Configurazione di Cisco IOS IPS con un router e un SDM

Sommario

Introduzione

In questo documento viene descritto come usare Cisco Router and Security Device Manager (SDM) versione 2.5 per configurare Cisco IOS® Intrusion Prevention System (IPS) nella versione 12.4(15)T3 e successive.

I miglioramenti apportati a SDM 2.5 in relazione a IOS IPS sono:

- Numero totale di firme compilate visualizzato nell'interfaccia utente dell'elenco delle firme
- File di firma SDM (formato file zip; ad esempio, sigv5-SDM-S307.zip) e pacchetti di firma CLI (formato file pkg; ad esempio, IOS-S313-CLI.pkg) può essere scaricato insieme in una sola operazione
- I pacchetti di firma scaricati possono essere automaticamente inviati al router come opzione

Le attività coinvolte nel processo di provisioning iniziale sono:

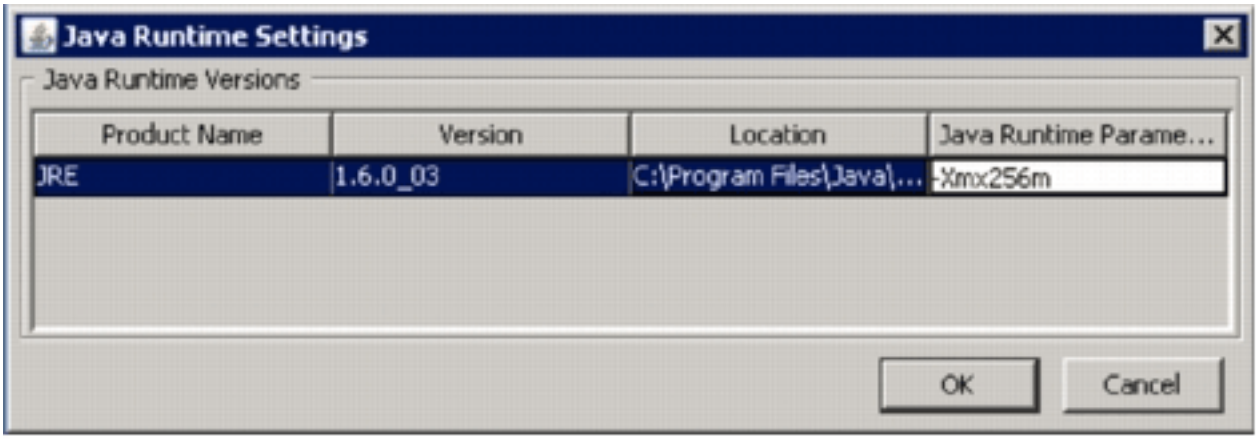
1. Scaricare e installare SDM 2.5.
2. Usare SDM Auto Update per scaricare il pacchetto della firma IPS IOS su un PC locale.
3. Per configurare IPS di IOS, avviare la Configurazione guidata criteri IPS.
4. Verificare che la configurazione e le firme IPS di IOS siano caricate correttamente

Cisco SDM è uno strumento di configurazione basato sul Web che semplifica la configurazione dei router e della sicurezza tramite procedure guidate intelligenti che consentono ai clienti di installare, configurare e monitorare un router Cisco in modo rapido e semplice senza dover conoscere l'interfaccia della riga di comando (CLI).

SDM versione 2.5 può essere scaricato da Cisco.com all'indirizzo http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (solo utenti registrati). La nota sulla versione è disponibile all'indirizzo http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

Nota: Cisco SDM richiede una risoluzione dello schermo di almeno 1024 x 768.

Nota: per configurare IOS IPS, Cisco SDM richiede una dimensione heap della memoria Java non inferiore a 256 MB. Per modificare le dimensioni dell'heap della memoria Java, aprire il pannello di controllo Java, fare clic sulla scheda **Java**, fare clic su **Visualizza** in Impostazioni runtime applet Java e quindi immettere **-Xmx256m** nella colonna Parametro runtime Java.



Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS IPS nella versione 12.4(15)T3 e successive
- Cisco Router and Security Device Manager (SDM) versione 2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

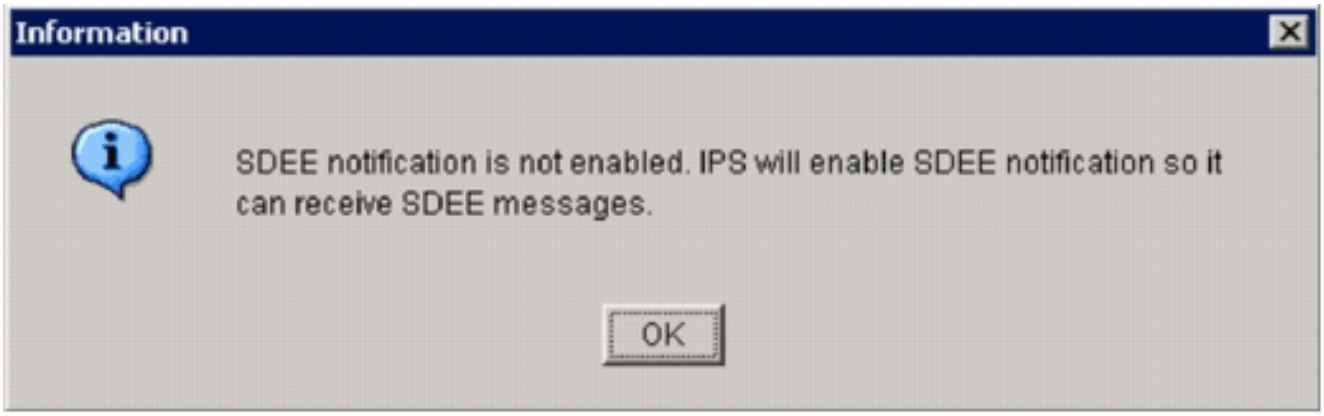
Configurazione

Nota: aprire una sessione console o telnet sul router (con 'term monitor' attivato) per monitorare i messaggi quando si utilizza SDM per effettuare il provisioning di IPS IOS.

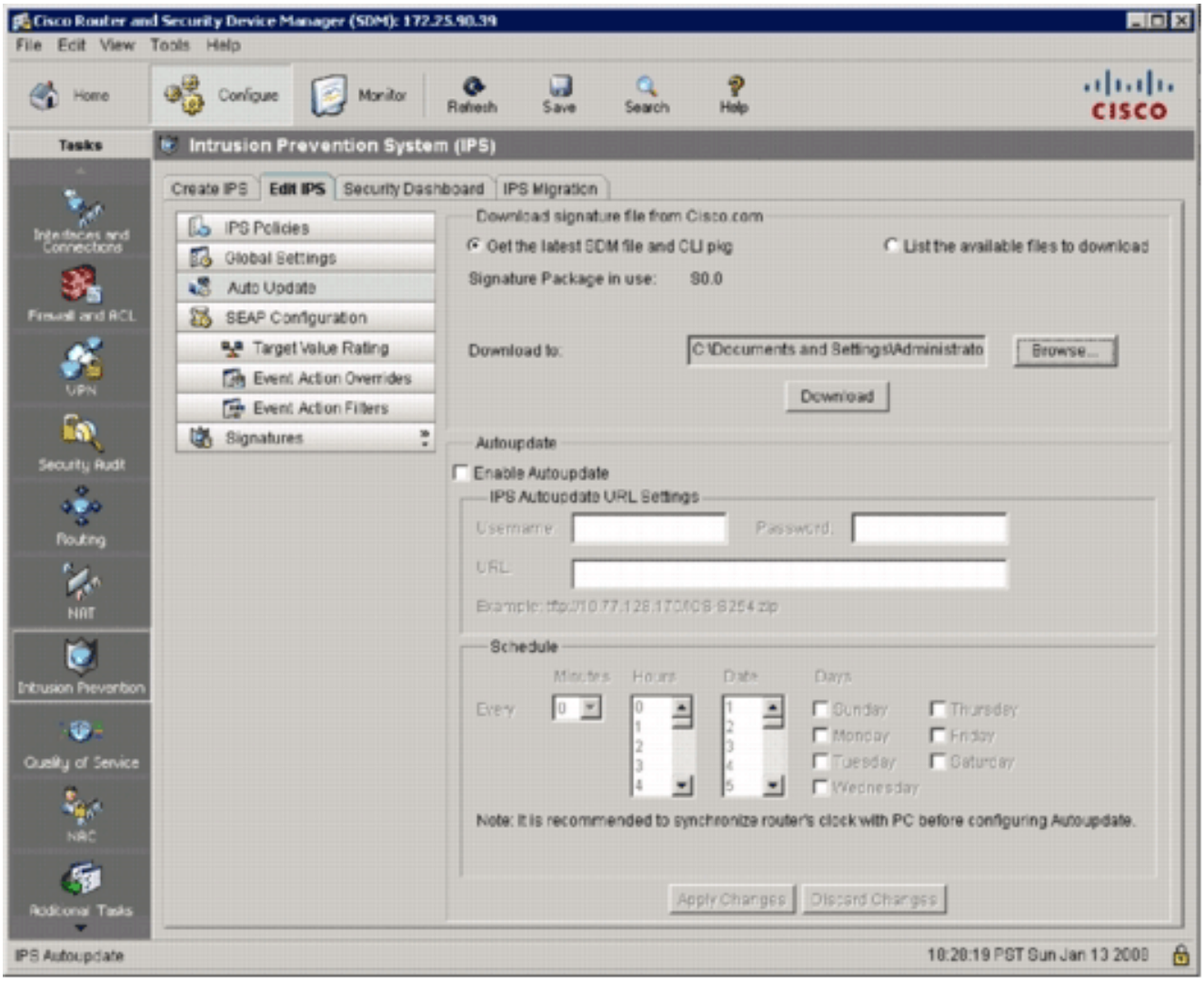
1. Scaricare SDM 2.5 da Cisco.com all'indirizzo http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm (solo utenti registrati) e installarlo su un PC locale.
2. Eseguire SDM 2.5 dal PC locale.
3. Quando viene visualizzata la finestra di dialogo Login a IOS IPS, immettere lo stesso nome

utente e la stessa password utilizzati per l'autenticazione SDM al router.

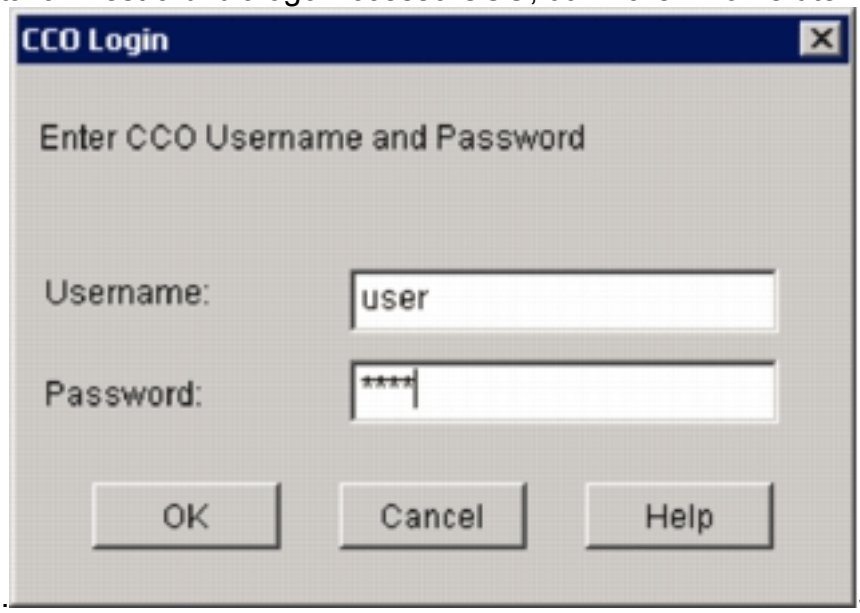
4. Dall'interfaccia utente di SDM, fare clic su **Configura**, quindi su **Prevenzione intrusioni**.
5. Fare clic sulla scheda **Modifica IPS**.
6. Se la notifica SDEE non è abilitata sul router, fare clic su **OK** per abilitarla.



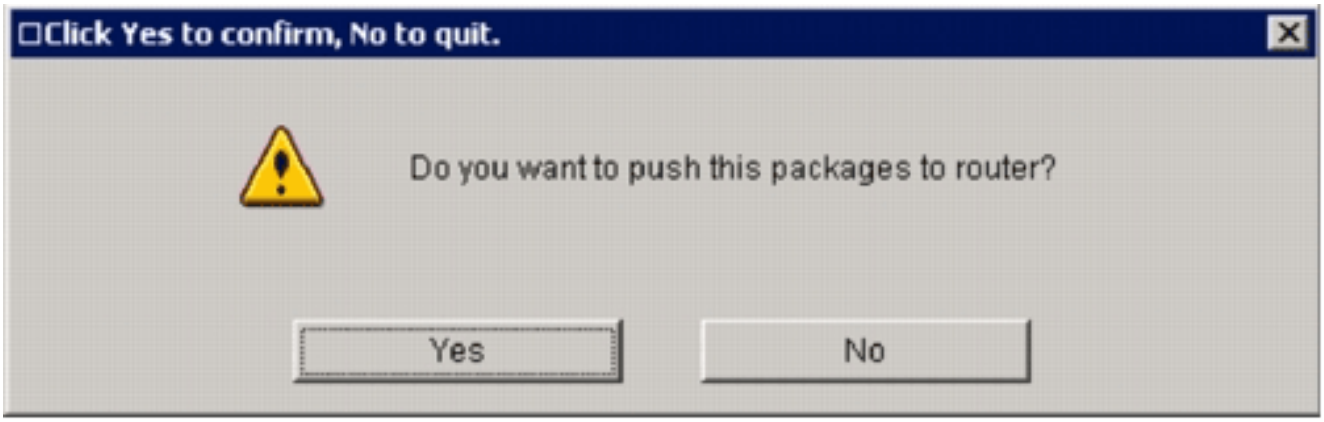
7. Nell'area Scarica file della firma da Cisco.com della scheda Modifica IPS, fare clic sul pulsante di opzione **Scarica il file SDM e il pacchetto CLI più recenti**, quindi fare clic su **Sfoglia** per selezionare una directory sul PC locale in cui salvare i file scaricati.Èpossibile scegliere la directory radice del server TFTP o FTP, che verrà utilizzata in seguito quando si distribuisce il pacchetto di firma al router.
8. Fare clic su **Download (Scarica).**



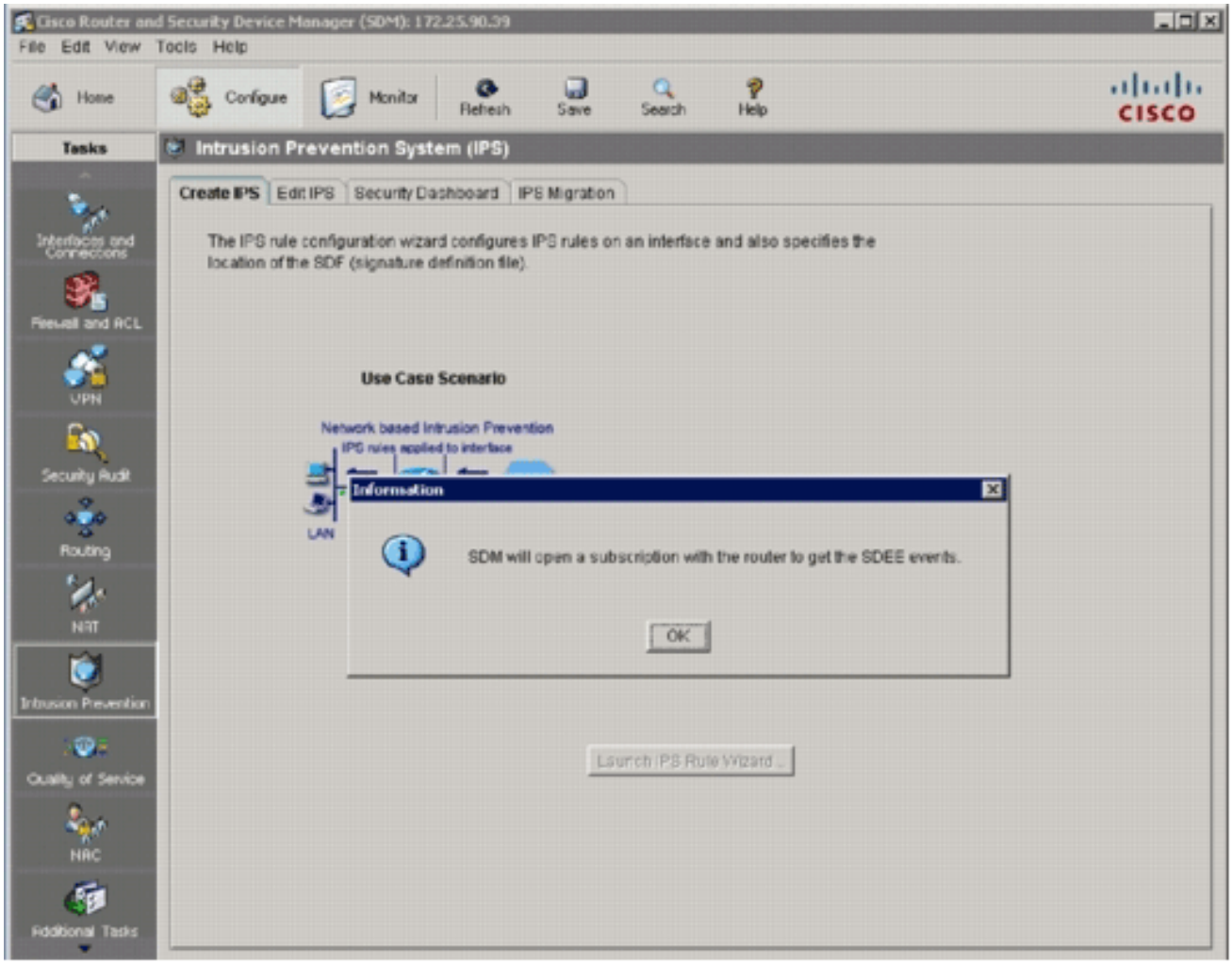
9. Quando viene visualizzata la finestra di dialogo Accesso CCO, utilizzare il nome utente e la password registrati CCO.



SDM si connette a Cisco.com e inizia a scaricare sia il file SDM (ad esempio, sigv5-SDM-S307.zip) che il file PKG della CLI (ad esempio, IOS-S313-CLI.pkg) nella directory selezionata al punto 7.Una volta scaricati entrambi i file, SDM chiede di inviare il pacchetto della firma scaricato al router.



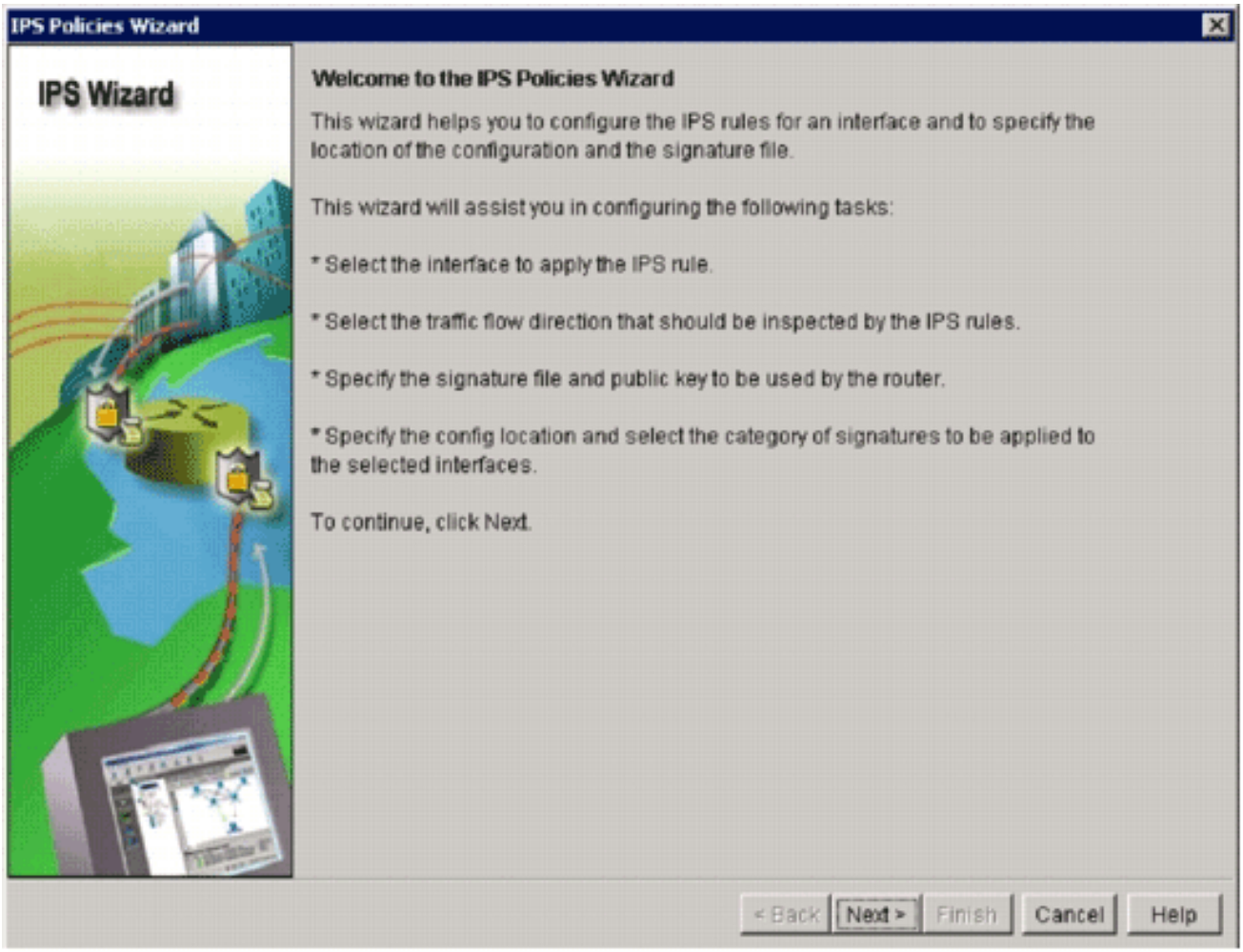
10. Fare clic su **No** poiché IOS IPS non è ancora stato configurato sul router.
11. Dopo aver scaricato l'ultimo pacchetto di firma CLI di IOS, fare clic sulla scheda **Create IPS** (Crea IPS) per creare la configurazione IPS IOS iniziale.
12. Se viene richiesto di applicare le modifiche al router, fare clic su **Applica modifiche**.
13. Fare clic su **Avvia Creazione guidata regola IPS**.Viene visualizzata una finestra di dialogo per informare l'utente che il modello SDM deve stabilire una sottoscrizione SDEE al router per recuperare gli
avvisi.



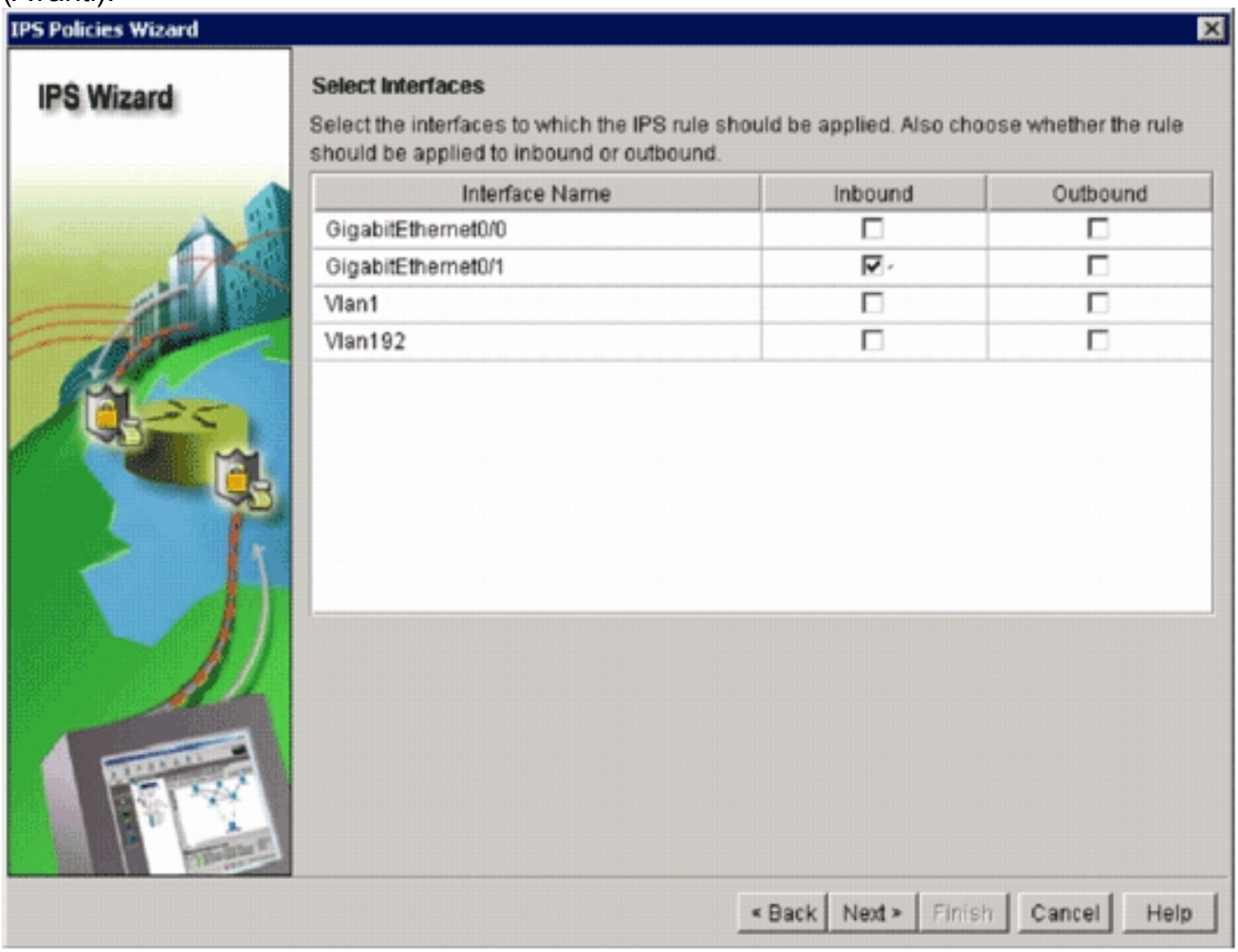
14. Fare clic su **OK**.Verrà visualizzata la finestra di dialogo Autenticazione

richiesta.

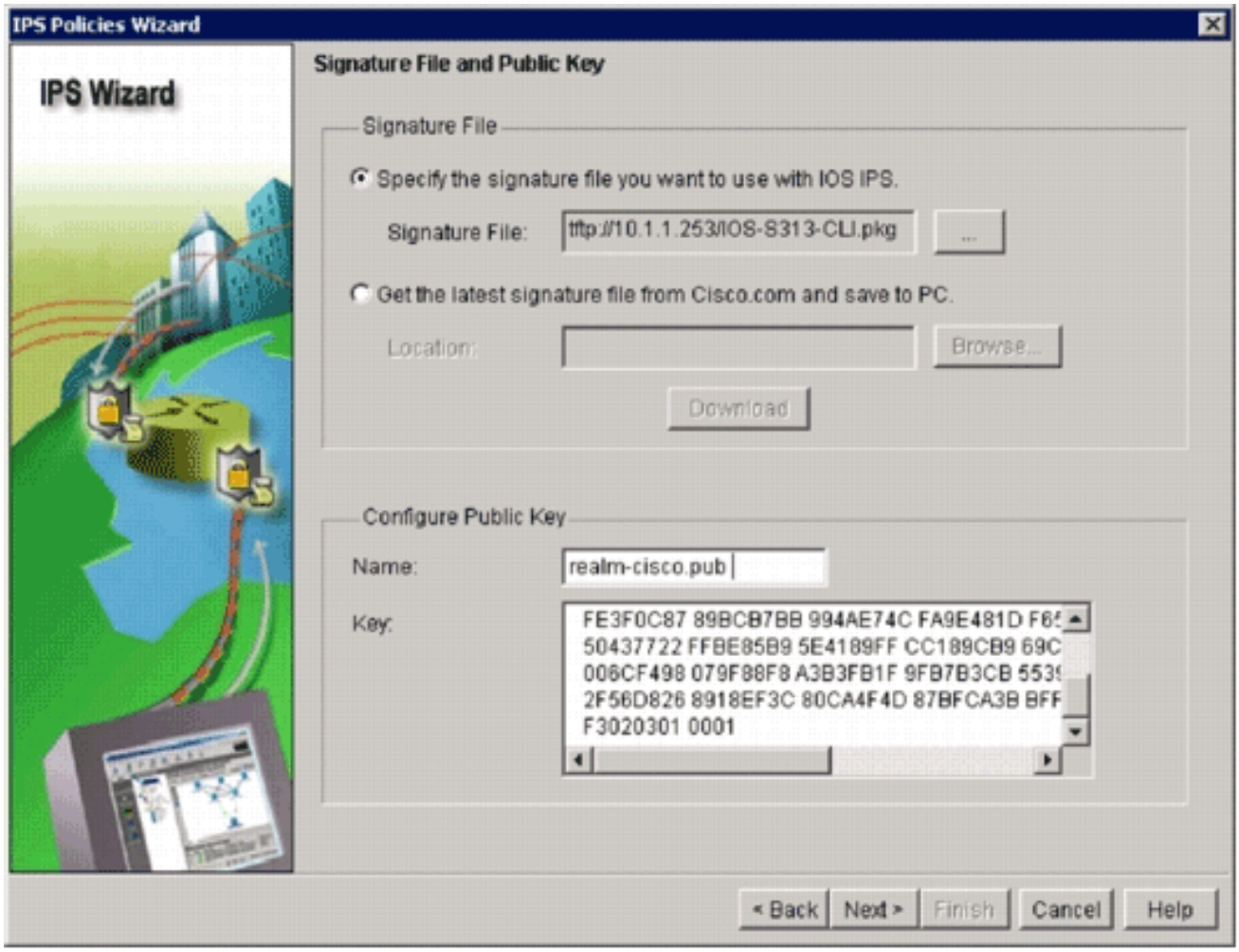
15. Immettere il nome utente e la password utilizzati per l'autenticazione SDM al router e fare clic su **OK**.Verrà visualizzata la finestra di dialogo Creazione guidata criteri IPS.



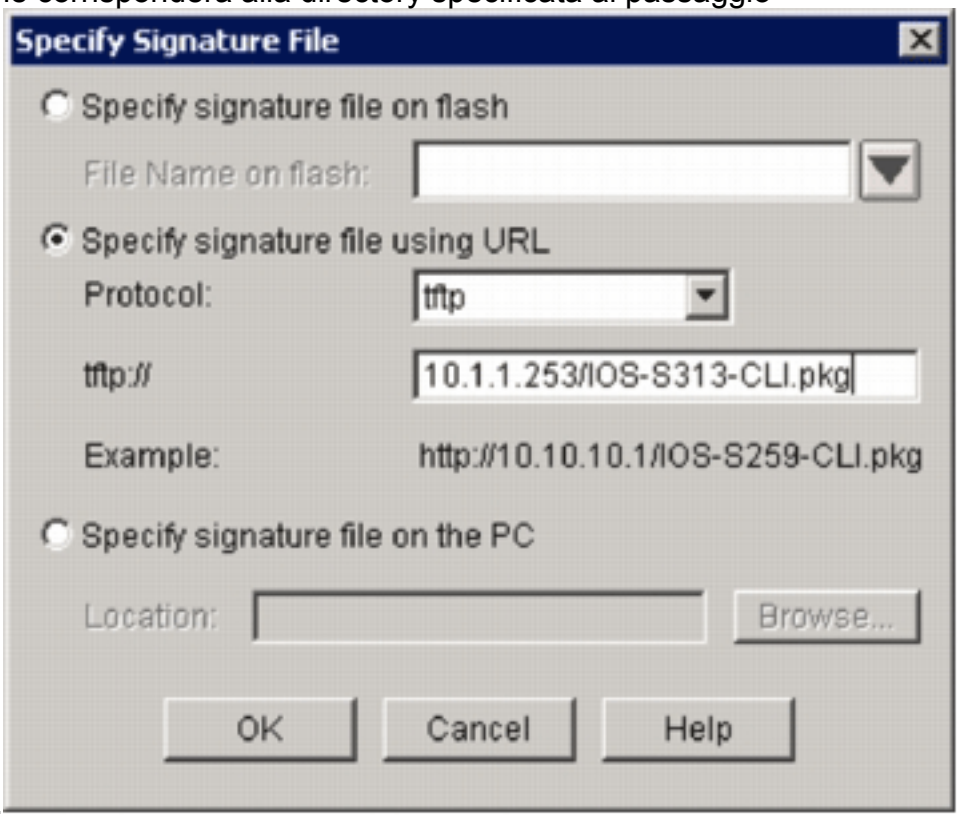
16. Fare clic su **Next** (Avanti).



17. Nella finestra Interfacce selezionate, scegliere l'interfaccia e la direzione a cui verrà applicato l'IPS IOS, quindi fare clic su **Avanti** per continuare.



18. Nell'area File della firma della finestra File della firma e chiave pubblica fare clic sul pulsante di opzione **Specifica il file della firma da utilizzare con IOS IPS** e quindi sul pulsante **File della firma** (...) per specificare la posizione del file del pacchetto della firma, che corrisponderà alla directory specificata al passaggio



7.

19. Fare clic sul pulsante di opzione **Specifica file di firma tramite URL** e scegliere un protocollo

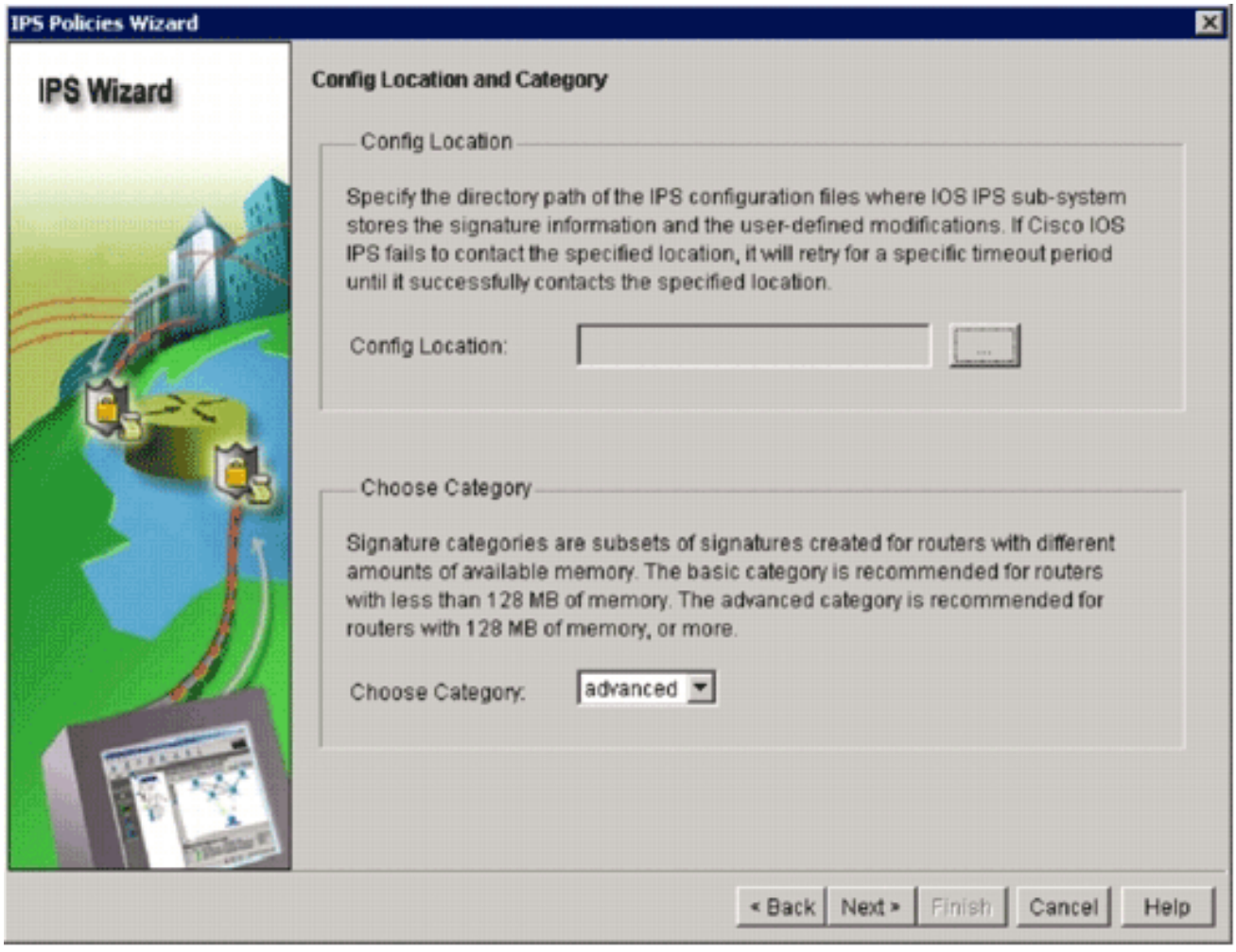
dall'elenco a discesa Protocollo.**Nota:** in questo esempio viene usato il protocollo TFTP per scaricare il pacchetto di firma sul router.

20. Immettere l'URL del file della firma e fare clic su **OK**.
21. Nell'area Configura chiave pubblica della finestra File della firma e chiave pubblica, immettere **realm-cisco.pub** nel campo Nome, quindi copiare la chiave pubblica e incollarla nel campo Chiave.

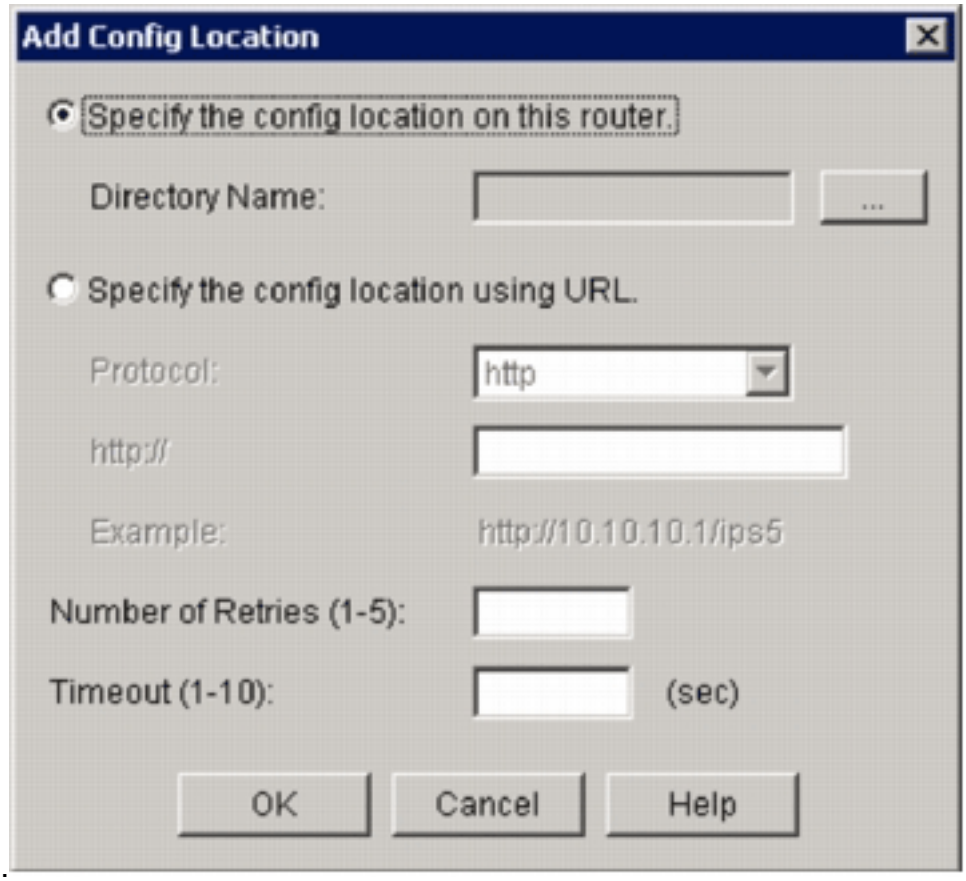
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

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
```

Nota: Questa chiave pubblica può essere scaricata da Cisco.com all'indirizzo: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup (solo utenti registrati).

22. Fare clic su **Avanti** per continuare.

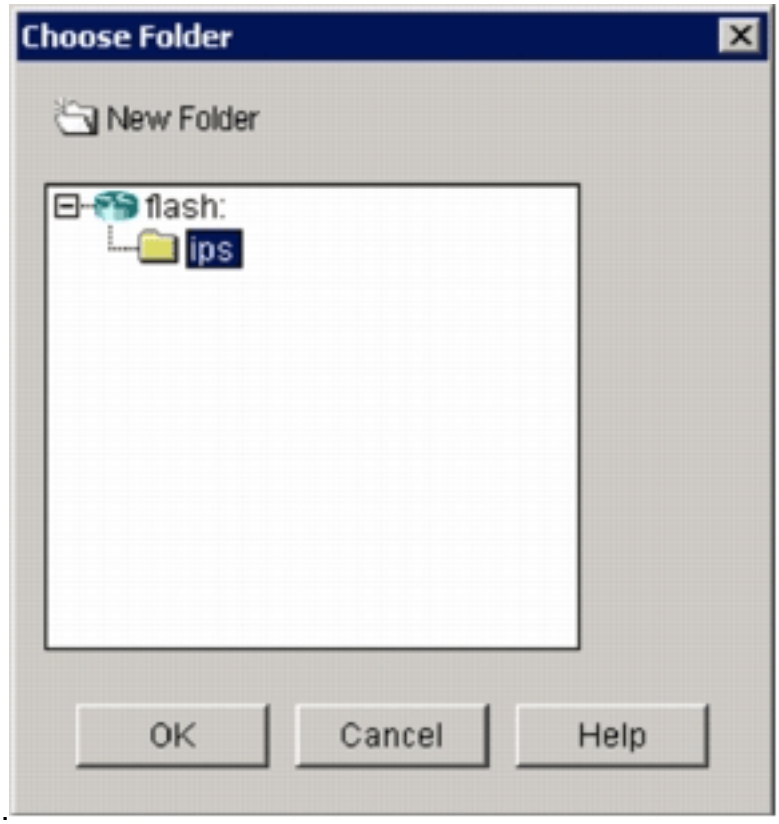


23. Nella finestra Posizione e categoria configurazione, fare clic sul pulsante **Posizione configurazione** (...) per specificare una posizione in cui verranno memorizzati i file di configurazione e di definizione delle firme.Viene visualizzata la finestra di dialogo **Aggiungi posizione di**

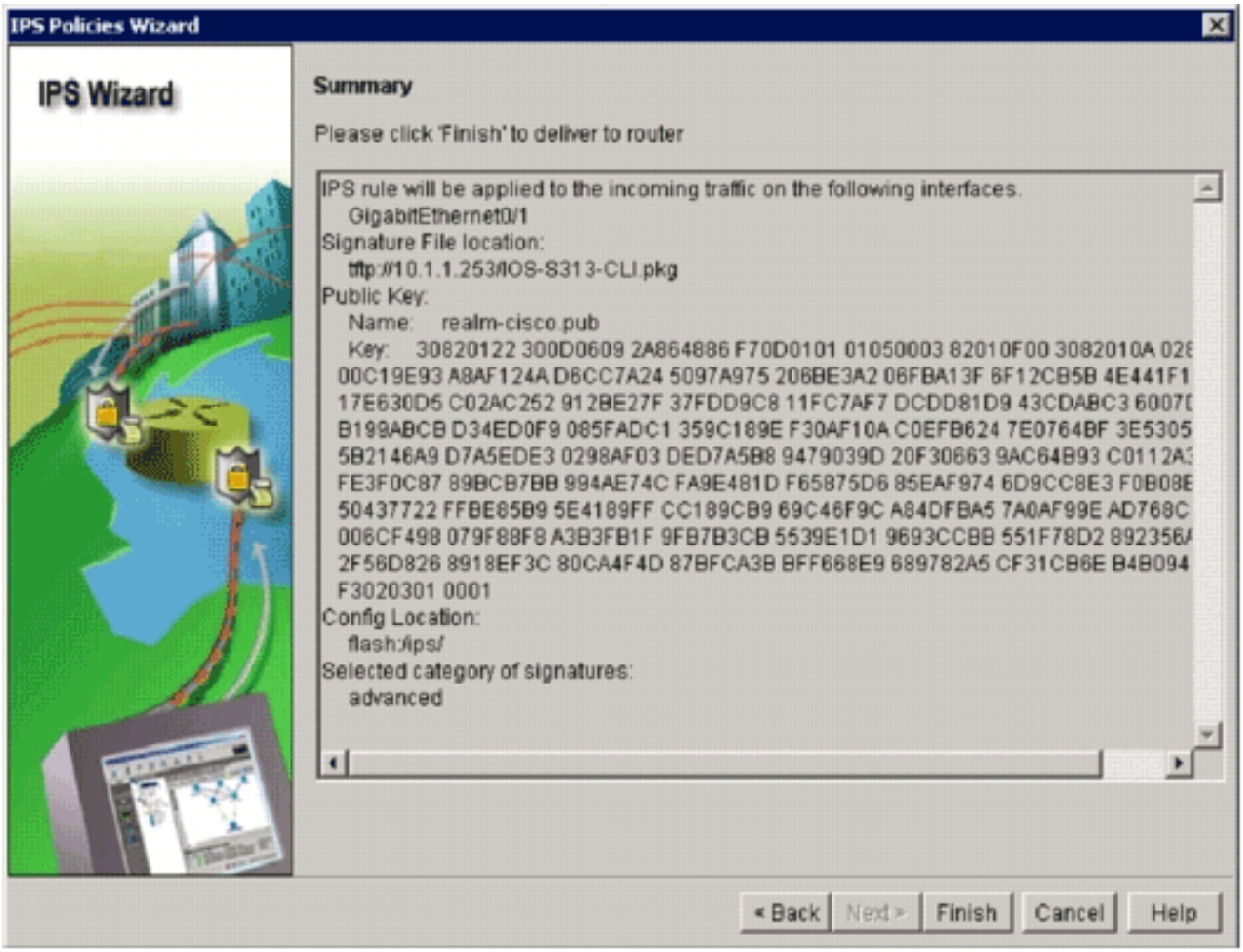


configurazione.

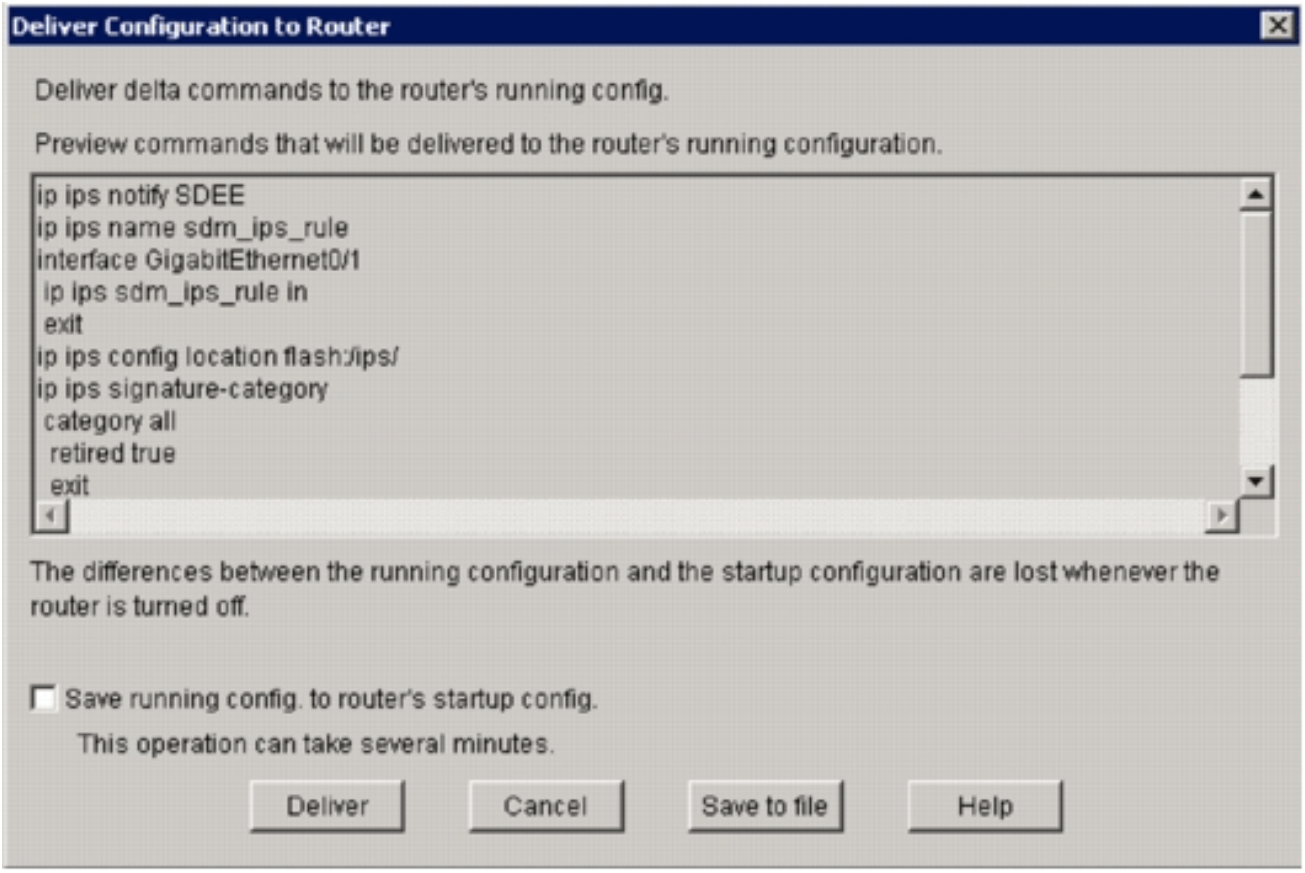
24. Nella finestra di dialogo Aggiungi percorso di configurazione, fare clic sul pulsante di opzione **Specifica il percorso di configurazione su questo router**, quindi fare clic sul pulsante **Nome directory** (...) per individuare il file di configurazione.Viene visualizzata la finestra di dialogo Scegli cartella che consente di selezionare una directory esistente o di creare una nuova directory sul flash del router per memorizzare i file di configurazione e definizione

della firma. 

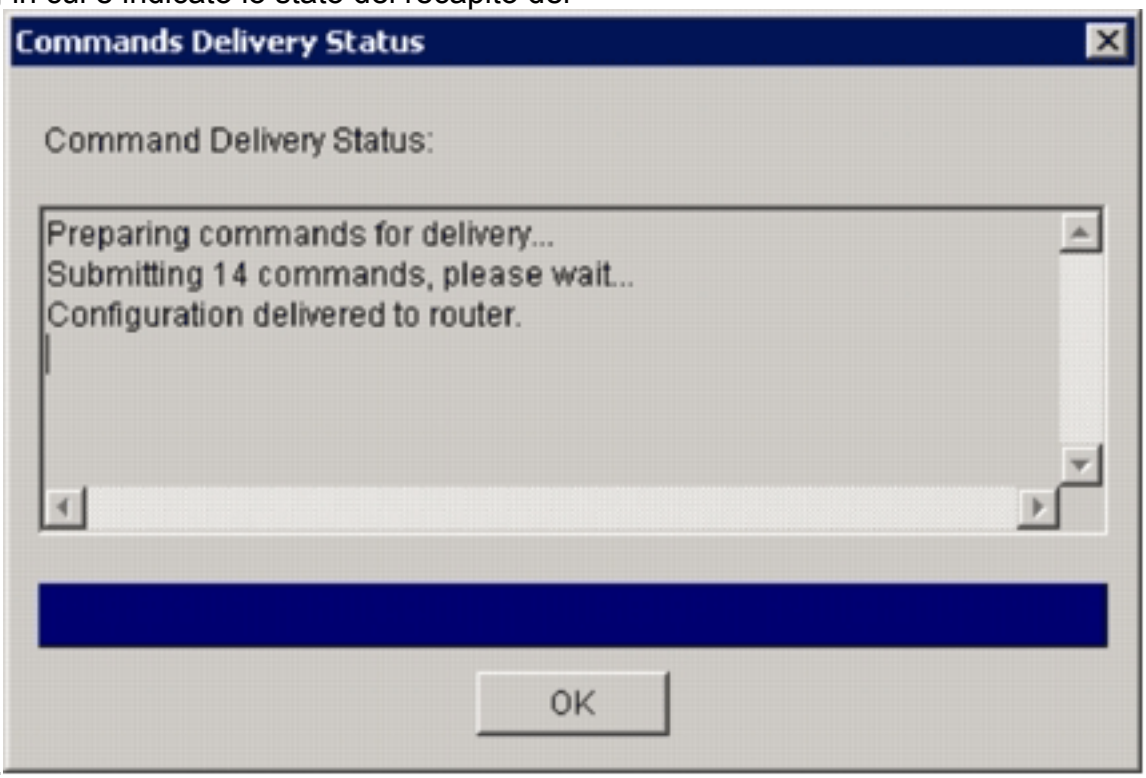
25. Se si desidera creare una nuova directory, fare clic su **Nuova cartella** nella parte superiore della finestra di dialogo.
26. Dopo aver selezionato la directory, fare clic su **OK** per applicare le modifiche e quindi su **OK** per chiudere la finestra di dialogo Aggiungi posizione di configurazione.
27. Nella finestra di dialogo Creazione guidata criteri IPS selezionare la categoria della firma in base alla quantità di memoria installata sul router. In SDM è possibile scegliere tra due categorie di firma: Basic e Advanced.Se sul router sono installati 128 MB di DRAM, Cisco consiglia di scegliere la categoria Basic per evitare errori di allocazione della memoria. Se sul router sono installati almeno 256 MB di DRAM, è possibile scegliere una delle due categorie.
28. Dopo aver selezionato una categoria da utilizzare, fare clic su **Avanti** per passare alla pagina di riepilogo.La pagina di riepilogo fornisce una breve descrizione delle attività di configurazione iniziale IPS
    IOS.



29. Fare clic su **Fine** nella pagina di riepilogo per inviare le configurazioni e il pacchetto di firma al router.Se l'opzione preview commands è abilitata nelle impostazioni Preferences in SDM, SDM visualizza la finestra di dialogo Delivery Configuration to Router che mostra un riepilogo dei comandi CLI che SDM invia al
router.

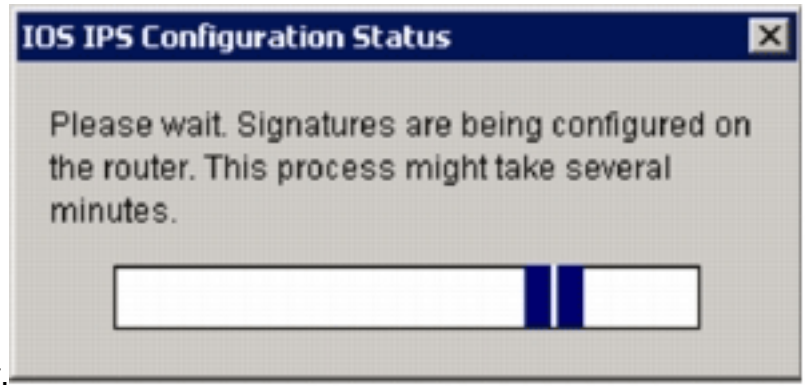


30. Per continuare, fare clic su **Consegna**.Verrà visualizzata la finestra di dialogo Stato recapito comandi, in cui è indicato lo stato del recapito dei



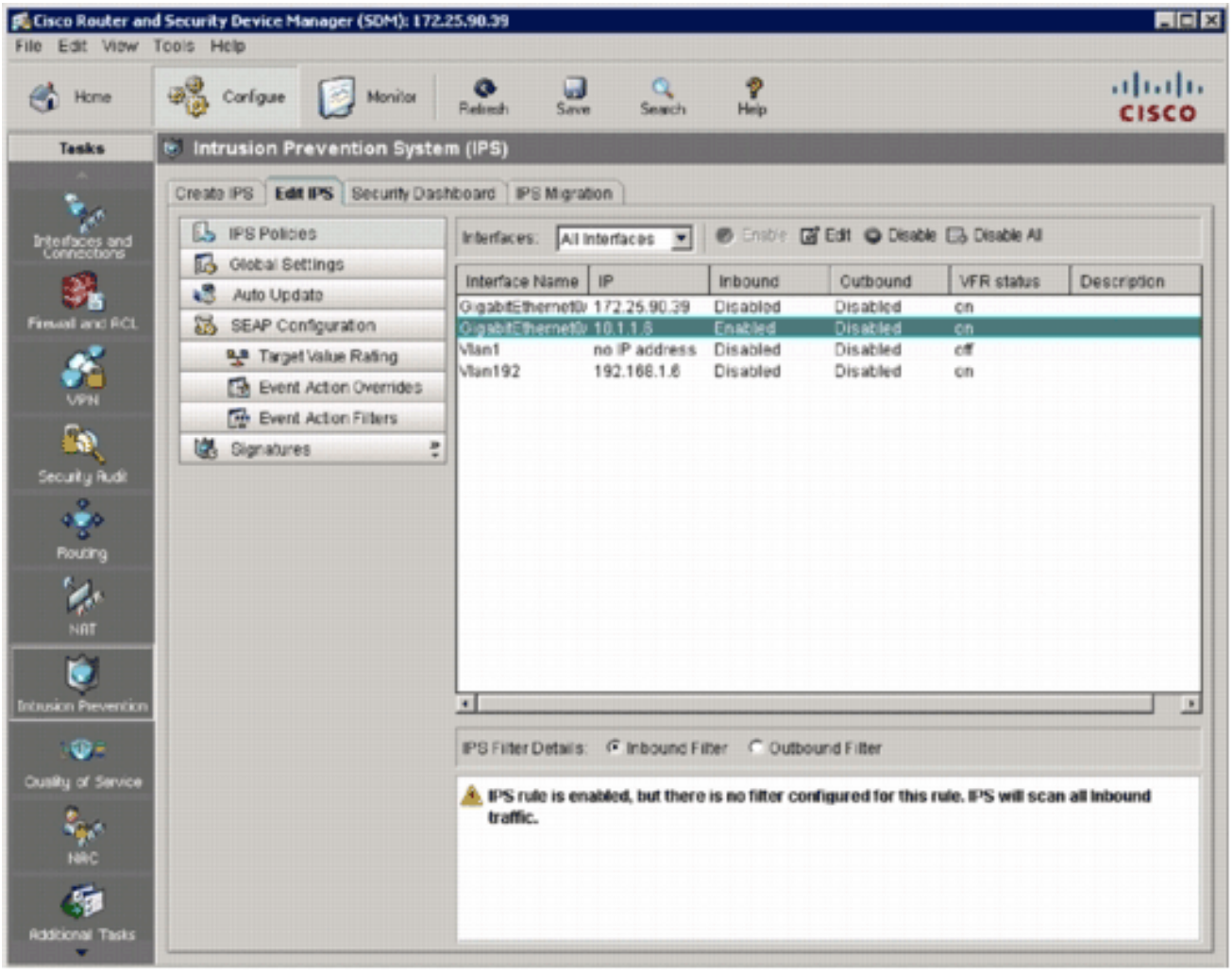
comandi.

31. Quando i comandi vengono recapitati sul router, fare clic su **OK** per continuare.Nella finestra di dialogo Stato configurazione IPS IOS viene visualizzato che le firme vengono

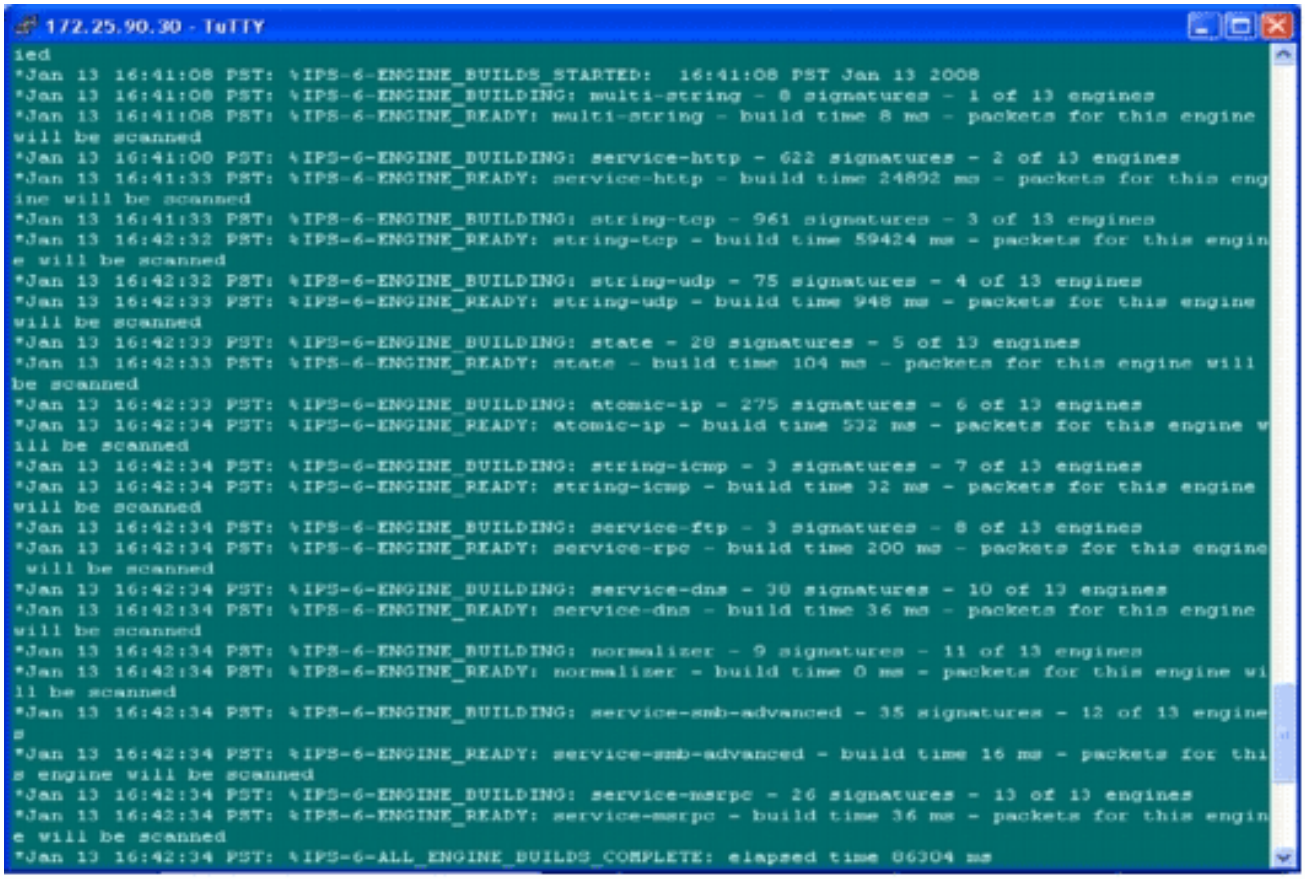


caricate sul router.

32. Quando le firme vengono caricate, SDM visualizza la scheda **Modifica IPS** con la configurazione corrente. Per verificare la configurazione, controllare l'interfaccia e la direzione in cui IOS IPS è abilitato.



La console del router mostra che le firme sono state caricate.

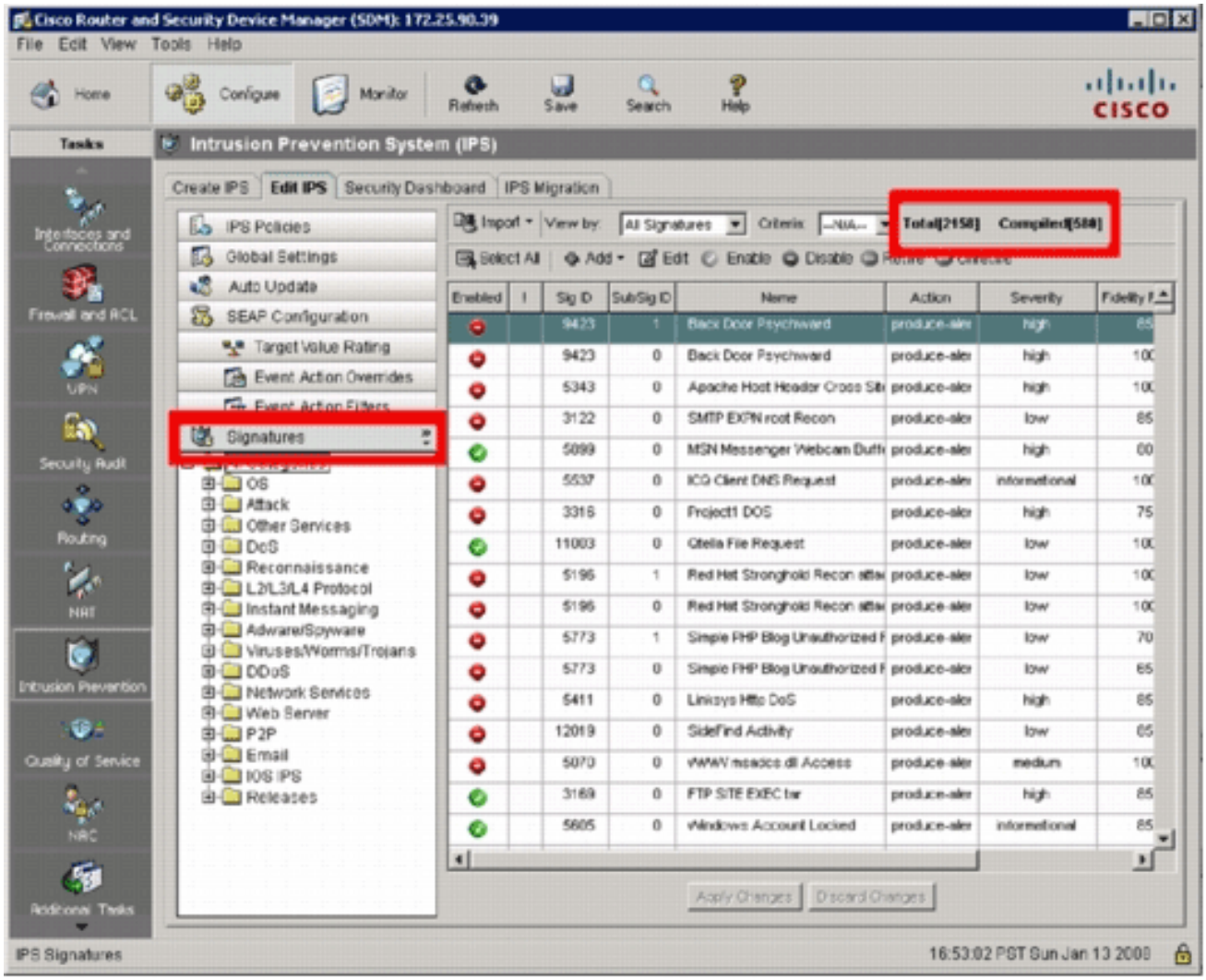


33. Per verificare che le firme siano caricate correttamente, usare il comando **show ip ips signatures count**.

```
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
```

Provisioning iniziale di IPS IOS con SDM 2.5 completato.

34. Verificare i numeri della firma con il modulo SDM, come mostrato nell'immagine.



Informazioni correlate

- Cisco IOS IPS su Cisco.com
- Pacchetto di firme IPS Cisco IOS
- File delle firme IPS Cisco IOS per SDM
- Guida introduttiva a Cisco IOS IPS con formato della firma 5.x
- Guida alla configurazione di Cisco IOS IPS
- Cisco IDS Event Viewer
- Documentazione e supporto tecnico – Cisco Systems