Konfigurationsbeispiel für Router und Security Device Manager (SDM) und Cisco IOS CLI im Cisco IOS Intrusion Prevention System (IPS)

Inhalt

Einleitung

Im Cisco Router and Security Device Manager (SDM) 2.2 ist die Cisco IOS® IPS-Konfiguration in die SDM-Anwendung integriert. Zum Konfigurieren von Cisco IOS IPS müssen Sie kein separates Fenster mehr öffnen.

In Cisco SDM 2.2 führt Sie ein neuer IPS-Konfigurationsassistent durch die erforderlichen Schritte zur Aktivierung von Cisco IOS IPS auf dem Router. Darüber hinaus können Sie die erweiterten Konfigurationsoptionen weiterhin verwenden, um Cisco IOS IPS mit Cisco SDM 2.2 zu aktivieren, zu deaktivieren und anzupassen.

Cisco empfiehlt, Cisco IOS IPS mit den vordefinierten Signaturdefinitionsdateien (SDFs) auszuführen: attack-drop.sdf, 128 MB.sdf und 256 MB.sdf. Diese Dateien werden für Router mit unterschiedlichem Arbeitsspeicher erstellt. Die Dateien werden mit Cisco SDM gebündelt, das bei der ersten Aktivierung von Cisco IOS IPS auf einem Router SDFs empfiehlt. Diese Dateien können auch unter http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup heruntergeladen werden (nur registrierte Kunden).

Die Vorgehensweise zum Aktivieren der Standard-SDFs ist in Enable Cisco IOS IPS with a Factory Default SDF detailliert. Wenn die Standard-SDFs nicht ausreichen oder Sie neue Signaturen hinzufügen möchten, können Sie die unter Zusätzliche Signaturen anhängen beschriebene Prozedur verwenden, nachdem Sie Default SDF aktiviert haben.

Voraussetzungen

Anforderungen

Java Runtime Environment (JRE) Version 1.4.2 oder höher ist für die Verwendung von Cisco SDM 2.2 erforderlich. Eine von Cisco empfohlene und angepasste Signaturdatei (basierend auf DRAM) ist im Lieferumfang von Cisco SDM enthalten (im Flash-Speicher des Routers mit Cisco SDM geladen).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Router and Security Device Manager (SDM) 2.2.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Cisco IOS IPS mit einem werkseitigen Standard-SDF aktivieren

CLI-Verfahren

Führen Sie dieses Verfahren aus, um mithilfe der CLI einen Cisco Router der Serie 1800 mit Cisco IOS IPS so zu konfigurieren, dass er 128 MB.sdf auf den Router-Flash lädt.

1. Konfigurieren Sie den Router so, dass die SDEE-Ereignisbenachrichtigung (Security Device Event Exchange) aktiviert wird.
   ```
   yourname#conf t
   ```

2. Geben Sie die Konfigurationsbefehle ein (eine pro Zeile), und drücken Sie dann Strg+Z, um das Dialogfeld zu beenden.
   ```
   yourname(config)#ip ips notify sdee
   ```

3. Erstellen Sie einen IPS-Regelnamen, der für die Zuordnung zu Schnittstellen verwendet wird.
   ```
   yourname(config)#ip ips name myips
   ```

4. Konfigurieren Sie einen IPS-Standortbefehl, um festzulegen, aus welcher Datei das Cisco IOS IPS-System Signaturen liest.In diesem Beispiel wird die Datei im Flash-Speicher verwendet: 128 MB.sdf. Der URL-Teil dieses Befehls kann eine beliebige gültige URL sein, die Flash, Datenträger oder Protokolle über FTP, HTTP, HTTPS, RTP, SCP und TFTP verwendet, um auf die Dateien zu zeigen.
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

Hinweis: Sie müssen den **Terminal-Monitor-**Befehl aktivieren, wenn Sie den Router über eine Telnet-Sitzung konfigurieren. Andernfalls werden die SDEE-Meldungen nicht angezeigt, wenn die Signatur-Engine erstellt wird.

5. Aktivieren Sie IPS auf der Schnittstelle, auf der das Cisco IOS IPS den Datenverkehr scannen soll. In diesem Fall aktivierten wir in beiden Richtungen FastEthernet 0 für die Schnittstelle.

```
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
```

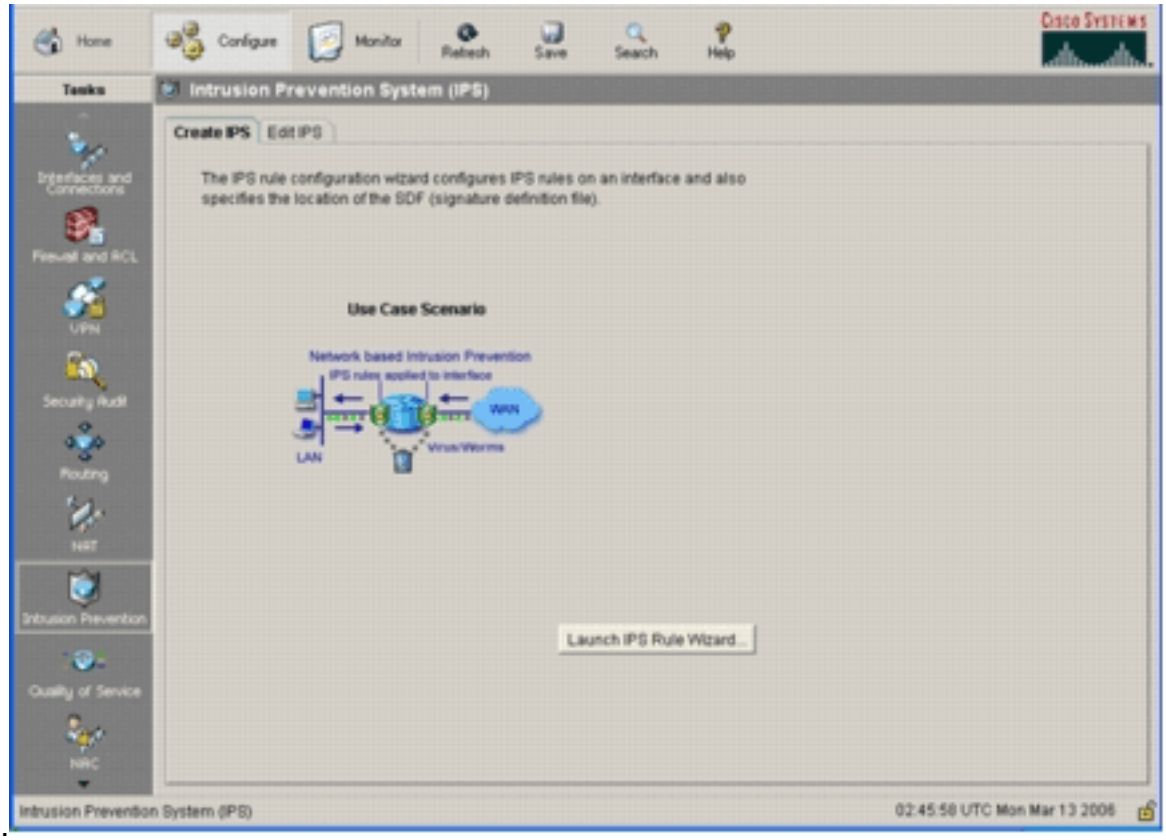
Wenn eine IPS-Regel erstmals auf eine Schnittstelle angewendet wird, startet Cisco IOS IPS Buildsignaturen aus der Datei, die durch den Befehl SDF location angegeben wird. SDEE-Meldungen werden an der Konsole protokolliert und, falls konfiguriert, an den Syslog-Server gesendet. Die SDEE-Meldungen mit <*number*> von <*number*> Engines geben den Signaturmodulerstellungsprozess an. Wenn die beiden Zahlen übereinstimmen, werden alle Engines gebaut.**Hinweis:** Die virtuelle IP-Reassemblierung ist eine Schnittstellenfunktion, die bei Aktivierung fragmentierte Pakete, die über diese Schnittstelle in den Router gelangen, automatisch neu zusammensetzt. Cisco empfiehlt, die IP-virtuelle Assembly auf allen Schnittstellen zu aktivieren, auf denen der Datenverkehr in den Router eingeht. Im obigen Beispiel wird neben der Aktivierung der "ip virtual-assembly" für interface fastEthernet 0 auch für die interne Schnittstelle VLAN 1 konfiguriert.

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

SDM 2.2 - Verfahren

Führen Sie dieses Verfahren aus, um mit Cisco SDM 2.2 einen Cisco Router der Serie 1800 mit Cisco IOS IPS zu konfigurieren.

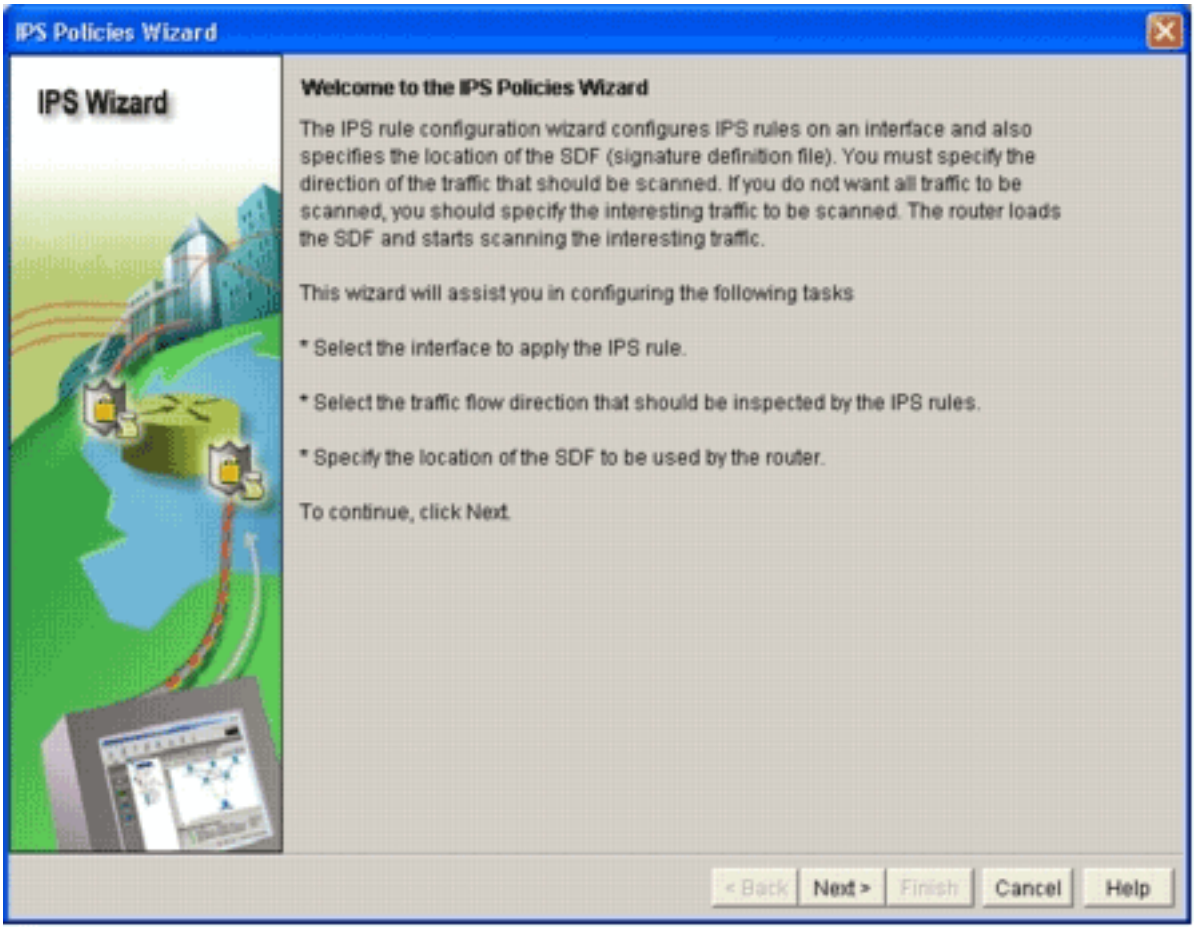
1. Klicken Sie in der SDM-Anwendung auf **Konfigurieren** und dann auf **Intrusion**



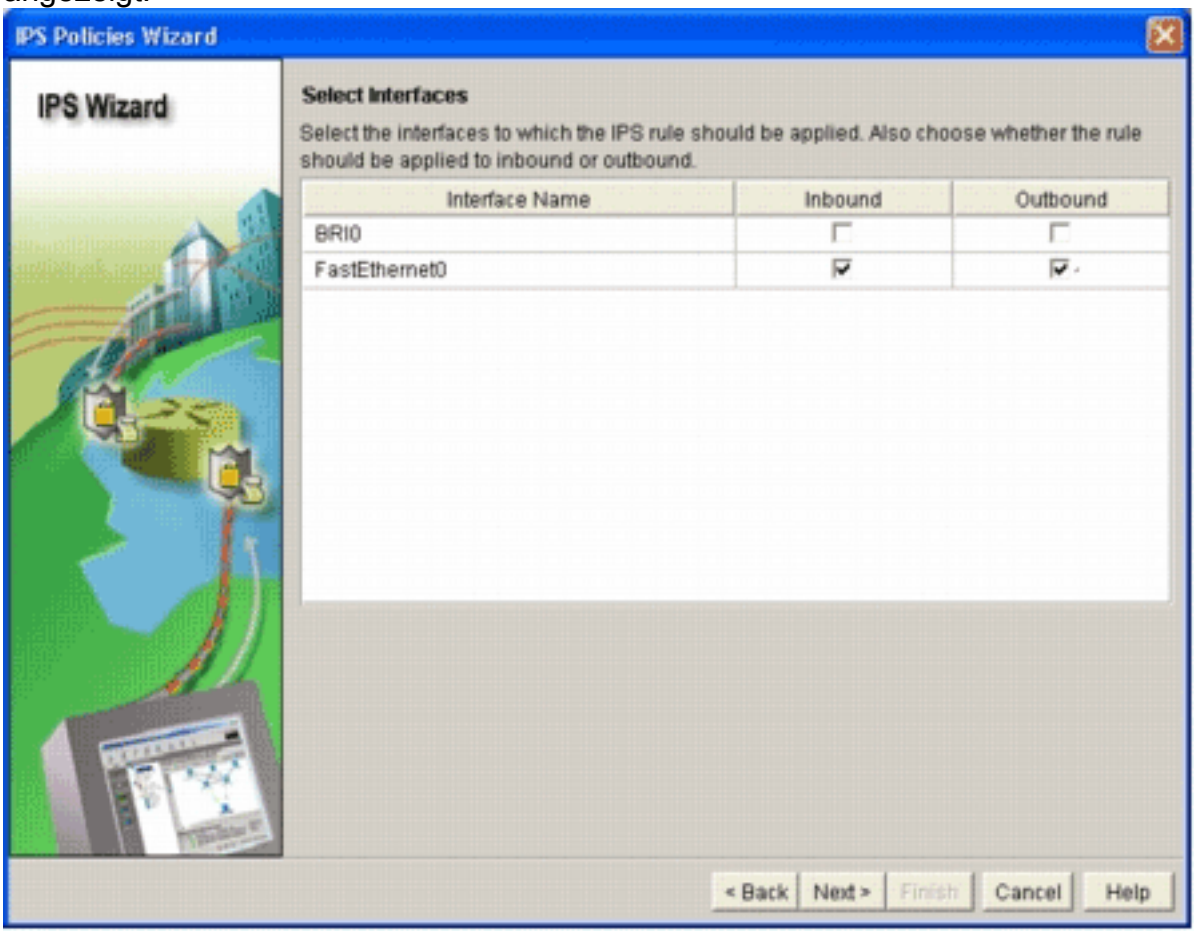
Prevention.

2. Klicken Sie auf die Registerkarte **Create IPS (IPS erstellen)** und anschließend auf **Launch IPS Rule Wizard (IPS-Regelassistent starten)**.Cisco SDM erfordert eine IPS-Ereignisbenachrichtigung über SDEE, um die Cisco IOS IPS-Funktion zu konfigurieren. Standardmäßig ist die SDEE-Benachrichtigung nicht aktiviert. Das Cisco SDM fordert Sie auf, die IPS-Ereignisbenachrichtigung über SDEE zu aktivieren, wie in diesem Bild gezeigt:

3. Klicken Sie auf **OK**.Das Fenster Welcome to the IPS Policies Wizard (Willkommen beim IPS-Richtlinienassistenten) des Dialogfelds IPS Policies Wizard (IPS-Richtlinienassistent) wird angezeigt.



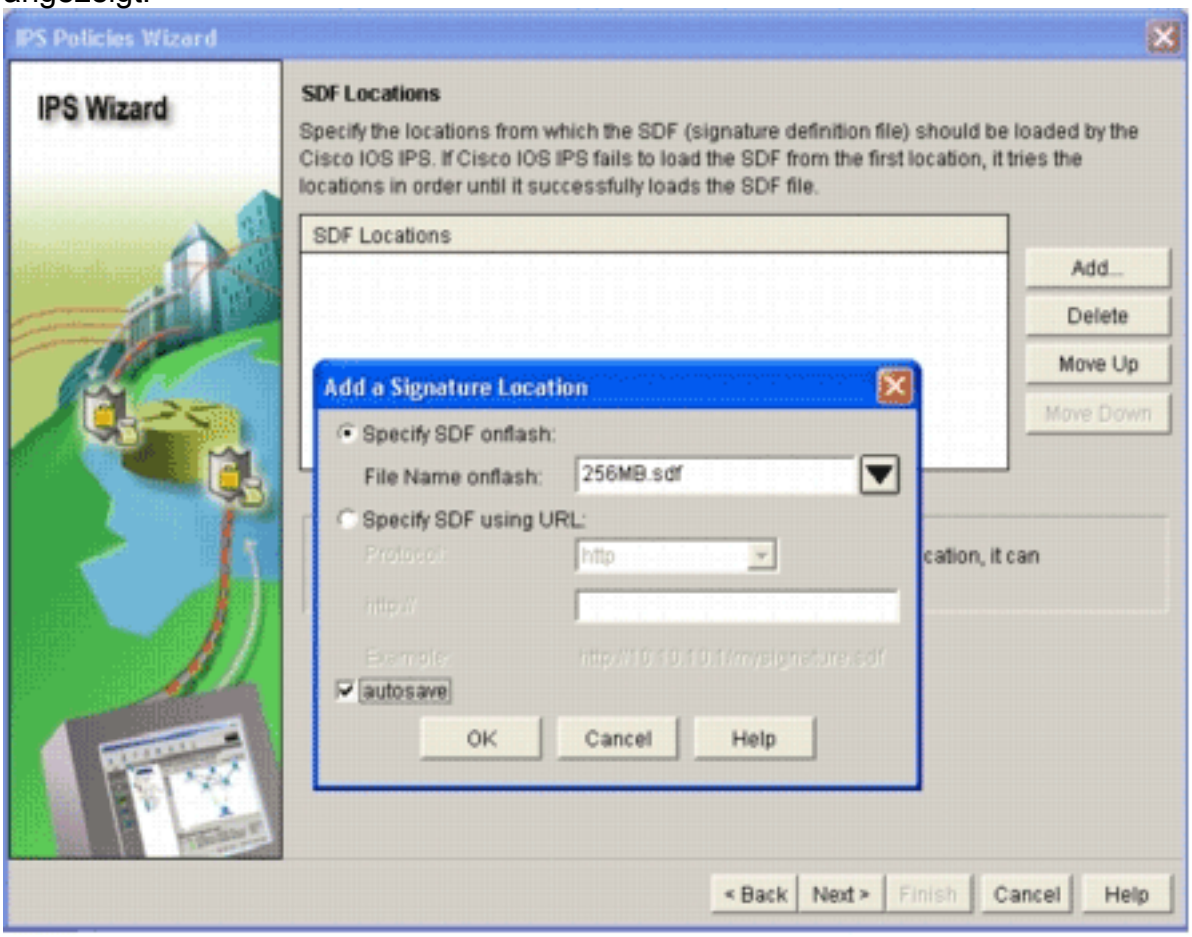
4. Klicken Sie auf **Weiter**.Das Fenster Schnittstellen auswählen wird angezeigt.



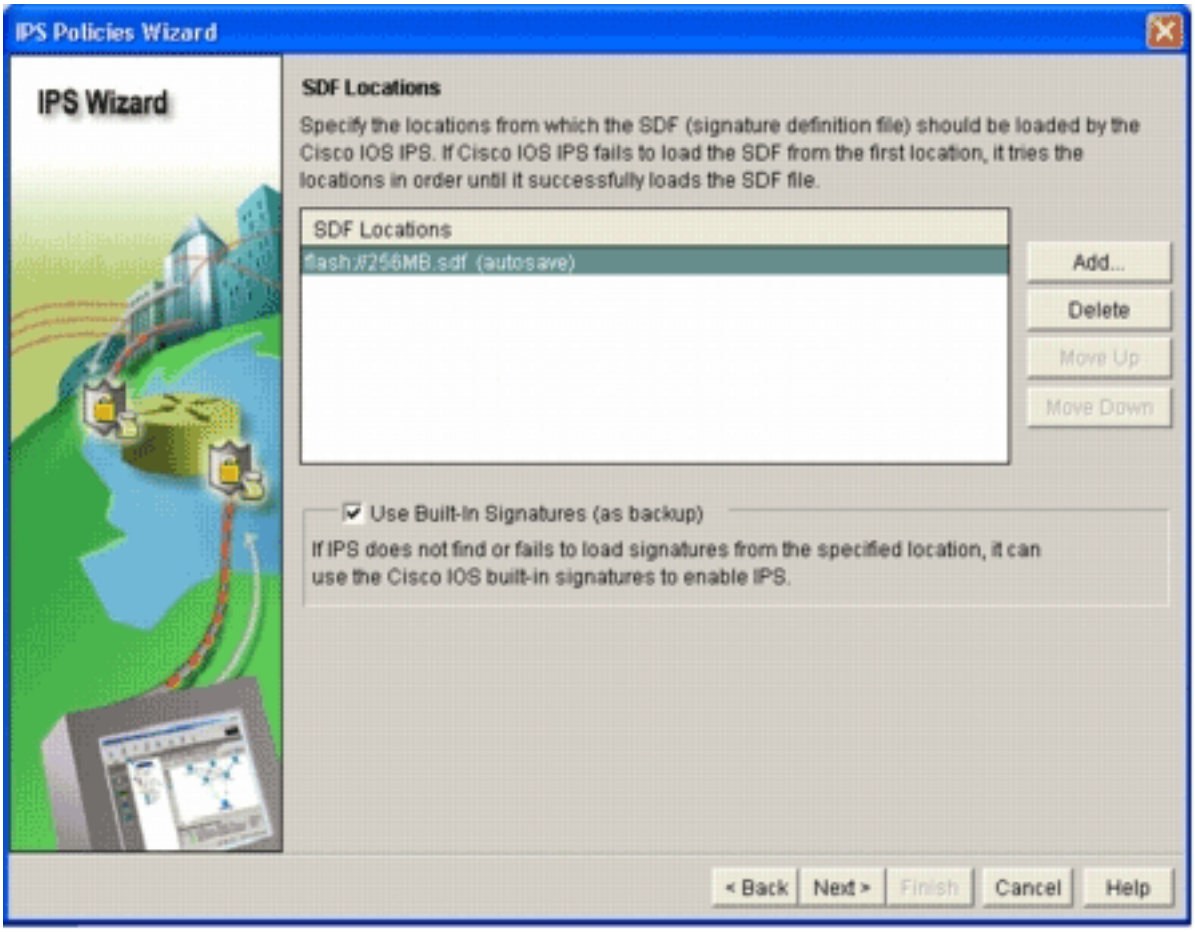
5. Wählen Sie die Schnittstellen aus, für die IPS aktiviert werden soll, und klicken Sie entweder auf das Kontrollkästchen **Eingehend** oder **Ausgehend**, um die Richtung dieser Schnittstelle

anzugeben.**Hinweis:** Wenn Sie IPS auf einer Schnittstelle aktivieren, empfiehlt Cisco, sowohl eingehende als auch ausgehende Anweisungen zu aktivieren.

6. Klicken Sie auf **Weiter**.Das Fenster SDF Locations (SDF-Speicherorte) wird angezeigt.
7. Klicken Sie auf **Hinzufügen**, um einen SDF-Speicherort zu konfigurieren.Das Dialogfeld Speicherort für Signaturen hinzufügen wird angezeigt.

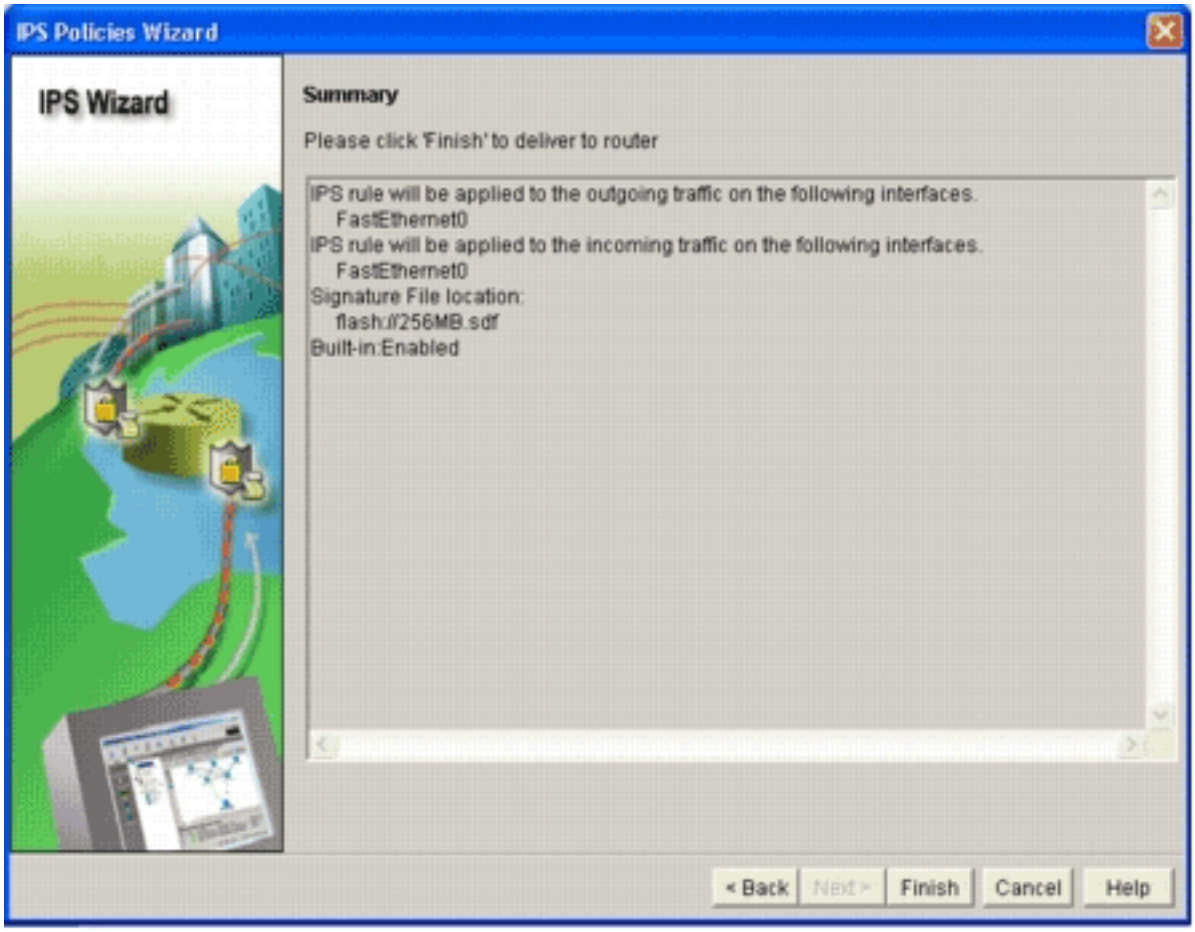


8. Klicken Sie auf das Optionsfeld **SDF im Flash-Speicher angeben**, und wählen Sie in der Dropdown-Liste **Dateiname im Flash-**Speicher die Option 256MB.sdf aus.
9. Aktivieren Sie das Kontrollkästchen **Autosave**, und klicken Sie auf **OK**.**Hinweis:** Bei einer Signaturänderung wird die Signaturdatei automatisch durch die Option autosave gespeichert.Im Fenster SDF Locations (SDF-Standorte) wird der neue SDF-Speicherort angezeigt.

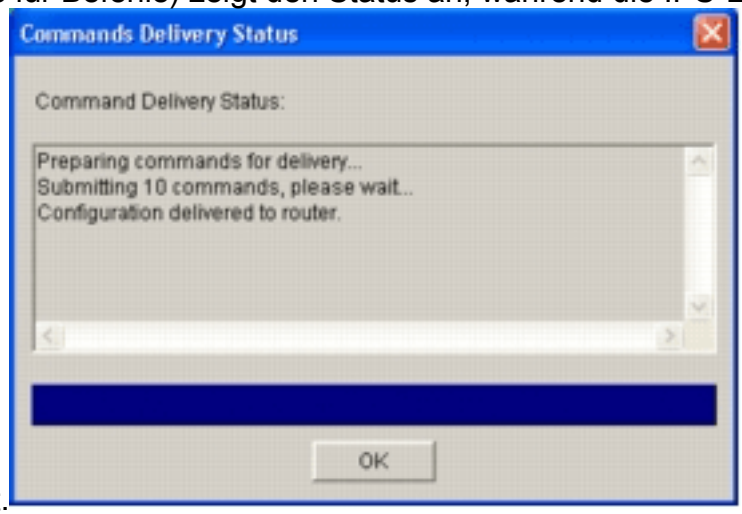


Hinweis: Sie können zusätzliche Signaturstandorte hinzufügen, um eine Sicherung festzulegen.

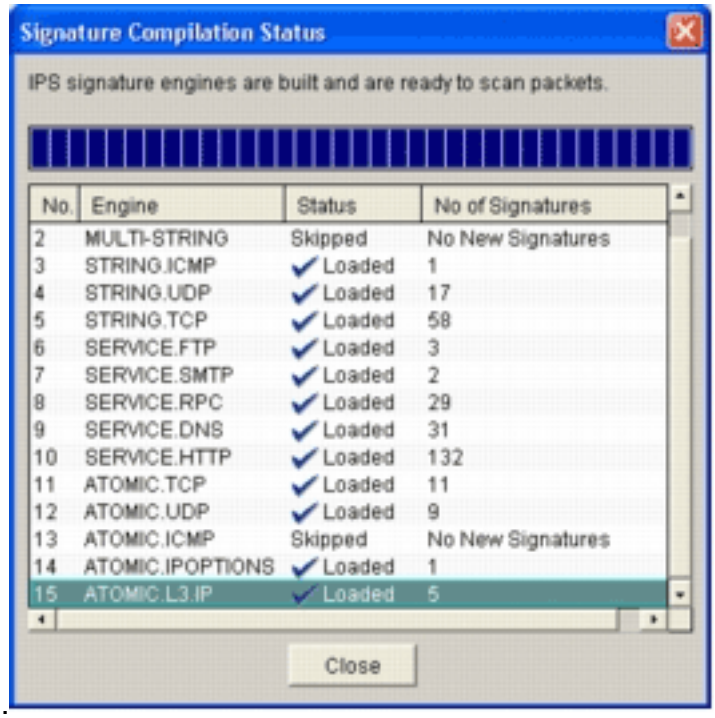
10. Klicken Sie auf das Kontrollkästchen **Integrierte Signaturen (als Backup verwenden)**.**Hinweis:** Cisco empfiehlt, die Option für die integrierte Signatur nur zu verwenden, wenn Sie einen oder mehrere Speicherort angegeben haben.
11. Klicken Sie auf **Weiter**, um fortzufahren.Das Fenster Zusammenfassung wird angezeigt.



12. Klicken Sie auf **Fertig stellen**.Das Dialogfeld "Commands Delivery Status" (Bereitstellungsstatus für Befehle) zeigt den Status an, während die IPS-Engine alle Signaturen kompiliert.

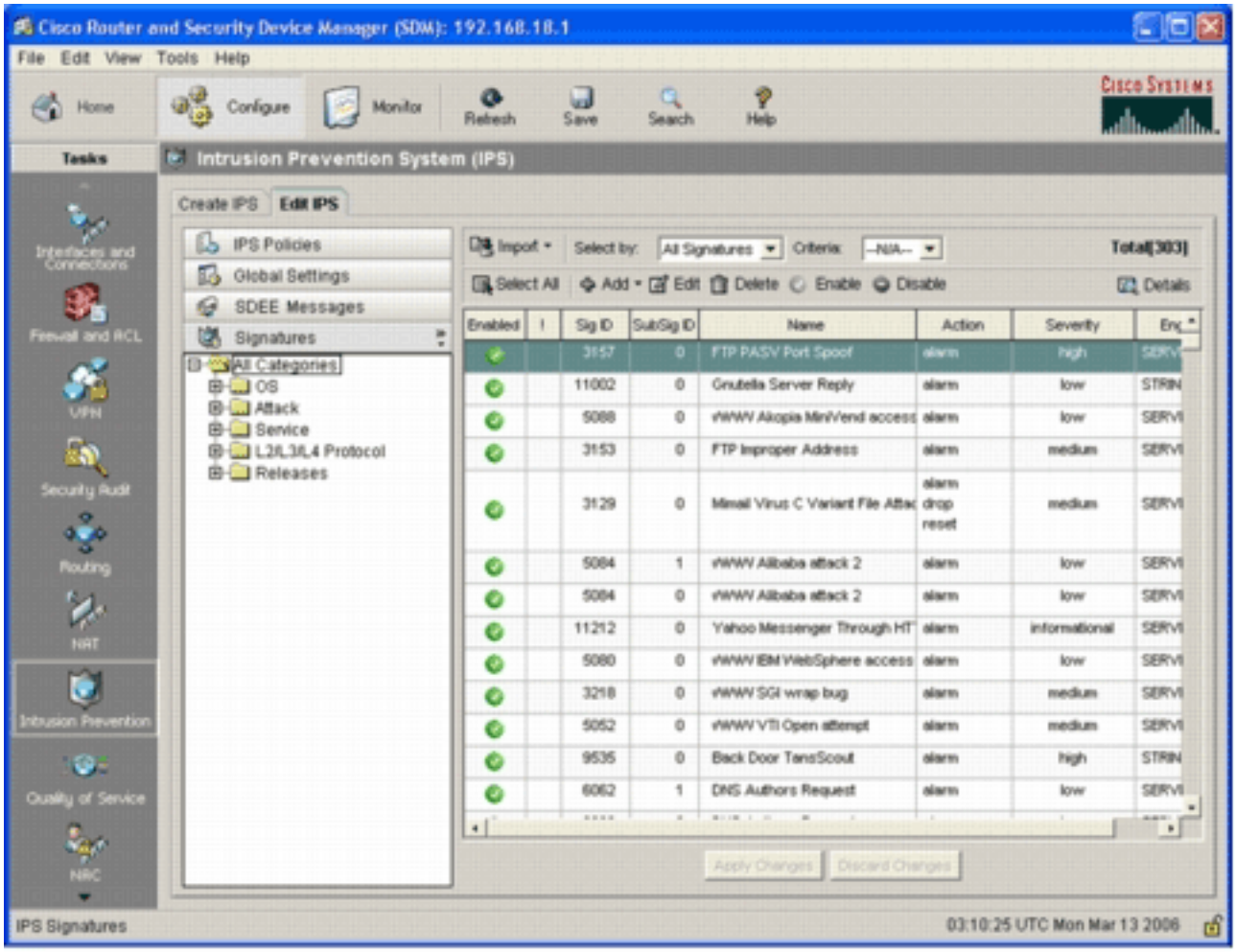


13. Klicken Sie nach Abschluss des Vorgangs auf **OK**.Das Dialogfeld Signaturkompilierungsstatus zeigt die Informationen zur Signaturkompilierung



an. Diese Informationen zeigen, welche Engines kompiliert wurden und wie viele Signaturen in diesem Modul vorhanden sind. Bei Engines, die in der Statusspalte *Übersprungen* anzeigen, wird für diese Engine keine Signatur geladen.

14. Klicken Sie auf **Schließen**, um das Dialogfeld Signaturerstellungsstatus zu schließen.
15. Um zu überprüfen, welche Signaturen derzeit auf dem Router geladen sind, klicken Sie auf **Konfigurieren**, und klicken Sie dann auf **Intrusion Prevention**.
16. Klicken Sie auf die Registerkarte **Edit IPS (IPS bearbeiten)** und anschließend auf **Signaturen**.Die Liste der IPS-Signaturen wird im Fenster Signaturen angezeigt.



Hinzufügen weiterer Signaturen nach Aktivieren von Standard-SDF

CLI-Verfahren

Es ist kein CLI-Befehl zum Erstellen von Signaturen oder Lesen von Signaturinformationen aus der verteilten Datei IOS-Sxxx.zip verfügbar. Cisco empfiehlt, die Signaturen auf Cisco IOS IPS-Systemen entweder mit SDM oder dem Management Center für IPS-Sensoren zu verwalten.

Für Kunden, die bereits über eine Signaturdatei verfügen und diese Datei mit dem SDF zusammenführen möchten, das auf einem Cisco IOS IPS-System ausgeführt wird, können Sie den folgenden Befehl verwenden:

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

Die Signaturdatei, die durch den Signaturspeicherbefehl definiert wird, ist der Ort, an dem der Router Signaturdateien lädt, wenn er neu geladen wird oder das IOS IPS des Routers neu konfiguriert wird. Damit der Zusammenführungsprozess erfolgreich verläuft, muss auch die mit dem Befehl zum Speicherort der Signaturdatei definierte Datei aktualisiert werden.

1. Verwenden Sie den Befehl **show**, um die aktuell konfigurierten Signaturspeicherorte zu überprüfen.Die Ausgabe zeigt die konfigurierten Signaturstandorte an. Dieser Befehl zeigt an, von wo aus die aktuellen Signaturen geladen werden.
   ```
   yourname#show ip ips signatures
   Builtin signatures are configured
   ```

Signaturen wurden zuletzt vom Flash geladen:128 MB.sdfCisco SDF Version S128.0Trend SDF Version V0.0

2. Verwenden Sie den Befehl **copy <*url*> ips-sdf** zusammen mit den Informationen aus dem vorherigen Schritt, um Signaturdateien zusammenzuführen.

```
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#
```

Nachdem Sie den Befehl **copy** ausgegeben haben, lädt der Router die Signaturdatei in den Speicher und erstellt dann die Signaturmodule. In der Konsolen-SDEE-Nachrichtenausgabe wird der Gebäudestatus für jedes Signaturmodul angezeigt.%IPS-6-ENGINE_BUILD_SKIPPED gibt an, dass keine neuen Signaturen für diese Engine vorhanden sind.%IPS-6-ENGINE_READY gibt an, dass neue Signaturen vorliegen und die Engine bereit ist. Wie zuvor zeigt die Meldung "15 von 15 Engines" an, dass alle Engines gebaut wurden.IPS-7-UNSUPPORTED_PARAM gibt an, dass ein bestimmter Parameter von Cisco IOS IPS nicht unterstützt wird. Beispielsweise CapturePacket und ResetAfterIdle.**Hinweis:** Diese Meldungen dienen nur zu Informationszwecken und haben keine Auswirkungen auf die Funktion oder Leistung der Cisco IOS IPS-Signatur. Diese Protokollierungsmeldungen können deaktiviert werden, indem die Protokollierungsebene höher als beim Debuggen (Stufe 7) eingestellt wird.

3. Aktualisieren Sie das mit dem Befehl für den Signaturspeicherort definierte SDF, sodass beim Neuladen des Routers der zusammengeführte Signatursatz mit aktualisierten Signaturen enthalten ist. Dieses Beispiel zeigt den Unterschied in der Dateigröße, nachdem die zusammengeführte Signatur in der Flash-Datei 128 MB.sdf gespeichert wurde.

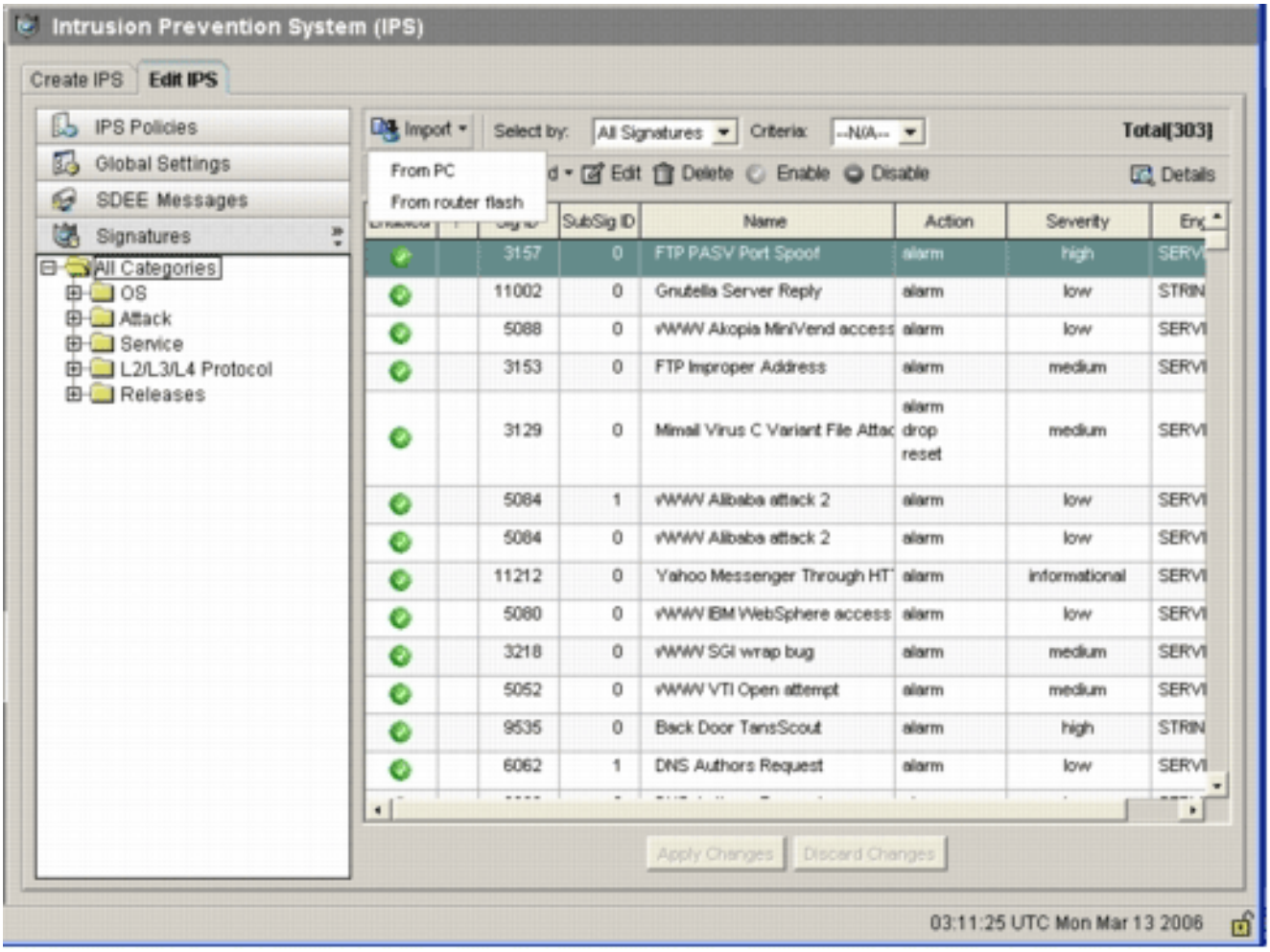
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

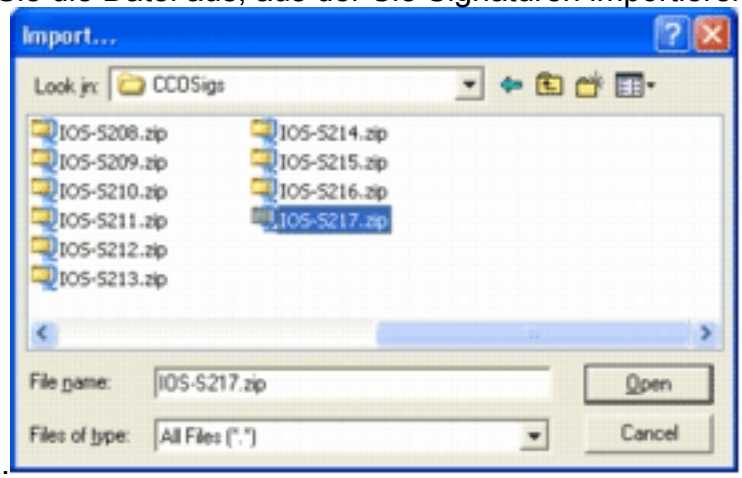
Warnung: Die neue 128MB.sdf enthält nun Signaturen, die vom Kunden zusammengeführt wurden. Der Inhalt unterscheidet sich von der Standarddatei Cisco 128 MB.sdf. Cisco empfiehlt, diese Datei in einen anderen Namen zu ändern, um Verwirrung zu vermeiden. Wenn der Name geändert wird, muss auch der Befehl für den Speicherort der Signatur geändert werden.

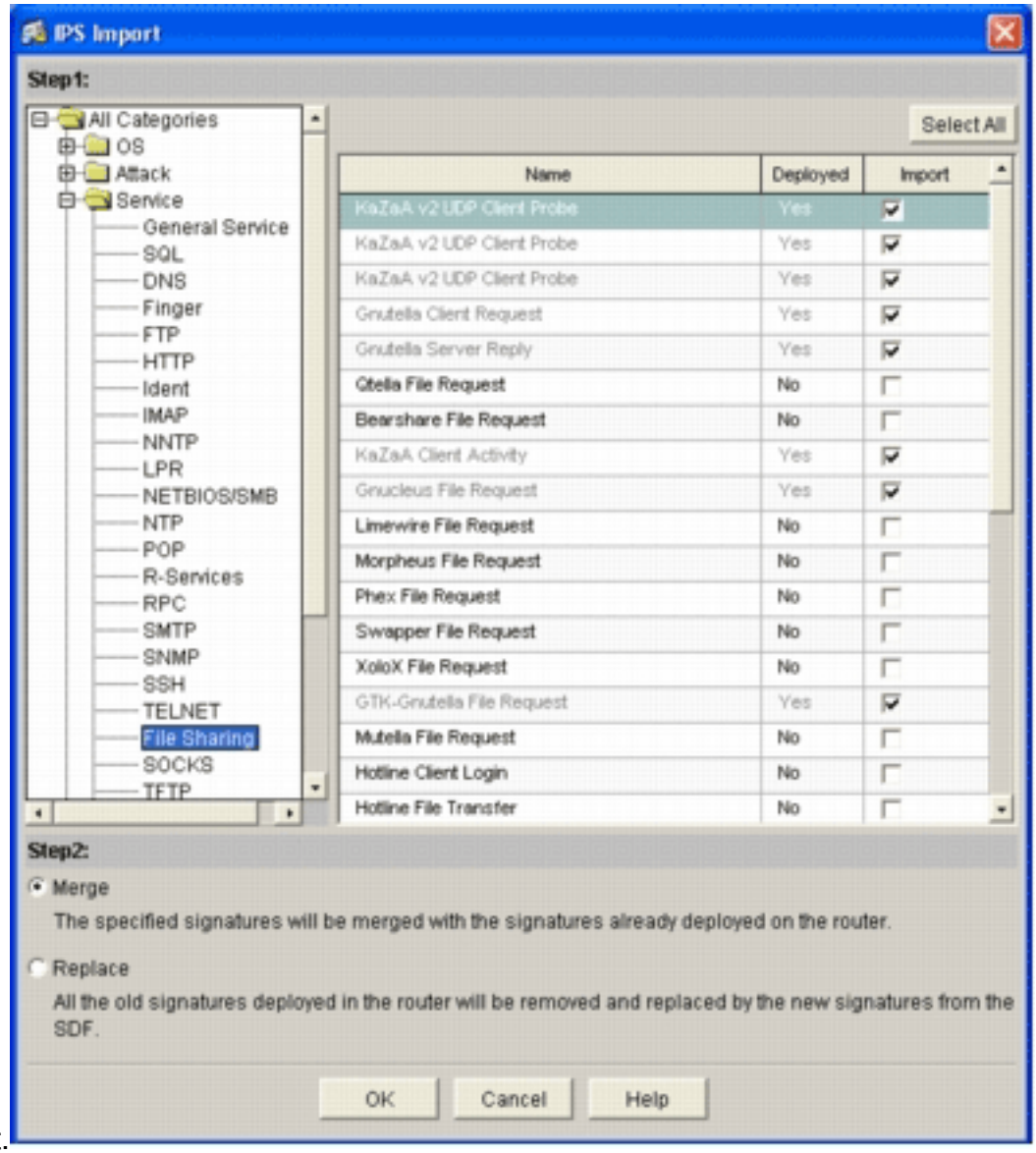
SDM 2.2 - Verfahren

Nachdem Cisco IOS IPS aktiviert wurde, können dem Router, der mit der Cisco SDM-Importfunktion einen Signaturensatz ausführt, neue Signaturen hinzugefügt werden. Gehen Sie wie folgt vor, um neue Signaturen zu importieren:

1. Wählen Sie die Standard-SDFs oder die IOS-Sxxx.zip-Aktualisierungsdatei, um zusätzliche Signaturen zu importieren.
2. Klicken Sie auf **Konfigurieren** und dann auf **Intrusion Prevention**.
3. Klicken Sie auf die Registerkarte **Edit IPS (IPS bearbeiten)** und anschließend auf **Importieren**.

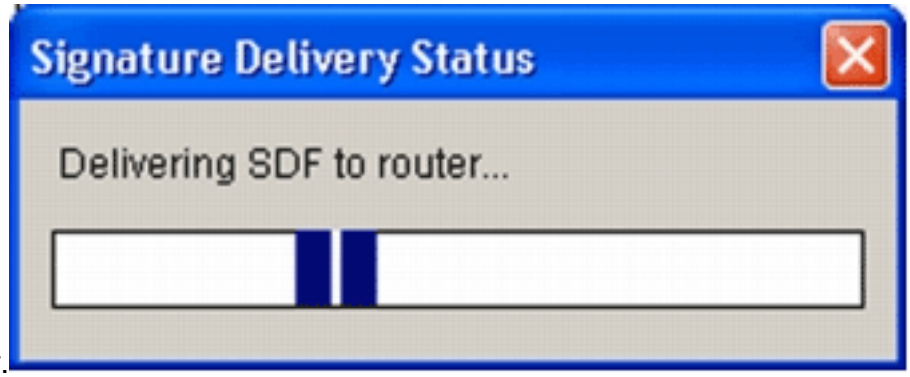


4. Wählen Sie **Aus PC** aus der Dropdown-Liste Importieren aus.
5. Wählen Sie die Datei aus, aus der Sie Signaturen importieren möchten. 
In diesem Beispiel wird die neueste von Cisco.com heruntergeladene und auf der lokalen PC-Festplatte gespeicherte Aktualisierung verwendet.
6. Klicken Sie auf **Öffnen**.**Warnung:** Aufgrund von Speicherbeschränkungen können nur eine begrenzte Anzahl neuer Signaturen zusätzlich zu bereits bereitgestellten Signaturen hinzugefügt werden. Wenn zu viele Signaturen ausgewählt wurden, kann der Router möglicherweise nicht alle neuen Signaturen laden, da kein Speicher zur Verfügung steht.Nach Abschluss des Ladevorgangs der Signaturdatei wird das Dialogfeld IPS-Import



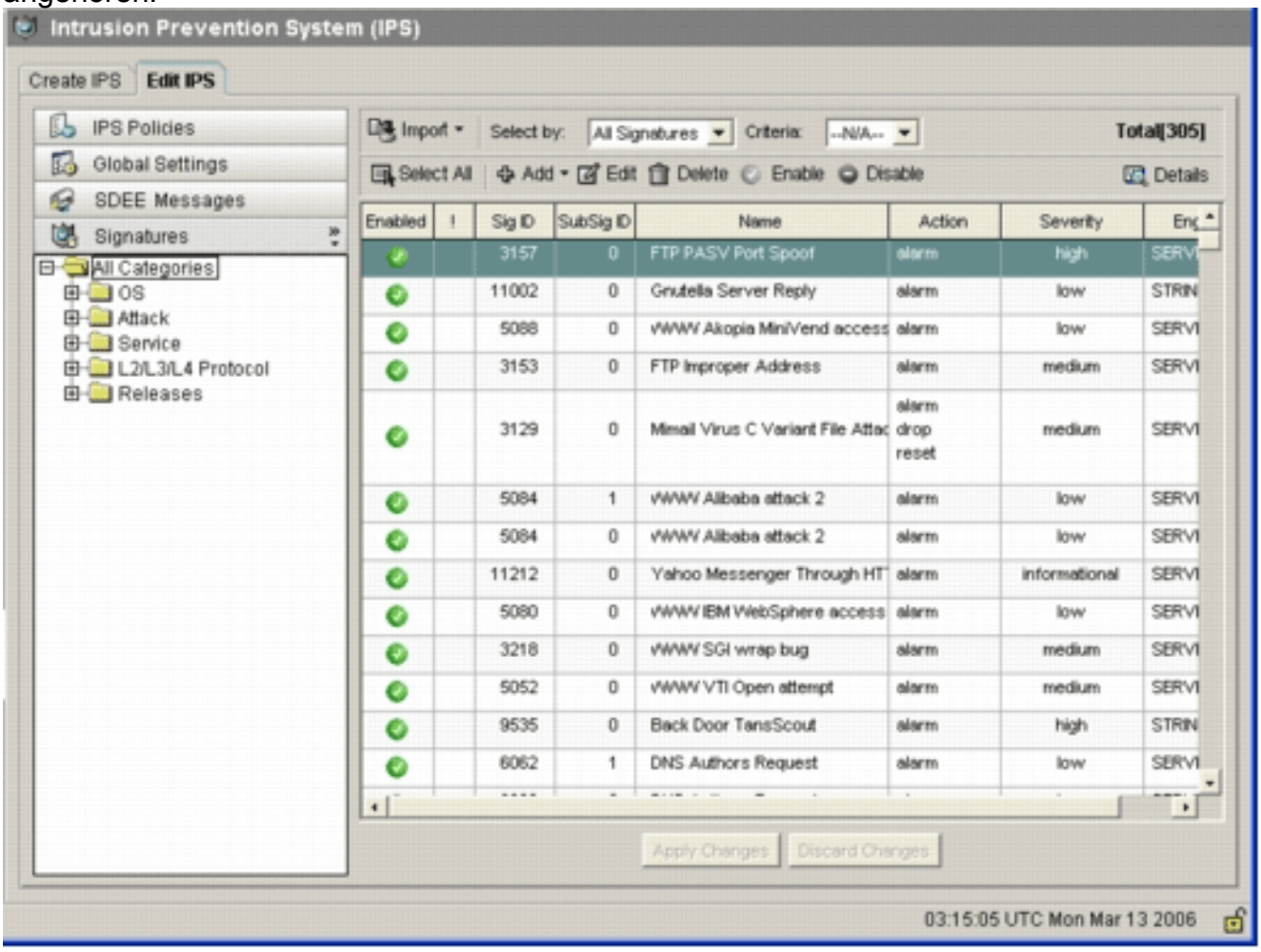
angezeigt.

7. Navigieren Sie durch die linke Strukturansicht, und klicken Sie auf das Kontrollkästchen **Importieren** neben den Signaturen, die Sie importieren möchten.
8. Klicken Sie auf das Optionsfeld **Zusammenführen** und anschließend auf **OK**.**Hinweis:** Die Option Ersetzen ersetzt den aktuellen Signatursatz auf dem Router durch die Signaturen, die Sie importieren möchten.Sobald Sie auf OK klicken, übergibt die Cisco SDM-Anwendung die Signaturen an den



Router.**Hinweis:** Beim Kompilieren und Laden von Signaturen wird eine hohe CPU-Auslastung festgestellt. Nachdem Cisco IOS IPS auf der Schnittstelle aktiviert wurde, wird die Signaturdatei geladen. Der Router benötigt etwa fünf Minuten, um das SDF zu laden. Sie können den Befehl **show process cpu** verwenden, um die CPU-Auslastung in der CLI der Cisco IOS Software anzuzeigen. Versuchen Sie jedoch nicht, zusätzliche Befehle zu verwenden oder andere SDFs zu laden, während der Router das SDF lädt. Dies kann dazu führen, dass die

Erstellung der Signatur länger dauert (da die CPU-Auslastung zum Zeitpunkt des Ladevorgangs fast 100 Prozent beträgt). Möglicherweise müssen Sie die Liste der Signaturen durchsuchen und die Signaturen aktivieren, wenn sie sich nicht im *aktivierten* Zustand befinden.Die Gesamtzahl der Signaturen ist auf 519 gestiegen. Diese Nummer enthält alle in der Datei IOS-S193.zip verfügbaren Signaturen, die der Unterkategorie Dateifreigabe
angehören.



Weitere Informationen zur Verwendung von Cisco SDM zur Verwaltung der Cisco IOS IPS-Funktion finden Sie in der Dokumentation zu Cisco SDM unter der URL:

Signaturen auswählen und Signaturkategorien bearbeiten

Um festzustellen, wie die richtigen Signaturen für ein Netzwerk effektiv ausgewählt werden, müssen Sie einige Dinge über das Netzwerk wissen, das Sie schützen. Aktualisierte Informationen zu Signaturkategorien in Cisco SDM 2.2 und höher unterstützen Kunden außerdem bei der Auswahl der richtigen Signaturensätze zum Schutz des Netzwerks.

Die Kategorie ist eine Möglichkeit, Signaturen zu gruppieren. Sie hilft, die Auswahl der Signaturen auf eine Untergruppe von Signaturen einzugrenzen, die für die jeweiligen Signaturen relevant sind. Eine Signatur kann nur einer Kategorie angehören oder mehreren Kategorien angehören.

Die fünf wichtigsten Kategorien sind:

- Betriebssystem - betriebssystembasierte Signaturkategorisierung
- Angriff - Kategorisierung angriffsbasierter Signaturen

- Service - Service-basierte Signaturkategorisierung
- Layer-2-4-Protokoll - Signaturkategorisierung auf Protokollebene
- Versionen - Release-basierte Signaturkategorisierung

Jede dieser Kategorien ist weiter in Unterkategorien unterteilt.

Betrachten Sie beispielsweise ein Heimnetzwerk mit einer Breitbandverbindung zum Internet und einen VPN-Tunnel zum Unternehmensnetzwerk. Auf dem Breitband-Router ist die Cisco IOS-Firewall für die offene (Nicht-VPN-)Internetverbindung aktiviert, um zu verhindern, dass eine Verbindung aus dem Internet stammt und mit dem Heimnetzwerk verbunden ist. Der gesamte Datenverkehr vom Heimnetzwerk zum Internet ist zulässig. Angenommen, der Benutzer verwendet einen Windows-basierten PC und Anwendungen wie HTTP (Surfen im Internet) und E-Mail.

Die Firewall kann so konfiguriert werden, dass nur die Anwendungen, die der Benutzer benötigt, den Router durchlaufen dürfen. So wird der Fluss von unerwünschtem und potenziell schädlichem Datenverkehr kontrolliert, der sich im gesamten Netzwerk ausbreiten kann. Bedenken Sie, dass der Heimbenutzer keinen bestimmten Service benötigt oder verwendet. Wenn dieser Dienst die Firewall durchlaufen darf, besteht ein potenzielles Loch, das ein Angriff im Netzwerk durchlaufen kann. Best Practices lassen nur Services zu, die benötigt werden. Jetzt ist es einfacher auszuwählen, welche Signaturen aktiviert werden sollen. Sie müssen Signaturen nur für die Dienste aktivieren, die Sie für den Durchfluss durch die Firewall zulassen. In diesem Beispiel umfassen Dienste E-Mail und HTTP. Cisco SDM vereinfacht diese Konfiguration.

Um die Kategorie zur Auswahl der erforderlichen Signaturen zu verwenden, wählen Sie **Service > HTTP**, und aktivieren Sie alle Signaturen. Dieser Auswahlprozess funktioniert auch im Signaturimport-Dialogfeld, in dem Sie alle HTTP-Signaturen auswählen und in den Router importieren können.

Weitere Kategorien müssen ausgewählt werden: DNS, NETBIOS/SMB, HTTPS und SMTP.

Signaturen für Standard-SDF-Dateien aktualisieren

Die drei pro Baustein erstellten SDFs (attack-drop.dsf, 128 MB.sdf und 256 MB.sdf) sind derzeit auf Cisco.com unter http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup verfügbar (nur registrierte Kunden). Neuere Versionen dieser Dateien werden veröffentlicht, sobald sie verfügbar sind. Um Router zu aktualisieren, die Cisco IOS IPS mit diesen Standard-SDFs ausführen, gehen Sie zur Website und laden Sie die neuesten Versionen dieser Dateien herunter.

CLI-Verfahren

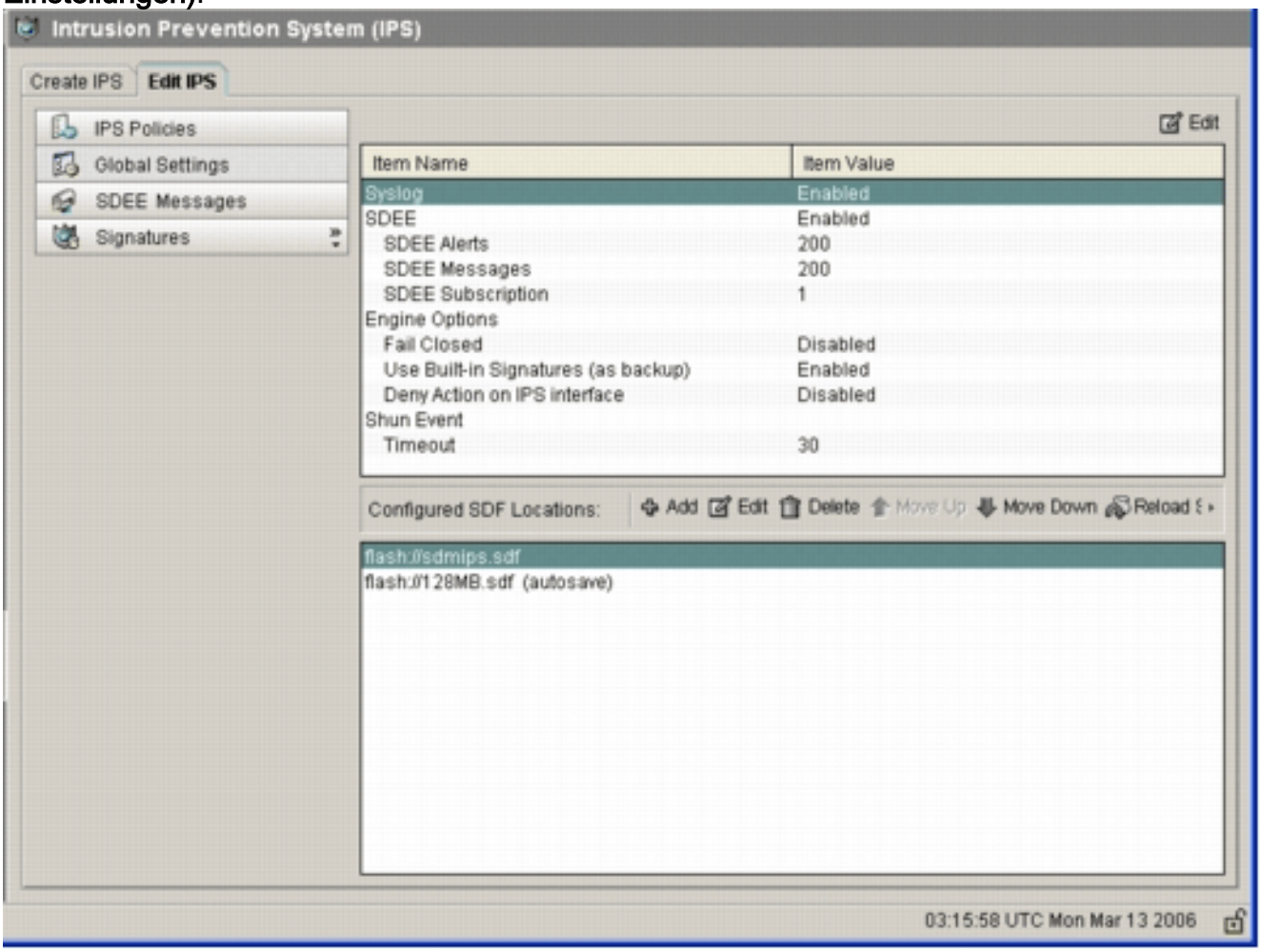
1. Kopieren Sie die heruntergeladenen Dateien an den Speicherort, von dem der Router für das Laden dieser Dateien konfiguriert ist. Um herauszufinden, wo der Router derzeit konfiguriert ist, verwenden Sie **show running-config. | in ip ips sdf**-Befehl.
   ```
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```
   In diesem Beispiel verwendet der Router im Flash-Speicher 256 MB.sdf. Die Datei wird aktualisiert, wenn Sie die neu heruntergeladenen 256MB.sdf in den Router-Flash-Speicher kopieren.
2. Laden Sie das Cisco IOS IPS-Subsystem neu, um die neuen Dateien auszuführen.Es gibt zwei Möglichkeiten, Cisco IOS IPS neu zu laden: den Router neu laden oder Cisco IOS IPS neu konfigurieren, um das IOS IPS-Subsystem zum erneuten Laden der Signaturen

auszulösen. Um Cisco IOS IPS neu zu konfigurieren, entfernen Sie alle IPS-Regeln von den konfigurierten Schnittstellen, und wenden Sie die IPS-Regeln dann wieder auf die Schnittstellen an. Dadurch wird das Cisco IOS IPS-System neu geladen.

SDM 2.2 - Verfahren

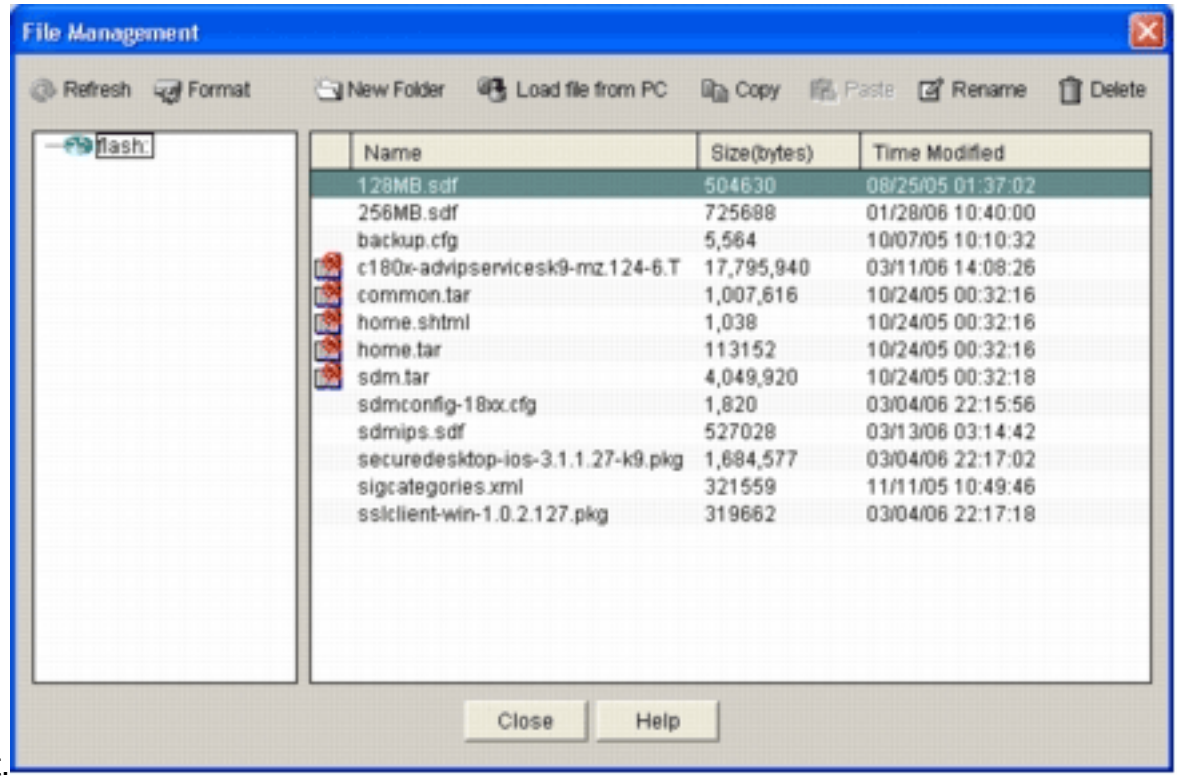
Gehen Sie wie folgt vor, um die Standard-SDFs auf dem Router zu aktualisieren:

1. Klicken Sie auf **Konfigurieren** und dann auf **Intrusion Prevention**.
2. Klicken Sie auf die Registerkarte **Edit IPS (IPS bearbeiten**) und anschließend auf **Global Settings (Globale Einstellungen)**.



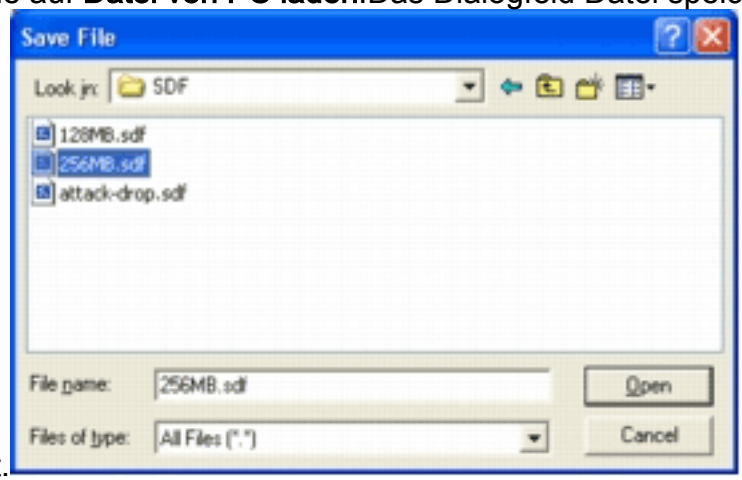
Der obere Teil der Benutzeroberfläche zeigt die globalen Einstellungen. Die untere Hälfte der Benutzeroberfläche zeigt die aktuell konfigurierten SDF-Standorte. In diesem Fall wird die Datei 256 MB.sdf aus dem Flash-Speicher konfiguriert.

3. Wählen Sie **Dateiverwaltung** im Menü Datei aus.Das Dialogfeld Dateiverwaltung wird



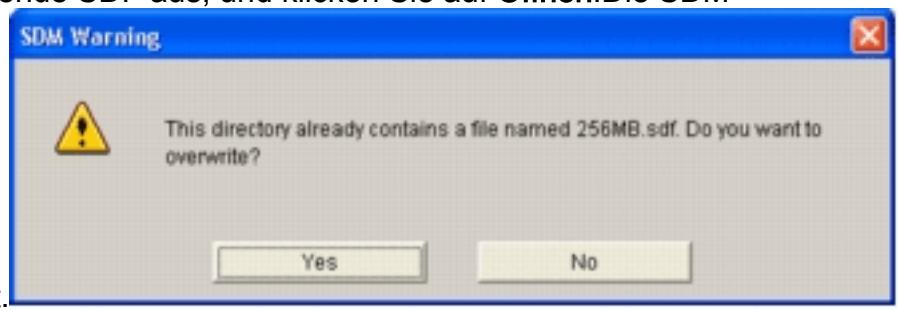
angezeigt.

4. Klicken Sie auf **Datei von PC laden**.Das Dialogfeld Datei speichern wird



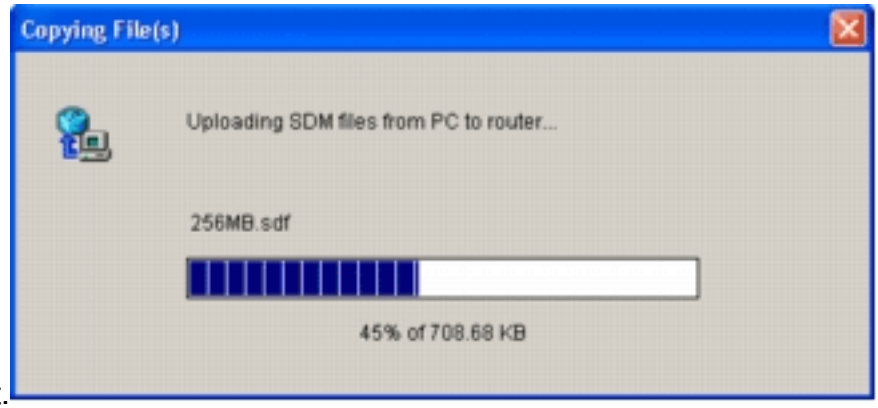
angezeigt.

5. Wählen Sie die zu aktualisierende SDF aus, und klicken Sie auf **Öffnen**.Die SDM-



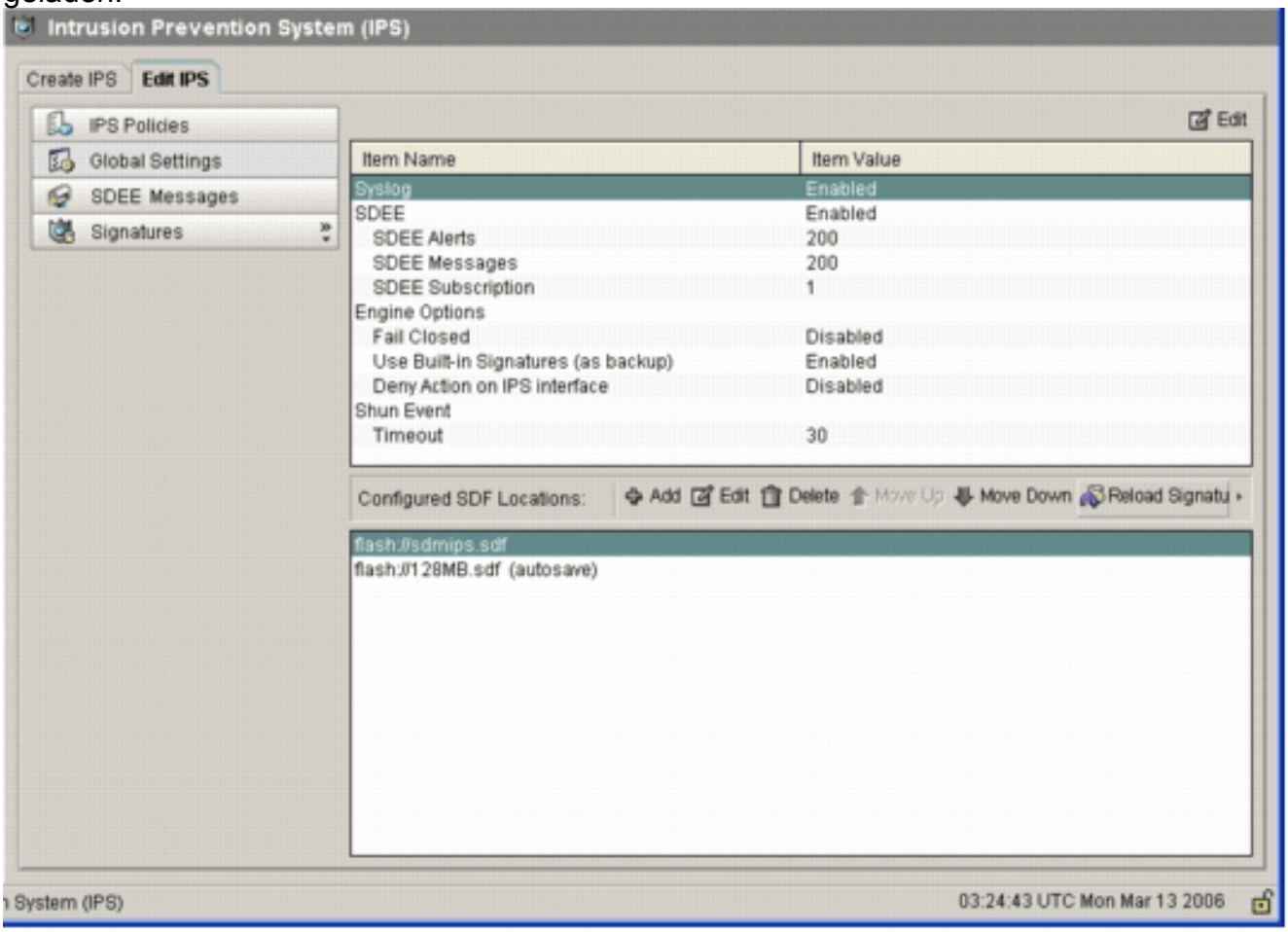
Warnmeldung wird angezeigt.

6. Klicken Sie auf **Ja**, um die vorhandene Datei zu ersetzen.In einem Dialogfeld wird der Fortschritt des Upload



angezeigt.

7. Wenn der Upload abgeschlossen ist, klicken Sie in der Symbolleiste zum SDF-Speicherort auf **Signaturen neu laden**. Bei dieser Aktion wird das Cisco IOS IPS neu geladen.



Hinweis: Das Paket IOS-Sxxx.zip enthält alle Signaturen, die von Cisco IOS IPS unterstützt werden. Aktualisierungen dieses Signaturpakets werden auf Cisco.com veröffentlicht, sobald sie verfügbar sind. Informationen zum Aktualisieren der in diesem Paket enthaltenen Signaturen finden Sie in Schritt 2.

Zugehörige Informationen

- Cisco Intrusion Prevention System
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)
- Technischer Support – Cisco Systems