Диспетчер устройств системы защиты от проникновения Intrusion Prevention System Device Manager 5.1 - опознавательная мелодия

Содержание

Введение

Система предотвращения вторжений (IPS) 5.1 содержит более чем 1000 встроенных подписей по умолчанию. Вы не можете переименовать или удалить подписи из списка встроенных подписей, но можно исключить подписи для удаления их из механизма считывания. Можно позже активировать исключенные подписи. Однако этот процесс требует, чтобы механизмы считывания восстановили свою конфигурацию, которая занимает время и могла задержать обработку трафика. Можно настроить встроенные подписи при регулировке нескольких параметров подписи. Встроенные подписи, которые модифицировались, называют *настроенными подписями*.

Этот документ иллюстрирует шаги в использование для настройки подписи с помощью диспетчера устройств IPS (IDM). IDM является находящимся на web, Приложение Java, которое позволяет вам настроить и управлять своим Датчиком. Web-сервер для IDM находится на Датчике. Можно обратиться к нему через Internet Explorer, Netscape или web-браузеры Mozilla.

Примечание: Можно создать подписи, которые называют *пользовательскими подписями*. Пользовательские идентификаторы подписи начинаются в 60000. Можно настроить их для нескольких вещей, таких как соответствие строк на UDP - подключениях, отслеживании сетевых лавинных рассылок и просмотрах. Каждая подпись создана с помощью устройства для подписи, специально предназначенного для типа трафика, который проверен.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Менеджере устройств системы предотвращения вторжений Cisco (IPS) 5. x.

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.

Общие сведения

Для настройки Датчика для мониторинга сетевого трафика для особой подписи, необходимо включить подпись. По умолчанию самые важные подписи включены при установке обновления подписи. Когда атака обнаружена, который совпадает с включенной подписью, Датчик генерирует предупреждение, которое сохранено в хранилище события Датчика. Предупреждения, а также другие события, могут быть получены из хранилища события находящимися на web клиентами. По умолчанию Датчик регистрирует все информационные предупреждения или выше.

Некоторые подписи имеют вспомогательные подписи. Т.е. подпись разделена на подкатегории. При настройке вспомогательной подписи изменения, внесенные в параметры одной вспомогательной подписи, применяются только к той вспомогательной подписи. Например, если вы редактируете вспомогательную подпись подписи 3050 1 и изменяете степени серьезности ошибки, изменение степеней серьезности ошибки применяется только к вспомогательной подписи 1 а не к 3050 2, 3050 3, и 3050 4.

Подписи мелодии

+ значок указывает, что больше опций доступно для этого параметра. Нажмите **+** значок, чтобы развернуть раздел и просмотреть оставшиеся параметры.

Зеленый значок указывает, что параметр в настоящее время использует значение по умолчанию. Нажмите зеленый значок для изменения его на красный, который активирует поле parameter, таким образом, можно отредактировать значение.

Пошаговая процедура

Выполните эти шаги для настройки подписей:

1. Войдите к IDM с помощью учетной записи с привилегиями администратора или оператора.
2. Выберите **Configuration> Signature Definition> Signature Configuration**.Область Signature Configuration появляется.
3. Для определения местоположения подписи выберите опцию сортировки из **Выбрать** списка **By**.Например, если вы ищете подпись Лавинной рассылки UDP, выбираете **L2/L3/L4 Protocol** и затем **Лавинные рассылки UDP**.Обновления области Signature Configuration и показы только те подписи, которые совпадают с вашими критериями сортировки.
4. Для настройки существующей подписи выберите подпись и выполните эти шаги:Нажмите **Edit** для открытия диалогового окна Edit Signature.Рассмотрите значения параметра и измените значение любого параметра, который вы хотите настроить.**Примечание:** Для выбора нескольких действий события удержите в нажатом состоянии **клавишу CTRL**.Под Статусом выберите **Yes** для включения подписи.**Примечание:** Подпись должна быть позволена для Датчика активно обнаружить атаку, заданную подписью.Под Статусом задайте, исключена ли эта подпись. Нажмите **No** для активации подписи. Это размещает подпись в механизм.**Примечание:** Подпись должна быть активирована для Датчика для активного обнаружения атаки, заданной подписью.**Примечание:** Нажмите **Cancel**, чтобы отменить ваши изменения и закрыть диалоговое окно Edit Signature.**Нажмите кнопку ОК.**Отредактированная подпись теперь появляется в списке с набором Типа к Настроенному.**Примечание:** Если вы хотите отменить свои изменения, нажмите **Reset**.
5. Нажмите **Apply**, чтобы применить ваши изменения и сохранить пересмотренную конфигурацию.

Дополнительные сведения

- Cisco Intrusion Prevention System
- Cisco Systems – техническая поддержка и документация