Пример настройки маршрутизатора и диспетчера устройств безопасности в системе предотвращения атак (IPS) Cisco IOS

Содержание

Введение

Этот документ описывает, как использовать Cisco Router and Security Device Manager (SDM) версия 2.5 для настройки Cisco IOS® Intrusion Prevention System (IPS) в 12.4 (15) T3 и более поздние версии.

Усовершенствования в SDM 2.5, отнесенном к IPS IOS:

- Общий скомпилированный номер подписи отобразился в GUI списка подписи
- Файлы цифровой подписи SDM (формат файла архива zip; например, sigv5-SDM-S307.zip) и пакеты подписи CLI (pkg формат файла; например, IOS-S313-CLI.pkg), может быть загружен вместе в одной операции
- Загруженные пакеты подписи могут быть выдвинуты автоматически к маршрутизатору как опция

Задачи, вовлеченные в начальный процесс инициализации:

1. Загрузка и SDM 2.5 установки.
2. Используйте Автоматическое обновление SDM для загрузки пакета подписи IPS IOS к локальному компьютеру.
3. Запустите Мастера Политики IPS для настройки IPS IOS.
4. Проверьте, что должным образом загружены конфигурация IPS IOS и подписи

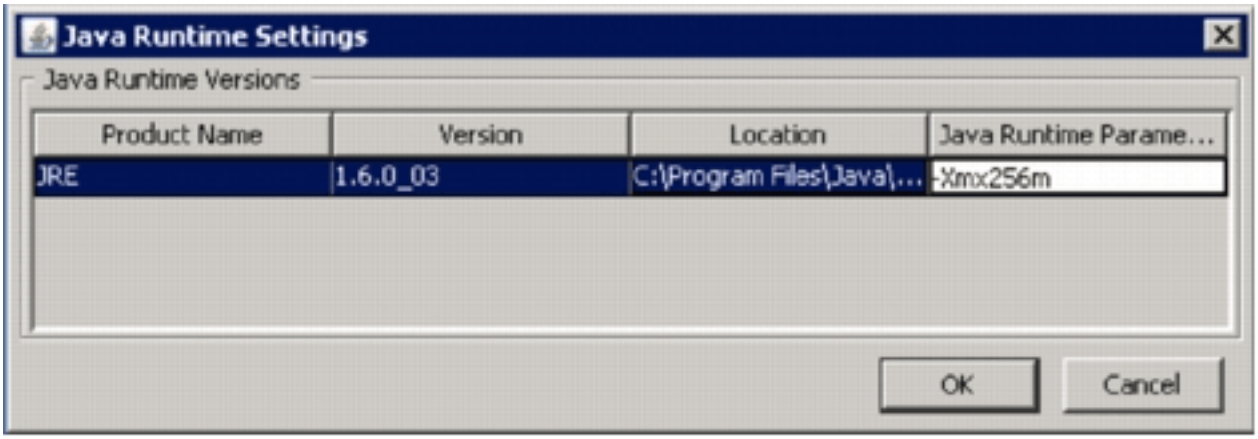
SDM Cisco является находящимся на web средством конфигурации, которое упрощает маршрутизатор и конфигурацию безопасности через умных мастеров, которые помогают клиентам быстро и легко развертывают, настраивают и контролируют маршрутизатор Cisco, не требуя знания интерфейса командной строки (CLI).

Версия 2.5 SDM может быть загружена от Cisco.com в http://www. cisco . com/pcgi-bin/tablebuild.pl/sdm (только зарегистрированные клиенты). Комментарии к выпуску могут

быть найдены в http://www. cisco . com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

Примечание: SDM Cisco требует разрешения экрана по крайней мере 1024 x 768.

Примечание: SDM Cisco требует, чтобы размер динамически распределяемой области памяти Java составил не менее чем 256 МБ, для настройки IPS IOS. Для изменения размера динамически распределяемой области памяти Java откройте Панель управления Java, нажмите вкладку **Java**, нажмите **View**, расположенный при Параметрах настройки Времени выполнения приложения Java, и затем введите**-Xmx256m** в Столбец параметров Среды исполнения Java.



Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- IPS Cisco IOS в 12.4 (15) T3 и более поздние версии
- Cisco Router and Security Device Manager (SDM) версия 2.5

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

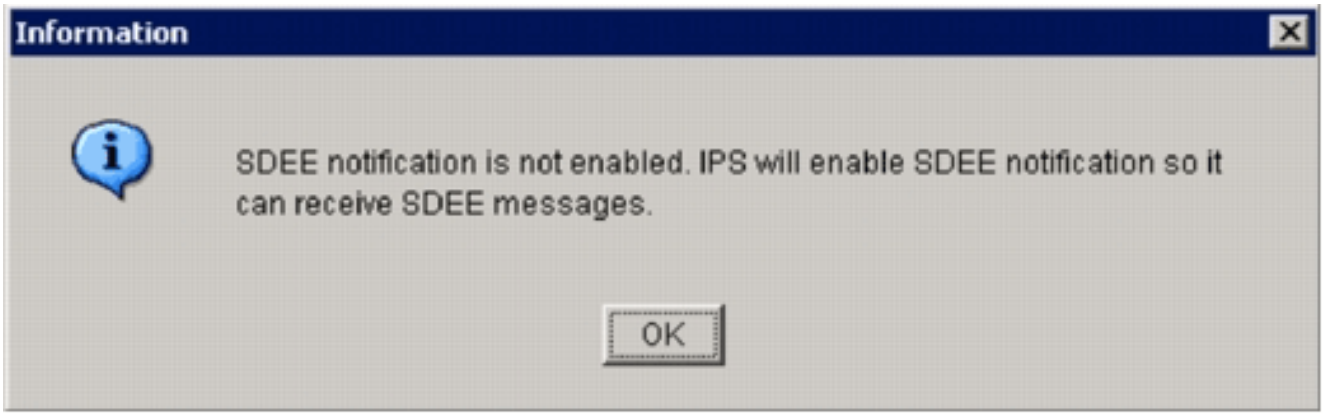
Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

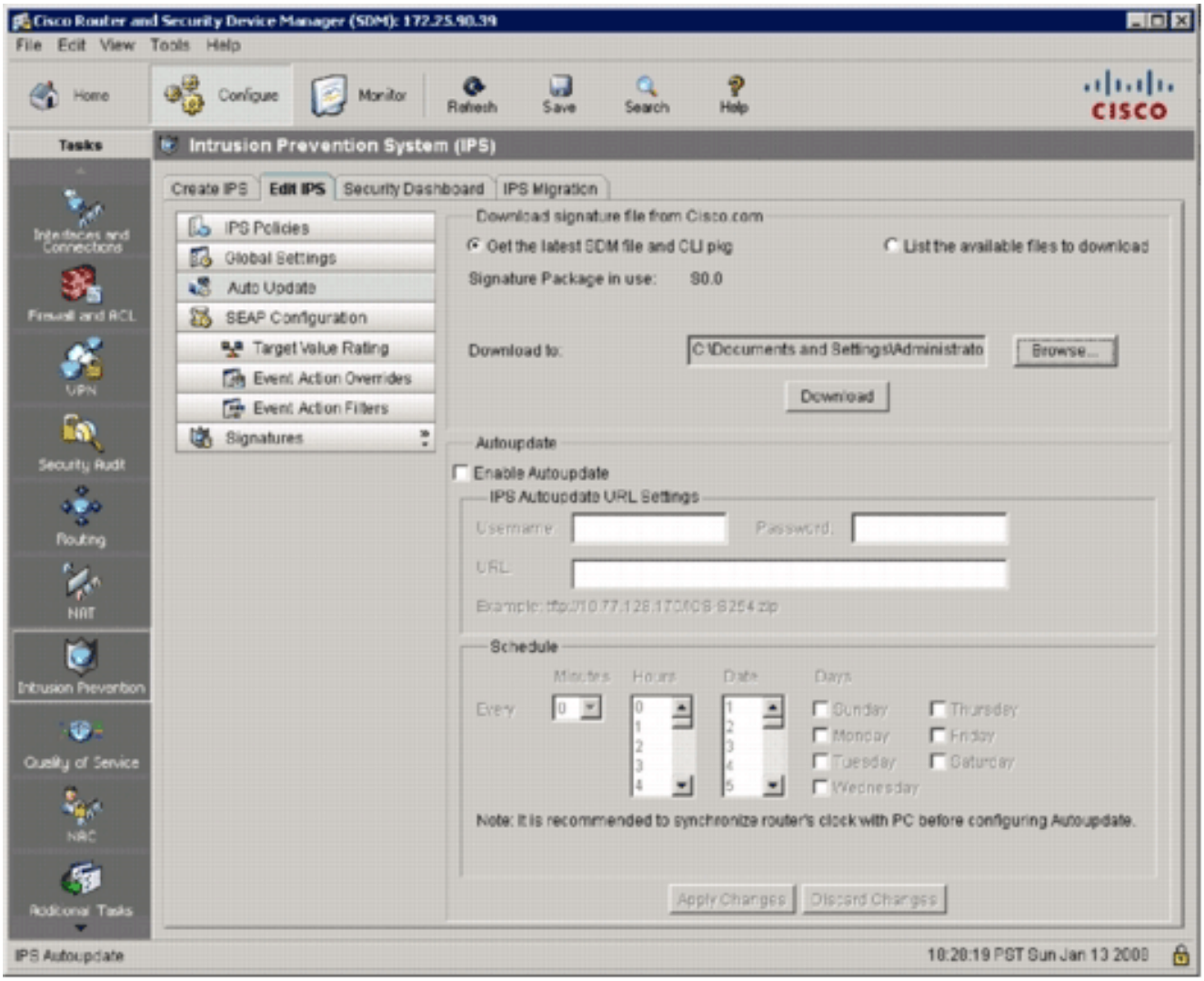
Примечание: Откройте сеанс консоли или Telnet для маршрутизатора (с 'монитором условия' на) для мониторинга сообщений при использовании SDM для инициализации IPS IOS.

1. SDM 2.5 загрузки от Cisco.com в http://www. cisco . com/pcgi-bin/tablebuild.pl/sdm (только зарегистрированные клиенты) и устанавливают его на локальном компьютере.
2. Выполните SDM 2.5 от локального компьютера.
3. Когда диалоговое окно IOS IPS Login появляется, введите то же имя пользователя и пароль, которое вы используете для аутентификации SDM для маршрутизатора.

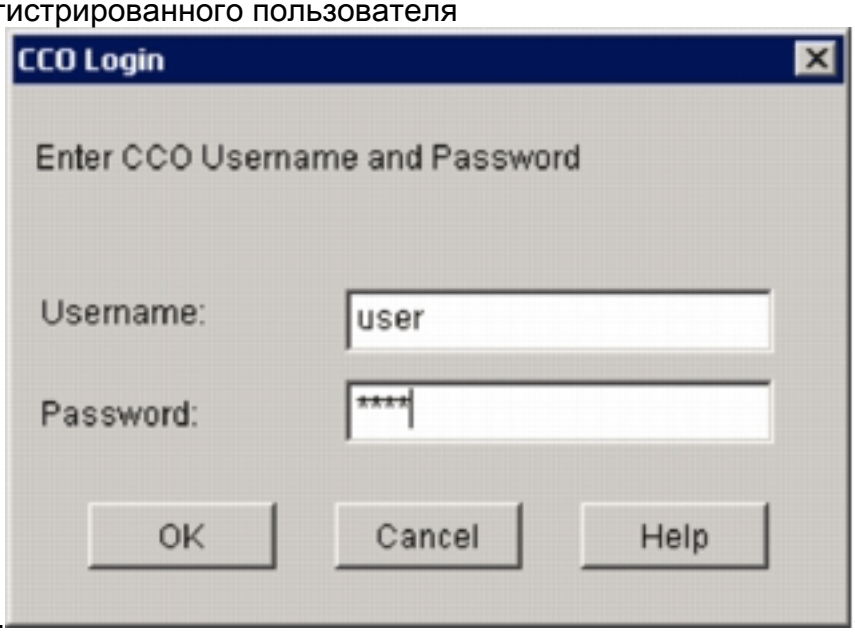
4. От интерфейса пользователя SDM нажмите **Configure**, и затем нажмите **Intrusion Prevention**.
5. Нажмите вкладку **Edit IPS**.
6. Если уведомление SDEE не включено на маршрутизаторе, нажмите **OK** для включения уведомления SDEE.



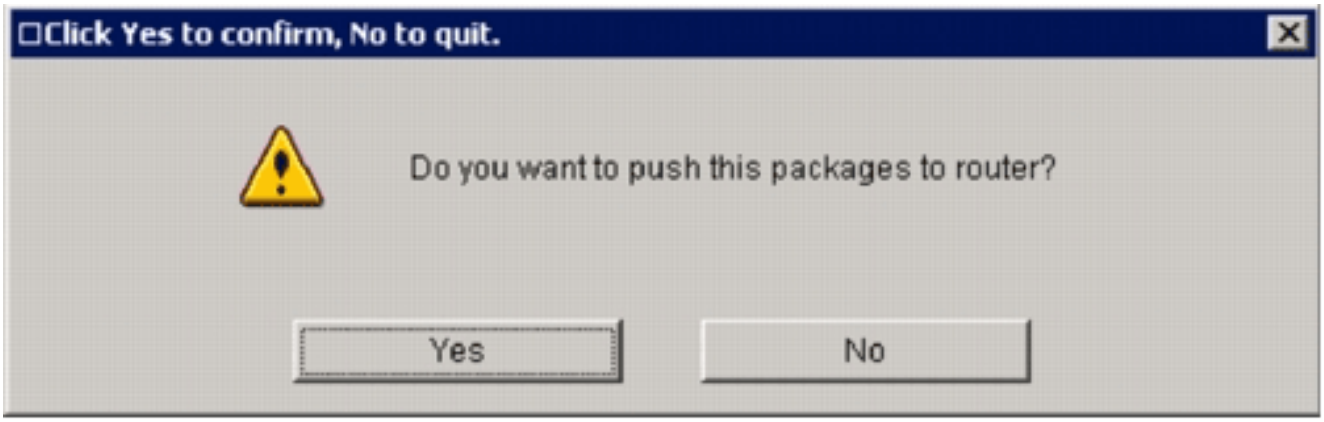
7. В Файле цифровой подписи Загрузки от области Cisco.com вкладки Edit IPS нажмите **Get последний файл SDM и CLI pkg** кнопка с зависимой фиксацией, и затем нажмите **Browse** для выбора каталога на локальном компьютере, в котором можно сохранить загружаемые файлы.Можно выбрать TFTP или корневой каталог сервера FTP, который будет использоваться позже, когда вы развернете пакет подписи на маршрутизаторе.
8. Нажмите **Download**.



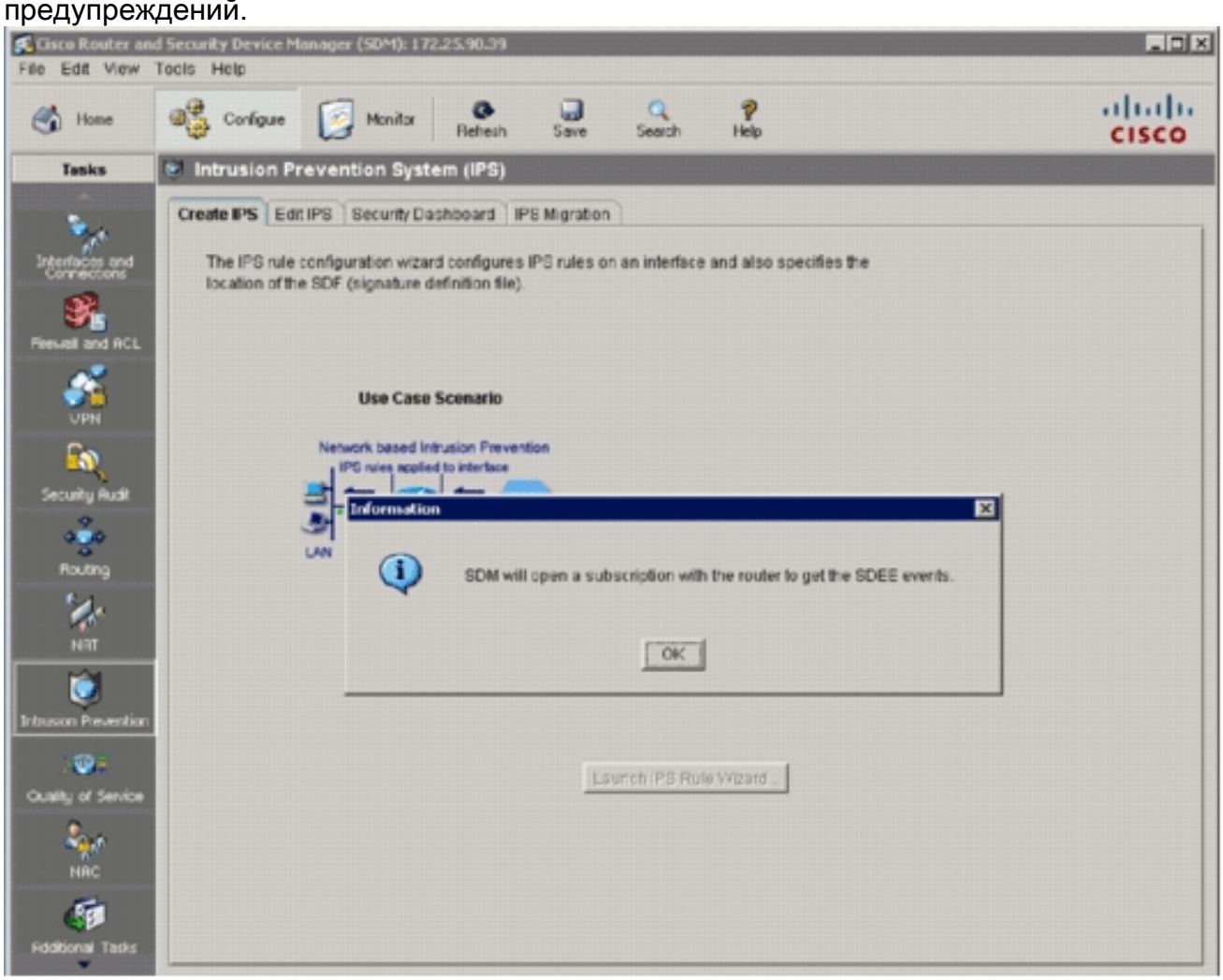
9. Когда диалоговое окно CCO Login появится, используйте свое имя и пароль зарегистрированного пользователя



CCO. SDM соединяется с Cisco.com и начинает загружать обоих файл SDM (например, sigv5-SDM-S307.zip) и CLI pkg файл (например, IOS-S313-CLI.pkg) к каталогу, выбранному в шаге 7.Как только оба файла загружены, SDM побуждает вас выдвигать загруженный пакет подписи к маршрутизатору.



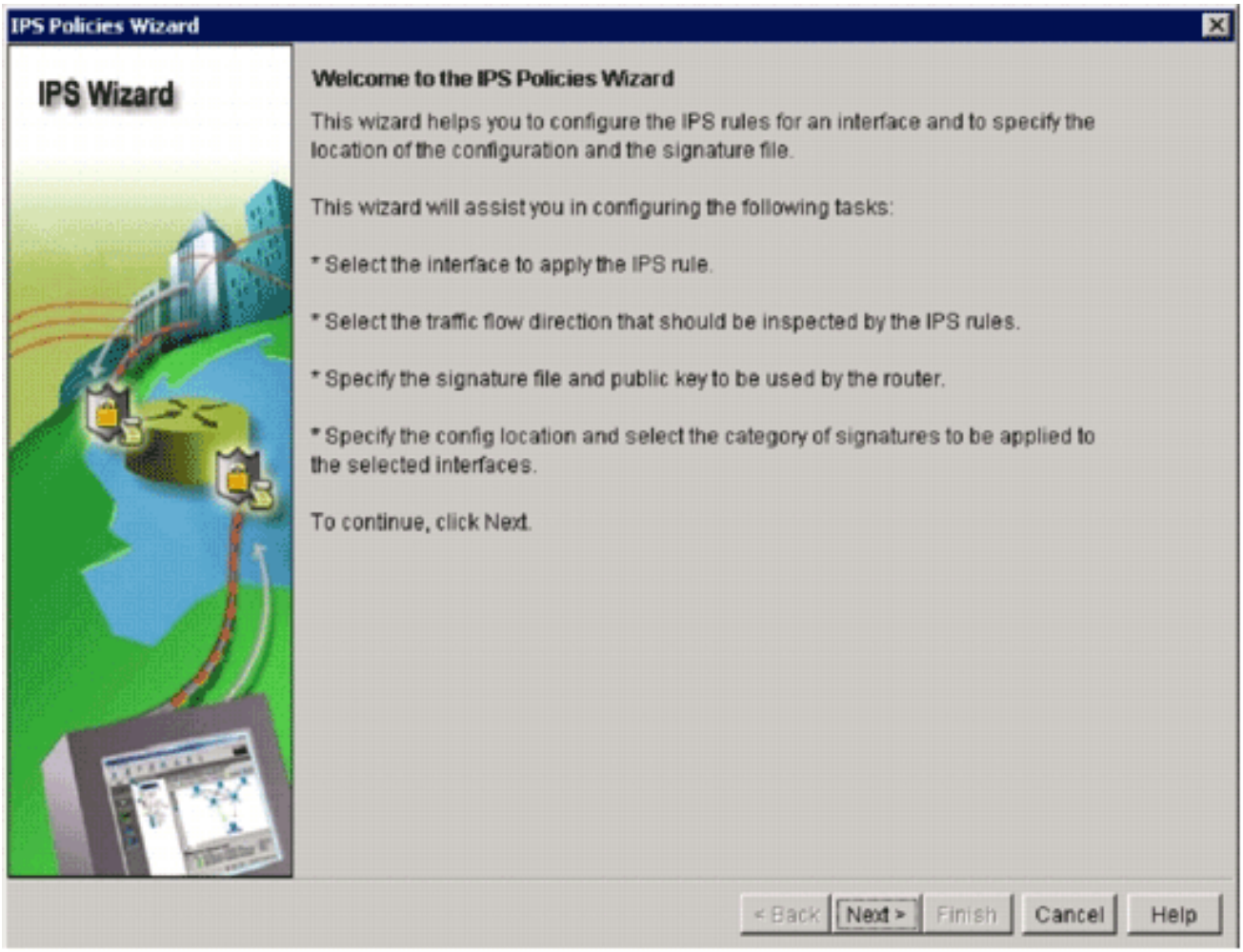
10. Нажмите **No**, так как IPS IOS еще не был настроен на маршрутизаторе.
11. После того, как SDM загружает последний пакет подписи интерфейса командной строки IOS, нажмите вкладку **Create IPS** для создания начальной конфигурации IPS IOS.
12. Если вам предлагают применить изменения к маршрутизатору, нажмите **Apply Changes**.
13. Нажмите **Launch IPS Rule Wizard**.Диалоговое окно, кажется, сообщает вам, что SDM должен установить подписку SDEE к маршрутизатору для получения предупреждений.



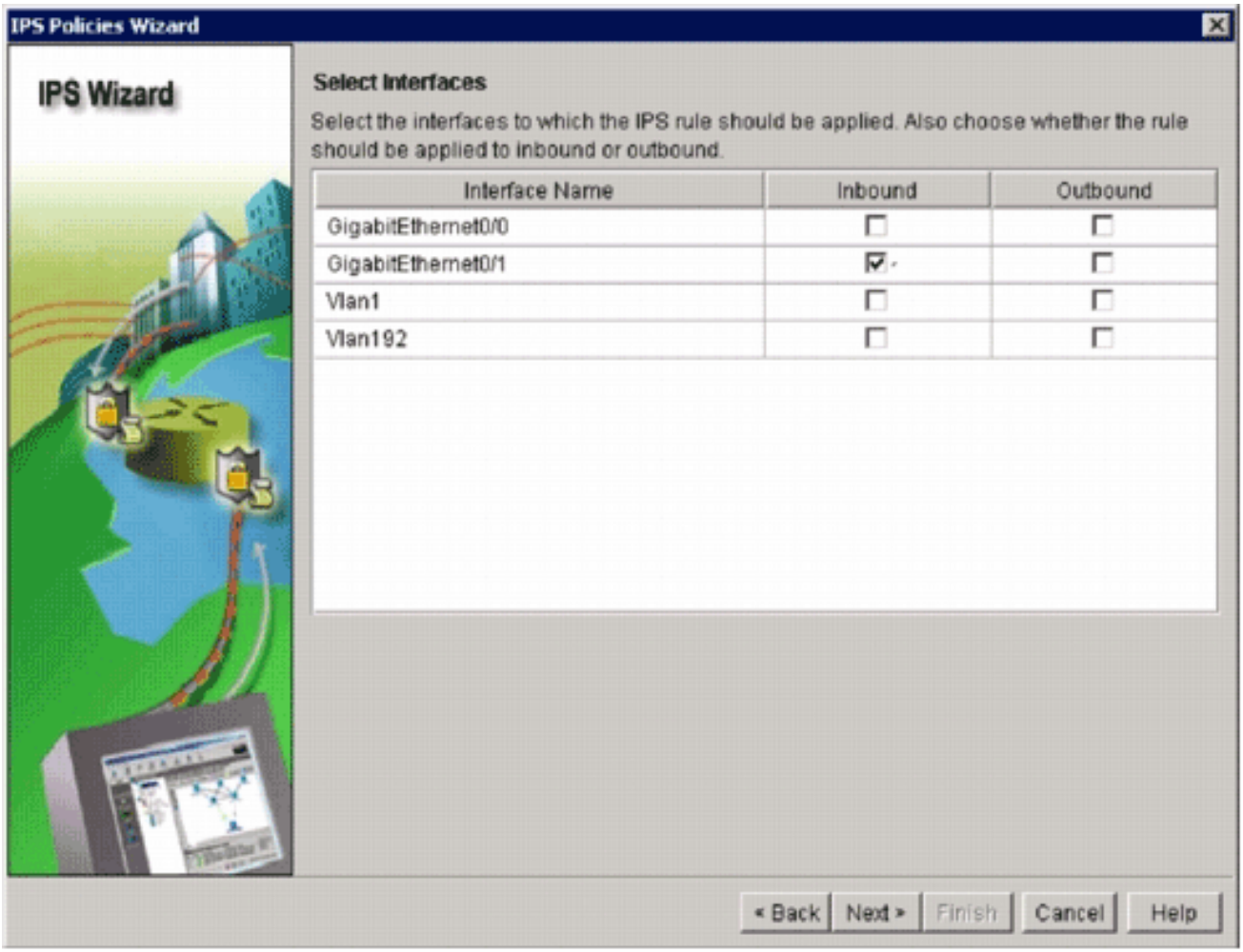
14. **Нажмите кнопку ОК.**Диалоговое окно Authentication Required

появляется.

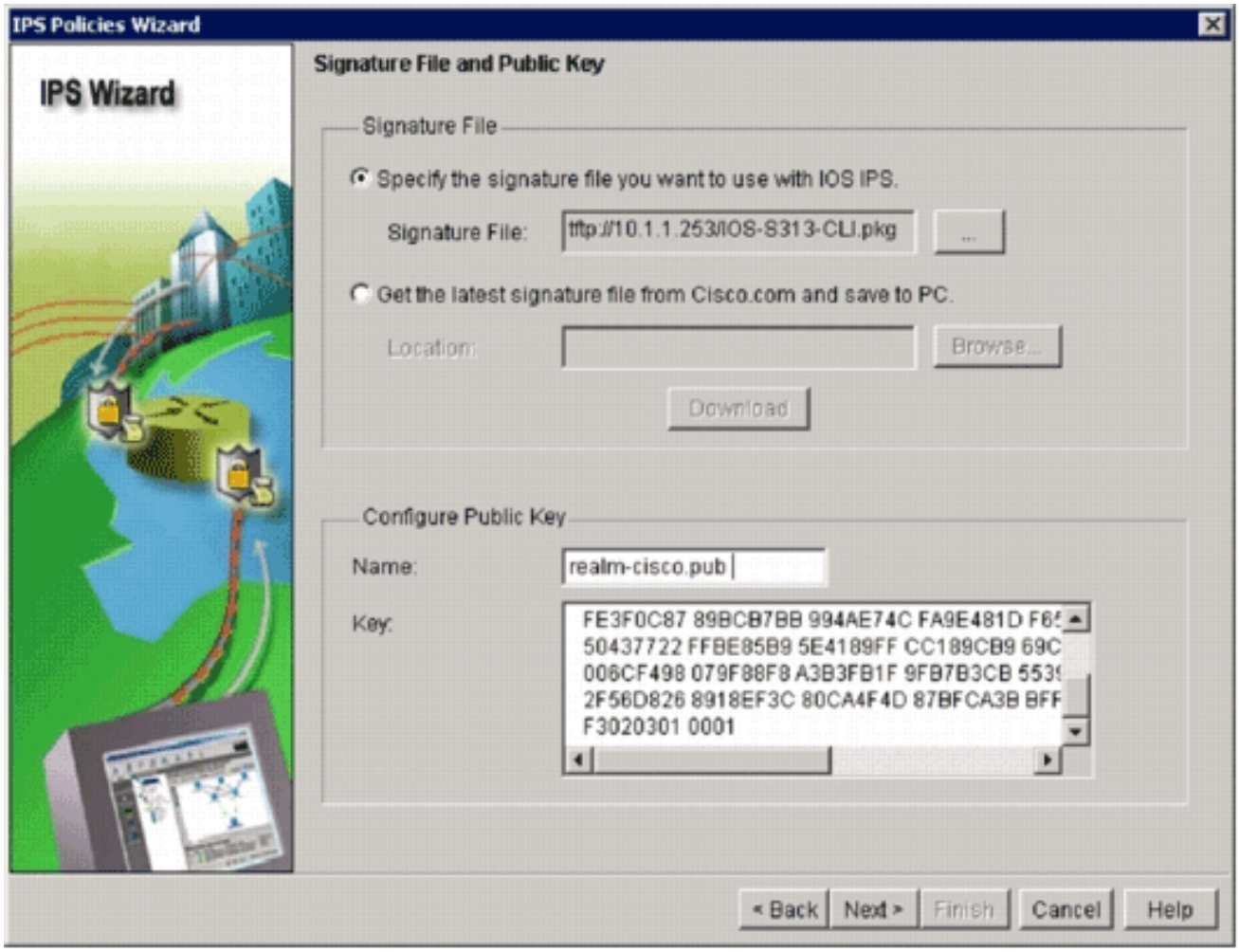
15. Введите имя пользователя и пароль, которое вы использовали для SDM аутентифицировать на маршрутизаторе и нажимать **OK**.Диалоговое окно IPS Policies Wizard
появляется.



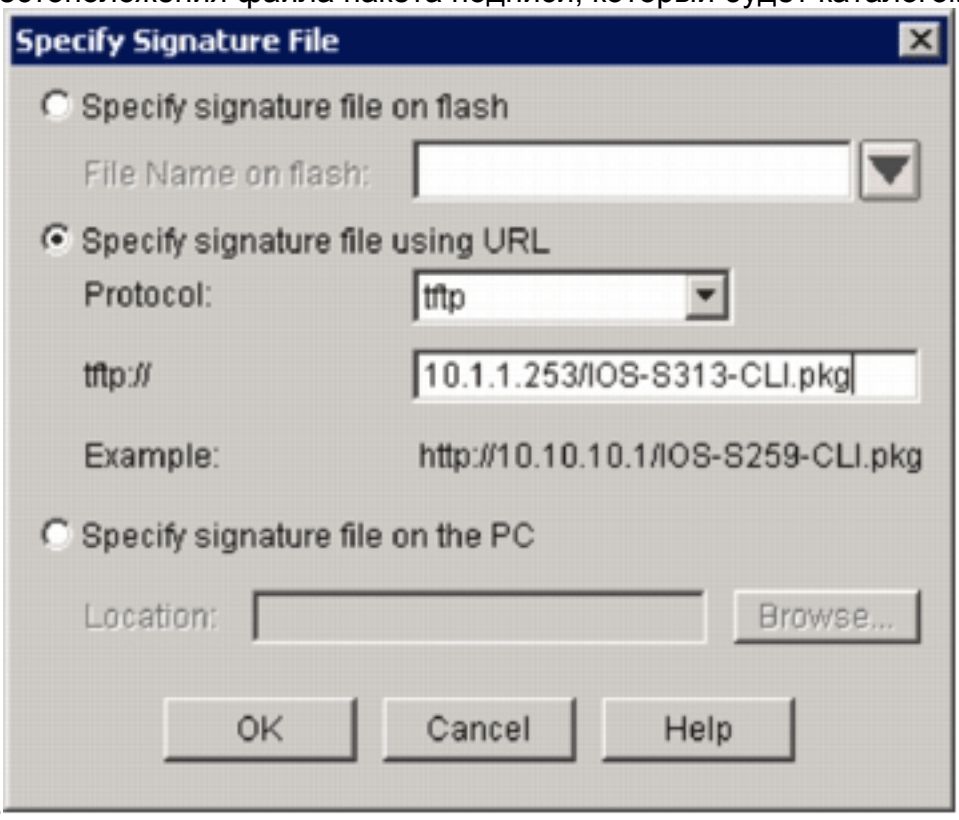
16. Нажмите кнопку **Next.**



17. В окне Selected Interfaces выберите интерфейс и направление, к которому тот IPS IOS будет применен, и затем нажимать **Next** для продолжения.



18. В области Signature File окна Signature File и Public Key нажмите **Specify Файл цифровой подписи, который вы хотите использовать с** кнопкой с зависимой фиксацией **IOS IPS**, и затем нажать кнопку **Signature File** (...) для определения местоположения файла пакета подписи, который будет каталогом, заданным в шаге 7.



19. Нажмите **Файл цифровой подписи Specify с помощью** кнопки с зависимой фиксацией

URL и выберите протокол из выпадающего списка Протокола.**Примечание:** Данный пример использует TFTP для загрузки пакета подписи к маршрутизатору.

20. Введите URL для Файла цифровой подписи и нажмите **OK**.
21. В области Configure Public Key окна Signature File и Public Key введите **область-cisco.pub** в Поле имени, и затем скопируйте этот открытый ключ и вставьте его в Ключевое поле.`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`

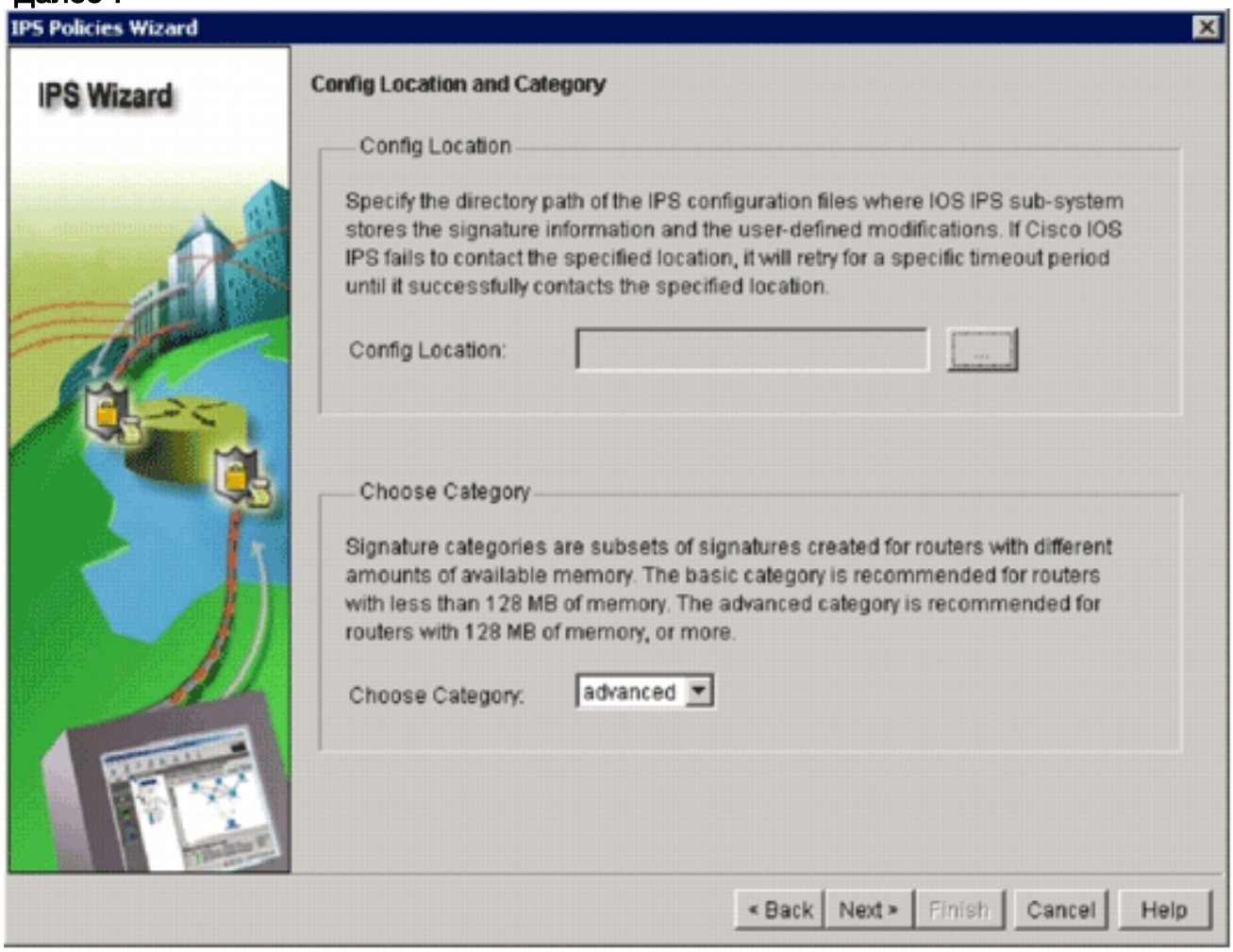
    `FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85`

    `50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36`

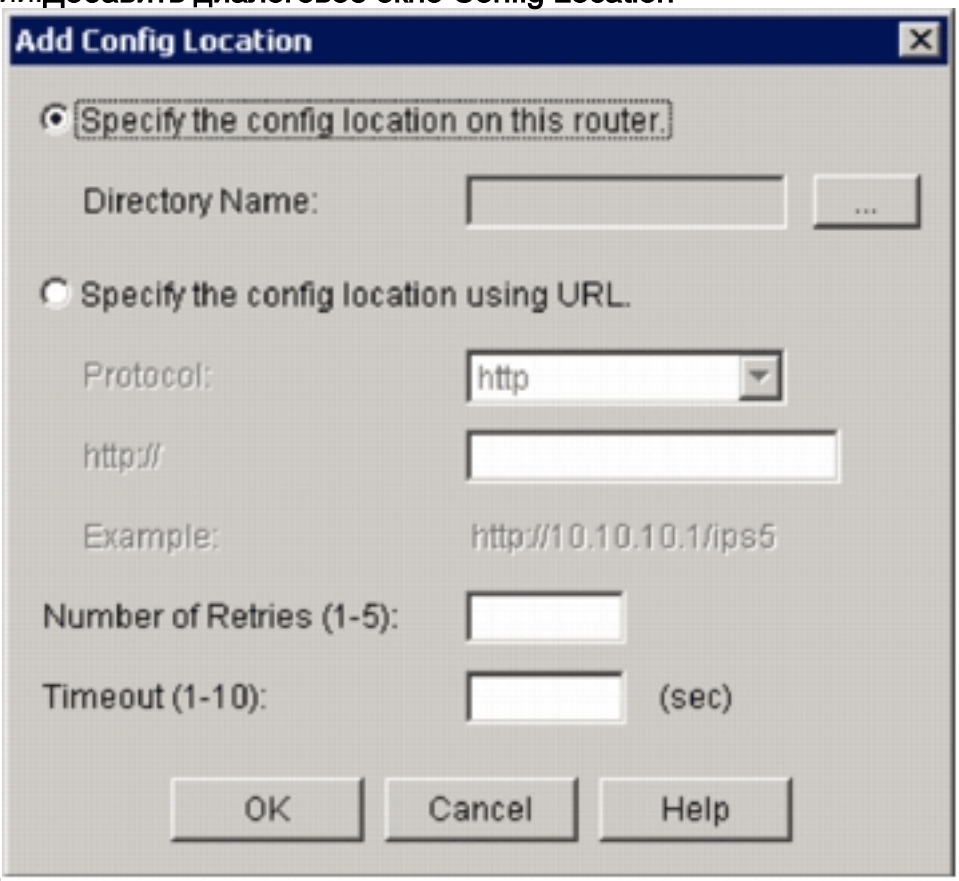
    `006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE`

    `2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3`

    `F3020301 0001`**Примечание:** Этот открытый ключ может быть загрузкой от Cisco.com в: http://www. cisco . com/pcgi-bin/tablebuild.pl/ios-v5sigup (только зарегистрированные клиенты).
22. **Для продолжения щелкните кнопку "Далее".**

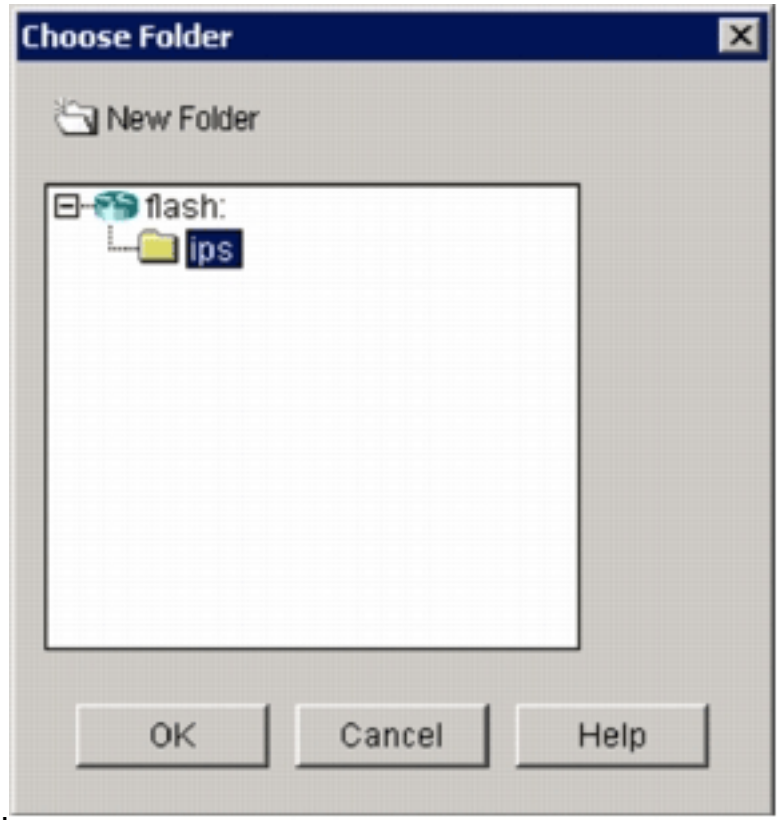


23. В окне Config Location и Category нажмите **кнопку Config Location** (...) для определения местоположения, где будут сохранены определение подписей и файлы конфигурации.**Добавить диалоговое окно Config Location**



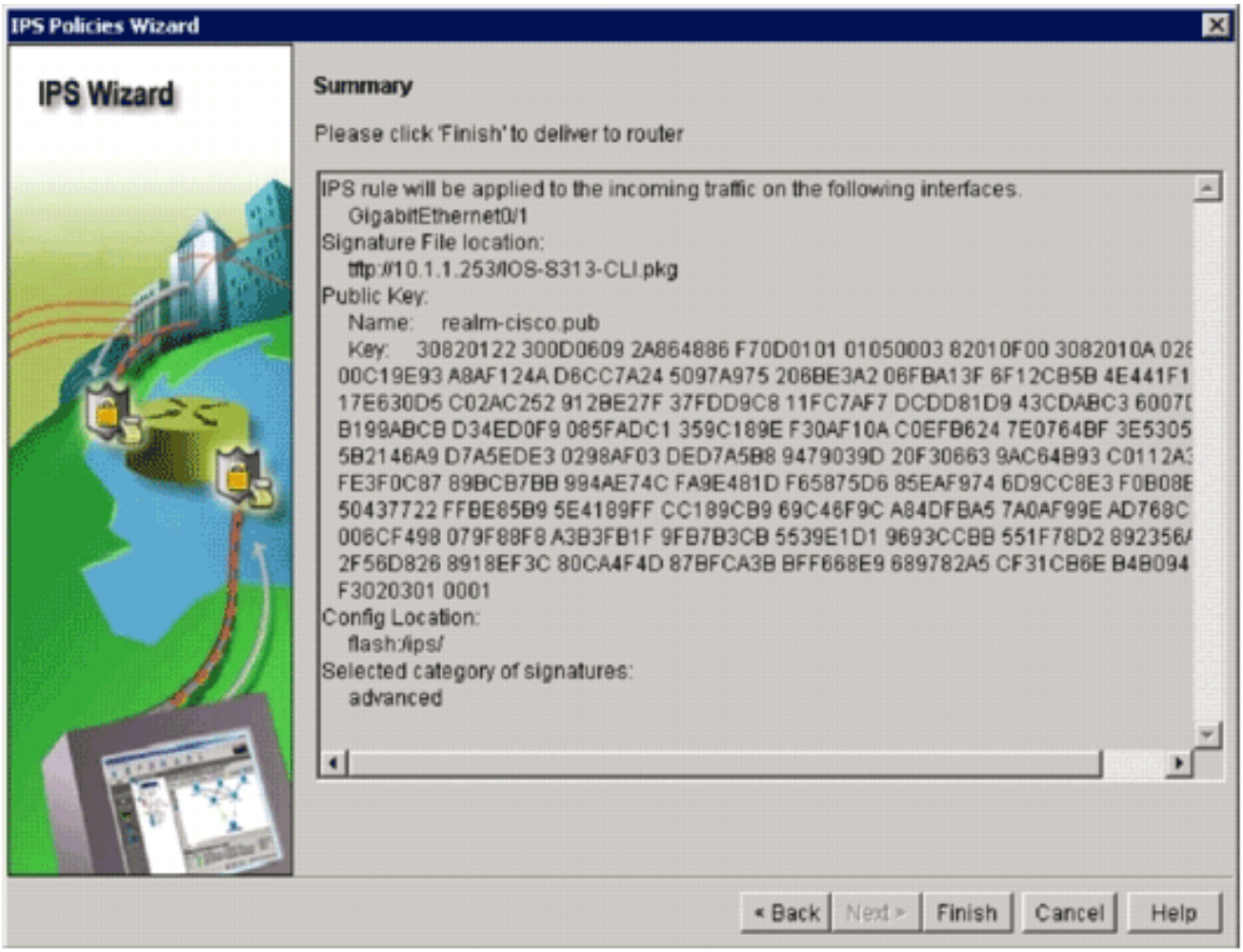
появляется.

24. В Добавить диалоговом окне Config Location нажмите **Specify config location на этой** кнопке с зависимой фиксацией **маршрутизатора**, и затем нажмите кнопку **Directory Name** (...) для определения местоположения файла конфигурации.Диалоговое окно Choose Folder появляется, чтобы позволить вам выбирать существующий каталог или создавать новый каталог на флэше - памяти маршрутизатора для хранения определения подписи и файлов

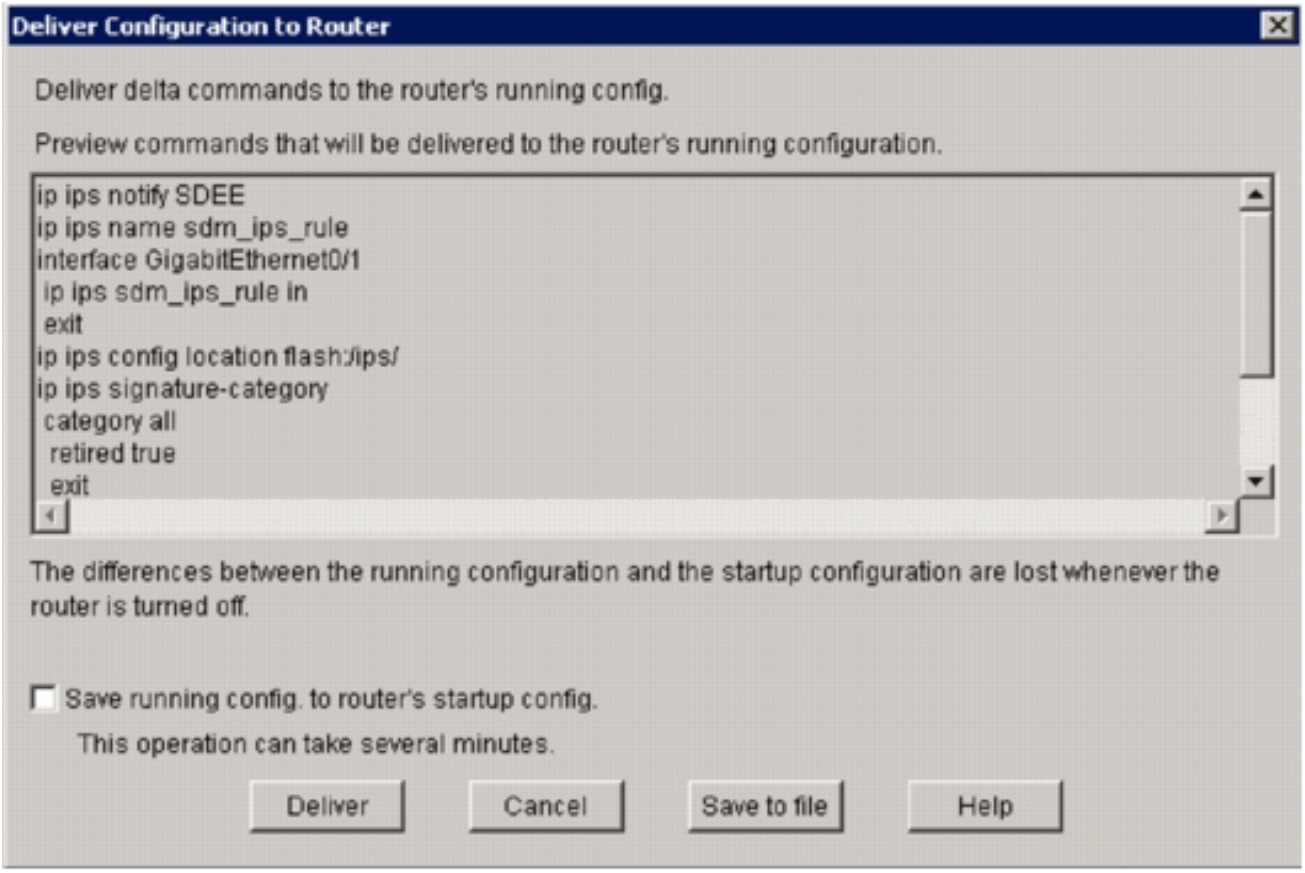


конфигурации.

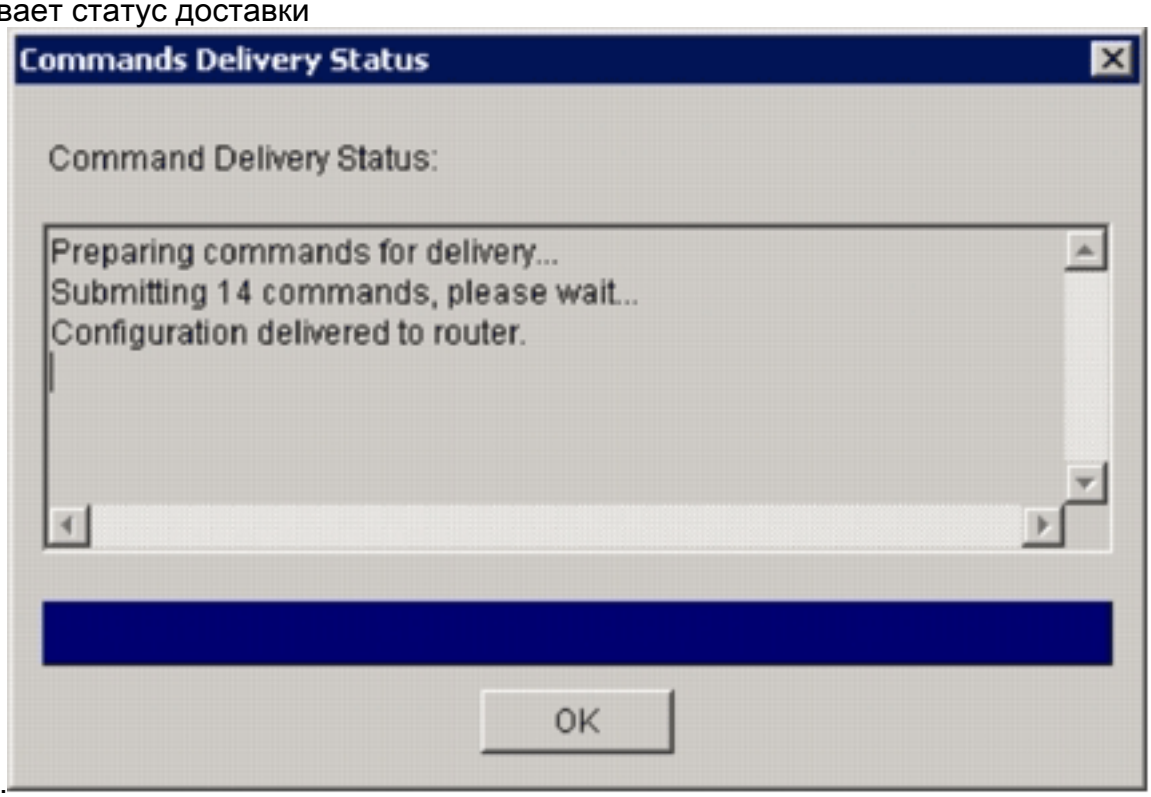
25. Нажмите **New Folder**, расположенный наверху диалогового окна, если вы хотите создать новый каталог.
26. Как только вы выбираете каталог, нажмите **OK**, чтобы применить изменения, и затем нажать **OK** для закрытия Добавить диалогового окна Config Location.
27. На диалоговом окне IPS Policies Wizard выберите категорию подписи согласно количеству памяти, установленному на маршрутизаторе. Существует две категории подписи, которые можно выбрать в SDM: Основной и Усовершенствованный.Если маршрутизатору установили DRAM 128 МБ, Cisco рекомендует выбрать Основную категорию во избежание ошибок выделения памяти. Если маршрутизатор имеет 256 МБ или больше установленного DRAM, можно выбрать любую категорию.
28. Как только вы выбираете категорию для использования, нажмите **Next** для продолжения к сводной странице.Сводная страница предоставляет краткое описание о начальной конфигурации IPS IOS
    задач.



29. Нажмите **Finish** на сводной странице для отправки конфигураций и пакета подписи к маршрутизатору.Если опция команд предварительного просмотра включена на Привилегированных параметрах настройки в SDM, SDM отображает диалоговое окно Deliver Configuration to Router, которое показывает сводку команд CLI, что SDM поставляет к
маршрутизатору.

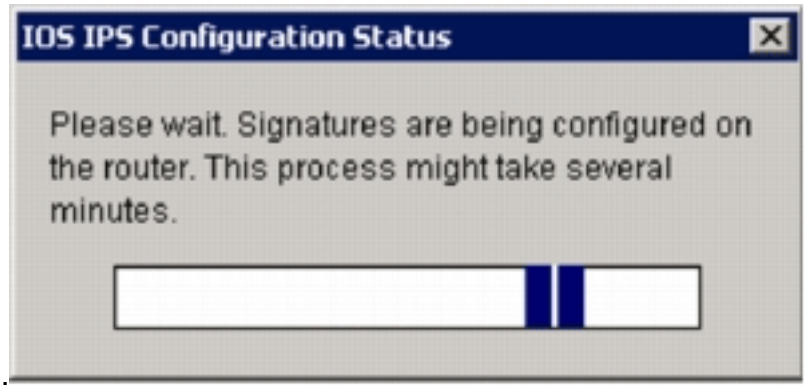


30. Нажмите **Deliver** для перехода.Коробка Диалога состояния Доставки Команд, кажется, показывает статус доставки



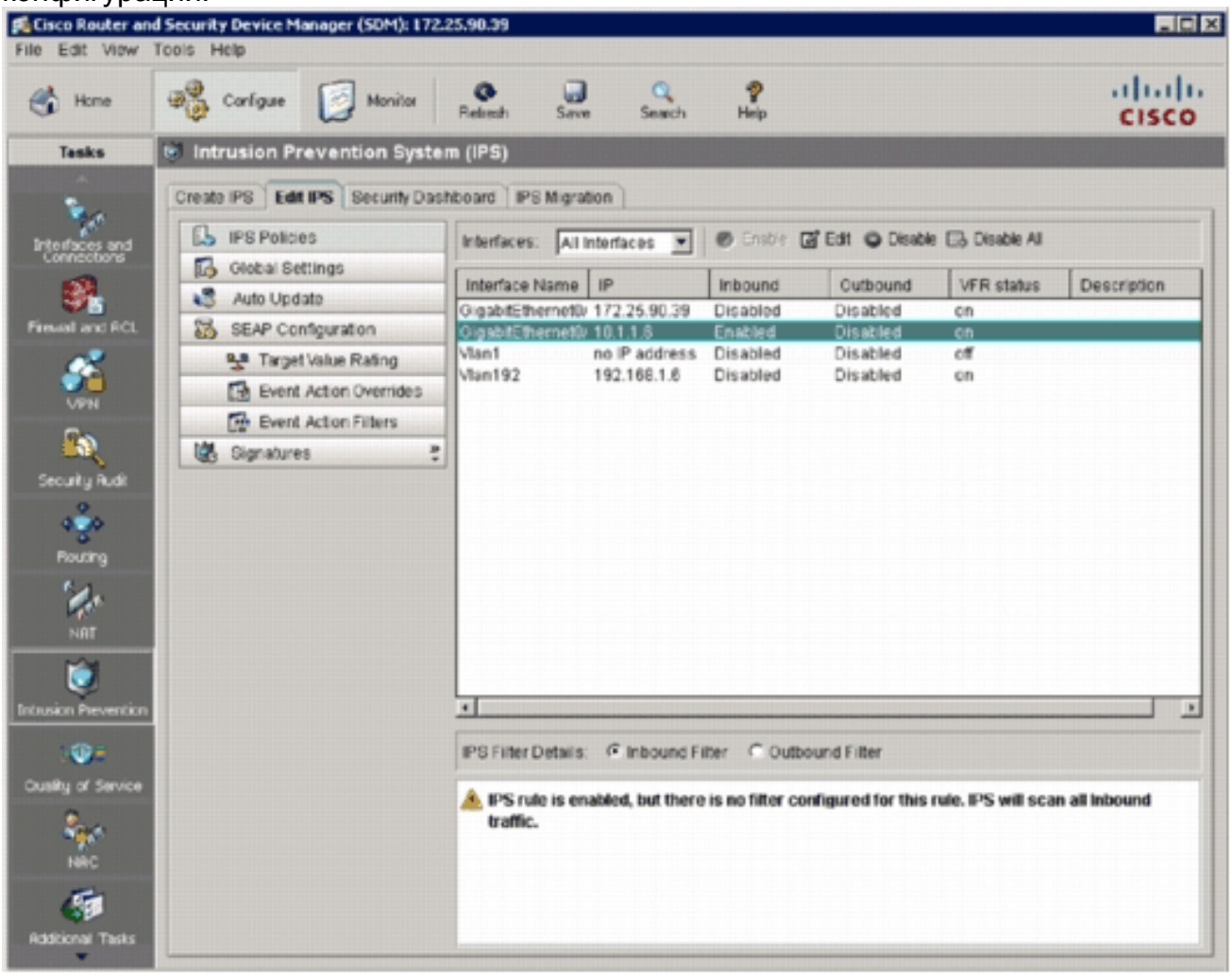
команд.

31. Когда команды отправлены маршрутизатору, нажмите **OK** для продолжения.Диалоговое окно IOS IPS Configuration Status показывает, что подписи

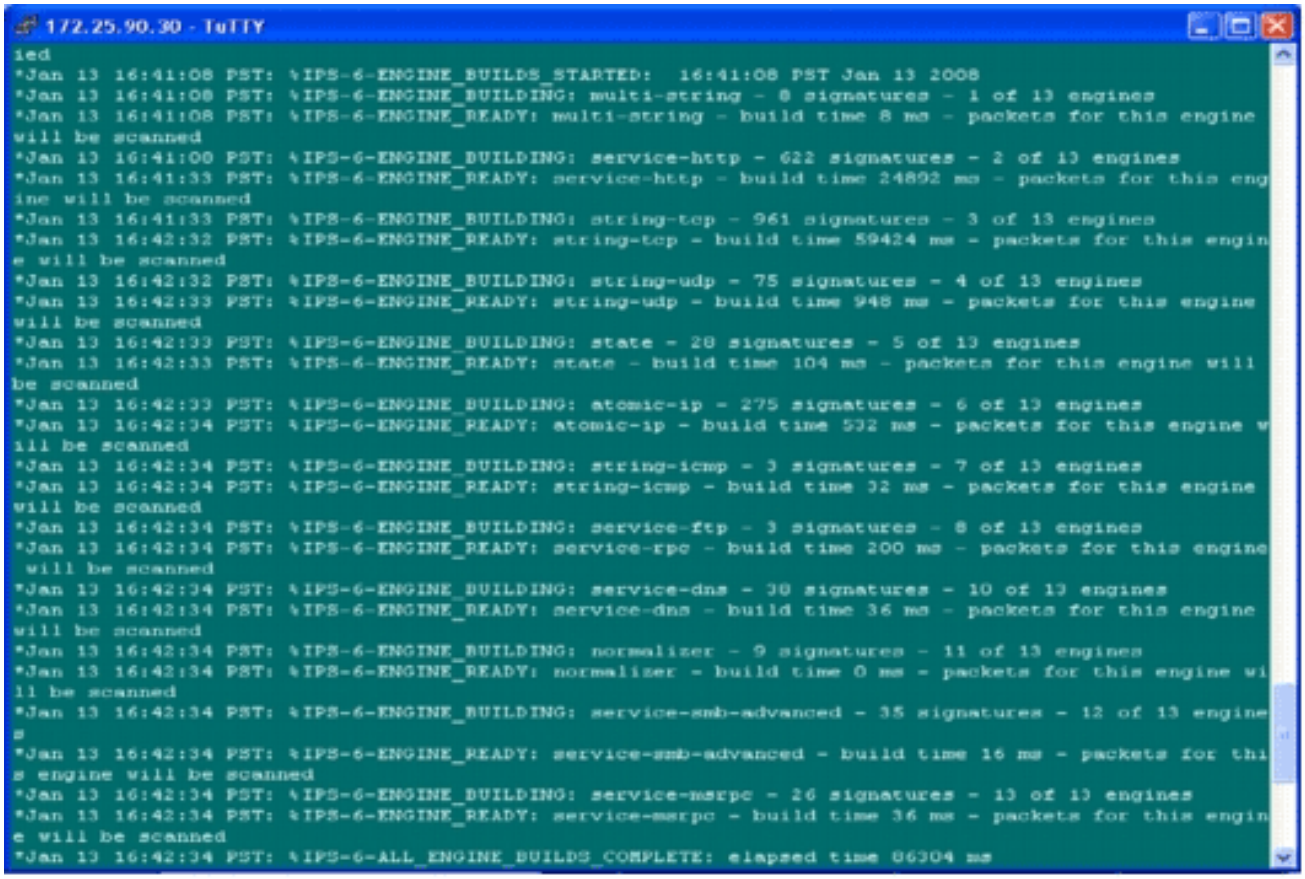


загружаются на маршрутизаторе.

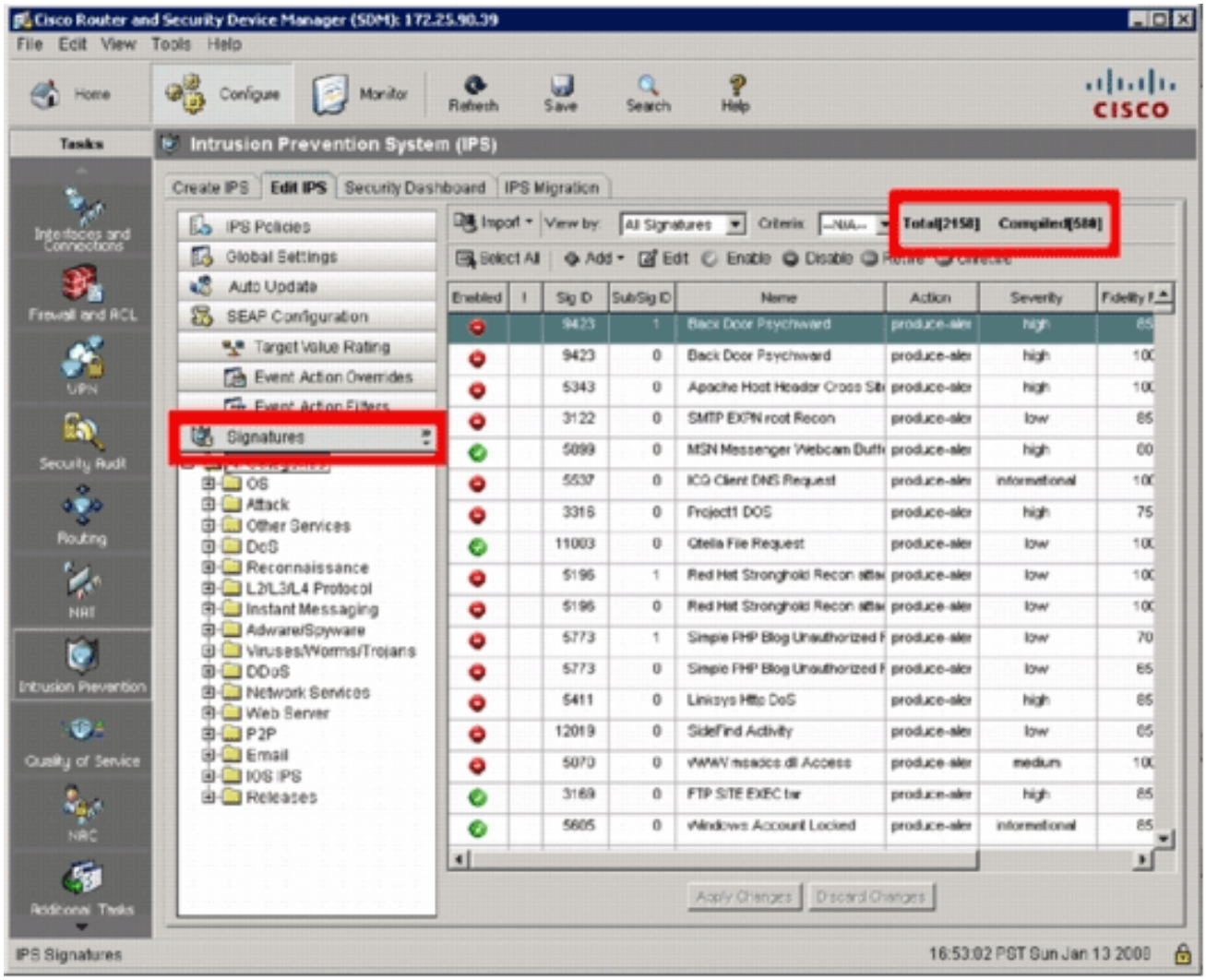
32. Когда подписи загружены, SDM отображает вкладку **Edit IPS** с текущей конфигурацией. Проверьте, какой интерфейс и в том, какое направление IPS IOS включено для проверки конфигурации.



Консоль маршрутизатора показывает, что были загружены подписи.



33. Используйте **команду show ip ips signatures count**, чтобы проверить, что подписи загружены должным образом.`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` Начальная инициализация IPS IOS с помощью SDM 2.5 завершена.
34. Проверьте номера подписи с SDM как показано в этом образе.



Дополнительные сведения

- IPS Cisco IOS на Cisco.com
- Пакет Подписи IPS Cisco IOS
- Файлы цифровой подписи IPS Cisco IOS для SDM
- Начало работы с IPS Cisco IOS с 5.x формат подписи
- Руководство по конфигурации IPS Cisco IOS
- Просмотр событий Cisco IDS
- Cisco Systems – техническая поддержка и документация