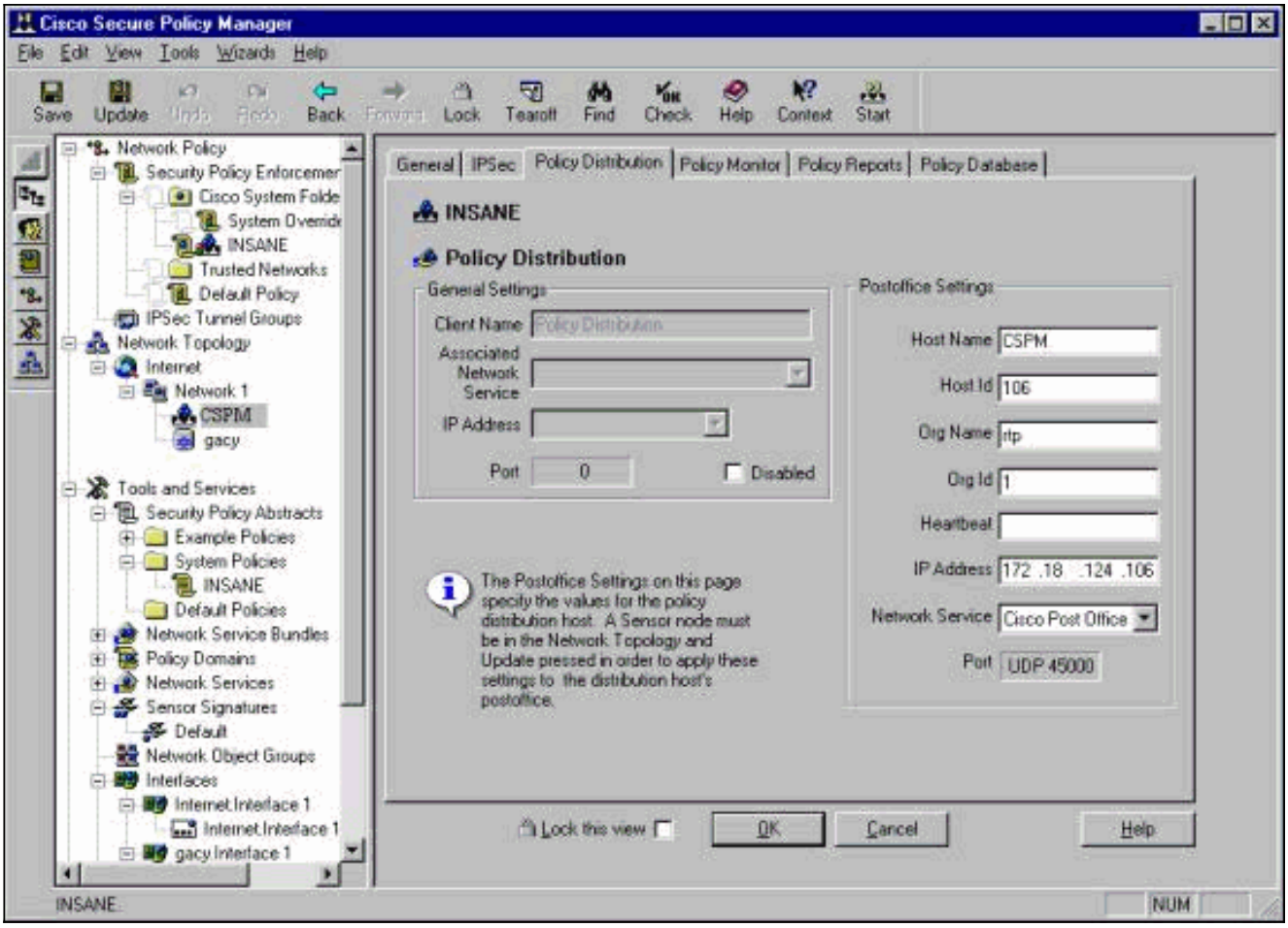
   `>nrconns Connection Status for gacy.rtp insane.rtp Connection 1: 172.18.124.194 45000 1 [SynSent] sto:5000 syn NOT rcvd! netrangr@gacy:/usr/nr` Se este é o caso, consiga um farejador de rastreamento ver se os ambos os lados estão enviando pacotes UDP 45000. Os dispositivos IDS utilizam UDP 45000 para se comunicarem entre si. Para testar isto no sensor, na **SU** para enraizar e (segundo que sensor você tem) para executar a **espião - porta 45000 d iprb1** (para um sensor IDS 4210) e **espião - porta 45000 do iprb0 d** (para algum outro modelo do sensor).Use o **<control-c>** para estoirar de uma sessão da espião.Esta saída aparece se não há nenhuma comunicação entre o sensor e o

CSPM:`netrangr@gacy:/usr/nr`

`>su - Password: Sun Microsystems Inc. SunOS 5.8 Generic February 2000 # snoop -d spwr0 port 45000 Using device /dev/spwr (promiscuous mode) 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 172.18.124.100 -> 172.18.124.106 UDP D=45000 S=45000 LEN=52 ^C#` Na saída acima, o sensor envia pacotes UDP 45000, mas não recebe alguns. Uma configuração correta produz a saída similar a esta:`# snoop -d spwr0 port 45000 Using device /dev/iprb (promiscuous mode) 172.18.124.106 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.106 UDP D=45000 S=45000 LEN=56 172.18.124.142 -> gacy UDP D=45000 S=45000 LEN=56 gacy -> 172.18.124.194 UDP D=45000 S=45000 LEN=56` Na saída acima, o tráfego UDP 45000 vai nos ambos sentidos.Se os pacotes UDP 45000 fluem nos ambos sentidos e a saída dos **nrconns no** sensor ainda diz que não há nenhuma conexão estabelecida, os parâmetros de postoffice no sensor e no host CSPM não combinam.Para verificar os parâmetros de postoffice no CSPM hospede manualmente:Use o Windows Explorer para navegar a onde você tem o CSPM instalado na máquina de NT.



Edite o host, rota, e os arquivos organizacionais com escrevem ou Wordpad (não use o bloco de notas porque o formato será corrompido).Verifique se esses arquivos parecem corretos para sua instalação. Se alguns dos valores não estão corretos, edite-os e recarregue-o seu computador de NT usando estas etapas:Clique sobre o **ícone CSPM na** topologia de rede.Clique sobre a aba da distribuição da política para incorporar seus parâmetros de postoffice.Salve e atualize suas alterações.Reinicialize o computador do NT.



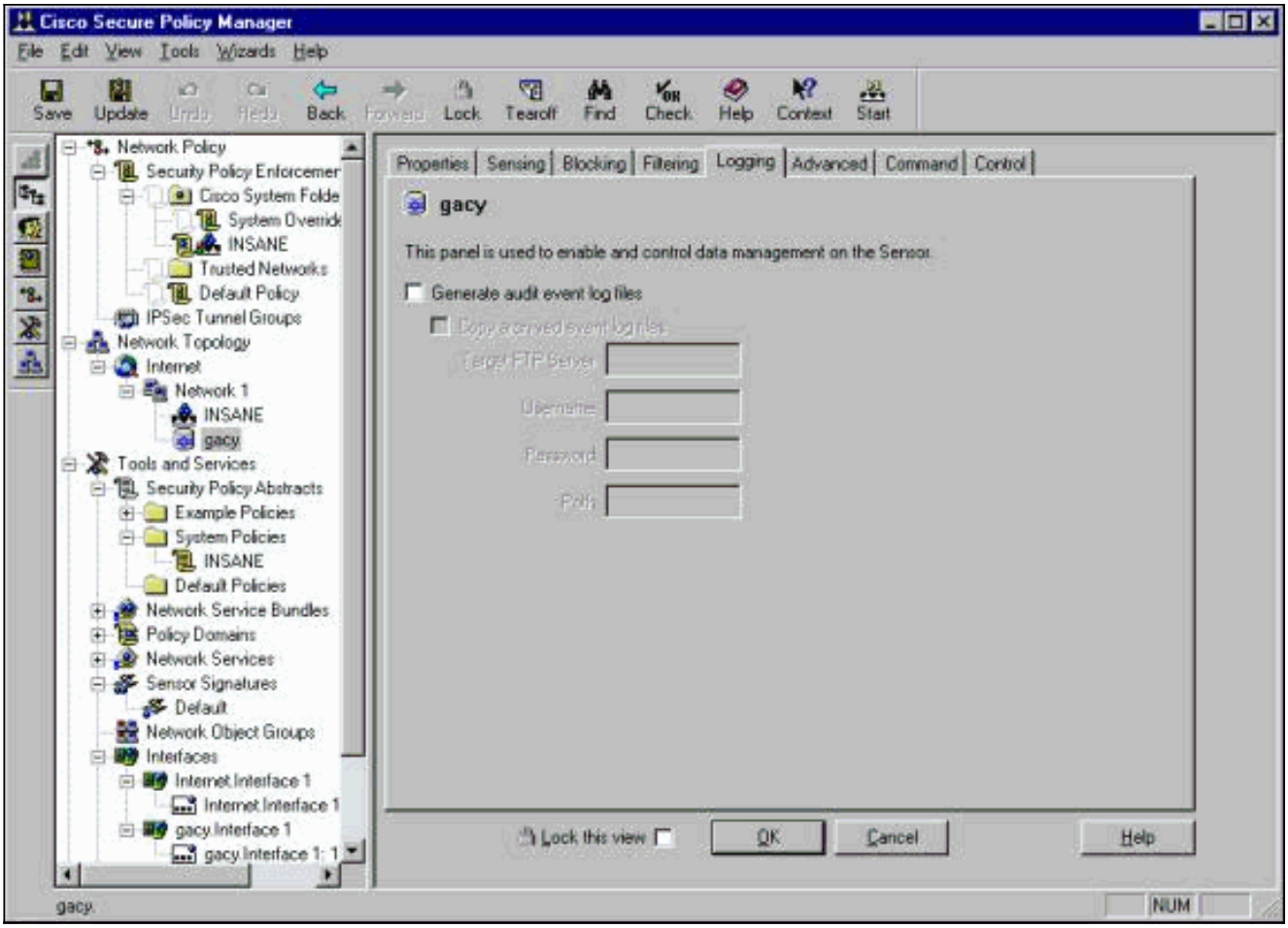
Configure o sensor

Depois que a configuração salvar no CSPM, configurar o sensor. A fim fazer isto, ajuste primeiramente o sensor para escrever os alarmes que consideram a seu próprio log. Ajuste então o sensor “para aspirar” na relação correta.

Gravar alarmes no registro

Use este procedimento para escrever alarmes ao log.

1. Clique na caixa Generate audit event log files para solicitar que o sensor envie os alarmes para os registros locais.Igualmente envia alarmes à caixa CSPM à revelia depois que você lhe abaixa uma configuração
   para.

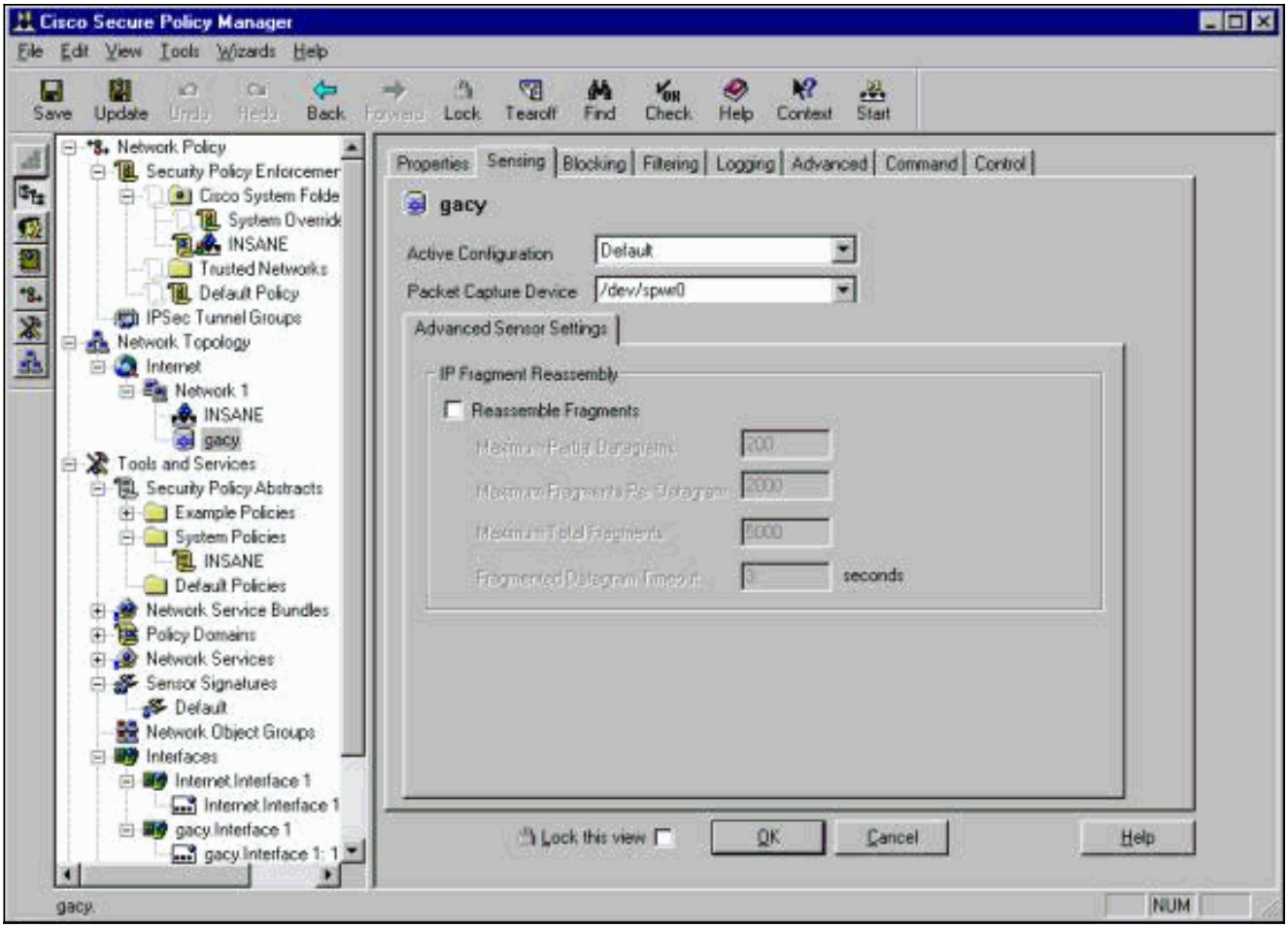


2. Clique em OK para continuar.

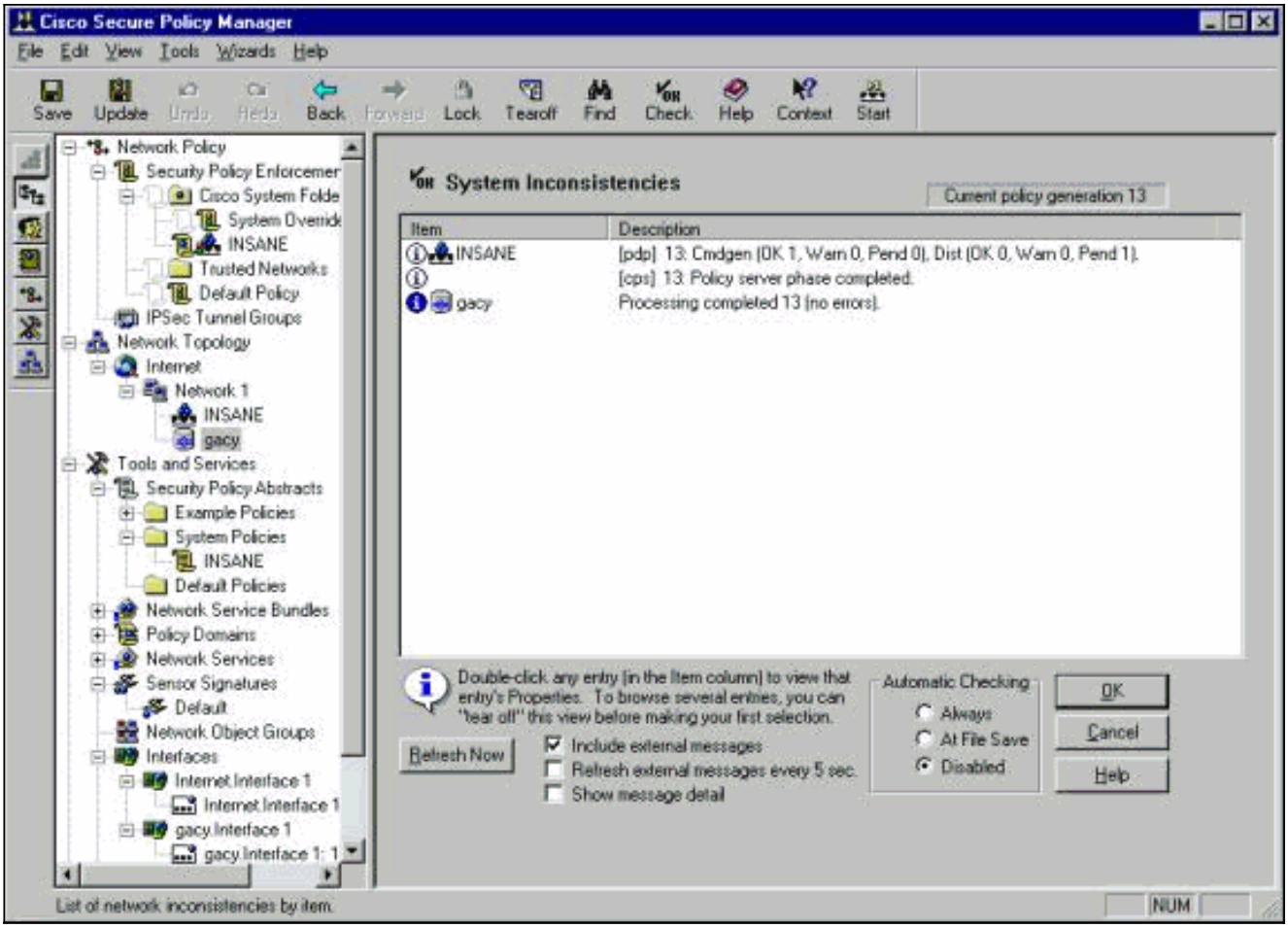
Ajuste o sensor “para aspirar”

Use este procedimento para ajustar o sensor “para aspirar”.

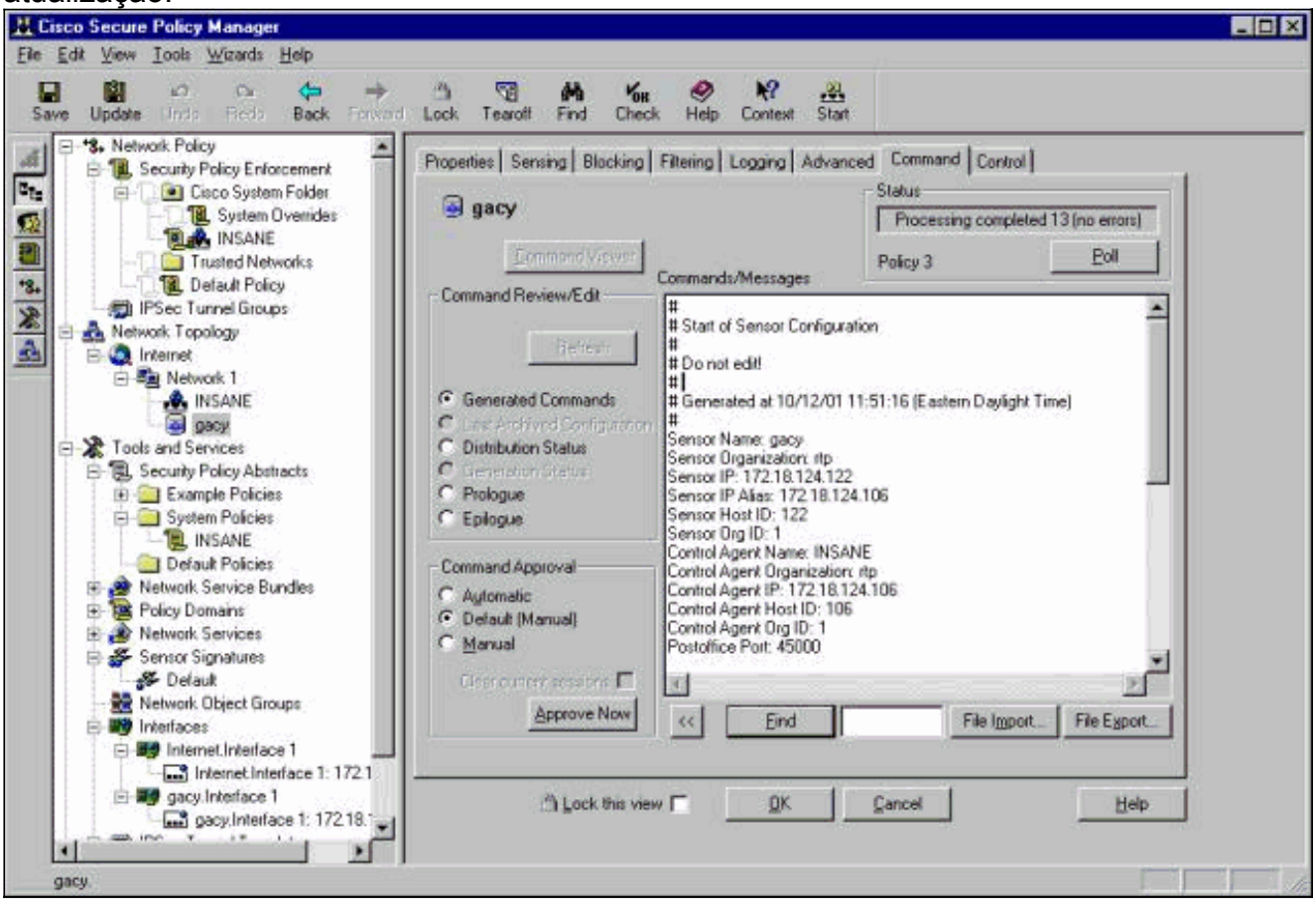
1. Selecione o sensor na topologia CSPM e clique na guia Sensing.
2. Defina o dispositivo de captura de pacote:iprb0 - para um sensor IDS 4210spwr0 - para algum outro modelo do
   sensor



3. Clique em OK para continuar.
4. Clique no ícone Update na barra de menus do CSPM para atualizar o CSPM com as informações.**Nota:** Se tudo vai bem, uma tela similar a esta aparece. Observe que não há nenhum erro em vermelho. Os avisos amarelos estão normalmente corretos.

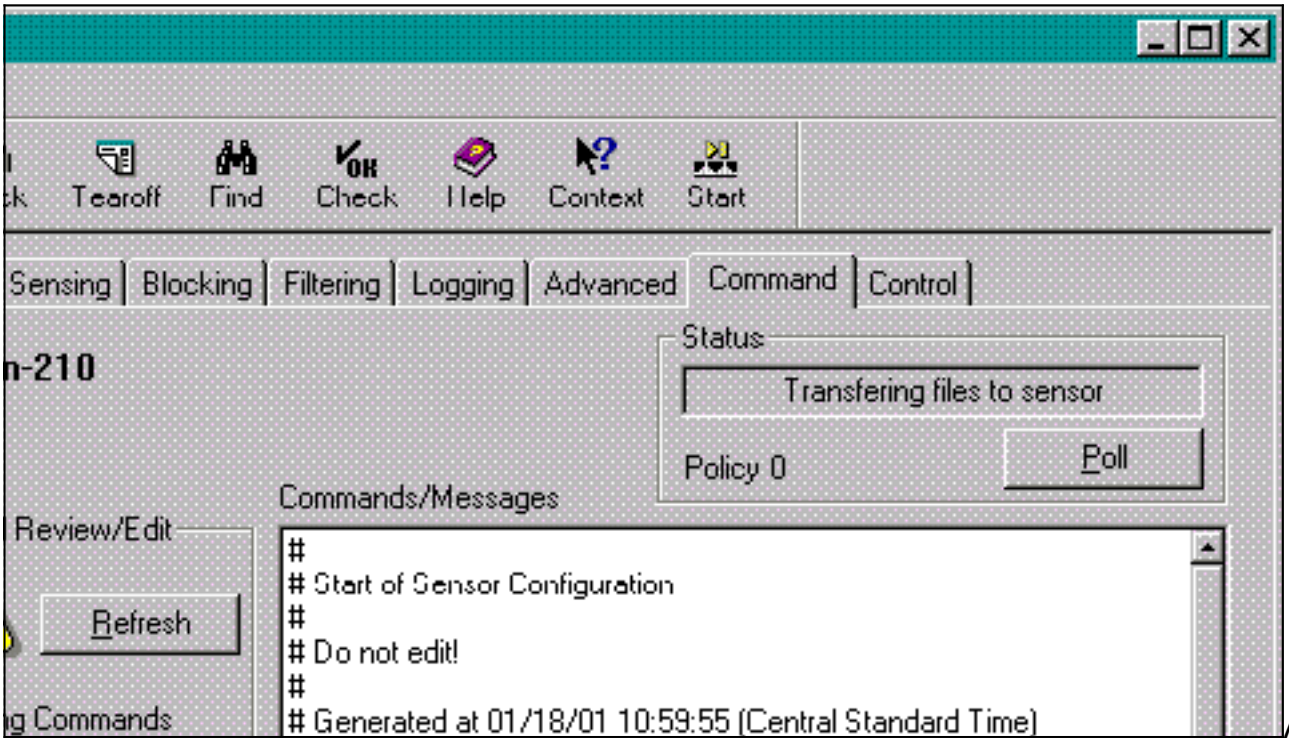


5. Selecione o sensor na topologia da rede e clique na guia Command para lhe enviar a configuração de atualização.

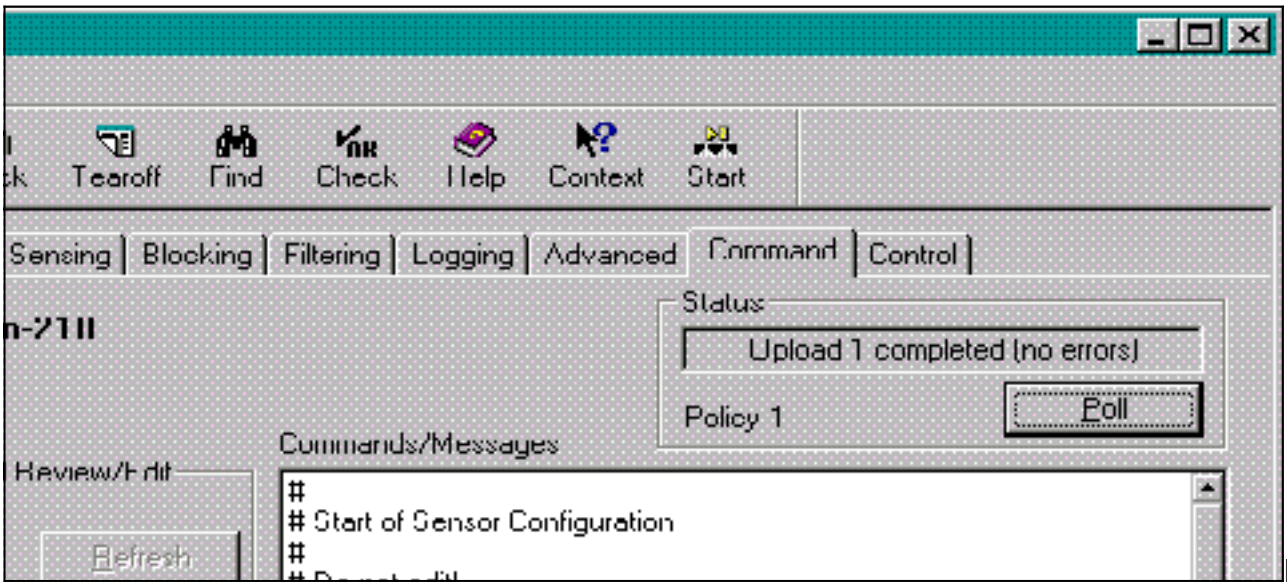


6. Clique o **botão Approve Now Button** para enviar a configuração ao

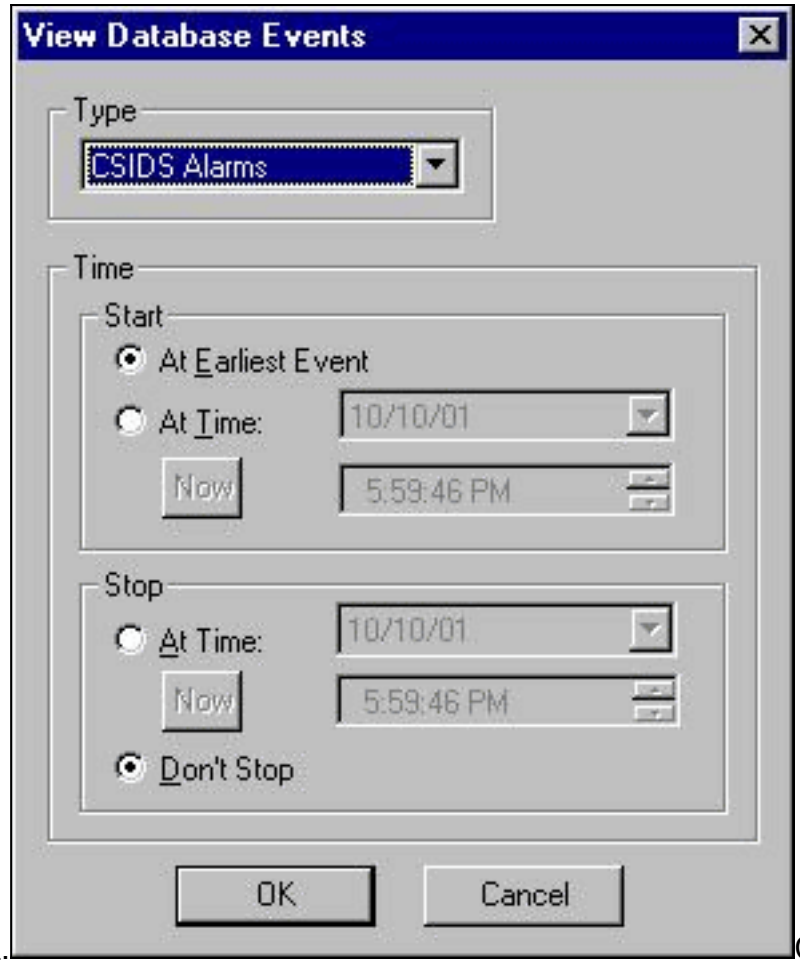
sensor.



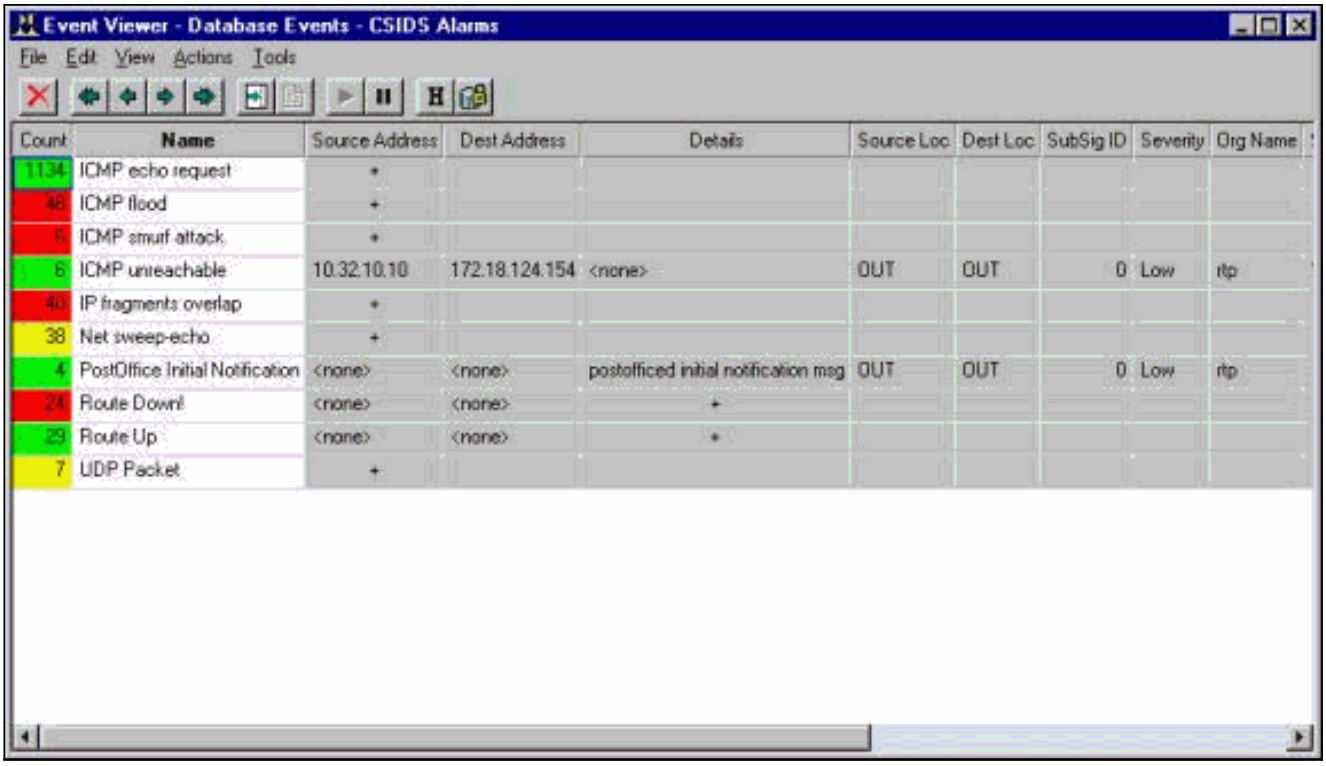
A placa do estado indica da “a mensagem terminada **<#>** transferência de arquivo pela rede”. Isto indica um processo válido e completo de transferência. O sensor agora é atualizado e deve agora ser executado normalmente.Se o sensor não estiver funcionando corretamente, volte para ele e verifique a saída do comando nrconns para certificar-se de que a conexão entre o host CSPM e o sensor esteja
estabelecida.



D epois que isso estiver concluído, você pode procurar por alarmes que o Sensor envia para o host de CSPM no Event Viewer. Para ver o visualizador de eventos, das **ferramentas do** menu principal CSPM **>** dos **eventos >** do **base de dados** seletos do **sensor da**



vista. Clique em OK para exibir a janela do banco de dados de eventos. Sua tela variará segundo os alarmes que você pode obter.



Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	SubSig ID	Severity	Org Name
1134	ICMP echo request	*							
46	ICMP flood	*							
5	ICMP smurf attack	*							
6	ICMP unreachable	10.32.10.10	172.18.124.154	<none>	OUT	OUT	0	Low	ntp
40	IP fragments overlap	*							
38	Net sweep-echo	*							
4	PostOffice Initial Notification	<none>	<none>	postofficed initial notification msg	OUT	OUT	0	Low	ntp
24	Route Down!	<none>	<none>	*					
29	Route Up	<none>	<none>	*					
7	UDP Packet	*							

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems