CS 3.x: Добавьте сенсоры IDS и модули к инвентарю менеджера безопасности

Содержание

Введение

Этот документ предоставляет сведения о том, как добавить датчики Системы обнаружения проникновения (IDS), и модули (включает IDSM на Коммутаторах Catalyst 6500, CID NM на маршрутизаторах и SSM AIP на ASA) в Cisco Security Manager (CSM).

Примечание: CSM 3.2 не поддерживает IPS 6.2. Это поддерживается в CSM 3.3.

Предварительные условия

Требования

Этот документ предполагает, что CSM и Устройства IDS установлены и работают должным образом.

Используемые компоненты

Сведения в этом документе основываются на CSM 3.0.1.

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Добавьте устройства к материально-техническим ресурсам менеджера безопасности

Когда вы добавляете устройство к Менеджеру безопасности, вы вводите диапазон определения информации для устройства, такого как его имя DNS и IP-адрес. После добавления устройства это появляется в сведениях об устройствах Менеджера безопасности. Можно управлять устройством в Менеджере безопасности только после добавления его к материально-техническим ресурсам.

Можно добавить устройства к материально-техническим ресурсам Менеджера безопасности с этими методами:

- Добавьте устройство от сети.
- Add A New Device, который еще не находится в сети
- Добавьте одно или более устройств от Репозитория Устройства и Учетных данных (DCR).
- Добавьте одно или более устройств от файла конфигурации.

Примечание: Этот документ фокусируется на методе: Add A New Device, который еще не находится в сети.

Шаги для добавления сенсора IDS и модулей

Используйте добавление Новой Опции устройства для добавления одиночного устройства к материально-техническим ресурсам Менеджера безопасности. Можно использовать эту опцию для предварительной инициализации. Можно создать устройство в системе, назначить политику на устройство и генерировать файлы конфигурации перед получением оборудования устройства.

При получении оборудования устройства необходимо подготовить устройства, которые будут управляемы Менеджером безопасности. См. Подготовку Устройств для Менеджера безопасности для Управления для получения дополнительной информации.

Эта процедура показывает, как добавить новый Детектор обнаружения несанкционированного доступа (IDS Sensor) и модули:

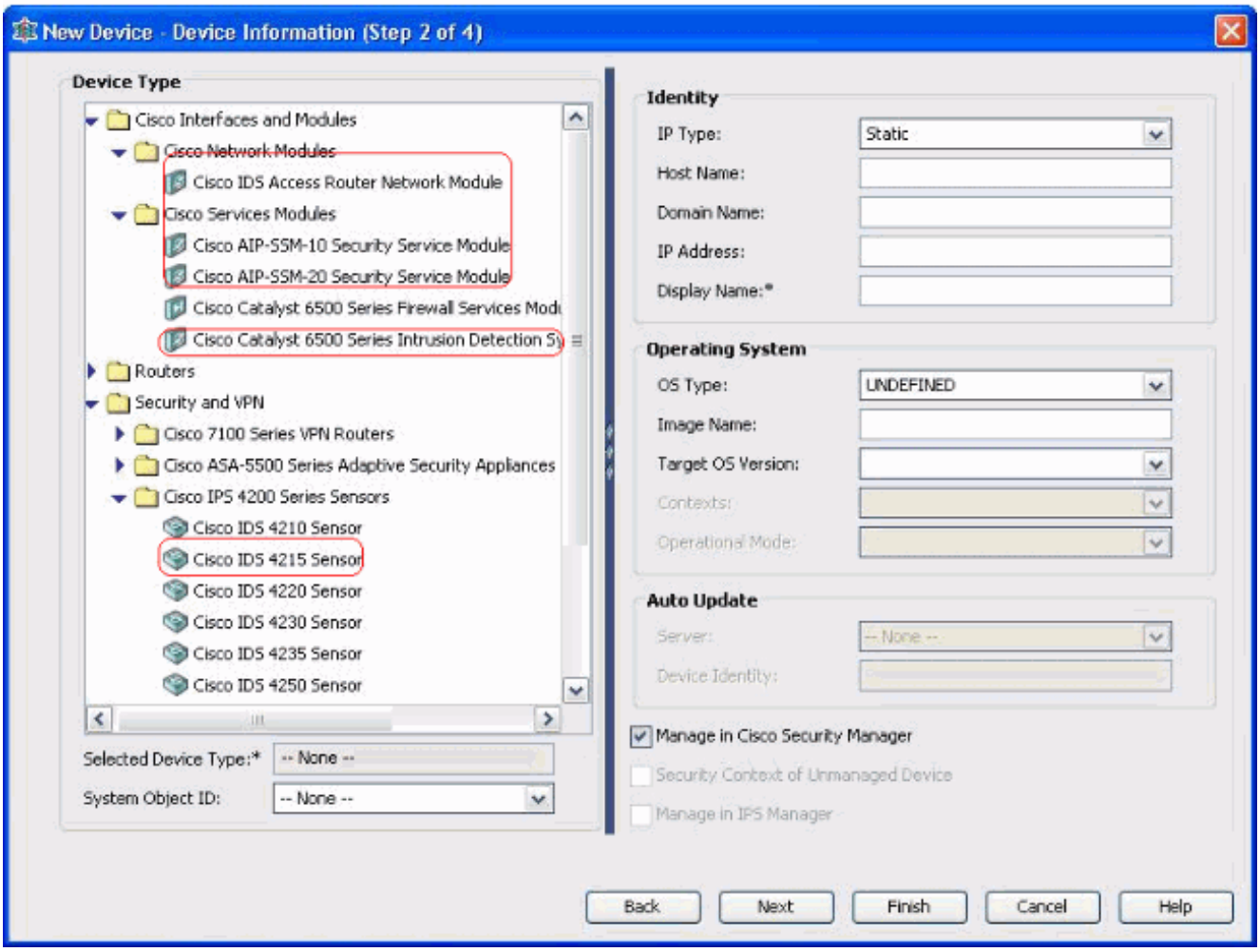
1. Нажмите кнопку **Device View** на панели инструментов.Страница Devices появляется.
2. Нажмите **кнопку Add** в Селекторе устройств.Новое Устройство - Выбирает, страница Method появляется с четырьмя опциями.
3. Выберите **Add New Device**, затем нажмите **Next**.Страница New Device - Device Information появляется.
4. Введите сведения об устройстве в соответствующие поля.Посмотрите Обеспечение Сведений об устройстве — Новый раздел Устройства для получения дополнительной информации.
5. **Нажмите кнопку Finish.**Система выполняет задачи проверки устройства:Если данные являются неправильными, система генерирует сообщения об ошибках и отображает страницу, на которой ошибка происходит со значком красной ошибки, который

соответствует ему.Если данные корректны, устройство добавлено к материально-техническим ресурсам, и это появляется в Селекторе устройств.

Обеспечение сведений об устройстве — новое устройство

Выполните следующие действия:

1. Выберите тип устройства для нового устройства:Выберите папку типа устройства верхнего уровня для отображения семейств поддерживаемого устройства.Выберите папку семейства устройств для отображения типов поддерживаемого устройства.Выберите **Cisco Interfaces and Modules> Cisco Network Modules** для добавления **модуля Cisco IDS Access Router Network Module**. Аналогично, выберите **Cisco Interfaces and Modules> Cisco Services Modules** для добавления SSM AIP и показанных модулей IDSM.Выберите **Security and VPN> Cisco IPS 4200 Series Sensors** для добавления датчика Cisco IDS 4210 к материально-техническим ресурсам CSM.



Выберите тип устройства.**Примечание:** После добавления устройства вы не можете изменить тип устройства.ID системного объекта для того типа устройства отображены в поле SysObjectId. Первый ID системного объекта выбран по умолчанию. Можно выбрать другой в случае необходимости.
2. Введите идентификационную информацию устройства, такую как тип IP (статичный или динамичный), имя хоста, доменное имя, IP-адрес и название показа.
3. Введите информацию об операционной системе устройства, такую как тип ОС, имя образа, предназначайтесь для Версии операционной системы, контекстов и

операционного режима.

4. Поле Auto Update или CNS-Configuration Engine появляется, который зависит от типа устройства, который вы выбираете:Автоматическое обновление — Отображенный для Межсетевого экрана PIX и устройств ASA.Механизм Конфигурации CNS — Отображенный для маршрутизаторов Cisco IOS®.**Примечание:** Это поле не активно для Catalyst 6500/7600 и устройства FWSM.
5. Выполните следующие действия:Автоматическое обновление — Щелчок стрелка для отображения списка серверов. Выберите сервер, который управляет устройством. Если сервер не появляется в списке, выполните эти шаги:Нажмите стрелку, затем выберите **+, Добавляет Сервер**... Диалоговое окно Server Properties появляется.Введите информацию в обязательные поля.**Нажмите кнопку ОК.** Новый сервер добавлен к списку доступных серверов.Механизм Конфигурации CNS — Другая информация отображена, который зависит от того, выбираете ли вы статичный или тип динамического IP:**Статичный** — Щелчок стрелка для отображения списка Механизмов Конфигурации. Выберите Configuration Engine, который управляет устройством. Если Механизм Конфигурации не появляется в списке, выполните эти шаги:Нажмите стрелку, затем выберите **+, Добавляет Механизм Конфигурации**... Диалоговое окно со свойствами Механизма Конфигурации появляется.Введите информацию в обязательные поля.**Нажмите кнопку ОК.** Новый Механизм Конфигурации добавлен к списку доступных Механизмов Конфигурации.**Dynamic** — Нажмите стрелку для отображения списка серверов. Выберите сервер, который управляет устройством. Если сервер не появляется в списке, выполните эти шаги:Нажмите стрелку, затем выберите **+, Добавляет Сервер**... Диалоговое окно Server Properties появляется.Введите информацию в обязательное поле.**Нажмите кнопку ОК.** Новый сервер добавлен к списку доступных серверов.
6. Выполните следующие действия:Для управления устройством в Менеджере безопасности проверьте флажок **Manage in Cisco Security Manager**. !--- Это стандартный вариант.Если единственная функция устройства, которое вы добавляете, должна служить оконечная точкой VPN, снимите флажок с флажком **Manage in Cisco Security Manager**.Менеджер безопасности не будет управлять конфигурациями или загружать или загружать конфигурации на этом устройстве.
7. Проверьте флажок Security Context of Unmanaged Device для управления контекстом безопасности, родительским устройством которого (межсетевой экран PIX, ASA или FWSM) не управляет Менеджер безопасности.Можно разделить Межсетевой экран PIX, ASA или FWSM во множественные межсетевые экраны безопасности, также известные как контексты безопасности. Каждый контекст является независимой системой с ее собственной конфигурацией и политикой. Можно управлять этими автономными контекстами в Менеджере безопасности, даже при том, что родителем (межсетевой экран PIX, ASA или FWSM) не управляет Менеджер безопасности.**Примечание:** Это поле активно, только если устройство, которое вы выбрали в Селекторе устройств, является устройством с функциями межсетевого экрана, таким как Межсетевой экран PIX, ASA или FWSM, который поддерживает контекст безопасности.
8. Проверьте **Управление во флажке Manager IPS** для управления маршрутизатором Cisco IOS в Менеджере IPS.Это поле активно, только если вы выбрали маршрутизатор Cisco IOS от Селектора устройств.**Примечание:** Менеджер IPS может управлять функциями IPS только на маршрутизаторе Cisco IOS, который имеет возможности IPS. Для получения дополнительной информации см. документацию IPS.При проверке

Управления во флажке Manager IPS необходимо проверить флажок Manage in Cisco Security Manager также.Если выбранное устройство является IDS, это поле не активно. Однако флажок проверен, потому что Менеджер IPS управляет Детекторами обнаружения несанкционированного доступа (IDS Sensor).Если выбранным устройством является Межсетевой экран PIX, ASA или FWSM, это поле не активно, потому что Менеджер IPS не управляет этими типами устройства.

9. **Нажмите кнопку Finish.**Система выполняет задачи проверки устройства:Если данные, которые вы ввели, являются неправильными, система генерирует сообщения об ошибках и отображает страницу, где происходит ошибка.Если данные, которые вы ввели, корректны, устройство добавлено к материально-техническим ресурсам, и это появляется в Селекторе устройств.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Сообщения об ошибках

Когда вы добавляете IPS к CSM, сообщение об ошибках `Invalid device: Could not deduce the SysObjId for the platform type` появляется.

Решение

Выполните эти шаги для решения этого сообщения об ошибках.

1. Остановите сервис Демона CSM в Windows, и затем выберите **Program Files> CSCOpx> MDC> Афина> config> Каталог**, где можно найти `VMS-SysObjID.xml`.
2. В системе CSM замените исходный файл VMS-SysObjID.xml, расположенный по умолчанию в `C:\Program Files\CSCOpx\MDC\athena\config\directory` с последним файлом `VMS-SysObjID.xml`.
3. Перезапустите Менеджера демона CSM сервис (CRMDmgtd) и повторная попытка, чтобы добавить или обнаружить устройство (устройства), на которое влияют, снова.

Дополнительные сведения

- Страница технической поддержки Cisco Security Manager
- Страница технической поддержки Cisco Intrusion Detection System
- Cisco Systems – техническая поддержка и документация