Een Cisco Secure IDS-sensor in CSPM configureren

Inhoud

Inleiding

Dit document legt de procedure uit die wordt gebruikt om een Cisco Secure Inbraakdetectiesysteem (IDS)-sensor (Cisco Secure Policy Manager (CSPM) te configureren. Bij dit document wordt ervan uitgegaan dat u CSPM versie 2.3.I op uw computer hebt geïnstalleerd. Versie "I" maakt het beheer mogelijk van IDS-apparaten (toevoersensoren, Cisco IOS® routers of IDS-blades) in een Cisco Catalyst® 6000 switch. Dit document gaat er ook van uit dat de IDS-postoffsparameters correct zijn gedefinieerd. Hieronder vallen HOSTID, ORGID, HOSTNAME en ORGNAME. Let erop dat de CSPM-host voor communicatie met een sensor de ORGID en ORGNAME overeenkomt met wat op de Sensor is gedefinieerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op CSPM 2.3.I en later.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

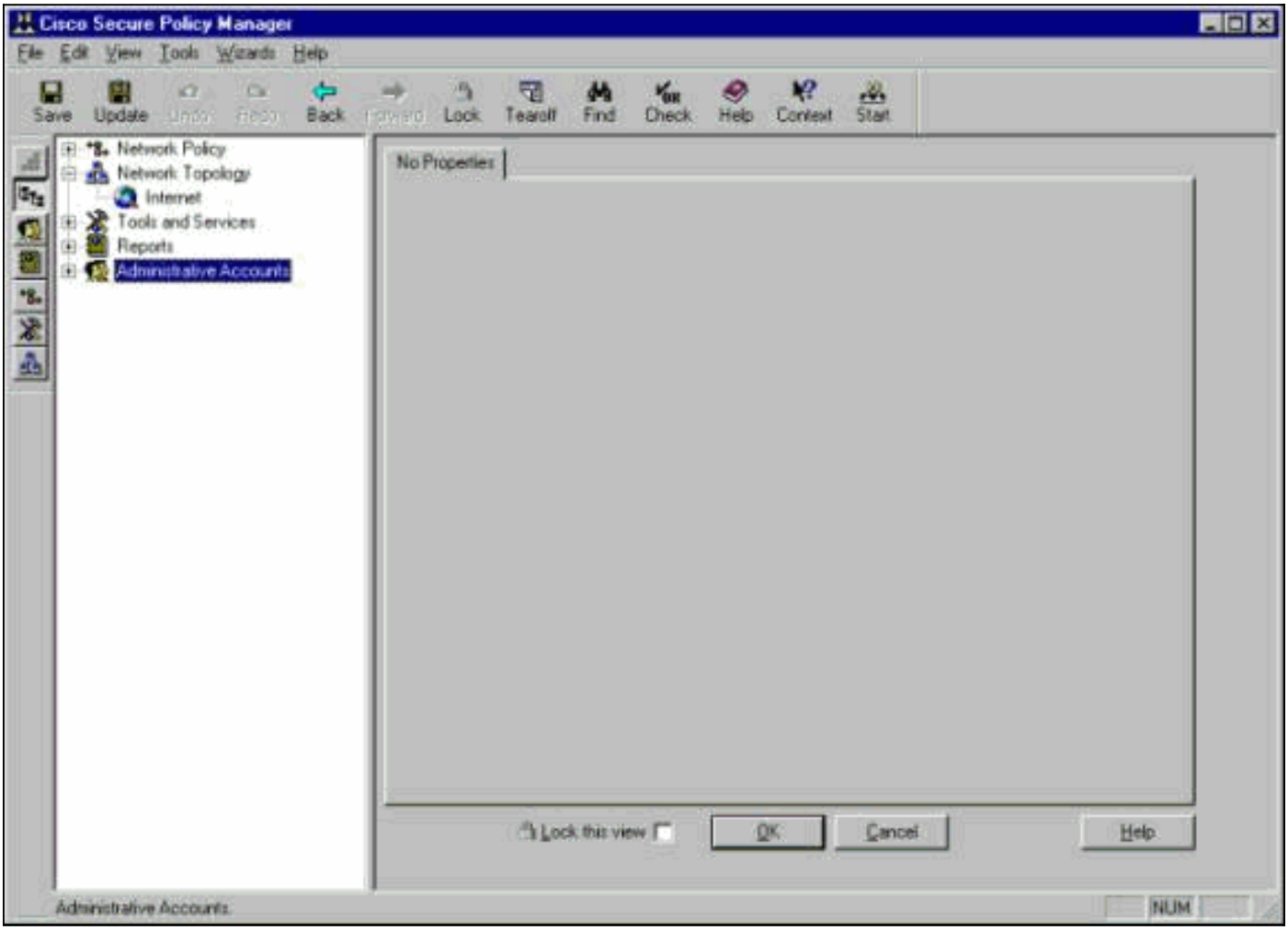
Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configuratie

In deze secties wordt het proces uitgelegd dat wordt gebruikt om een IDS-sensor in CSPM te configureren.

Start CSPM en log in. Er verschijnt een blancosjabloon (eerste lancering) waarmee u uw netwerk kunt definiëren.



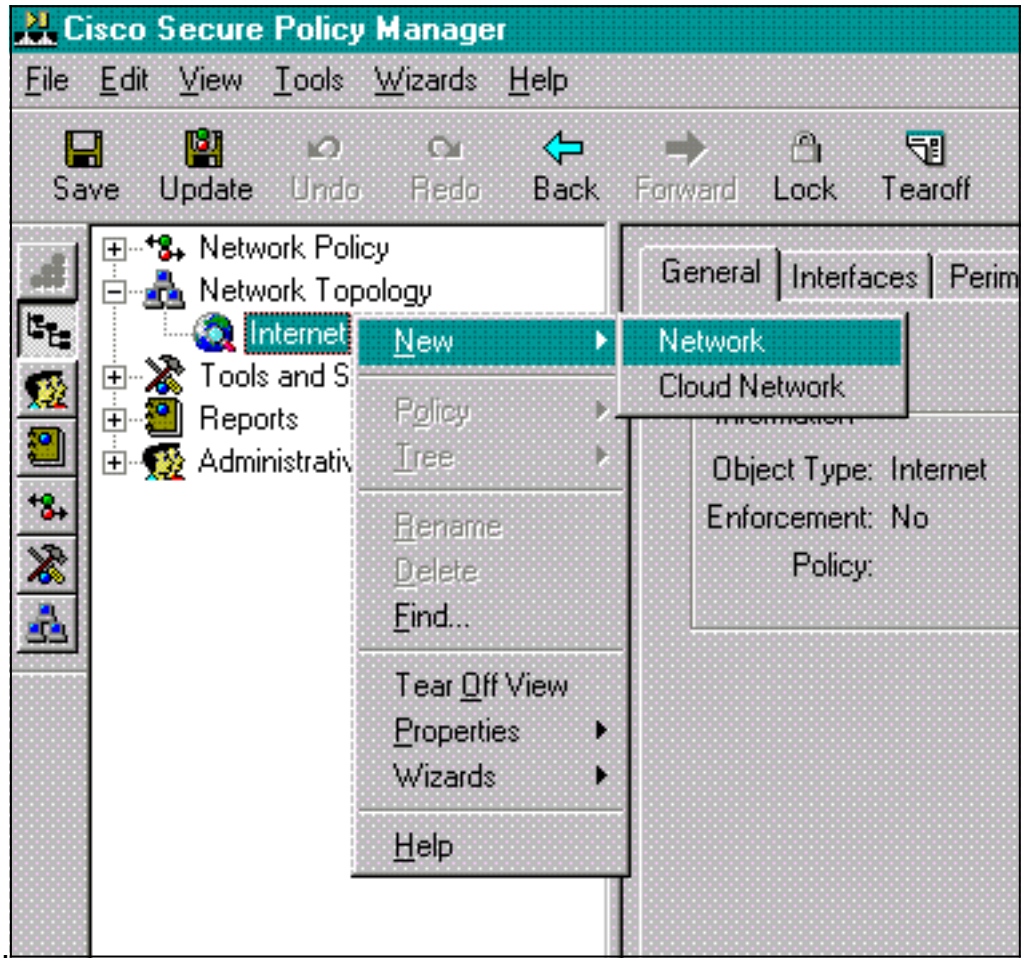
Deze drie definities zijn vereist in de CSPM-topologie voor IDS.

1. Bepaal het netwerk waarin de controle interface van de Sensor en het netwerk waar de gastheer CSPM verblijft. Als ze op hetzelfde net zijn, hoeft slechts één netwerk te worden gedefinieerd. Defineert eerst dit netwerk.
2. Defineert de CSPM-host in het netwerk. Zonder de CSPM host-definitie kan de sensor niet worden beheerd.
3. Defineer de sensor in zijn netwerk.

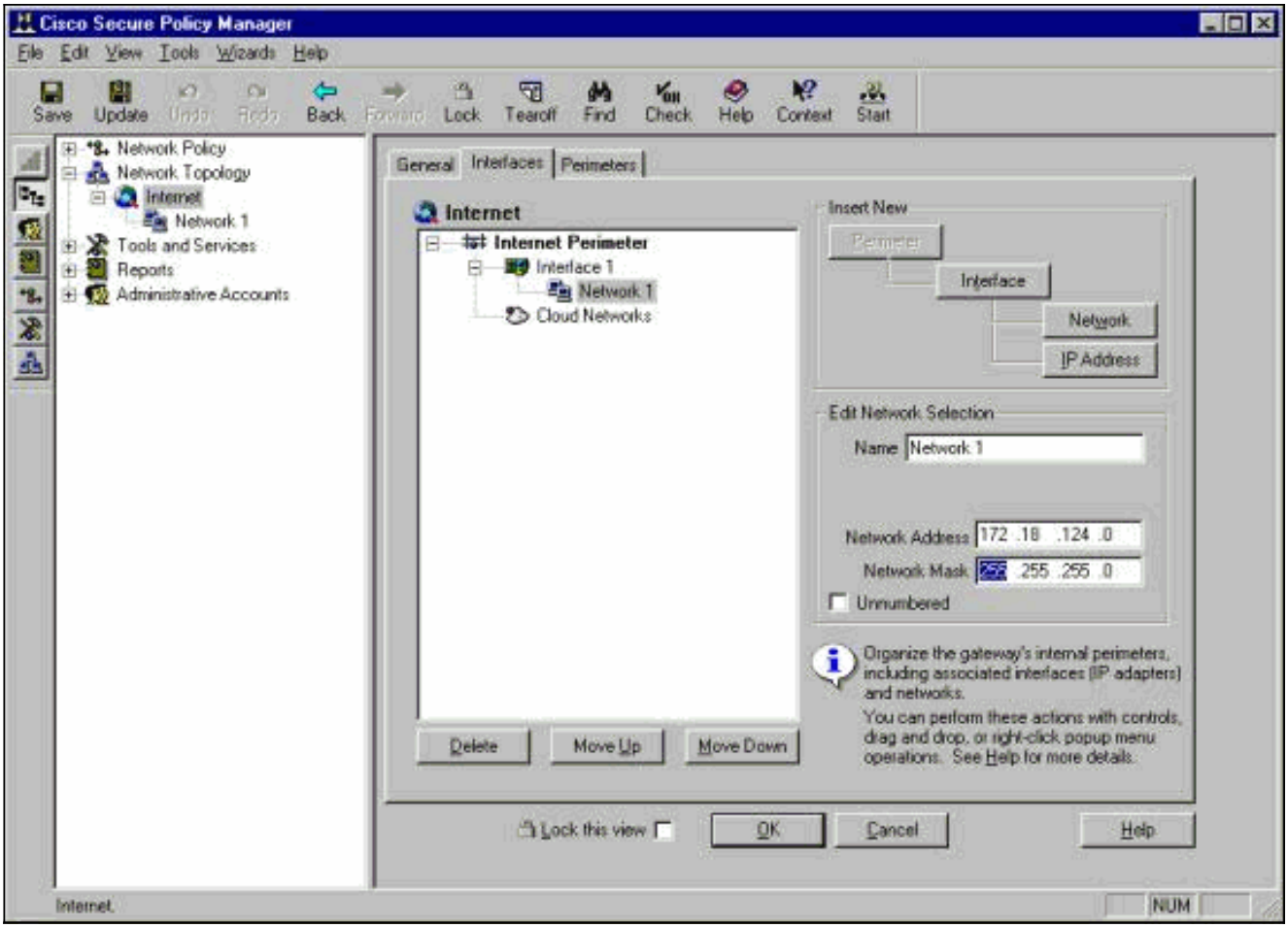
Bepaal het netwerk waarop de CSPM-host verblijft

Voer de volgende stappen uit:

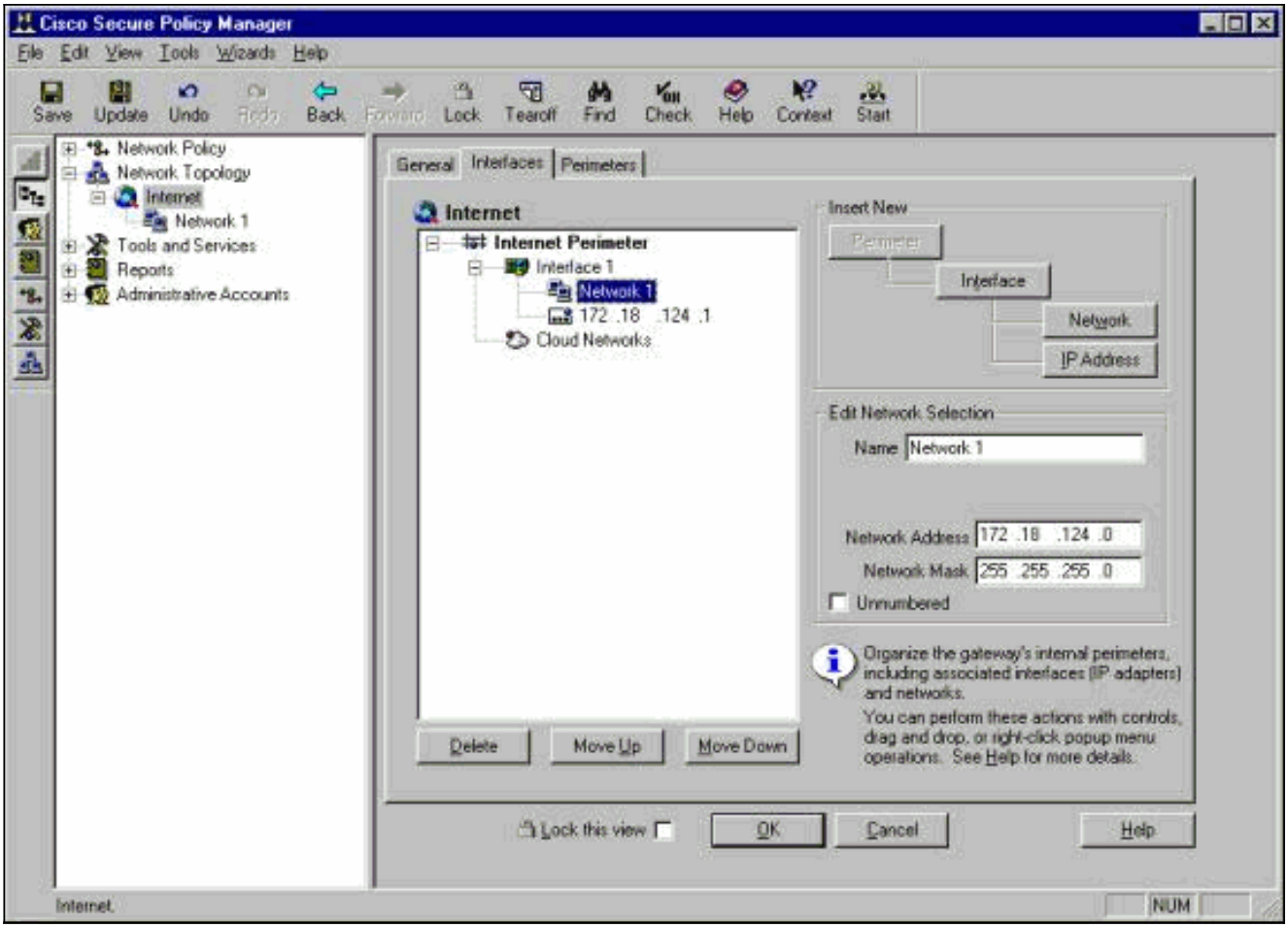
1. Klik met de rechtermuisknop op het pictogram **Internet** in de topologie en selecteer **Nieuw** > **Netwerk** om een nieuw netwerk te creëren.



2. Aan de rechterkant van het paneel van het Netwerk, voeg de naam van het nieuwe netwerk, het netwerkadres, en het netwerkmasker toe dat zal worden gebruikt.



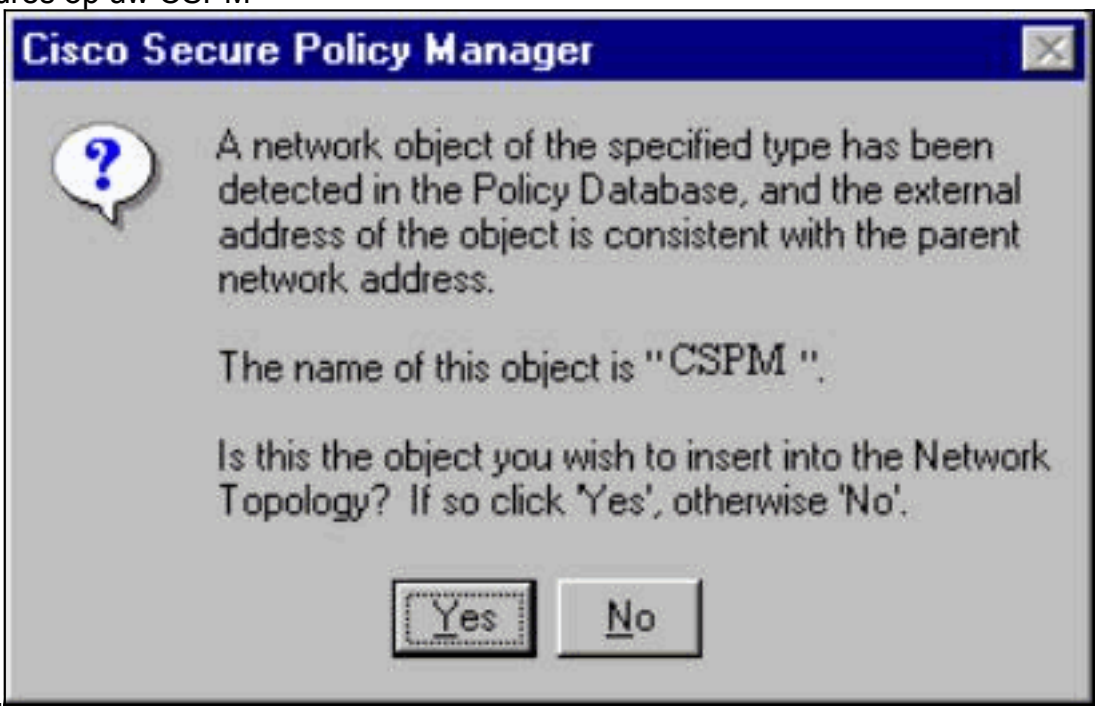
3. Klik op de knop **IP-adres** en voer het IP-adres in voor het netwerk dat wordt gebruikt om het internet te bereiken.Normaal gesproken is het de standaardgateway voor het netwerk.**Opmerking:** wanneer u sensoren beheert, hoeft het adres van de poort niet noodzakelijkerwijs te zijn correct aangezien de Sensor deze standaard gateway-informatie niet verstuurd heeft. Het zou al in de Sensor moeten worden gedefinieerd.
4. Klik op **OK**. Het netwerk wordt zonder enige fouten aan de topologie kaart toegevoegd.



Voeg de CSPM-host toe

Gebruik deze procedure om de CSPM-host toe te voegen.

1. In de Topologie van het Netwerk, klik op het netwerk dat u enkel toevoegde en selecteer **Nieuw > Host**.CSPM brengt een scherm dat hierop lijkt. Als niet, dan is het netwerk dat u zojuist hebt gedefinieerd niet het netwerk waarin uw CSPM-host zich bevindt. Controleer het IP-adres op uw CSPM-



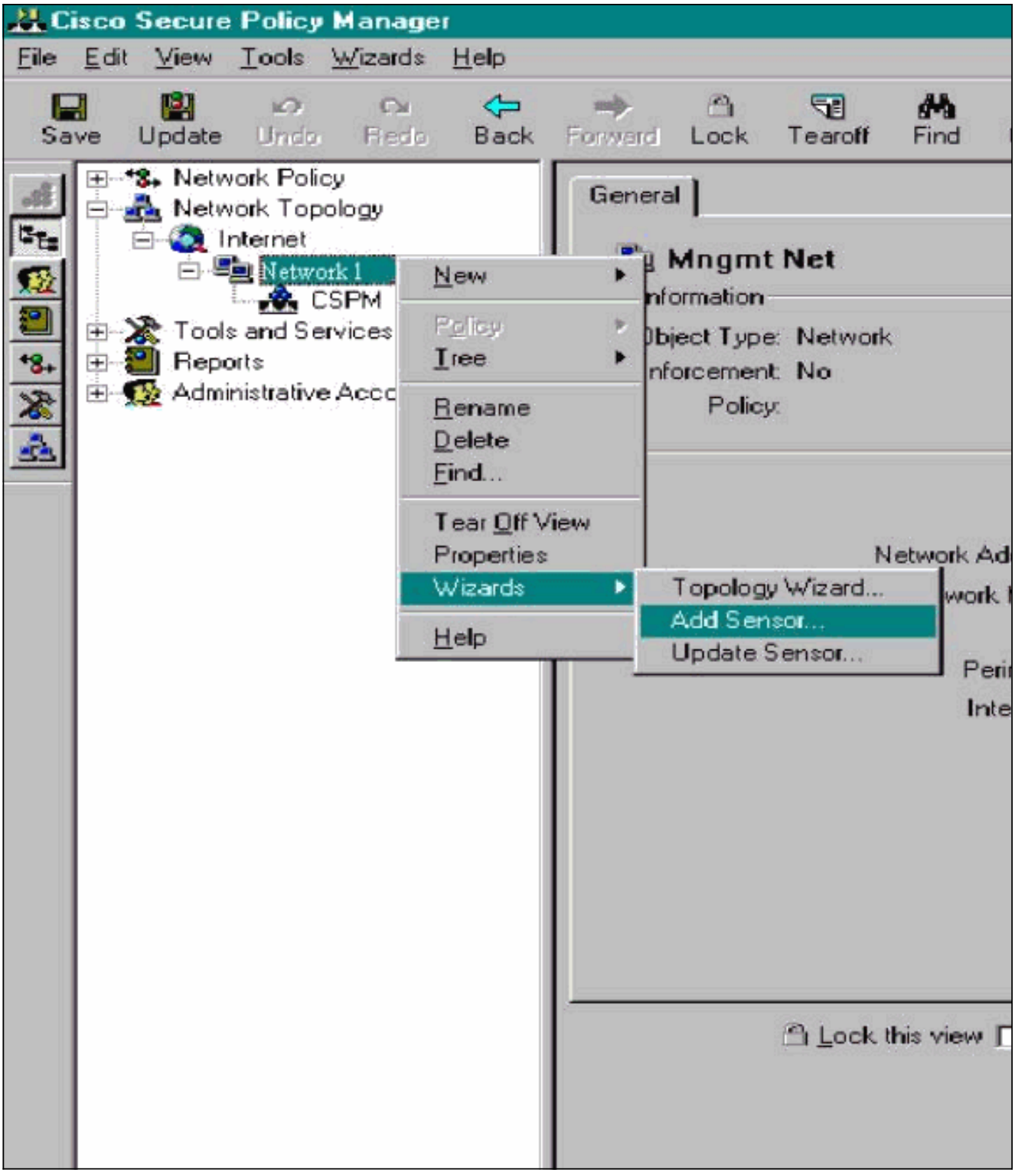
host.

2. Klik op **Ja** om de CSPM-host in de topologie te installeren.
3. Controleer of de informatie op het Algemene scherm voor de CSPM-host niet geschikt is.
4. Klik op **OK** op het Algemene scherm van de CSPM-host.

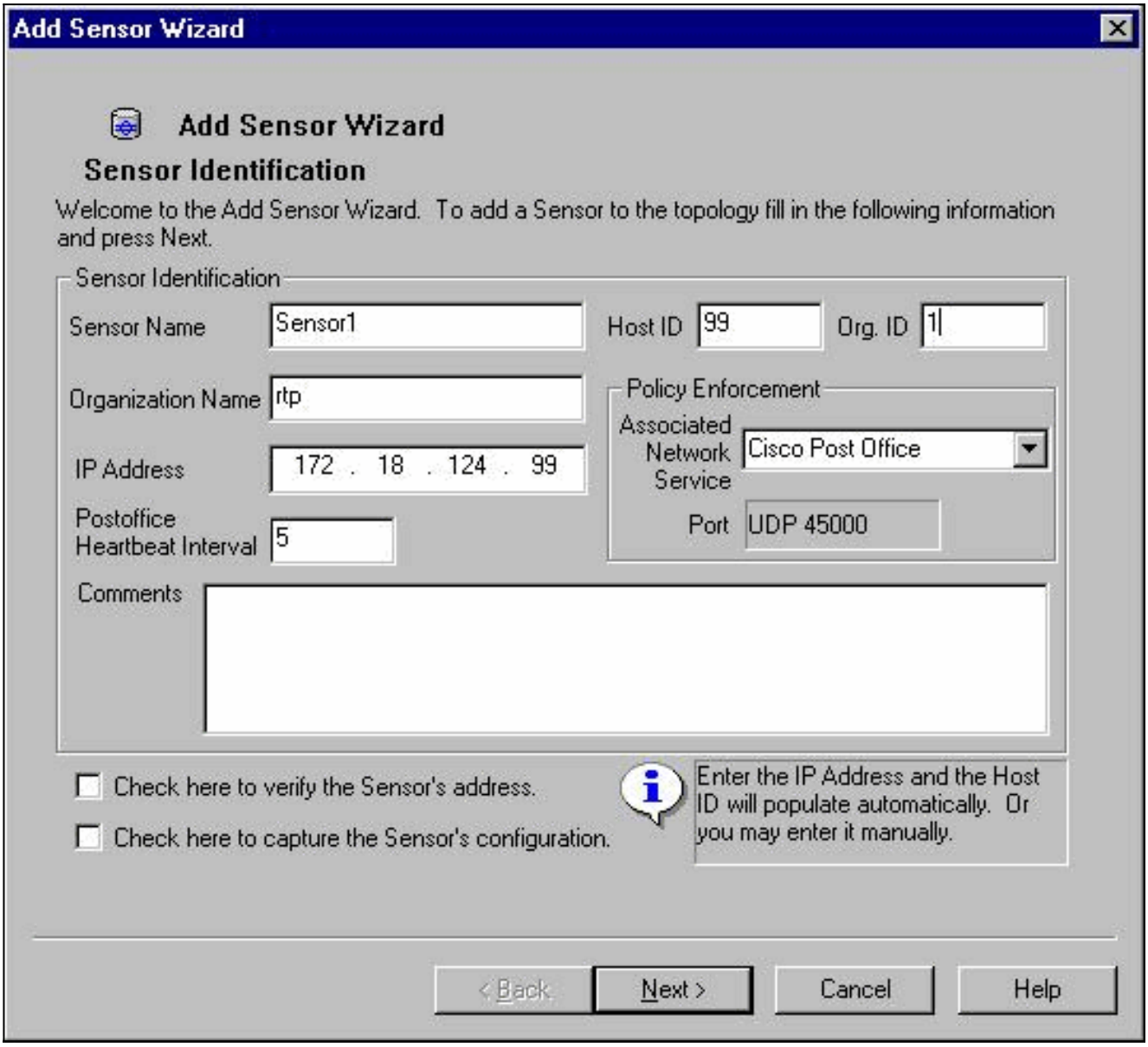
Het sensor-apparaat toevoegen

Gebruik deze procedure om het Sensor-apparaat toe te voegen.

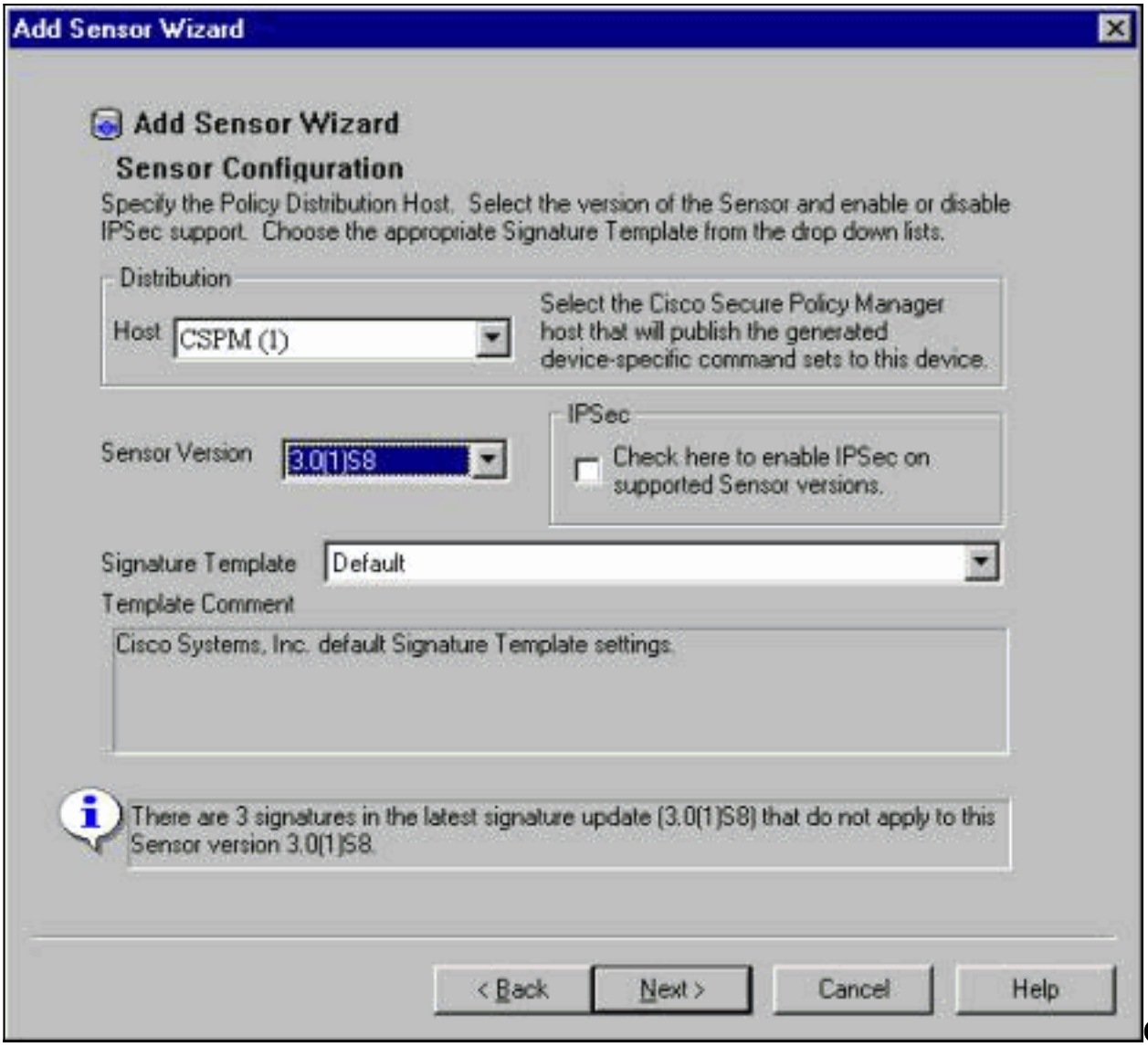
1. Klik met de rechtermuisknop op het netwerk waar uw sensor staat en selecteer **Wizard > Sensor toevoegen**.**Opmerking:** Als de CSPM-host en de regelinterface van uw sensor niet in hetzelfde netwerk zijn, specificeert u het netwerk waarin de sensor staat.



2. Voer de juiste postoffparameters in voor de sensor.



3. Klik **hier op Controleer om het adres van de sensor te controleren**.**N.B.:** Als dit de eerste keer is dat u deze Sensor instelt, dan wilt u niet de configuratie van de Sensor opnemen. Als u deze Sensor eerder elders hebt geconfigureerd, via een UNIX-directeur of een andere CSPM-host en u wijzigingen hebt aangebracht in de configuratie van de Sensors-handtekeningen, dan wilt u de configuratie van de Sensor opnemen.
4. Klik op **Next** om de kenmerkende versies op de sensor te definiëren. U kunt ook de opdracht vers geven om dit op de sensor te controleren.



Opmerking: Als CSPM niet de juiste versie van de Sensor heeft die u op uw sensor gebruikt, update de handtekeningen op uw CSPM-host. Zie Software Download (alleen geregistreerde klanten) voor updates.

5. Klik op de knop **Volgende** om verder te gaan
6. Klik op **Voltooien** om de installatie van de sensor in de topologie te voltooien.
7. Selecteer in het hoofdmenu CSPM de optie **Bestand > Opslaan** en **bijwerken** om de in de topologie ingevoerde informatie in CSPM te compileren. Let erop dat deze stap nodig is om het postprotocol op de CSPM-host te starten.
8. Controleer dat alles werkt door in uw sensor te loggen als de netwerkgebruiker.
9. Voer de **nrconns** opdracht uit.

```
>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

>
```

Opmerking: Als de Sensor en de CSPM-host niet communiceren, wordt er in plaats daarvan een soortgelijke uitvoer weergegeven:

```
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
```

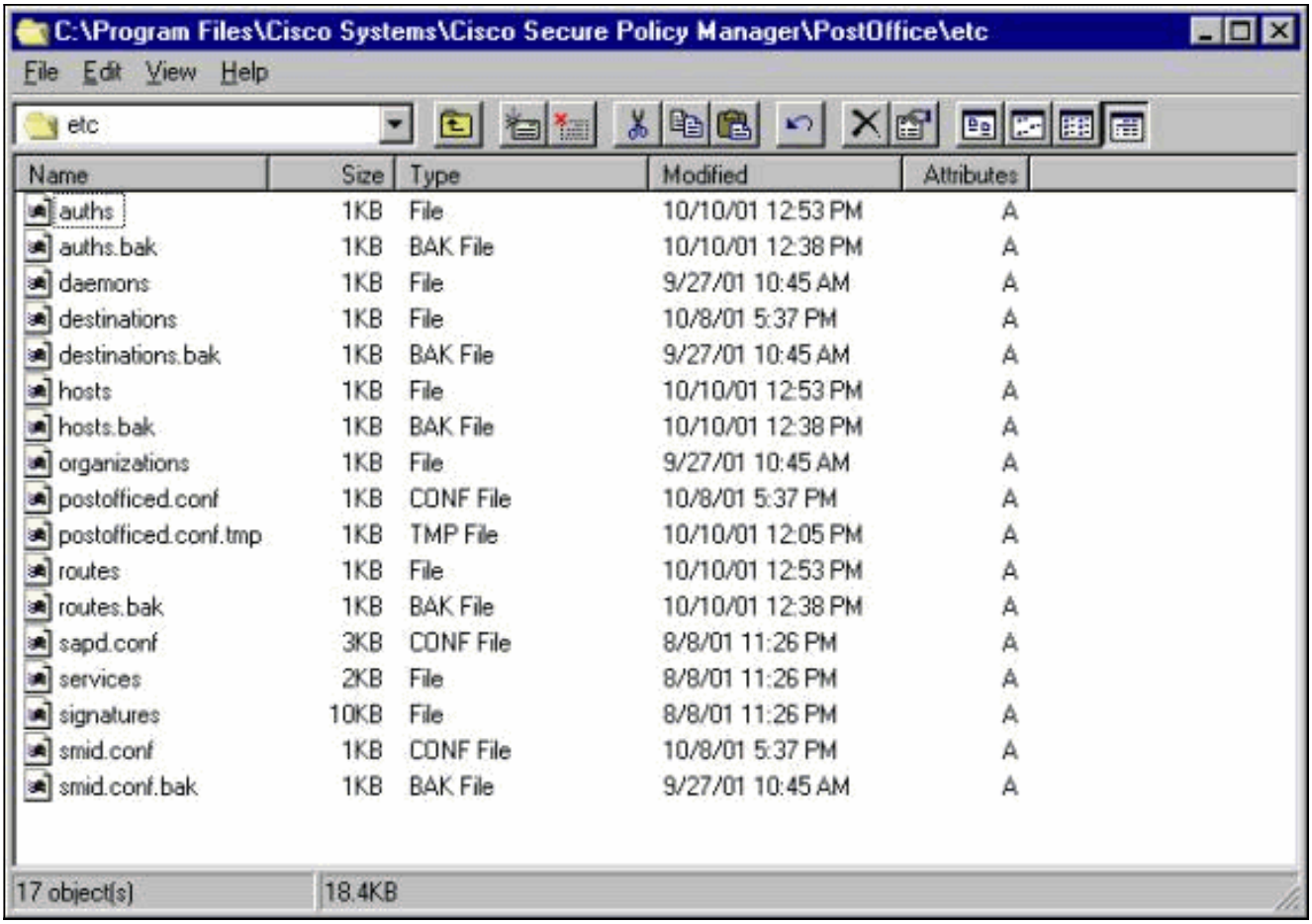
Als dit probleem zich voordoet, kunt u een snuffelspoor bekijken om te zien of beide kanten UDP 45000-pakketten verzenden. UDP 45000 is wat IDS-apparaten gebruiken om met elkaar te communiceren. Om dit op de Sensor te testen, **moet u** roken en (afhankelijk van welke Sensor u heeft) **snoop -d iprb1 poort 45000** (voor een IDS 4210-sensor) en **snoop -d iprb0 poort 45000** (voor elk ander model van Sensor) uitvoeren).Gebruik **<control-c>** om uit een sneeuwsessie te breken.Deze output verschijnt als er geen communicatie is tussen de Sensor en 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#
```

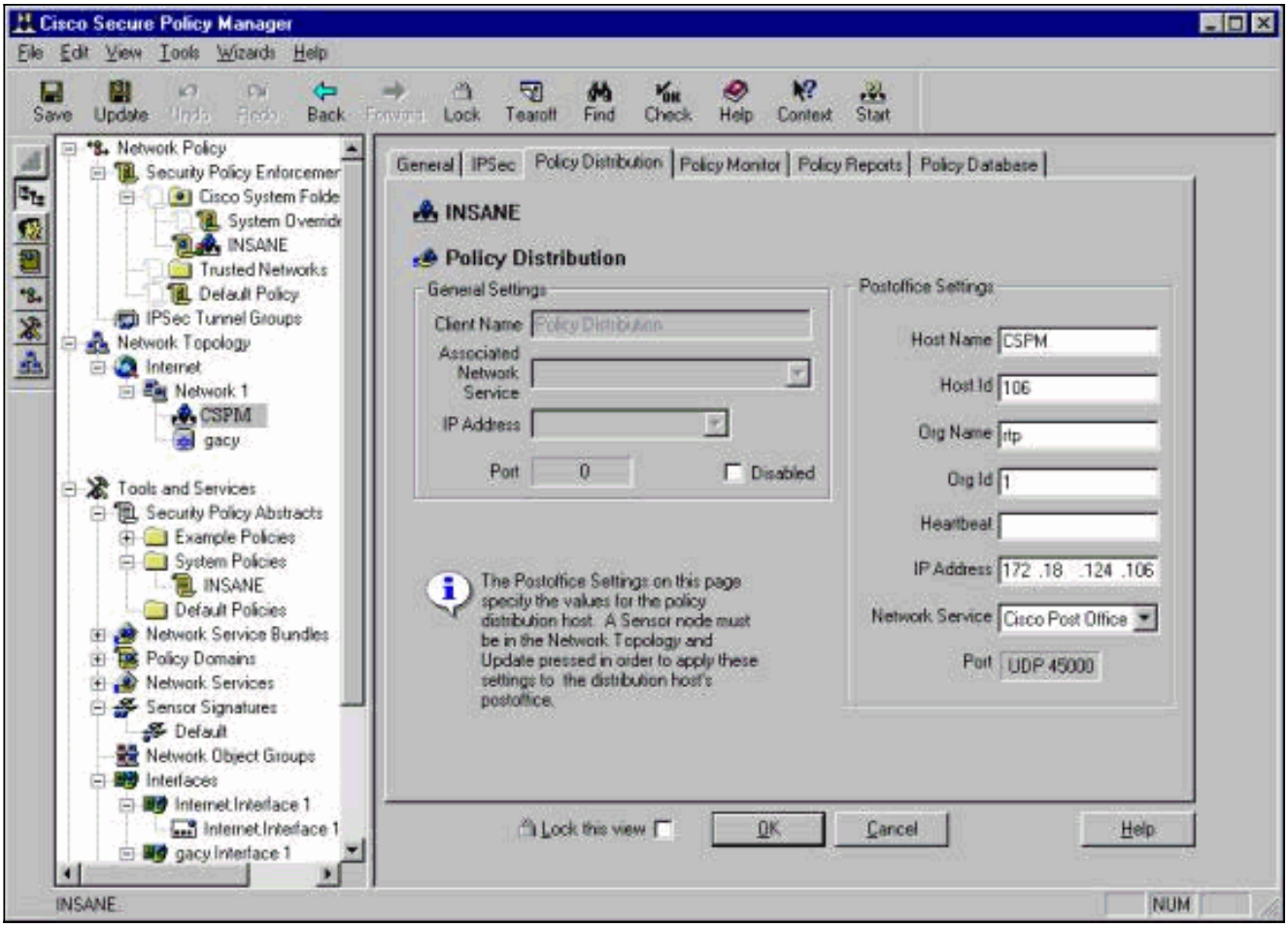
In de bovenstaande uitvoer stuurt de Sensor UDP 45000 pakketten, maar ontvangt deze niet. Een correcte configuratie produceert uitvoer gelijkend op dit:

```
# 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
```

In de bovenstaande uitvoer gaat UDP 45000-verkeer in beide richtingen.Als UDP 45000 pakketten in beide richtingen stromen en de uitvoer van **nBn** op de Sensor nog steeds zegt dat er geen verbinding is vastgesteld, komen de postoffparameters op de Sensor en de CSPM host niet overeen.U kunt de postoffsparameters als volgt handmatig op de CSPM-host controleren:Gebruik Windows Verkenner om naar de locatie te navigeren waar CSPM op de NT-machine is
geïnstalleerd.



Bewerk de host-, route- en organisatiebestanden met Schrijf- of Word-pad (gebruik geen Kladblok omdat de opmaak beschadigd zal zijn).Zorg ervoor dat deze bestanden op de juiste manier voor uw installatie lijken. Als een van de waarden niet correct is, bewerk ze en start de NT-computer opnieuw met behulp van deze stappen:Klik op het pictogram **CSPM** in de netwerktopologie.Klik op het tabblad Beleidsdistributie om de posteringsparameters in te voeren.**Sla** uw wijzigingen **op** en **update** ze.Herstart de NT-computer.



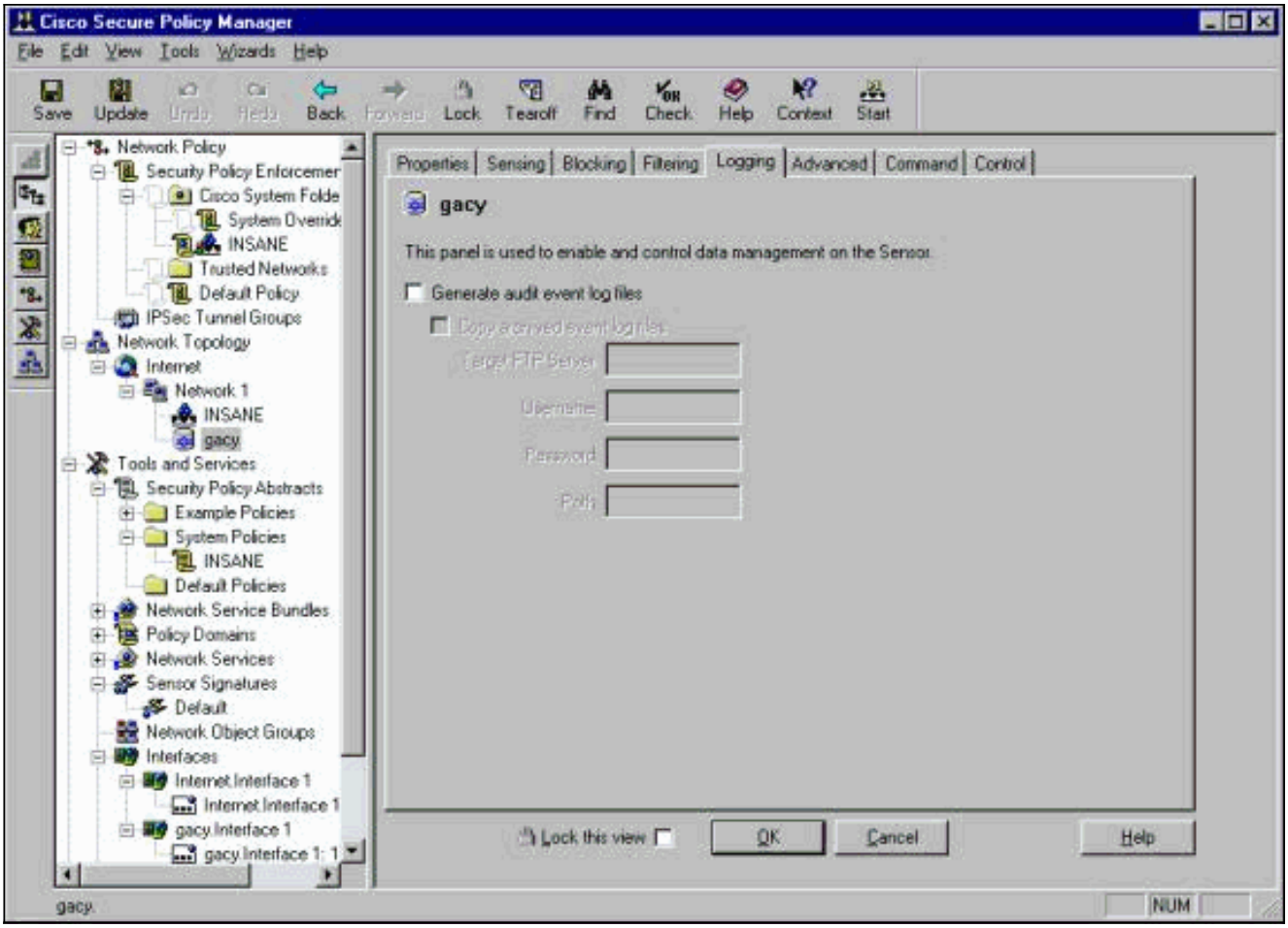
De sensor configureren

Nadat de configuratie in CSPM is opgeslagen, moet u de sensor configureren. Om dit te doen, stelt u eerst de Sensor in om de alarmen te schrijven die hij op zijn eigen blog ziet. Stel de sensor vervolgens in op "sniff" op de juiste interface.

Schrijf alarmen in het logboek

Gebruik deze procedure om alarmen aan het logbestand te schrijven.

1. Klik op het vak **Logbestanden van** audit **genereren** om de sensor te vertellen om de alarm naar zijn lokale logbestanden te sturen.Het stuurt ook een alarmsignaal naar de CSPM-doos, nadat je er een configuratie naar beneden
   duwt.

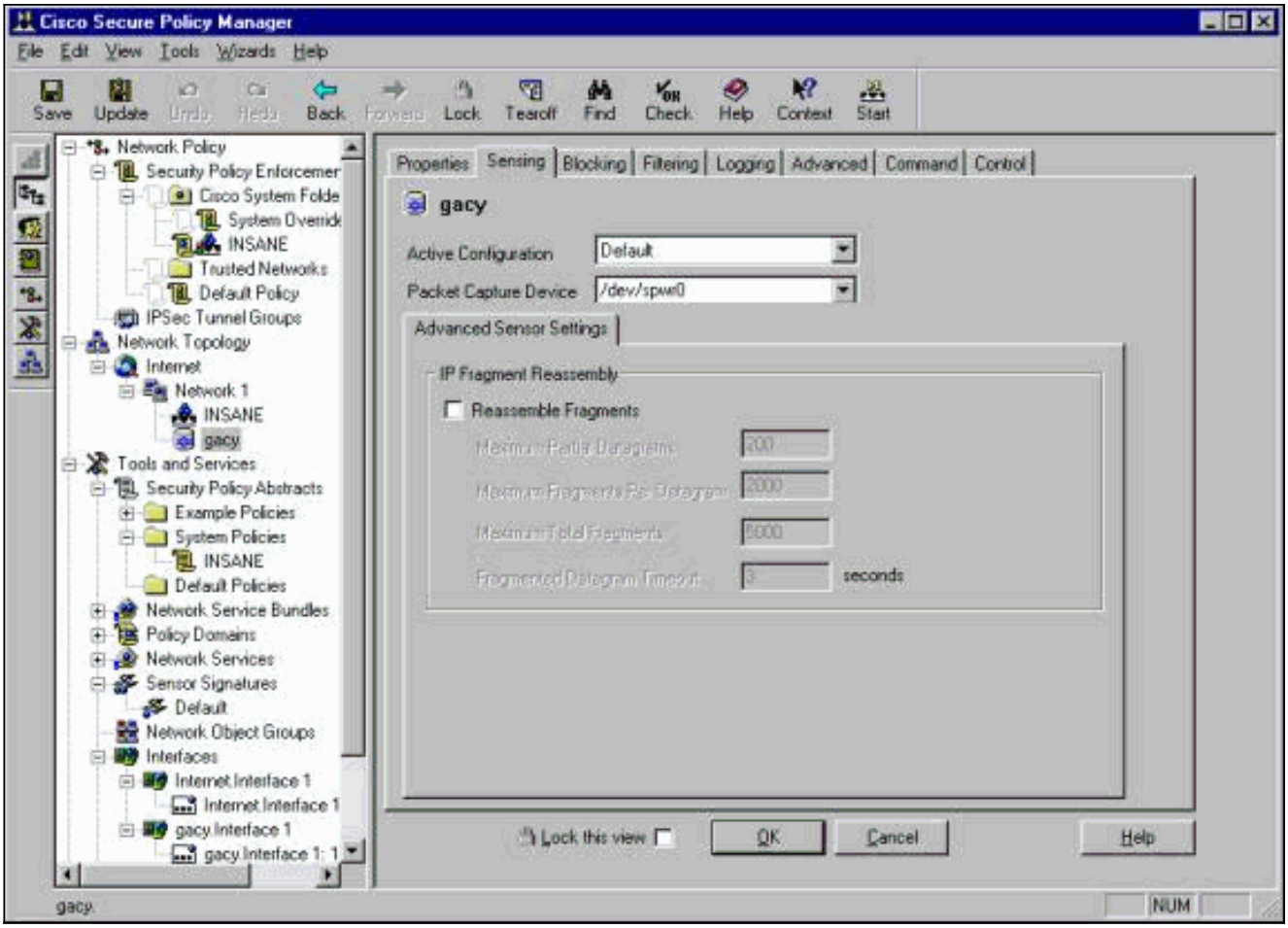


2. Klik op **OK** om verder te gaan.

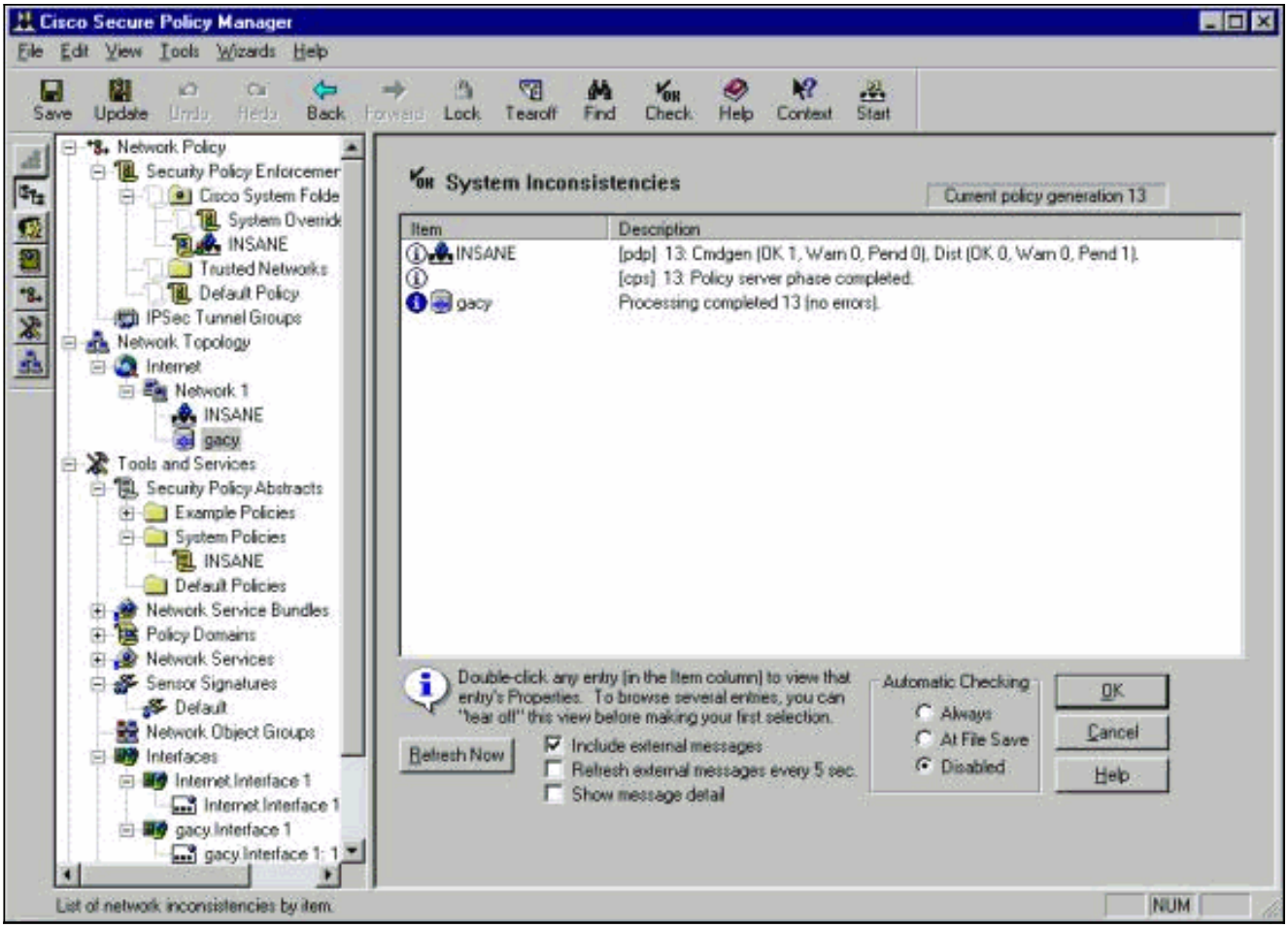
Stel de sensor in op "Sniff"

Gebruik deze procedure om de sensor in te stellen op "Sniff".

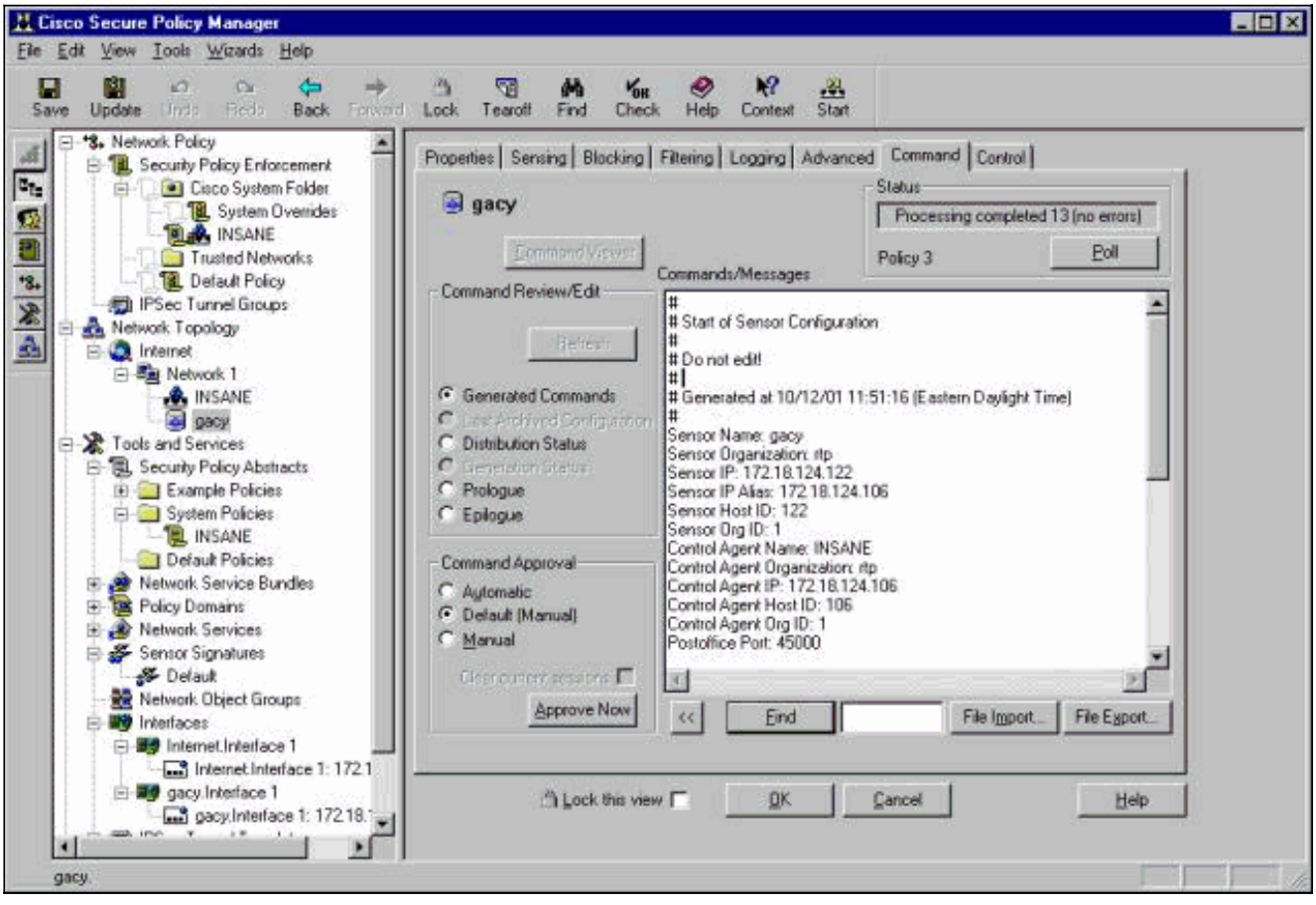
1. Selecteer de sensor in uw topologie van CSPM en klik op het tabblad Sensing.
2. Defineert het Packet Capture apparaat:iprb0 - voor een IDS 4210 sensorSPW0 - voor elk ander Sensor-
   model



3. Klik op **OK** om verder te gaan.
4. Klik het pictogram **Update** op de menubalk van CSPM om CSPM met de informatie bij te werken.**Opmerking:** als alles goed gaat, verschijnt er een vergelijkbaar scherm. Merk op dat er geen rode fouten zijn. Gele waarschuwingen zijn doorgaans in orde.

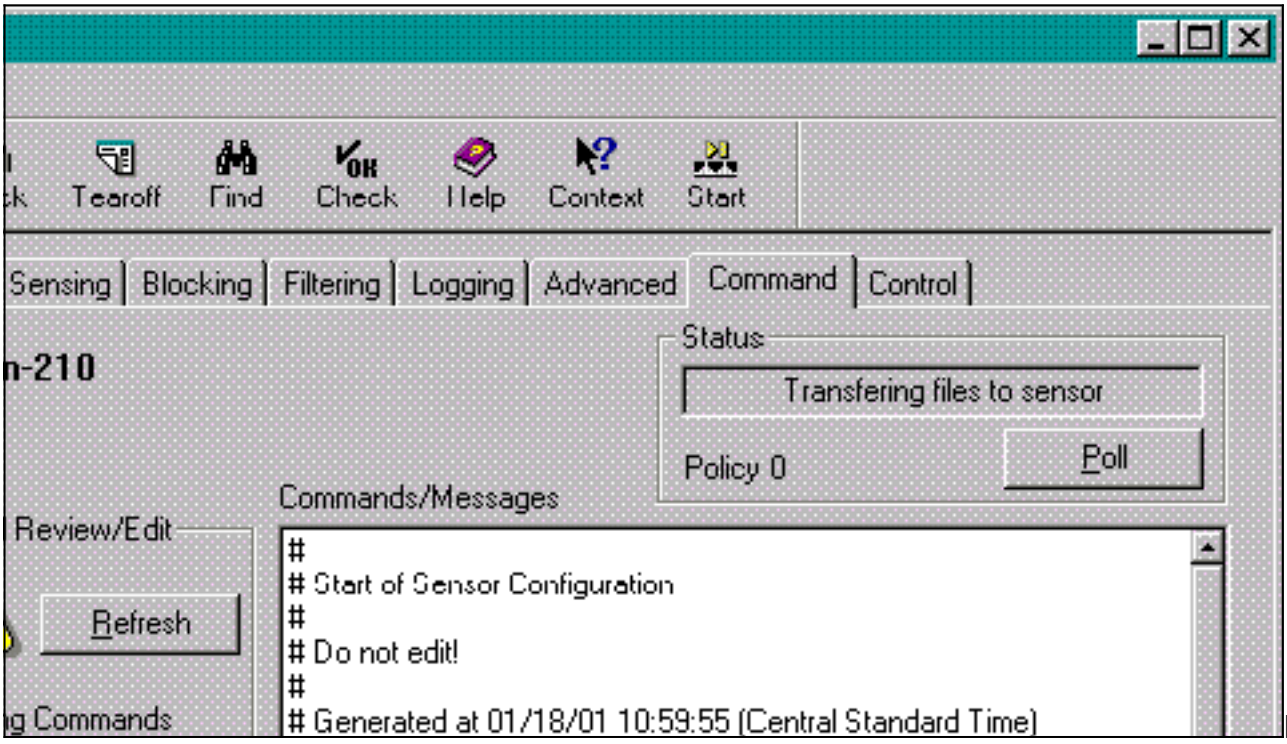


5. Selecteer de sensor in de netwerktopologie en klik op het tabblad Opdracht om de bijgewerkte configuratie naar de sensor te verzenden.

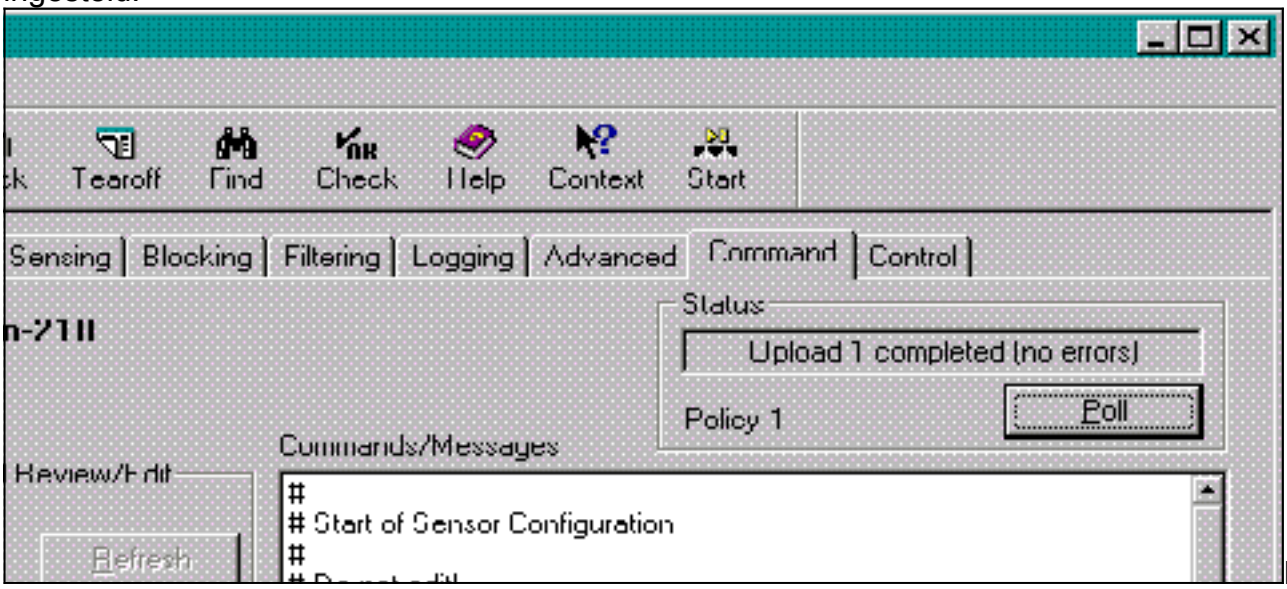


6. Klik op de knop **Nu** goedkeuren om de configuratie naar de sensor te

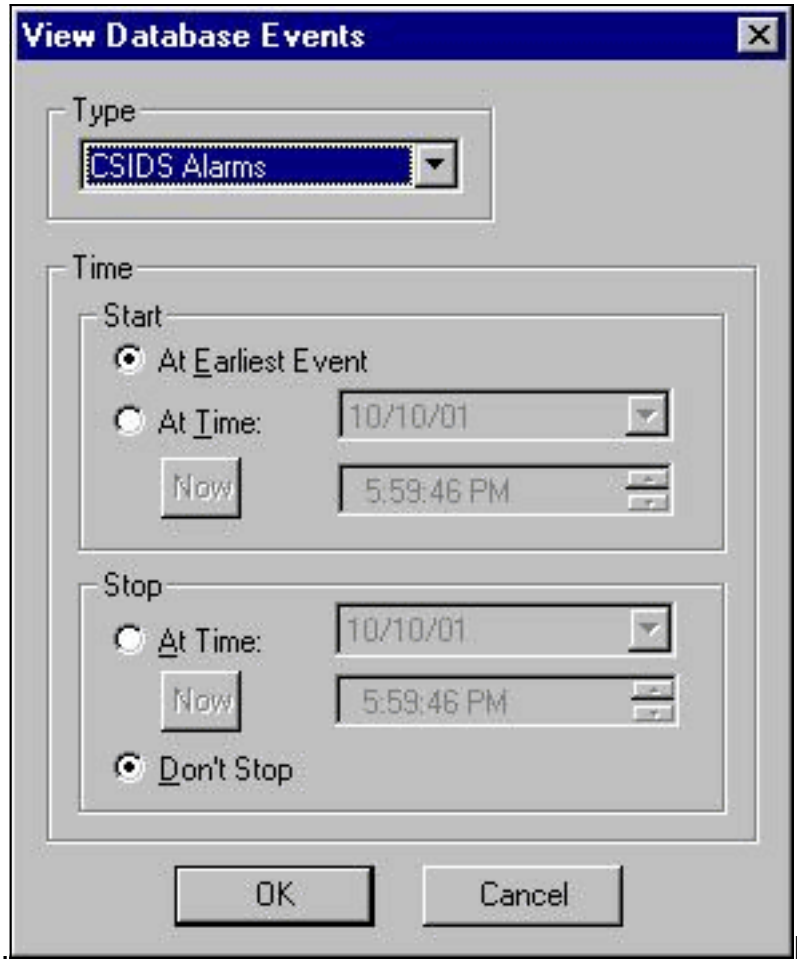
sturen.



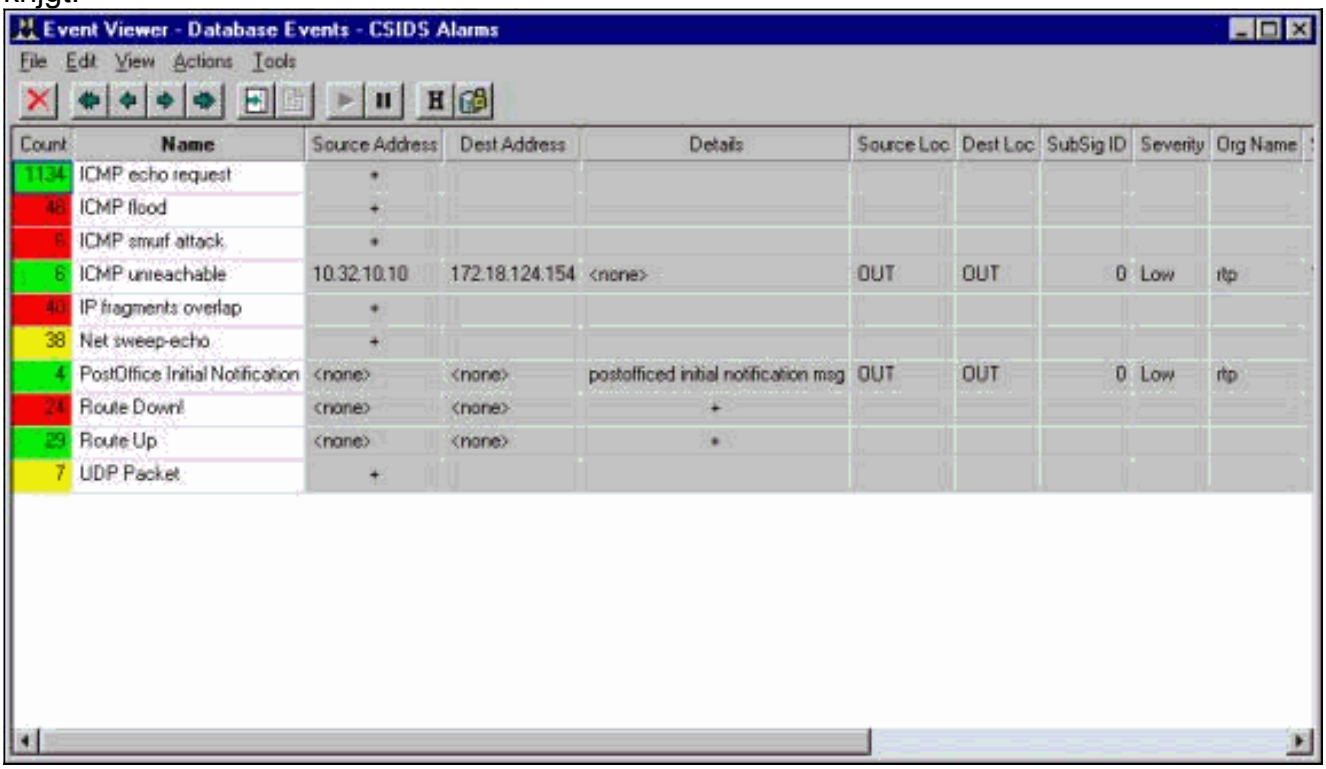
Het Statusvenster geeft het bericht "Upload <#> Klaar" weer. Dit duidt op een geldig en volledig overdrachtproces. De sensor wordt nu bijgewerkt en werkt nu normaal.Als de sensor niet normaal werkt, ga dan terug naar de Sensor en controleer de uitvoer van de opdrachtregel om er zeker van te zijn dat de verbinding tussen de CSPM-host en de sensor is
ingesteld.



Nadat dit is voltooid, kunt u op zoek gaan naar alarmen die de Sensor naar de CSPM host in de eventviewer stuurt. Om de evenementenviewer te bekijken, selecteert u in het hoofdmenu van CSPM **Gereedschappen > Sensor gebeurtenissen >**



Databaseverhouding. Klik op **OK** om het venster van de events-database weer te geven. Uw scherm zal variëren afhankelijk van de alarmen die u krijgt.



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	rtp
40	IP fragments overlap	*							
38	Net sweep-echo	*							
4	PostOffice Initial Notification	<none>	<none>	postofficed initial notification msg	OUT	OUT	0	Low	rtp
24	Route Down!	<none>	<none>	*					
29	Route Up	<none>	<none>	*					
7	UDP Packet	*							

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems