ルータおよびSDMを使用したCisco IOS IPSの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[設定](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Router and Security Device Manager（SDM）バージョン 2.5 を使用して、12.4(15)T3 リリース以降の Cisco IOS® Intrusion Prevention System（IPS）を設定する方法を説明します。

ISDM 2.5 リリースでの OS IPS に関連する機能強化は次のとおりです。

- シグニチャ リスト GUI にコンパイル済みシグニチャの合計数が表示されるようになりました。
- SDM シグニチャ ファイル（zip ファイル形式。たとえば、sigv5-SDM-S307.zip）と CLI シグニチャ パッケージ（pkg ファイル形式。たとえば、IOS S313 CLI.pkg）を 1 つの操作で同時にダウンロードできます。
- ダウンロードしたシグニチャ パッケージをオプションとして自動的にルータにプッシュできます。

初期プロビジョニング プロセスに必要なタスクは次のとおりです。

1. SDM 2.5 をダウンロードしてインストールします。
2. SDM 自動更新を使用して、IOS IPS シグニチャ パッケージをローカル PC にダウンロードします。
3. IPS ポリシー ウィザードを起動して、IOS IPS を設定します。
4. IOS IPS 設定およびシグニチャが正しくロードされていることを確認します

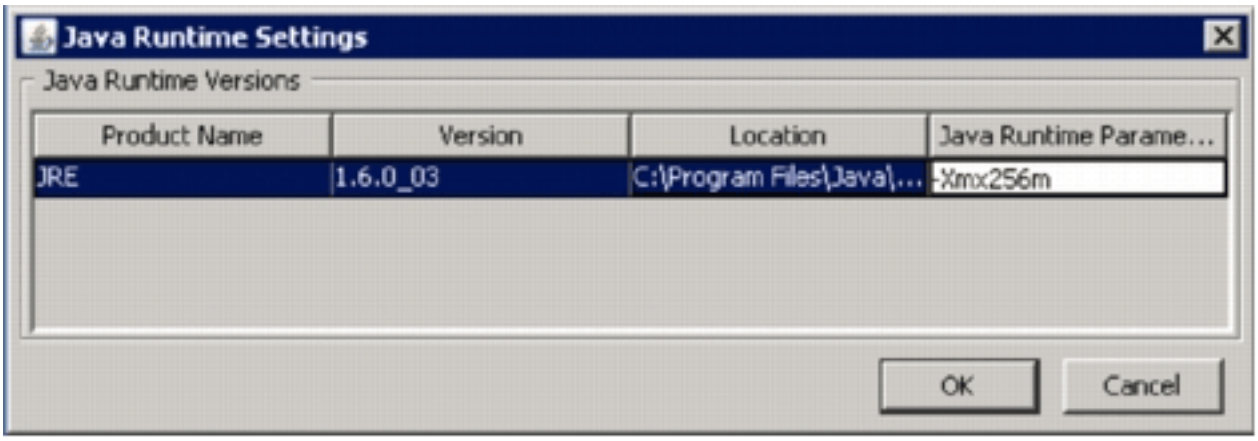
Cisco SDM は、スマート ウィザードによってルータとセキュリティの設定を簡略化する Web ベースの設定ツールです。これらのスマート ウィザードでは、コマンドライン インターフェイス（CLI）の知識がなくても、シスコ ルータをすばやく簡単に導入、設定、モニタすることができます。

SDM バージョン 2.5 は、Cisco.com（http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm（登録ユーザ専用））からダウンロードできます。 リリース ノートは http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/soft

ware/release/notes/SDMr25.html にあります。

注：Cisco SDMでは、1024 x 768以上の画面解像度が必要です。

注：Cisco SDMでは、IOS IPSを設定するために、Javaメモリヒープサイズを256MB以上にする必要があります。Java メモリ ヒープ サイズを変更するには、Java コントロール パネルを開き、[Java] タブをクリックし、[Java Applet Runtime Settings] セクションにある [View] をクリックして、[Java Runtime Parameter] 列に **-Xmx256m と入力します。**



前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS IPS 12.4(15)T3 以降のリリース
- Cisco Router and Security Device Manager (SDM) バージョン 2.5

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

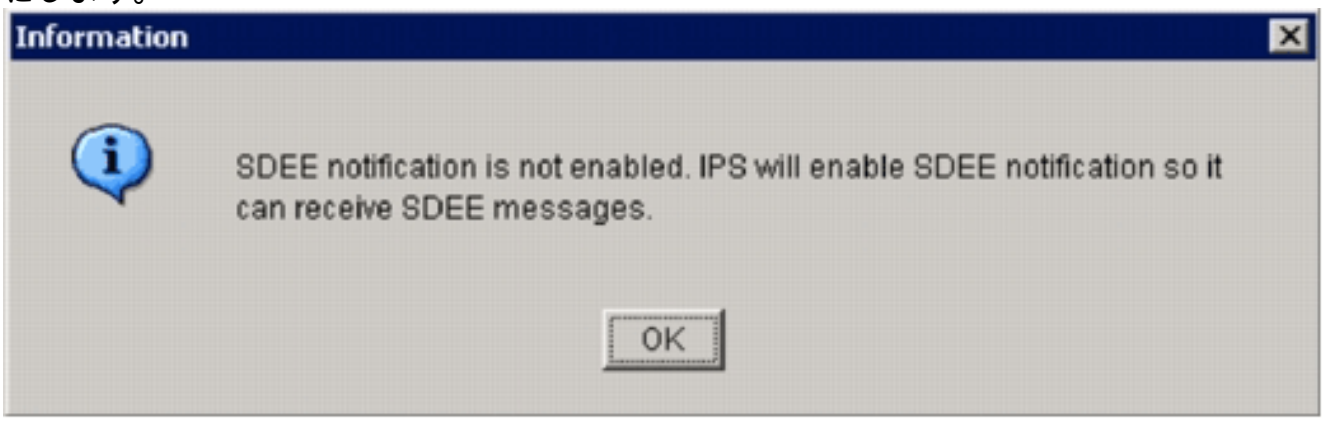
注：SDMを使用してIOS IPSをプロビジョニングするときに、メッセージをモニタするには、ルータへのコンソールまたはTelnetセッション（「term monitor」がオン）を開きます。

1. Cisco.com（ http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm（登録ユーザ専用））から SDM

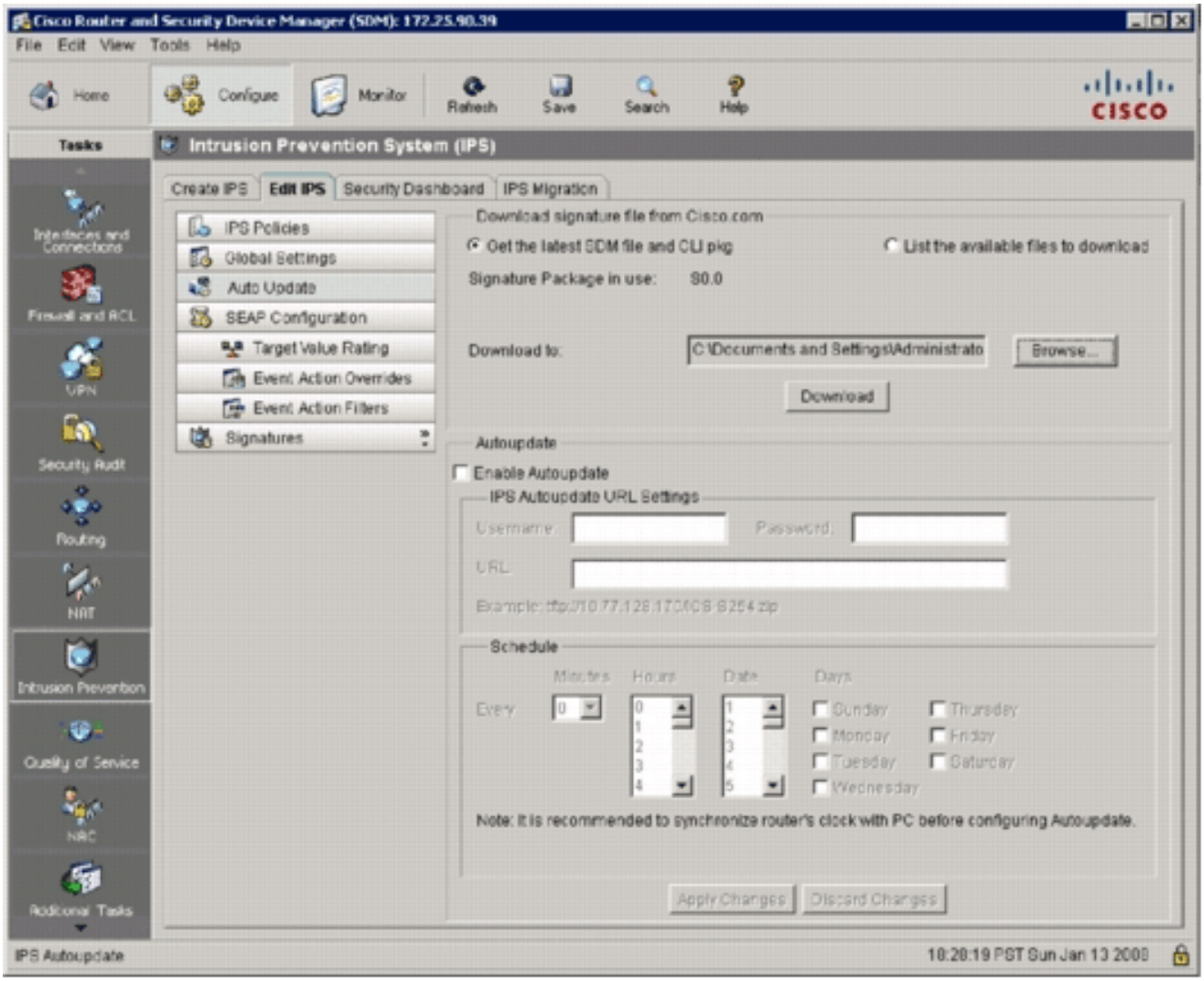
2.5 をダウンロードして、ローカル PC にインストールします。

2. ローカル PC から SDM 2.5 を実行します。
3. [IOS IPS Login] ダイアログボックスが表示されたら、ルータに対する SDM 認証に使用するユーザ名およびパスワードと同じユーザ名とパスワードを入力します。

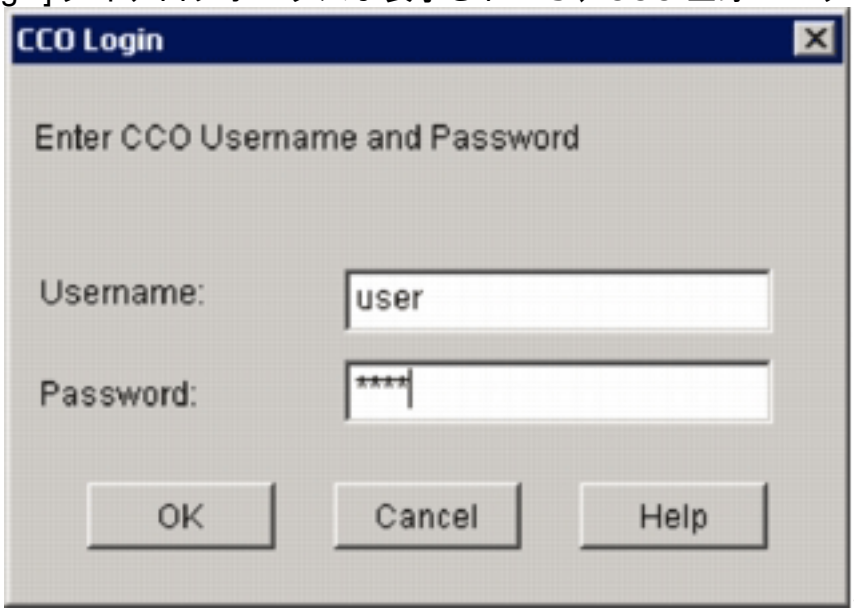
4. SDM ユーザ インターフェイスで、[Configure]、[Intrusion Prevention] の順にクリックします。
5. [Edit IPS] **タブをクリックします。**
6. ルータで SDEE 通知が有効にされていない場合は、[OK] をクリックして SDEE 通知を有効にします。



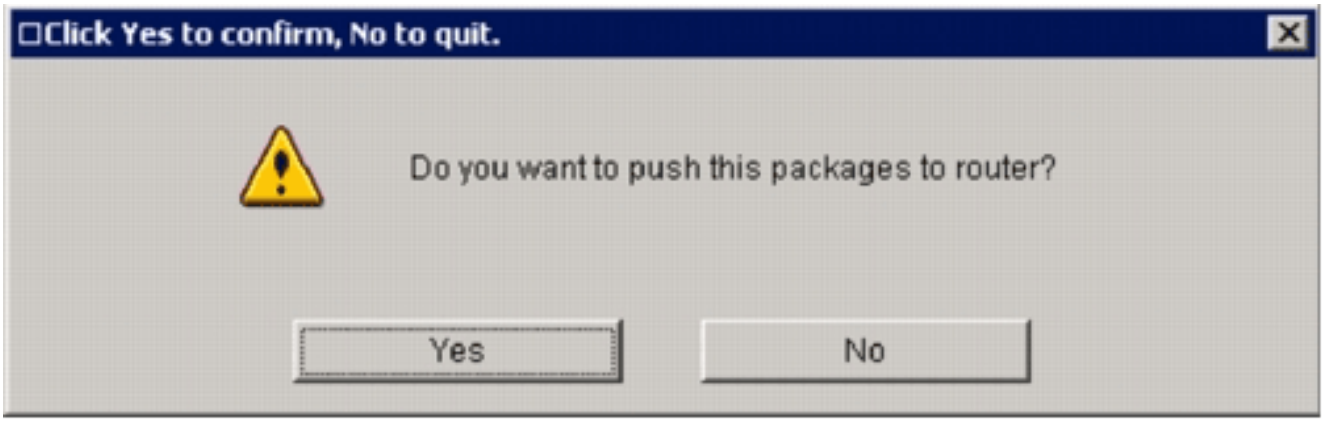
7. [Edit IPS] タブの [Download signature file from Cisco.com] 領域で、[Get the latest SDM file and CLI pkg] **オプション ボタンをクリックしてから [Browse]** をクリックし、ダウンロードしたファイルが保存されているローカル PC 上のディレクトリを選択します。TFTP または FTP サーバのルート ディレクトリを選択できます。選択したディレクトリが、後でシグニイチャ パッケージをルータに導入する際に使用されます。
8. [Download] をクリックします。



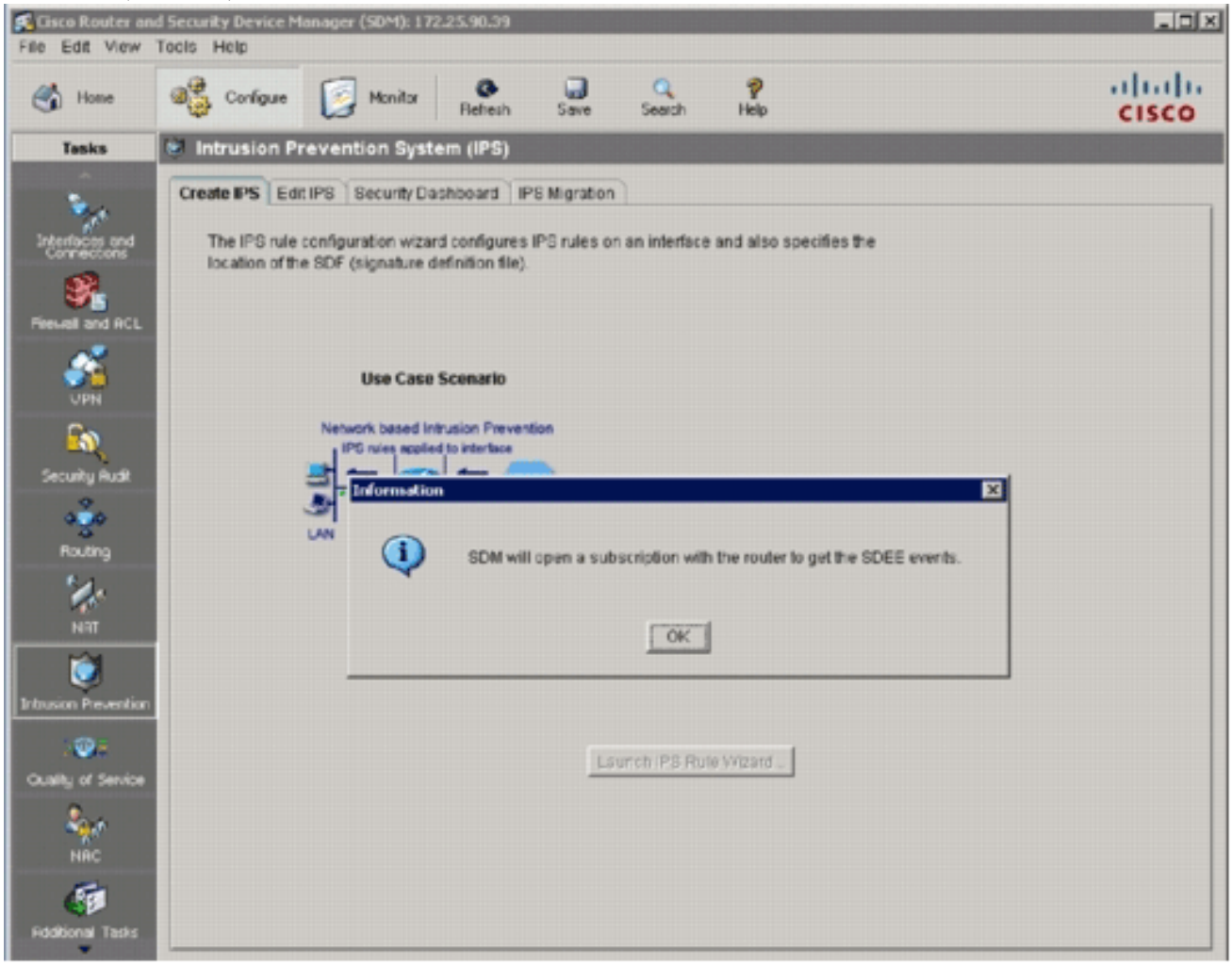
9. [CCO Login] ダイアログボックスが表示されたら、CCO 登録ユーザ名とパスワードを入力します。



SDM が Cisco.com に接続し、SDM ファイル（例：sigv5-SDM-S307.zip）と CLI pkg ファイル（例：IOS-S313-CLI.pkg）の両方を、ステップ 7 で選択したディレクトリにダウンロードします。両方のファイルのダウンロードが完了すると、SDM がダウンロードしたシグニチャ パッケージをルータにプッシュするかどうかを尋ねてきます。

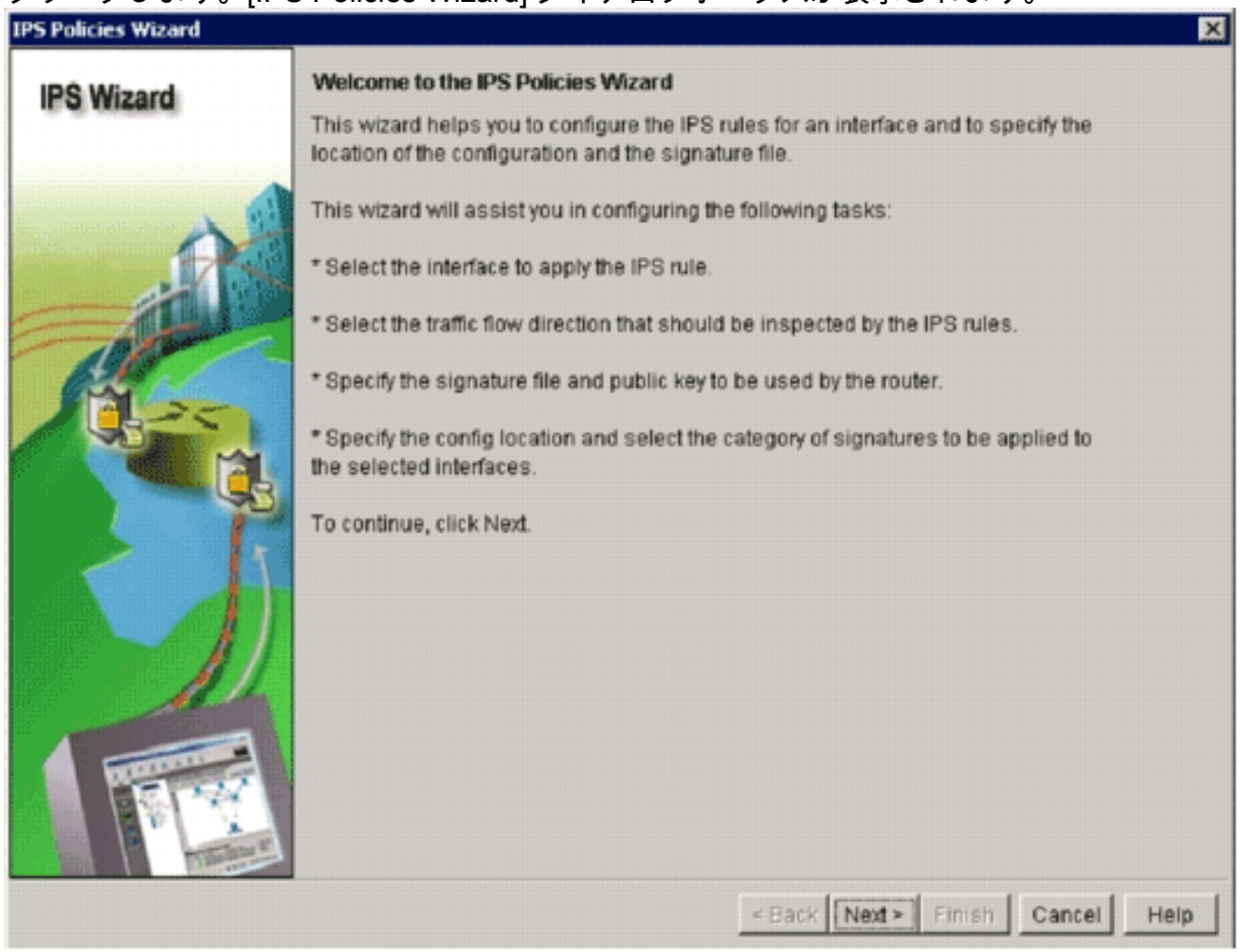


10. IOS IPS はまだルータに設定されていないため、[No] をクリックします。
11. SDM が最新の IOS CLI シグニチャ パッケージをダウロードした後、初期 IOS IPS 設定を作成するために、[Create IPS] **タブをクリックします。**
12. 変更をルータに適用するよう求められたら、[Apply Changes] をクリックします。
13. [Launch IPS Rule Wizard] をクリックします。ダイアログボックスが表示され、アラートを取得するには SDM がルータに対する SDEE サブスクリプションを確立する必要があることを通知します。

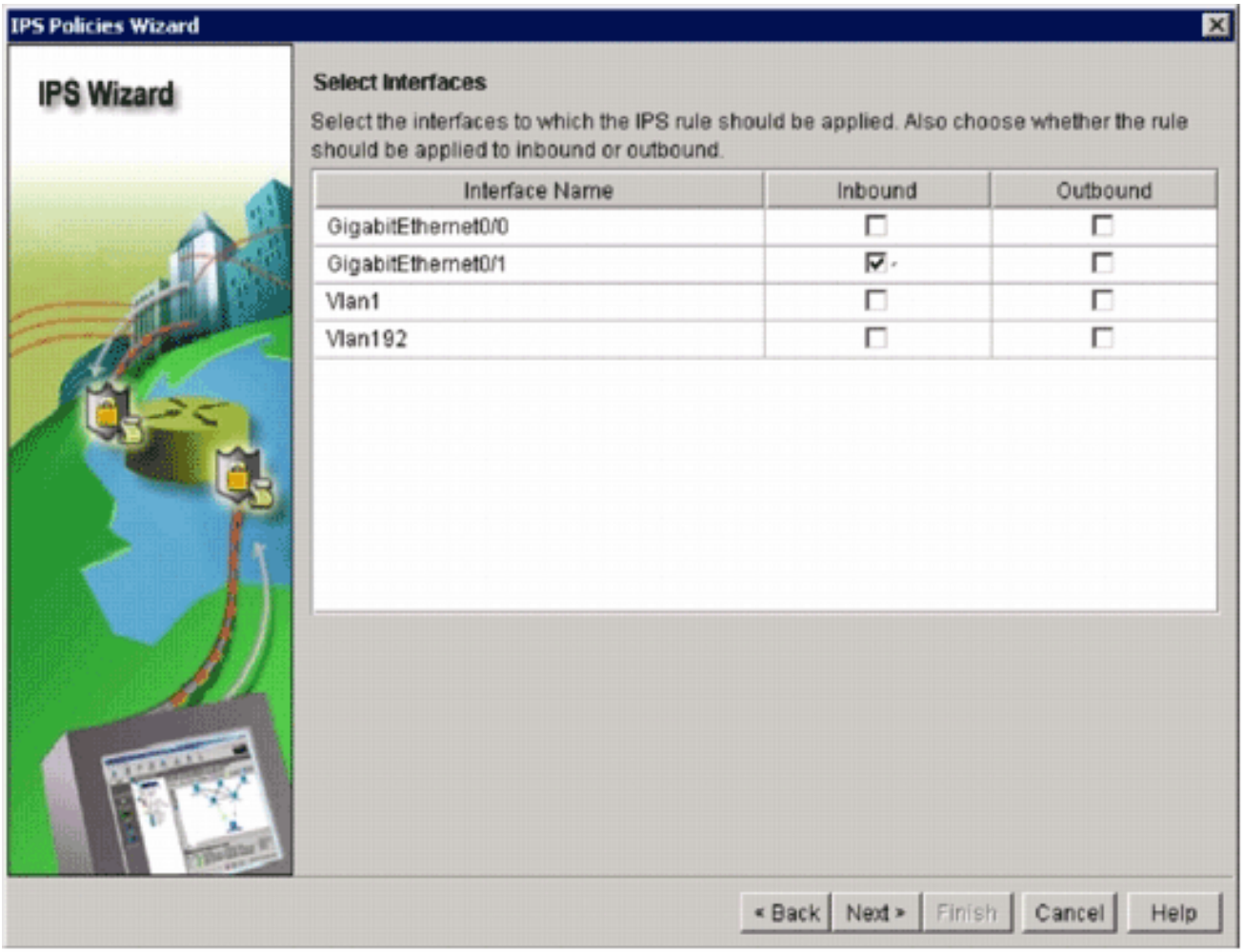


14. [OK] をクリックします。[Authentication Required] ダイアログボックスが表示されます。

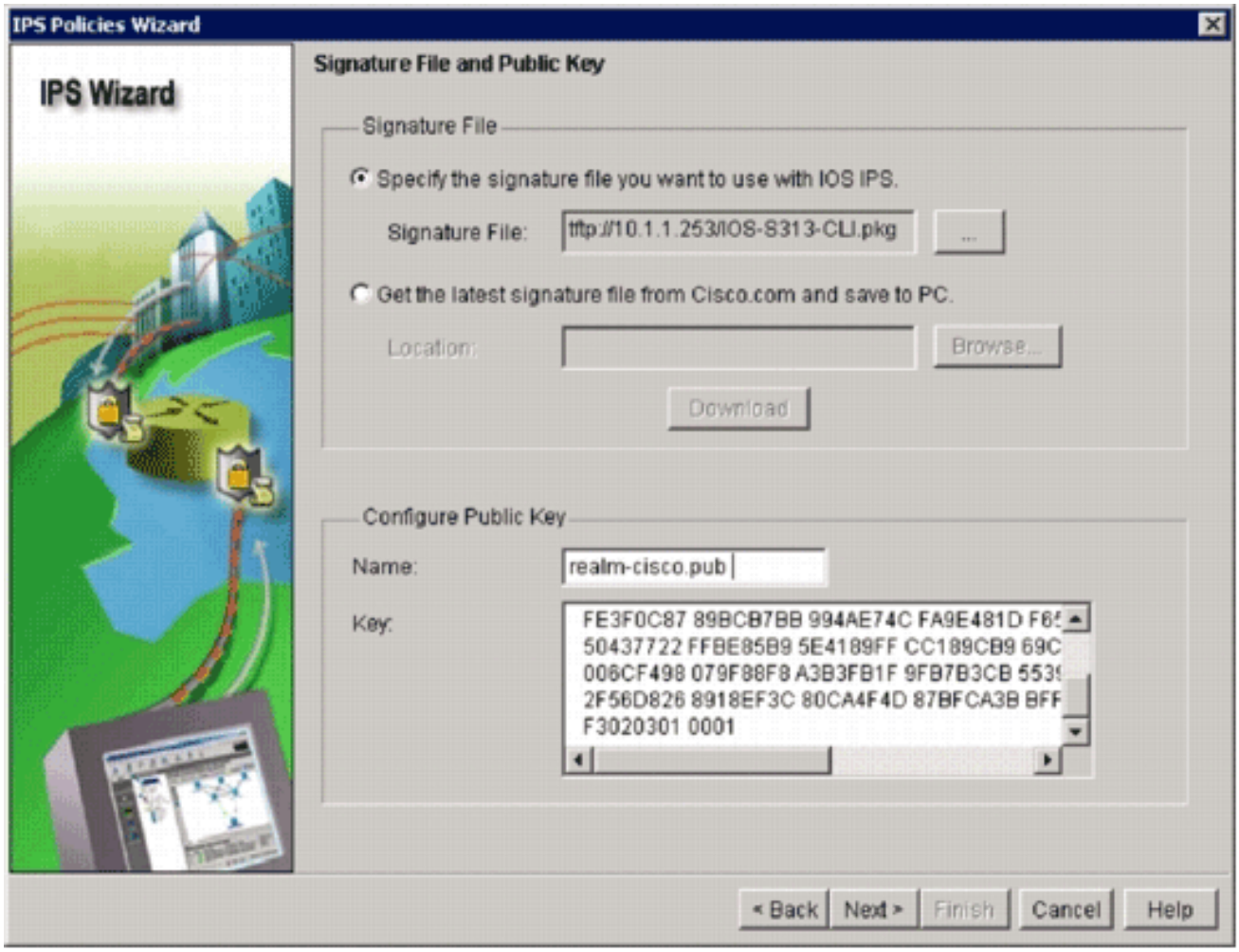
15. ルータに対して SDM を認証するために使用するユーザ名とパスワードを入力し、[OK] をクリックします。[IPS Policies Wizard] ダイアログボックスが表示されます。



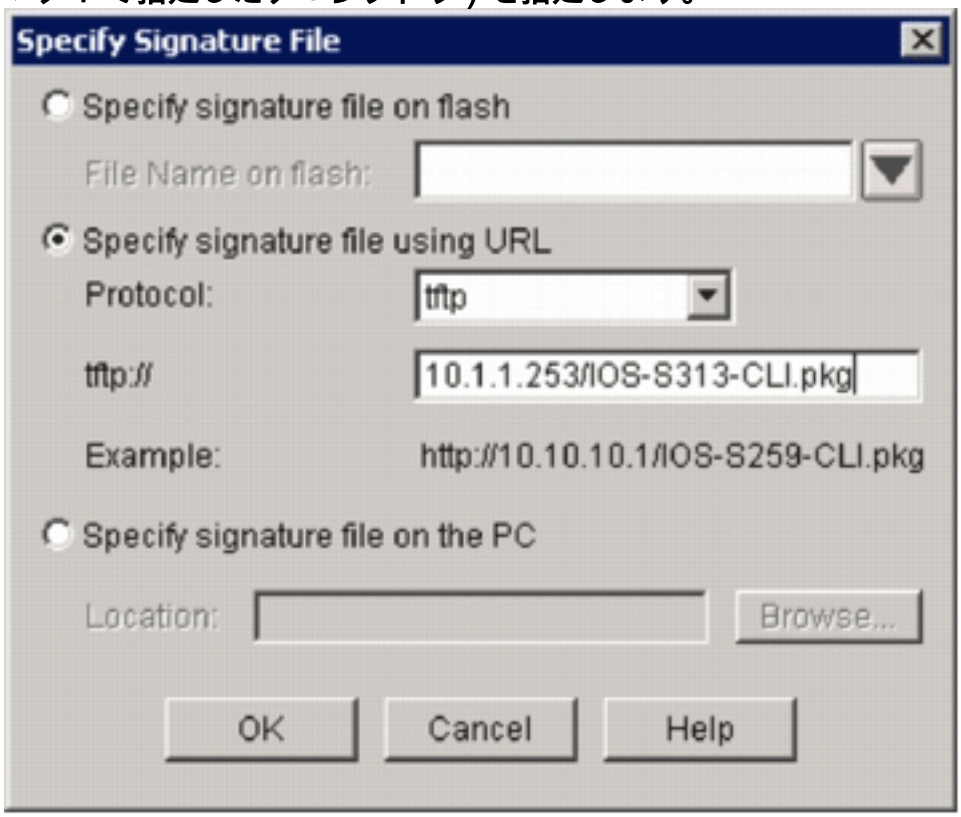
16. [next] をクリックします。



17. [Selected Interfaces] ウィンドウで、インターフェイスと、IOS IPS を適用する方向を選択し、[Next] **をクリックして続行します。**



18. [Signature File and Public Key] ウィンドウの [Signature File] 領域で、[Specify the signature file you want to use with IOS IPS] **オプション ボタンをクリックしてから [Signature File] ボタン (...) をクリックし、シグニチャ パッケージ ファイルの場所 (ステップ 7 で指定したディレクトリ) を指定します。**



19. [Specify signature file using URL] **オプション ボタンをクリックし、[Protocol] ドロップダ**

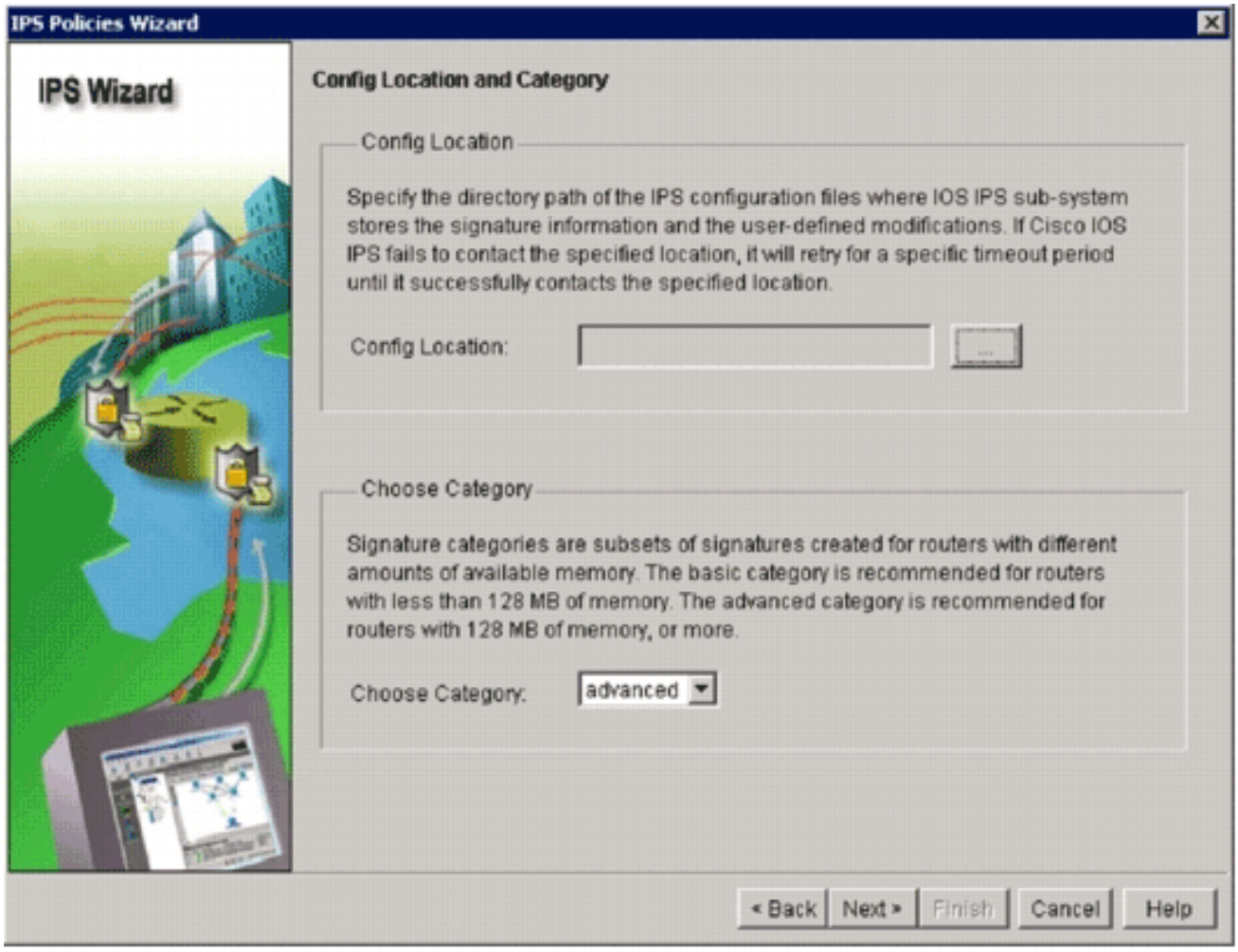
ウン リストからプロトコルを選択します。注：この例では、シグニチャパッケージをルータにダウンロードするためにTFTPを使用しています。

20. シグニチャ ファイルの URL を入力し、[OK] をクリックします。
21. [Signature File and Public Key] ウィンドウの [Configure Public Key] 領域で、[Name] フィールドに **realm-cisco.pub と入力してから、以下の公開キーをコピーして [Key] フィールドに貼り付けます。**

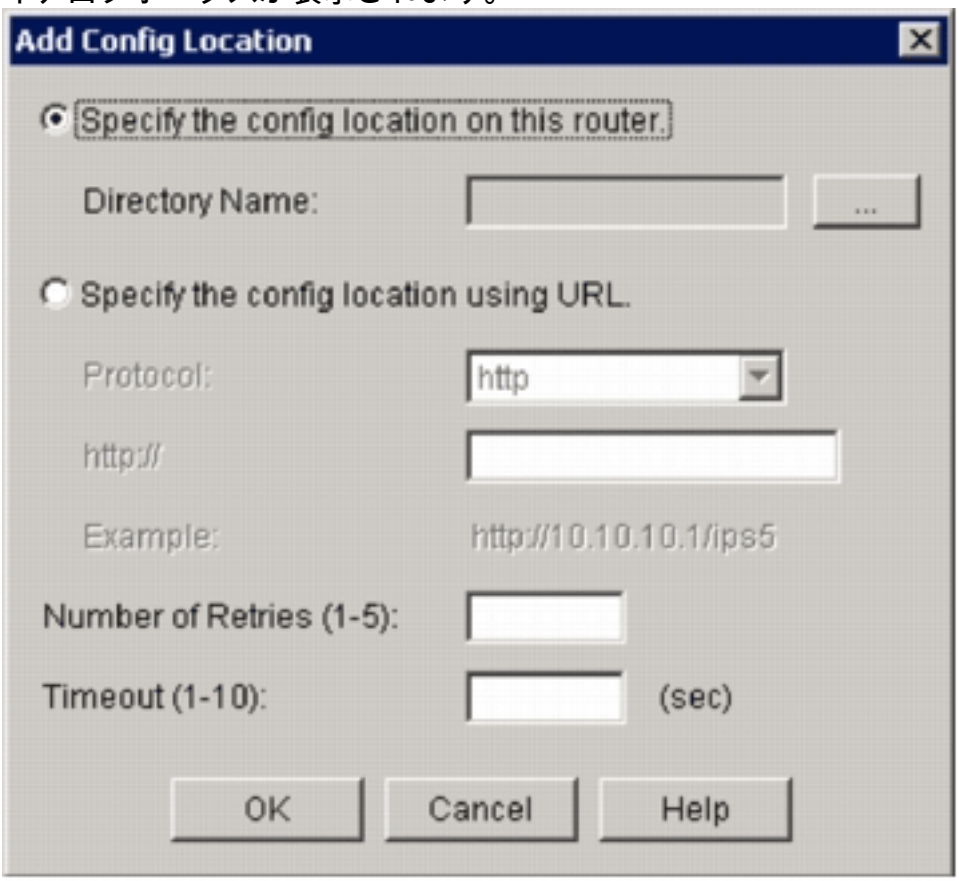
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

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
```

注： この公開キーは Cisco.com (http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup（登録ユーザ専用）)からダウロードできます。

22. [Next] をクリックして次に進みます。

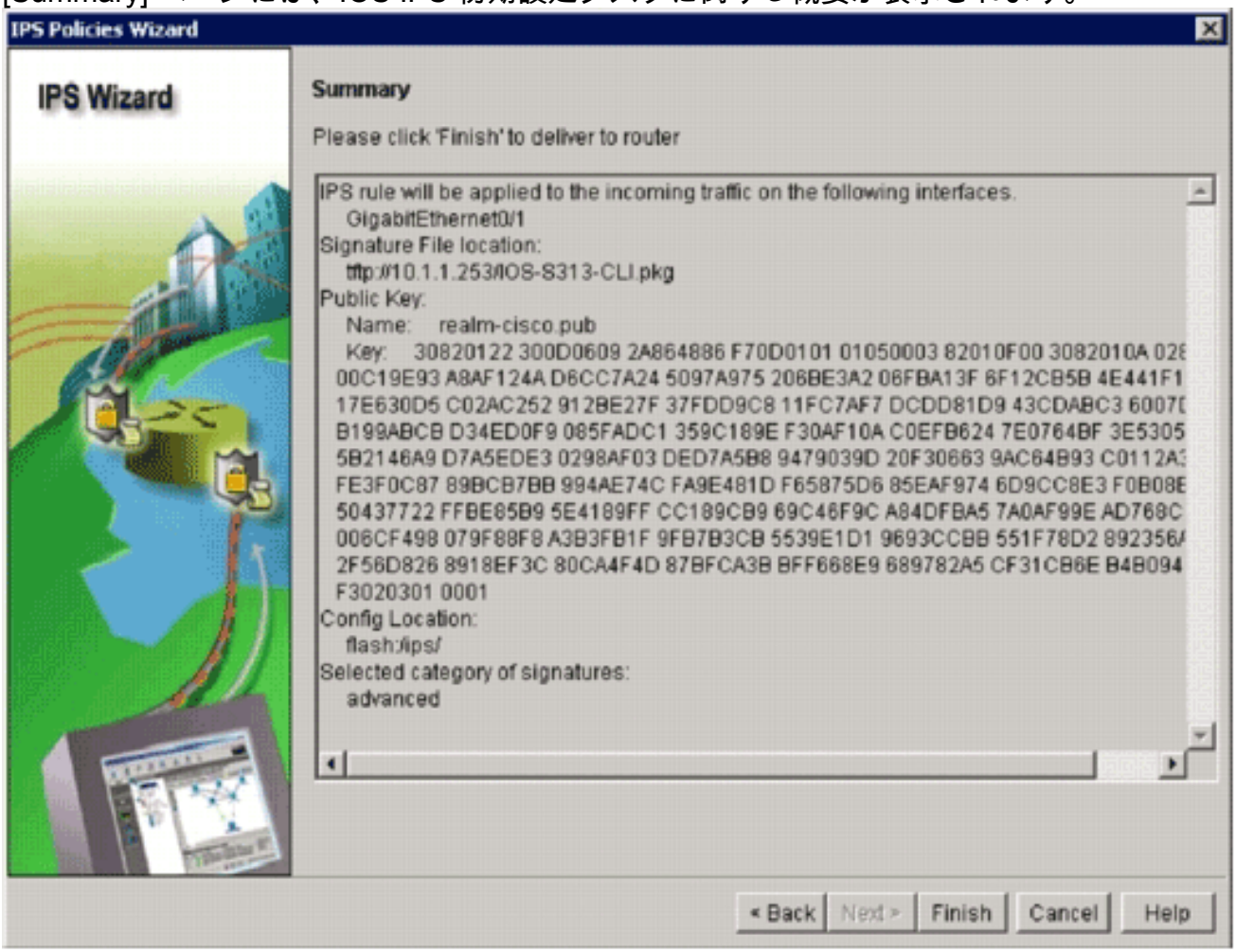


23. [Config Location and Category] ウィンドウで、[Config Location] **ボタン (...) をクリックし、シグニチャ定義と設定ファイルを保管する場所を指定します。**[Add Config Location] ダイアログボックスが表示されます。

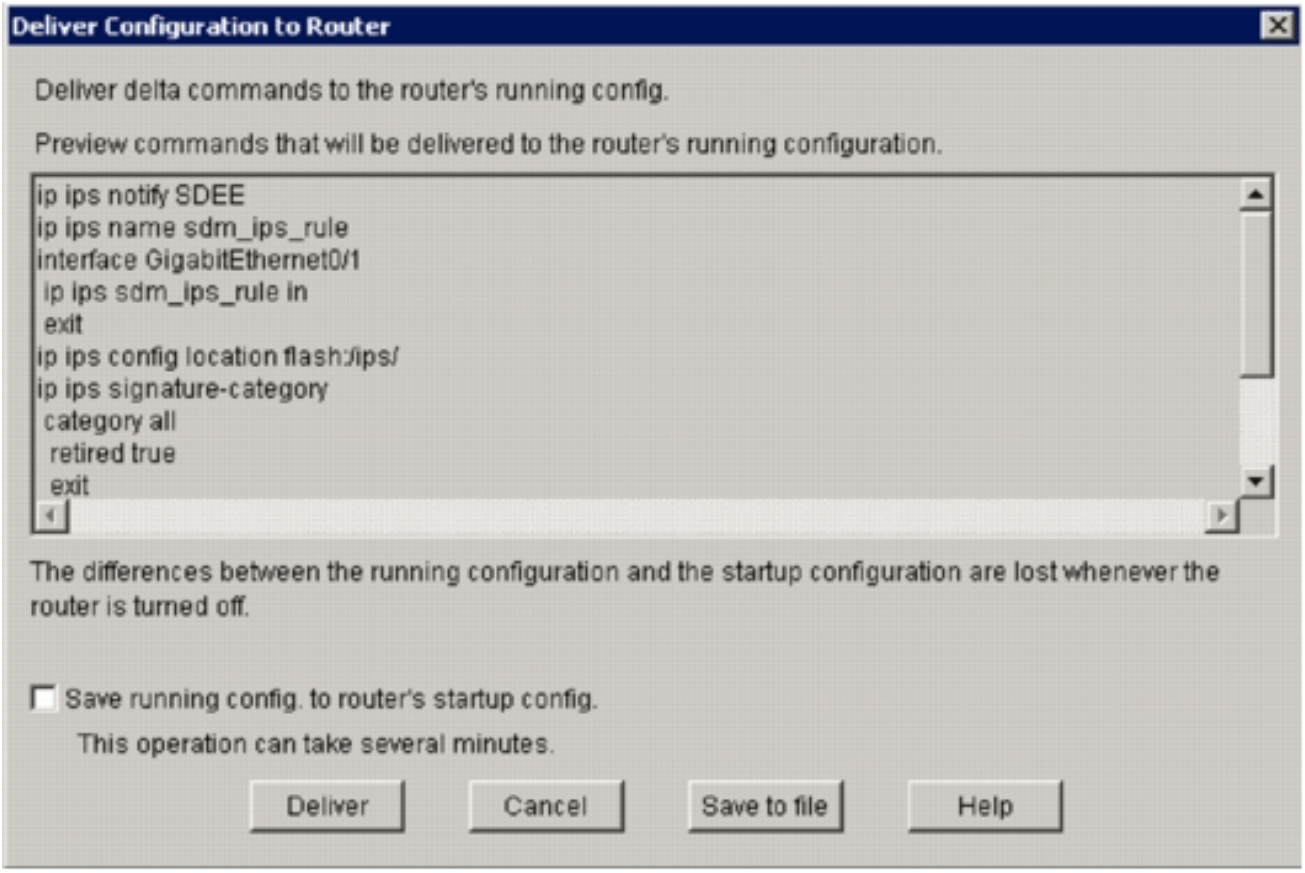


24. [Add Config Location] ダイアログボックスで、[Specify the config location on this router] **オプション ボタンをクリックしてから、設定ファイルの場所を指定するために [Directory Name] ボタン (...) をクリックします。**[Choose Folder] ダイアログボックスが表示されます。このダイアログボックスで、シグニチャ定義と設定ファイルを保管する場所として、既存のディレクトリを選択するか、ルータ フラッシュ上に新規ディレクトリを作成できます。

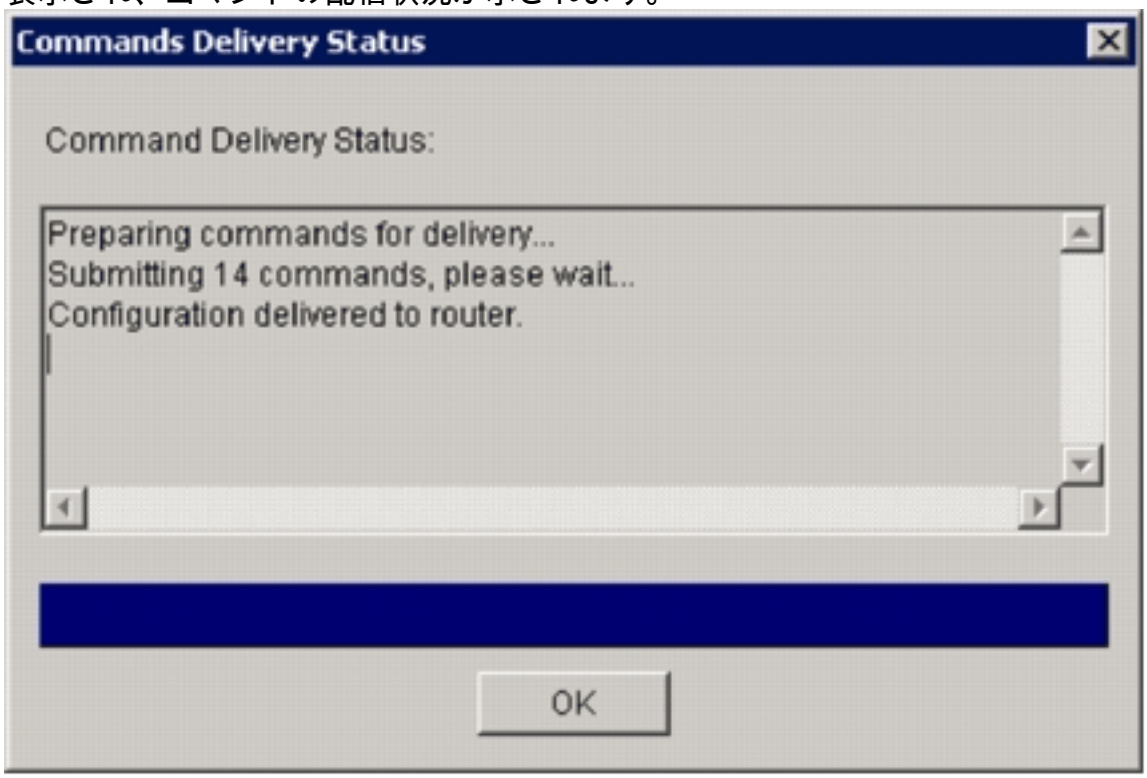
25. 新規ディレクトリを作成する場合は、ダイアログボックスの上部にある [New Folder] をクリックします。
26. ディレクトリを選択したら、[OK] をクリックして変更を適用してから、[OK] をクリックして [Add Config Location] ダイアログボックスを閉じます。
27. [IPS Policies Wizard] ダイアログボックスで、ルータにインストールされているメモリの量に応じてシグニチャ カテゴリを選択します。SDM で選択できるシグニチャ カテゴリは、[Basic] と [Advanced] の 2 つです。ルータにインストールされている DRAM が 128MB の場合、メモリ割り当ての失敗を避けるために [Basic] カテゴリを選択することを推奨します。ルータにインストールされている DRAM が 256MB を超えている場合は、どちらのカテゴリを選択しても構いません。
28. 使用するカテゴリを選択したら、[Next] をクリックして [Summary] ページに進みます。[Summary] ページには、IOS IPS 初期設定タスクに関する概要が表示されます。



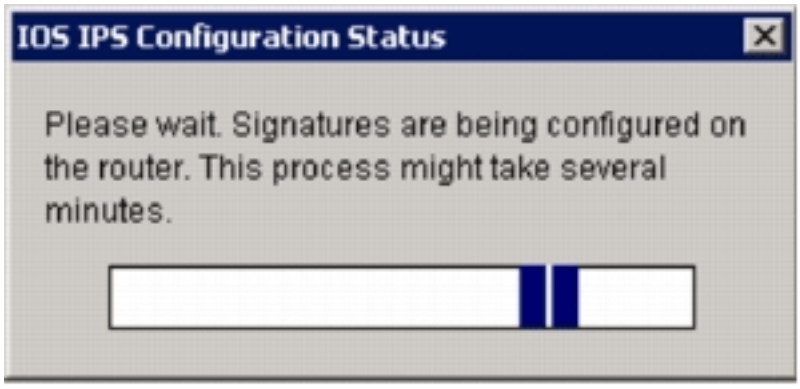
29. [Summary] ページで [Finish] をクリックすることによって、設定およびシグニチャ パッケージをルータに配信します。SDM の [Preferences] 設定でプレビュー コマンド オプションが有効になっている場合、SDM に、SDM がルータに配信する CLI コマンドの要約を示す [Deliver Configuration to Router] ダイアログボックスが表示されます。



30. [Deliver] をクリックして続行します。[Commands Delivery Status] ダイアログボックスが表示され、コマンドの配信状況が示されます。

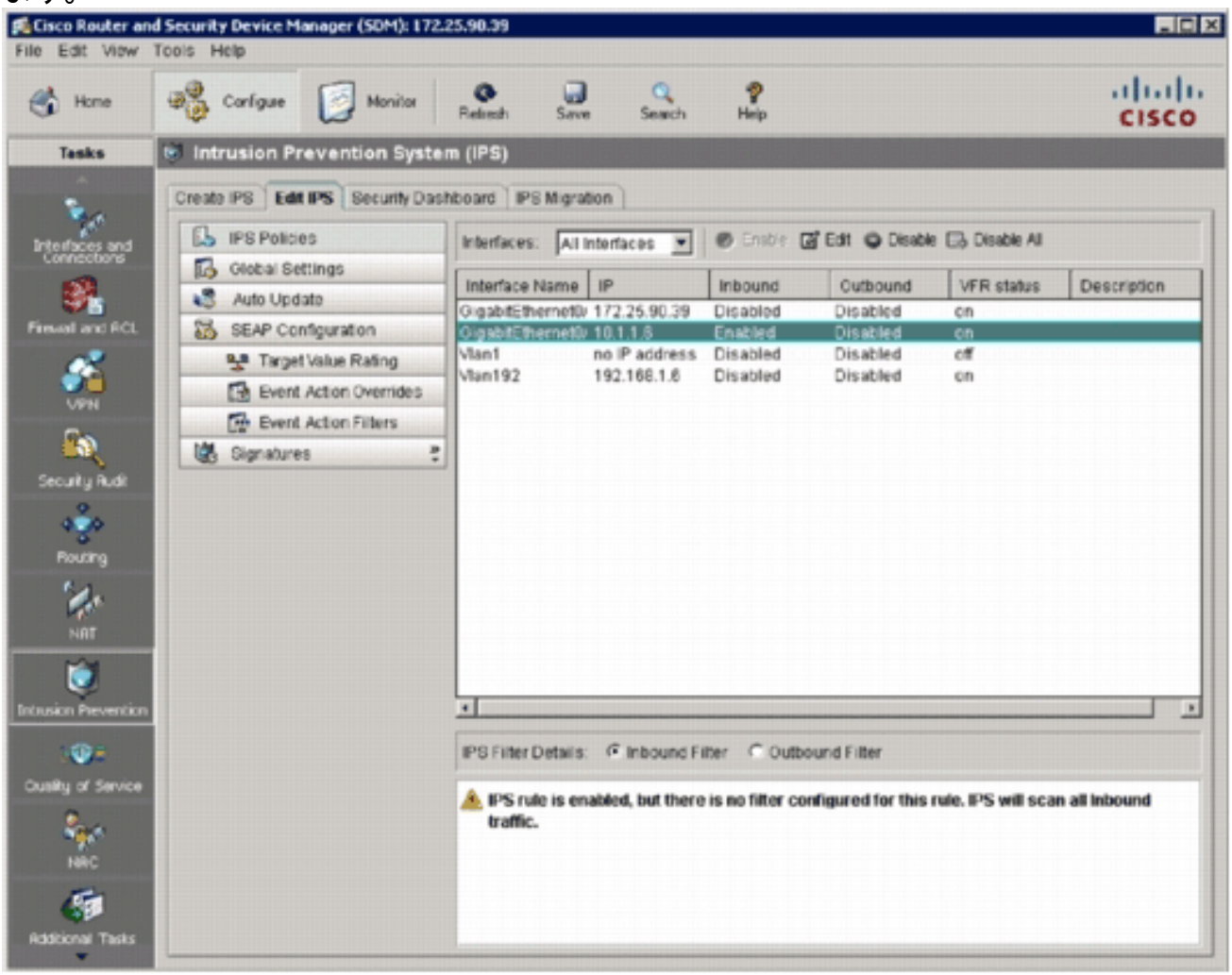


31. コマンドがルータに配信されたら、[OK] をクリックして続行します。[IOS IPS Configuration Status] ダイアログボックスに、ルータにロード中のシグニチャが表示されま

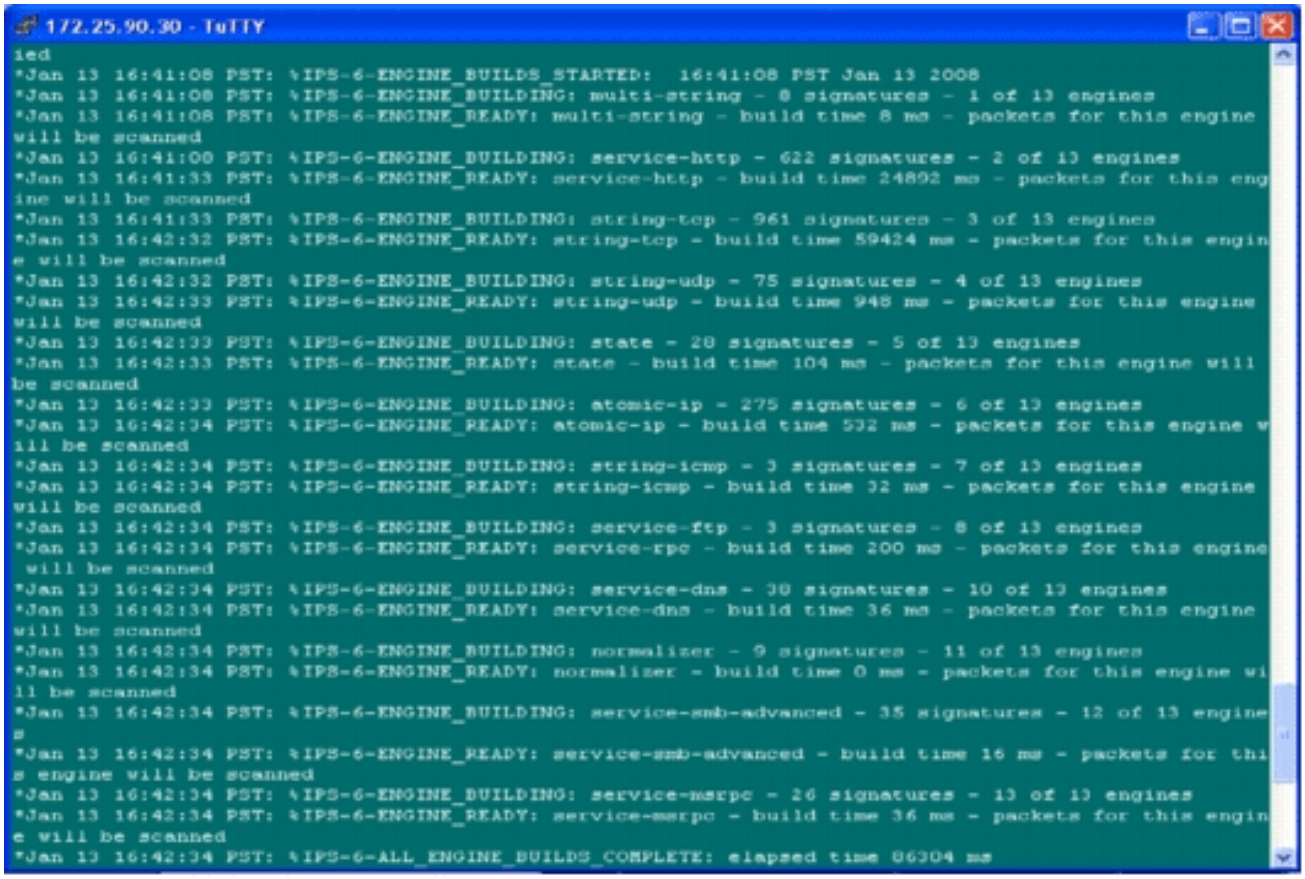


す。

32. シグニチャがロードされると、SDM の [Edit IPS] タブに現在の設定が表示されます。IOS IPS がどのインターフェイスのどの方向で有効になっているのかを調べて、設定を検証します。



ルータ コンソールに、シグニチャがロードされたことが示されます。

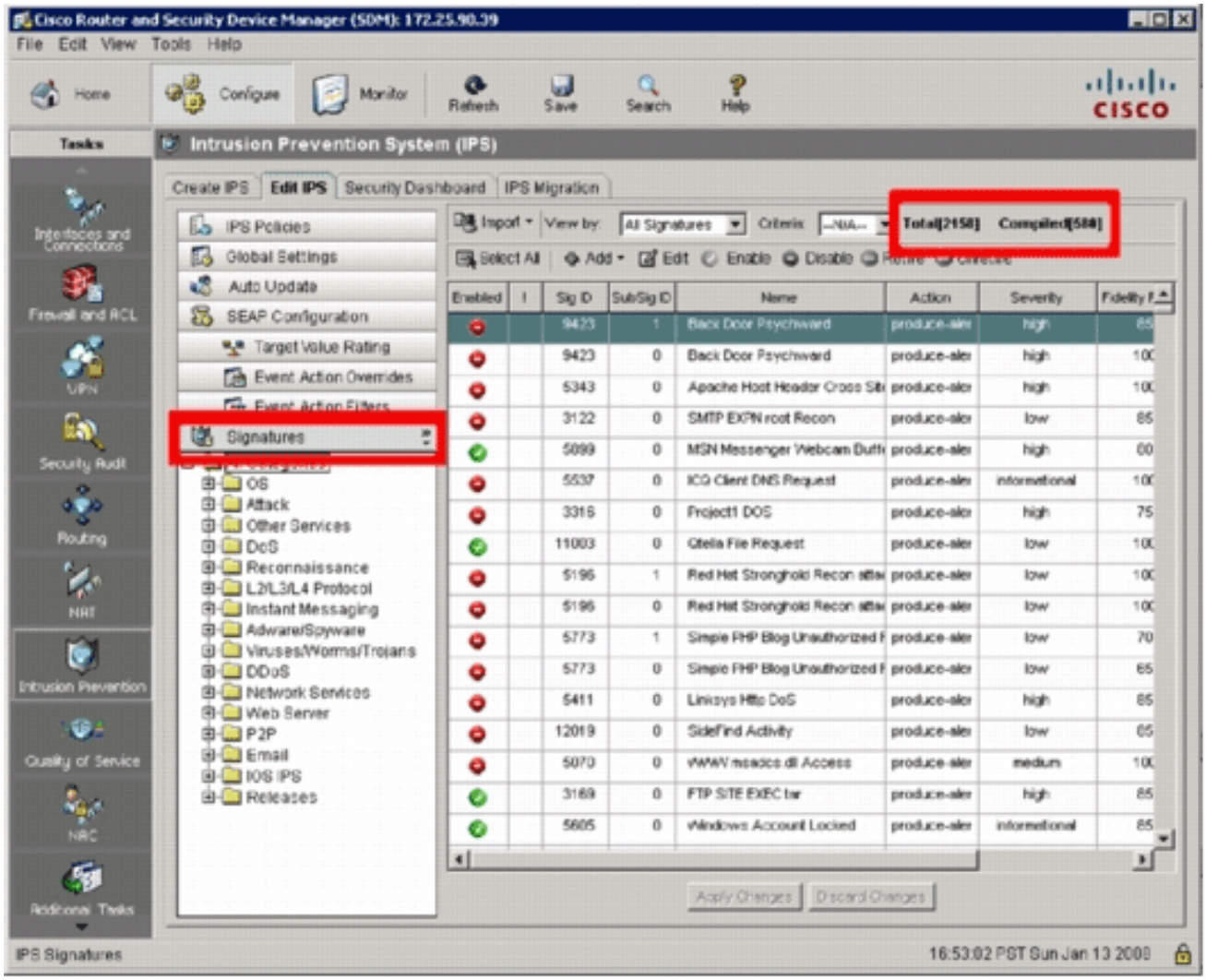


33. **show ip ips signatures count コマンドを使用して、シグニチャ パッケージが適切にロードされていることを検証します。**

```
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
```

これで、SDM 2.5 を使用した IOS IPS の初期プロビジョニングが完了しました。

34. SDM で、次の図に示すシグニチャ番号を確認してください。



関連情報

- Cisco.com の Cisco IOS IPS
- Cisco IOS IPS シグニチャ パッケージ
- SDM 用 Cisco IOS IPS シグニチャ ファイル
- 5.x シグニチャ形式を使用した Cisco IOS IPS の導入
- Cisco IOS IPS Configuration Guide
- Cisco IDS イベント ビューア
- テクニカル サポートとドキュメント – Cisco Systems