Security Manager configureren in Cisco IOS IPS

Inhoud

Inleiding

Cisco Security Manager maakt deel uit van Cisco Security Management Suite, dat uitgebreid beleidsbeheer en -handhaving biedt voor het Cisco Zelfverdedigend Network. Cisco Security Manager is een toonaangevende toepassing op bedrijfsniveau voor het beheer van de beveiliging. Cisco Security Manager richt op configuratiebeheer van firewall, VPN en IPS (Inbraakpreventiesysteem) security services voor Cisco routers, security apparaten en beveiligingsservicesmodules.

Voor een samenvatting van de functies en voordelen van Cisco Security Manager, evenals de nieuwe functies in versie 3.1, raadpleegt u het Cisco Security Manager 3.1 gegevensblad op http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html. U kunt Cisco Security Manager 3.1 downloaden van Cisco.com op http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app (alleen [geregistreerde](#) klanten).

Dit document beschrijft hoe u Cisco Security Manager 3.1 kunt gebruiken om initiële configuratie van IOS IPS uit te voeren. Voor routers die al met IOS IPS zijn ingesteld, kunnen klanten Cisco Security Manager 3.1 rechtstreeks gebruiken voor provisioningtaken.

Opmerking: Cisco Security Manager 3.1 ondersteunt alleen IOS 12.4(11)T2 en later IOS-afbeeldingen om IOS IPS te configureren.

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 Security Manager 3.1
- Cisco IOS-softwarerelease 12.4(11)T2

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.
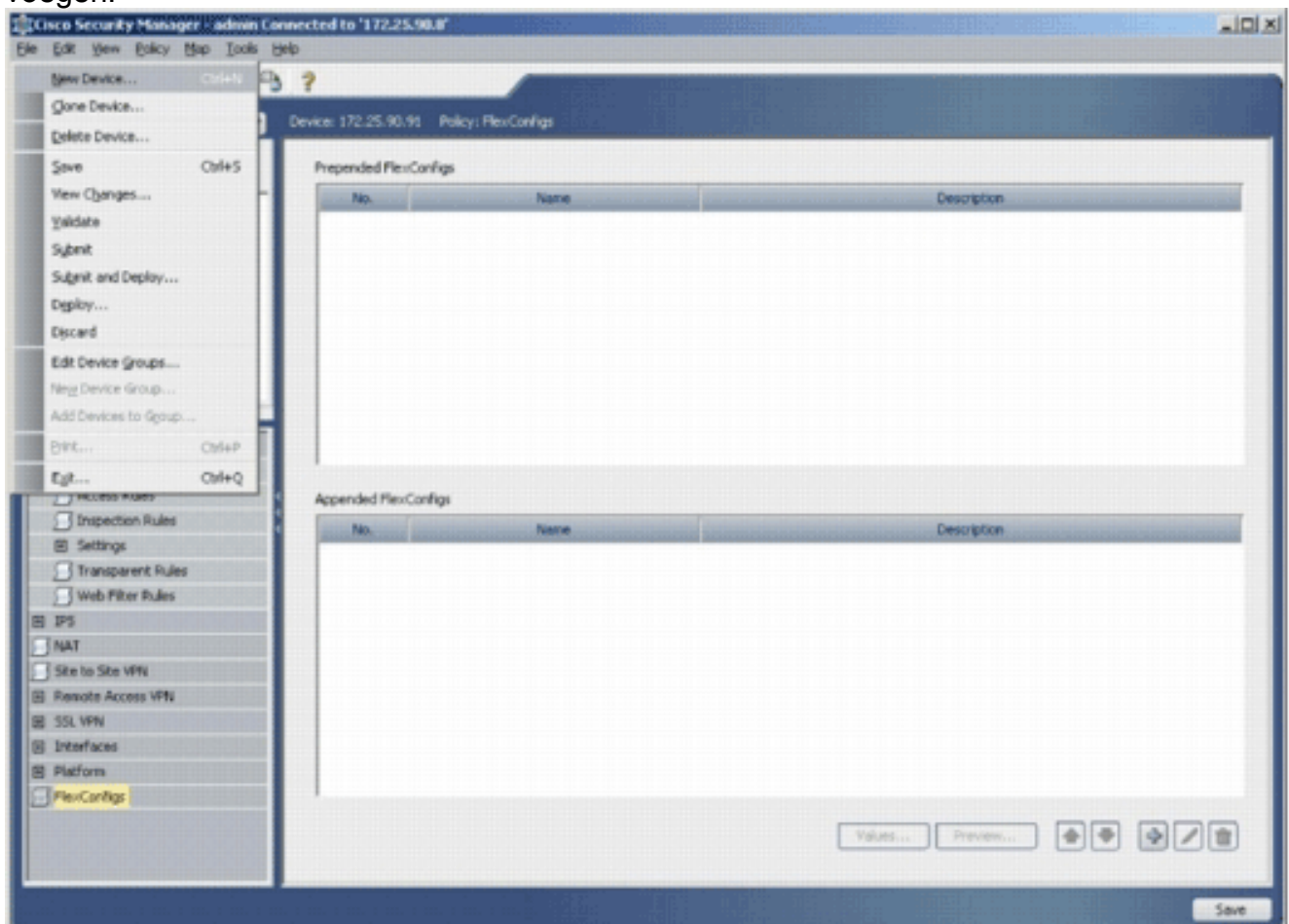
Conventies

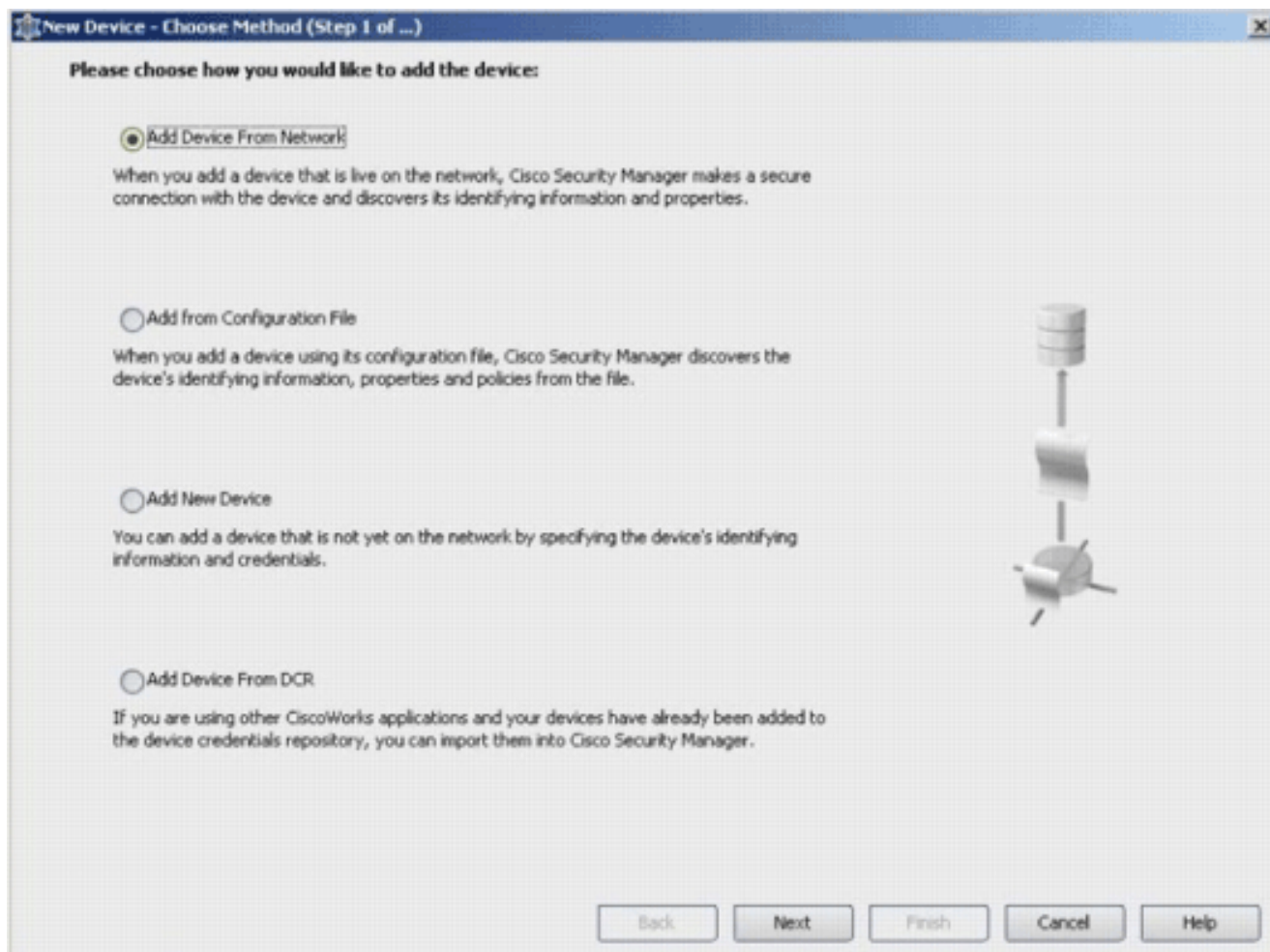Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Voltooi deze stappen om IOS IPS te configureren:

1. Start de Cisco Security Manager 3.1 client op uw lokale pc.
2. Kies **Nieuw apparaat** in het menu Bestand om een apparaat aan Cisco Security Manager 3.1 toe te voegen.

3. Kies in het venster Nieuw apparaat hoe u het apparaat wilt toevoegen. Dit voorbeeld voegt het apparaat van het netwerk toe.

```
New Device - Choose Method (Step 1 of ...)                              [x]

Please choose how you would like to add the device:

  ⦿ Add Device From Network
    When you add a device that is live on the network, Cisco Security Manager makes a secure
    connection with the device and discovers its identifying information and properties.


  ◯ Add from Configuration File
    When you add a device using its configuration file, Cisco Security Manager discovers the
    device's identifying information, properties and policies from the file.


  ◯ Add New Device
    You can add a device that is not yet on the network by specifying the device's identifying
    information and credentials.


  ◯ Add Device From DCR
    If you are using other CiscoWorks applications and your devices have already been added to
    the device credentials repository, you can import them into Cisco Security Manager.




            [ Back ]   [ Next ]   [ Finish ]   [ Cancel ]   [ Help ]
```

4. Klik op **Volgende**.
5. Voer de identiteitsgegevens in voor het apparaat dat u wilt toevoegen. Bijvoorbeeld, naam van de gastheer en IP adres.

6. Klik op **Volgende**.

7. Voer de primaire geloofsbrieven in, zoals gebruikersnaam, wachtwoord, Wachtwoord voor de IOS router in die u wilt toevoegen.

8. Klik op **Voltooien** om het apparaat aan Cisco Security Manager toe te voegen.**Opmerking:** Dit voorbeeld veronderstelt dat de gebruiker reeds een vooraf ingestelde router heeft en aan de router met de juiste geloofsbrieven kan inloggen.

Wanneer "Discovery fied" in het venster Discovery Status verschijnt, hebt u met succes een apparaat aan Cisco Security Manager toegevoegd. Zodra u een apparaat aan Cisco Security Manager hebt toegevoegd, moet u een openbare sleutel toewijzen om IPS mogelijk te maken.

Discovery Status — 100%

Status: Discovery completed with warnings
Devices to be discovered: 1
Devices discovered successfully: 1
Devices discovered with errors: 0

Discovery Details

Type	Name	Severity	State	Discovered From
🌐	172.25.90.91	ⓘ	Discovery Completed with Warnings	Live Device

Messages	Severity
Interfaces wide open for traffic	⚠
Policies discovered	ⓘ
Existing policy objects reused	ⓘ
IPS signature policy not discovered.	⚠
Add Device Successful	ⓘ

Description
The following interfaces are wide open for traffic as there is no ACL applied on them. Adding a new Access-rule on these interfaces means that there will no longer be such implicit permission of traffic anymore:
FastEthernet0
FastEthernet1
FastEthernet2
FastEthernet3
FastEthernet4

Action
Please verify whether these interfaces need to be wide open for all types of traffic. If not, configure an access rule or ACL accordingly.

Abort | Close | Help

9. Blader in het menu links naar het configuratiescherm FlexConfiguration.
10. Klik op de FlexConfiguration-gebruikersinterface aan de rechterkant van het scherm en klik
vervolgens op het pictogram
Add.
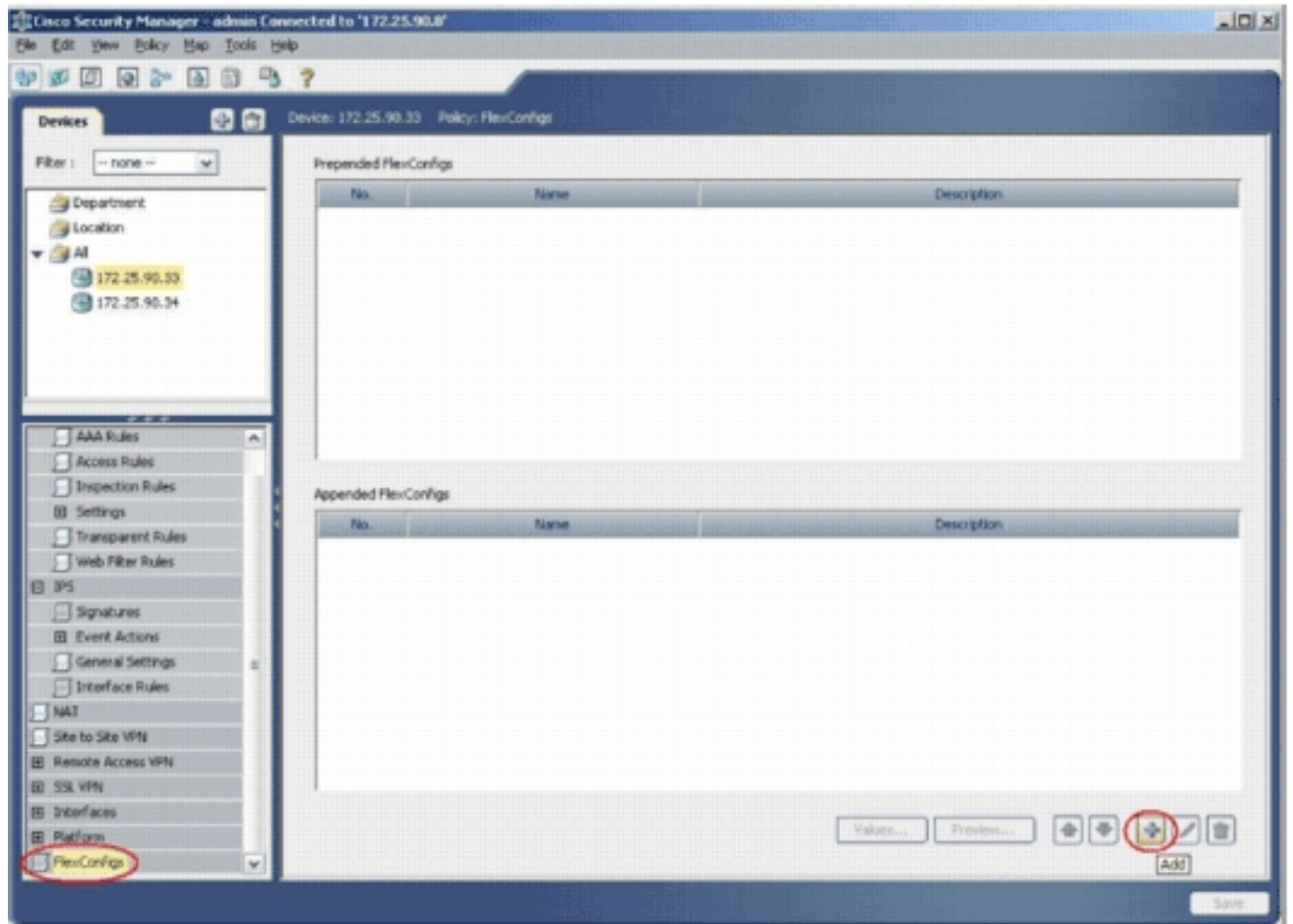
11. In de Geselecteerde FlexConfiguration lijst kiest u **IOS_IPS_PUBLIC_KEY** en klikt u op **OK**.
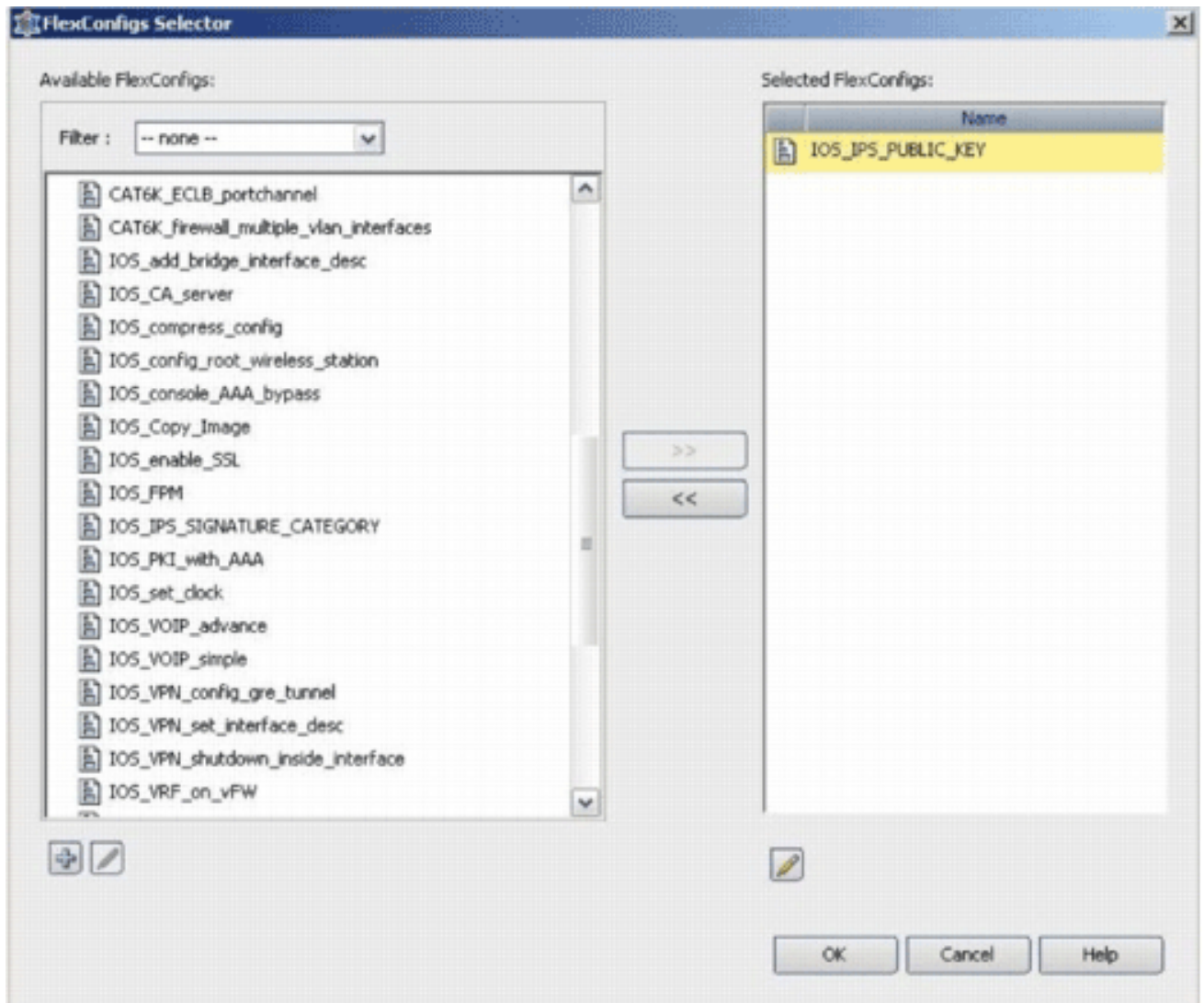
12. Klik op **Opslaan** om de wijzigingen op te slaan.**Opmerking:** IOS_IPS_PUBLIC_KEY FlexConfig houdt de configuratie voor de openbare toets vast.

13. Kies in het menu links de optie **Algemene instellingen** onder de IPS-kop.

14. Geef de configuratielocatie van IPS op de flitser op. Dit is de plaats waar de IPS configuraties worden geplaatst.
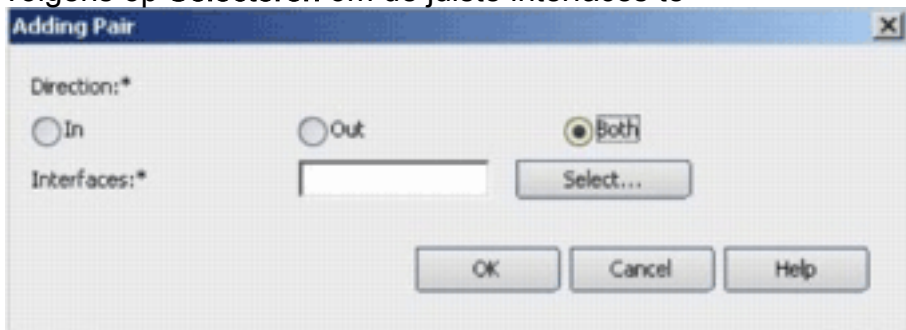
15. Klik op **Opslaan** om de wijzigingen op te slaan.
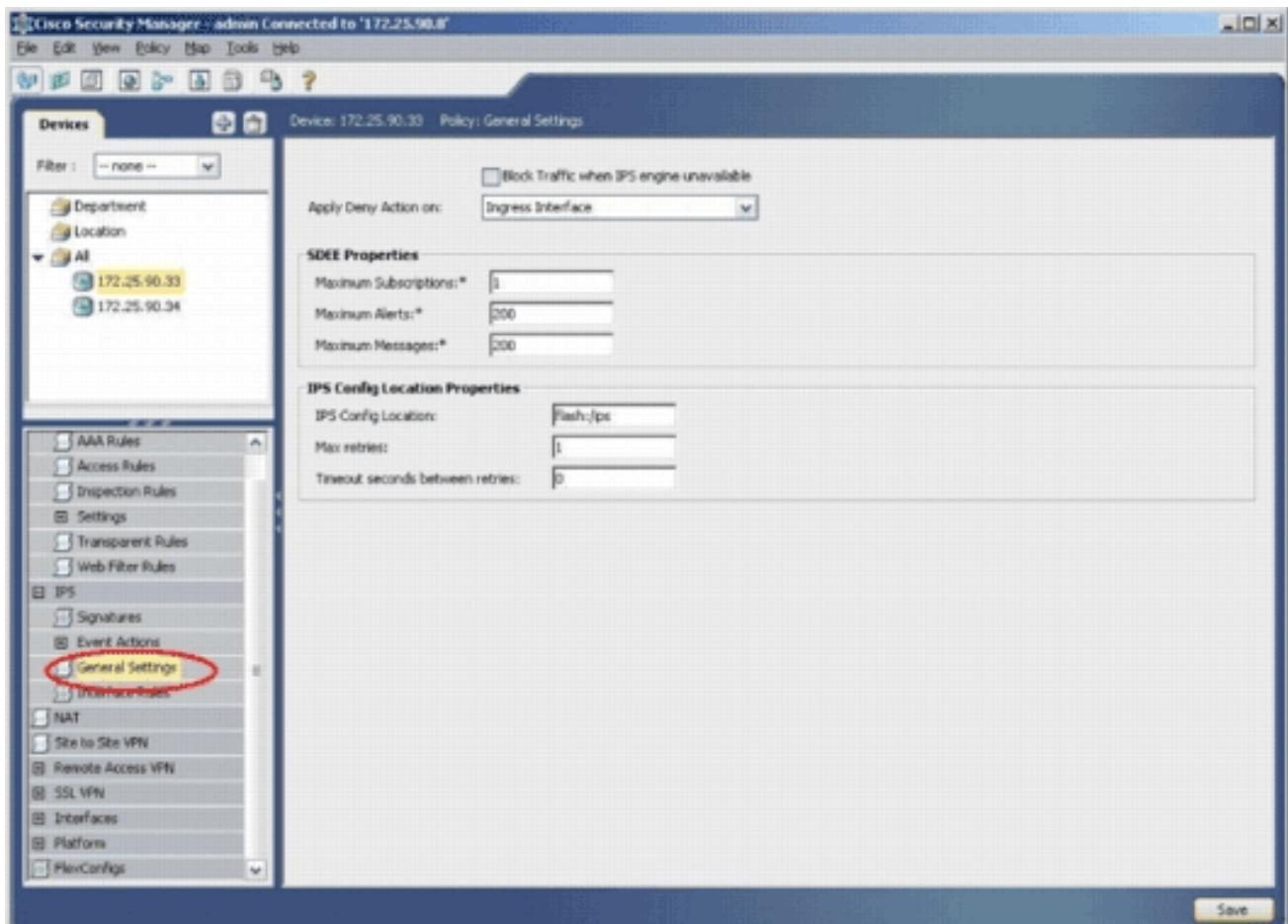
Opmerking: Controleer of de locatiemap al op routerflitser is gemaakt. Als dit niet het geval is, gebruik dan de opdracht **mkdir <folder_name>** om de adresmap te maken.

16. Om IPS mogelijk te maken, navigeer naar interfaceregels, controleer het vakje **IPS inschakelen** en klik vervolgens op **Weg toevoegen**.

17. In het dialoogvenster Toevoegen IPS-regel typt u een naam voor de IPS-regel in het veld Naam regel en vervolgens klikt u op **Row toevoegen** om de interfaces op te nemen waarop IPS moet worden
toegepast.
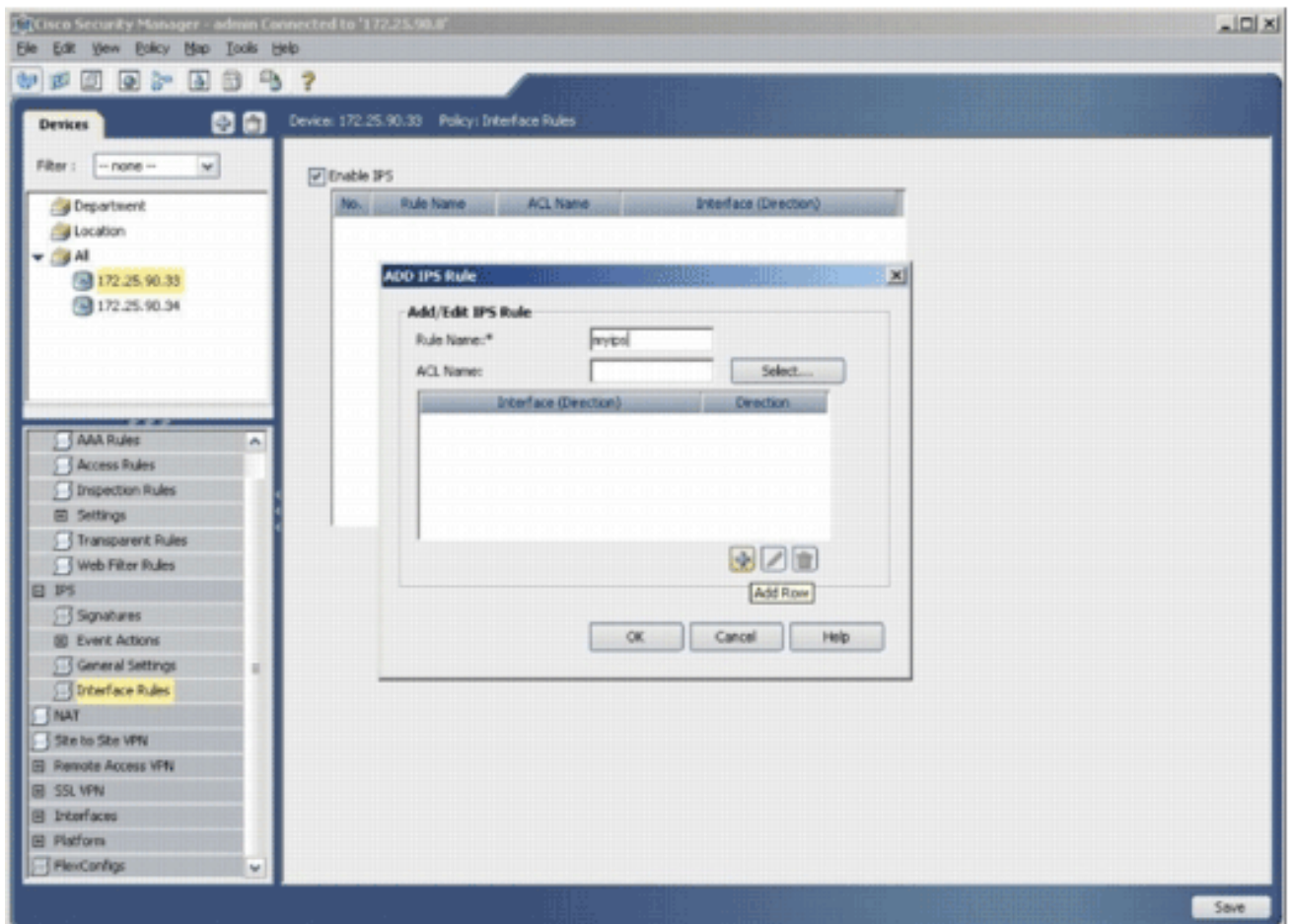
18. Klik op de radioknop die aangeeft in welke richting de IPS-regel moet worden toegepast en klik vervolgens op **Selecteren** om de juiste interfaces te

kiezen.

19. Kies een interface in de lijst Interfaceselector en klik op
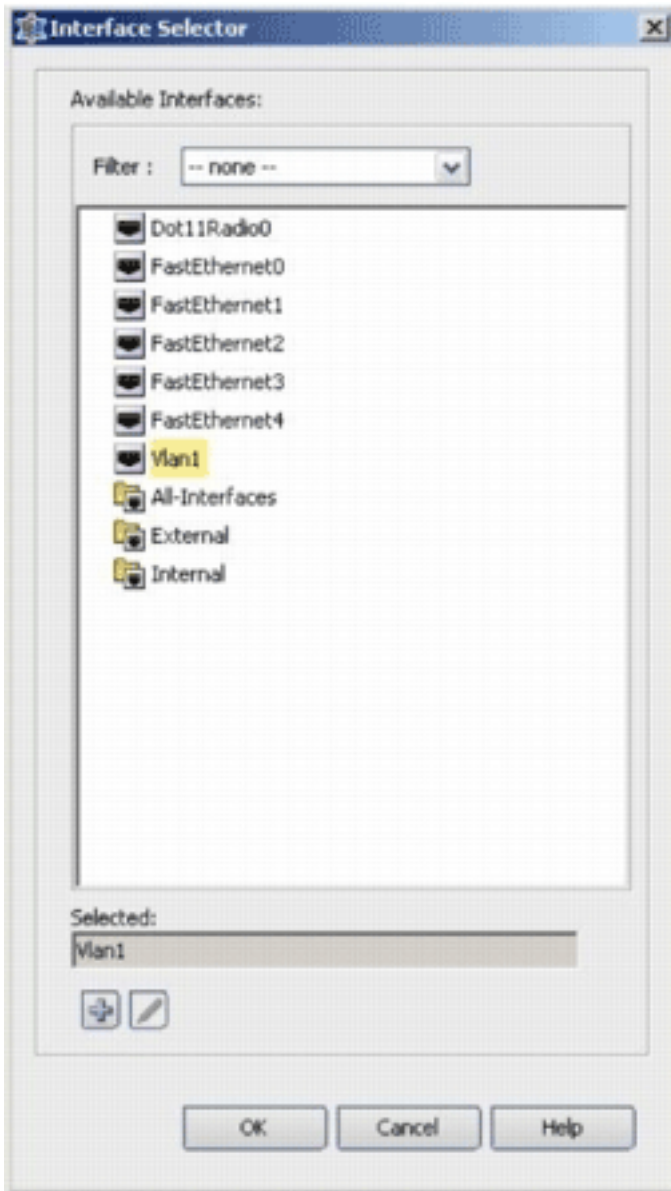
OK.

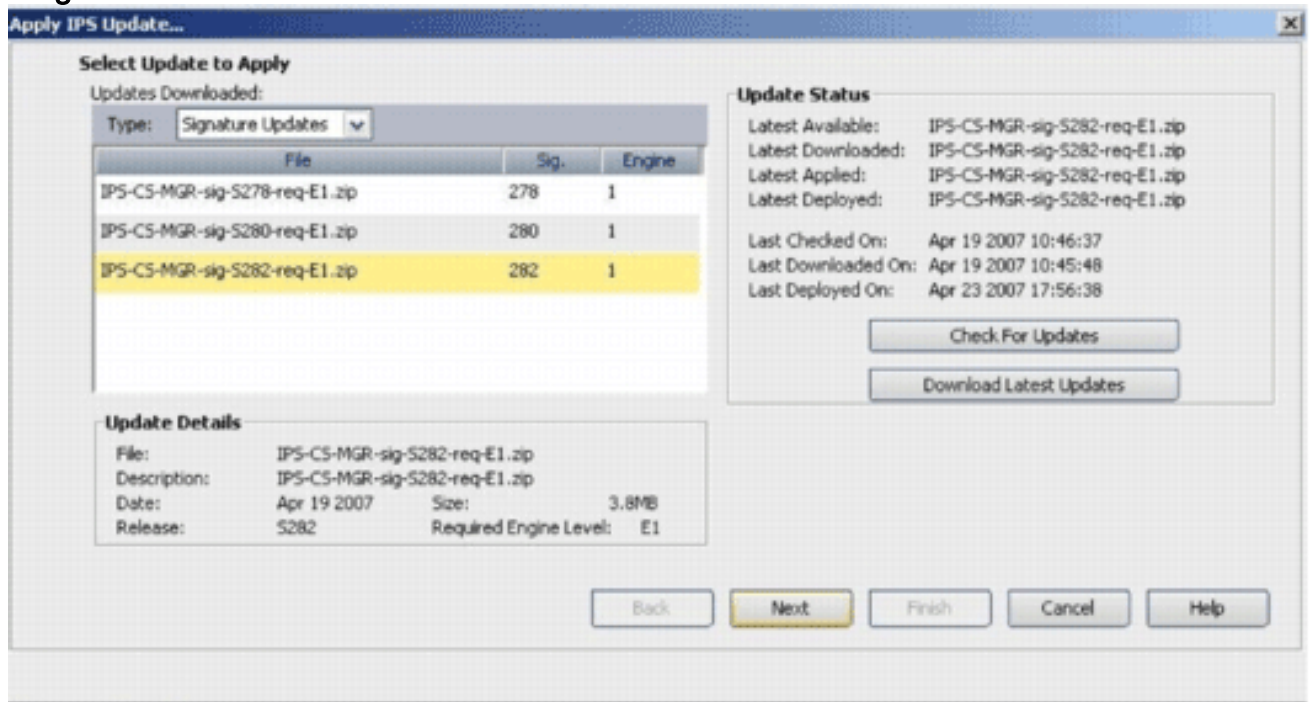20. Klik op **Opslaan** om de wijzigingen op te
slaan.
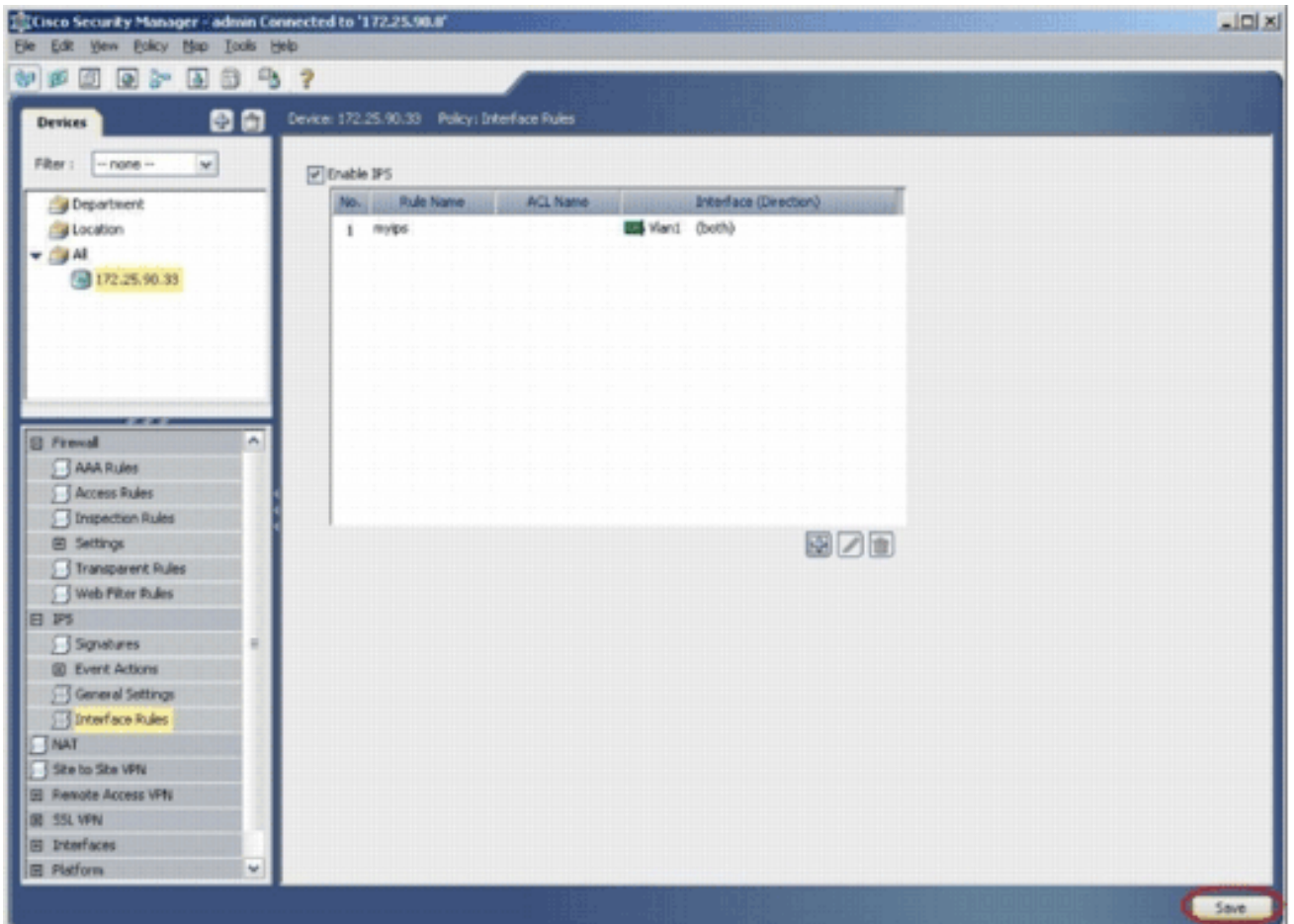
21. Kies **Gereedschappen > IPS**-bijwerking **toepassen** om de laatste IPS-handtekeningen te installeren.
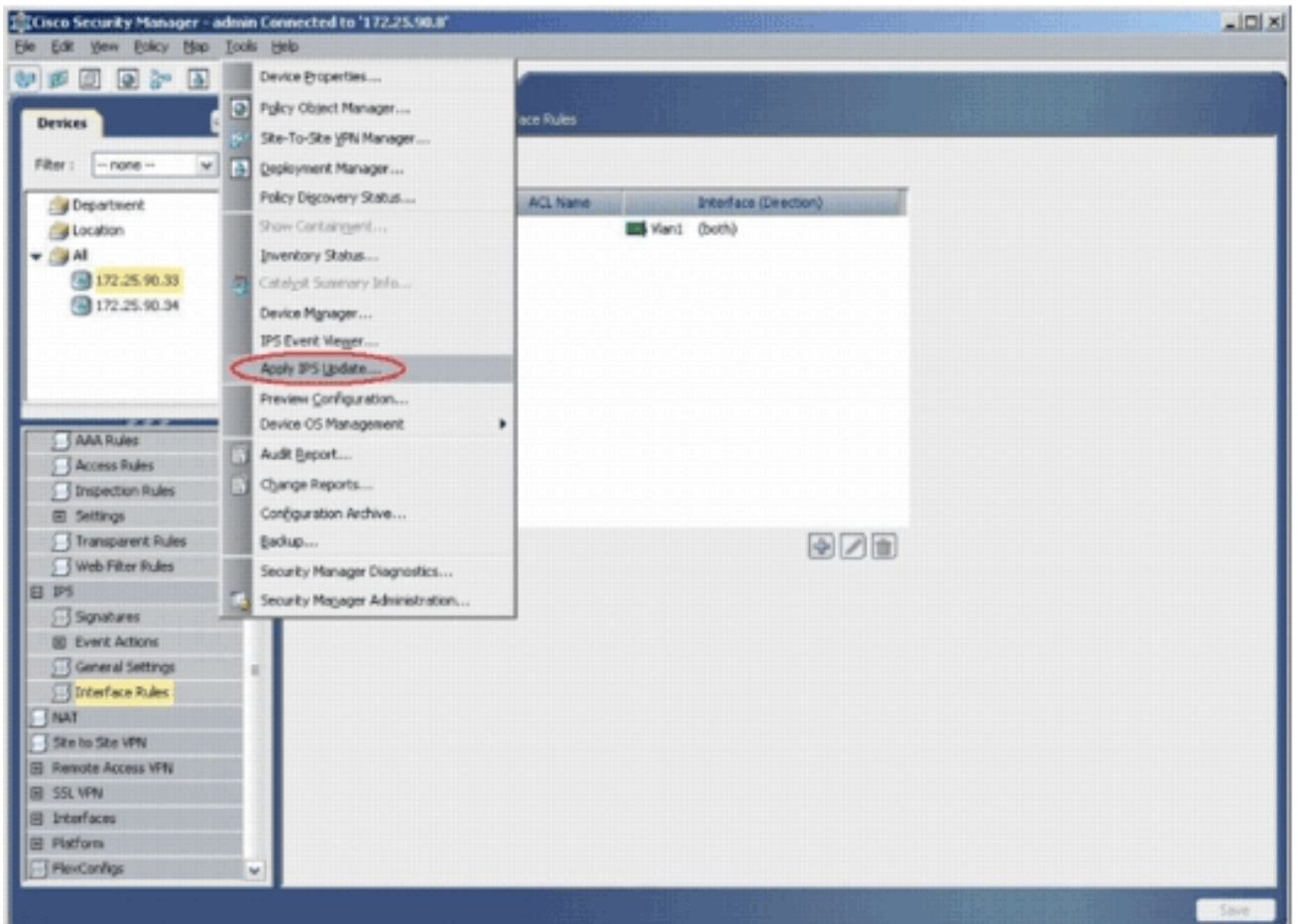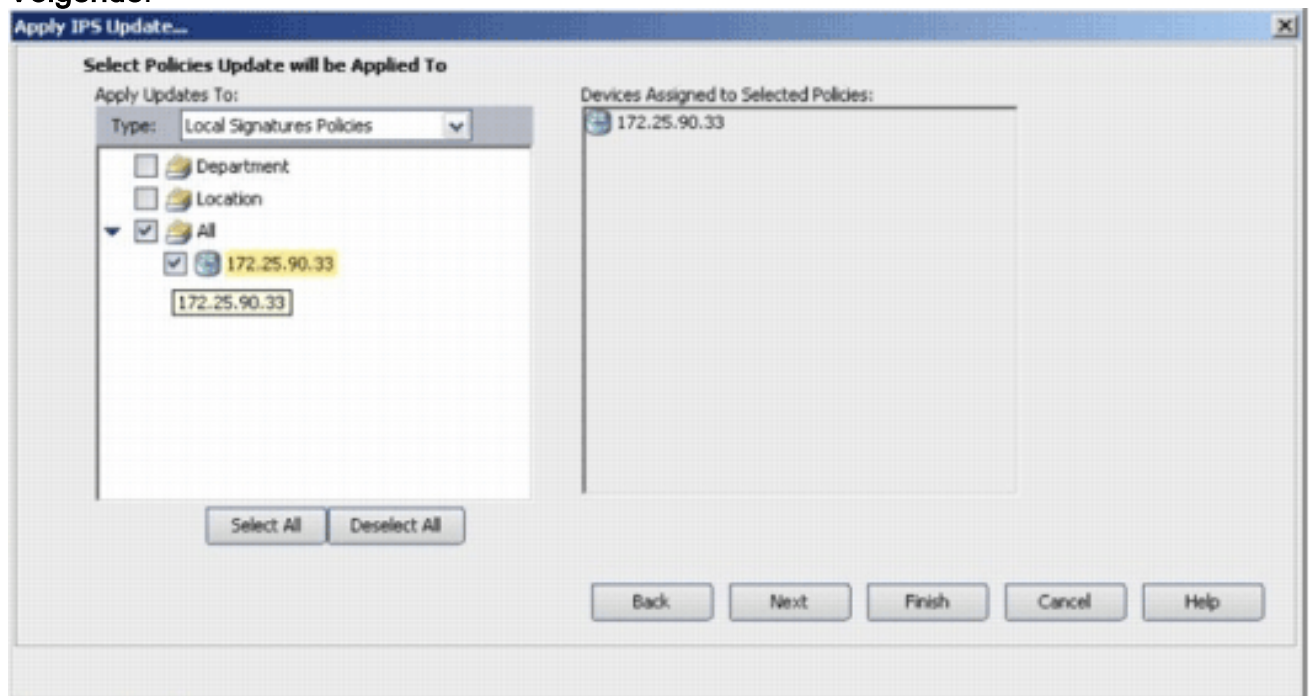

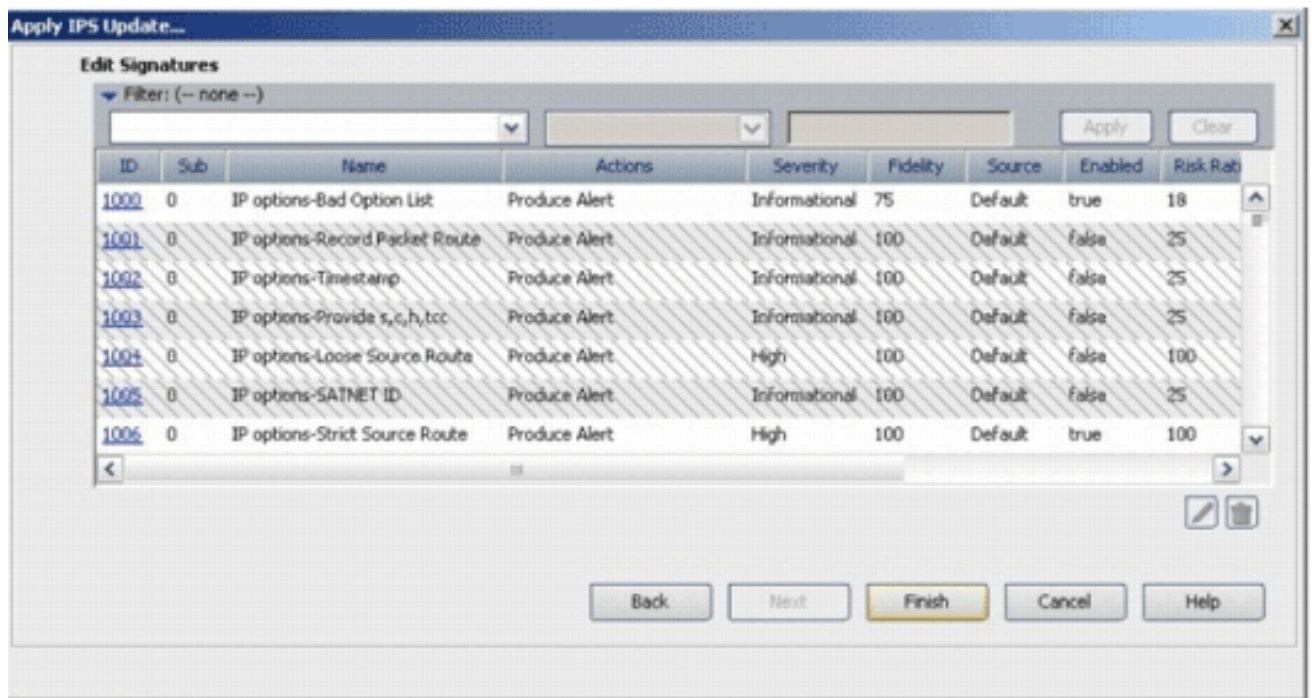
22. Kies het nieuwste bestand voor handtekening en klik op
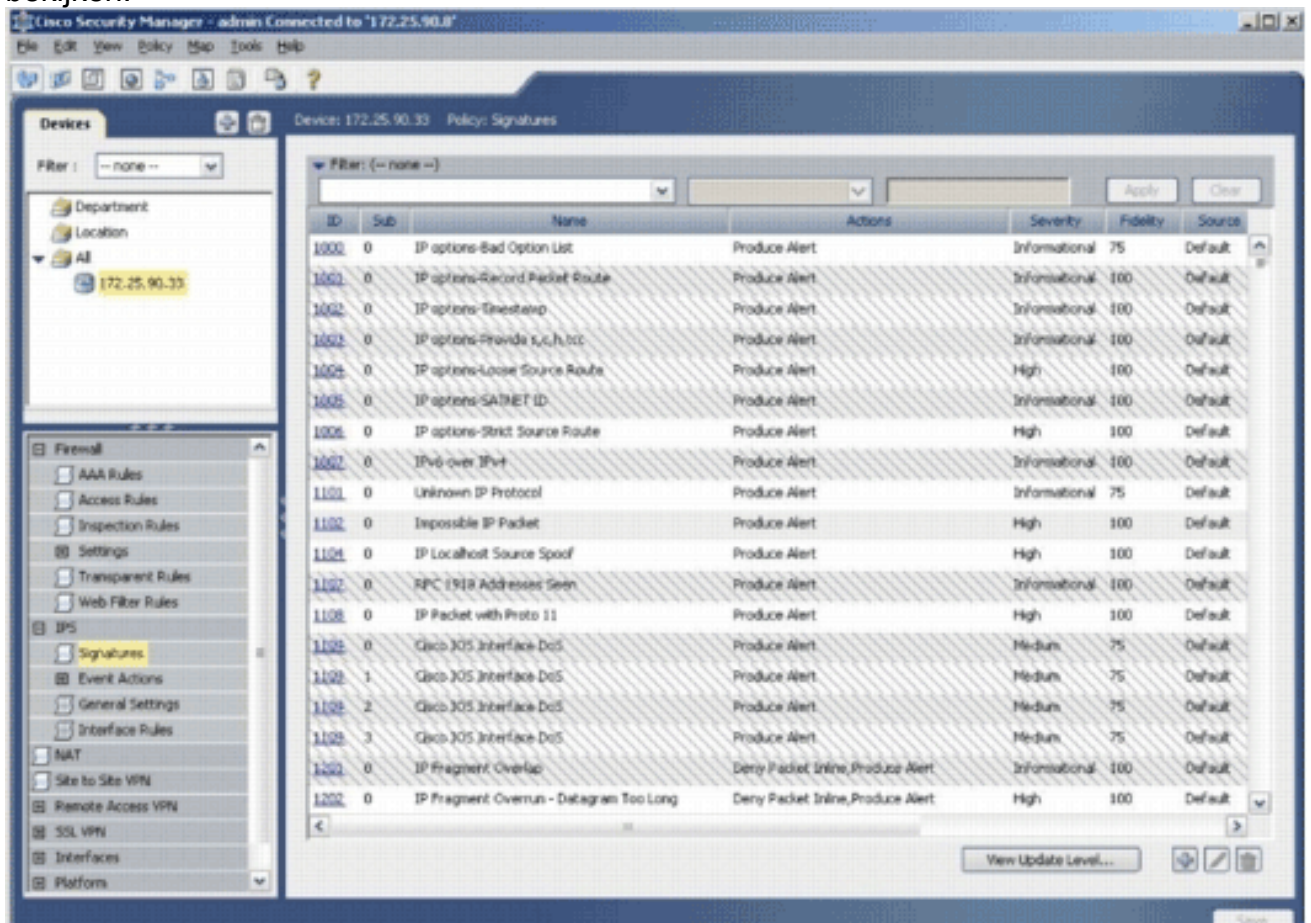
Volgende.

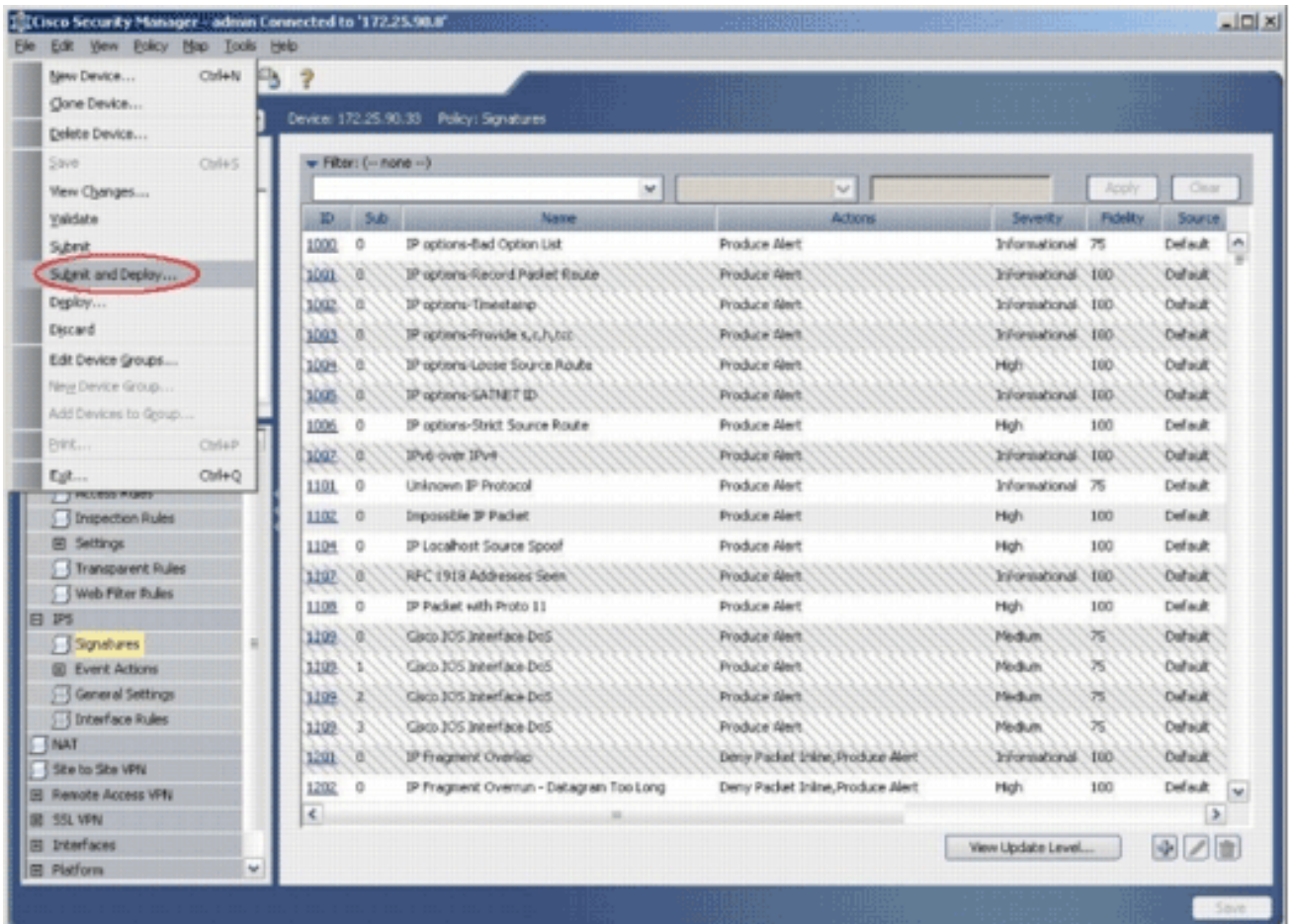23. Kies de apparaten waarop de IPS-update moet worden toegepast en klik op **Volgende**.

24. Klik op **Voltooien** om de handtekeningen toe te passen.
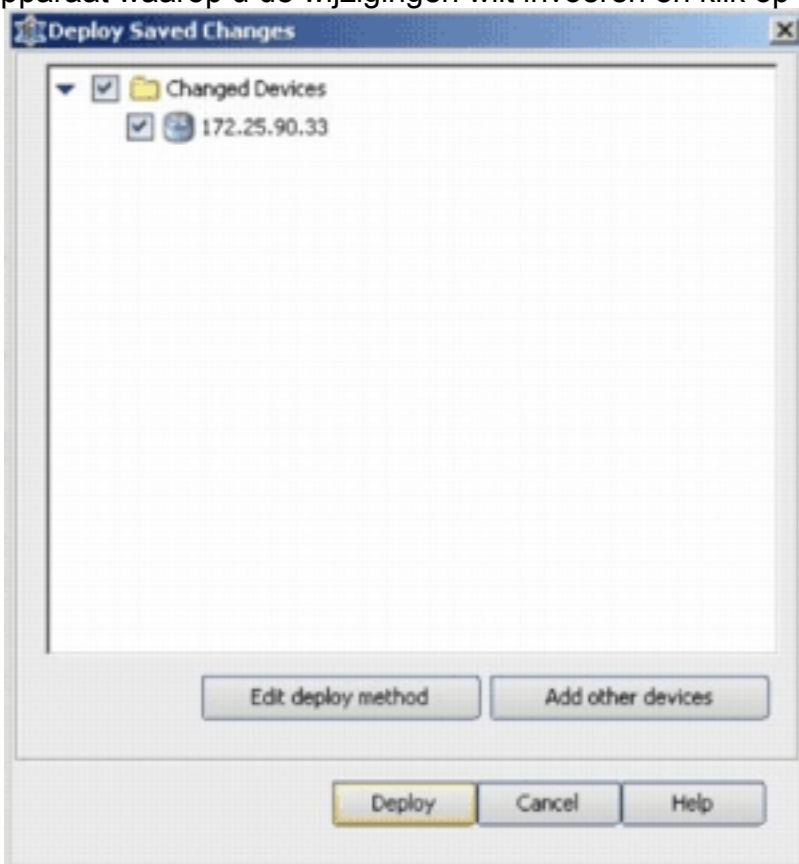
25. Blader naar IPS en kies **Handtekeningen** om de lijst met alle handtekeningen te bekijken.

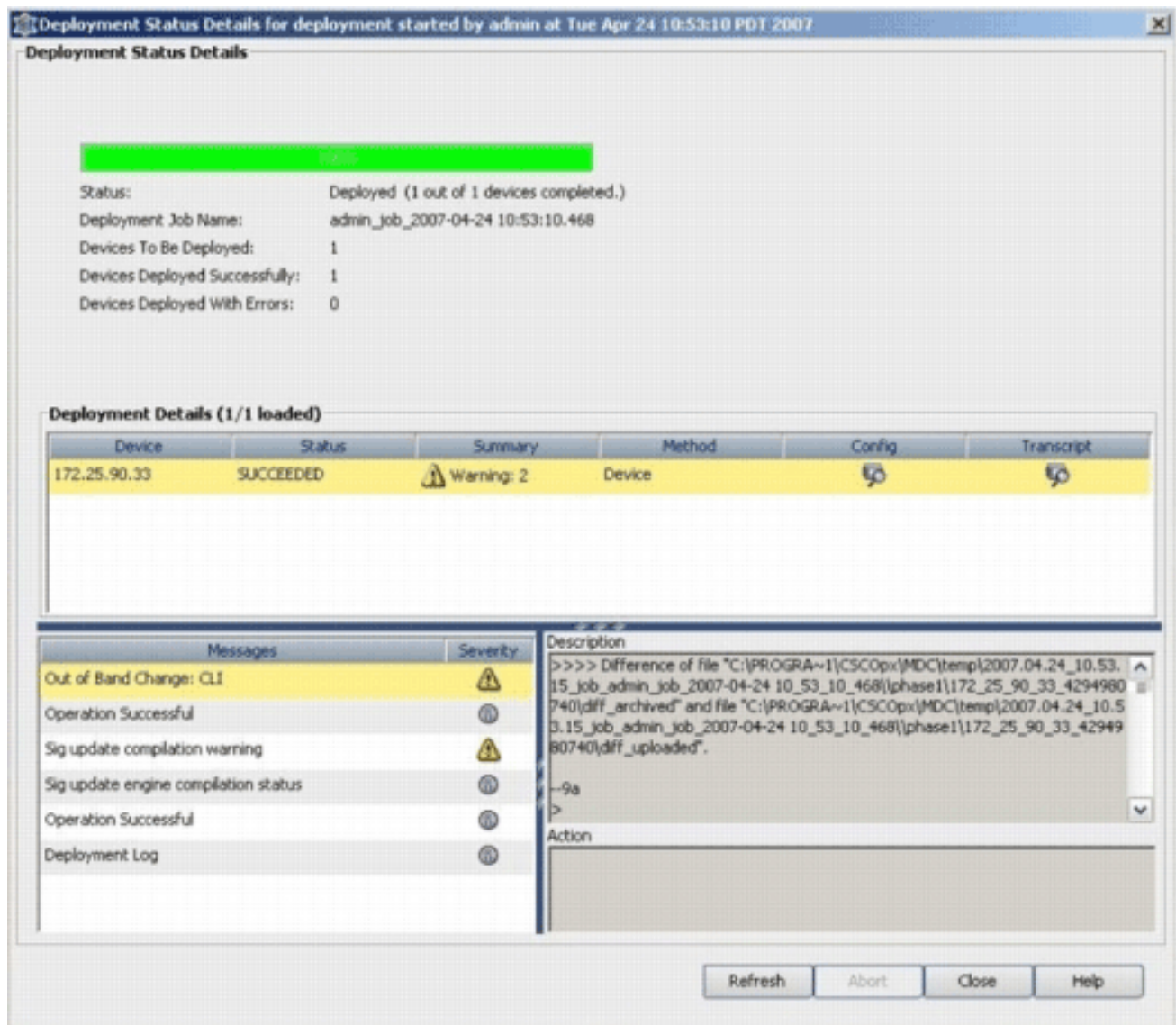26. Kies **Bestand > Verzenden en implementeren** om IPS op de IOS-router in te voeren.

27. Kies het apparaat waarop u de wijzigingen wilt invoeren en klik op

Uitvoeren.

28. Bekijk de implementatiestatus om te controleren of er fouten zijn.

Gerelateerde informatie

- Cisco IOS IPS-pagina (Inbraakpreventiesysteem) voor producten en services
- Om aan de slag te gaan met Cisco IOS IPS met bestandsindeling voor 5.x-handtekeningen
- Verbeteringen in IPS 5.x-signaalindeling en bruikbaarheid
- Cisco-inbraakpreventiesysteem
- Security meldingen uit het veld (inclusief Cisco Secure Inbraakdetectie)
- Technische ondersteuning - Cisco-systemen