Configureer Cisco IOS IPS met een router en endpointgebeurtenissen

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Router en Security Devices Manager (DSM) versie 2.5 kunt gebruiken om Cisco IOS® Inbraakpreventiesysteem (IPS) te configureren in 12.4(15)T3 en later releases.

De verbeteringen in PDM 2.5 verwant aan IOS IPS zijn:

- Totaal gecompileerd handtekening nummer weergegeven in de lijst met handtekeningen GUI
- DM-bestanden (zip-bestandsformaat); bij voorbeeld sigv5-DSM-S307.zip) en CLI-signaalpakketten (pkg bestandsformaat; kan bijvoorbeeld IOS-S313-CLI.pkg) in één bewerking worden gedownload
- Downloadde pakketten voor handtekeningen kunnen automatisch naar de router worden geduwd als optie

De taken van het eerste voorzieningsproces zijn:

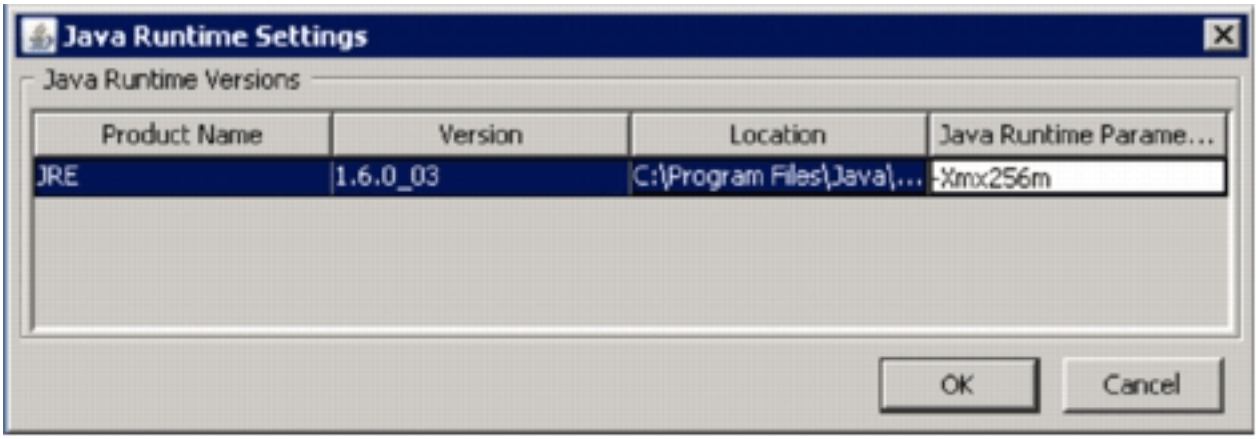
1. Downloaden en installeren vanaf 2.5.
2. Gebruik de Auto Update van de Auto om van de IOS IPS te downloaden van een lokale PC.
3. Start de IPS Policy Wizard om IOS IPS te configureren.
4. Controleer of de IOS IPS-configuratie en -handtekeningen correct geladen zijn

Cisco dm is een op web-gebaseerd configuratiehulpmiddel dat router en veiligheidsconfiguratie door slimme tovenaars vereenvoudigt die klanten snel en gemakkelijk helpen een router van Cisco in te stellen, te vormen en te controleren zonder kennis van de commando-lijn interface (CLI) te vereisen.

Versie 2.5 kan vanaf Cisco.com worden gedownload op http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (alleen geregistreerde klanten). Het persbericht is te vinden op http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr.25.html

Opmerking: Cisco SDM vereist een schermresolutie van minimaal 1024 x 768.

Opmerking: Cisco PDM vereist dat de grootte van de Java-geheugenzeep niet minder dan 256MB is om IOS IPS te kunnen configureren. Als u de grootte van de Java-geheugenzeep wilt wijzigen, opent u het Java-bedieningspaneel en klikt u op het tabblad **Java**, klikt u op **Weergave** onder de instellingen van de Java-**applicatie** en vervolgens voert u **-Xmx256m** in de kolom Java-parameter in.



Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS IPS in 12.4(15)T3 en latere releases
- Cisco Router en Security Devices Manager (DSM) versie 2.5

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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

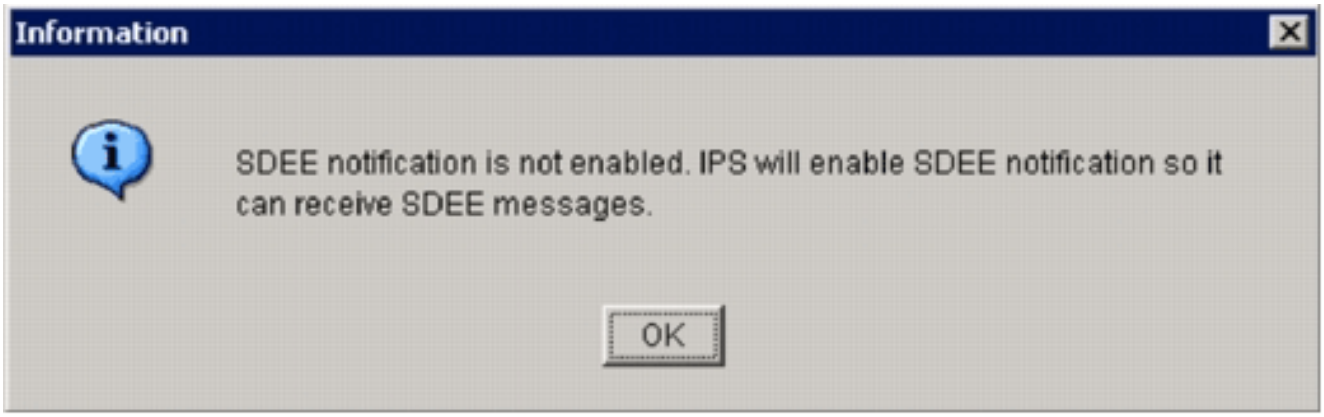
Configureren

Opmerking: Open een console of telnet sessie aan de router (met term monitor' op) om berichten te controleren wanneer u middel van een dm op voorziening van IOS IPS gebruikt.

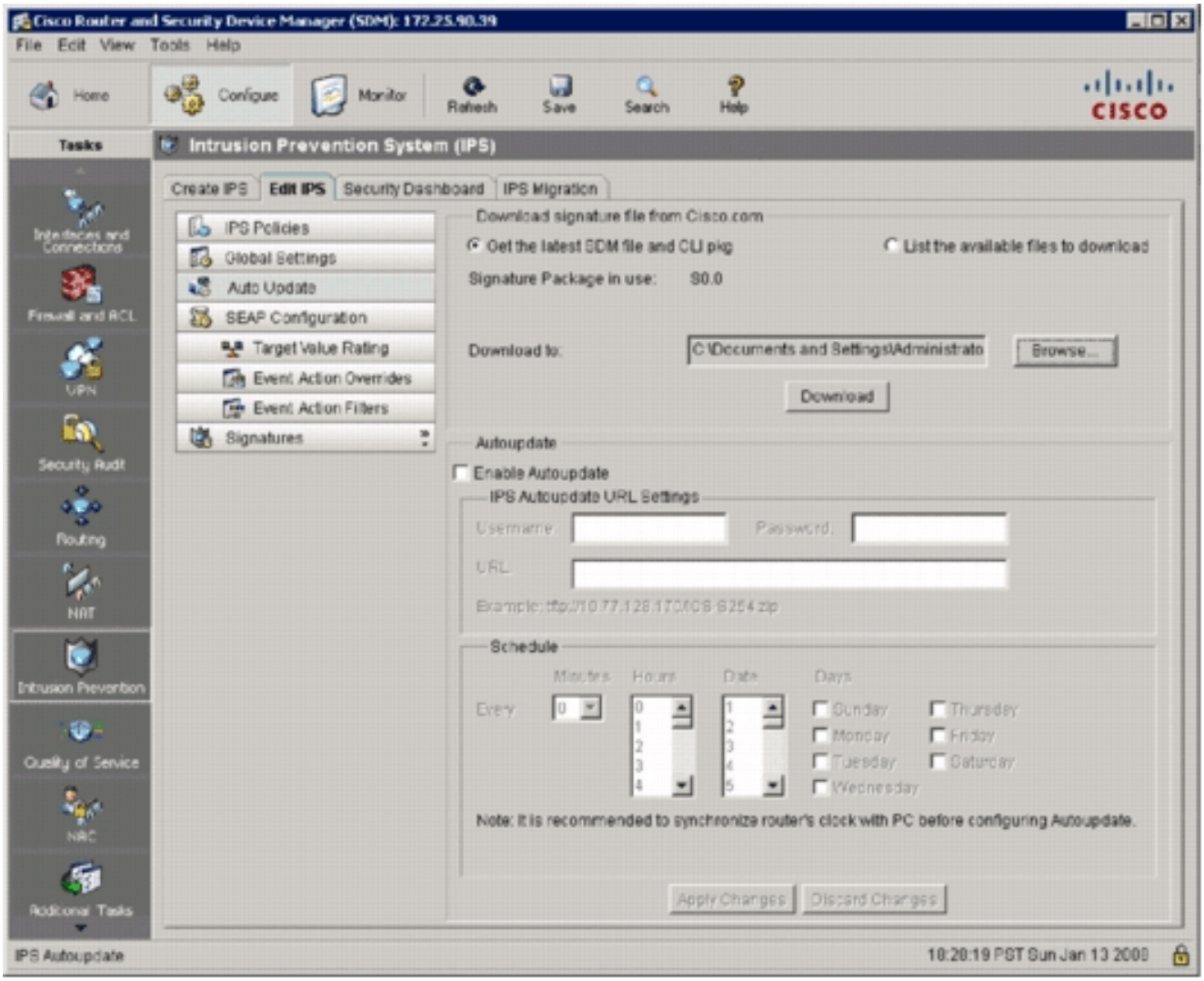
1. Download DM 2.5 van Cisco.com op http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (alleen geregistreerde klanten) en installeer het op een lokale PC.
2. Start 2.5 vanaf de lokale pc.

3. Wanneer het dialoogvenster Aanmelden voor IOS IPS verschijnt geeft u dezelfde naam en hetzelfde wachtwoord in als u voor de verificatie van DM op de router gebruikt.

4. Van de gebruikersinterface van verPDN, klik **Configureren**, en klik dan **Inbraakpreventie**.
5. Klik op het tabblad **IPS bewerken**.
6. Als het SDEE-bericht op de router niet is ingeschakeld, klikt u op **OK** om SDEE-melding in te schakelen.

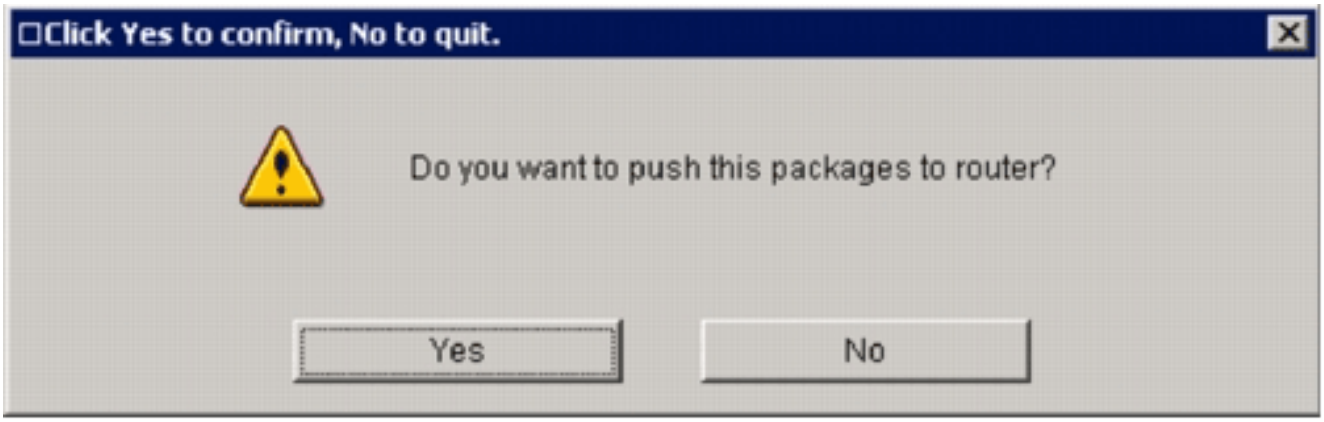


7. In het gebied van de Handtekening van de Download van Cisco.com van het tabblad Bewerken IPS, klik op het **tabblad**, **het meest recente** radioknop **van het** bestand **en CLI pkg**, en klik vervolgens **Bladeren** om een folder op uw lokale PC te selecteren waarin u de gedownload bestanden kunt opslaan.U kunt de TFTP of FTP server root folder kiezen, die later gebruikt zal worden wanneer u het signatuur pakket in de router implementeert.
8. Klik op **Download (Downloaden).**

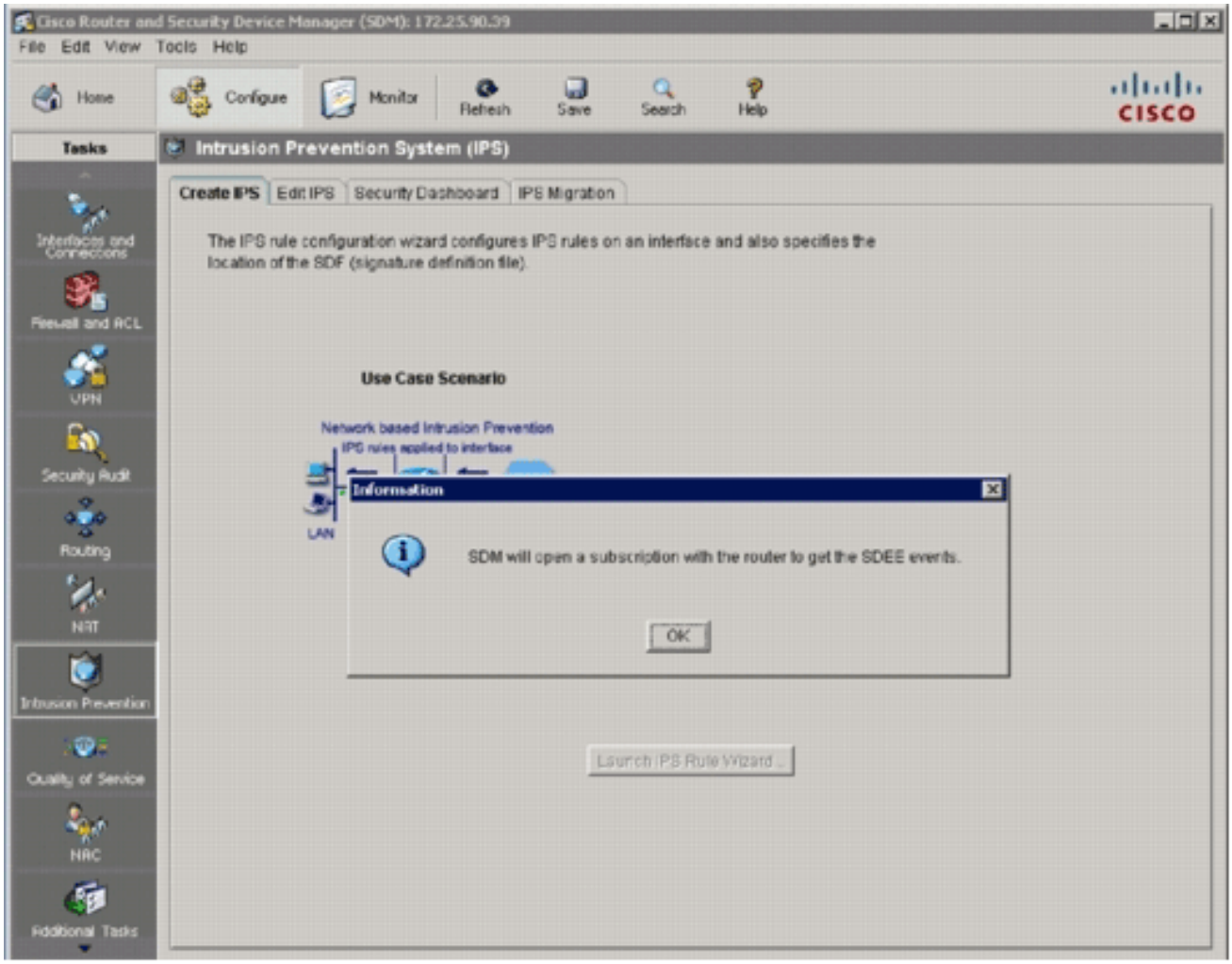


9. Wanneer het dialoogvenster CCO Login verschijnt, gebruikt u de geregistreerde gebruikersnaam en het wachtwoord van

CCO.Aansluiting op Cisco.com en start om zowel het hiermede volgende bestand (bijvoorbeeld sigv5-DM-S307.zip) als het CLI pkg-bestand (bijvoorbeeld IOS-S313-CLI.pkg) te downloaden naar de map die in stap 7 is geselecteerd.Zodra beide bestanden zijn gedownload, vraagt het dm-toestel u om het gedownload signatuur pakket naar de router te
duwen.



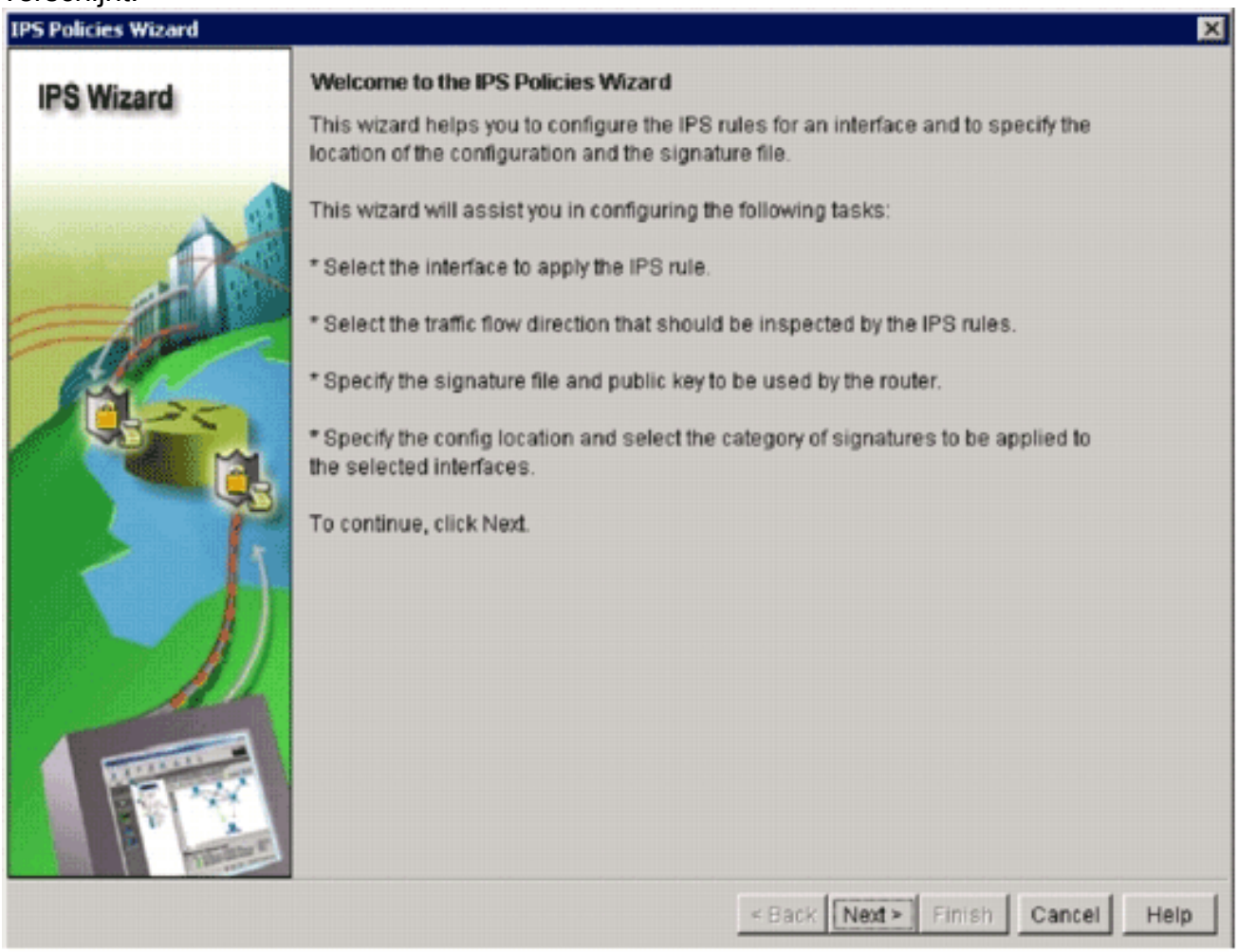
10. Klik op **Nee** aangezien IOS IPS niet op de router is ingesteld.
11. Na het downloaden van het meest recente IOS CLI ondertekeningspakket, klik op het tabblad **Create IPS** om de eerste IOS IPS-configuratie te maken.
12. Als u wordt gevraagd wijzigingen in de router toe te passen, klikt u op **Wijzigingen toepassen**.
13. Klik op **Opstarten van de IPS-regelwizard**.Een dialoogvenster verschijnt om u te informeren dat het SDEE-abonnement op de router moet worden ingesteld om waarschuwingen op te halen.



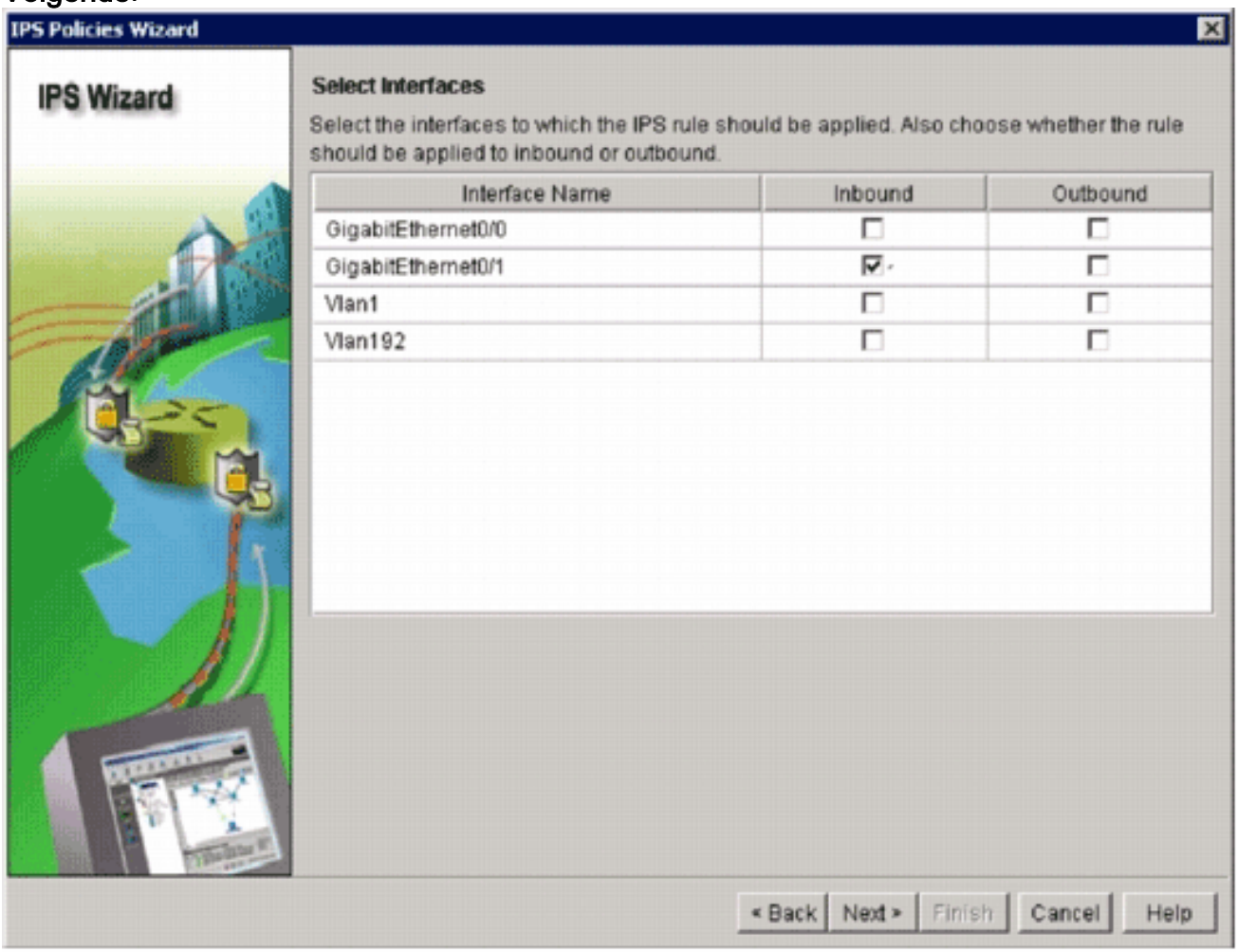
14. Klik op **OK**.Het gewenste dialoogvenster met verificatie

verschijnt.

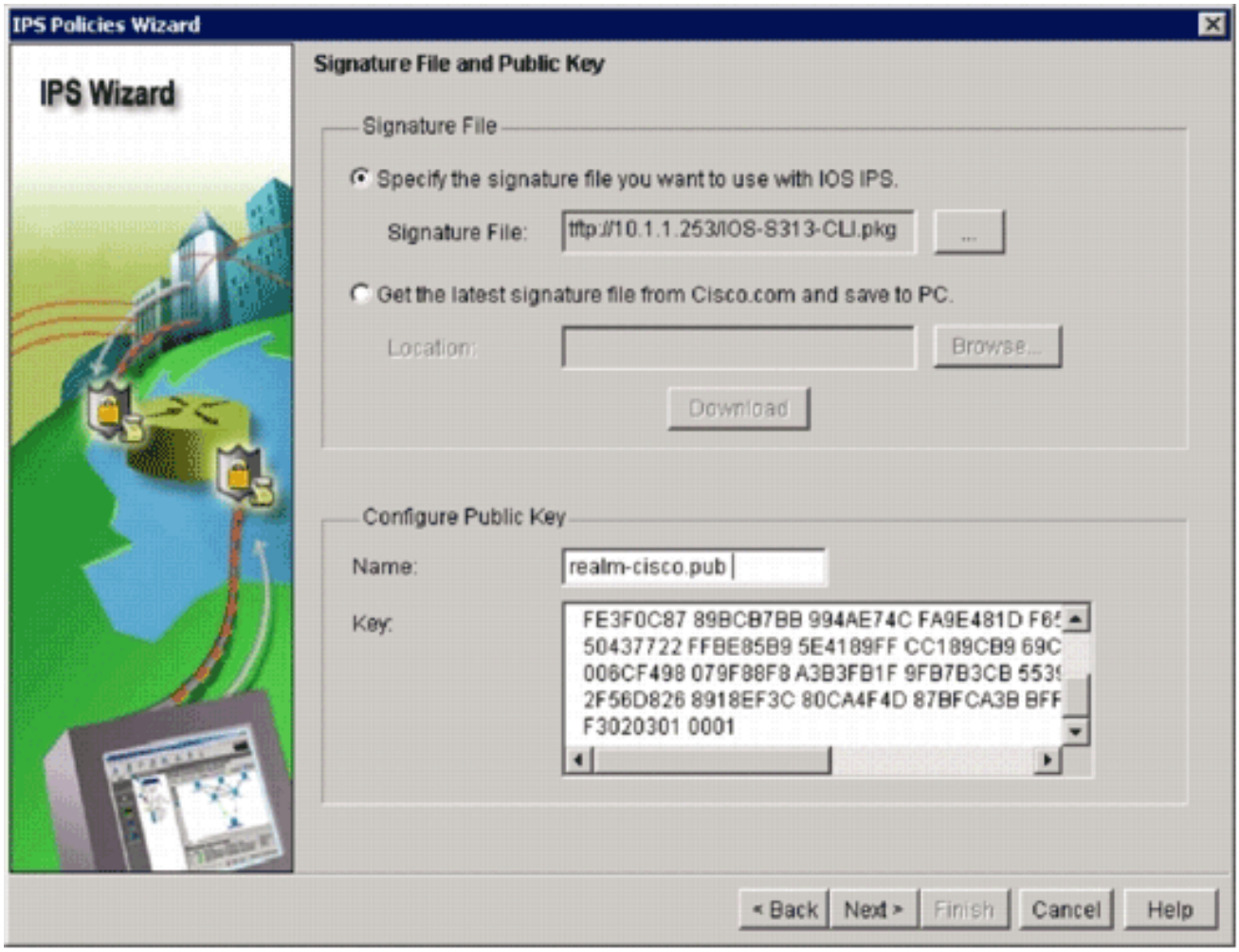
15. Voer de naam van de gebruiker in en het wachtwoord dat u voor het authenticeren van de router hebt gebruikt, en klik **OK**.Het dialoogvenster Wizard IPS-beleid verschijnt.



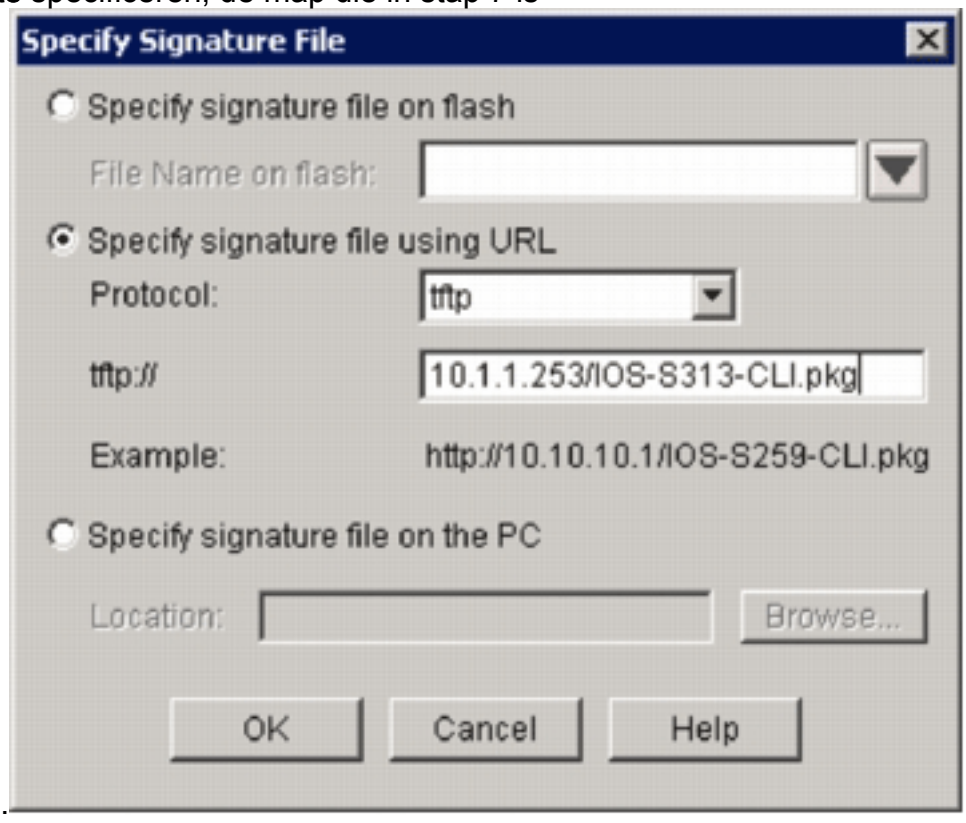
16. Klik op
    Volgende.



17. In het venster Geselecteerde interfaces kiest u de interface en de richting waarop die IOS IPS zal worden toegepast, en klikt u vervolgens op **Volgende** om verder te gaan.



18. In het gedeelte Signature File van het venster Signature File and Public Key klikt u op het **bestand opgeven van het bestand dat u met de** radioknop **van IOS IPS wilt gebruiken** en vervolgens klikt u op de knop **Signature File** (...) om de locatie van het bestand voor de handtekening **te** specificeren, de map die in stap 7 is



gespecificeerd.

19. Klik op het **bestand voor handtekening specificeren met behulp van de URL**-radioknop, en

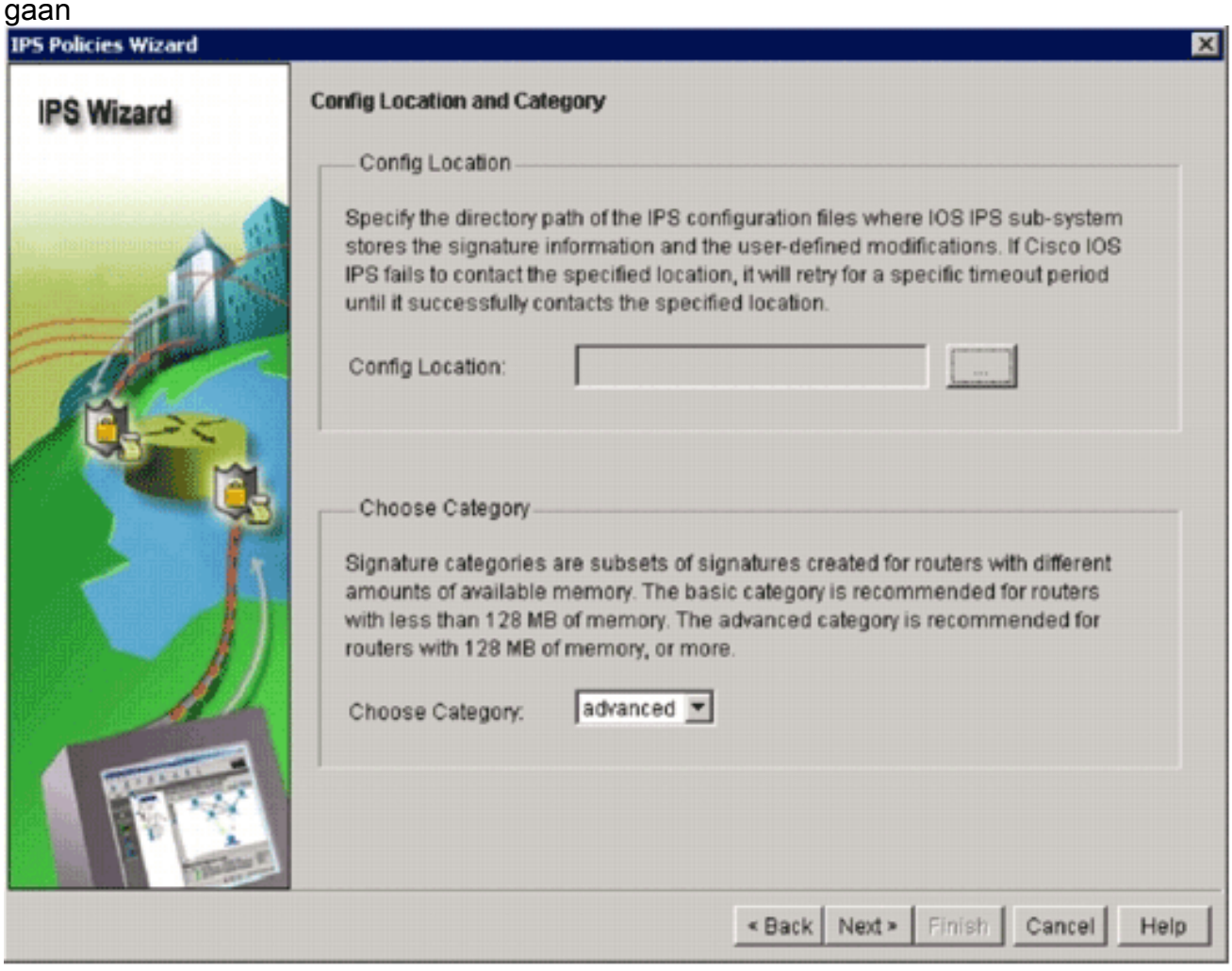
kies een protocol in de vervolgkeuzelijst Protocol.**Opmerking:** Dit voorbeeld gebruikt TFTP om het pakket voor handtekeningen aan de router te downloaden.

20. Voer de URL in voor het bestand voor handtekening en klik op **OK**.
21. In het veld Openbare sleutel van het venster Handtekeningen en Openbare sleutel invoeren **gaat** u **realm-cisco.pub** in het veld Naam in en kopieert u deze openbare sleutel en voegt u deze toe aan het veld Key.

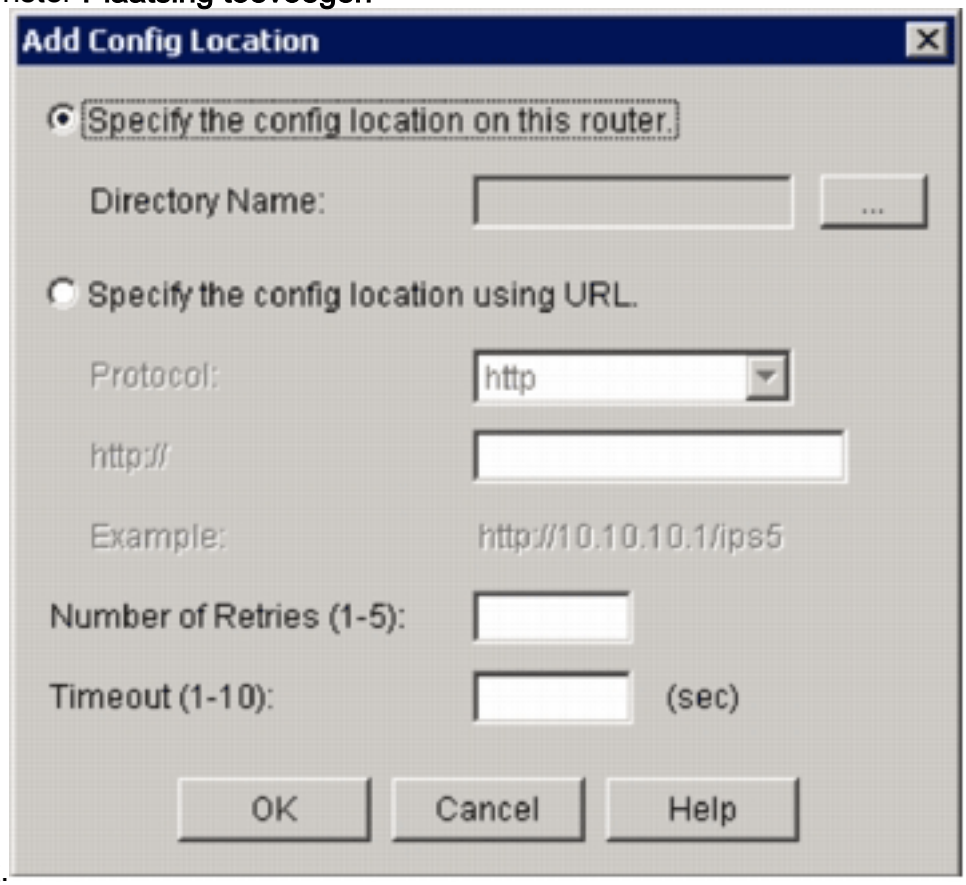
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001
```

Opmerking: Deze openbare sleutel kan worden gedownload van Cisco.com op: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (alleen geregistreerde klanten) .

22. Klik op **Volgende** om verder te gaan

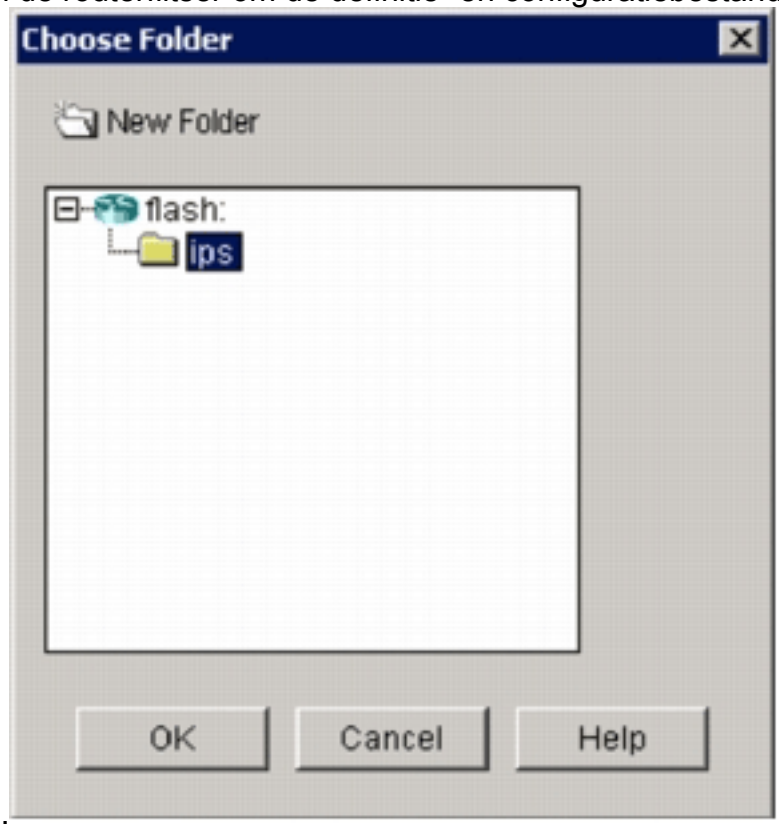


23. Klik in het venster Locatie en Category op de knop **Config Locatie** (...) om een locatie op te geven waar de configuratie-bestanden van de handtekeningen worden opgeslagen.Het dialoogvenster **Plaatsing toevoegen**



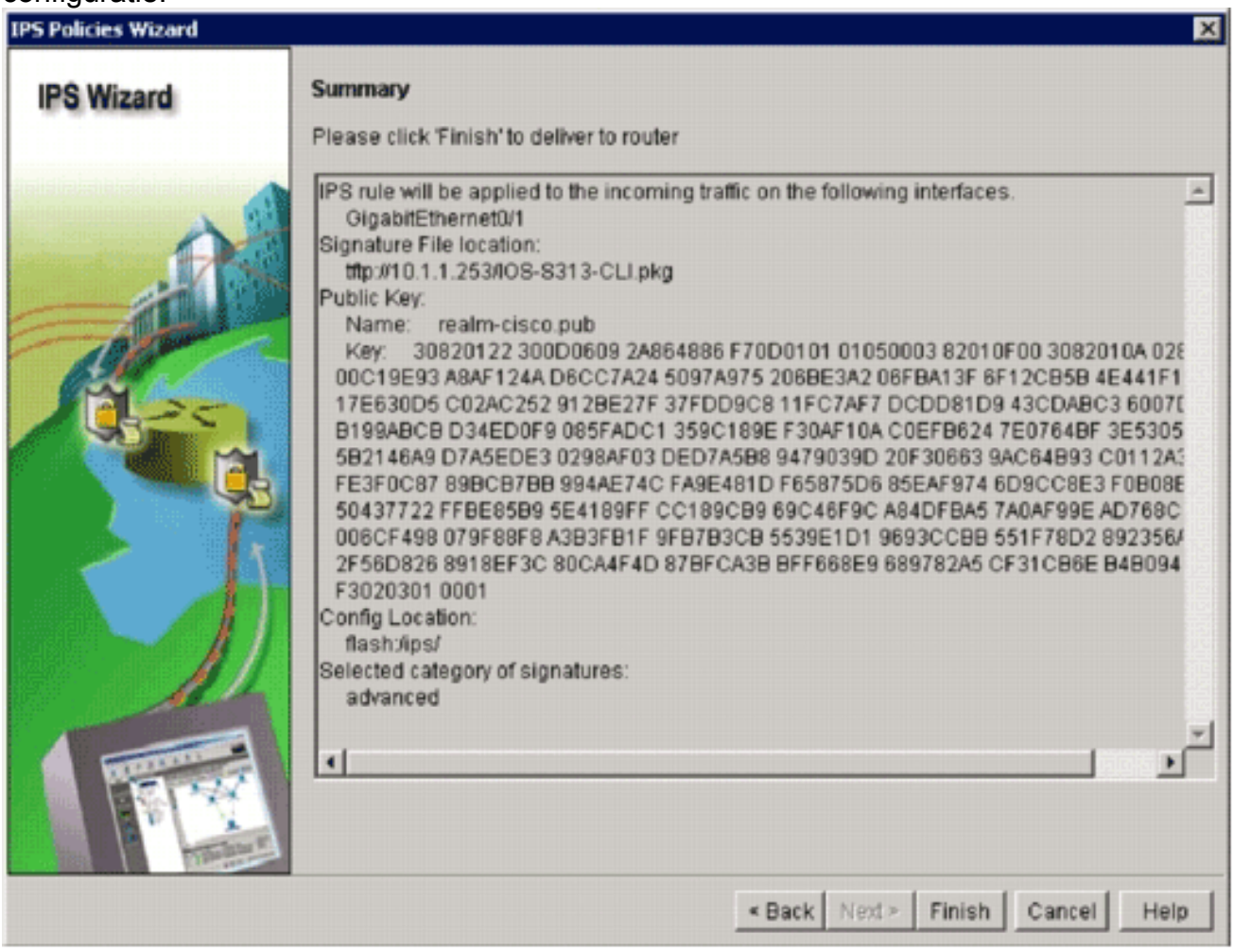
verschijnt.

24. In het dialoogvenster Locatie toevoegen klikt u op de **knop Locatie opgeven op deze router** en vervolgens klikt u op de knop **Map Name** (...) om het configuratiebestand te vinden.Het dialoogvenster Map kiezen verschijnt als u een bestaande map wilt selecteren of een nieuwe map wilt maken in de routerflitser om de definitie- en configuratiebestanden van de handtekening op te slaan.

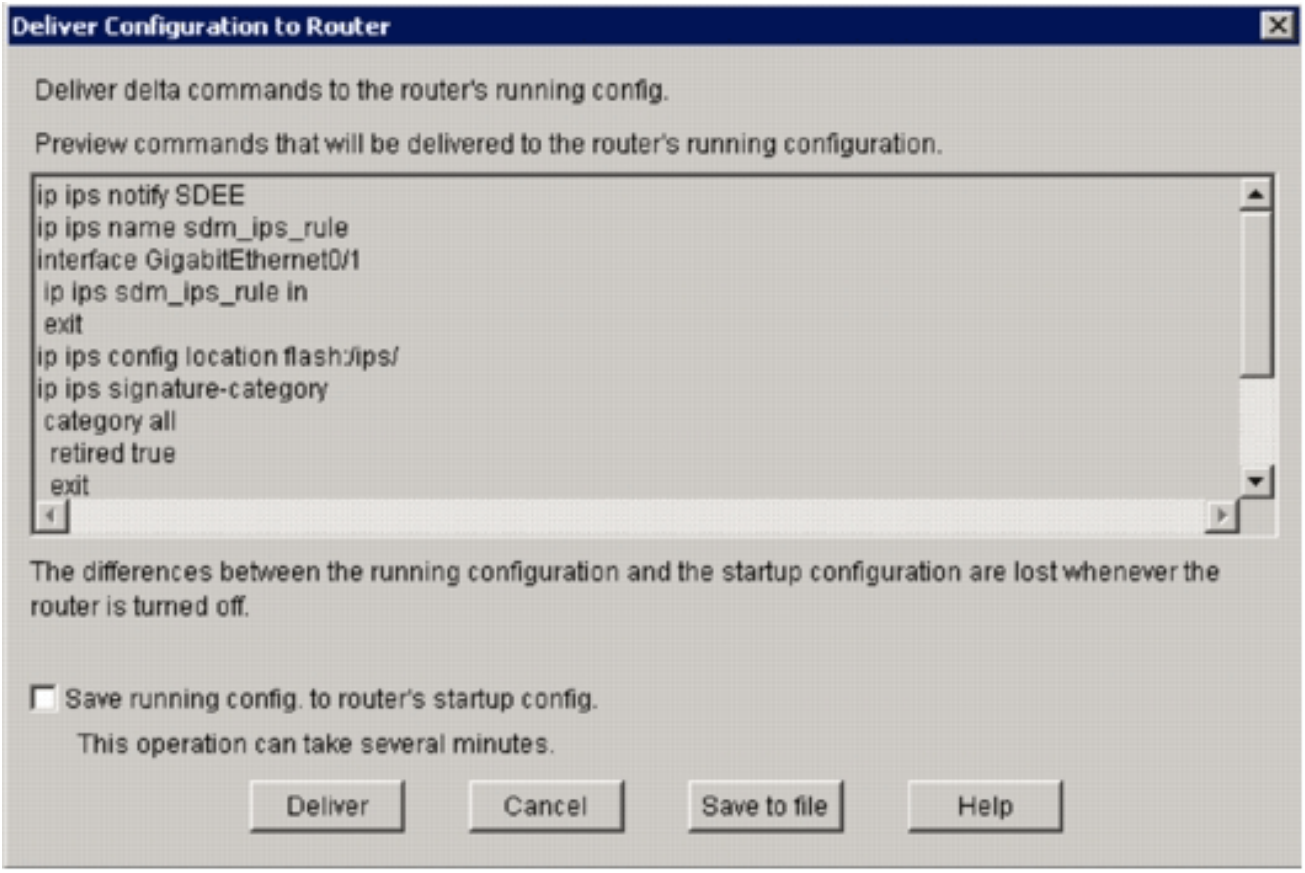


25. Klik op **Nieuwe map** boven in het dialoogvenster als u een nieuwe map wilt maken.

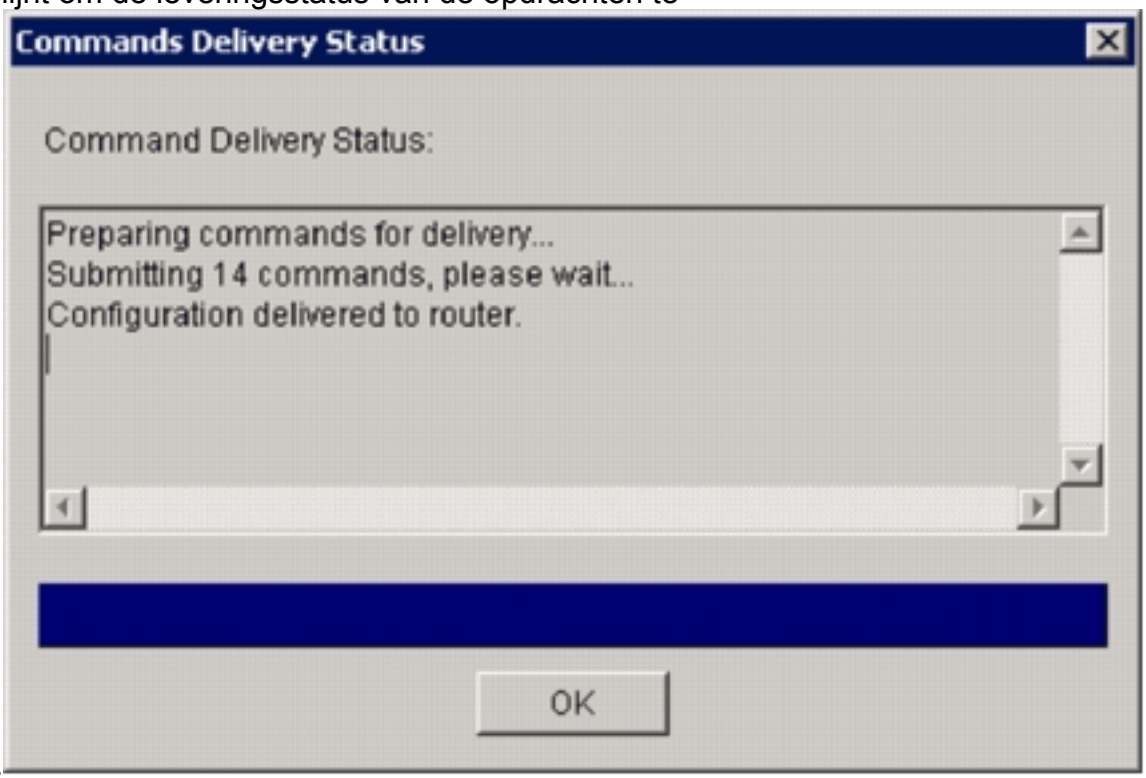
26. Nadat u de map hebt geselecteerd, klikt u op **OK** om wijzigingen toe te passen en vervolgens klikt u op **OK** om het dialoogvenster Plaatsing toevoegen te sluiten.
27. In het dialoogvenster Wizard Beleid van IPS selecteert u de categorie voor de handtekening op basis van de hoeveelheid geheugen die op de router is geïnstalleerd. Er zijn twee signatuur categorieën u kunt kiezen in middel van het middel. Basis en geavanceerd.Als de router 128 MB DRAM geïnstalleerd heeft, raadt Cisco u aan om de Basiscategorie te kiezen om fouten in de geheugentoewijzing te voorkomen. Als de router 256MB of meer DRAM heeft geïnstalleerd, kunt u een van beide categorieën kiezen.
28. Nadat u een te gebruiken categorie hebt geselecteerd, klikt u op **Volgende** om verder te gaan naar de overzichtspagina.De summiere pagina biedt een korte beschrijving van de taken IOS IPS eerste
configuratie.



29. Klik op **Voltooien** op de overzichtspagina om de configuraties en het pakket voor handtekeningen aan de router te leveren.Als de voorproefopdrachten optie op de instellingen Voorkeuren in DIT wordt ingeschakeld, toont dm de configuratie van de Levering aan het dialoogvenster van de router die een samenvatting van de opdrachten van CLI toont die sdm aan de router
levert.

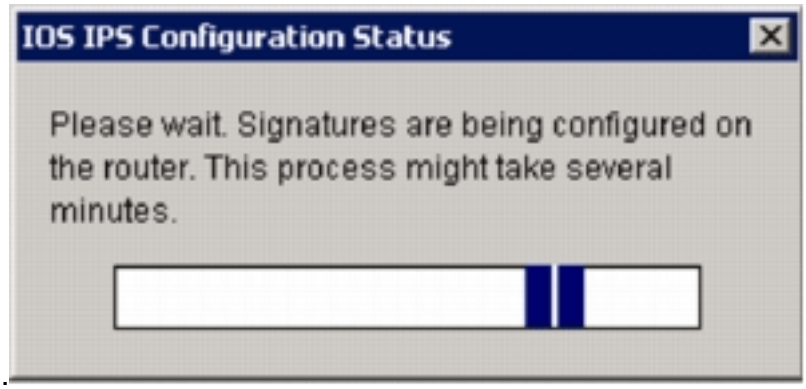


30. Klik op **Levering** om verder te gaan.Het dialoogvenster Leveringsstatus van Opdrachten verschijnt om de leveringsstatus van de opdrachten te



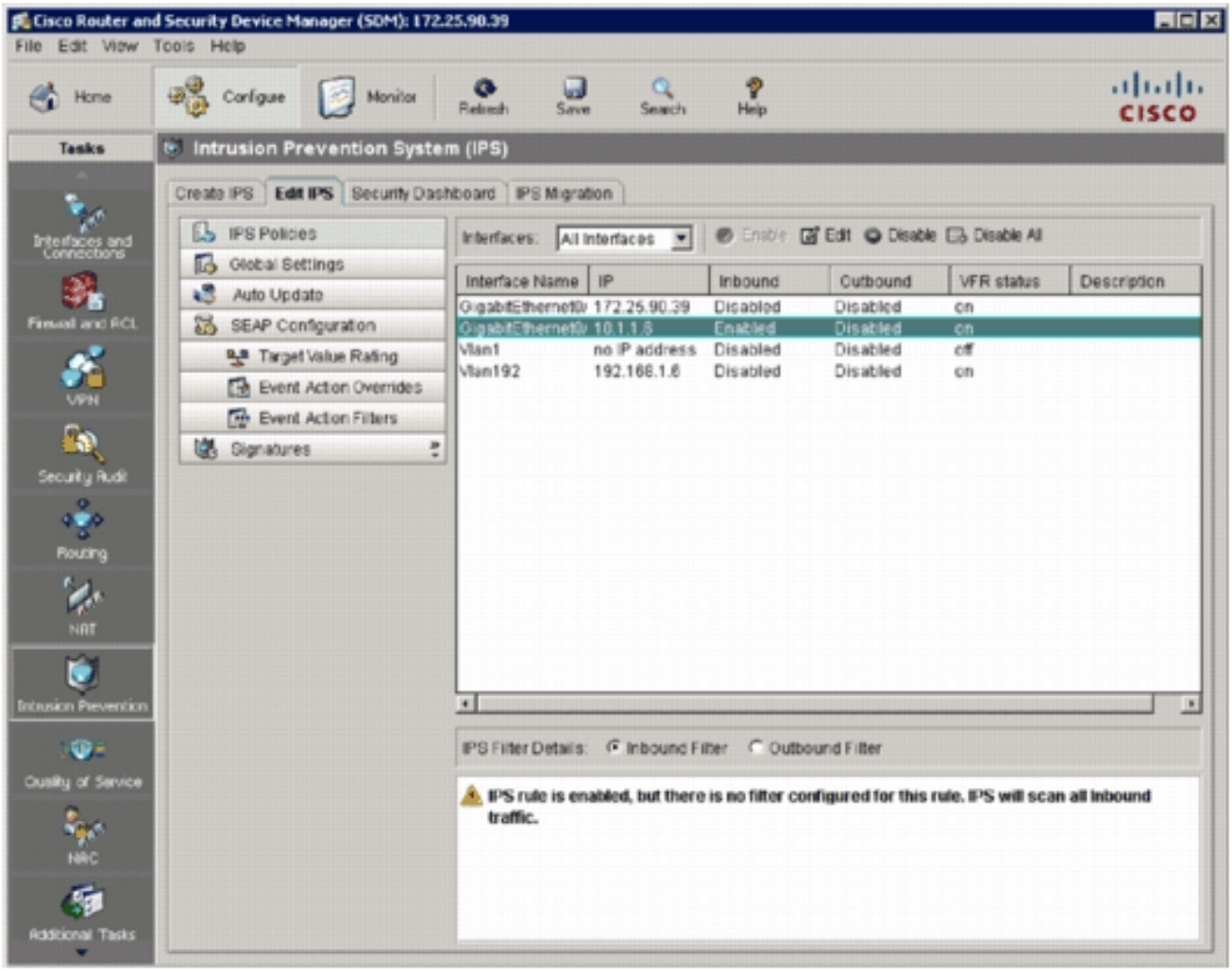
tonen.

31. Wanneer de opdrachten aan de router worden afgeleverd, klikt u op **OK** om door te gaan.Het dialoogvenster IOS IPS Configuration Status toont aan dat de handtekeningen op

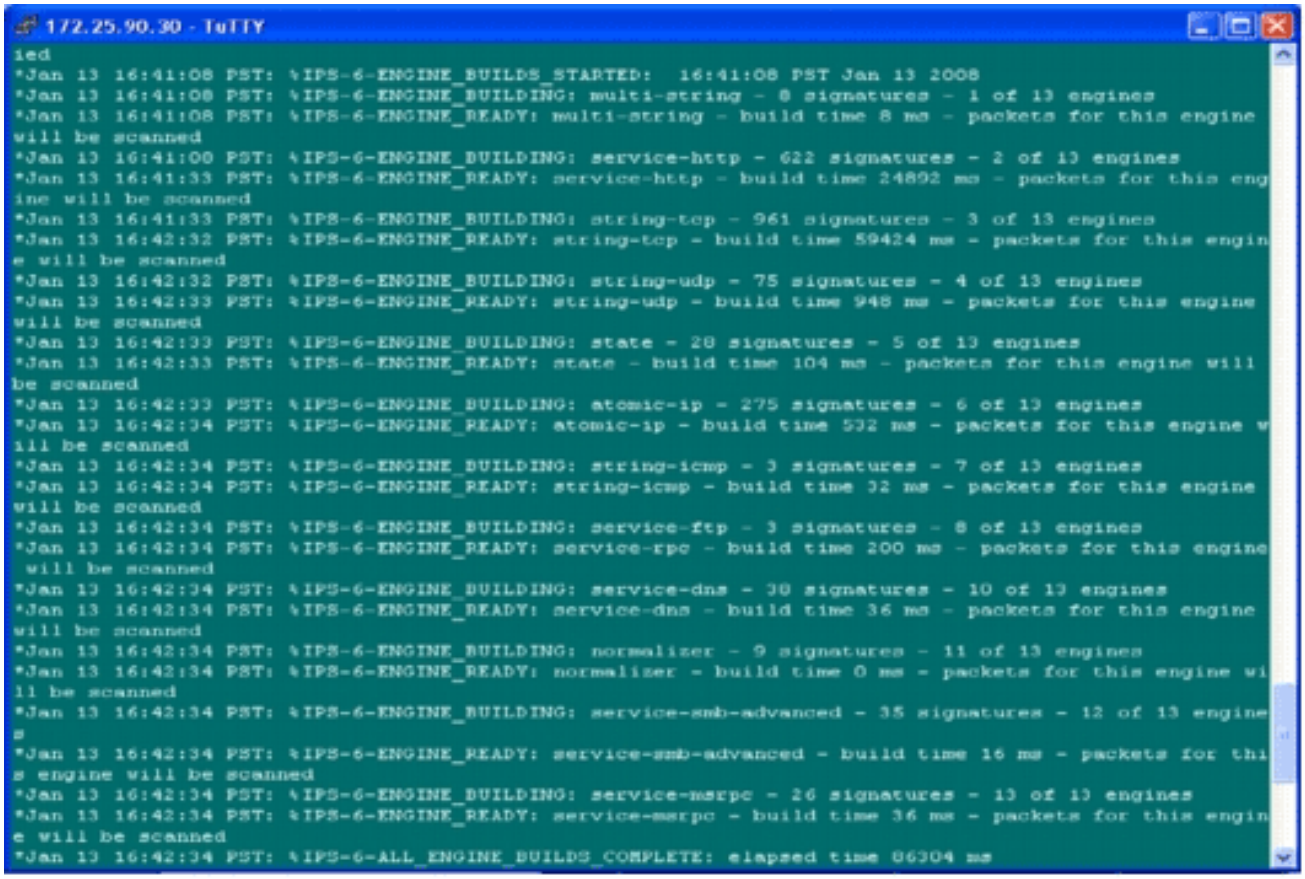


de router worden geladen.

32. Wanneer de handtekeningen worden geladen, toont het tabblad **Bewerken IPS** met de huidige configuratie. Controleer welke interface en in welke richting IOS IPS is ingeschakeld om de configuratie te controleren.



De routerconsole toont aan dat de handtekeningen zijn geladen.

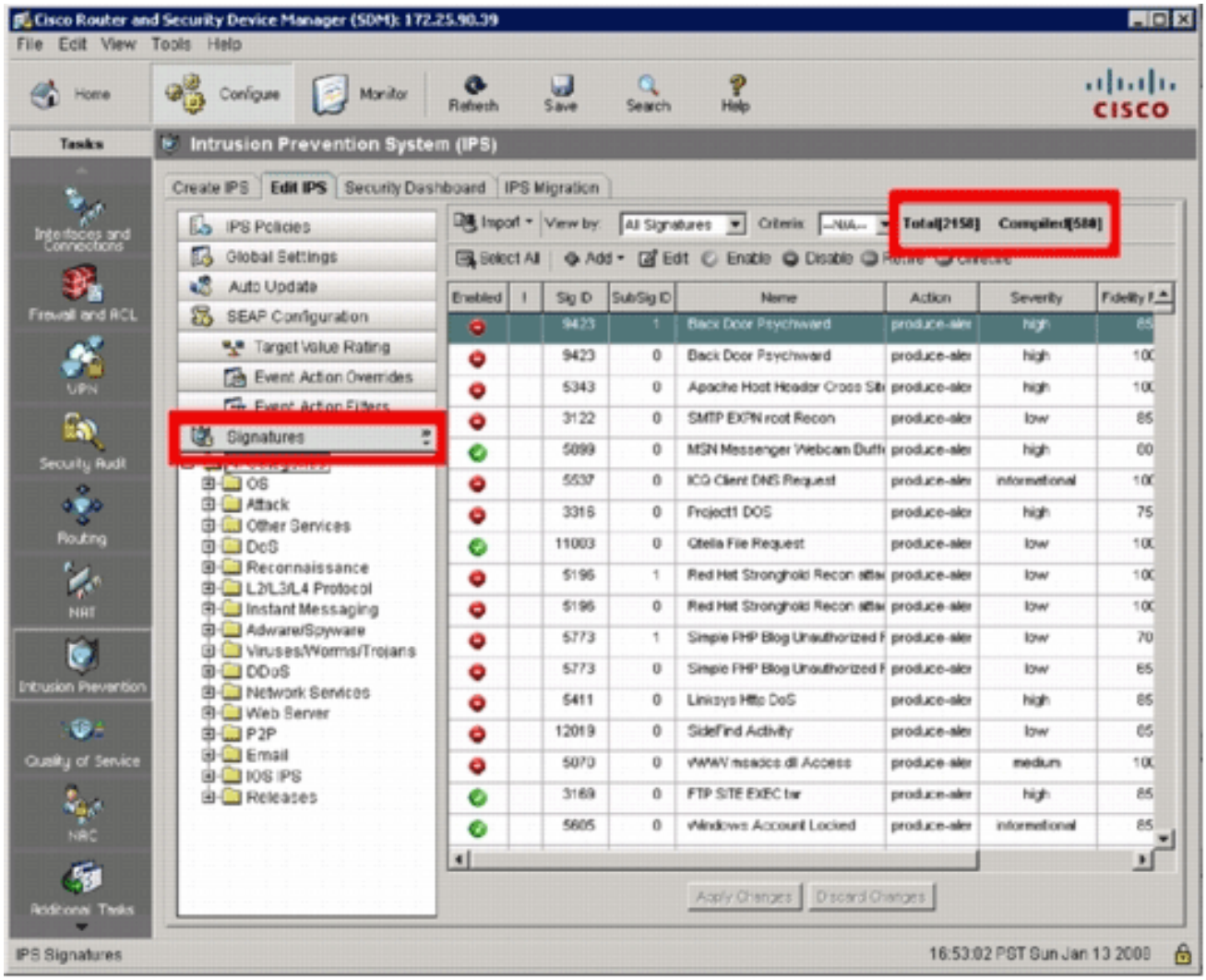


33. Gebruik de opdracht **ip IPS-handtekeningen tellen** om te controleren of de handtekeningen correct geladen zijn.

```
router#show ip ips signatures count
Cisco SDF release version S313.0
Trend SDF release version V0.0
|
snip
|
Total Signatures: 2158
 Total Enabled Signatures: 829
 Total Retired Signatures: 1572
 Total Compiled Signatures: 580
 Total Signatures with invalid parameters: 6
         Total Obsoleted Signatures: 11
```

De eerste voorziening van IOS IPS met middel van dm 2.5 is compleet.

34. Controleer de handtekening nummers met sdm zoals getoond in deze afbeelding.



Gerelateerde informatie

- Cisco IOS IPS op Cisco.com
- Cisco IOS IPS-signaalpakket
- Cisco IOS IPS-handtekeningen voor DSM
- Om aan de slag te gaan met Cisco IOS IPS met bestandsindeling voor 5.x-handtekeningen
- Cisco IOS IPS-configuratiegids
- Cisco IDS-Event Viewer
- Technische ondersteuning en documentatie – Cisco Systems