Менеджер безопасности 4.3: общие проблемы IPS и решения

Содержание

Введение

Этот документ описывает Типичные проблемы и способы их решения к системе предотвращения вторжений Cisco (IPS) (IPS) проблемы в Cisco Security Manager.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии 4.3 Cisco Security Manager.

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.

Родственные продукты

Этот документ описывает типичные проблемы, с которыми встречаются в Cisco Security Manager 4.3. В то время как этот документ фокусируется на версии 4.3 Cisco Security Manager, возможно, что те же проблемы и решения применяются к другим версиям также.

Не может соединиться с IPS

Проблема

Вы больше не можете соединяться с IPS через Cisco Security Manager. Однако можно соединиться с Secure Shell (SSH) и диспетчером устройств IPS (IDM) от сервера Cisco Security Manager.

Решение

Проверьте, что IPS использует текущий сертификат X.509. **Всем заправляйте команда version** в CLI IPS для проверки версии сертификата. Если сертификат истек, выполнял **ключевую для tls генерирует** команду для получения нового сертификата. После того, как вы генерируете ключ, импортируете сертификат IPS.

Датчик SSM AIP, не распознанный после обновления к 7.1 (6) E4

Проблема

После обновления Cisco ASA Усовершенствованный Модуль Сервисов безопасности Контроля и Предотвращения (SSM AIP) модуль к версии 7.1 (6) E4 в версии 4.3 Cisco Security Manager Cisco Security Manager не распознает датчик SSM AIP.

Решение

Для решения этой проблемы необходимо установить Пакет обновления версии 4.3 Cisco Security Manager 1 или Пакет обновления 2, к серверу Cisco Security Manager так, чтобы это поддержало SSM AIP с программным обеспечением на 7.1 дюйм в секунду.

Подписи IPS, не автоматически обновленные в течение льготного периода

Проблема

Cisco Security Manager автоматически не обновляет ваше событие подписей IPS невзирая на то, что ваш IPS все еще в льготном периоде.

Решение

Если датчик в течение льготного периода, Cisco Security Manager не обновляет подписи автоматически. Для решения этой проблемы выберите **Tools> обновления Apply IPS** в интерфейсе Cisco Security Manager для ручного обновления подписей.

Большое число запросов RADIUS к устройствам IPS

Проблема

Вы видите большое число Запросов RADIUS с Cisco Security Manager на ваши устройства IPS.

Решение

Когда Cisco Security Manager быстро опрашивает проверенные устройства, эта проблема происходит. По умолчанию затрагиваемые версии Мониторинга событий (обработка событий) функция на Cisco Security Manager могут попытаться опросить проверенные устройства несколько раз в секунду. Если другие опции мониторинга Cisco Security Manager (состояние и Менеджер Монитора производительности и/или Отчёта) активированы, дополнительные опросы устройства происходят.

Для решения этой проблемы можно изменить время ожидания по умолчанию (интервал сна). Интервал сна по умолчанию между опросами устройства установлен в 250 мс по умолчанию. Это значение может быть изменено вручную на большую, более рыночную стоимость. Для изменения значения времени ожидания отредактируйте communication.properties файл на сервере Cisco Security Manager; этот файл расположен в <*NMSROOT*> \MDC\eventing\config\communication.properties.

В communication.properties файле, замене `SLEEP_INTERVAL_SYNCH_CALLS=250` с `SLEEP_INTERVAL_SYNCH_CALLS=2000`.

> **Примечание:** Значение задано в миллисекундах (мс); поэтому, 2000 составляет уравнение к 2 секундам.

Внимание. : Проявите осмотрительность при редактировании этого файла. Изменяется на этот файл кроме упомянутого выше того, может вызвать нежелательные влияния к Cisco Security Manager.

После того, как вы измените и сохраните файл, гарантируете, что все клиентские приложения Cisco Security Manager закрыты, и затем перезапускают Менеджера демона Cisco Security Manager (CRMDmgtd) сервис.

Дополнительные сведения

- Cisco Security Manager 4.3 установки и руководство по обновлению
- Cisco Systems – техническая поддержка и документация