Configureer router en sloten en Cisco IOS CLI in Cisco IOS IPS

Inhoud

Inleiding

In Cisco de router en de Manager van het Veiligheidsapparaat (middel dm) 2.2, de configuratie van Cisco IOS® IPS binnen de toepassing sm wordt geïntegreerd. U hoeft niet langer een afzonderlijk venster te starten om Cisco IOS IPS te configureren.

In Cisco slecht 2.2, zal een nieuwe IPS configuratie wizard u door de stappen leiden die nodig zijn om Cisco IOS IPS op de router in te schakelen. Daarnaast kunt u nog de geavanceerde configuratieopties gebruiken om Cisco IOS IPS met Cisco DSM 2.2 in te schakelen, uit te schakelen en af te stemmen.

Cisco raadt aan dat u Cisco IOS IPS met de geprezen kenmerkende bestanden (SDF's) draait: aanval-drop.sdf, 128 MB.sdf en 256 MB.sdf. Deze bestanden worden gemaakt voor routers met verschillende hoeveelheden geheugen. De bestanden worden gebundeld met Cisco DSM, dat SDF's aanbeveelt wanneer u eerst Cisco IOS IPS op een router toestaat. Deze bestanden kunnen ook worden gedownload van http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (alleen geregistreerde klanten).

Het proces om de standaard SDF's in te schakelen is gedetailleerd in Cisco IOS IPS met een fabrieksstandaard SDF. Wanneer de standaard SDF's niet volstaan of u nieuwe handtekeningen wilt toevoegen, kunt u de procedure gebruiken die is beschreven in Extra handtekeningen toevoegen nadat U Default SDF hebt ingeschakeld.

Voorwaarden

Vereisten

Java Runtime Environment (JRE) versie 1.4.2 of hoger is vereist om Cisco DM 2.2 te gebruiken. Een door Cisco aanbevolen en aangepast bestand voor handtekeningen (gebaseerd op DRAM) is gebundeld met Cisco DSM (geladen op routergeheugen met Cisco DSM).

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Router en Security Devices Manager (DSM) 2.2.

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

Cisco IOS IPS met fabrieksstandaard SDF inschakelen

CLI-procedure

Voltooi deze procedure om de CLI te gebruiken om een Cisco 1800 Series router met Cisco IOS IPS te configureren om 128MB.sdf op de routerflitser te laden.

1. Configureer de router om de melding van de Security Devices Exchange (SDEE)-gebeurtenis in te schakelen.
   ```
   yourname#conf t
   ```
2. Voer configuratieopdrachten in (één per regel) en druk vervolgens op Cntl+Z om te eindigen.
   ```
   yourname(config)#ip ips notify sdee
   ```
3. Maak een IPS regel naam die wordt gebruikt om aan interfaces te associëren.
   ```
   yourname(config)#ip ips name myips
   ```
4. Configuratie een IPS plaatsopdracht om te specificeren van welk bestand het Cisco IOS IPS-systeem handtekeningen zal lezen.Dit voorbeeld gebruikt het bestand op flitser: 128 MB.sdf. Het URL-gedeelte van deze opdracht kan een geldige URL zijn die flitser, schijf of protocollen via FTP, HTTP, HTTPS, RTP, SCP en TFTP gebruikt om naar de bestanden te wijzen.
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   Opmerking: U moet de opdracht van de **terminalmonitor** inschakelen als u de router via een Telnet-sessie configureren of u de SDEE-berichten niet ziet wanneer de ondertekenaar-machine bezig is met bouwen.
5. Schakel IPS op de interface in waar u Cisco IOS IPS wilt in om verkeer te scannen. In dit geval, hebben we op beide richtingen op interface FastEthernet 0 geactiveerd.

```
yourname(config)#interface fastEthernet 0
yourname(config-if)#ip ips myips in
*Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS:
        SDF loaded successfully from opacl
*Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS:
        SDF loaded successfully from flash:128MB.sdf
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
        OTHER - 4 signatures - 1 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_READY:
        OTHER - 0 ms - packets for this engines will be scanned
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
        MULTI-STRING - 0 signatures - 2 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED:
        MULTI-STRING - there are no new signature definitions for this engine
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
        STRING.ICMP - 1 signatures - 3 of 15 engines
*Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
        STRING.ICMP - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING:
        STRING.UDP - 17 signatures - 4 of15 engines
*Oct 26 00:32:31.393: %IPS-6-ENGINE_READY:
        STRING.UDP - 448 ms - packets for this engine will be scanned
*Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING:
        STRING.TCP - 58 signatures - 5 of 15 engines
*Oct 26 00:32:33.641: %IPS-6-ENGINE_READY:
        STRING.TCP - 2248 ms - packets for this engine will be scanned
*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING:
        SERVICE.FTP - 3 signatures - 6 of 15 engines
*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY:
        SERVICE.FTP - 16 ms - packets for this engine will be scanned
*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING:
        SERVICE.SMTP - 2 signatures - 7 of 15 engines
*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY:
        SERVICE.SMTP - 28 ms - packets for this engine will be scanned
*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
        SERVICE.RPC - 29 signatures - 8 f 15 engines
*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
        SERVICE.RPC - 92 ms - packets for this engine will be scanned
*Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING:
        SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 00:32:33.801: %IPS-6-ENGINE_READY:
        SERVICE.DNS - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING:
        SERVICE.HTTP - 132 signatures - 10 of 15 engines
*Oct 26 00:32:44.505: %IPS-6-ENGINE_READY:
        SERVICE.HTTP - 10704 ms - packets for this engine will be scanned
*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING:
        ATOMIC.TCP - 11 signatures - 11 of 15 engines
*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY:
        ATOMIC.TCP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING:
        ATOMIC.UDP - 9 signatures - 12 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.UDP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.ICMP - 0 signatures - 13 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED:
        ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.L3.IP - 5 signatures - 15 of 15 engines
```

```
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned
yourname(config-if)#ip ips myips out
yourname(config-if)#ip virtual-reassembly
```

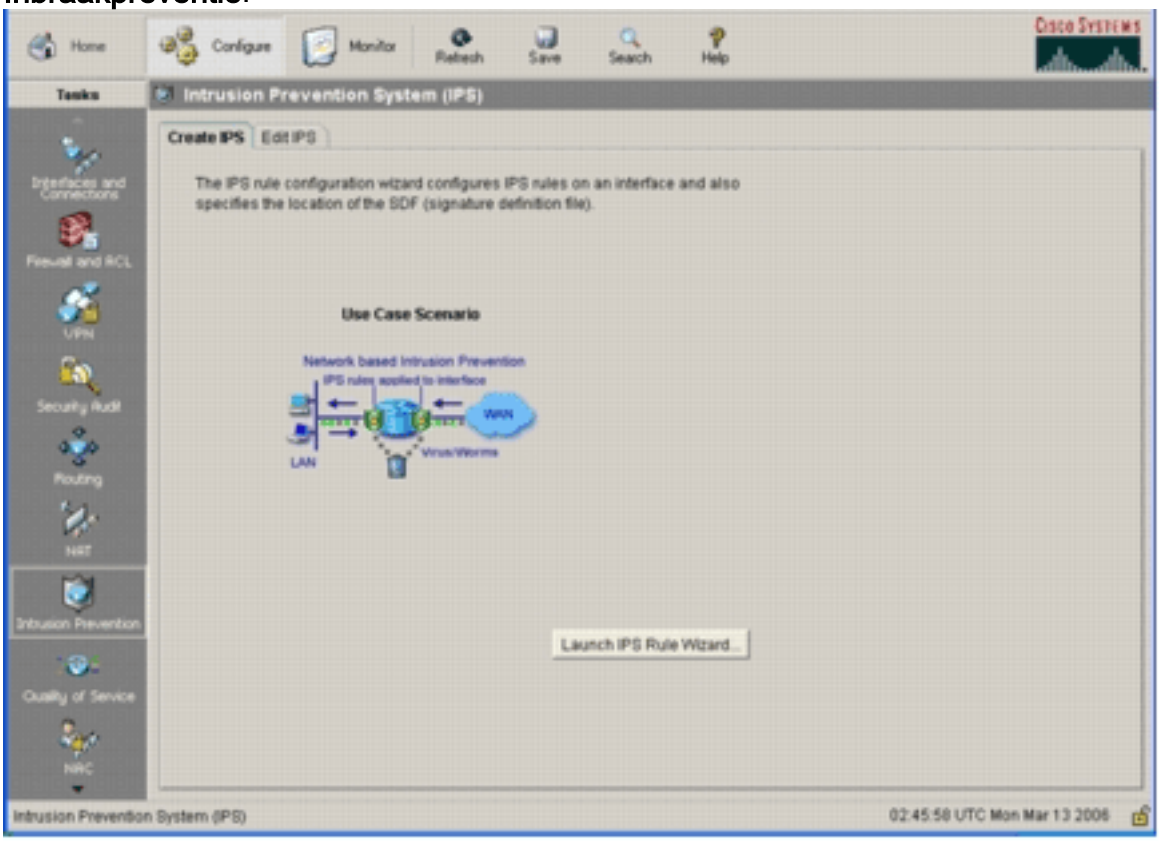
De eerste keer dat een IPS-regel op een interface wordt toegepast, begint Cisco IOS IPS bouwde handtekeningen van het bestand dat door de opdracht SDF-locaties wordt gespecificeerd. SDEE-berichten worden ingelogd op de console en naar de syslig-server verzonden indien geconfigureerd. De SDEE-berichten met <*nummer*> van <*aantal*> motoren geven het proces voor het bouwen van de motor voor handtekeningen aan. Tenslotte, als de twee getallen gelijk zijn, worden alle motoren gebouwd.**Opmerking:** IP virtuele reassemblering is een interfaceoptie die (wanneer ingeschakeld) automatisch gefragmenteerde pakketten reassembleert die in de router door die interface komen. Cisco raadt u aan om IP virtueel-assembleren op alle interfaces toe te staan waar het verkeer in de router komt. In het bovenstaande voorbeeld, naast het inschakelen van "ip Virtual-assembleren" op interface FastEthernet 0, vormen we het ook op de binnenkant interface VLAN 1.

```
yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly
```

PROCEDURE 2.2

Voltooi deze procedure om Cisco DSM 2.2 te gebruiken om een Cisco 1800 Series router met Cisco IOS IPS te configureren.

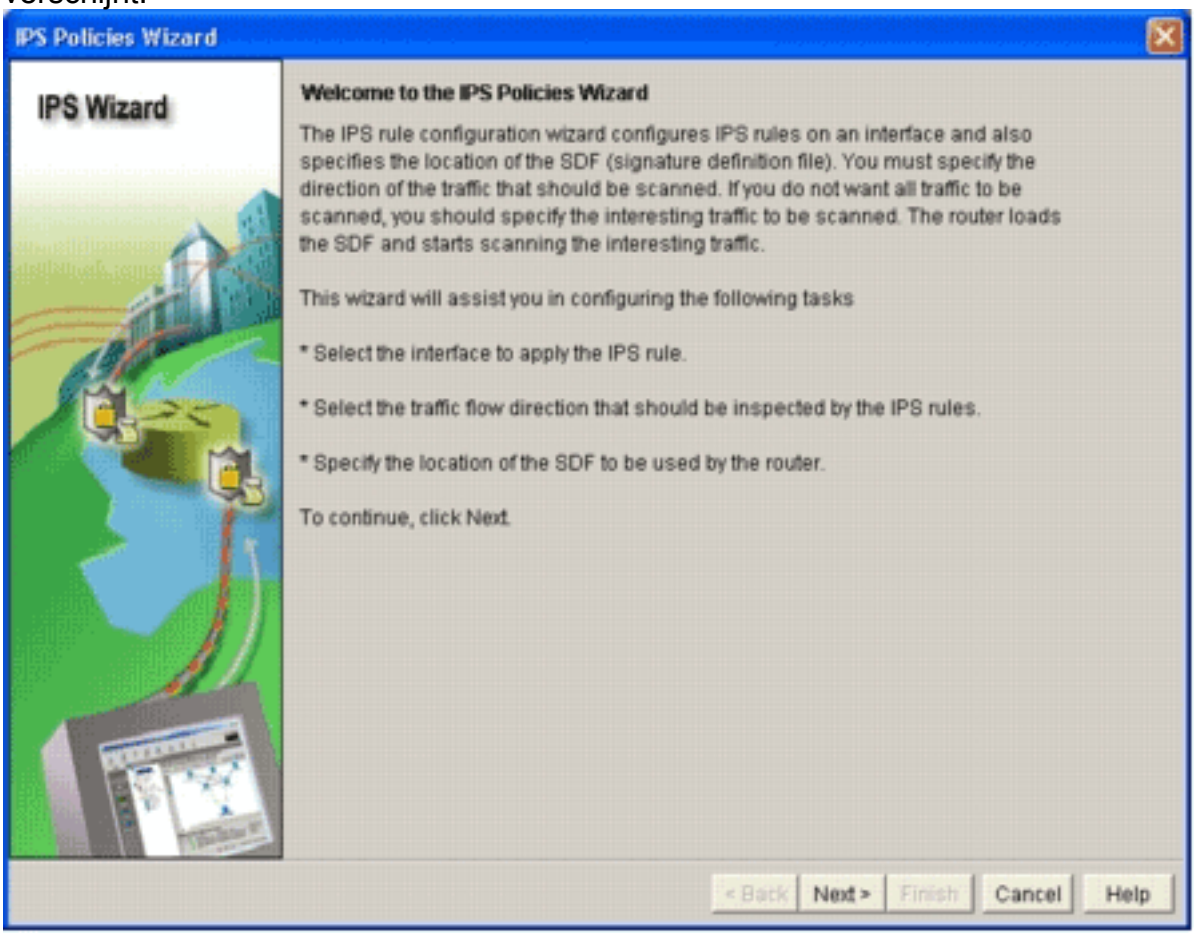
1. In de toepassing sm, klik **Configureren**, en klik dan **Inbraakpreventie**.



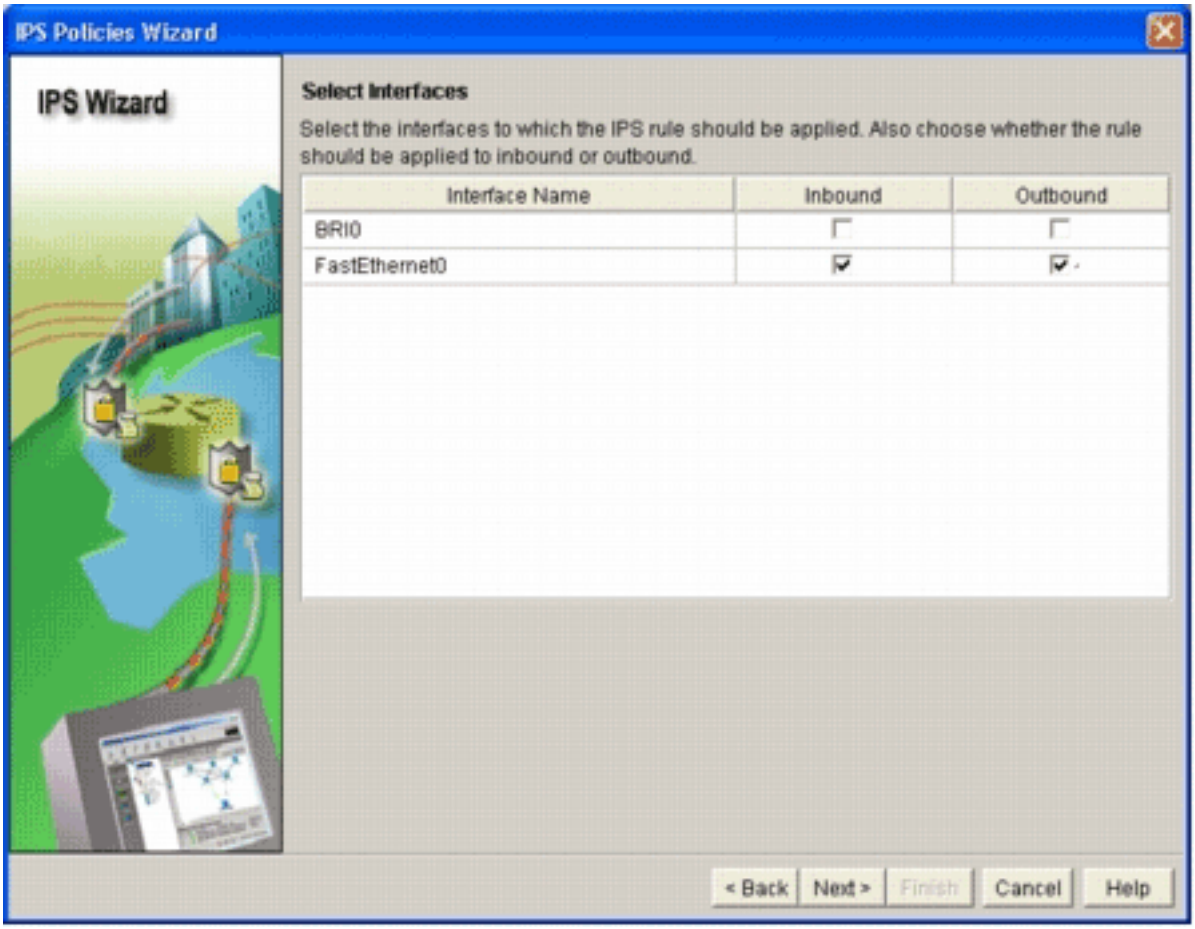
2. Klik op het tabblad **IPS maken** en klik vervolgens op **Wizard IPS-regel starten**.Cisco PDM vereist IPS-eventkennisgeving via SDEE om de Cisco IOS IPS-functie te configureren. Standaard is het SDEE-bericht niet ingeschakeld. Cisco dm vraagt u om IPS gebeurtenis

kennisgeving via SDEE zoals in dit beeld te toelaten:

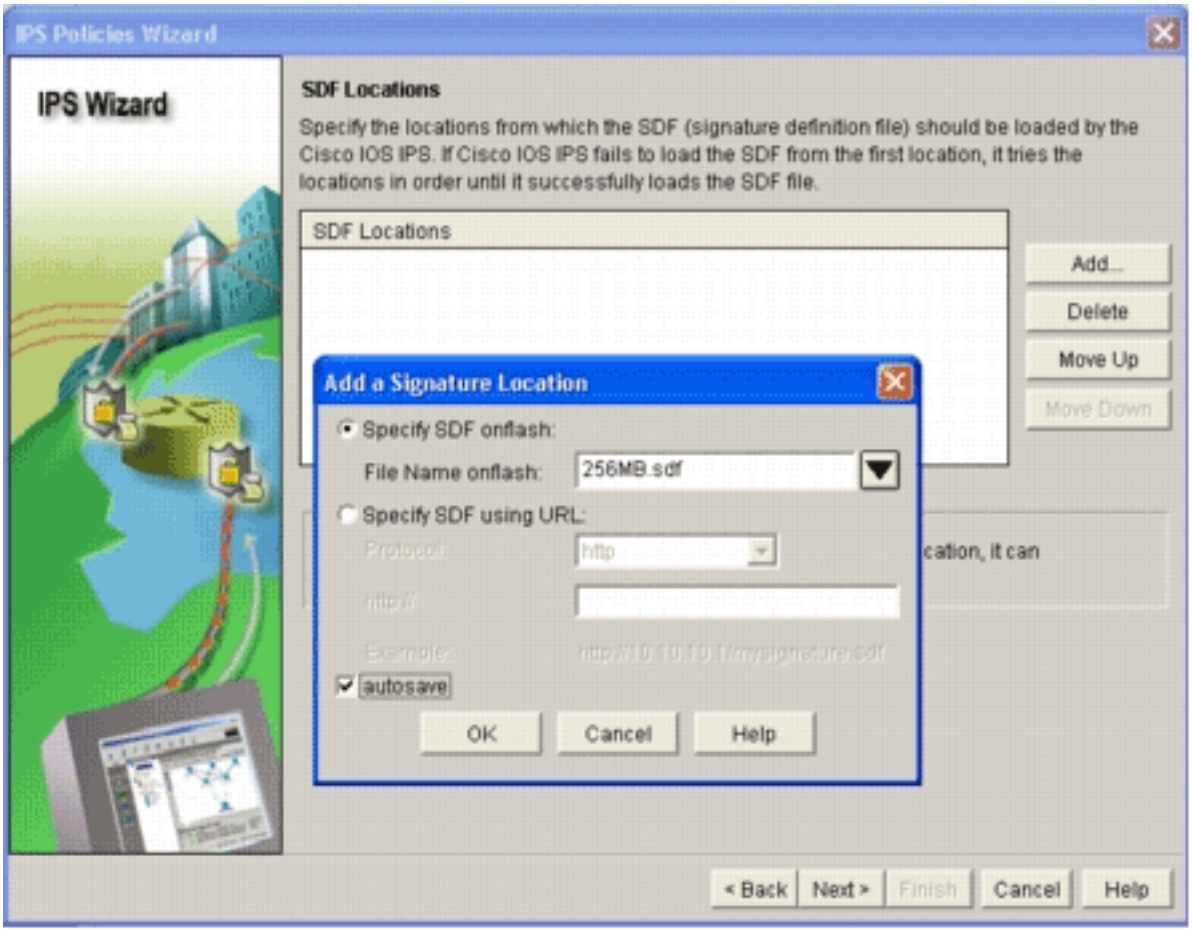
3. Klik op **OK**.Het venster Welcome to the IPS Policy Wizard van het dialoogvenster IPS-beleidswizard verschijnt.



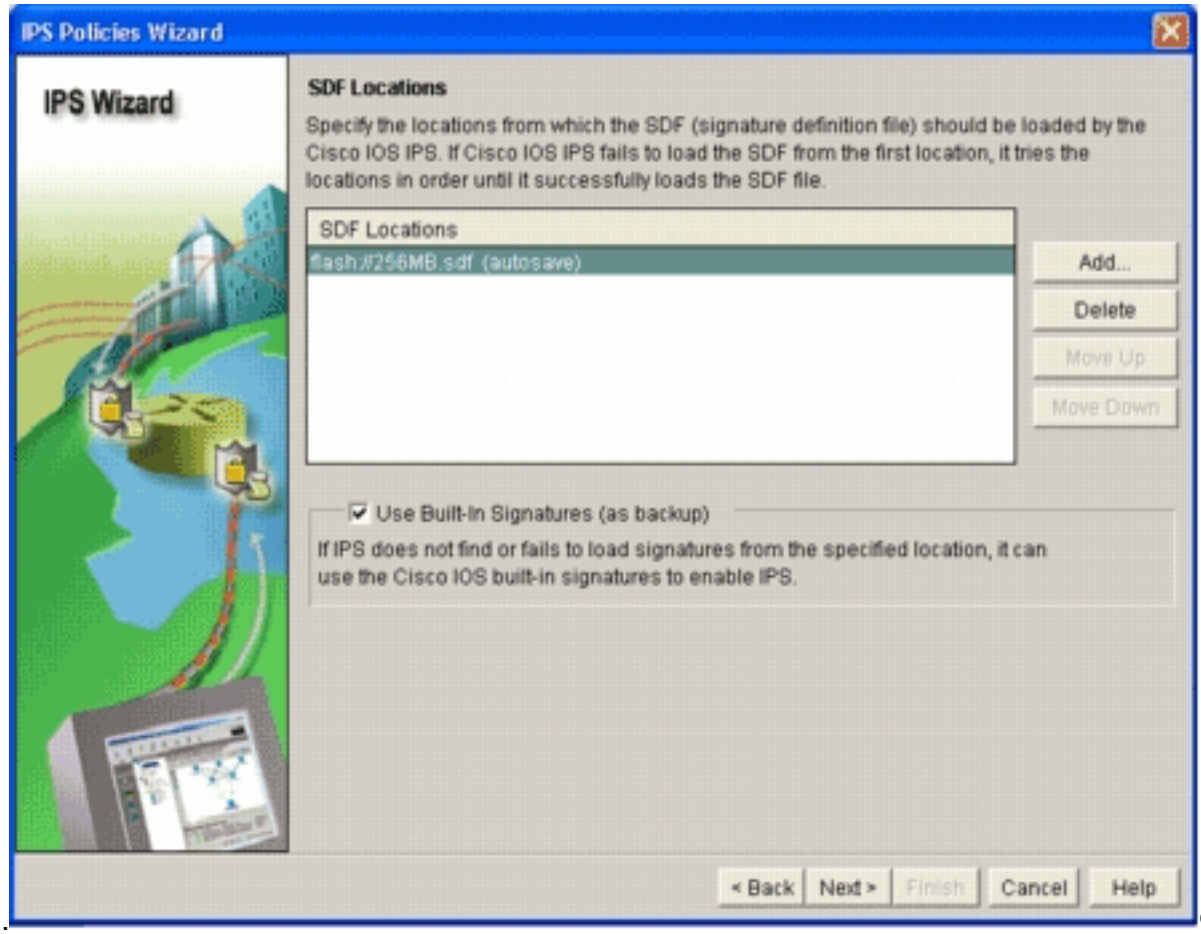
4. Klik op **Volgende**.Het venster Interfaces selecteren verschijnt.



5. Kies de interfaces waarvoor u IPS wilt inschakelen en klik op het selectieteken **Inbound** of **Outbound** om de richting van die interface aan te geven.**Opmerking:** Cisco raadt u aan om zowel inkomende als uitgaande richtingen in te schakelen wanneer u IPS op een interface activeert.
6. Klik op **Volgende**.Het venster voor SDF-locaties verschijnt.
7. Klik op **Add** om een SDF-locatie te configureren.Het dialoogvenster Locatie toevoegen verschijnt.



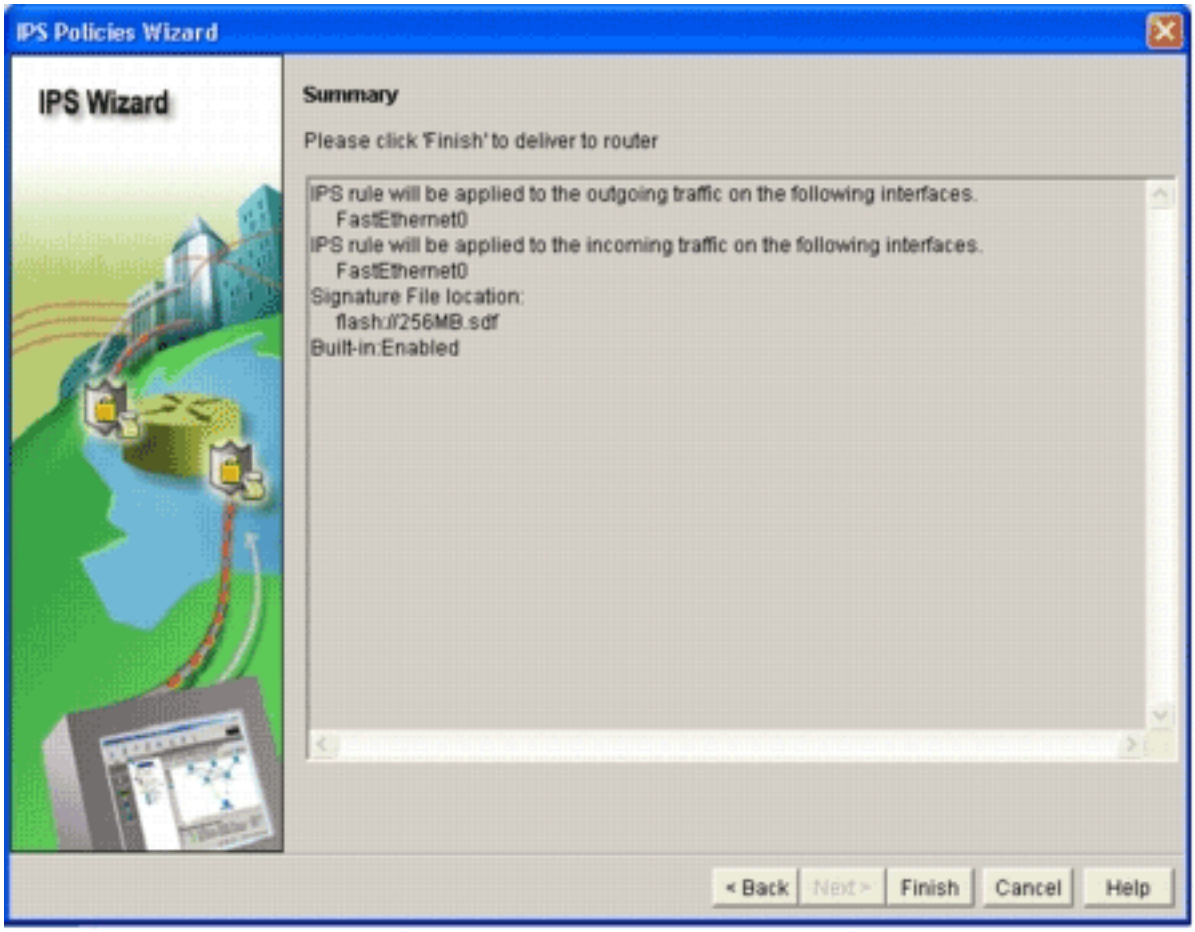
8. Klik op de knop **SDF opgeven op** de **flitser-**radioknop en kies 256MB.sdf in de vervolgkeuzelijst **Bestandsnaam op** de **flitser**.
9. Klik op het selectieteken **automatisch opslaan** en klik op **OK**.**OPMERKING:** De optie IntraSave zal automatisch het bestand opslaan wanneer er een wijziging in de handtekening is aangebracht.Het venster SDF-instellingen toont de nieuwe SDF-



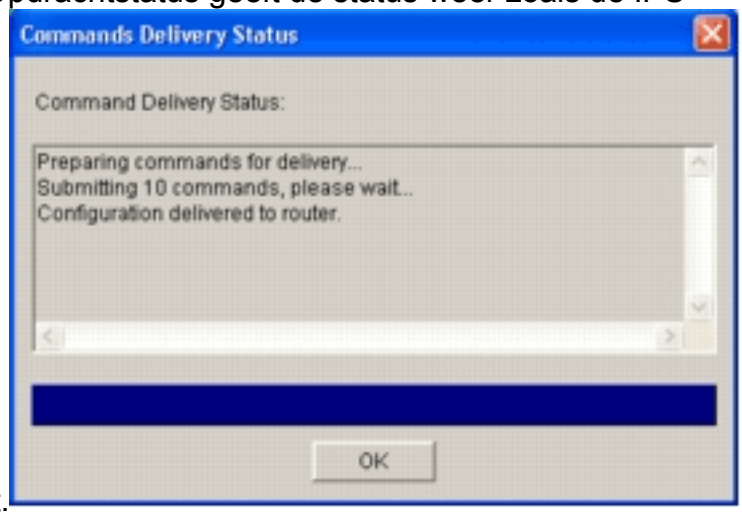
locatie.**O**

pmerking: U kunt extra locaties voor handtekening toevoegen om een back-up aan te wijzen.

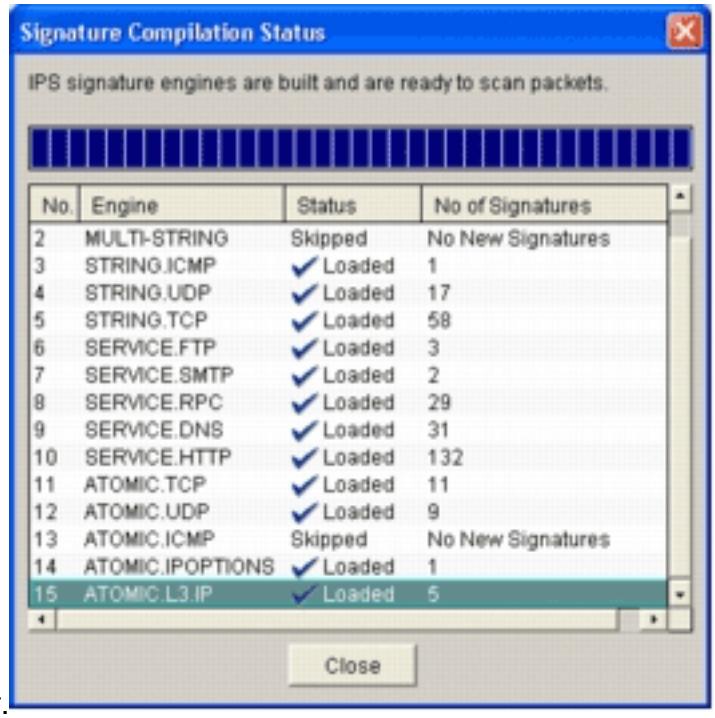
10. Klik op het aanvinkvakje **Ingebouwde handtekeningen gebruiken (als back-up)**.**Opmerking:** Cisco raadt u aan de ingebouwde signatuur niet te gebruiken tenzij u een of meer locaties hebt opgegeven.
11. Klik op **Volgende** om verder te gaanHet venster Samenvatting verschijnt.



12. Klik op **Voltooien**.Het dialoogvenster Opdrachtstatus geeft de status weer zoals de IPS-motor alle handtekeningen samenstelt.

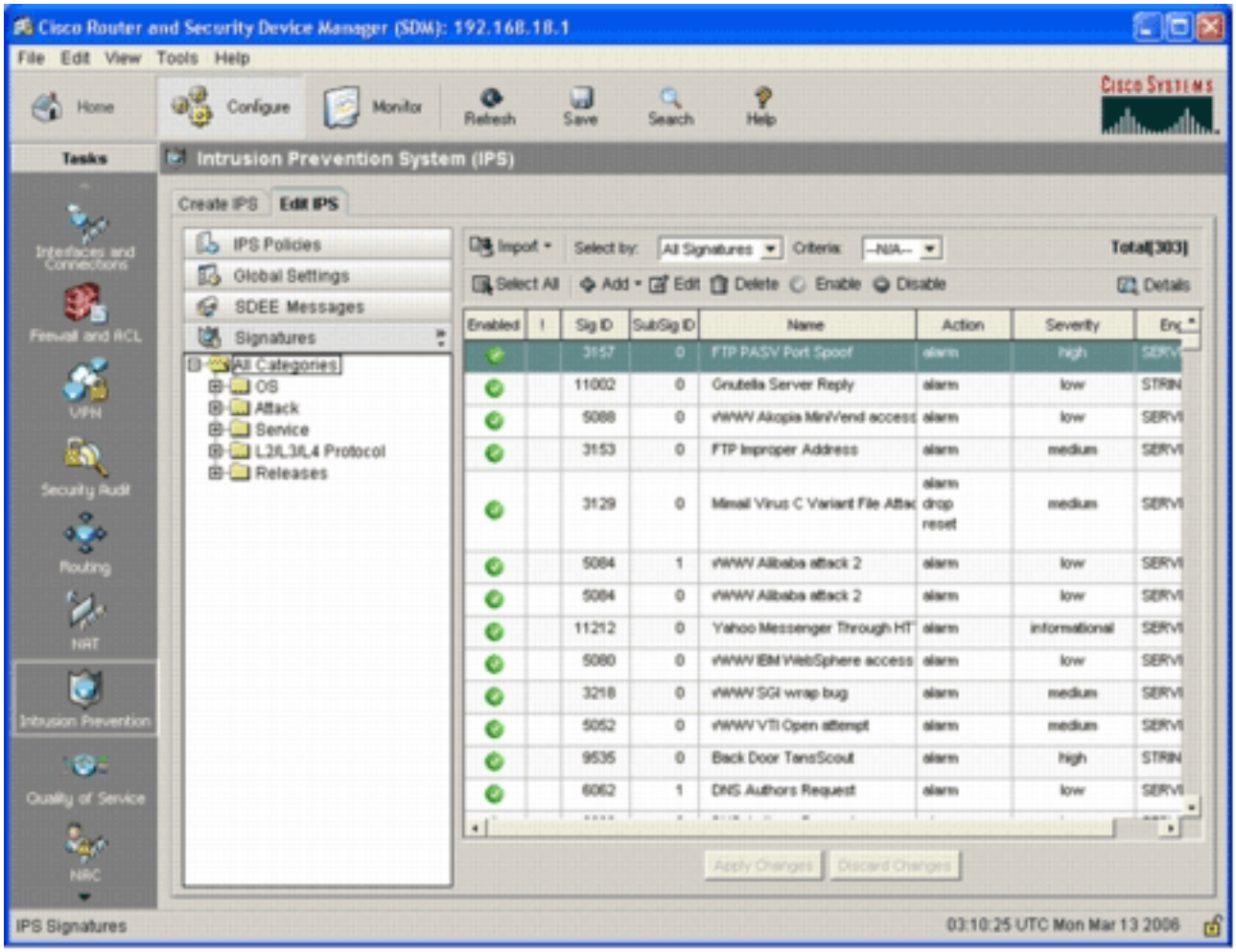


13. Klik op **OK** nadat het proces is voltooid.Het dialoogvenster Compilatiestatus van handtekeningen geeft de informatie over de compilatie van handtekeningen



weer.Deze informatie laat zien welke motoren zijn samengesteld en hoeveel handtekeningen in die motor zijn aangebracht. Voor motoren die in de statuskolom zijn *gemonteerd*, is er geen handtekening geladen voor die motor.

14. Klik op **Sluiten** om het dialoogvenster Compilatiestatus van de handtekening te sluiten.
15. Om te verifiëren welke handtekeningen op het ogenblik op de router worden geladen, klik op **Configureren** en klik vervolgens op **Inbraakpreventie**.
16. Klik op het tabblad **IPS bewerken** en vervolgens op **Handtekeningen**.De lijst met IPS-handtekeningen verschijnt in het venster Handtekeningen.



Extra handtekeningen toevoegen nadat standaard SDF is ingeschakeld

CLI-procedure

Er is geen CLI-opdracht beschikbaar om handtekeningen te maken of informatie te lezen over de handtekening in het gedistribueerde IOS-Sxxx.zip-bestand. Cisco raadt u aan om of het Centrum van het Beheer voor IPS Sensoren te gebruiken om de handtekeningen op Cisco IOS IPS systemen te beheren.

Voor klanten die al een ondertekend bestand klaar hebben en dit bestand met SDF willen samenvoegen dat op een Cisco IOS IPS-systeem draait, kunt u deze opdracht gebruiken:

```
yourname#show running-config | include ip ips sdf
ip ips sdf location flash:128MB.sdf
yourname#
```

Het bestand van de handtekening dat door het commando van de locatie van de handtekening wordt gedefinieerd, is waar de router bestanden van de handtekeningen laadt wanneer het wordt herladen of wanneer de router IOS IPS wordt hergeconfigureerd. Om het fuserende proces succesvol te zijn, moet het bestand dat door de opdracht voor het lokaliseren van het bestand wordt gedefinieerd ook worden bijgewerkt.

1. Gebruik de opdracht **tonen** om de momenteel geconfigureerde ondertekenlocaties te controleren.De uitvoer toont de geconfigureerde locaties van handtekeningen. Deze opdracht toont aan waar de huidige actieve handtekeningen zijn geladen.
   ```
   yourname#show ip ips signatures
   ```

```
Builtin signatures are configured
```

De handtekeningen zijn voor het laatst geladen vanaf flitser:128MB.sdfCisco SDF-release versie S.128.0Trend SDF-release versie V0.0

2. Gebruik de opdracht **kopie <*url*> IPS-sdf** samen met de informatie uit de vorige stap om bestanden met handtekeningen samen te voegen.

```
yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
Loading mysignatures.xml from 10.10.10.5 (via Vlan1): !
[OK - 1612 bytes]
*Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport
4715
*Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from
        tftp://10.10.10.5/mysignatures.xml
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature
        definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures -
        2 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures -
        3 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures -
        4 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures -
        5 of 15 engines
*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False -
        This parameter is not supported
*Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this
        engine will be scanned
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures -
        6 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures -
        7 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures -
        8 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures -
        9 of 15 engines
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures -
        10 of 15 engines
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
        11 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures -
        12 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are
        no new signature definitions for this engine
```

```
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures -
        13 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures -
        14 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures -
        15 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are
        no new signature definitions for this engine
yourname#
```

Nadat u de opdracht **kopie** geeft, laadt de router het signatebestand in het geheugen en bouwt dan de signatuur motoren. In de SDEE-berichtuitvoer van de console wordt de bouwstatus voor elke kenmerkende motor weergegeven.%IPS-6-ENGINE_BUILD_SKIPPED geeft aan dat er geen nieuwe handtekeningen voor deze motor zijn.%IPS-6-ENGINE_READY geeft aan dat er nieuwe handtekeningen zijn en dat de motor klaar is. Zoals voorheen geeft het bericht "15 van 15 motoren" aan dat alle motoren zijn gebouwd.IPS-7-UNSUPPORTED_PARAM geeft aan dat een bepaalde parameter niet door Cisco IOS IPS wordt ondersteund. Bijvoorbeeld CapturePacket en ResetAfterIdle.**OPMERKING:** Deze berichten zijn alleen ter informatie en hebben geen effect op de functies of prestaties van Cisco IOS IPS-handtekeningen. Deze houtlogberichten kunnen worden uitgeschakeld door het logniveau hoger in te stellen dan het fouilleren (niveau 7).

3. Update de SDF die door de opdracht voor de locatie van de handtekeningen wordt gedefinieerd, zodat wanneer de router wordt herladen, de gefuseerde handtekeningen worden ontvangen met een aangepaste handtekening. Dit voorbeeld toont het verschil in bestandsgrootte nadat de samengevoegde handtekening is opgeslagen in het 128MB.sdf flitsbestand.

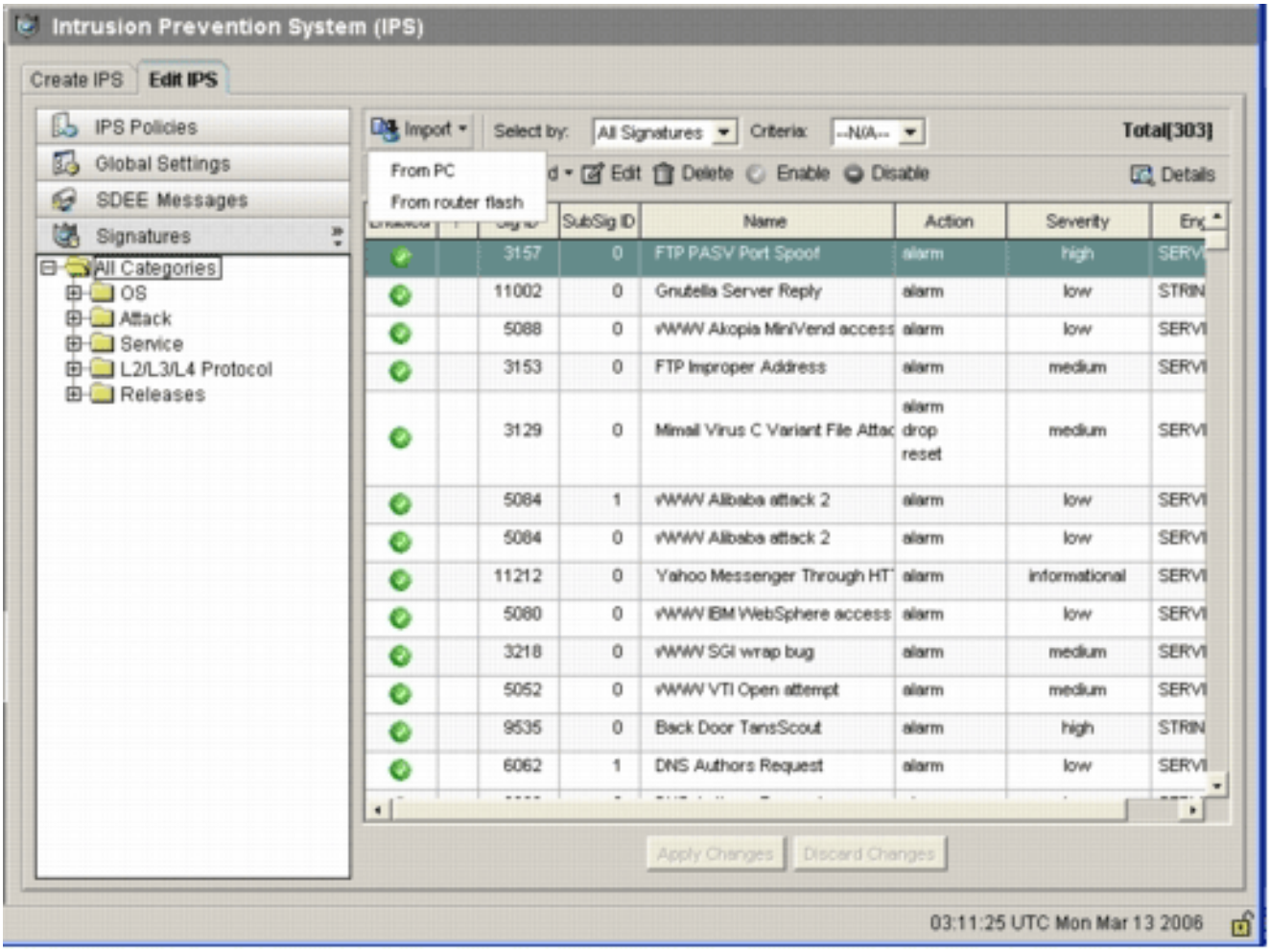
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

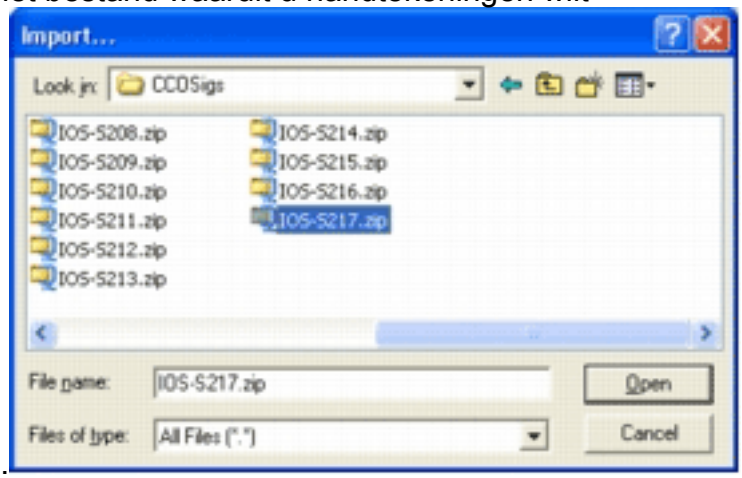
Waarschuwing: de nieuwe 128MB.sdf bevat nu door de klant samengevoegde handtekeningen. De inhoud is anders dan het Cisco standaard 128MB.sdf-bestand. Cisco raadt u aan dit bestand met een andere naam te wijzigen om verwarring te voorkomen. Als de naam wordt gewijzigd, moet de opdracht voor de locatie van de handtekening ook worden gewijzigd.

PROCEDURE 2.2

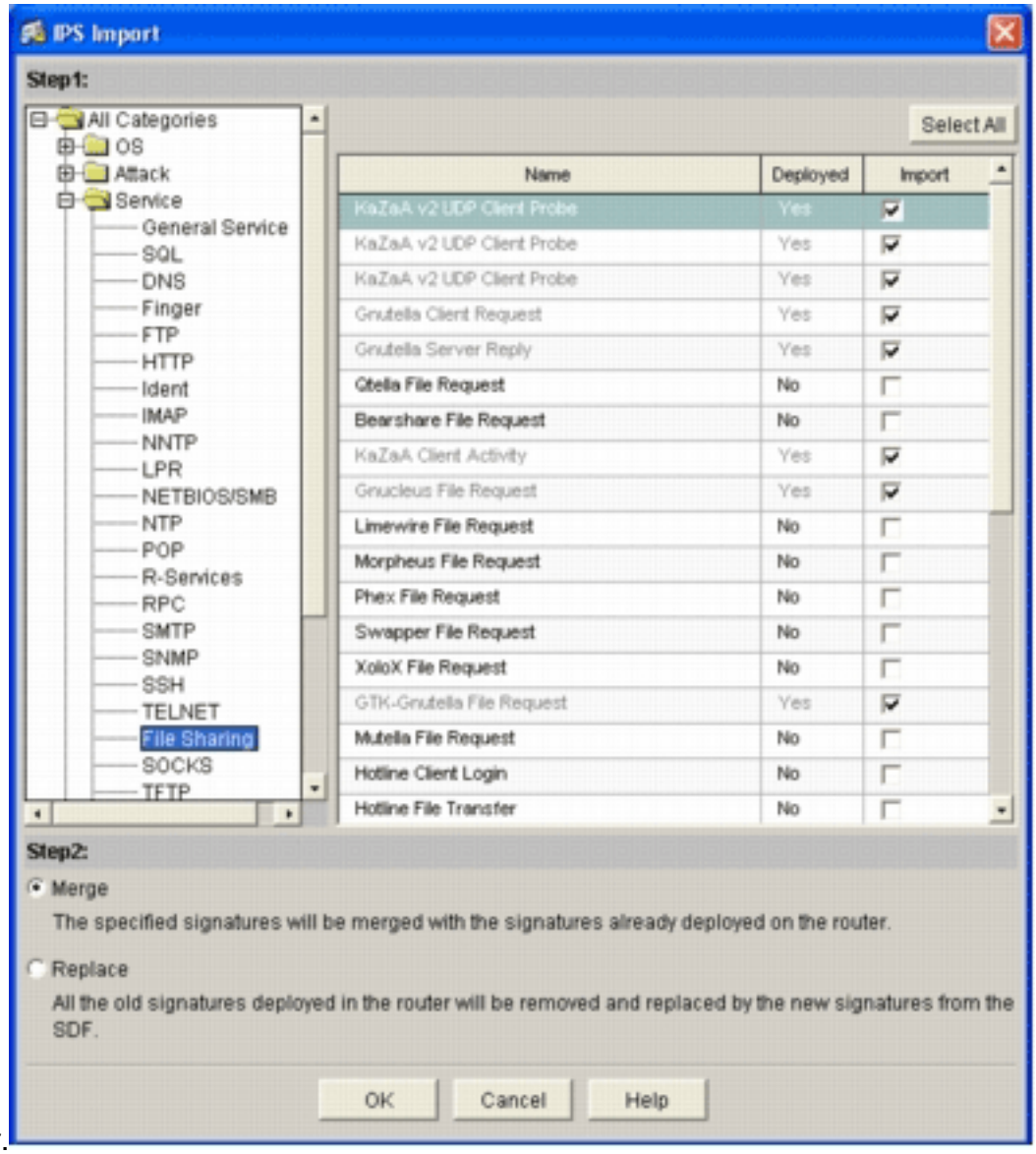
Nadat Cisco IOS IPS is toegelaten, kunnen de nieuwe handtekeningen in de router worden toegevoegd die een signatuur die met de de invoerfunctie van Cisco PDM loopt. Voltooi deze stappen om nieuwe handtekeningen te importeren:

1. Kies de standaard SDFs of het update bestand van IOS-Sxxx.zip om extra handtekeningen te importeren.
2. Klik op **Configureren** en vervolgens op **Inbraakpreventie**.
3. Klik op het tabblad **IPS bewerken** en vervolgens op **Importeren**.



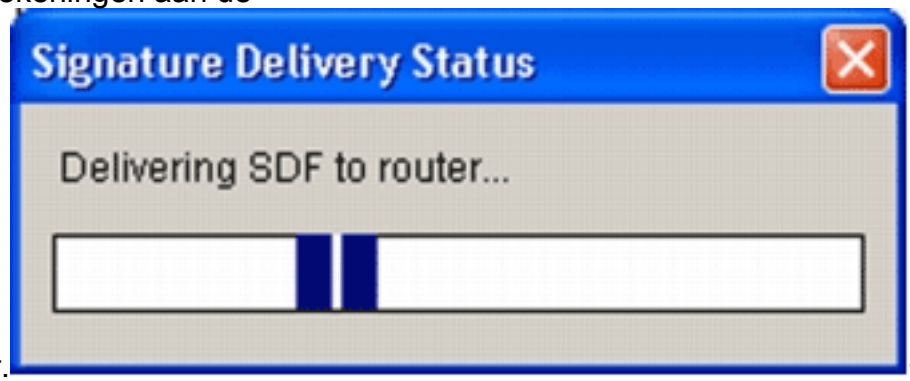
4. Kies **van PC** in de vervolgkeuzelijst Importeren.
5. Selecteer het bestand waaruit u handtekeningen wilt importeren. 

Dit voorbeeld gebruikt de nieuwste update die van Cisco.com is gedownload en op de lokale vaste schijf van de PC is opgeslagen.
6. Klik op **Openen**.**Waarschuwing:** vanwege geheugenbeperkingen kunnen slechts een beperkt aantal nieuwe handtekeningen worden toegevoegd bovenop handtekeningen die al zijn ingezet. Als te veel handtekeningen zijn geselecteerd, kan de router mogelijk niet alle nieuwe handtekeningen vanwege gebrek aan geheugen laden.Nadat de bestandslading voor handtekening is voltooid, verschijnt het dialoogvenster IPS-



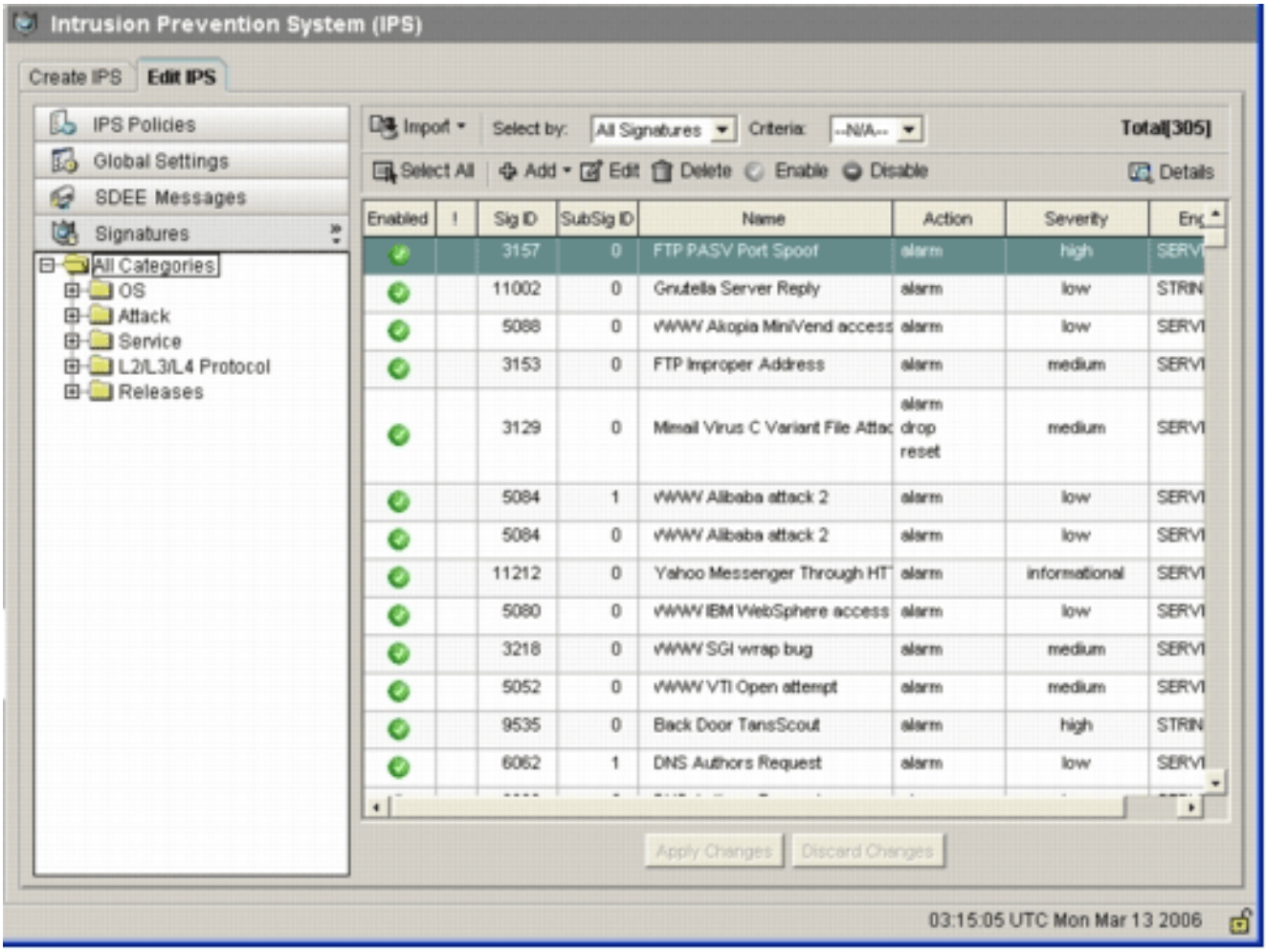
invoer.

7. Navigeer door de linkerboomweergave en klik op het aanvinkvakje **Importeren** naast de handtekeningen die u wilt importeren.
8. Klik op de knop **Merge** en vervolgens op **OK**.**Opmerking:** De optie Vervangen vervangt de huidige handtekening die op de router is ingesteld, door de handtekeningen die u hebt geselecteerd om te importeren.Zodra u OK klikt, levert de toepassing Cisco PDM de handtekeningen aan de



router.**Opmerking:** Bij het compileren en laden van handtekeningen wordt gebruik gemaakt van hoge CPU's. Nadat Cisco IOS IPS op de interface is ingeschakeld, start het bestand voor handtekeningen. De router duurt ongeveer vijf minuten om SDF te laden. U kunt proberen de opdracht **Show proces cpu** te gebruiken om het CPU-gebruik van de Cisco IOS-software CLI te bekijken. Probeer echter geen extra opdrachten te gebruiken of andere SDF's te laden terwijl de router SDF's laadt. Dit kan ertoe leiden dat het proces voor het samenstellen van handtekeningen

langer duurt (aangezien het CPU-gebruik bij het laden van de SDF dicht bij 100 procent ligt). Het kan nodig zijn om door de lijst met handtekeningen te bladeren en de handtekeningen in te schakelen als deze niet in enabled-status zijn.Het totale aantal handtekeningen is toegenomen tot 519. Dit aantal bevat alle handtekeningen die in het IOS-S193.zip-bestand beschikbaar zijn en behoren tot de subcategorie Bestand
delen.



Voor geavanceerde onderwerpen over hoe te om Cisco PDM te gebruiken om de functie van Cisco IOS IPS te beheren, verwijs naar de documentatie van Cisco PDM bij deze URL:

Selecteer Handtekeningen en werk met handtekeningen

Om effectief de juiste handtekeningen voor een netwerk te selecteren moet u een paar dingen over het netwerk weten die u beschermt. Bijgewerkte informatie van de categorie van handtekeningen in Cisco slecht 2.2 en hulp later klanten verder om de juiste reeks handtekeningen te selecteren om het netwerk te beschermen.

Deze categorie is een manier om handtekeningen te groeperen. Het helpt de selectie van handtekeningen te beperken tot een subset van handtekeningen die voor elkaar relevant zijn. Eén handtekening zou tot één categorie kunnen behoren of tot meerdere categorieën kunnen behoren.

Dit zijn de vijf topcategorieën:

- Besturing op basis van het besturingssysteem
- Attack-gebaseerde kenmerkende categorisatie voor aanvallen
- Service-/op service gebaseerde kenmerkende categorisatie

- Layer 2-4 protocol/protocol-gebaseerde gecategorisatie op protocolniveau
- Release-op release gebaseerde kenmerkende categorisatie

Elk van deze categorieën wordt verder onderverdeeld in subcategorieën.

Neem bijvoorbeeld een thuisnetwerk met een breedbandverbinding naar het internet en een VPN-tunnel naar het bedrijfsnetwerk. De breedbandrouter heeft Cisco IOS Firewall die op de open (niet-VPN) verbinding met het internet is ingeschakeld om te voorkomen dat een verbinding van het internet afkomstig is en op het thuisnetwerk wordt aangesloten. Al het verkeer dat van het thuisnetwerk naar internet afkomstig is, is toegestaan. Stel dat de gebruiker een op Windows gebaseerde PC gebruikt en toepassingen zoals HTTP (web browsing) en e-mail gebruikt.

De firewall kan zo worden geconfigureerd dat alleen de toepassingen die de gebruiker nodig heeft, door de router kunnen stromen. Dit zal de stroom van ongewenst en potentieel slecht verkeer controleren die door het netwerk kan zich verspreiden. Denk eraan dat de thuisgebruiker geen specifieke service nodig heeft of gebruikt. Als die service door de firewall is toegestaan, is er een mogelijk gat dat een aanval kan gebruiken om door het netwerk te stromen. De beste praktijken maken alleen diensten mogelijk die nodig zijn. Nu is het gemakkelijker om te selecteren welke handtekeningen u kunt toelaten. U hoeft alleen handtekeningen in te schakelen voor de services die u in de firewall kunt gebruiken. In dit voorbeeld omvatten de diensten e-mail en HTTP. Cisco PDM vereenvoudigt deze configuratie.

Om de categorie te gebruiken om de vereiste handtekeningen te selecteren, kies **Service > HTTP** en selecteer alle handtekeningen. Dit selectieproces werkt ook in het dialoogvenster voor de invoer van handtekeningen, waarin u alle HTTP-handtekeningen kunt selecteren en in uw router kunt importeren.

Extra categorieën die moeten worden geselecteerd zijn DNS, NEToverheid/MKB, HTTPS en MTP.

Handtekeningen voor standaard SDF-bestanden bijwerken

De drie per-gebouwde SDF's (aanval-drop.dsf, 128MB.sdf en 256MB.sdf) worden momenteel op Cisco.com gepost op http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (alleen geregistreerde klanten). Nieuwe versies van deze bestanden worden gepubliceerd zodra ze beschikbaar zijn. Om routers bij te werken die Cisco IOS IPS met deze standaard SDF's uitvoeren, gaat u naar de website en download de nieuwste versies van deze bestanden.

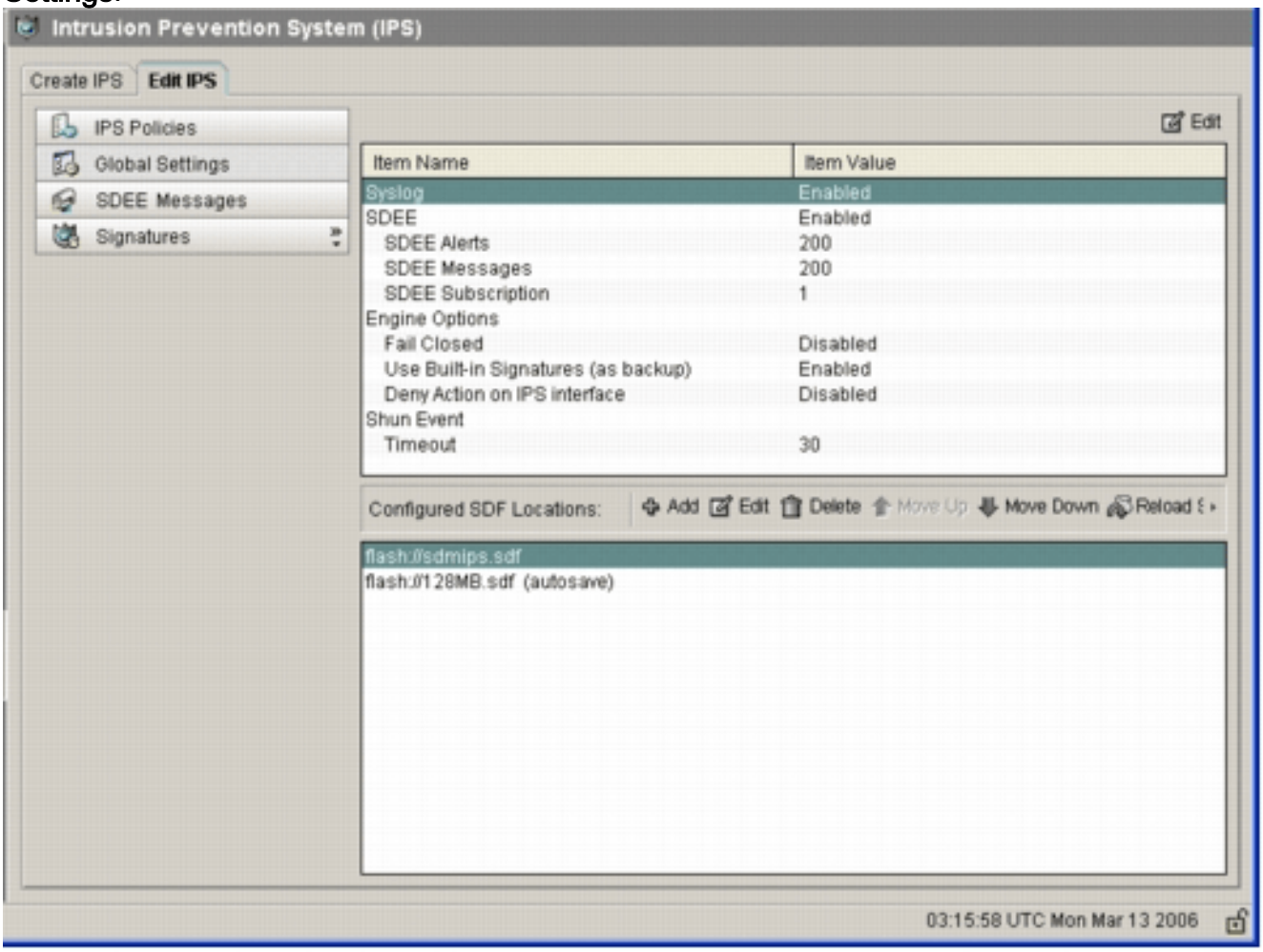
CLI-procedure

1. Kopieer de gedownload bestanden naar de locatie waar de router is ingesteld om deze bestanden te laden. Om te weten te komen waar de router momenteel wordt gevormd, gebruik de **show in werking stellen- | in ip ips sdf** opdracht.
   ```
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```
   In dit voorbeeld gebruikt de router 256MB.sdf op de flitser. Het bestand wordt bijgewerkt wanneer u de nieuwe gedownload 256MB.sdf naar de routerflitser kopieert.
2. Herladen van het Cisco IOS IPS-subsysteem om de nieuwe bestanden te starten.Er zijn twee manieren om Cisco IOS IPS te herladen: herladen van de router of opnieuw configureren Cisco IOS IPS om het IOS IPS-subsysteem te activeren om handtekeningen opnieuw te laden. Om Cisco IOS IPS aan te passen verwijder alle IPS-regels van de geconfigureerde interfaces, en pas vervolgens de IPS-regels opnieuw toe op de interfaces. Dit zal het Cisco IOS IPS-systeem activeren om te herladen.

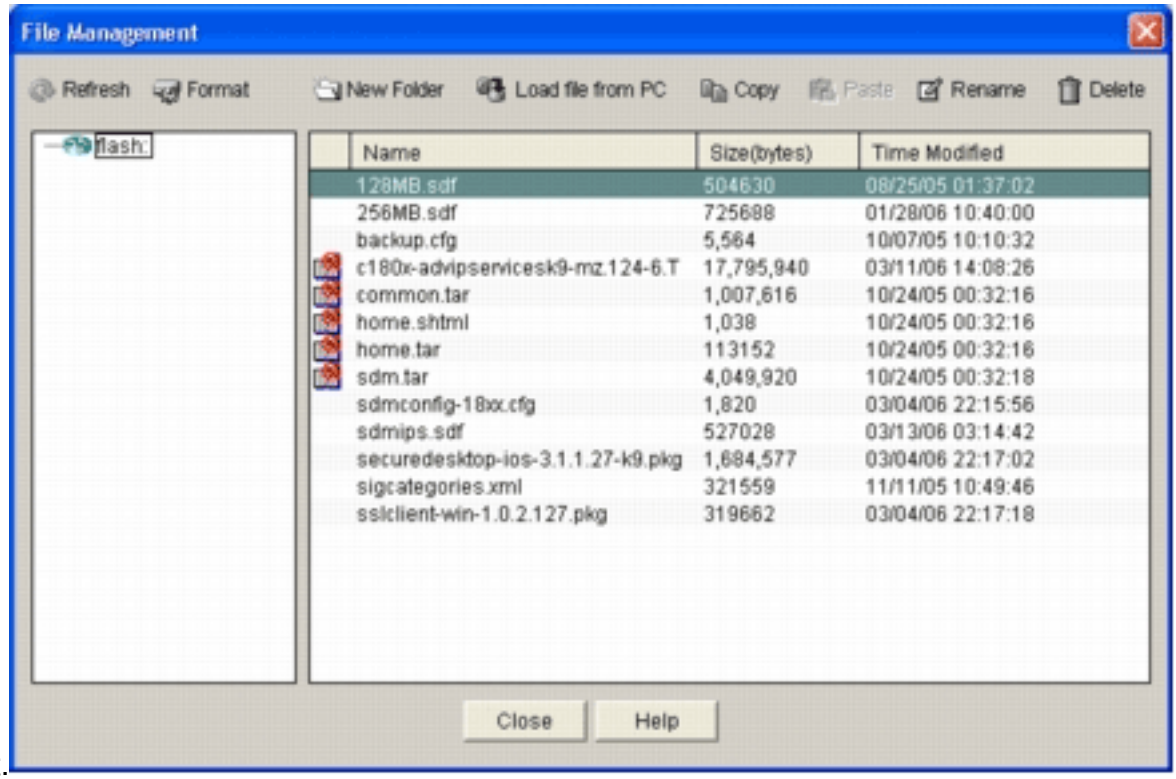
PROCEDURE 2.2

Voltooi deze stappen om de standaard SDFs op de router bij te werken:

1. Klik op **Configureren** en vervolgens op **Inbraakpreventie**.
2. Klik op het tabblad **IPS bewerken** en vervolgens op **Global Settings**.

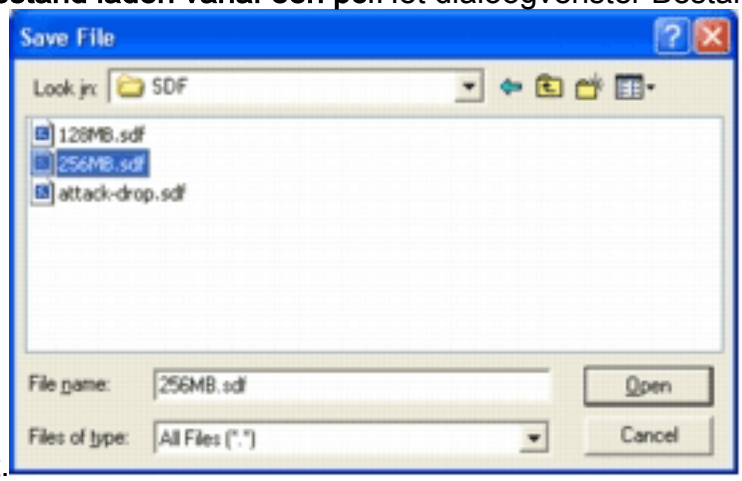


   De bovenkant van de UI toont de mondiale instellingen. De onderste helft van de UI toont momenteel gevormde SDF plaatsen. In dit geval wordt het 256MB.sdf-bestand uit flash-geheugen ingesteld.
3. Kies **Bestandsbeheer** uit het menu Bestand.Het dialoogvenster File Management



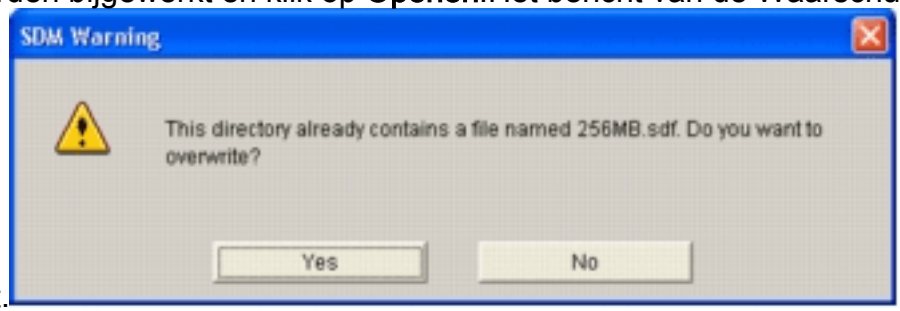
verschijnt.

4. Klik op **Bestand laden vanaf een pc**.Het dialoogvenster Bestand opslaan als



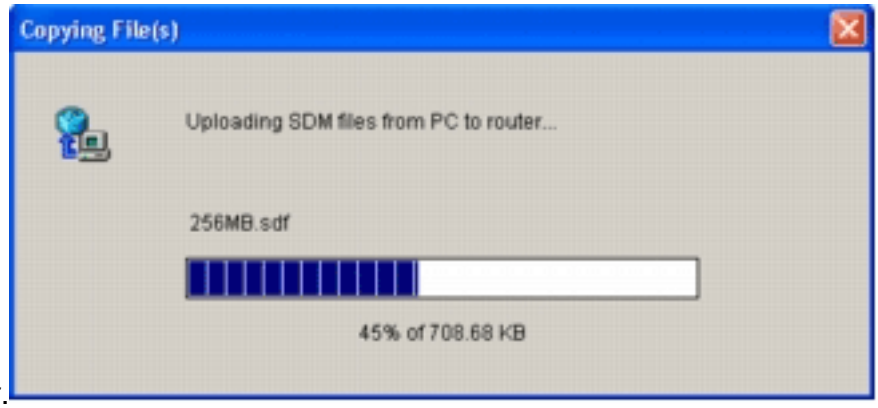
verschijnt.

5. Kies SDF dat moet worden bijgewerkt en klik op **Openen**.Het bericht van de Waarschuwing



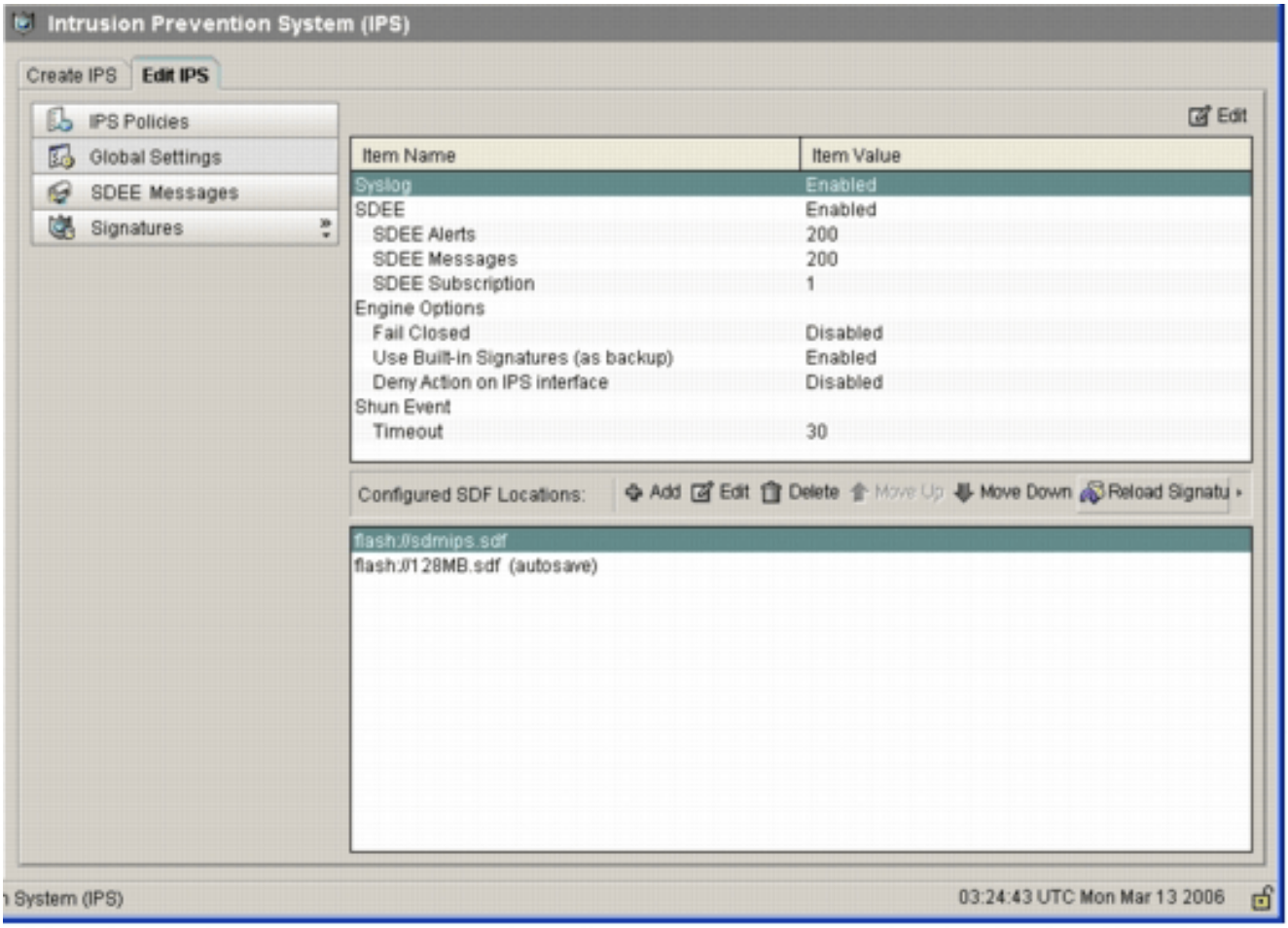
van het Sdm verschijnt.

6. Klik op **Ja** om het bestaande bestand te vervangen.Een dialoogvenster geeft de voortgang



van het uploadproces weer.

7. Nadat het uploadproces is voltooid, klikt u op **Handtekeningen opnieuw laden** op de SDF-locatie, werkbalk. Deze actie herlaadt de Cisco IOS IPS.



Opmerking: het IOS-Sxxx.zip-pakket bevat alle handtekeningen die Cisco IOS IPS ondersteunt. Uploads naar dit pakket handtekeningen worden op Cisco.com geplaatst zodra ze beschikbaar worden. Zie Stap 2 voor het bijwerken van de handtekeningen in dit pakket.

Gerelateerde informatie

- Cisco-inbraakpreventiesysteem
- Security meldingen uit het veld (inclusief Cisco Secure Inbraakdetectie)
- Technische ondersteuning - Cisco-systemen