

# Configurazione di router e SDM e CLI di Cisco IOS in Cisco IOS IPS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Abilitare Cisco IOS IPS con un SDF predefinito](#)

[Aggiungi firme aggiuntive dopo l'attivazione di SDF predefinito](#)

[Selezione di firme e utilizzo delle categorie di firme](#)

[Aggiorna firme per file SDF predefiniti](#)

[Informazioni correlate](#)

## Introduzione

In Cisco Router and Security Device Manager (SDM) 2.2, la configurazione IPS di Cisco IOS<sup>®</sup> è integrata nell'applicazione SDM. Non è più necessario avviare una finestra separata per configurare Cisco IOS IPS.

In Cisco SDM 2.2, una nuova configurazione guidata IPS guida l'utente attraverso i passaggi necessari per abilitare Cisco IOS IPS sul router. Inoltre, è ancora possibile utilizzare le opzioni di configurazione avanzate per abilitare, disabilitare e ottimizzare Cisco IOS IPS con Cisco SDM 2.2.

Cisco consiglia di eseguire Cisco IOS IPS con i file di definizione della firma (SDF, Signature Definition File) non sincronizzati: attack-drop.sdf, 128 MB.sdf e 256 MB.sdf. Questi file vengono creati per router con diverse quantità di memoria. I file sono forniti in bundle con Cisco SDM, che consiglia gli SDF quando si abilita Cisco IOS IPS su un router per la prima volta. Questi file possono essere scaricati anche dal sito <http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup> (solo utenti [registrati](#)).

Il processo per abilitare gli SDF predefiniti è descritto in [Abilitare Cisco IOS IPS con SDF predefinito in fabbrica](#). Se gli SDF predefiniti non sono sufficienti o si desidera aggiungere nuove firme, è possibile utilizzare la procedura descritta in [Aggiungi firme aggiuntive dopo aver attivato l'SDF predefinito](#).

## Prerequisiti

### Requisiti

Per utilizzare Cisco SDM 2.2, è necessario Java Runtime Environment (JRE) versione 1.4.2 o successive. Un file di firma ottimizzato e consigliato da Cisco (basato su DRAM) è fornito con Cisco SDM (caricato sulla memoria flash del router con Cisco SDM).

## Componenti usati

Il riferimento delle informazioni contenute in questo documento è il router Cisco e il Security Device Manager (SDM) 2.2.

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

### Abilitare Cisco IOS IPS con un SDF predefinito

#### Procedura CLI

Completare questa procedura per utilizzare la CLI per configurare un router Cisco serie 1800 con Cisco IOS IPS in modo da caricare il file 128MB.sdf sul flash del router.

1. Configurare il router per abilitare la notifica degli eventi SDEE (Security Device Event Exchange).

```
yourname#conf t
```

2. Immettere i comandi di configurazione (uno per riga), quindi premere Ctrl+Z per terminare.

```
yourname(config)#ip ips notify sdee
```

3. Creare un nome di regola IPS da utilizzare per l'associazione alle interfacce.

```
yourname(config)#ip ips name myips
```

4. Configurare un comando di posizione IPS per specificare il file dal quale il sistema IPS Cisco IOS leggerà le firme. In questo esempio il file viene utilizzato nella memoria flash: 128 MB.sdf. La parte relativa all'URL della posizione di questo comando può essere qualsiasi URL valido che utilizzi flash, disco o protocolli via FTP, HTTP, HTTPS, RTP, SCP e TFTP per puntare ai file.

```
yourname(config)#ip ips sdf location flash:128MB.sdf
```

**Nota:** è necessario abilitare il comando **terminal monitor** se si configura il router tramite una sessione Telnet, altrimenti i messaggi SDEE non verranno visualizzati durante la generazione del motore di firma.

5. Abilitare il protocollo IPS sull'interfaccia in cui si desidera abilitare il protocollo IPS di Cisco

IOS per la scansione del traffico. In questo caso, l'abilitazione è stata eseguita su entrambe le direzioni sull'interfaccia fastEthernet 0.

```
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 of 15 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

```

La prima volta che una regola IPS viene applicata a un'interfaccia, Cisco IOS IPS avvia le firme generate dal file specificato dal comando SDF locations. I messaggi SDEE vengono registrati sulla console e inviati al server syslog, se configurato. I messaggi SDEE con *<number>* di *<number>* motori indicano il processo di generazione del motore di firma. Infine, quando i due numeri sono uguali, tutti i motori sono costruiti. **Nota:** il riassettaggio virtuale IP è una funzione di interfaccia che (se attivata) ricompone automaticamente i pacchetti frammentati che entrano nel router tramite l'interfaccia. Cisco consiglia di abilitare l'assembly virtuale ip su tutte le interfacce su cui arriva il traffico nel router. Nell'esempio precedente, oltre a attivare "ip virtual-assembly" sull'interfaccia fast Ethernet 0, la configuriamo anche sull'interfaccia interna VLAN 1.

```

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

```

## Procedura SDM 2.2

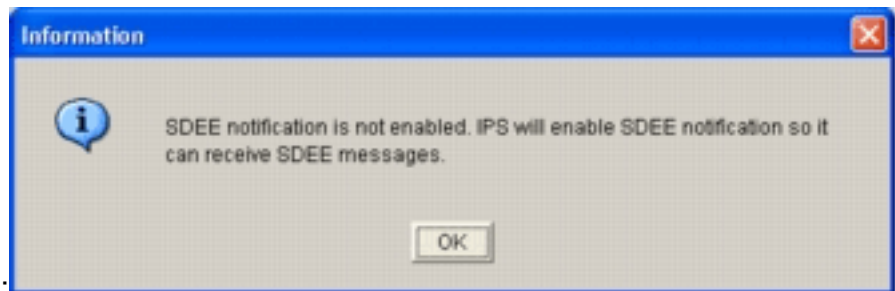
Completare questa procedura per utilizzare Cisco SDM 2.2 per configurare un router Cisco serie 1800 con Cisco IOS IPS.

1. Nell'applicazione SDM, fare clic su **Configura**, quindi su **Prevenzione**



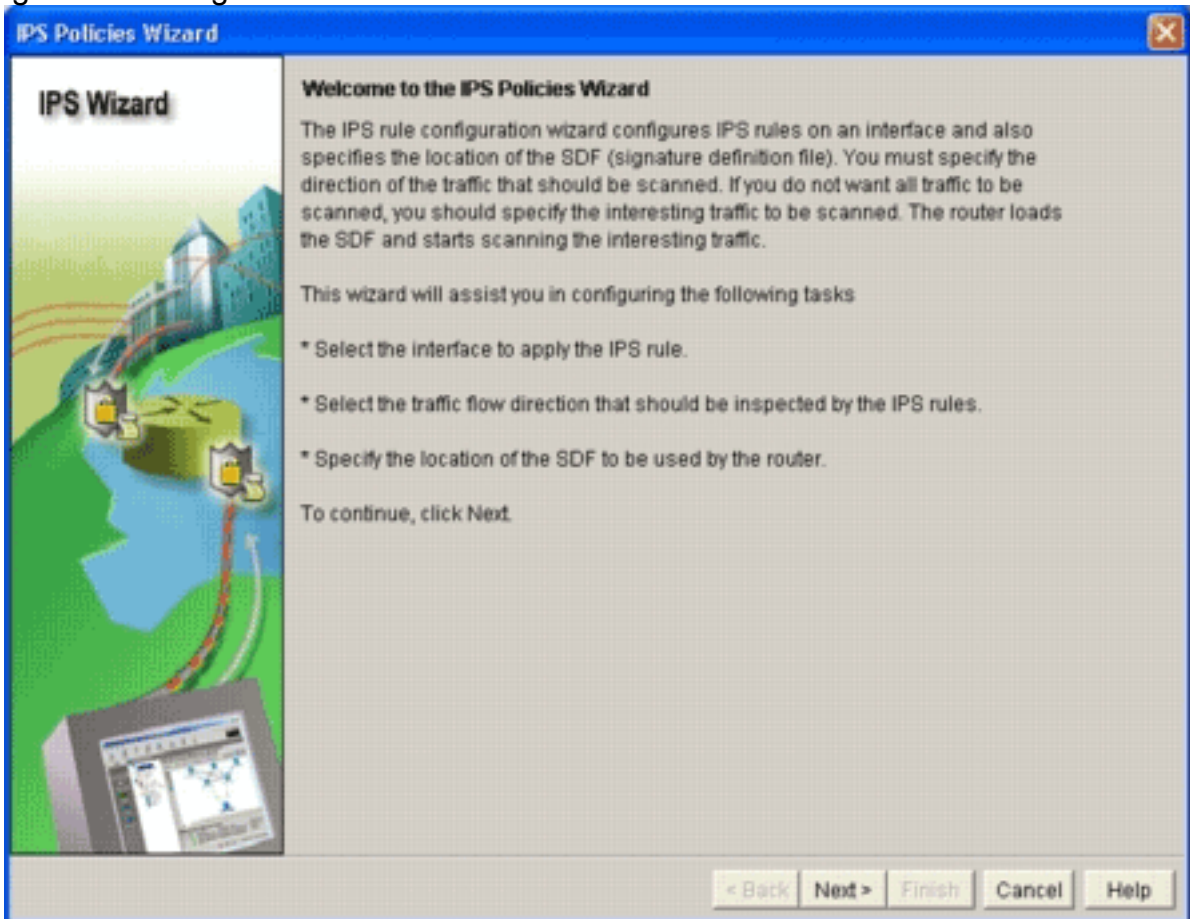
intrusioni.

2. Fare clic sulla scheda **Creazione guidata regola IPS** e quindi su **Avvia Creazione guidata regola IPS**. Per configurare la funzionalità IPS di Cisco IOS, il modello Cisco SDM richiede la notifica degli eventi IPS tramite SDEE. Per impostazione predefinita, la notifica SDEE non è attivata. Cisco SDM richiede di abilitare la notifica degli eventi IPS tramite SDEE, come



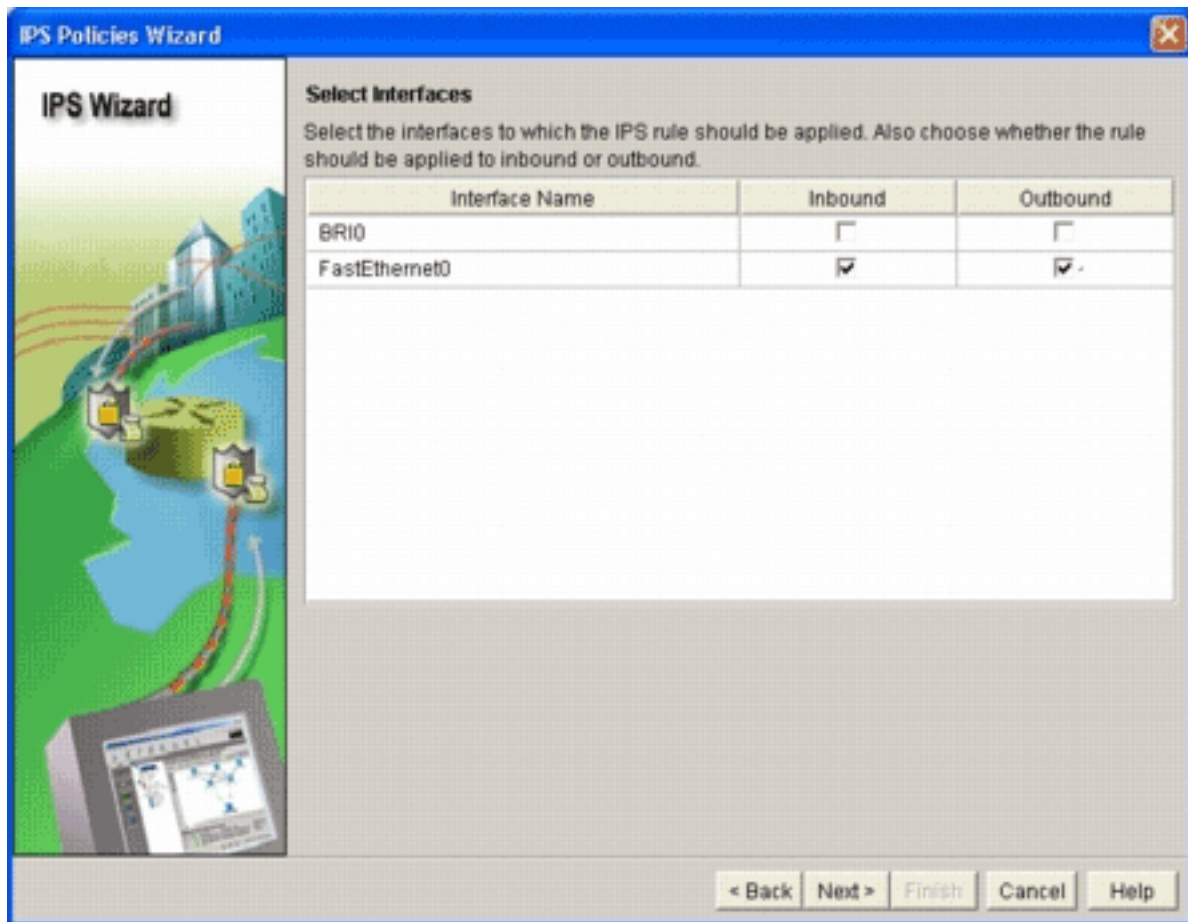
mostrato nell'immagine:

3. Fare clic su **OK**.Verrà visualizzata la finestra Impostazione guidata criteri IPS della finestra di dialogo Creazione guidata criteri



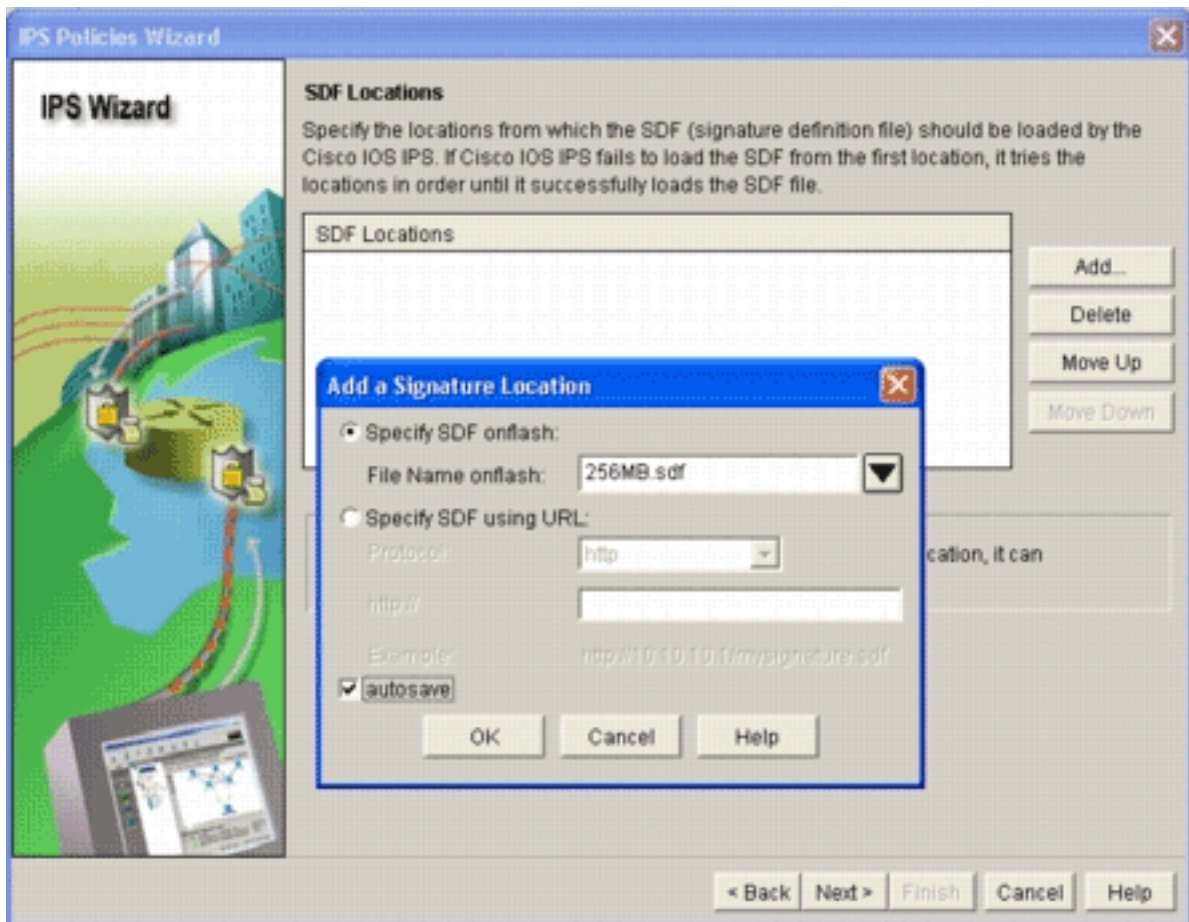
IPS.

4. Fare clic su **Next** (Avanti).Viene visualizzata la finestra Seleziona interfacce.



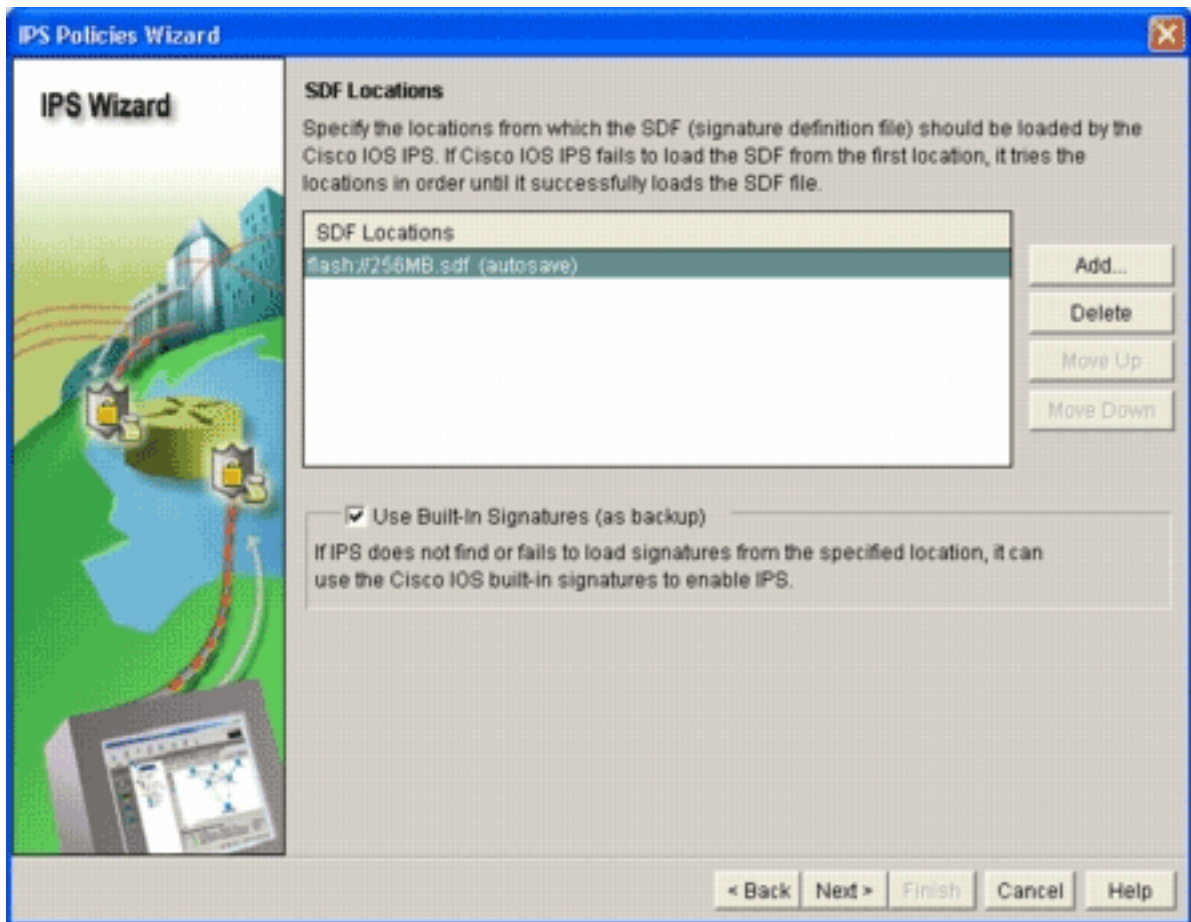
5. Selezionare le interfacce per le quali si desidera abilitare l'IPS e fare clic sulla casella di controllo **In entrata** o **In uscita** per indicare la direzione dell'interfaccia. **Nota:** quando si abilita IPS su un'interfaccia, Cisco consiglia di abilitare sia le direzioni in entrata che quelle in uscita.
6. Fare clic su **Next** (Avanti). Viene visualizzata la finestra Posizioni SDF.
7. Per configurare una posizione SDF, fare clic su **Add** (Aggiungi). Verrà visualizzata la finestra di dialogo Aggiungi posizione





firma.

8. Fare clic sul pulsante di scelta **Specifica SDF su flash**, quindi scegliere 256MB.sdf dall'elenco a discesa **Nome file su flash**.
9. Selezionare la casella di controllo **Salvataggio automatico** e fare clic su **OK**. **Nota:** L'opzione di salvataggio automatico consente di salvare automaticamente il file della firma quando viene apportata una modifica alla firma. La finestra Posizioni SDF visualizza la nuova posizione



SDF.

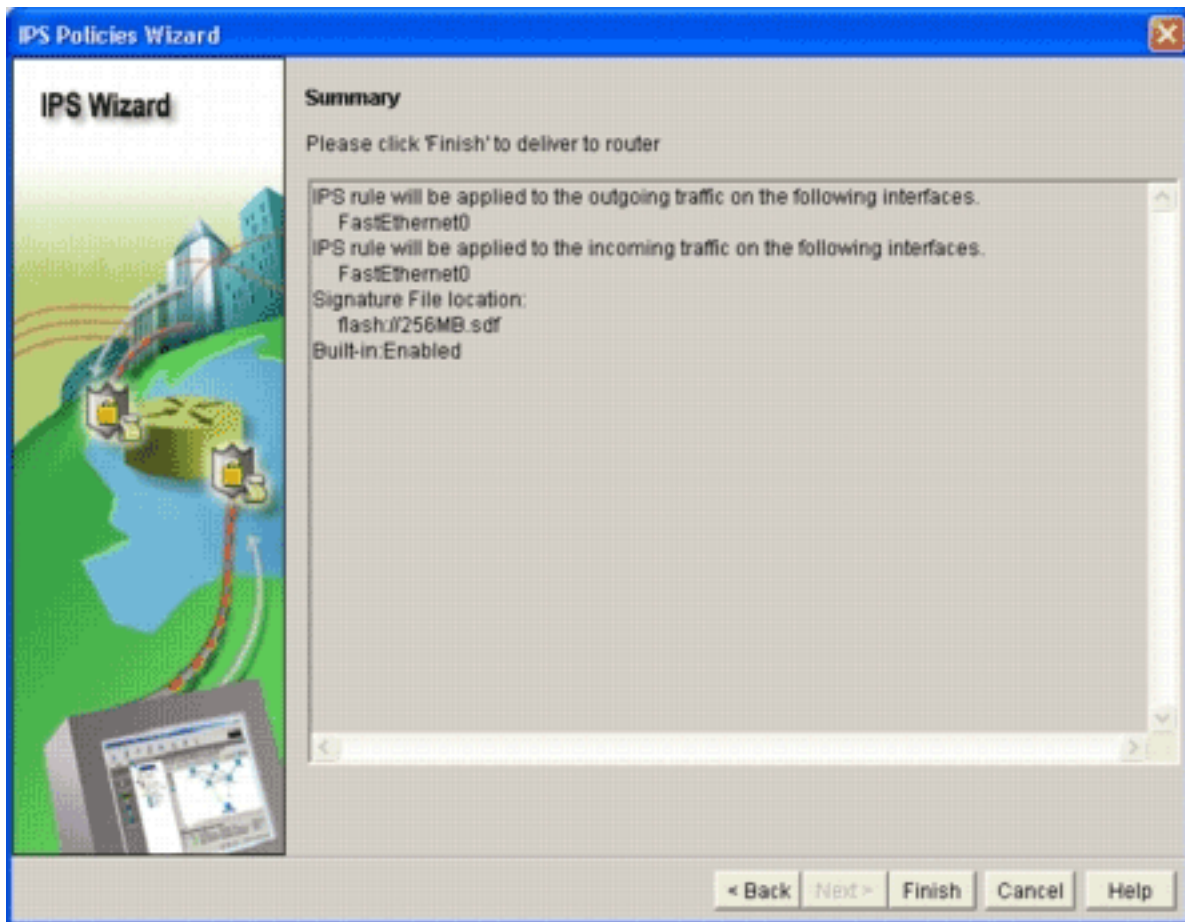
Not

a: è possibile aggiungere ulteriori percorsi di firma per definire un backup.

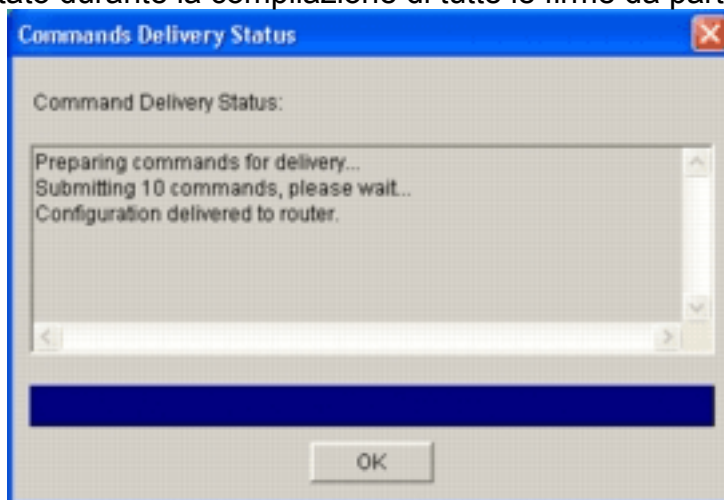
10. Selezionare la casella di controllo **Usa firme incorporate (come backup)**. Nota: Cisco consiglia di non utilizzare l'opzione di firma incorporata a meno che non siano stati specificati uno o più percorsi.

11. Per continuare, fare clic su **Avanti**. Viene visualizzata la finestra Riepilogo.



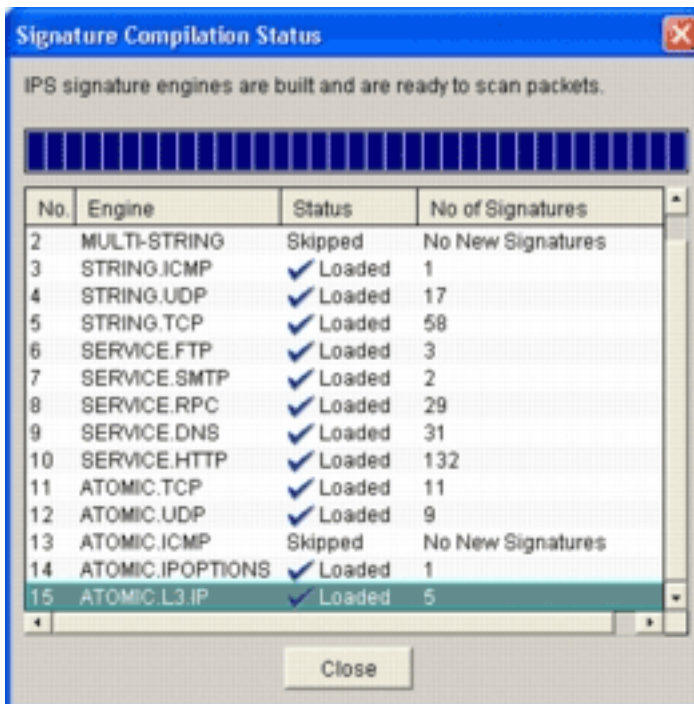


12. Fare clic su **Finish** (Fine). Nella finestra di dialogo Stato recapito comandi viene visualizzato lo stato durante la compilazione di tutte le firme da parte del motore



IPS.

13. Al termine del processo, fare clic su **OK**. Nella finestra di dialogo Stato compilazione firma vengono visualizzate le informazioni di compilazione della



firma.

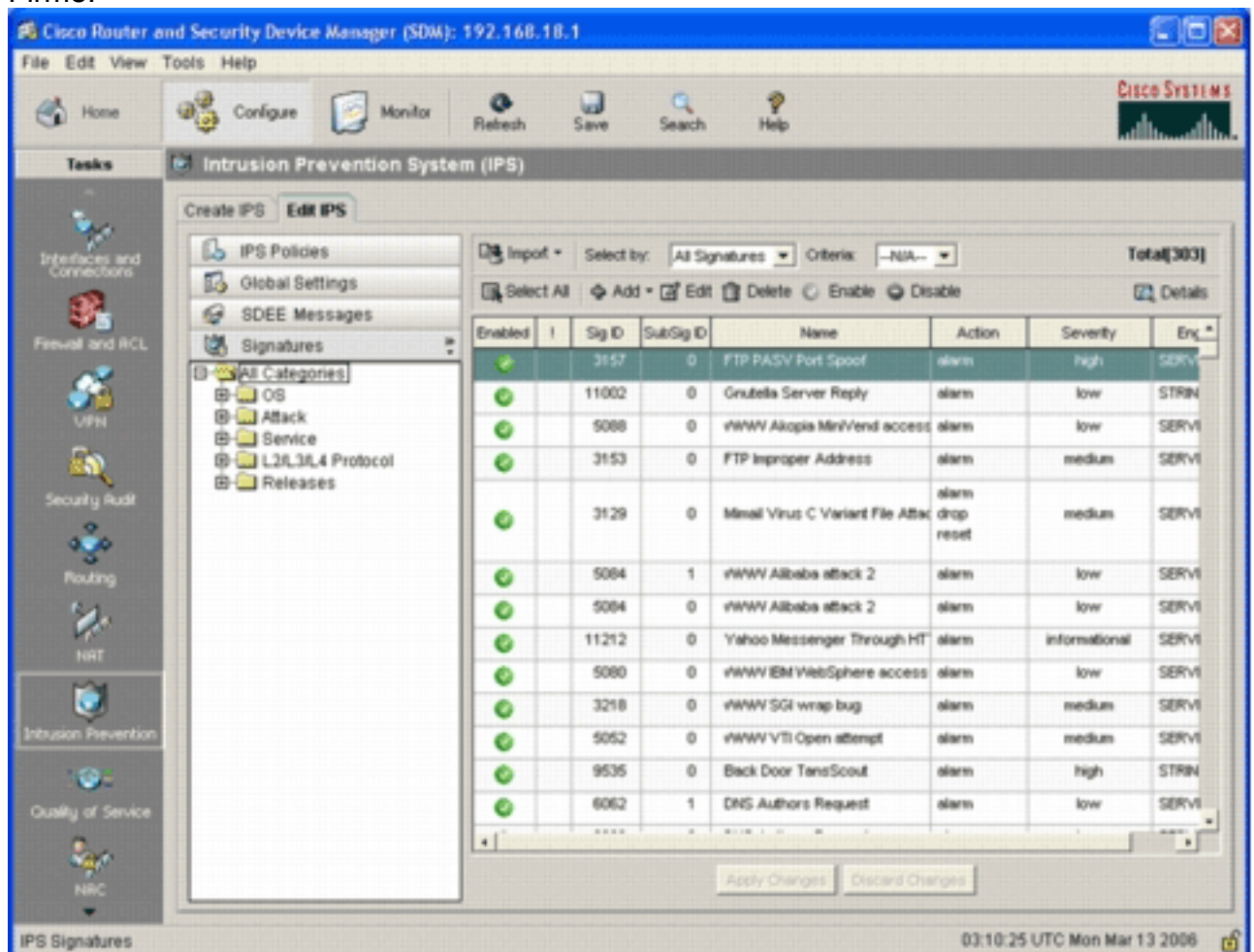
Queste informazioni mostrano quali

motori sono stati compilati e il numero di firme nel motore. Per i motori che visualizzano *Ignorato* nella colonna di stato, non è presente alcuna firma caricata per quel motore.

14. Per chiudere la finestra di dialogo Stato compilazione firma, fare clic su **Chiudi**.

15. Per verificare quali firme sono attualmente caricate sul router, fare clic su **Configura** e quindi su **Prevenzione intrusioni**.

16. Fare clic sulla scheda **Modifica IPS** e quindi su **Firme**.L'elenco delle firme IPS viene visualizzato nella finestra **Firme**.



## Aggiungi firme aggiuntive dopo l'attivazione di SDF predefinito

### Procedura CLI

Nessun comando CLI disponibile per creare firme o leggere le informazioni sulla firma dal file IOS-Sxxx.zip distribuito. Cisco consiglia di utilizzare il modello SDM o il Management Center for IPS Sensor per gestire le firme sui sistemi IPS Cisco IOS.

Per i clienti che hanno già pronto un file di firma e desiderano unire questo file con l'SDF in esecuzione su un sistema Cisco IOS IPS, è possibile utilizzare questo comando:

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

Il file di firma definito dal comando signature location è il percorso in cui il router carica i file di firma quando viene ricaricato o quando il router IOS IPS viene riconfigurato. Affinché il processo di unione riesca, è necessario aggiornare anche il file definito dal comando di posizione del file di firma.

1. Utilizzare il comando **show** per controllare i percorsi delle firme configurati. L'output mostra i percorsi delle firme configurati. Con questo comando viene indicato da dove vengono caricate le firme correnti in esecuzione.

```
yourname#show ip ips signatures
Builtin signatures are configured
```

Firme caricate per l'ultima volta da flash:128MB.sdf Cisco SDF versione S128.0 Trend SDF release versione V0.0

2. Per unire i file delle firme, usare il comando **copy <url> ips-sdf** insieme alle informazioni del passaggio precedente.

```
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#

Dopo aver eseguito il comando **copy**, il router carica il file della firma nella memoria e quindi crea i motori della firma. Nell'output del messaggio SDEE della console viene visualizzato lo stato di compilazione per ogni motore di firma. %IPS-6-ENGINE\_BUILD\_SKIPPED indica che non sono presenti nuove firme per questo motore. %IPS-6-ENGINE\_READY indica che sono presenti nuove firme e che il modulo è pronto. Come in precedenza, il messaggio "15 di 15 motori" indica che tutti i motori sono stati costruiti. IPS-7-UNSUPPORTED\_PARAM indica che un determinato parametro non è supportato da Cisco IOS IPS. Ad esempio, CapturePacket e ResetAfterIdle. **Nota:** Questi messaggi sono solo a scopo informativo e non influiranno sulle funzionalità di firma o sulle prestazioni di Cisco IOS IPS. È possibile disattivare questi messaggi di registrazione impostando un livello di registrazione superiore a quello di debug (livello 7).

3. Aggiornare l'SDF definito dal comando signature location, in modo che quando il router viene ricaricato, abbia la firma unita impostata con le firme aggiornate. Nell'esempio viene mostrata la differenza di dimensioni dopo il salvataggio della firma unita nel file flash 128MB.sdf.

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

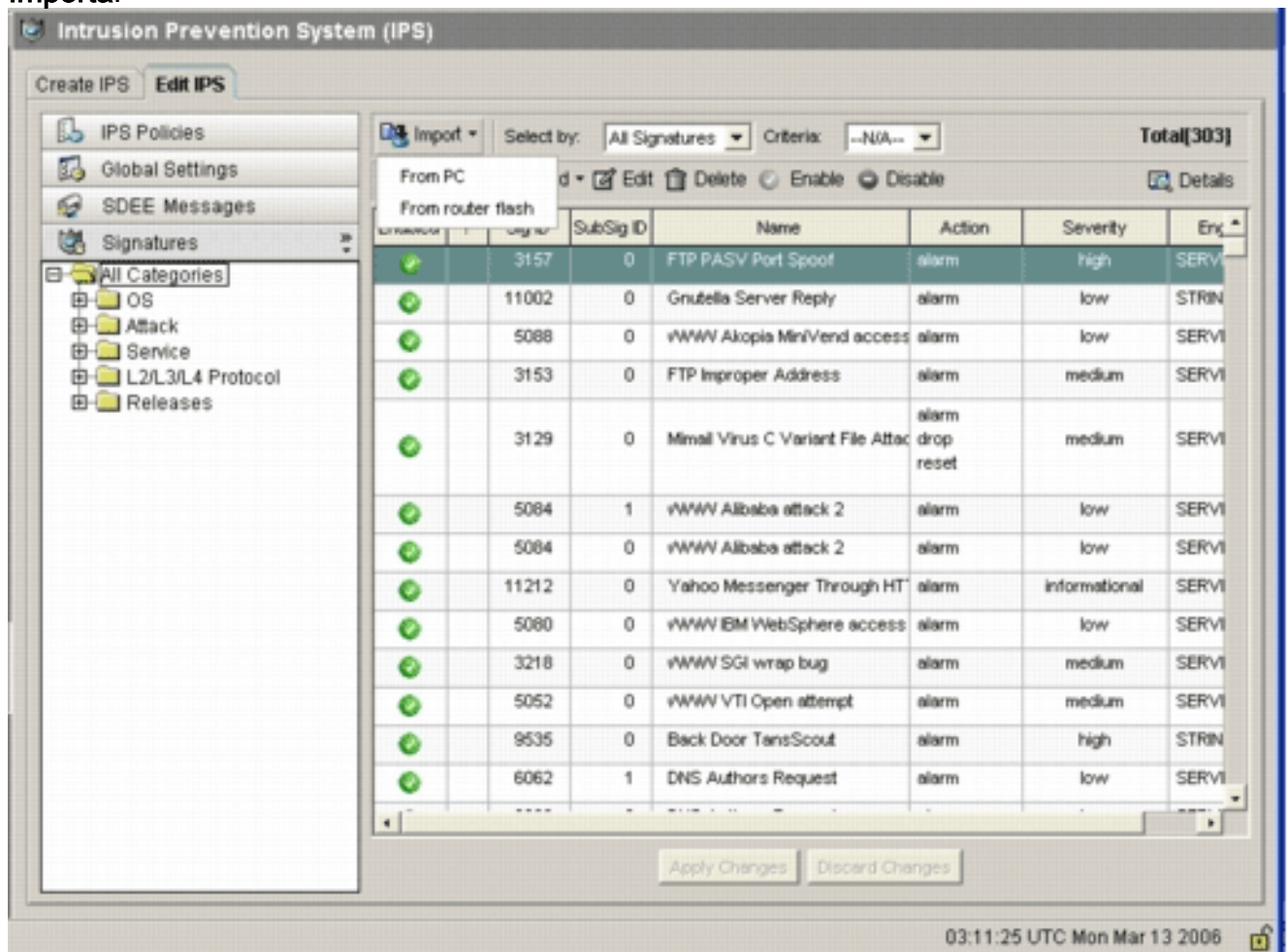
```

**Avviso:** il nuovo file 128MB.sdf contiene ora le firme acquisite dal cliente. il contenuto è diverso dal file predefinito 128MB.sdf di Cisco. Cisco consiglia di modificare il nome del file per evitare confusione. Se il nome viene modificato, è necessario modificare anche il comando di posizione della firma.

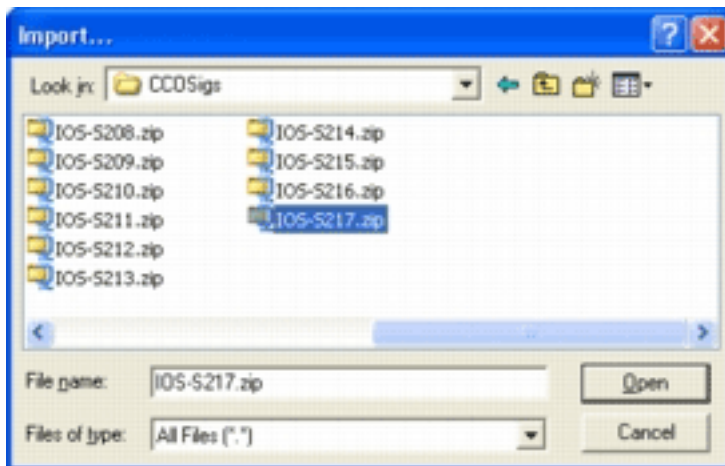
## Procedura SDM 2.2

Dopo aver abilitato Cisco IOS IPS, è possibile aggiungere nuove firme nel router che esegue un set di firme con la funzione di importazione Cisco SDM. Per importare nuove firme, completare i seguenti passaggi:

1. Scegliere gli SDF predefiniti o il file di aggiornamento IOS-Sxxx.zip per importare ulteriori firme.
2. Fare clic su **Configura** e quindi su **Prevenzione intrusioni**.
3. Fare clic sulla scheda **Modifica IPS** e quindi su **Importa**.

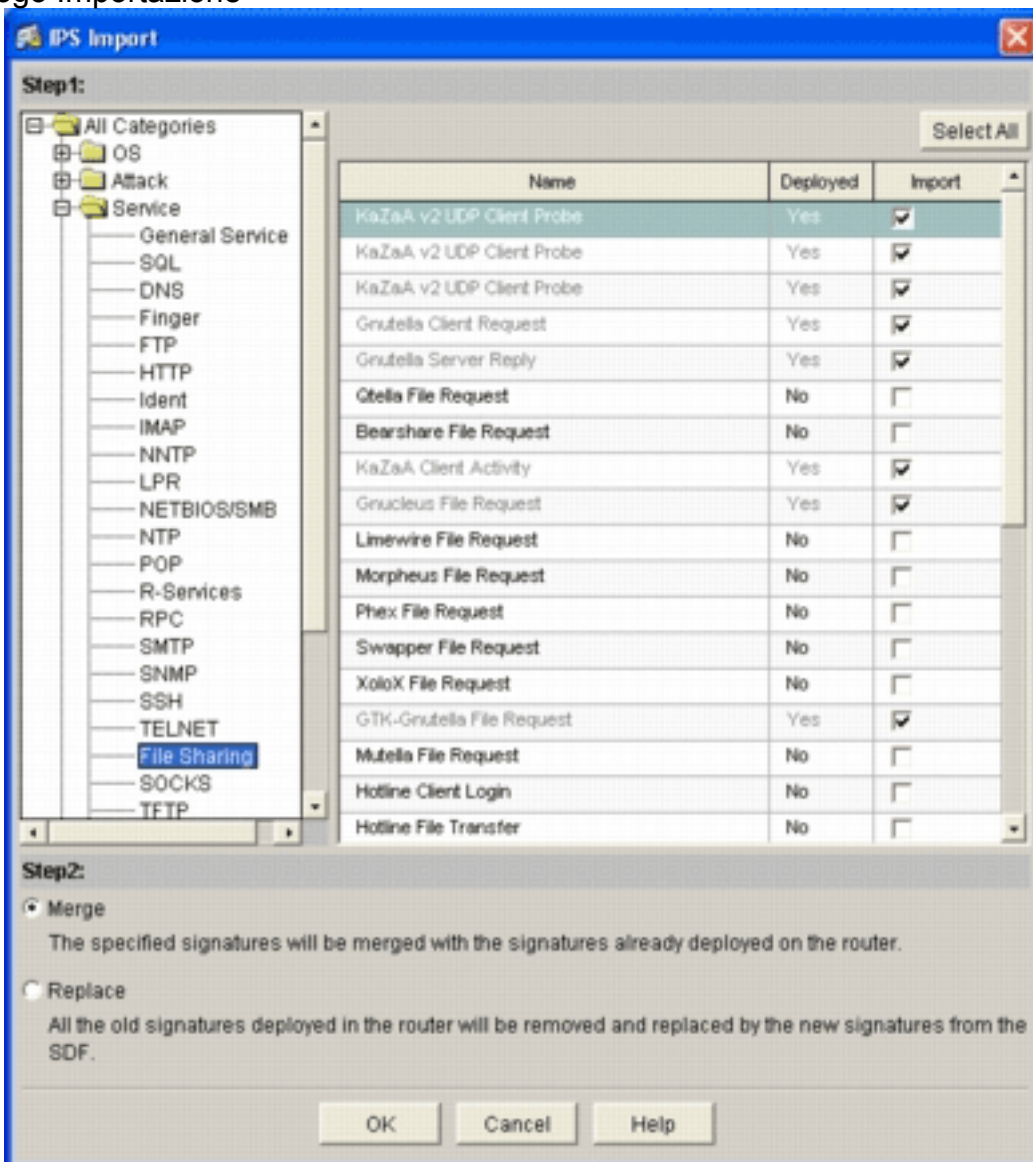


4. Selezionate **Dal PC (From PC)** dall'elenco a discesa Importa (Import).
5. Selezionare il file da cui si desidera importare le



firme. In questo esempio viene utilizzato l'ultimo aggiornamento scaricato da Cisco.com e salvato sul disco rigido del PC locale.

- Fare clic su **Apri.Avviso**: a causa dei vincoli di memoria, è possibile aggiungere solo un numero limitato di nuove firme alle firme già distribuite. Se vengono selezionate troppe firme, il router potrebbe non essere in grado di caricare tutte le nuove firme per mancanza di memoria. Al termine del caricamento del file della firma, verrà visualizzata la finestra di dialogo Importazione

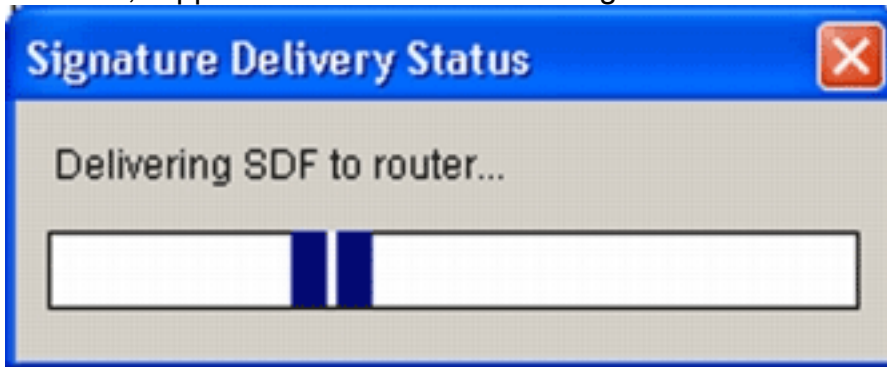


IPS.

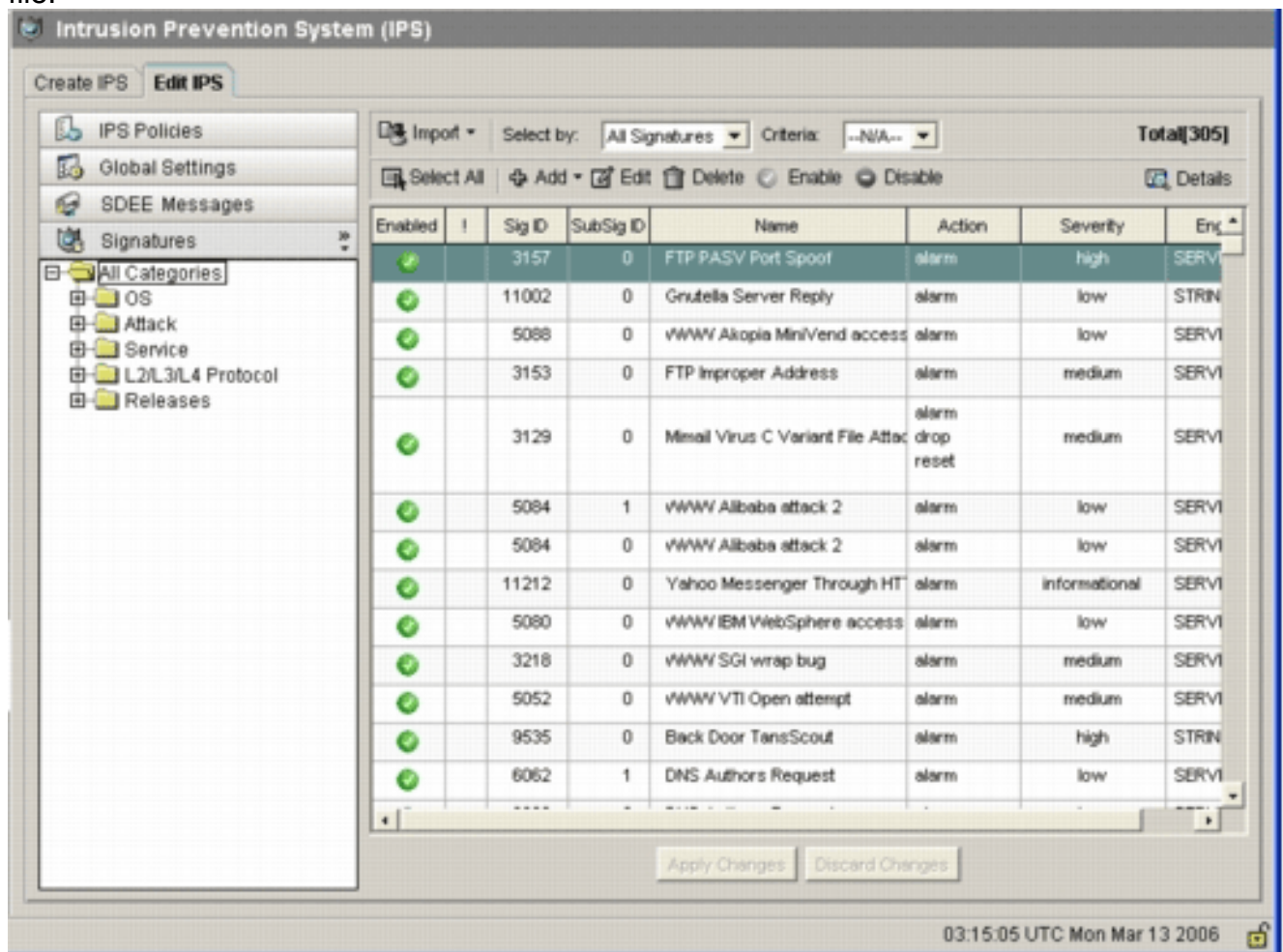
- Spostarsi nella struttura a sinistra e fare clic sulla casella di controllo **Importa** accanto alle firme che si desidera importare.
- Fare clic sul pulsante di opzione **Unisci** e quindi su **OK**. **Nota:** l'opzione Sostituisci sostituisce



la firma corrente impostata sul router con le firme selezionate per l'importazione. Dopo aver fatto clic su OK, l'applicazione Cisco SDM consegna le firme al



router. **Nota:** l'utilizzo elevato della CPU si verifica durante la compilazione e il caricamento delle firme. Dopo aver abilitato Cisco IOS IPS sull'interfaccia, il file della firma inizia a caricarsi. Il router impiega circa cinque minuti per caricare l'SDF. È possibile provare a utilizzare il comando **show process cpu** per visualizzare l'utilizzo della CPU dalla CLI del software Cisco IOS. Tuttavia, non tentare di utilizzare comandi aggiuntivi o di caricare altri SDF mentre il router sta caricando l'SDF. Il completamento del processo di compilazione della firma potrebbe richiedere più tempo (poiché l'utilizzo della CPU al momento del caricamento del file SDF è vicino al 100%). Potrebbe essere necessario scorrere l'elenco delle firme e attivarle se non sono *attivate*. Il numero totale di firme è aumentato a 519. Questo numero include tutte le firme disponibili nel file IOS-S193.zip che appartengono alla sottocategoria Condivisione file.



Per argomenti più avanzati su come utilizzare Cisco SDM per gestire la funzionalità IPS di Cisco IOS, consultare la documentazione Cisco SDM al seguente URL:

## Selezione di firme e utilizzo delle categorie di firme

Per determinare come selezionare in modo efficace le firme corrette per una rete, è necessario conoscere alcune informazioni sulla rete che si sta proteggendo. Le informazioni aggiornate sulla categoria della firma in Cisco SDM 2.2 e versioni successive consentono ai clienti di selezionare il set di firme corretto per proteggere la rete.

La categoria consente di raggruppare le firme. Consente di limitare la selezione delle firme a un sottoinsieme di firme rilevanti l'una per l'altra. Una firma può appartenere a una sola categoria o a più categorie.

Queste sono le cinque categorie principali:

- Sistema operativo: categorizzazione delle firme basata sul sistema operativo
- Attacco: categorizzazione delle firme basata su attacchi
- Servizio: categorizzazione delle firme basata sui servizi
- Protocollo di livello 2-4: categorizzazione delle firme basata su protocollo
- Releases: categorizzazione delle firme basata su release

Ciascuna di queste categorie è ulteriormente suddivisa in sottocategorie.

Ad esempio, si consideri una rete domestica con una connessione a banda larga a Internet e un tunnel VPN per la rete aziendale. Sul router a banda larga, Cisco IOS Firewall è abilitato sulla connessione aperta (non VPN) a Internet per impedire che qualsiasi connessione abbia origine da Internet e sia connessa alla rete domestica. È consentito tutto il traffico proveniente dalla rete domestica e diretto a Internet. Si supponga che l'utente utilizzi un PC basato su Windows e applicazioni quali HTTP (esplorazione del Web) e posta elettronica.

È possibile configurare il firewall in modo che solo le applicazioni necessarie all'utente possano passare attraverso il router. Ciò consente di controllare il flusso di traffico indesiderato e potenzialmente dannoso che può diffondersi nella rete. L'utente di casa non necessita di un servizio specifico o non lo utilizza. Se il servizio può passare attraverso il firewall, esiste un potenziale buco che un attacco può utilizzare per passare attraverso la rete. Le procedure ottimali consentono solo i servizi necessari. È ora più semplice selezionare le firme da attivare. È necessario attivare le firme solo per i servizi che consentono il passaggio attraverso il firewall. In questo esempio i servizi includono posta elettronica e HTTP. Cisco SDM semplifica questa configurazione.

Per utilizzare la categoria per selezionare le firme necessarie, scegliere **Servizio > HTTP** e abilitare tutte le firme. Questo processo di selezione funziona anche nella finestra di dialogo di importazione delle firme, in cui è possibile selezionare tutte le firme HTTP e importarle nel router.

Altre categorie da selezionare sono DNS, NETBIOS/SMB, HTTPS e SMTP.

## Aggiorna firme per file SDF predefiniti

I tre moduli SDF preconfigurati (attack-drop.dsfl, 128MB.sdf e 256MB.sdf) sono attualmente disponibili sul sito Cisco.com all'indirizzo <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup> (solo utenti [registrati](#)). Le versioni più recenti di questi file verranno pubblicate non appena disponibili. Per aggiornare i router che eseguono Cisco IOS IPS con questi SDF predefiniti, visitare il sito Web e scaricare le versioni più recenti di questi file.

## Procedura CLI

1. Copiare i file scaricati nella posizione da cui il router è configurato per caricare questi file. Per individuare la posizione corrente del router, usare il comando **show running-config | in ip ips sdf** nel comando **ip ips sdf**.

```
Router#show running-config | in ip ips sdf
ip ips sdf location flash://256MB.sdf autosave
```

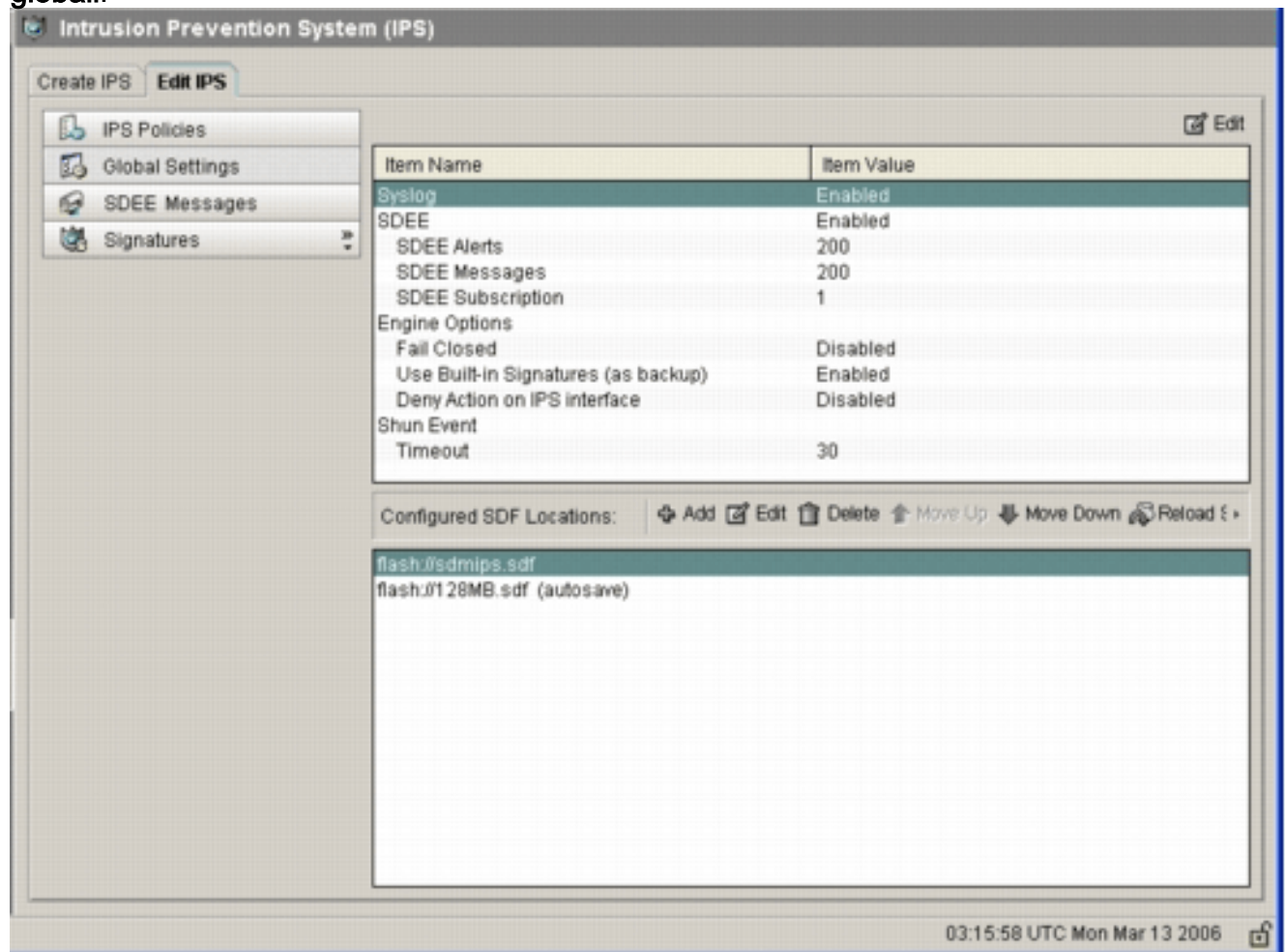
Nell'esempio, il router usa 256 MB.sdf sulla memoria flash. Il file viene aggiornato quando si copia il nuovo file scaricato da 256 MB.sdf sul router flash.

2. Ricaricare il sottosistema Cisco IOS IPS per eseguire i nuovi file. Per ricaricare l'IPS Cisco IOS, è possibile procedere in due modi: ricaricare il router o riconfigurare l'IPS Cisco IOS in modo che attivi il sottosistema IPS IOS per ricaricare le firme. Per riconfigurare l'IPS Cisco IOS, rimuovere tutte le regole IPS dalle interfacce configurate, quindi riapplicare le regole IPS alle interfacce. In questo modo, il sistema IPS Cisco IOS verrà ricaricato.

## Procedura SDM 2.2

Completare questa procedura per aggiornare gli SDF predefiniti sul router:

1. Fare clic su **Configura** e quindi su **Prevenzione intrusioni**.
2. Fare clic sulla scheda **Modifica IPS** e quindi su **Impostazioni globali**.



Item Name	Item Value
Syslog	Enabled
SDEE	Enabled
SDEE Alerts	200
SDEE Messages	200
SDEE Subscription	1
Engine Options	
Fail Closed	Disabled
Use Built-in Signatures (as backup)	Enabled
Deny Action on IPS interface	Disabled
Shun Event	
Timeout	30

Configured SDF Locations: Add Edit Delete Move Up Move Down Reload

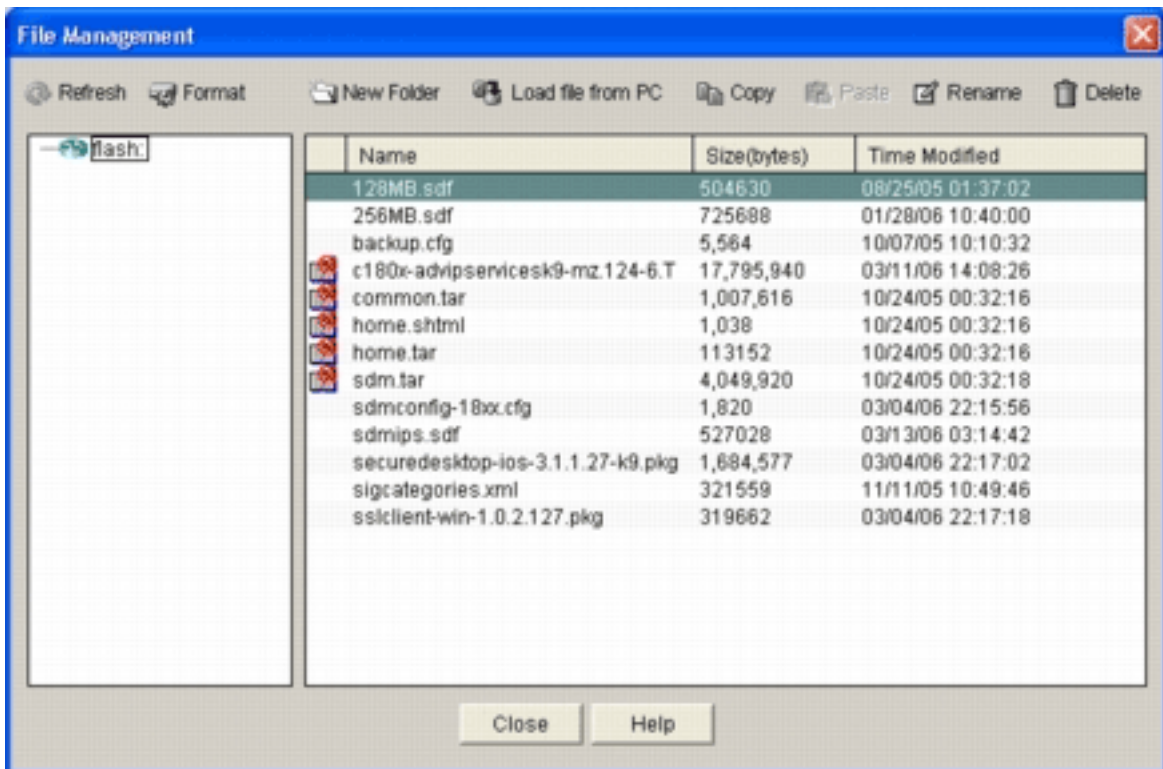
- flash://sdmips.sdf
- flash://128MB.sdf (autosave)

03:15:58 UTC Mon Mar 13 2006

Nella parte superiore dell'interfaccia utente vengono visualizzate le impostazioni globali.

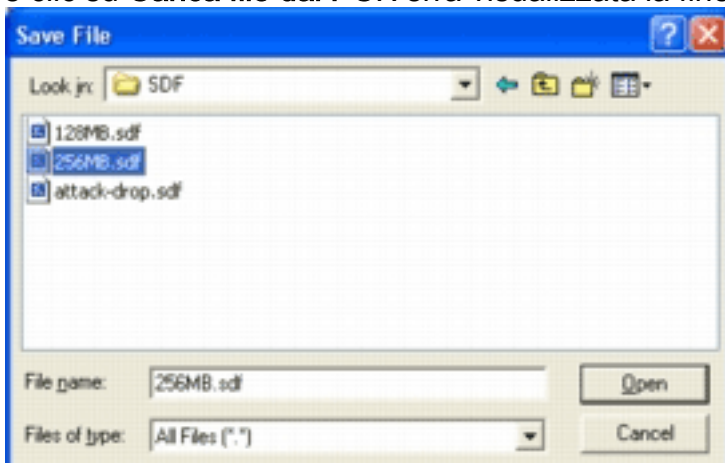
Nella metà inferiore dell'interfaccia utente vengono visualizzate le posizioni SDF attualmente configurate. In questo caso, è configurato il file 256MB.sdf dalla memoria flash.

3. Scegliere **Gestione file** dal menu File. Verrà visualizzata la finestra di dialogo Gestione



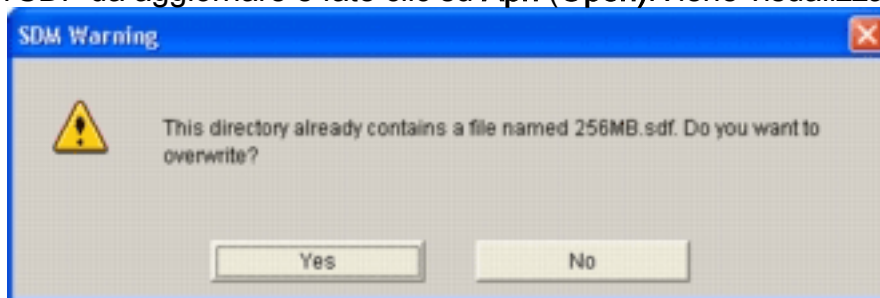
file.

4. Fare clic su **Carica file dal PC**. Verrà visualizzata la finestra di dialogo Salva



file.

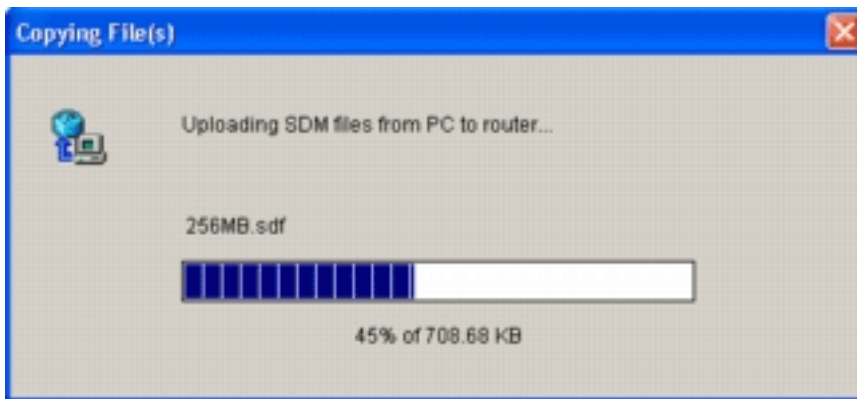
5. Selezionate l'SDF da aggiornare e fate clic su **Apri (Open)**. Viene visualizzato il messaggio di



avviso SDM.

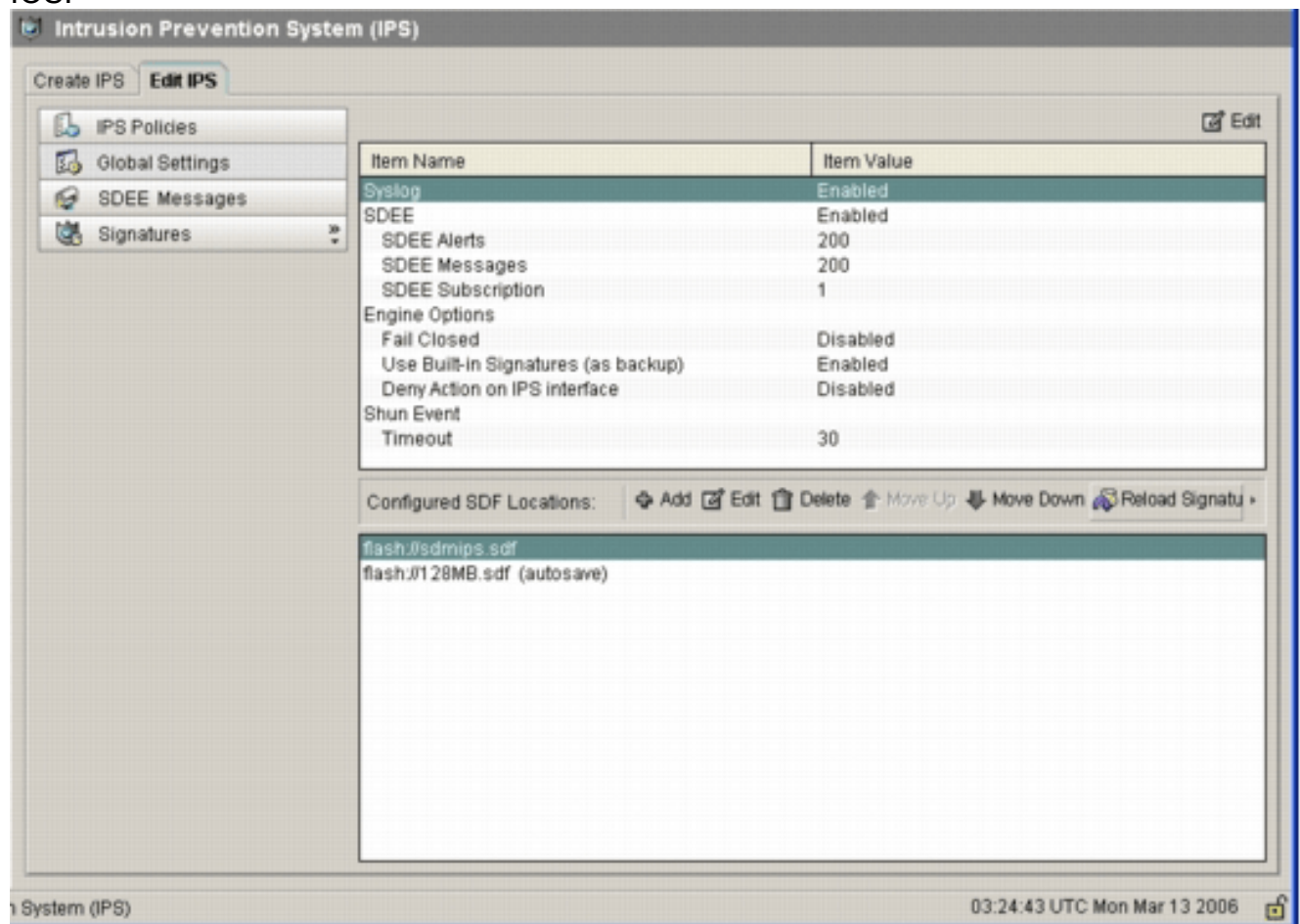
6. Per sostituire il file esistente, fare clic su **Sì**. Verrà visualizzata una finestra di dialogo con lo stato di avanzamento del processo di





caricamento.

7. Al termine del processo di caricamento, fare clic su **Ricarica firme** sulla barra degli strumenti della posizione SDF. Questa azione consente di ricaricare l'IPS Cisco IOS.



**Nota:** il pacchetto IOS-Sxxx.zip contiene tutte le firme supportate da Cisco IOS IPS. Gli aggiornamenti a questo pacchetto di firme sono pubblicati su Cisco.com non appena disponibili. Per aggiornare le firme contenute in questo pacchetto, vedere il [passaggio 2](#).

## [Informazioni correlate](#)

- [Cisco Intrusion Prevention System](#)
- [Avvisi sui prodotti per la sicurezza \(incluso Cisco Secure Intrusion Detection\)](#)
- [Supporto tecnico – Cisco Systems](#)