Cisco IOS IPSでのルータ、SDM、およびCisco IOS CLIの設定

内容

概要

Cisco Router and Security Device Manager(SDM)2.2では、Cisco IOS® IPS設定がSDMアプリケーションに統合されています。Cisco IOS IPS を設定するために、別のウィンドウを起動する必要はありません。

Cisco SDM 2.2 では、新しい IPS コンフィギュレーション ウィザードにより、ルータ上で Cisco IOS IPS をイネーブルにするために必要な手順が指示されます。また、Cisco SDM 2.2 で Cisco IOS IPS のイネーブル化、ディセーブル化、調整を行うための高度な設定も使用できます。

あらかじめ調整されたシグネチャ定義ファイル（SDF）を使って、Cisco IOS IPS を実行することを推奨します。attack-drop.sdf、128MB.sdf、256MB.sdf）。これらのファイルは、メモリ量が異なるルータに対して作成されます。ファイルは Cisco SDM にバンドルされています。ルータで Cisco IOS IPS 初めてイネーブルにする場合は SDF が推奨されます。これらのファイルは、http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup（登録ユーザ専用）からダウンロードすることもできます。

デフォルトの SDF をイネーブルにするプロセスは、「工場出荷時のデフォルトの SDF を使った Cisco IOS IPS の有効化」で詳細に説明します。デフォルトの SDF が十分でないか、新しいシグネチャを追加する場合、「Append Additional Signatures after Enabling Default SDF」に記載されている手順を使用できます。

前提条件

要件

Cisco SDM 2.2を使用するには、Java Runtime Environment(JRE)バージョン1.4.2以降が必要です。シスコが推奨する調整されたシグニチャファイル（DRAMに基づく）が、Cisco SDM（Cisco SDMのルータのフラッシュメモリにロードされる）にバンドルされています。

使用するコンポーネント

このドキュメントの情報は、Cisco ルータおよび Security Device Manager（SDM）2.2 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

工場出荷時のデフォルトの SDF を使ったCisco IOS IPS の有効化

CLI の手順

CLI を使って、ルータのフラッシュ上に 128 MB.sdf をロードするように Cisco IOS IPS を搭載した Cisco 1800 シリーズ ルータを構成するには、次の手順を実行します。

1. Security Device Event Exchange（SDEE）イベント通知をイネーブルにするようにルータを設定します。
   ```
   yourname#conf t
   ```

2. 終了するには、コンフィギュレーション コマンド（1行に 1 つずつ）を入力して、Cntl キーを押した状態で Z キーを押します。
   ```
   yourname(config)#ip ips notify sdee
   ```

3. インターフェイスの関連付けに使用される IPS ルール名を作成します。
   ```
   yourname(config)#ip ips name myips
   ```

4. Cisco IOS IPS システムがシグネチャを読み取るファイルを指定する IPS location コマンドを設定します。この例では、フラッシュ上の次のファイルを使用します。128MB.sdf.このコマンドの口ケーション URL の部分は、ファイルをポイントする、フラッシュ、ディスク、または FTP、HTTP、HTTPS、RTP、SCP、TFTP を介したプロトコルを使用する有効な URL になることがあります。
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   注：Telnetセッションを介してルータを設定する場合は、terminal monitorコマンドを有効にする必要があります。有効にしないと、シグニチャエンジンの構築時にSDEEメッセージが表示されません。

5. トラフィックをスキャンするため Cisco IOS IPS を有効にするインターフェイスで IPS を有効にします。このケースでは、インターフェイス fastEthernet 0 の双方向で有効にしました。

```
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
```

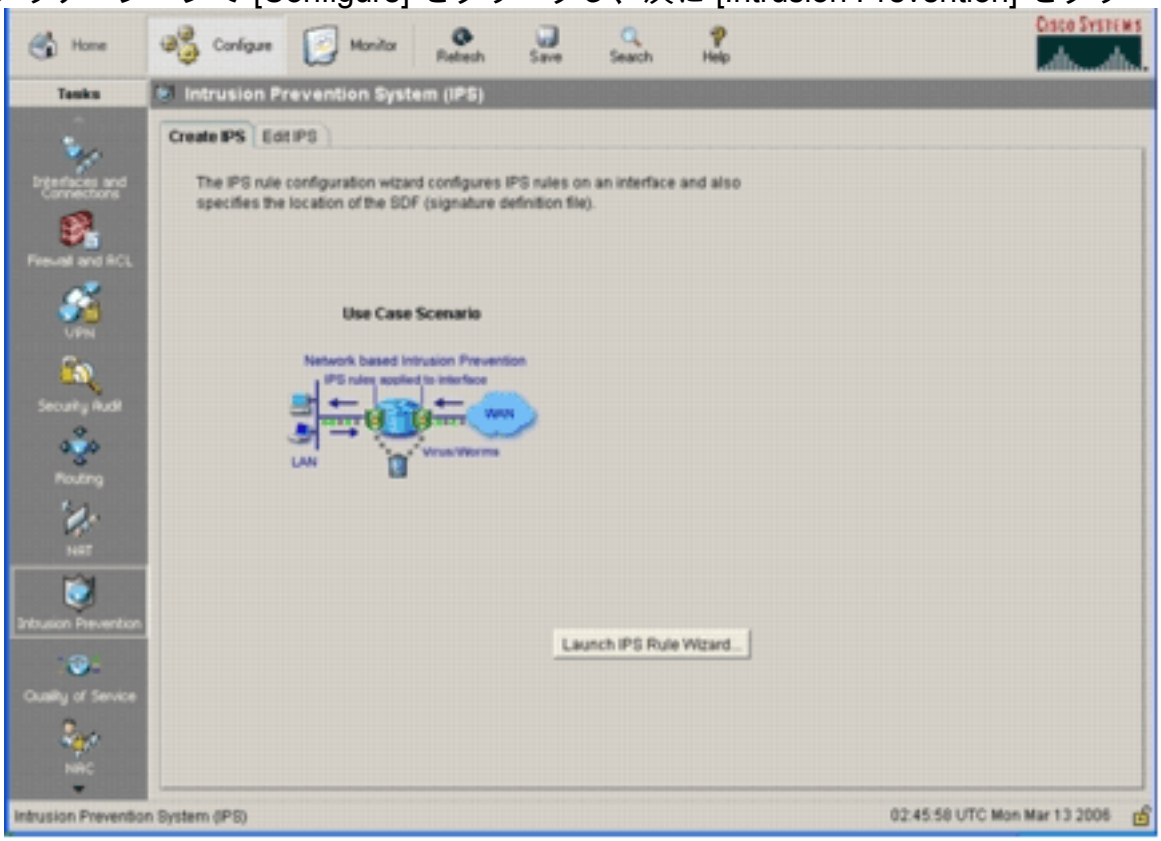
IPS ルールが初めてインターフェイスに適用されると、Cisco IOS IPS は SDF location コマンドで指定されたファイルからシグネチャを構築します。SDEE メッセージが コンソールに記録され、syslog サーバが設定されている場合は、syslog サーバに送信されます。<number> of <number> engines が付いた SDEE メッセージは、シグネチャ エンジンの構築プロセスを示しています。最後に、2 つの番号が同じである場合、すべてのエンジンが構築されます。**注：IP仮想**リアセンブリは、オンにすると、そのインターフェイスを通じてルータに着信するフラグメント化パケットを自動的に再構成するインターフェイス機能です。トラフィックがルータに着信するすべてのインターフェイスで、IP 仮想アセンブリを有効にすることを推奨します。上記の例では、インターフェイス fastEthernet 0 で「IP 仮想アセンブリ」をオンにするだけでなく、内部インターフェイス VLAN 1 でも同様にオンに設定します。

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

SDM 2.2 の手順

Cisco SDM 2.2 を使って Cisco IOS IPS を搭載した Cisco 1800 シリーズ ルータを設定するには、次の手順を実行します。

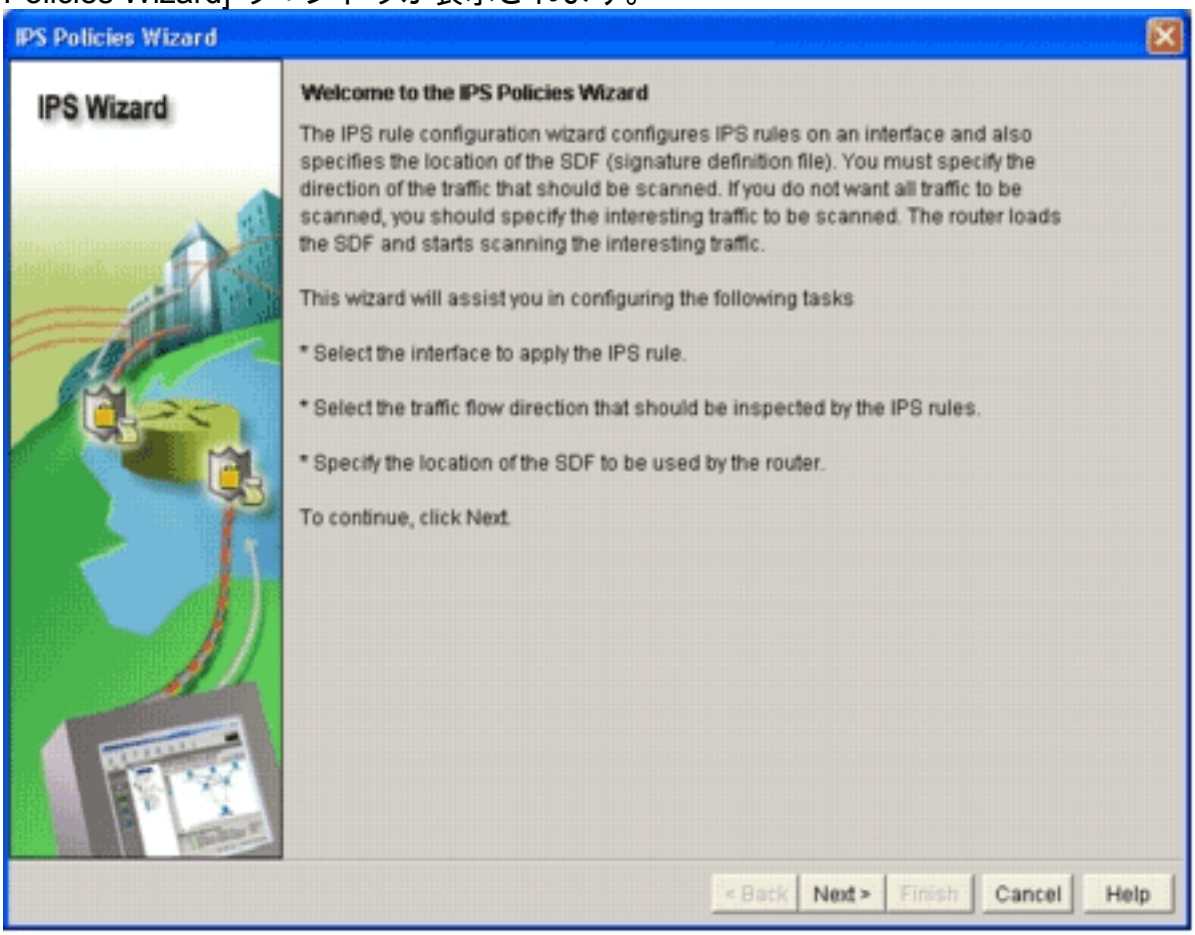
1. SDM アプリケーションで [Configure] をクリックし、次に [Intrusion Prevention] をクリックします。



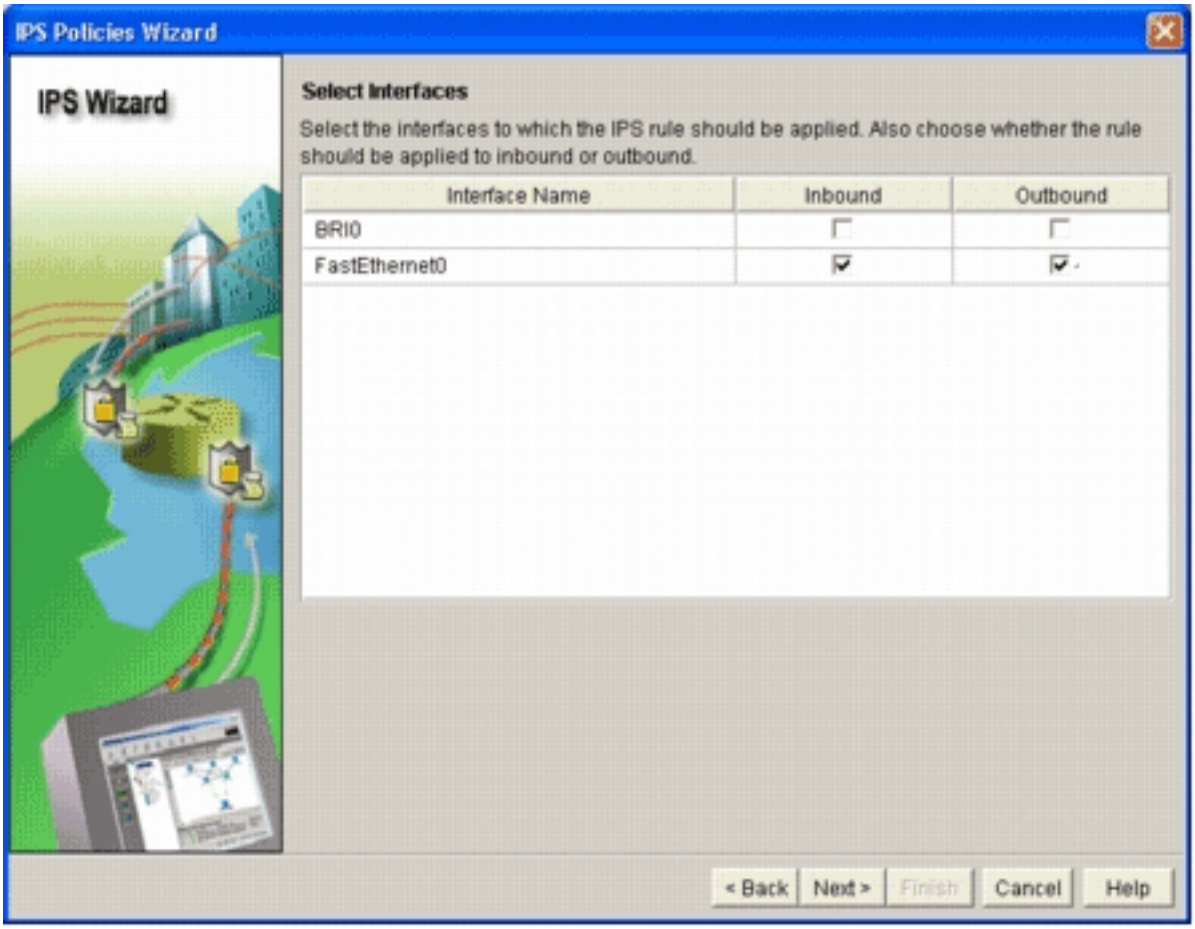
2. [Create IPS] タブをクリックし、次に [Launch IPS Rule Wizard] をクリックします。Cisco SDM では、Cisco IOS IP 機能を設定するため、SDEE を介した IPS イベント通知が必要で

す。デフォルトでは、この機能は無効になっています。Cisco SDM では、次の図に示すように、SDEE を介して IPSイベント通知を有効にするように指示されます。

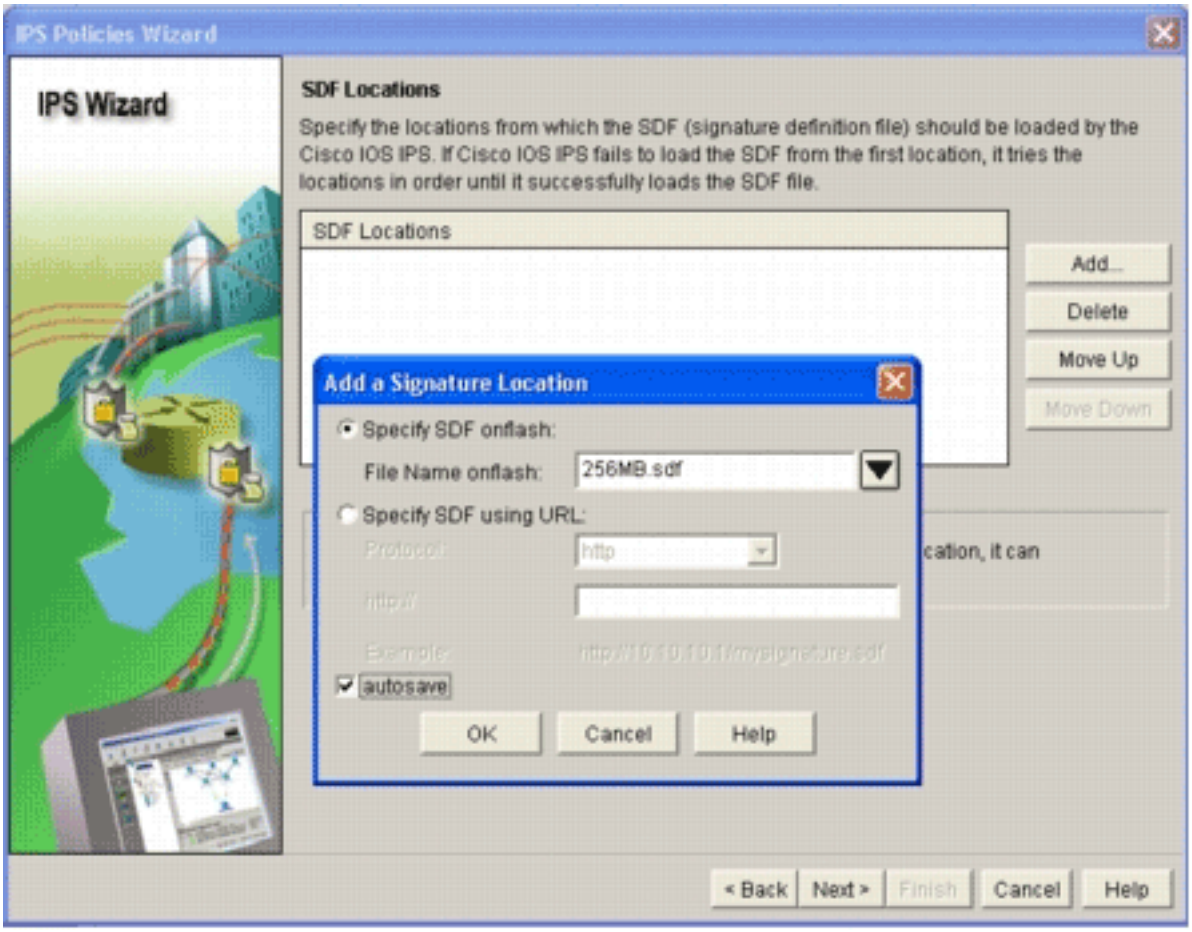
3. [OK] をクリックします。[IPS Policies Wizard] ダイアログボックスの [Welcome to the IPS Policies Wizard] ウィンドウが表示されます。



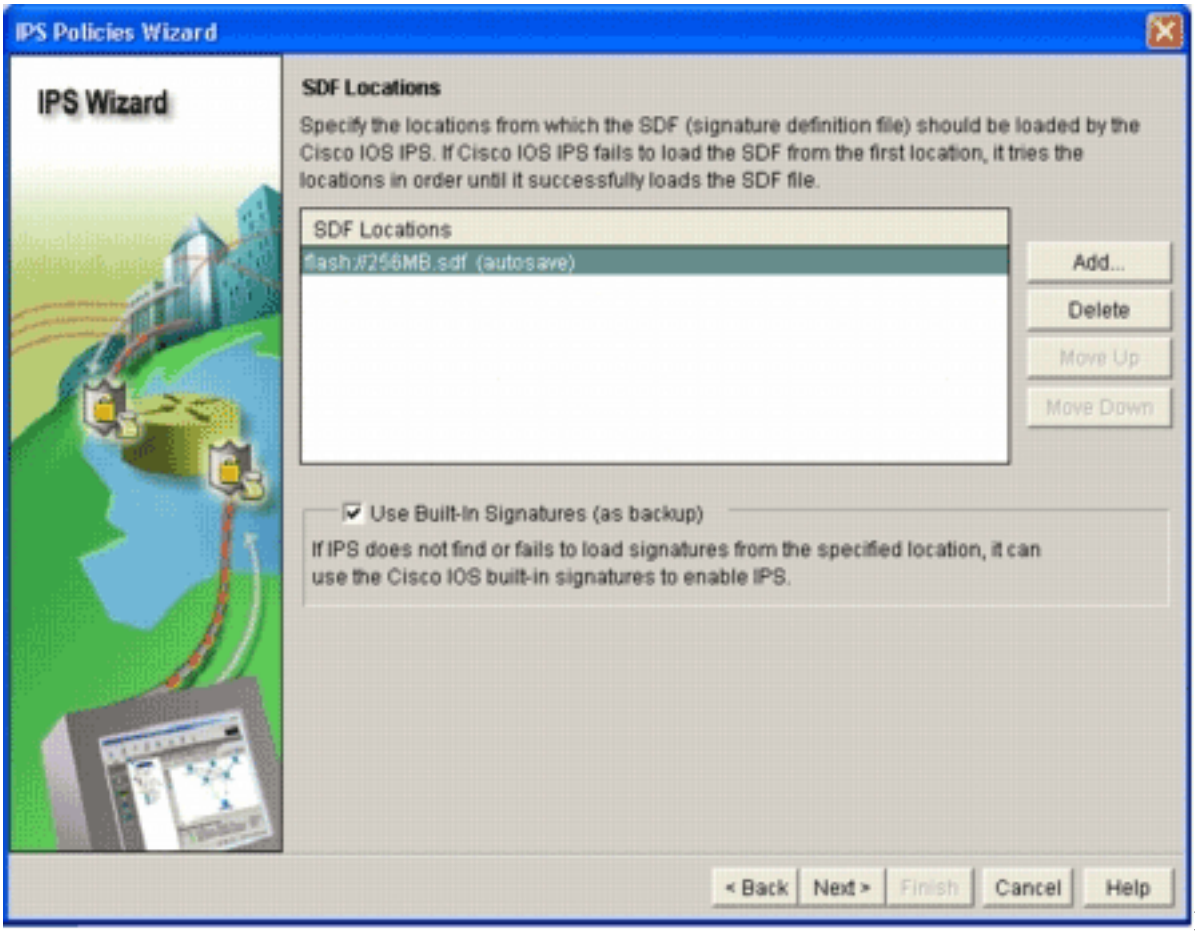
4. [next] をクリックします。[Select Interfaces] ウィンドウが表示されます。



5. IPS を有効にするインターフェイスを選択し、[Inbound] または [Outbound] チェックボックスのいずれかをオンにして、そのインターフェイスの方向を示します。**注：インター**フェイスでIPSを有効にする場合は、インバウンド方向とアウトバウンド方向の両方を有効にすることを推奨します。
6. [next] をクリックします。[SDF Locations] ウィンドウが表示されます。
7. SDF の場所を設定するには、[Add] をクリックします。[Add a Signature Location] ダイアログボックスが表示されます。

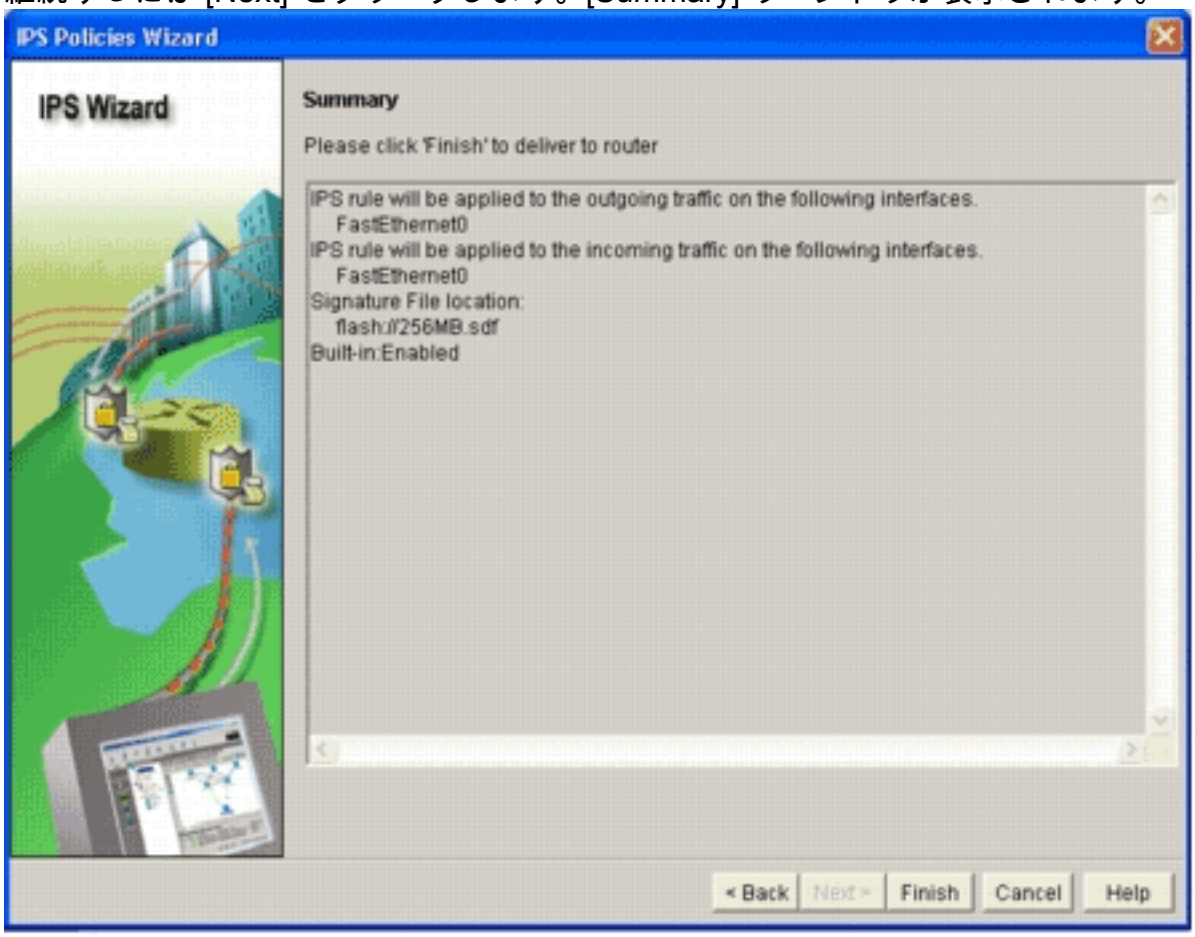


8. [Specify SDF on flash] ラジオ ボタンをクリックして、[File Name on flash] ドロップダウン リストから 256MB.sdf を選択します。
9. [Autosave] チェックボックスをオンにして、[OK] をクリックします。**注：** [Autosave] オプションにより、シグネチャが変更された場合、シグネチャファイルが自動的に保存されます。[SDF Locations] ウィンドウに新しい SDF の場所が表示されます。

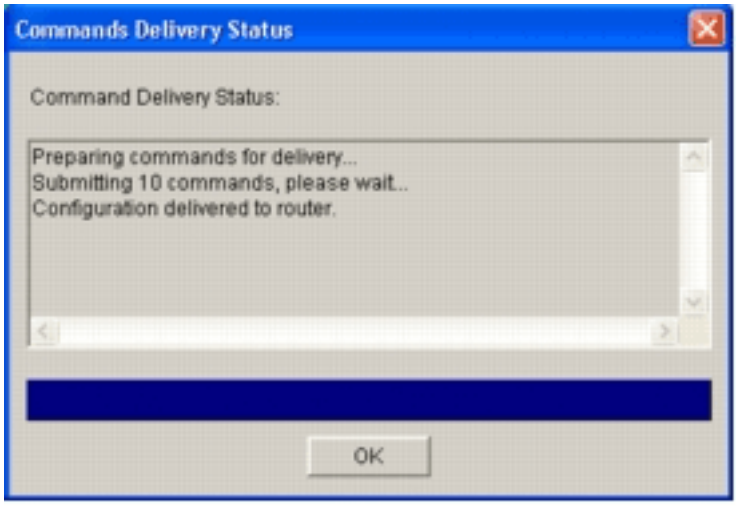


注：バックアップを指定するために、追加の署名場所を追加できます。

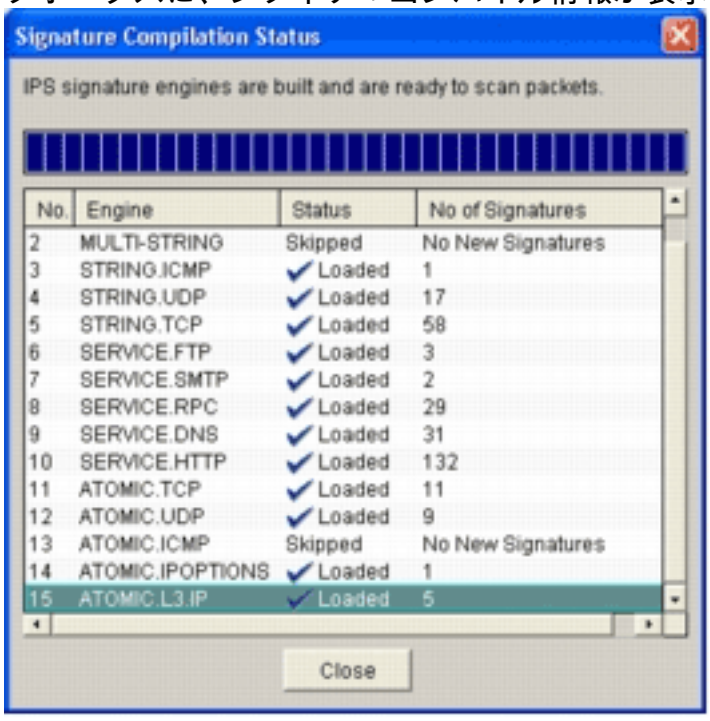
10. [Use Built-In Signatures (as backup)] チェックボックスをオンにします。**注：1つ以上の場所を指定していない限り、組み込みの署名オプションを使用しないことを推奨します。**
11. 継続するには [Next] をクリックします。[Summary] ウィンドウが表示されます。



12. [Finish] をクリックします。[Commands Delivery Status] ダイアログボックスに、IPS エンジンがすべてのシグネチャをコンパイルしたときのステータスが表示されます。

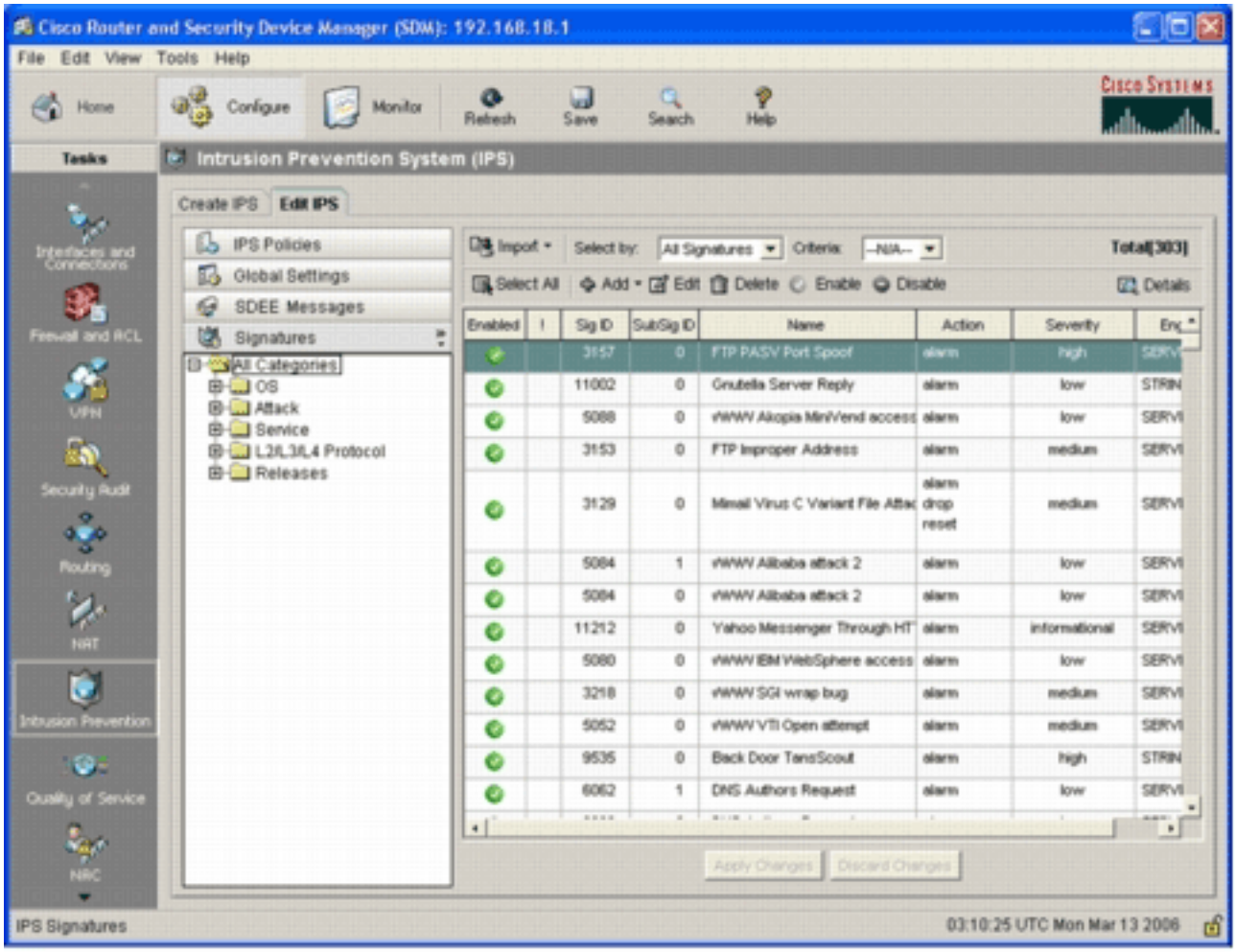


13. プロセスが完了したら、[OK] をクリックします。[Signature Compilation Status] ダイアログボックスに、シグネチャコンパイル情報が表示されます。



この情報には、コンパイルを実行したエンジンと、そのエンジン内のシグネチャ数が表示されます。スタータス列に [Skipped] と表示されたエンジンの場合、そのエンジン用にロードされたシグネチャはありません。

14. [Close] をクリックして、[Signature Compilation Status] ダイアログボックスを閉じます。
15. どのシグネチャがルータに現在ロードされているか検証するには、[Configure] をクリックし、次に [Intrusion Prevention] をクリックします。
16. [Edit IPS] タブをクリックし、次に [Signatures] をクリックします。[Signatures] ウィンドウに IPS シグネチャリストが表示されます。



デフォルトの SDF を有効にした後の追加シグネチャの追加

CLI の手順

シグネチャの作成、または配布済み IOS-Sxxx.zip ファイルのシグネチャ情報の読み取りに使用できる CLI コマンドはありません。SDM または IPS センサー 用 Management Center のいずれかを使って、Cisco IOS IPS システムのシグネチャを管理することを推奨します。

すでにシグネチャファイルを準備していて、このファイルを Cisco IOS IPS システムで実行している SDF とマージする場合は、次のコマンドを使用できます。

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

シグネチャ ロケーション コマンドで定義したシグネチャ ファイルは、ルータのリロード時、またはルータ IOS IPS の再設定時に、ルータがシグネチャ ファイルをロードするファイルです。マージ プロセスを正常に完了するには、シグネチャ ファイル ロケーション コマンドで定義されたファイルも更新する必要があります。

1. 現在設定されているシグネチャの場所を確認するには、**show コマンドを使用します。**出力には設定されたシグネチャの位置が表示されます。このコマンドは、現在実行されているシグネチャがどこからロードされたかを表示します。

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

   Signatures were last loaded from flash:128MB.sdfCisco SDF release version S128.0Trend

SDF release version V0.0

2. シグネチャ ファイルをマージするには、**copy <url> ips-sdf コマンドを、前の手順で取得した情報と併せて使用します。**

```
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#
```

copy コマンドを実行すると、ルータはシグネチャ ファイルをメモリにロードし、シグネチャ エンジンを構築します。コンソール SDEE メッセージの出力では、各シグネチャ エンジンの構築状態が表示されます。%IPS-6-ENGINE_BUILD_SKIPPED は、このエンジンには新規シグネチャがないことを示しています。%IPS-6-ENGINE_READY は、新規シグネチャがあり、エンジンが準備できていることを示しています。前述のとおり、「15 of 15 engines」というメッセージは、すべてのエンジンが構築済みであることを示しています。IPS-7-UNSUPPORTED_PARAM は、Cisco IOS IPS が特定のパラメータをサポートしていないことを示しています。たとえば CapturePacket と ResetAfterIdle です。**注：** これらのメッセージは情報専用で、Cisco IOS IPS のシグネチャ機能やパフォーマンスへの影響はありません。これらのログ メッセージは、ロギング レベルをデバッグ (レベル 7) より上に設定することでオフにできます。

3. シグネチャ ロケーション コマンドで定義されている SDF を更新し、ルータのリロード時に、更新されたシグネチャと一緒にマージされたシグネチャ セットが設定されるようにします。この例では、マージされたシグネチャを 128MB.sdf フラッシュ ファイルに保存した後のファイル サイズの差異を示しています。

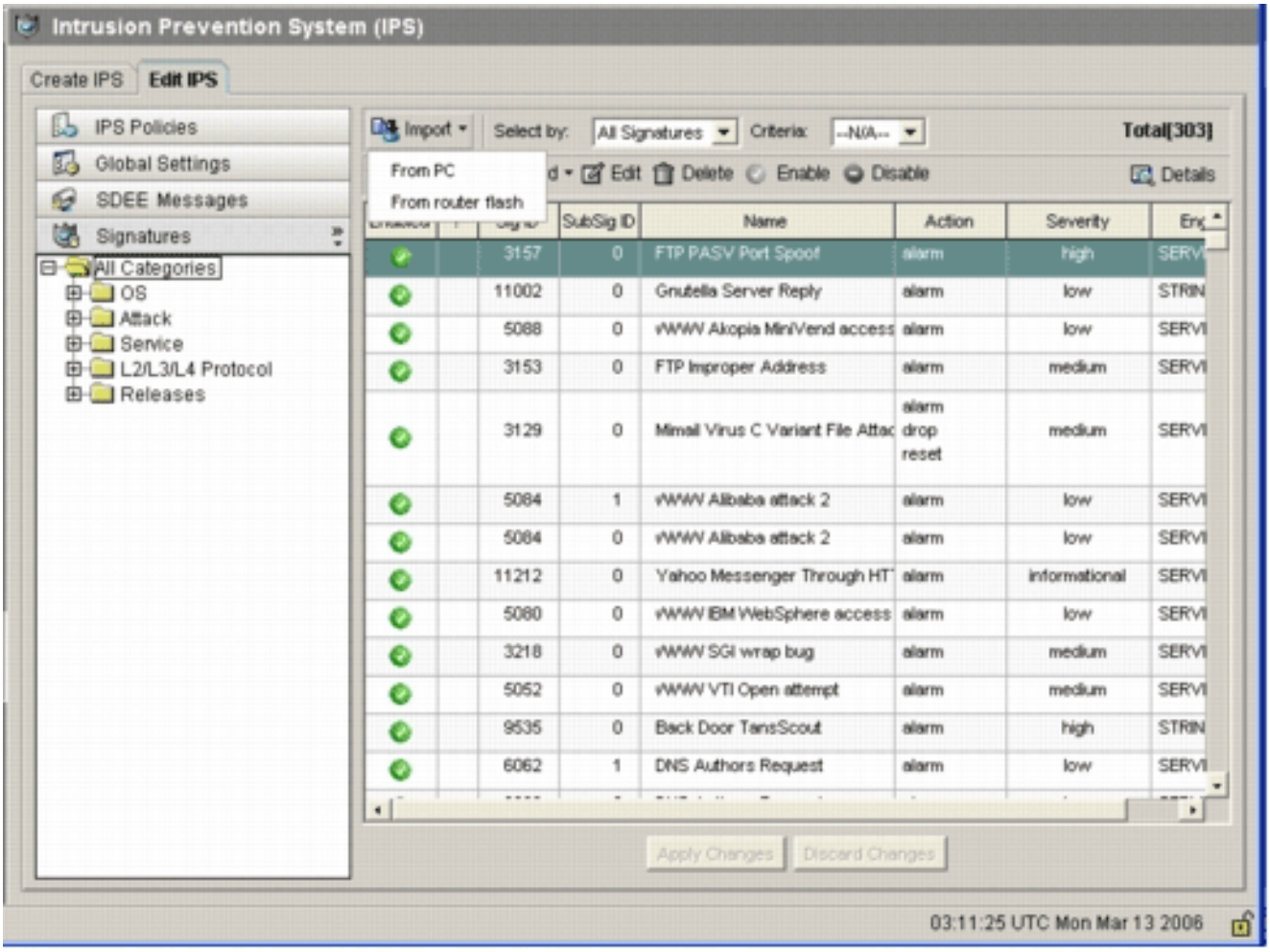
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

警告：新しい128MB.sdfには、お客様がマージしたシグニチャが含まれています。内容は、シスコのデフォルトの 128MB.sdf ファイルとは異なります混乱を避けるために、このファイルを別の名前に変更することを推奨します。名前を変更した場合、シグネチャ ロケーション コマンドも変更する必要があります。

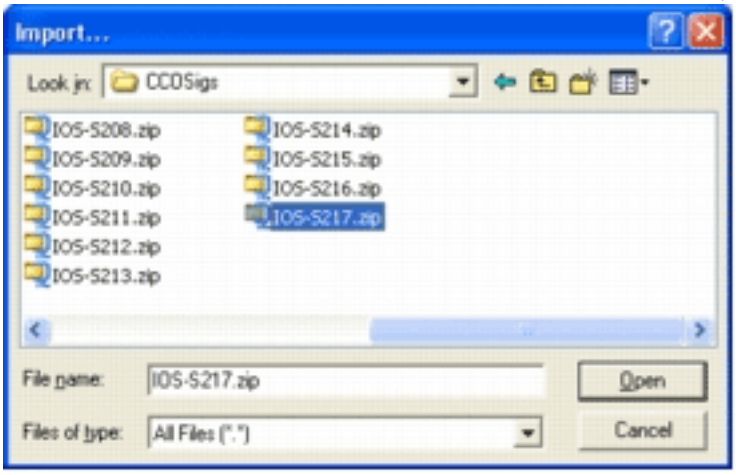
SDM 2.2 の手順

Cisco IOS IPS を有効にすると、Cisco SDM インポート機能を使って、シグネチャ セットを実行しているルータに新しいシグネチャを追加できます。新しいシグネチャをインポートするには、次の手順を実行します。

1. 追加のシグネチャをインポートするには、デフォルト SDF または IOS-Sxxx.zip 更新ファイルを選択します。
2. [Configure] をクリックし、次に [Intrusion Prevention] をクリックします。
3. [Edit IPS] タブをクリックし、次に [Import] をクリックします。

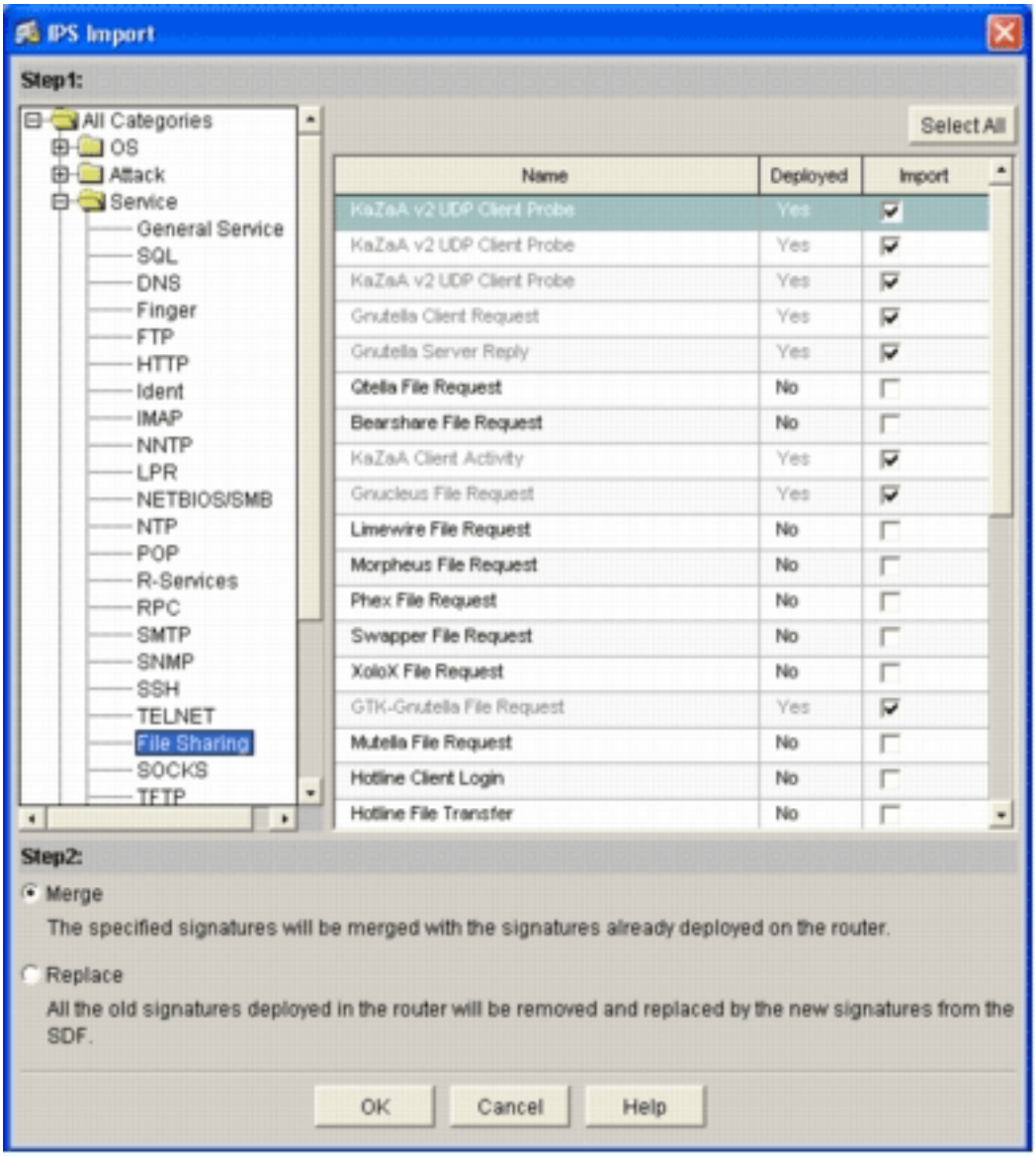


4. [Import] ドロップダウン リストから [From PC] を選択します。
5. シグネチャのインポート元のファイルを選択します。

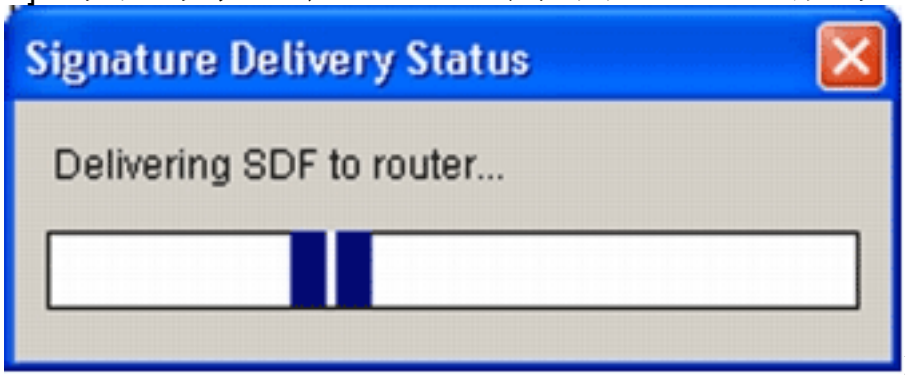


この例では、Cisco.com からダウンロードした最新のアップデートを、ローカルの PC ハード ディスクに保存します。

6. [Open] をクリックします。**警告：メモ**リの制約により、既に展開されているシグネチャの上に追加できる新しいシグネチャの数は限られています。選択したシグネチャの数が多すぎる場合、メモリ不足のため、ルータは新しいシグネチャをすべてロードできない場合があります。シグネチャ ファイルのロードが完了すると、[IPS Import] ダイアログボックスが表示

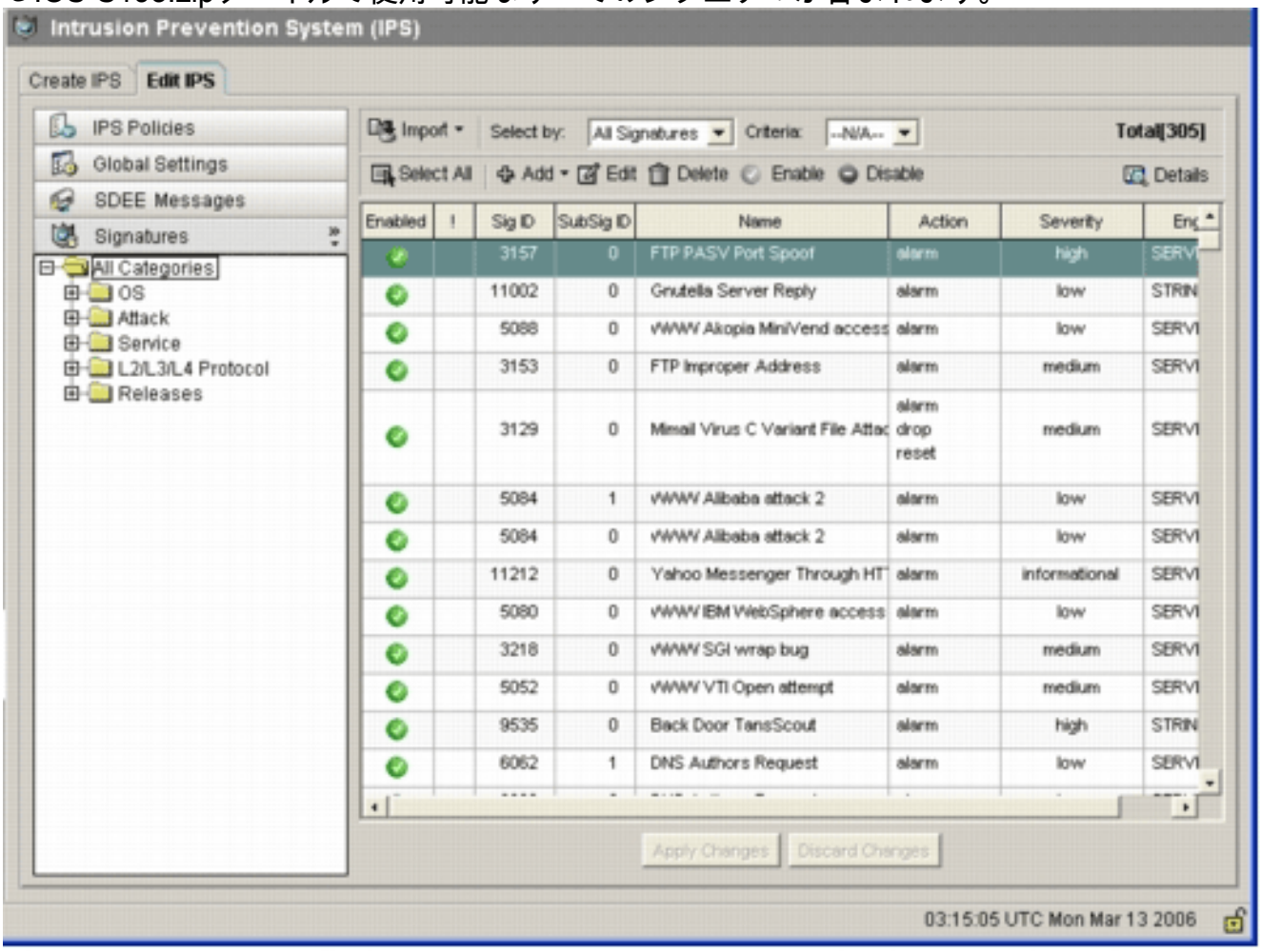


されます。

7. 左のツリー ビューに移動し、インポートするシグネチャの横の [Import] チェックボックスをオンにします。
8. [Merge] ラジオ ボタンをクリックし、次に [OK] をクリックします。**注：**[Replace]オプションは、ルータで設定されている現在のシグニチャを、インポートする選択したシグニチャに置き換えます。[OK] をクリックすると、Cisco SDM アプリケーションはルータにシグネチャを配布します。 

注：シグネチャのコンパイルおよびロード中に高いCPU使用率が発生します。インターフェイスで Cisco IOS IPS を有効にすると、シグネチャ ファイルのロードが開始されます。ルータで SDF のロードが完了するまで約 5 分かかります。Cisco IOS ソフトウェア CLI から **show process cpu コマンドを使って、CPU の使用率を表示できます。**ただし、ルータが SDF をロードしている間は、その他のコマンドや他の SDF のロードは実行しないでください。このような操作を実行すると、シグネチャ コンパイル プロセスが完了するまでの時間が長くなります（SDF のロード時に CPU 使用率が 100 パーセントに近くなるため）。 シグネチ

ャのリストを参照して、*enabled 状態でない場合、シグネチャを有効にする必要があります*。シグニチャの総数は519に増加しました。この数には、ファイル共有サブカテゴリに属するIOS-S193.zipファイルで使用可能なすべてのシグニチャが含まれます。



Cisco SDM を使って Cisco IOS IPS 機能を管理する方法についてのより高度なトピックについては、次の URL の Cisco SDM ドキュメントを参照してください。

シグネチャの選択とシグネチャ カテゴリの操作

ネットワーク用に正しいシグネチャを効果的に選択する方法を決定するには、保護対象のネットワークに関していくつか知らなければならないことがあります。Cisco SDM 2.2 以降では、更新されたシグネチャ カテゴリにより、ユーザはネットワークを保護する正しいシグネチャ セットを選択できます。

カテゴリは、シグネチャをグループ化する方法です。これにより、シグネチャの選択を、相互に関連するシグネチャのサブセットに狭めることができます。1 つのシグネチャは 1 カテゴリにだけ属することもあれば、複数のカテゴリに属することもあります。

上位 5 つのカテゴリを以下に示します。

- OS：運用システムベースのシグニチャ分類
- 攻撃 — 攻撃に基づくシグネチャの分類
- サービス — サービスに基づくシグネチャの分類
- レイヤ2 ~ 4プロトコル：プロトコルレベルのシグニチャ分類
- リリース — リリースに基づくシグネチャの分類

上記の各カテゴリは、さらにサブカテゴリに分類されます。

たとえば、インターネットと VPN 経由で企業ネットワークへのブロードバンド接続が確立しているホーム ネットワークを考えてみましょう。ブロードバンド ルータでは、すべての接続で、インターネットから発信されたトラフィックが接続されているホーム ネットワークへ送信されないように、インターネットへのオープン（非 VPN）接続で Cisco IOS Firewall が有効にされています。ホーム ネットワークからインターネットへのすべてのトラフィックは許可されます。Windows ベースの PC と、HTTP（Web ブラウジング）や電子メールなどのアプリケーションを使用するとします。

ユーザが必要とするアプリケーションだけがルータを介して通過できるように、ファイアウォールを設定します。これにより、ネットワーク全体に広がる、不要なトラフィックや潜在的に悪意のあるトラフィックのフローが制御されます。ホーム ユーザが特定のサービスを必要としなかったり、使用しない場合を考えてみましょう。そのサービスがファイアウォールを通過することが許可されている場合、攻撃に使用されて脅威がネットワーク全体に及ぶおそれのある穴が潜在することになります。ベスト プラクティスは、必要なサービスのみを許可することです。ここでは、有効にするシグネチャを選択する方がより簡単です。ファイアウォールを通過することを許可するサービスに対するシグネチャだけを有効にするだけですみます。この例では、サービスには電子メールと HTTP が含まれます。Cisco SDM はこの設定を簡略化します。

カテゴリを使って必要なシグネチャを選択するには、[Service] > [HTTP] の順に選択して、すべてのシグネチャを有効にします。この選択プロセスは、すべての HTTP シグネチャを選択し、そのシグネチャをルータにインポートできる、シグネチャのインポート ダイアログでも動作します。

選択する必要がある追加カテゴリには、DNS、NETBIOS/SMB、HTTPS および SMTP が含まれます。

デフォルト SDF ファイルのシグネチャの更新

構築された3つのSDF（attack-drop.dsf、128MB.sdf、および256MB.sdf）は、現在 http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup（登録ユーザ専用）のCisco.comで公開されています。 これらのファイルの新バージョンは、使用可能になるとすぐに公開されます。これらのデフォルトの SDF で Cisco IOS IPS を実行するルータを更新するには、Web サイトにアクセスして、これらのファイルの最新バージョンをダウンロードしてください。

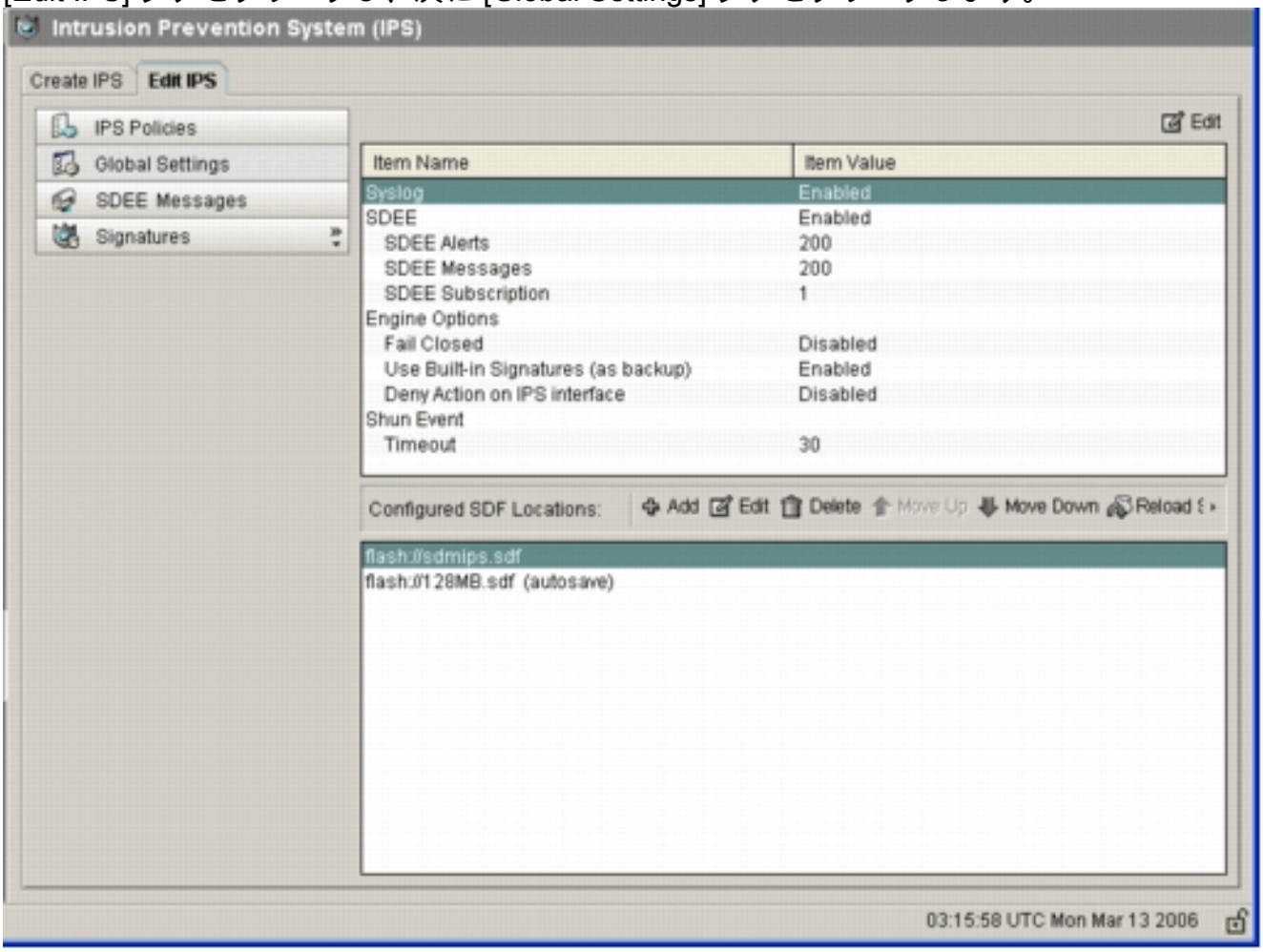
CLI の手順

1. ダウンロードしたファイルを、これらのファイルのダウンロード元としてルータで設定されている場所にコピーします。ルータで現在設定されている場所を確認するには、**show running-config | in ip ips sdf**コマンド
   ```
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```
   この例では、ルータは、フラッシュ上の 256MB.sdf を使用します。このファイルは、新しくダウンロードした 256MB.sdf をルータのフラッシュにコピーすると更新されます。
2. Cisco IOS IPS サブシステムをリロードして、新しいファイルを実行します。Cisco IOS IPS をリロードするには次の 2 つの方法があります。ルータをリロードするか、IOS IPS サブシステムを再設定して、シグネチャをリロードするようトリガーすることです。Cisco IOS IPS を再設定するには、設定済みのインターフェイスからすべての IPS ルールを削除し、インターフェイスに IPS ルールを適用し直すことです。これにより、Cisco IOS IPS システムのリロードがトリガーされます。

SDM 2.2 の手順

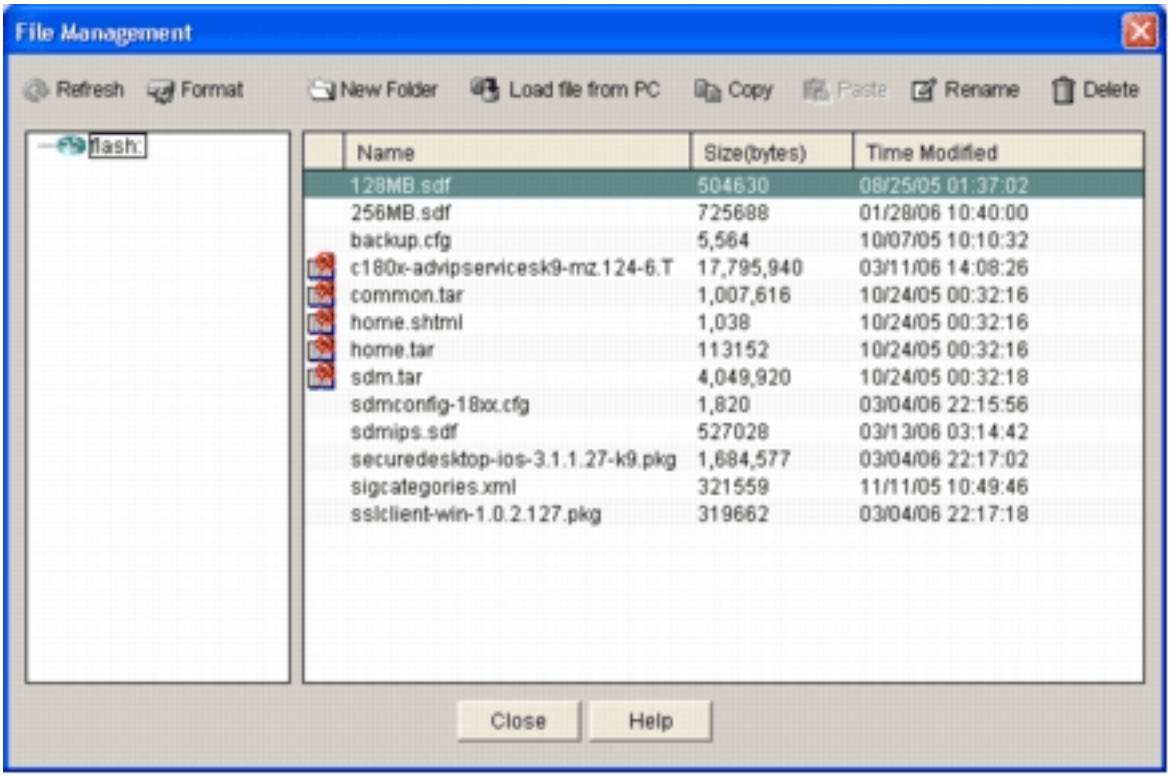
ルータ上のデフォルト SDF を更新するには、次の手順を実行します。

1. [Configure] をクリックし、次に [Intrusion Prevention] をクリックします。
2. [Edit IPS] タブをクリックし、次に [Global Settings] タブをクリックします。

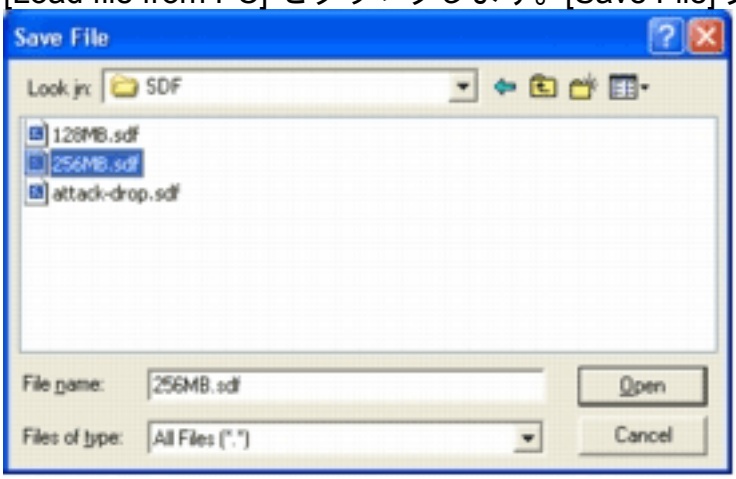


UI の上部にグローバル設定が表示されます。UI の下半分は、現在設定されている SDF の位置を示します。この場合、フラッシュ メモリから読み込まれた 256MB.sdf ファイルが設定されています。

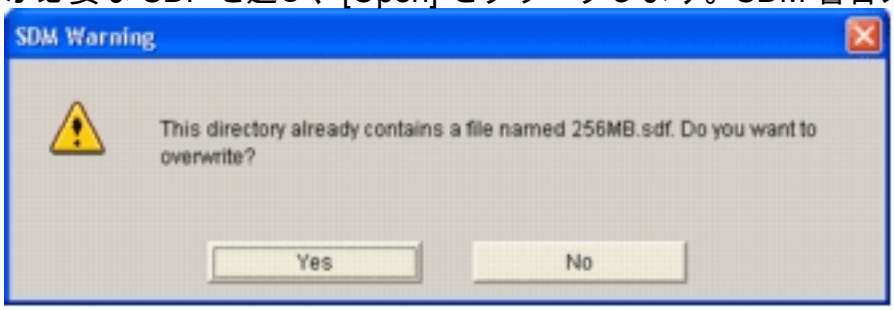
3. [File] メニューから [File Management] を選択します。[File Management] ダイアログボックスが表示されます。



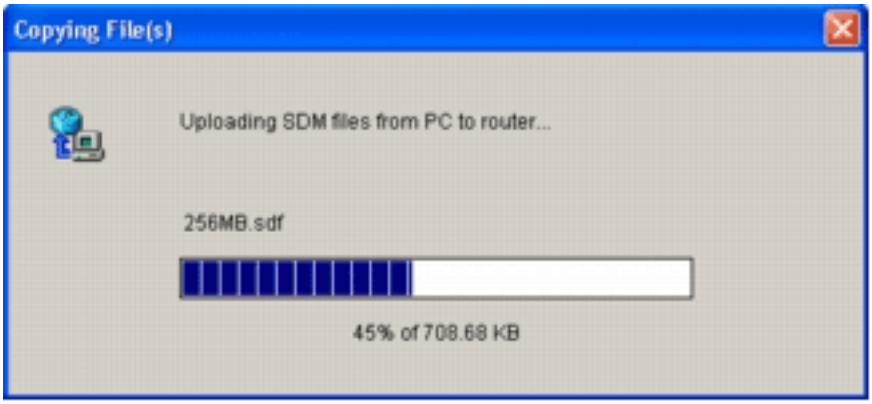
4. [Load file from PC] をクリックします。[Save File] ダイアログボックスが表示されます。



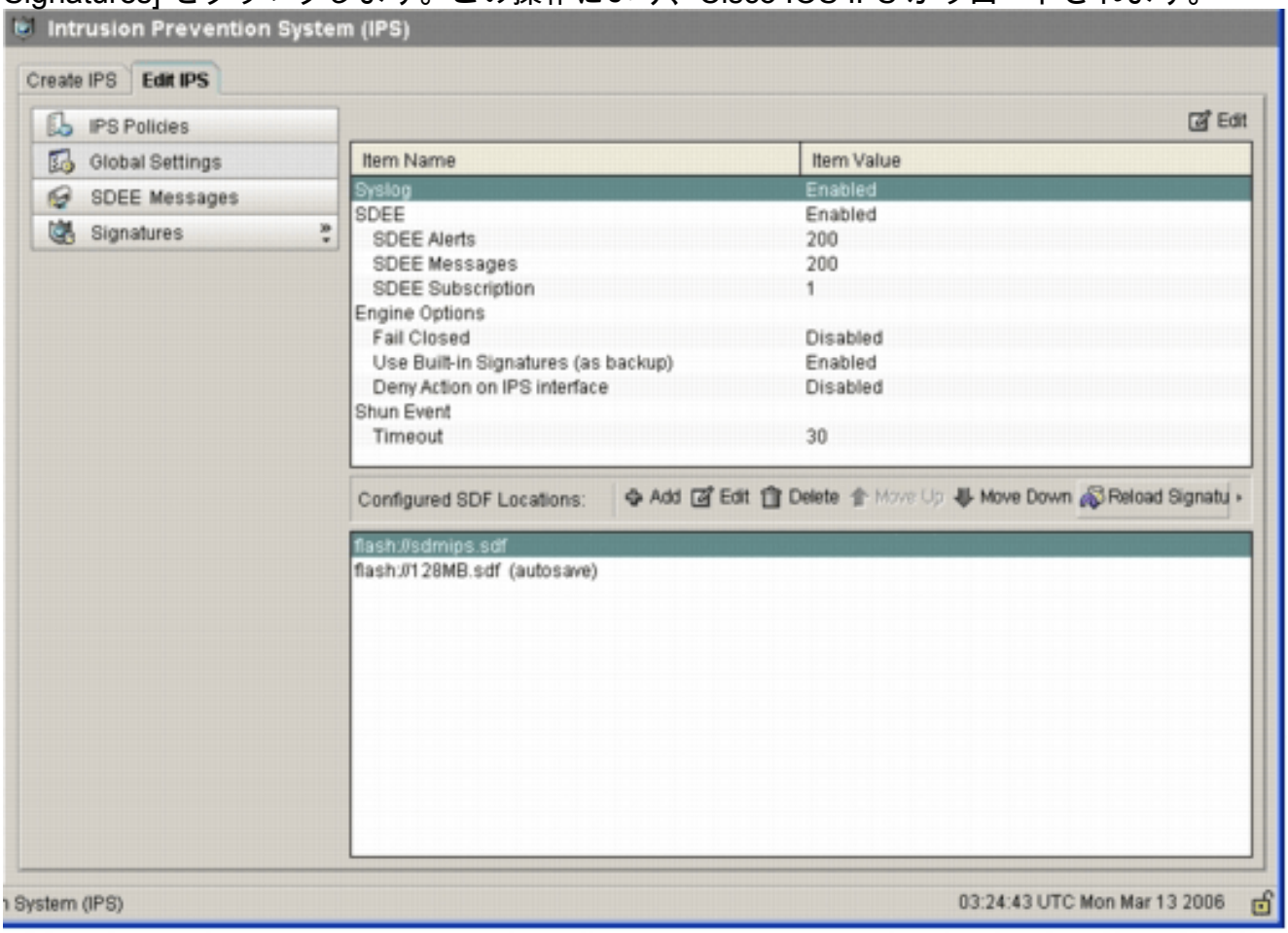
5. 更新が必要な SDF を選び、[Open] をクリックします。SDM 警告メッセージが表示されます。



6. 既存のファイルを置き換えるには、[Yes] をクリックします。ダイアログ ボックスが表示され、アップロードの進捗状況が示されます。



7. アップロード プロセスが完了したら、SDF ロケーション ツールバーの上にある [Reload Signatures] をクリックします。この操作により、Cisco IOS IPS がリロードされます。



注：IOS-Sxxx.zipパッケージには、Cisco IOS IPSがサポートするすべてのシグニチャが含まれています。このシグネチャ パッケージのアップグレードは、使用可能になり次第、Cisco.com で公開されます。このパッケージに含まれている署名を更新するには、ステップ2を参照してください。

関連情報

- Cisco Intrusion Prevention System
- セキュリティ製品に関する Field Notices (CiscoSecure Intrusion Detection を含む)
- テクニカルサポート - Cisco Systems