MARS CS: добавьте датчик Cisco IPS как устройство создания отчетов к примеру конфигурации MARS CS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Родственные продукты
Условные обозначения
Настройка
Добавьте и настройте Cisco IPS 6.x или 7.x устройство в MARS
Проверьте что События Получений по запросу MARS от Устройства Cisco IPS
Устранение неполадок
Дополнительные сведения

Введение

Этот документ объясняет, как подготовить устройство Системы предотвращения вторжений (IPS) Cisco Secure и любые настроенные действительные датчики для действия как устройства создания отчетов к Мониторингу Cisco Security, Анализу и Системе ответа (MARS CS).

Предварительные условия

Требования

Для Cisco IPS 5.x, 6.x, и 7.x устройства, MARS вытягивает журналы с помощью SDEE по SSL. Поэтому MARS должен иметь доступ HTTPS к датчику. Для подготовки датчика необходимо включить сервер HTTP на датчике, позволить TLS предоставить доступ HTTPS и удостовериться, что IP-адрес MARS определен как позволенный хост, тот, который может обратиться к датчику и вытянуть события. Если датчики были настроены для предоставления доступа от ограниченных хостов или подсетей в сети, можно использовать **команду access-list ip_address/netmask** для включения этого доступа.

Используемые компоненты

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

- Устройство MARS Cisco Secure, которое работает под управлением ПО версии 4.2.x и позже
- Устройство IPS Cisco серии 4200, которое работает под управлением ПО версии 6.0 и позже

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

Эта конфигурация может также использоваться с этими датчиками:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS-4270-20

Условные обозначения

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

Настройка

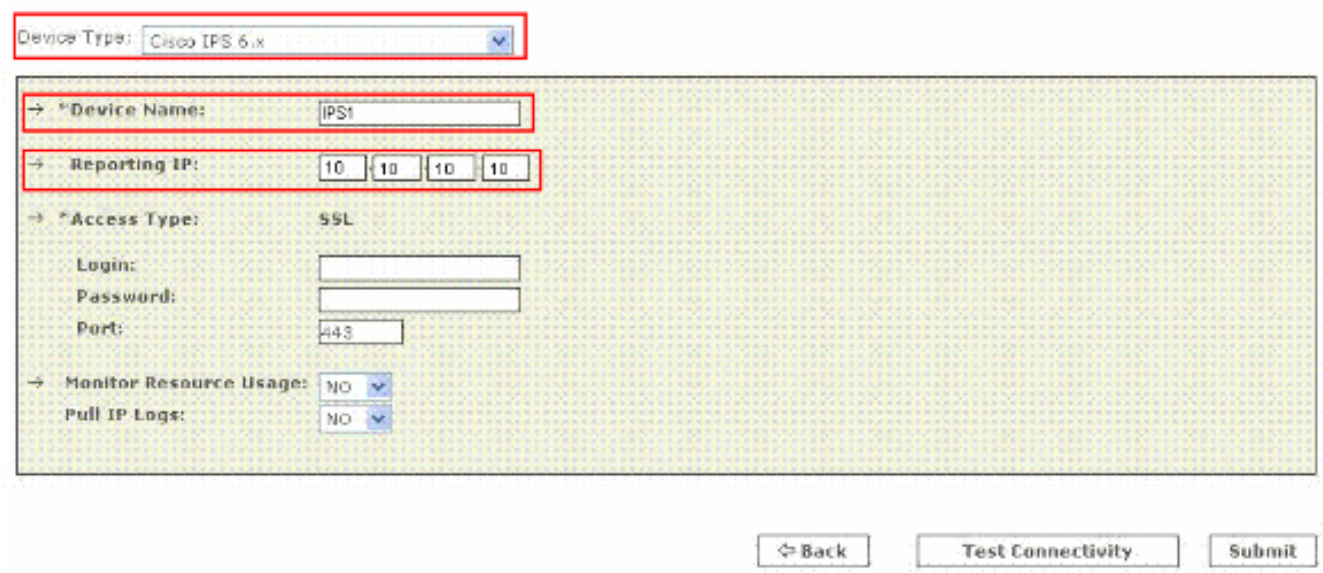
В этом разделе вам предоставляют информацию о том, как добавить и настроить датчик Системы предотвращения вторжений (IPS) Cisco Secure к Мониторингу Cisco Security, Анализу и Системе ответа (MARS CS) устройство.

Добавьте и настройте Cisco IPS 6.x или 7.x устройство в MARS

При определении Cisco IPS 6.x или 7.x устройство в MARS можно обнаружить любые действительные датчики, настроенные на устройстве. При обнаружении этих действительных датчиков это позволяет MARS разделять события, о которых сообщают, действительным датчиком. Это также позволяет вам настраивать список отслеживаемых сетей к каждому действительному датчику, который улучшает точность желаемого создания отчетов.

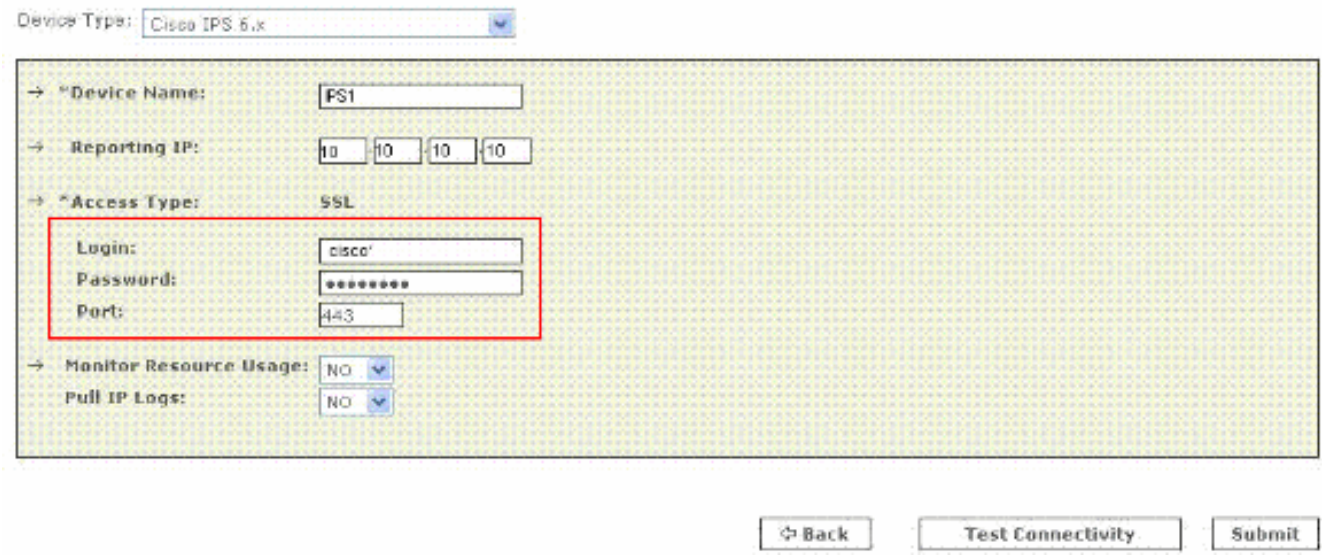
Выполните эти шаги, чтобы добавить и настроить Cisco IPS 6.x или 7.x устройство в MARS:

1. Выберите **Admin>> Security System Setup и Устройства мониторинга**. Затем щелкните **по Add**.
2. Выберите **Cisco IPS 6.x или Cisco IPS 7.x** из списка Типа устройства. Теперь введите имя хоста датчика в поле **Device Name** как показано здесь. IPS1 является Имя устройства, используемое в данном примере. Значение Имени устройства должно быть идентично настроенному названию
датчика.



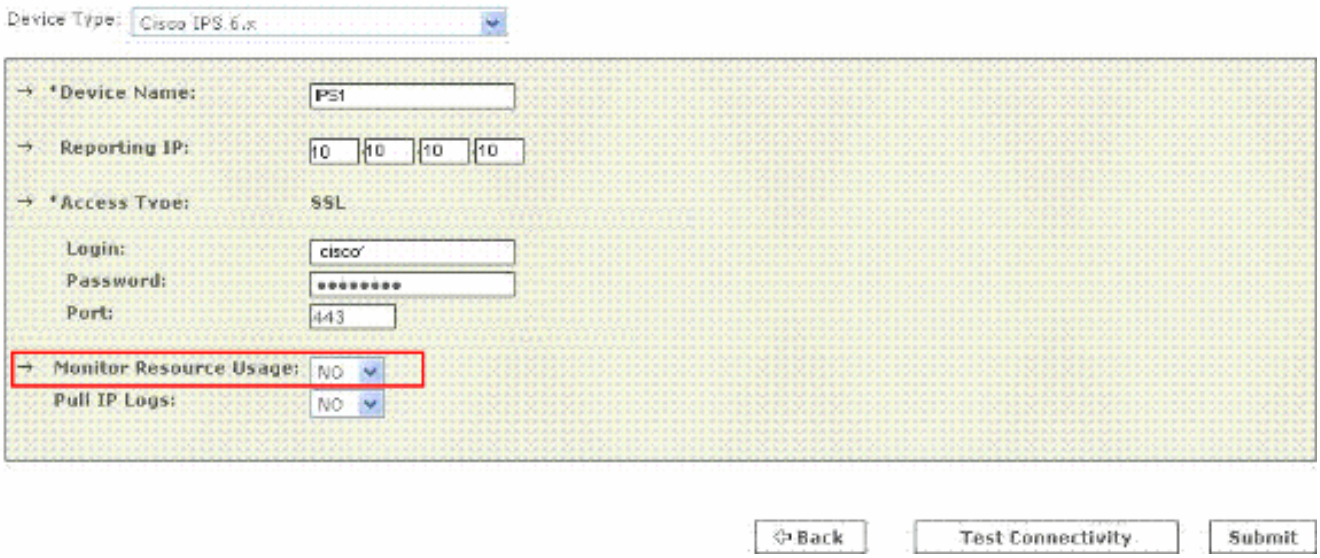
Теперь введите административный IP-адрес в поле **Reporting IP**. IP-адрес Создания отчетов является тем же адресом как административный IP-адрес.

3. В **поле Login** введите имя пользователя, привязанное к административной учетной записи, которая используется для доступа к устройству создания отчетов. Теперь, в **Поле Password**, введите пароль, привязанный к имени пользователя, заданному в **поле Login**. **Имя пользователя** является **Cisco**, и используемый **пароль** является **cisco123** в данном примере. Также введите номер порта TCP, на котором веб-сервер, работающий на датчике, прослушивает **поле Port**. Порт HTTPS по умолчанию 443.

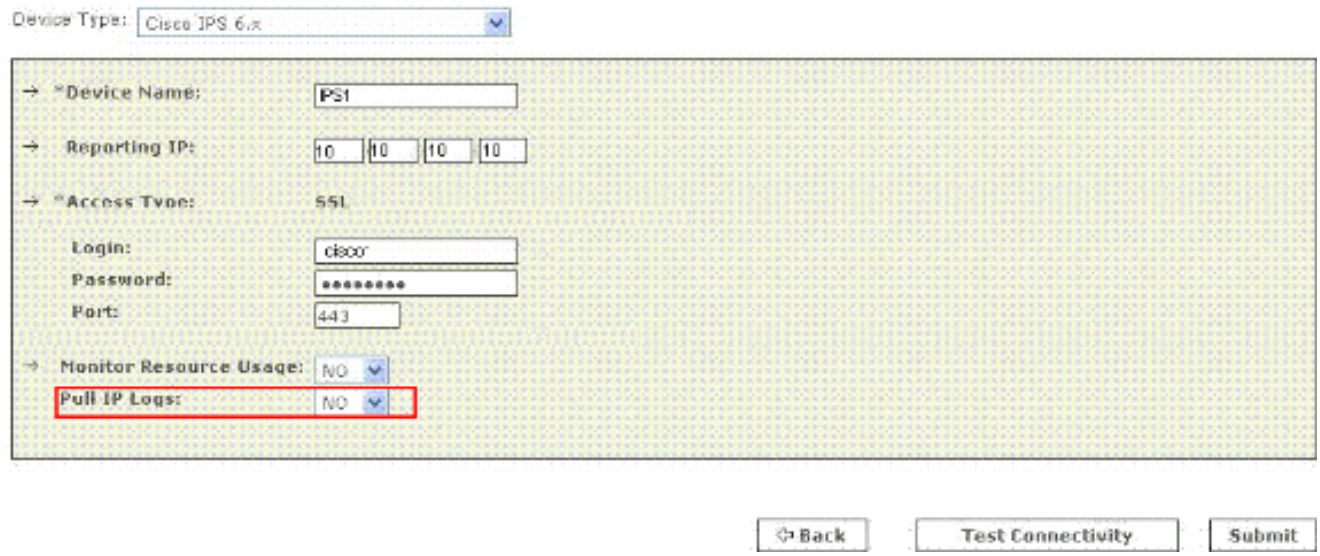


Примечание: В то время как возможно настроить HTTP только, MARS требует HTTPS.

4. Теперь проверьте, что **НЕ** chosed в списке **Использования ресурса Монитора**. В то время как опция Monitor Resource Usage появляется на этой странице, она не функционирует для Cisco IPS.

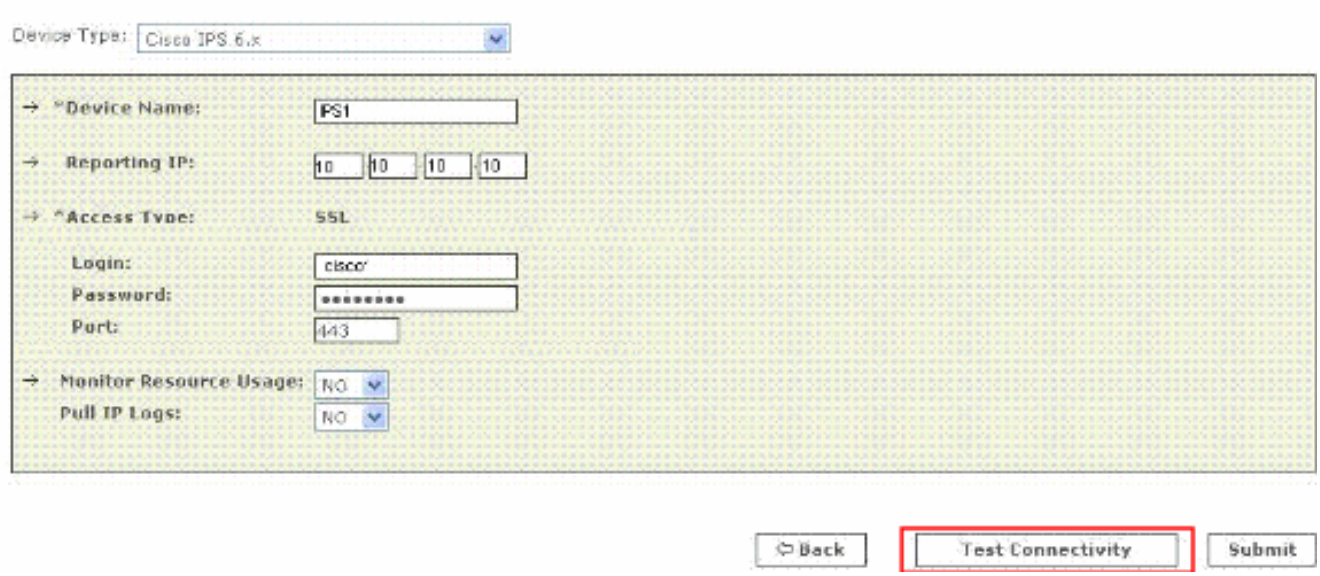


5. Для получения по запросу журналов IP от датчика выберите **Yes** из списка **Журналов IP Получения по запросу**. Это - дополнительная функция, которая может быть использована при
необходимости.

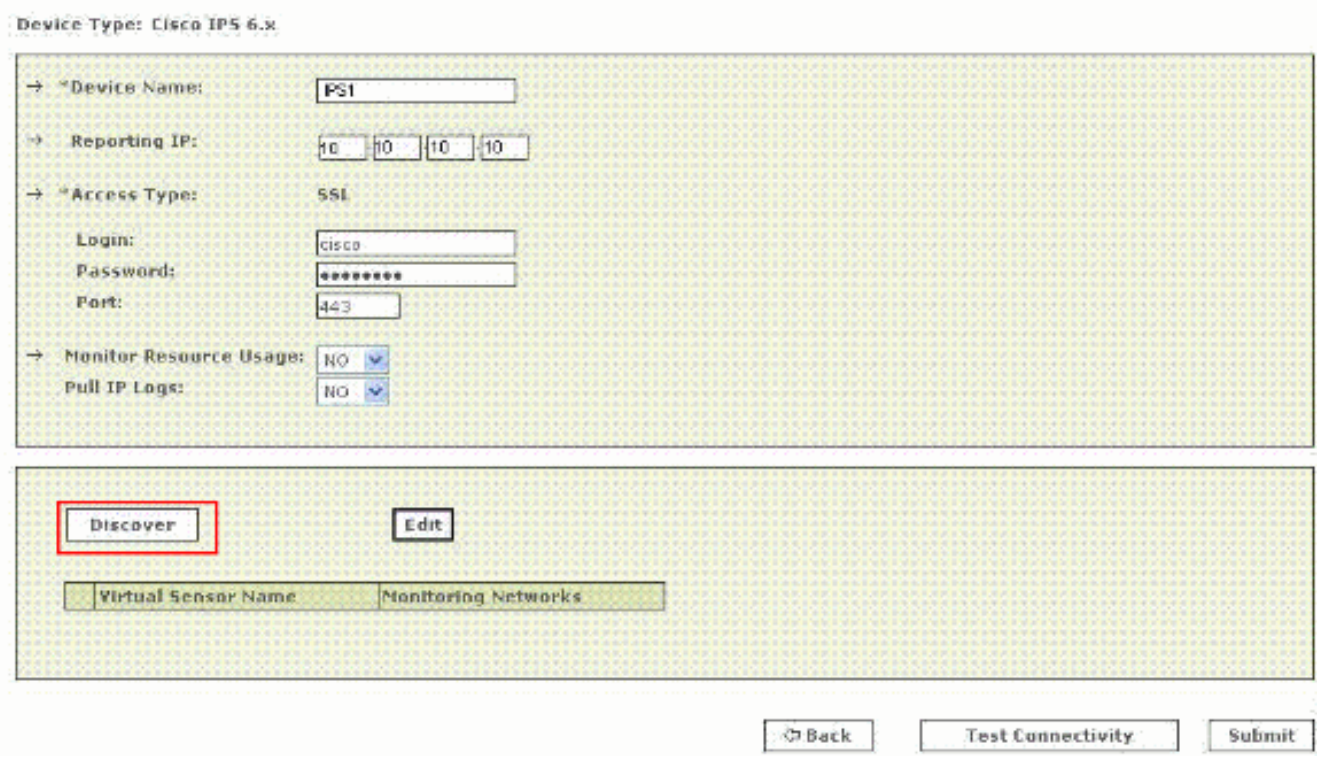


Эта установка применяется ко всему датчику, который включает те журналы, генерируемые для действительных предупреждений датчиков.

6. Нажмите **Test Connectivity**, чтобы проверить конфигурацию и включить обнаружение действительных
датчиков.

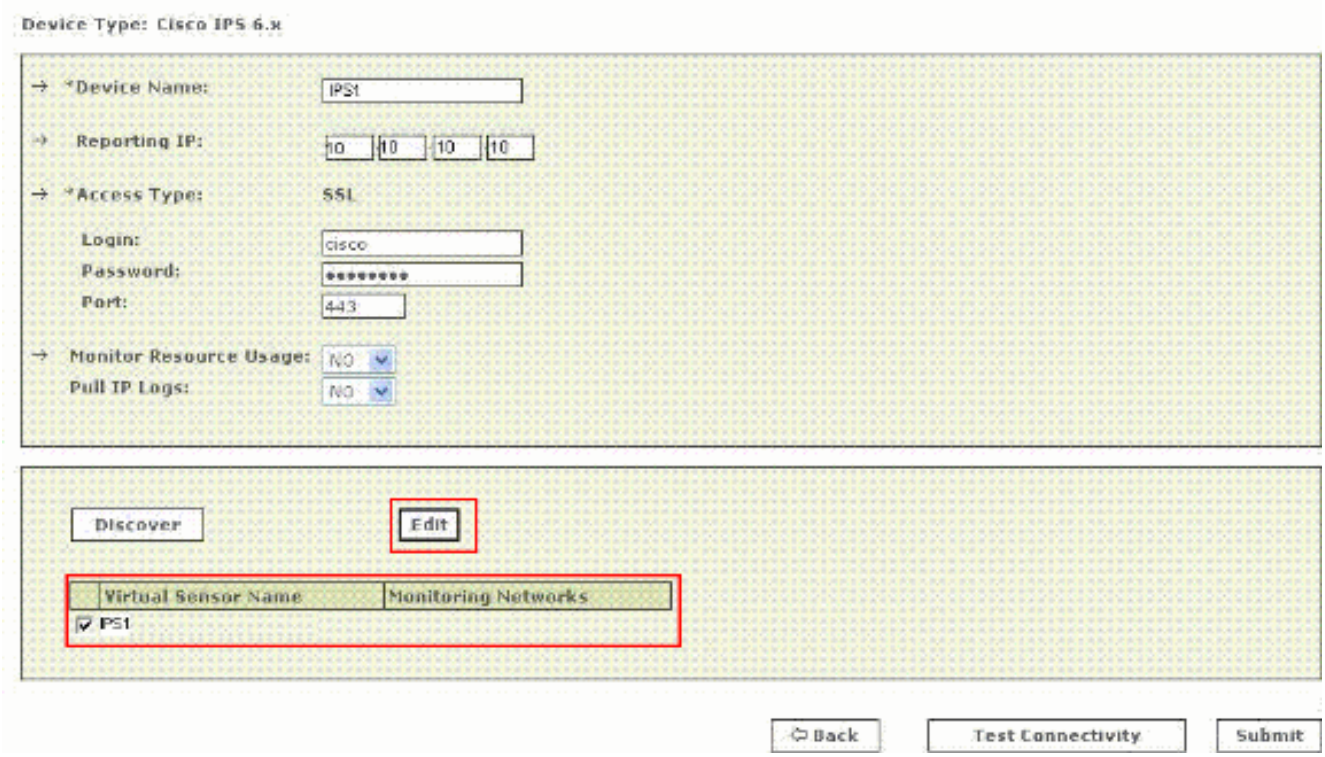


7. Нажмите **Discover** для обнаружения любых определенных действительных датчиков.

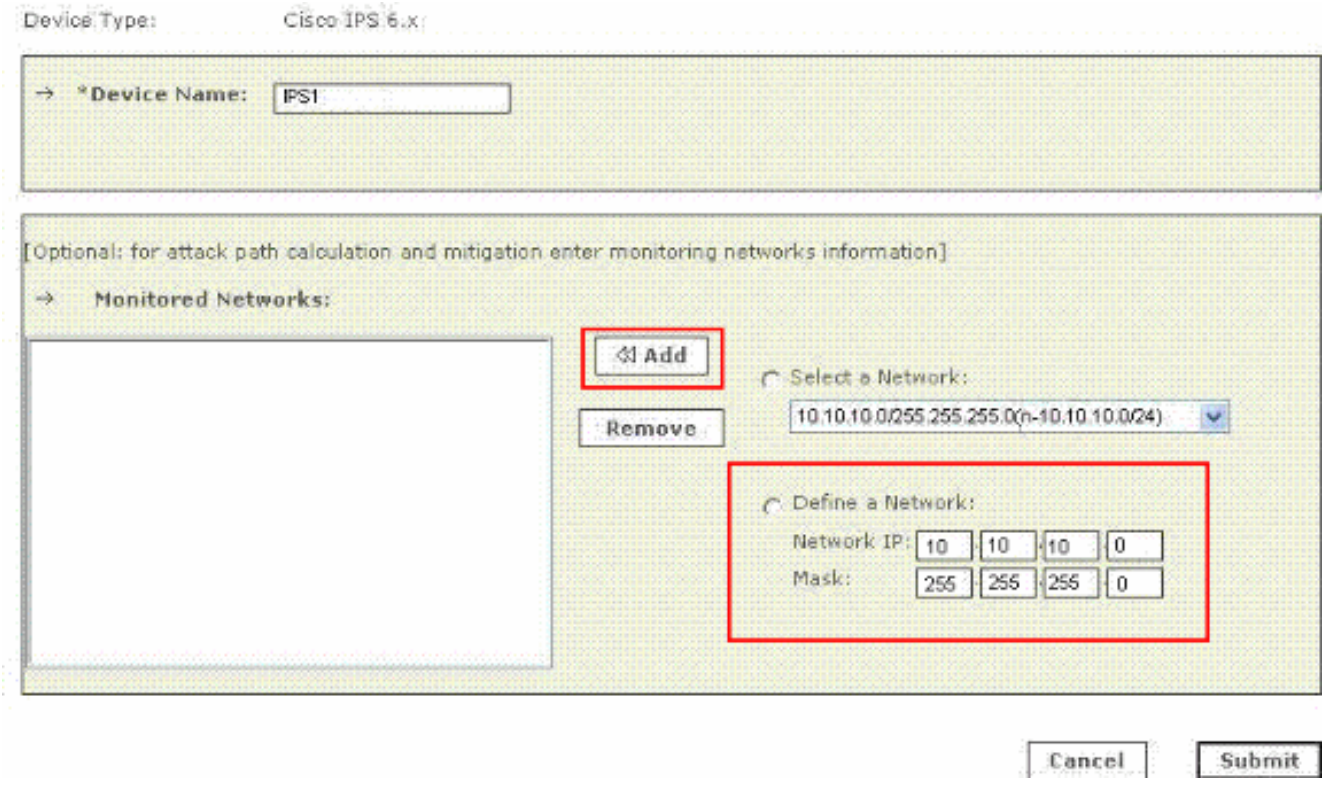


Примечание: MARS не знает об изменениях, внесенных в датчик. Каждый раз, когда вы вносите изменения в действительные параметры настройки датчика, необходимо нажать **Discover** на той странице конфигурации сенсора для обновления действительных подробных данных датчика в MARS.

8. Выберите флажок рядом с Действительным Названием Датчика и нажмите **Edit** для определения отслеживаемых сетей для каждого действительного датчика. Теперь страница IPS Module появляется как показано
здесь.



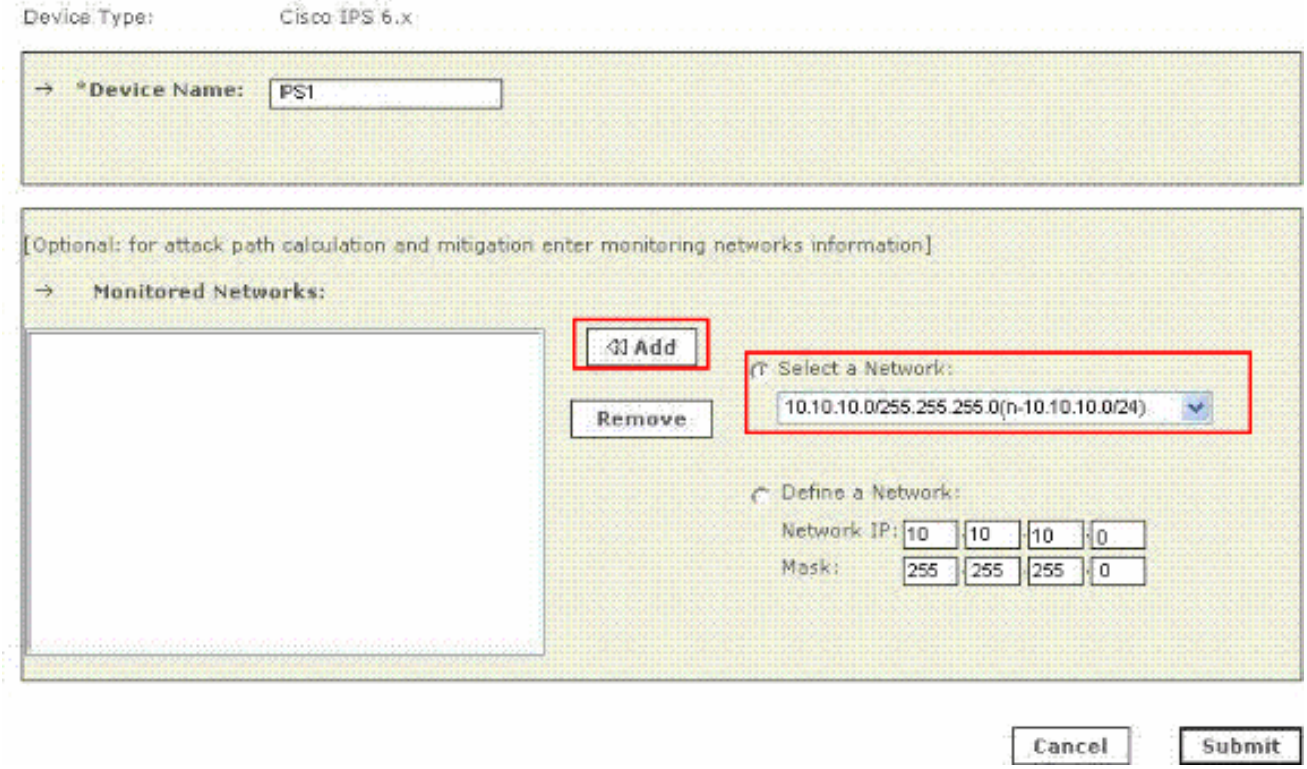
9. Для вычисления пути атаки и смягчения, задайте сети, проверяемые датчиком. Выберите кнопку с зависимой фиксацией **Define a Network** для ручного определения сети. Затем выполните эти шаги для определения Сети:Введите сетевой адрес в поле **Network IP**.Введите соответствующее значение маски сети в поле **Mask**.**Нажмите Add** для перемещения указанной сети в поле Monitored Networks.Повторите предыдущие шаги, если существует потребность определить больше сетей.



Примечание: Это - доступная дополнительная функция и может быть пропущено если не требуемый.

10. Нажмите кнопка с зависимой фиксацией **Select a Network** в заказе выбирают сети, которые присоединены к устройству. Затем выполните эти шаги для выбора сетей:Выберите сеть из **Выбора Список сети**.**Нажмите Add** для перемещения

указанной сети в поле Monitored Networks.Повторите предыдущие шаги, если существует потребность выбрать больше
сетей.



Примечание: Это - доступная дополнительная функция и может быть пропущено если не требуемый.

11. Повторите **шаг 8** посредством **шага 10** для каждого действительного датчика.
12. Нажмите **Submit** для сохранения изменений. Имя устройства появляется под Безопасностью и Контролирующим информационным списком. Отправлять операция делает запись изменений в таблицах базы данных. Но, это не загружает изменения в оперативную память Устройства MARS. Активировать загрузки операции отправили изменения в оперативную память.
13. Нажмите **Activate**, чтобы позволить MARS запуститься к sessionize событиям с этого устройства.MARS начинается к sessionize событиям, генерируемым этим модулем, и оцените те события с помощью определенных правил контроля и отбрасывания. Любые события, публикованные устройством в MARS перед активацией, можно делать запрос с IP-адресом создания отчетов устройства как критерий соответствия. См. Активируют Устройства Создания отчетов и Смягчения. для получения дополнительной информации об активировать действии.

Проверьте что События Получений по запросу MARS от Устройства Cisco IPS

Распространено создать мягкие события в сети для проверки потока данных. Выполните эти шаги для проверки потока данных между устройством Cisco IPS и MARS:

1. На устройстве Cisco IPS включите и предупредите на подписях 2000 и 2004. Подписи контролируют сообщения ICMP (эхо-запросы).
2. Пропингуйте устройство на подсети, на которой слушает устройство Cisco IPS. События генерирует и вытягивает MARS.

3. Проверьте, что события появляются в веб-интерфейсе MARS. Можно выполнить запрос с устройством Cisco IPS.
4. Как только поток данных проверен, можно отключить подписи 2000 и 2004 годов на устройстве Cisco IPS.**Примечание:** Если Тестовая операция Подключения не отказывает во время конфигурации устройства Cisco IPS в веб-интерфейсе MARS, то связь включена. Эта задача позволяет вам далее проверять, что предупреждения генерируют и вытягивают правильно.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Страница технической поддержки системы Cisco Security Monitoring, Analysis and Response System
- Страница технической поддержки системы предотвращения вторжений Cisco (IPS)
- Система Cisco Security Monitoring, Analysis and Response System - Информация о совместимости
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация