Пример настройки диспетчера безопасности в системе предотвращения атак Cisco IOS

Содержание

Введение

Cisco Security Manager является частью Cisco Security Система управления, которая отправляет всестороннее администрирование политик и осуществление для Cisco SDN. Cisco Security Manager является лидирующим приложением промышленного класса для управления безопасностью. Cisco Security Manager обращается к управлению конфигурацией межсетевого экрана, VPN и сервисов безопасности Системы предотвращения вторжений (IPS) через маршрутизаторы Cisco, устройства безопасности и модули сервисов безопасности.

Для сводки Функций и преимуществ Cisco Security Manager, а также новых характеристик в версии 3.1, ссылаются на таблицу данных Cisco Security Manager 3.1 в http://www. cisco . com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html. Можно загрузить Cisco Security Manager 3.1 от Cisco.com в http://www. cisco . com/cgi-bin/tablebuild.pl/csm-app (только зарегистрированные клиенты).

Этот документ описывает, как использовать Cisco Security Manager 3.1 для выполнения начальной конфигурации IPS IOS. Для маршрутизаторов, уже настроенных с IPS IOS, клиенты могут непосредственно использовать Cisco Security Manager 3.1 для инициализации задач.

Примечание: Cisco Security Manager 3.1 поддерживает только IOS 12.4 (11) T2 и более поздние Образы IOS для настройки IPS IOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco Security Manager 3.1
- Cisco IOS 12.4 (11) T2

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.

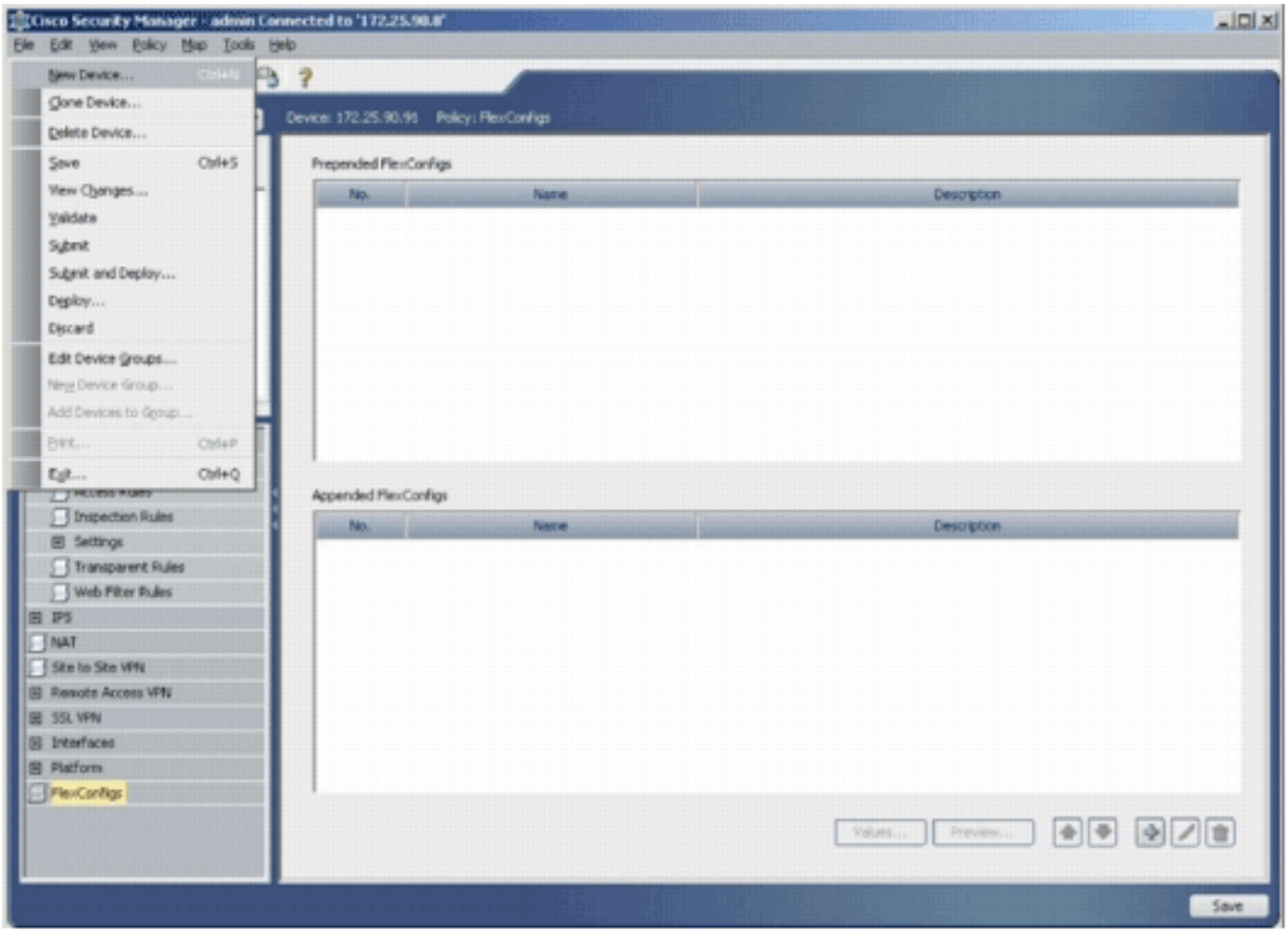
Условные обозначения

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

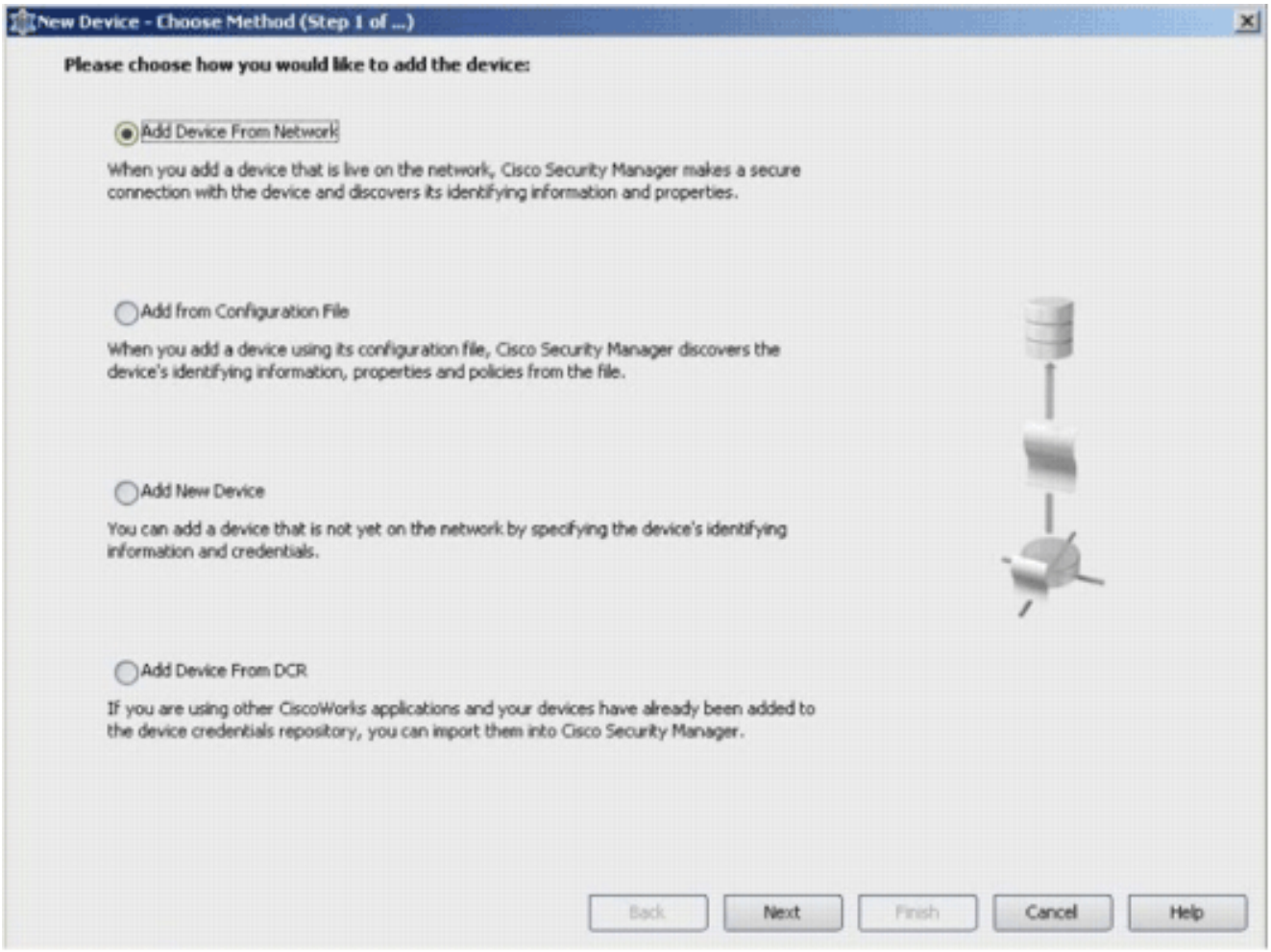
Настройка

Выполните эти шаги для настройки IPS IOS:

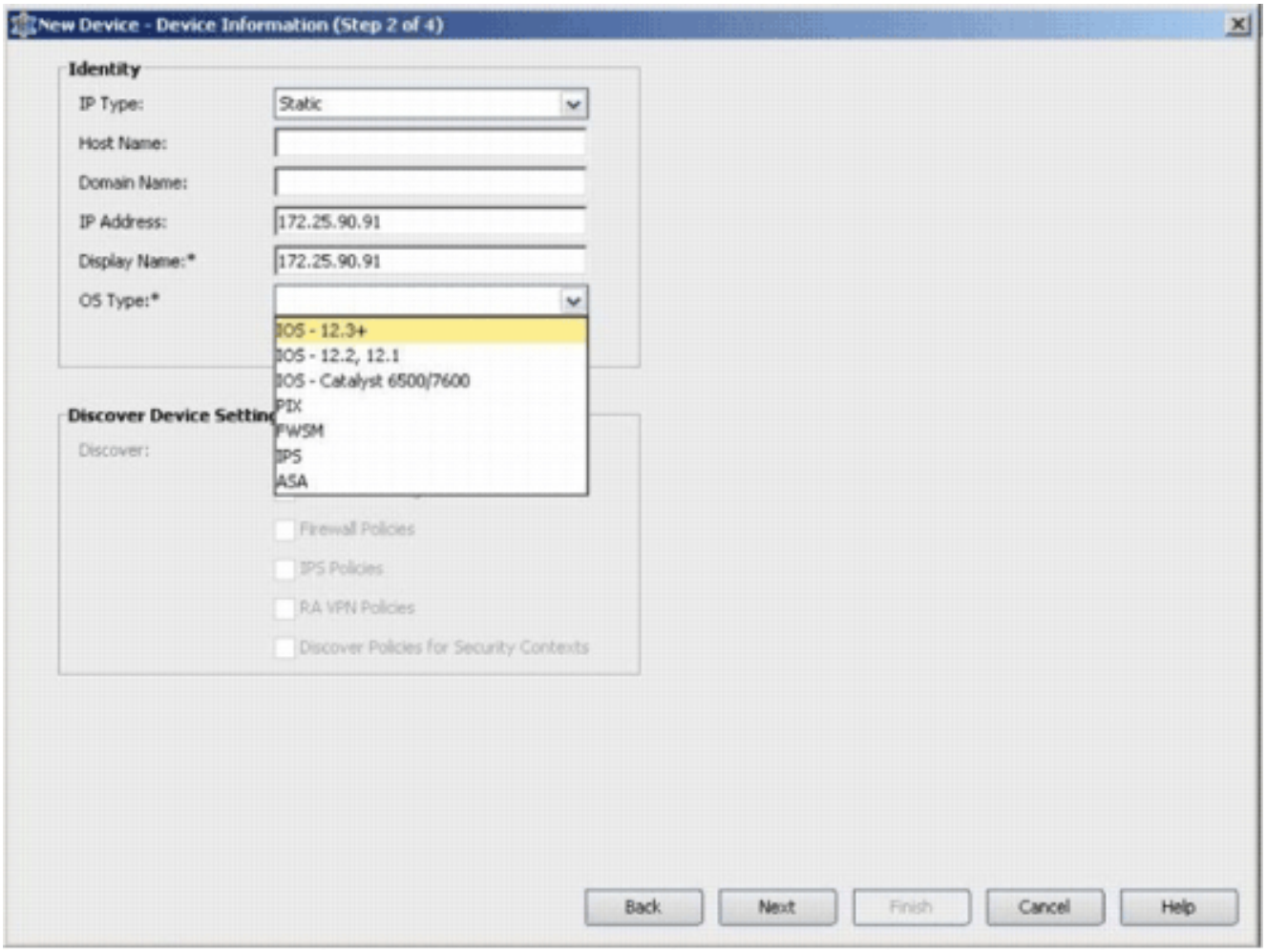
1. Выполните клиента Cisco Security Manager 3.1 от своего локального компьютера.
2. Выберите **New Device** из Меню Файл для добавления устройства на Cisco Security Manager
   3.1.



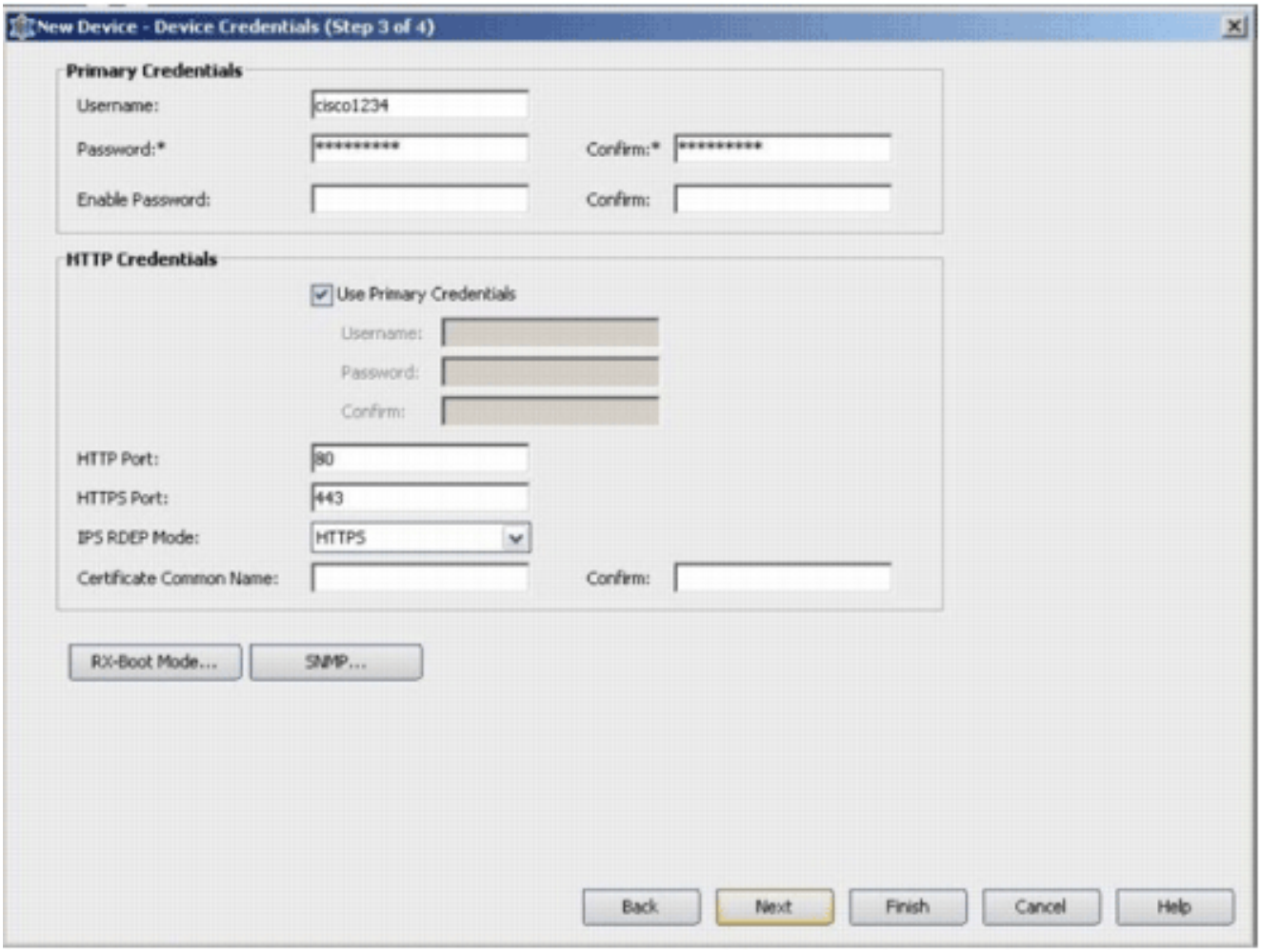
3. В Новом Окне устройства выберите, как требуется добавить устройство. Данный пример добавляет устройство от
сети.



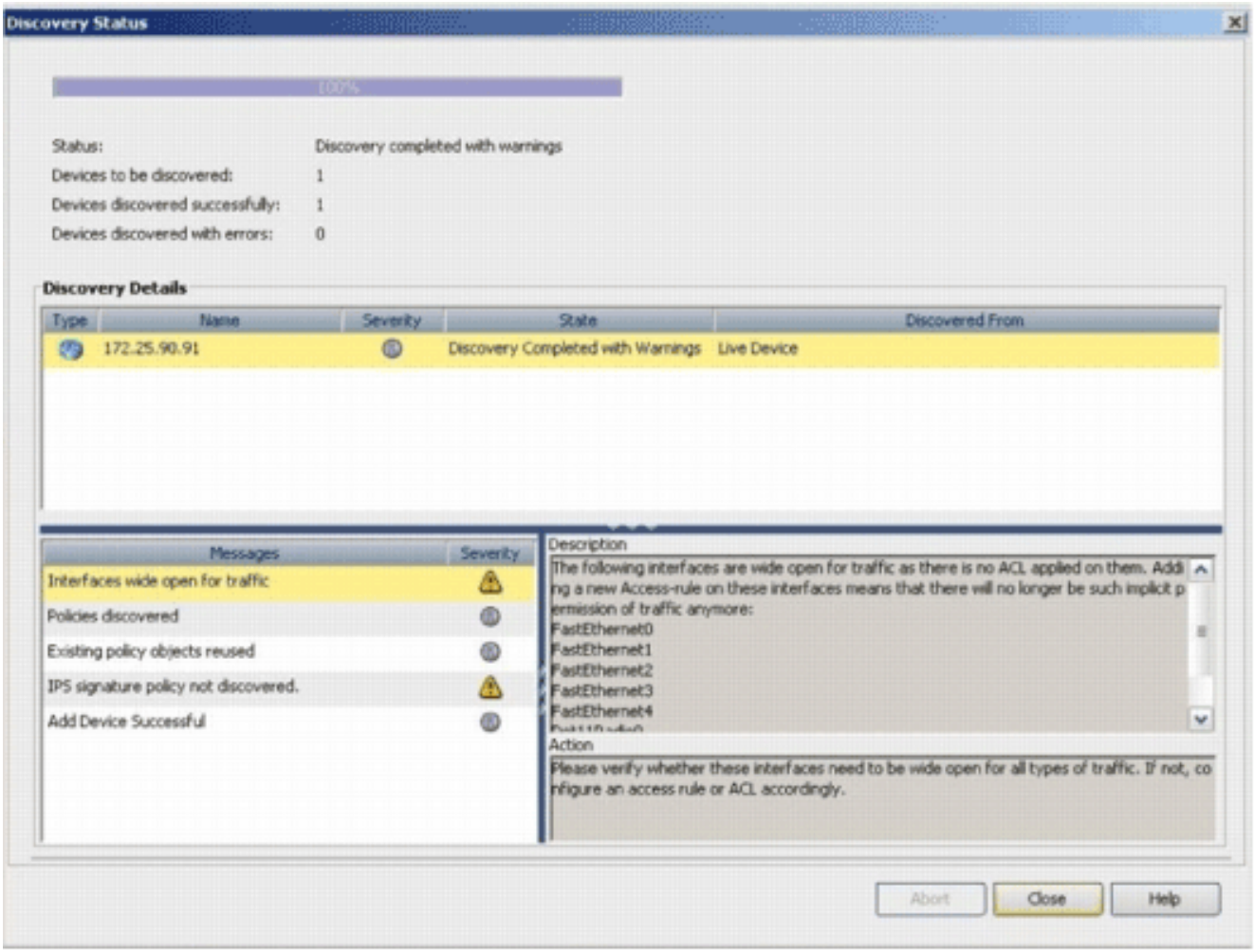
4. Нажмите кнопку Next.
5. Введите Идентификационные подробные данные для устройства, которое вы хотите добавить. Например, имя хоста и IP-
адрес.



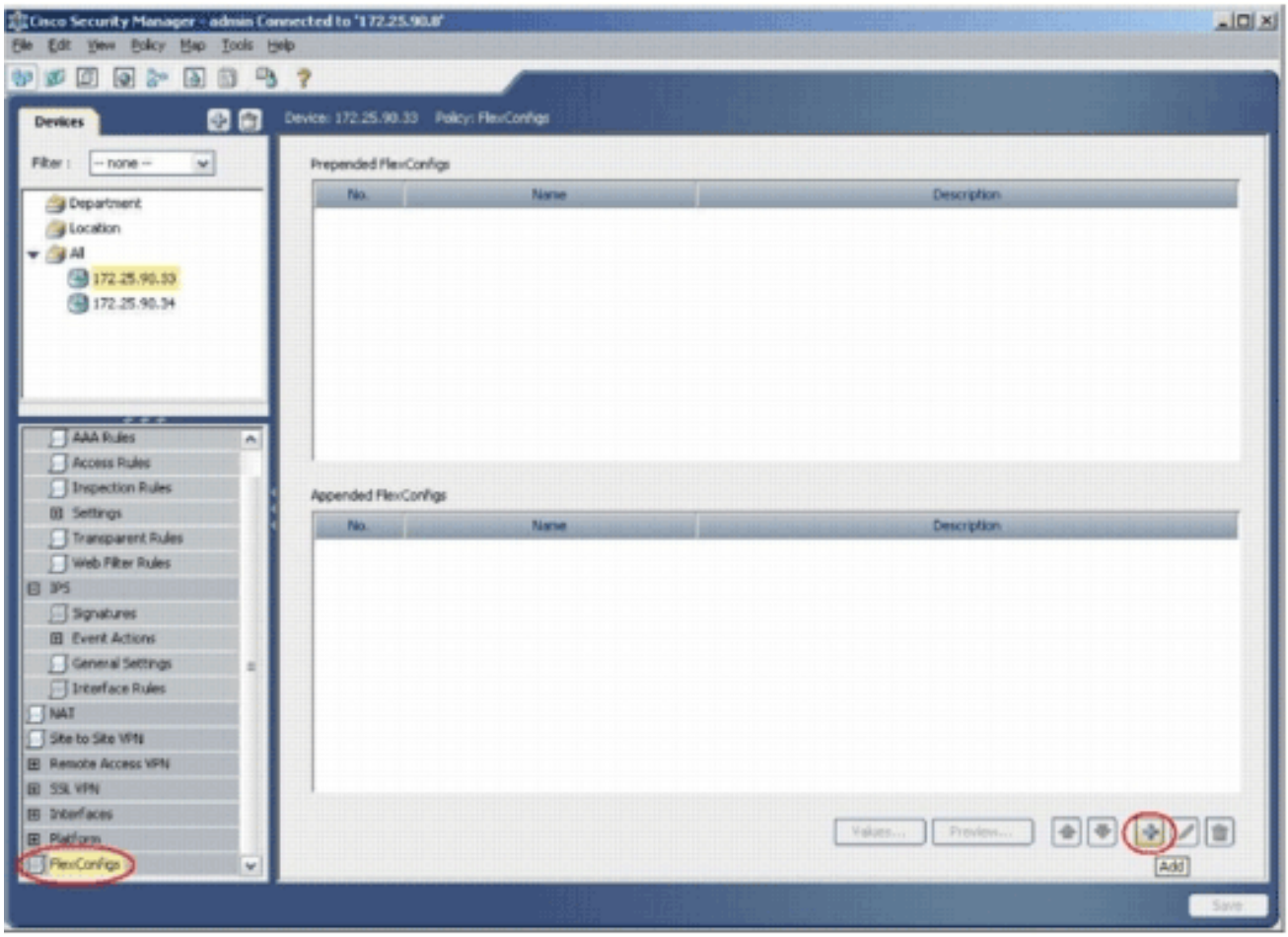
6. **Нажмите кнопку Next.**
7. Введите основные учетные данные, такие как имя пользователя, пароль, Enable password для Маршрутизатора IOS, который вы хотите добавить.
8. Нажмите **Finish** для добавления устройства на Cisco Security Manager.**Примечание:** Данный пример предполагает, что пользователь уже имеет предварительно сконфигурированный маршрутизатор и может войти к маршрутизатору с надлежащими учетными
данными.



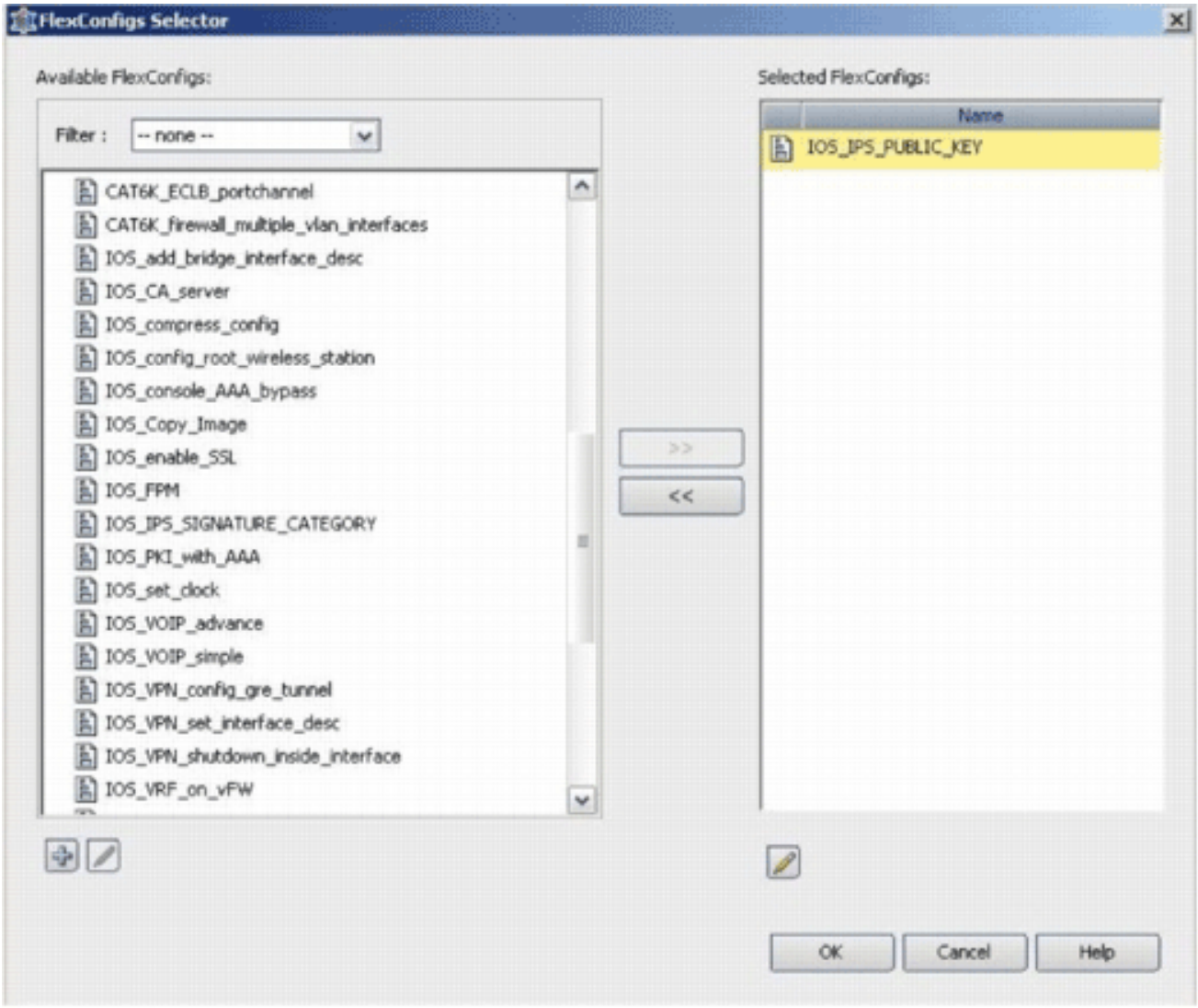
Когда "Обнаружение, завершенное", появляется в Окне состояния Обнаружения, вы успешно добавили устройство на Cisco Security Manager. Как только вы успешно добавили устройство на Cisco Security Manager, необходимо назначить открытый ключ для включения
IPS.



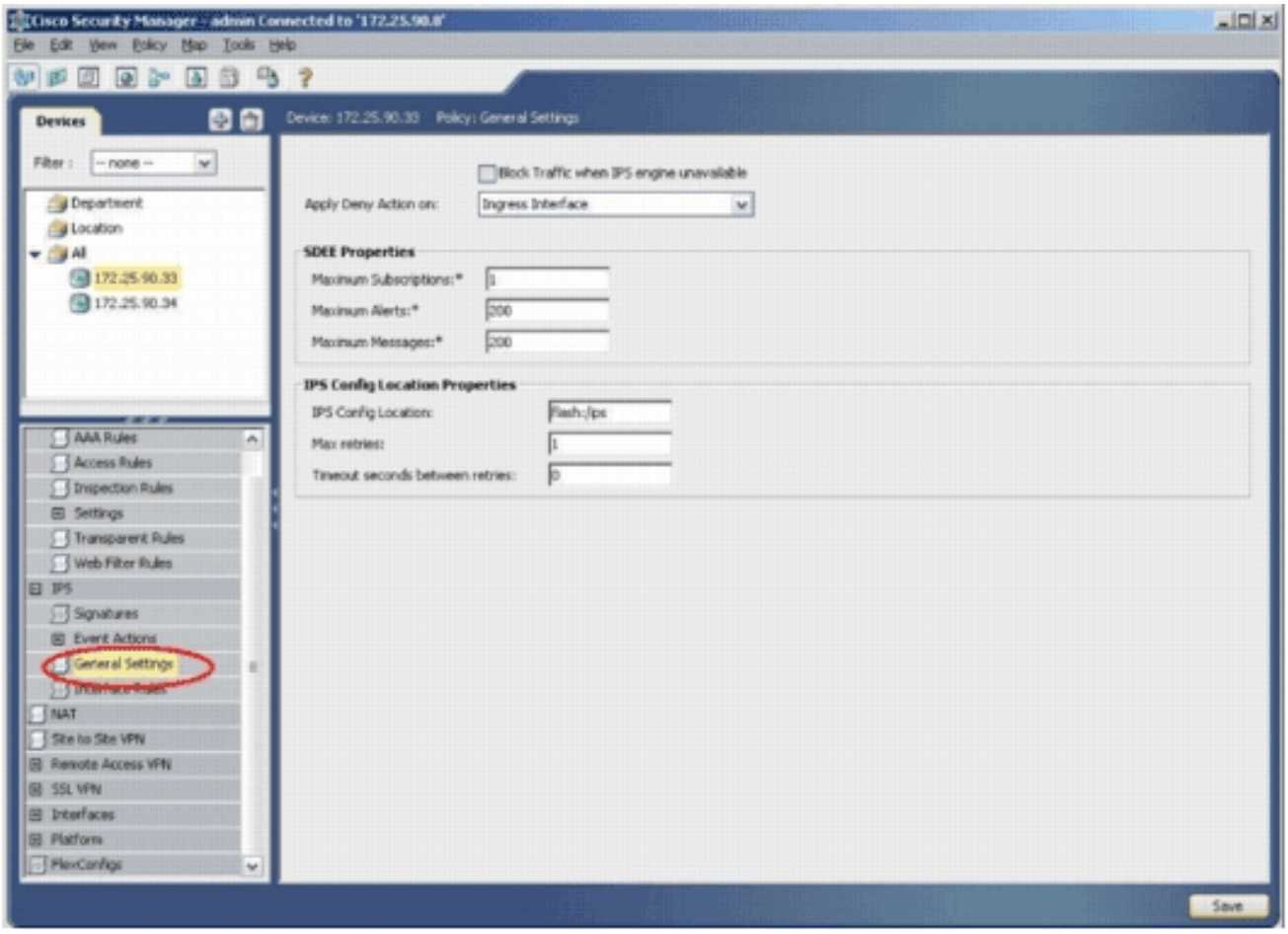
9. Из меню слева, перейдите к окну конфигурации FlexConfigs.
10. Нажмите интерфейс пользователя FlexConfigs на правой части экрана, и затем нажмите значок
    Add.



11. В Выбранном списке FlexConfigs выберите **IOS_IPS_PUBLIC_KEY** и нажмите **OK**.

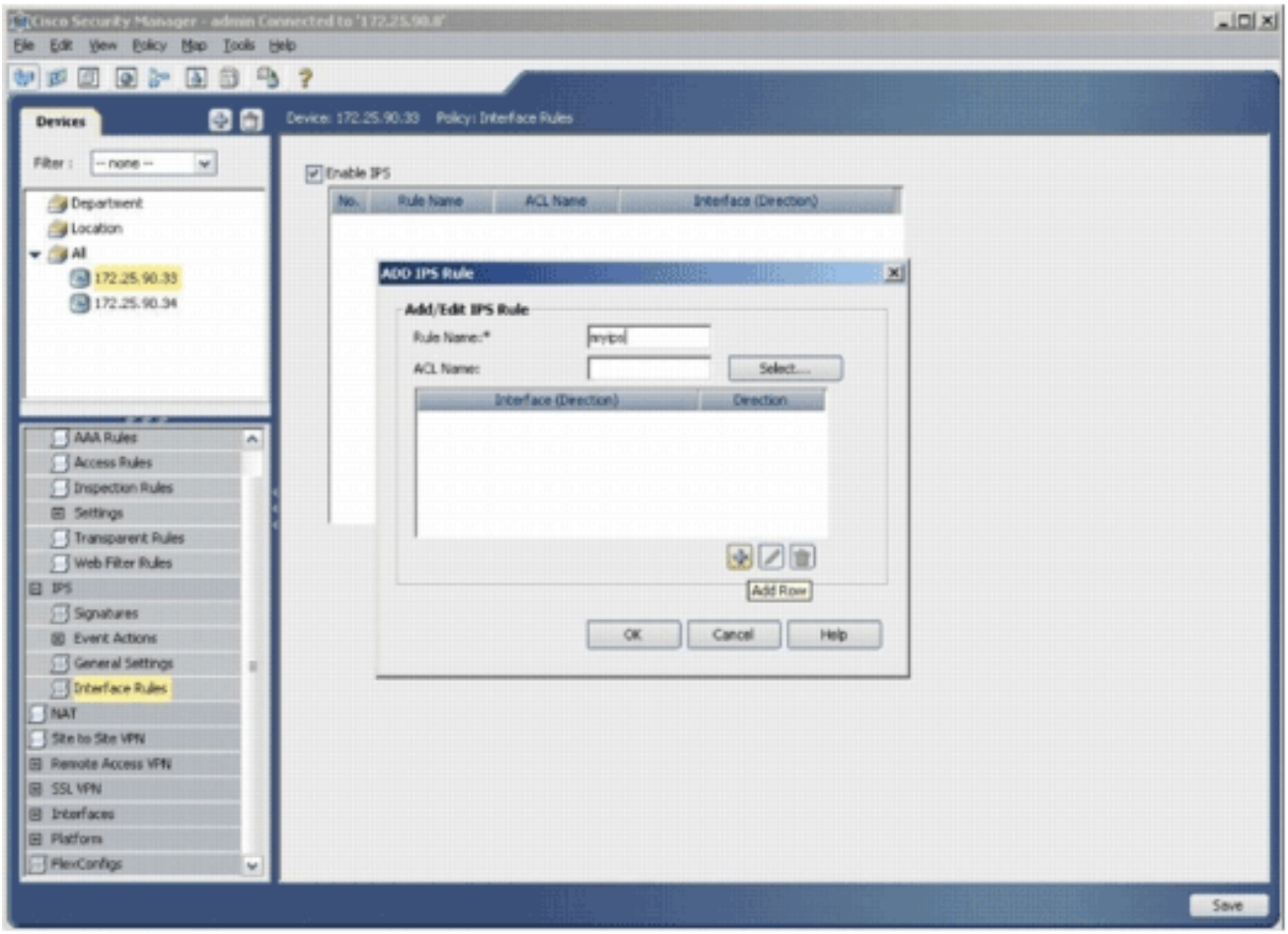


12. Нажмите **Save** для сохранения изменений.**Примечание:** IOS_IPS_PUBLIC_KEY FlexConfig держит конфигурацию для открытого ключа.
13. Из меню слева, выберите **General Settings**, расположенный ниже заголовка IPS.
14. Введите расположение настройки IPS во флэш-память. Это - местоположение, в которое размещены конфигурации IPS.
15. Нажмите **Save** для сохранения изменений.

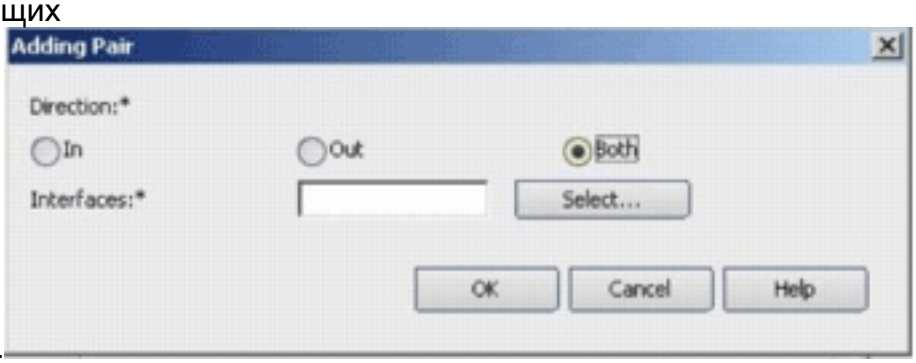


Примечание: Удостоверьтесь, что каталог location был уже создан на флэше - памяти маршрутизатора. В противном случае используйте **команду mkdir <directory_name>** для создания каталога location.

16. Для включения IPS перейдите для Взаимодействия через интерфейс Правил, проверьте флажок **Enable IPS**, и затем **нажмите Add строку**.
17. В диалоговом окне Add IPS Rule введите имя для правила IPS в поле Rule Name, и затем **нажмите Add строку** для включения интерфейсов, на которые должен быть применен
    IPS.

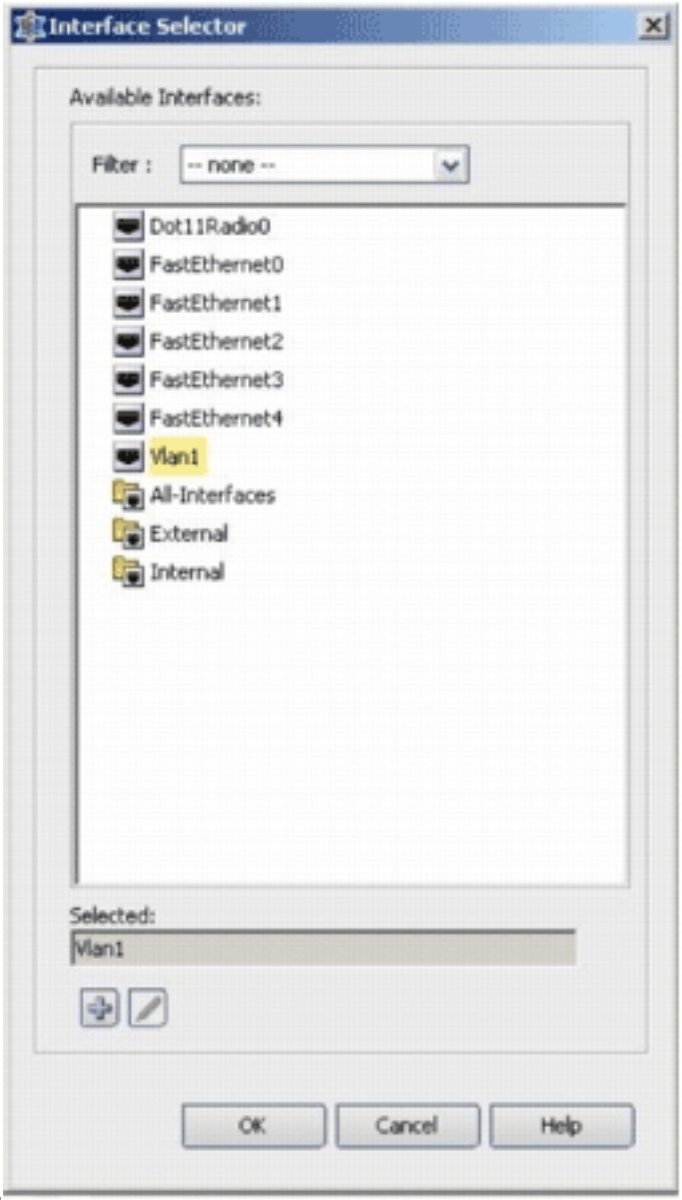


18. Нажмите кнопку с зависимой фиксацией, которая указывает, в котором направлении правило IPS должно быть применено, и затем нажать **Select** для выбора соответствующих



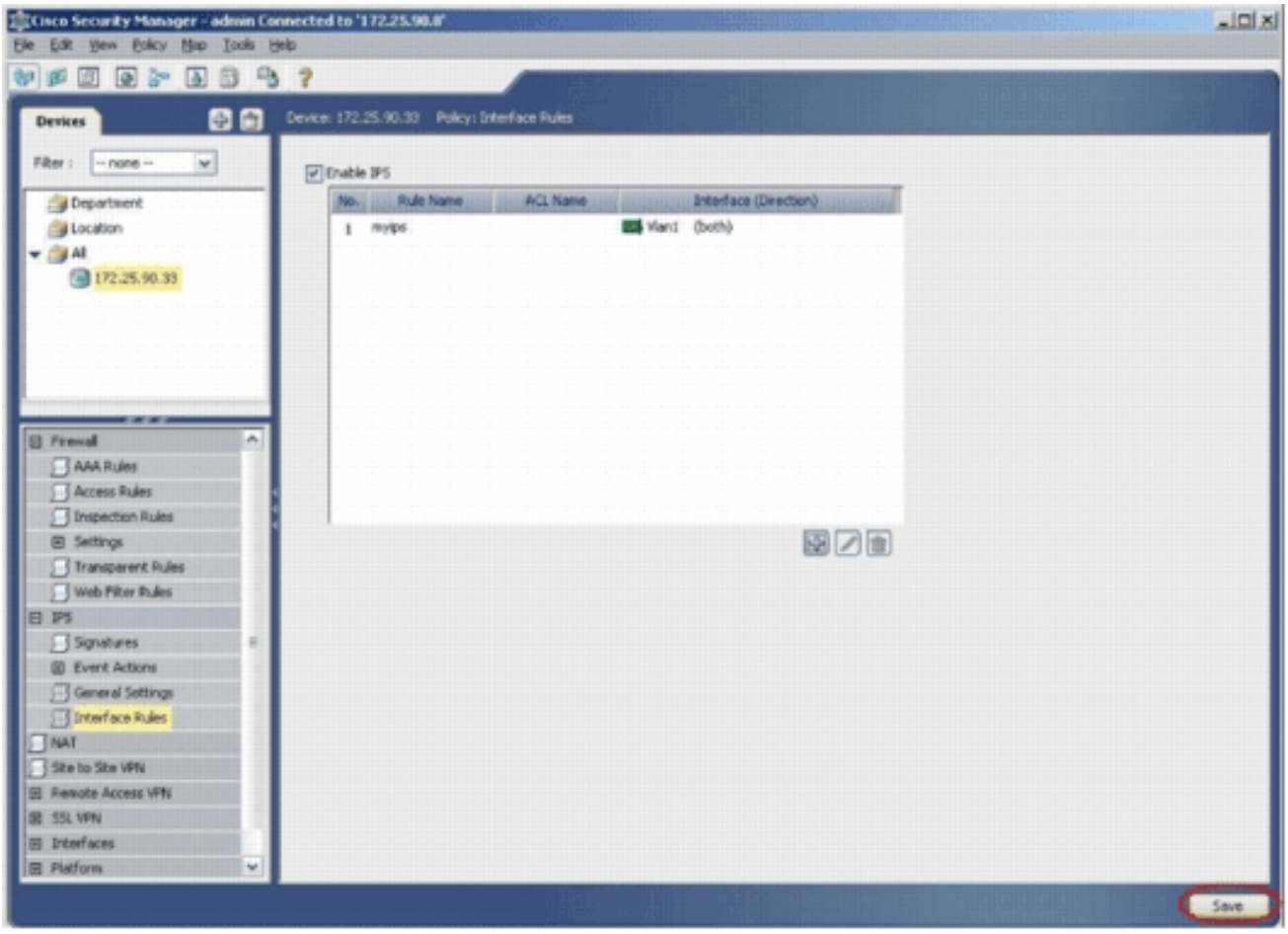
интерфейсов.

19. Выберите интерфейс из Интерфейсного Селекторного списка и нажмите

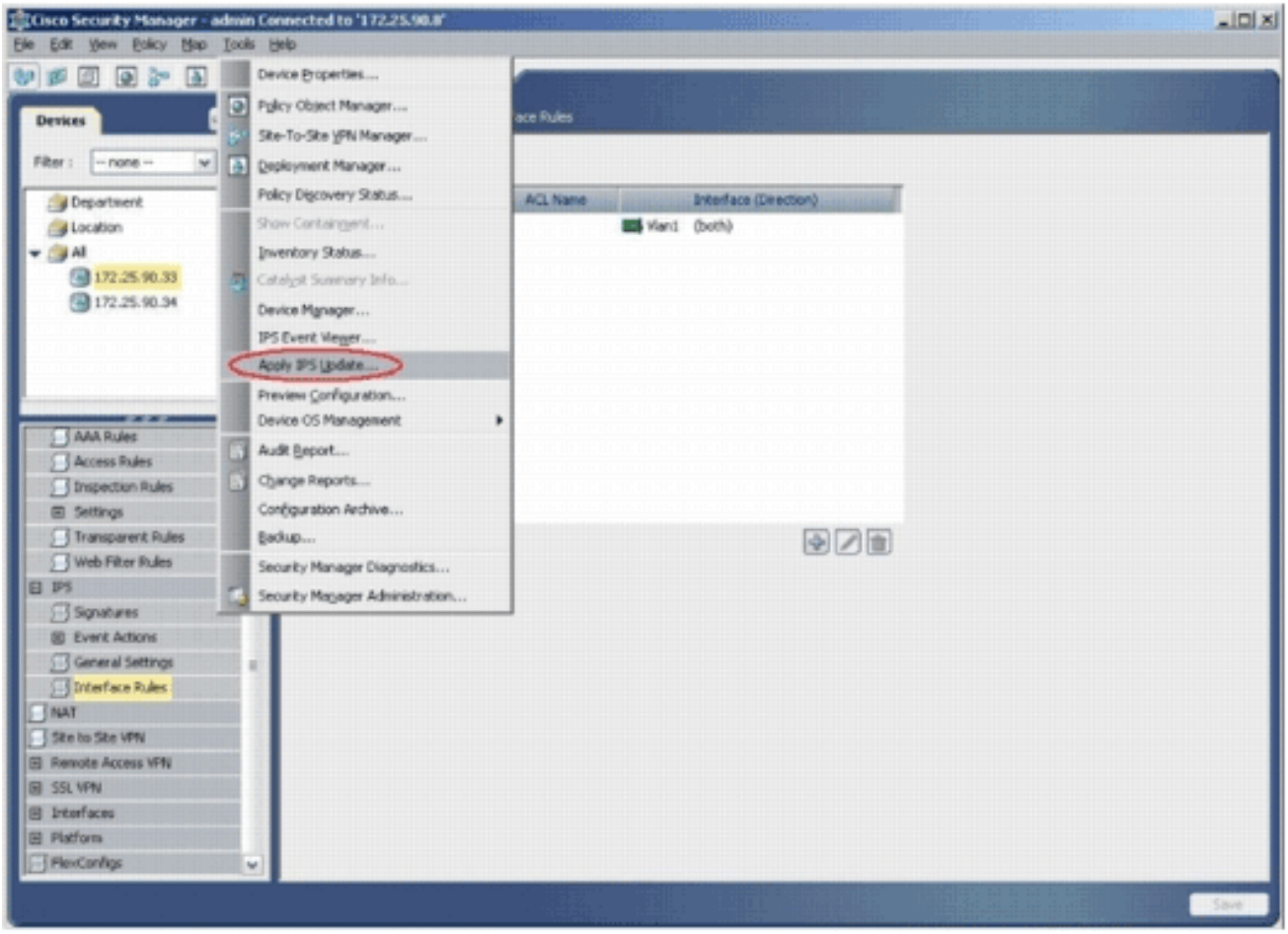


OK.

20. Нажмите **Save** для сохранения изменений.

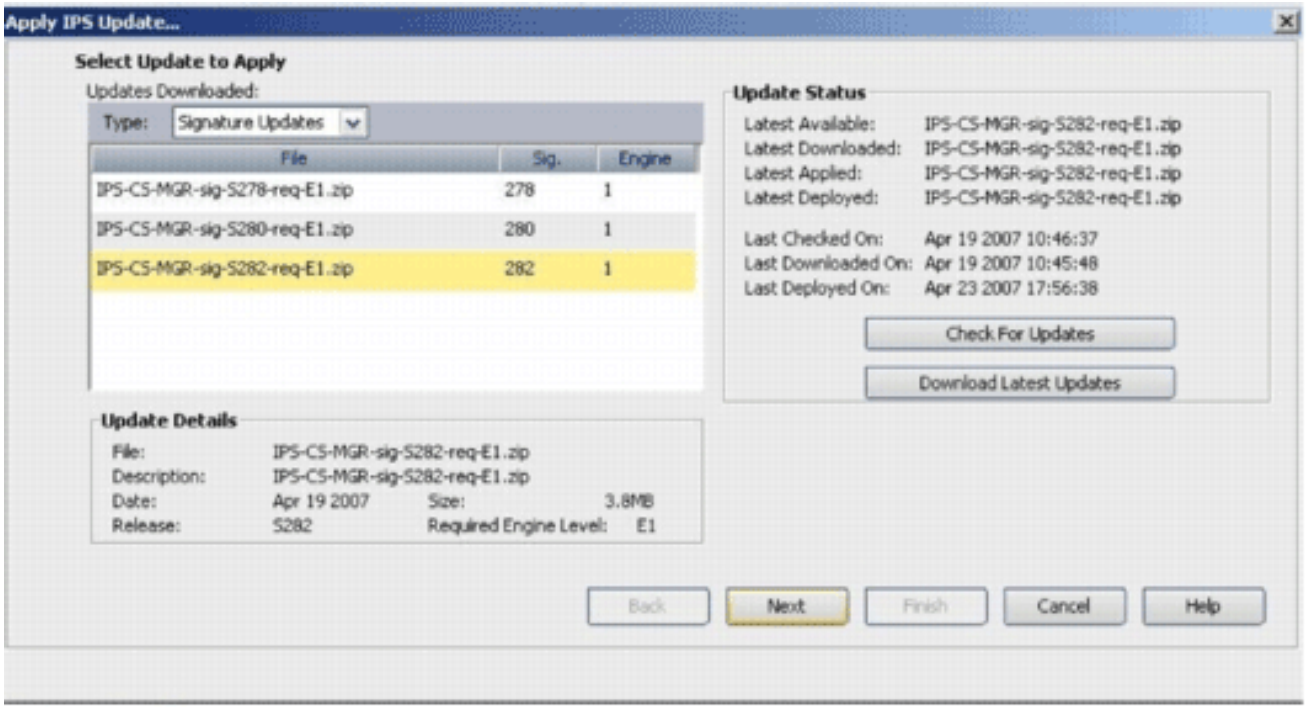


21. Выберите **Tools> Apply IPS Update** для установки последних подписей IPS.

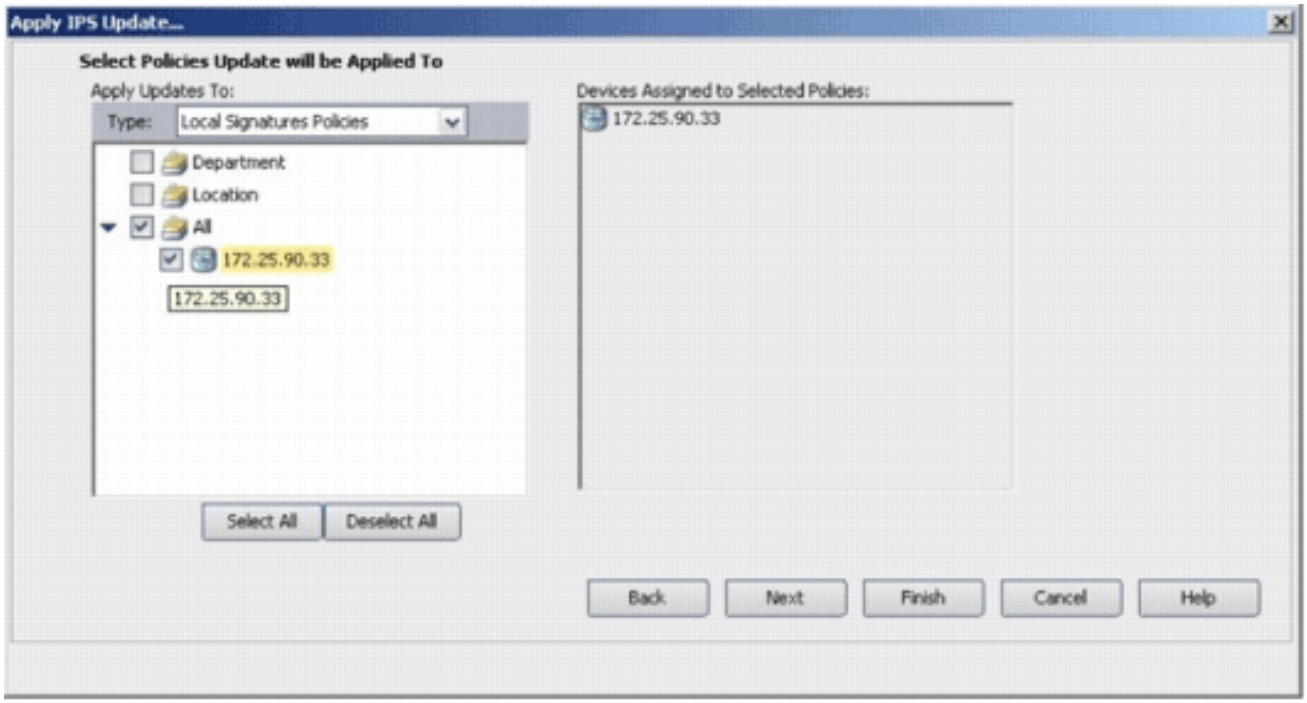


22. Выберите последний Файл цифровой подписи и нажмите

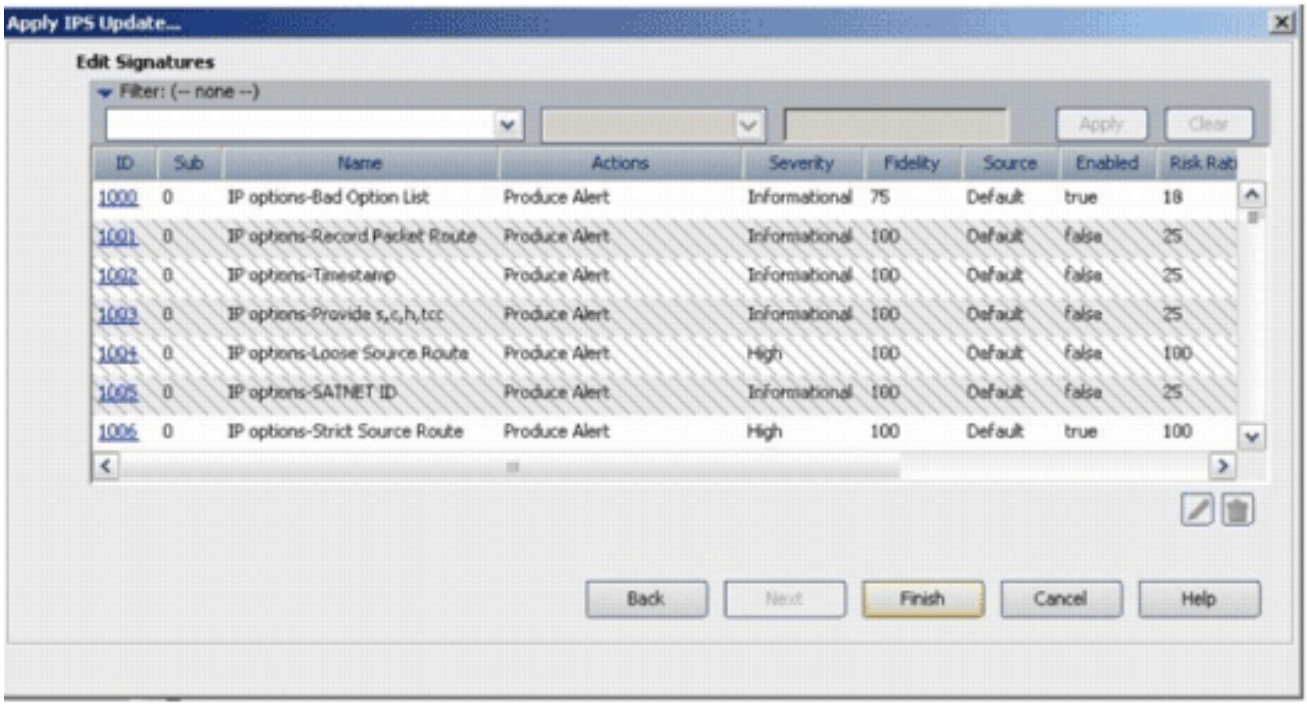
Next.



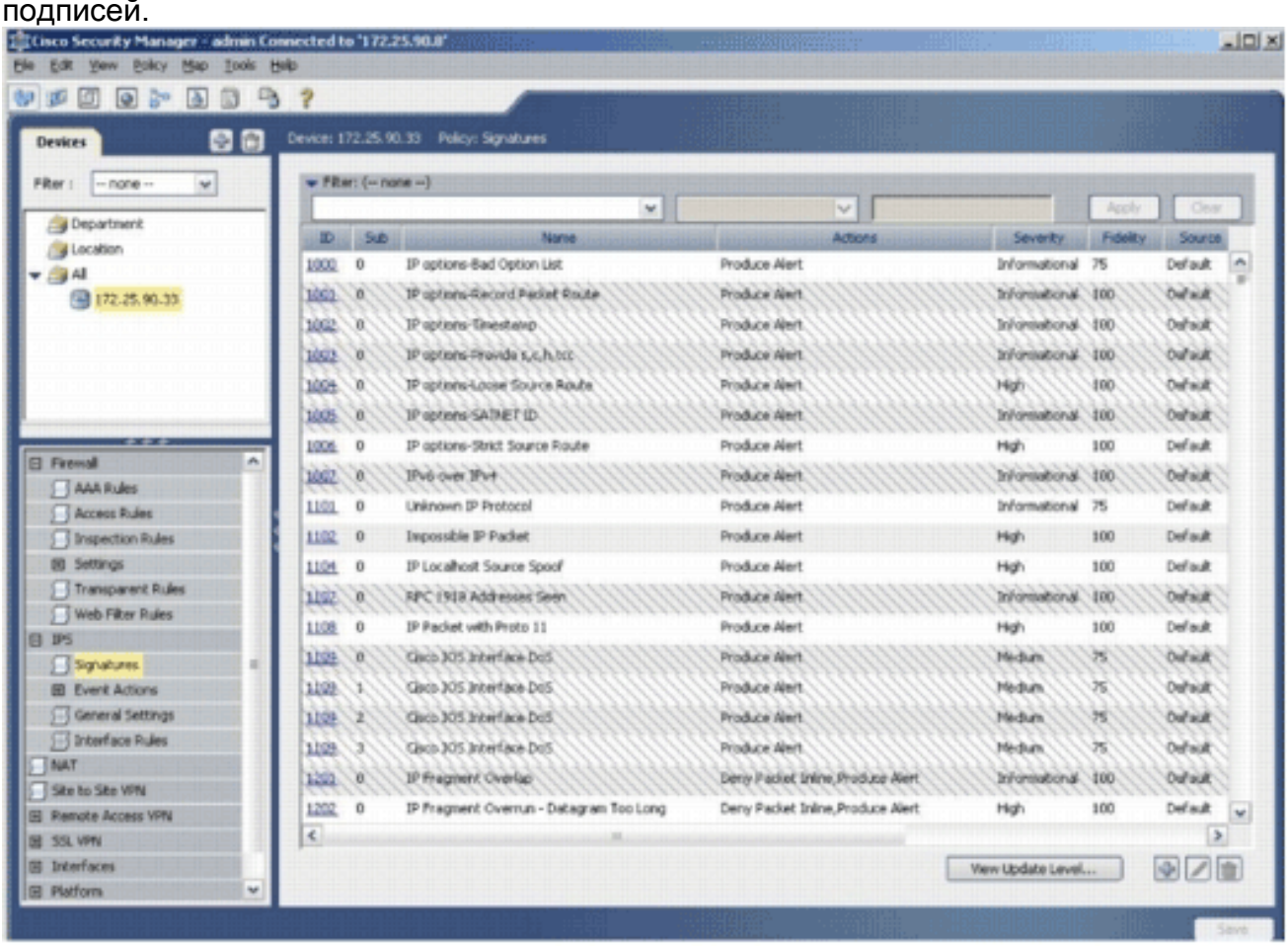
23. Выберите устройства, на которых обновление IPS должно быть применено, и нажимать **Next**.



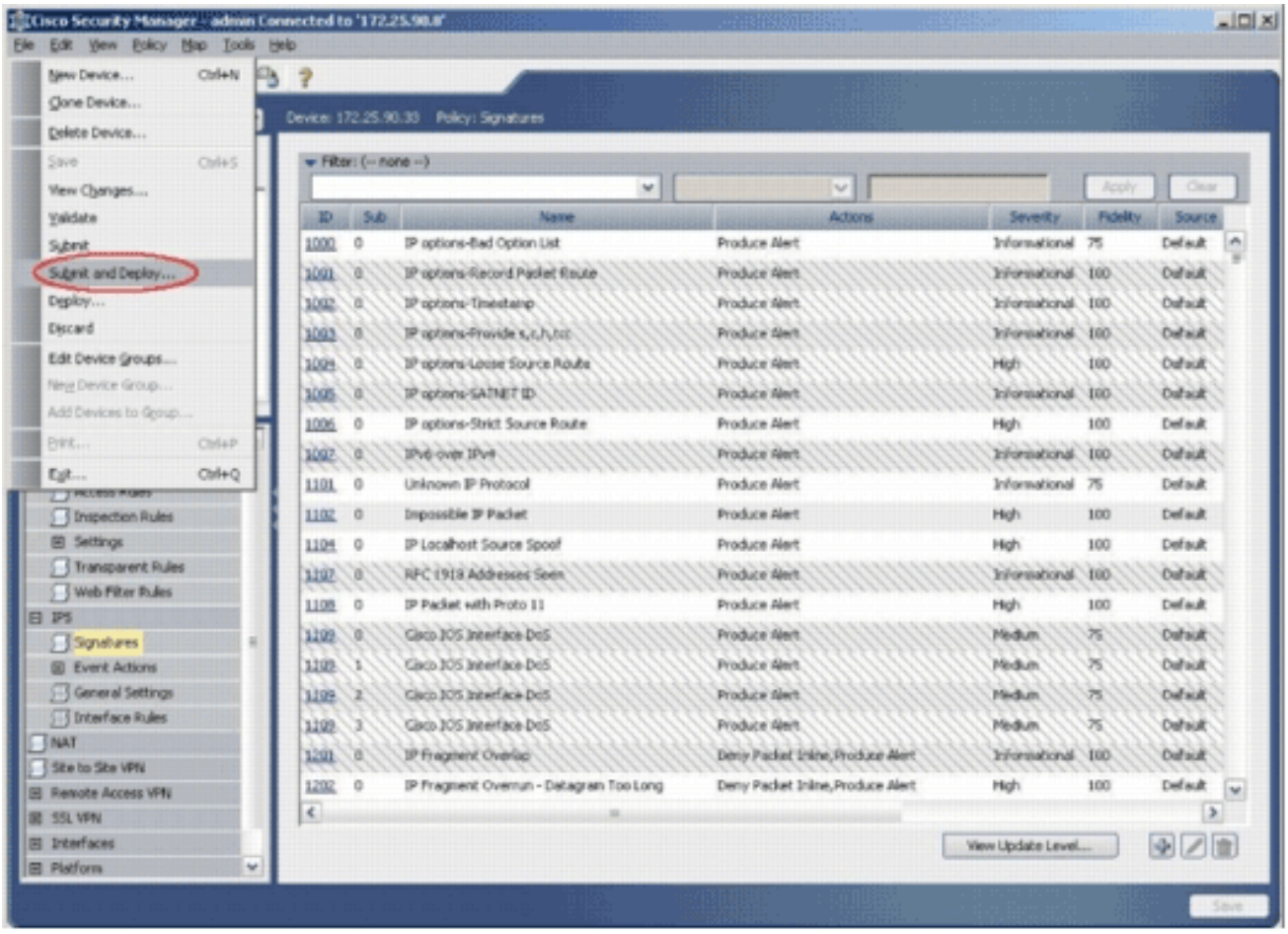
24. Нажмите **Finish** для применения подписей.



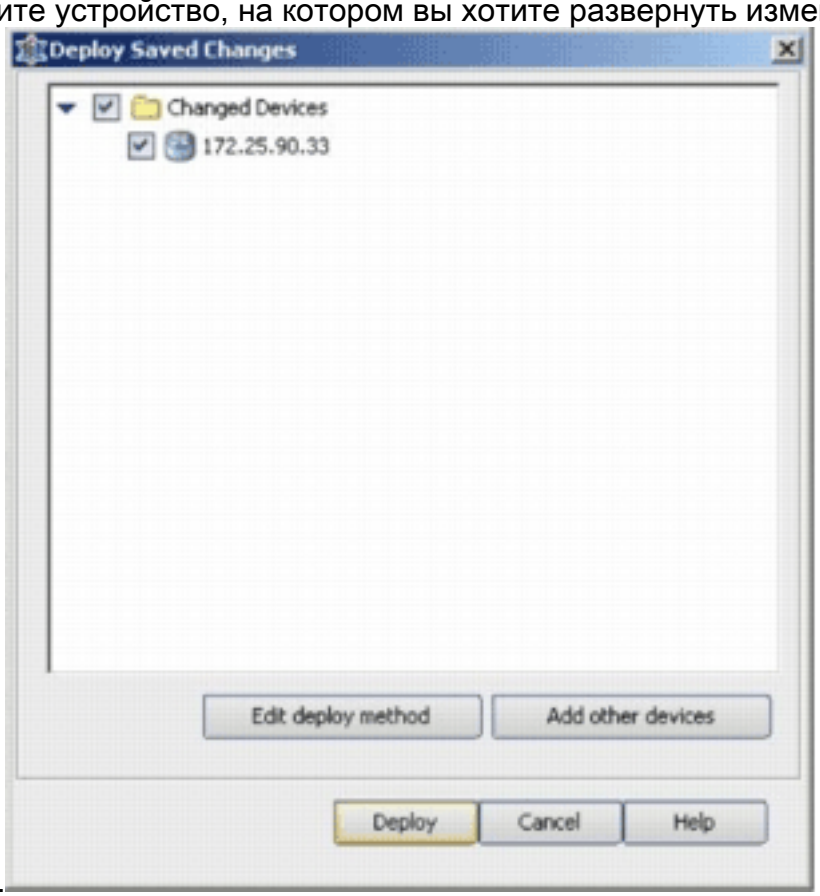
25. Перейдите к IPS и выберите **Signatures** для просмотра списка всех подписей.



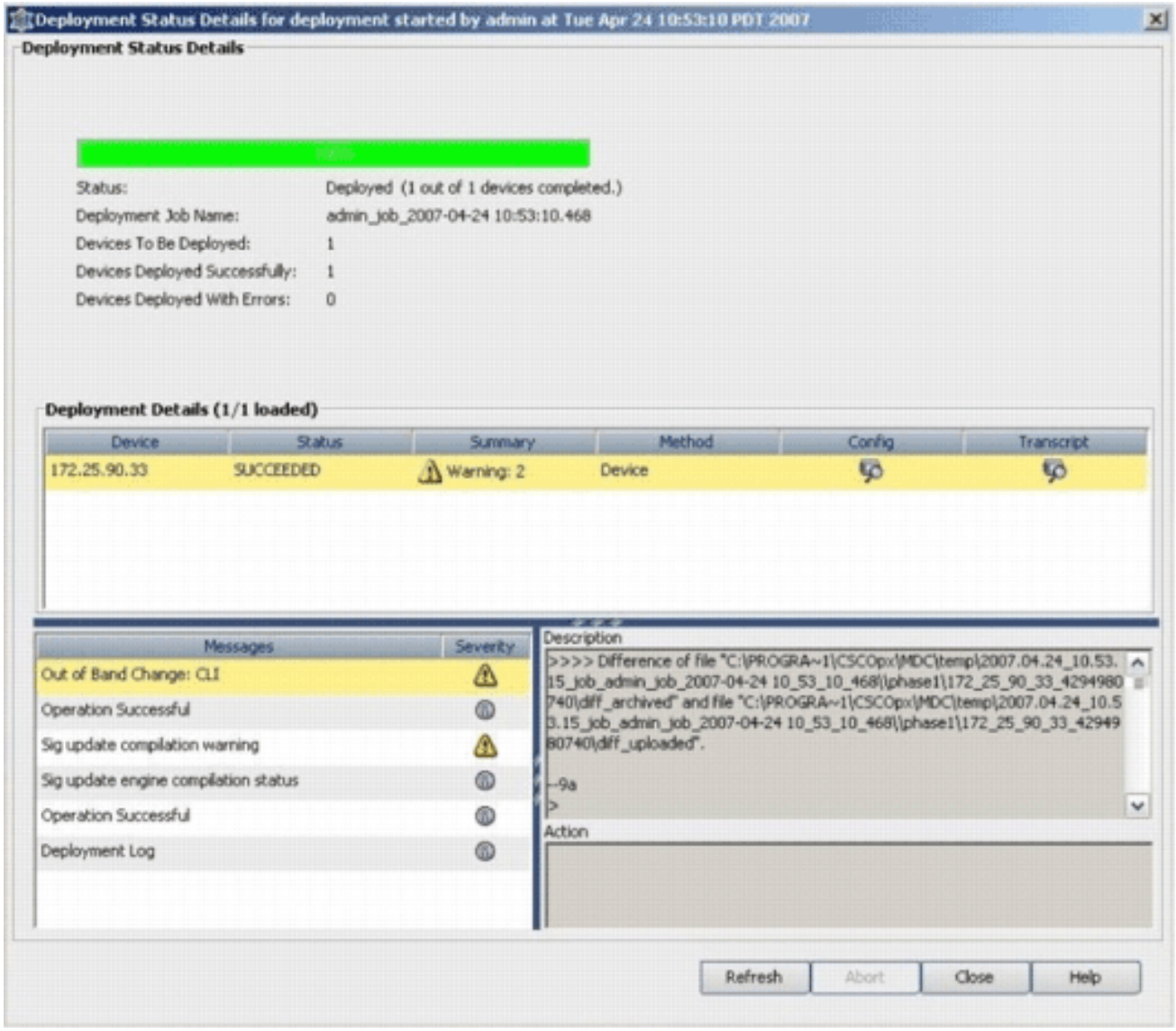
26. Выберите **File> Submit и Deploy** для развертывания IPS на маршрутизаторе IOS.



27. Выберите устройство, на котором вы хотите развернуть изменения и нажать **Deploy**.



28. Просмотрите развернуть статус, чтобы проверить, существуют ли какие-либо ошибки.



Дополнительные сведения

- Продукты Системы предотвращения вторжений (IPS) Cisco IOS и Страница Сервисов
- Начало работы с IPS Cisco IOS с 5.x формат подписи
- IPS 5.x поддержка формата подписи и усовершенствования удобства пользования
- Cisco Intrusion Prevention System
- Уведомления о дефекте для специалистов по продуктам безопасности (включая обнаружение несанкционированного доступа CiscoSecure)
- Техническая поддержка - Cisco Systems