Содержание

Введение

Этот документ предоставляет пояснения, преимущества и примеры для конфигурации суммирования на системе предотвращения вторжений Cisco (IPS) (IPS).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Устройство адаптивной защиты Cisco (ASA) 5500 или 5500x система предотвращения вторжений Cisco (IPS) (IPS) модули
- IPS 4200, 4300, или устройства IPS серии 4500
- МОДУЛЬ IPS NME
- Предупреждения подписи IPS

Используемые компоненты

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

- ASA 5500 или 5500x Модули ips

- IPS 4200, 4300 или устройства IPS серии 4500
- МОДУЛЬ IPS NME

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

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

Общие сведения

Суммирование IPS предоставляет режимы для агрегации событий в одиночное предупреждение, так, чтобы могла быть уменьшена громкость предупреждений, передаваемых датчиком. Каждая подпись создана с настройками по умолчанию, которые отражают предпочтительное, нормальное поведение. Однако каждая подпись имеет специальные параметры, которые влияют, как предупреждения обрабатываются, таким образом, поведение по умолчанию подписей может быть настроено в рамках ограничений для каждого типа модуля.

Суммирование и действия события обработаны после того, как meta механизм обработал события компонента. Это позволяет часам датчика для подозрительной операции по серии событий.

Основная агрегация предоставляет два режима:

- **Простой режим** - настраивает величину порога соответствий для подписи, которая должна быть встречена, прежде чем предупреждение передается.
- **Усовершенствованный режим** - настраивает величину порога соответствий в секунду (количество временного интервала) для подписи, которая должна быть встречена, прежде чем предупреждение передается.

Опции суммирования

- **огонь - все** - Запускают предупреждение каждый раз, когда подпись инициирована. Если порог установлен для суммирования, предупреждения запущены за каждое выполнение, пока не происходит суммирование. После того, как суммирование запускается, только одно предупреждение для каждого итогового интервала огни для каждого набора адреса. Предупреждения для других наборов адреса или все замечены или отдельно суммированы. Подпись возвращается для **увольнения - весь** режим после периода никаких предупреждений для той подписи.
- **сводка** - Запускает предупреждение первоначально, подпись инициирована. Дополнительные предупреждения для той подписи суммированы на время итогового интервала. Только один предупреждает, что каждый итоговый интервал должен сработать для каждого набора адреса. Если глобальный итоговый порог достигнут,

подпись входит в режим **глобального суммирования**.
- **глобальное суммирование** - Запускает предупреждение за каждый итоговый интервал. Подписи могут быть предварительно сконфигурированы для **глобального суммирования**.
- **огонь однажды** - Запускает предупреждение за каждый набор адреса. Этот режим может быть обновлен к режиму **глобального суммирования**.

Суммирование события

Общий сценарий должен подвергнуться периоду базовой настройки для определения hyper предупреждение подписей. Часто существует много низких уровней и подписей информационного уровня, которым нужно суммирование на основе соединения трафика. Рассмотрите эти подписи для определения надлежащих порогов.

> **Примечание:** Будьте осторожны каждый раз, когда вы уменьшаете сумму предупреждений, особенно предупреждений от подписей высокого уровня важности. Гарантируйте, что безопасность не поставилась под угрозу и что надлежащие действия существуют для любой подписи, которая суммирована.

!--- конфигурацию

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Лобовая атака перебором паролей SSH - подпись 3653

Быстрые сеансы Secure Shell (SSH), при активном предупреждении, могут быстро заполнить хранилище события. В настоящее время попытки грубой силы SSH запрещаются.

Если вам только нужны предупреждения каждые пять минут, используйте **итоговую** опцию для alert-frequency с итоговым интервалом 300 секунд:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 3653 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode summarize
sensor(config-sig-sig-ale-sum)# summary-interval 300
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-sum)# show settings
alert-frequency
-----------------------------------------------
summary-mode
-----------------------------------------------
summarize
-----------------------------------------------
summary-interval: 300 default: 15
summary-key: Axxx <defaulted>
specify-global-summary-threshold
-----------------------------------------------
```

```
yes
-----------------------------------------------
global-summary-threshold: 240 <defaulted>
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Чрезмерный SQL-запрос в запросах HTTP - подпись 5474

Выбор - От SQL-запроса, встроенного в запрос HTTP, является одним из наиболее распространенных hyper предупреждение подписей в граничных развертываниях.

Для просмотра подписи 5474 каждый час для пары атакующего/жертвы, используйте **огонь однажды** опция для alert-frequency с итоговым интервалом 3600 секунд:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 5474 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 3600
sensor(config-sig-sig-ale-fir-yes)# summary-interval 3600
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# show settings
fire-once
-----------------------------------------------
summary-key: Axxx default: Axxx
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 3600 default: 240
summary-interval: 3600 default: 15
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

AD Внутренний или Внешний Сканер TCP/UDP - Подписи 13000 - 13008

В данном примере срабатывает подпись, когда это обнаруживает Протокол управления передачей (TCP) / сканер Протокола UDP, который просматривает набор IP - адресов назначения, настроенных как зона, Внутренняя или Внешняя. Если IPS Manager Express (IME) передает по умолчанию, события высокого уровня важности как почтовые уведомления, могли бы быть тысячи электронных почт.

> **Примечание:** Удостоверьтесь, что огни не являются атакой ошибочного допуска. Измените настройки для Обнаружения отклонения, чтобы "изучить режим" в течение

48 часов, затем положить обратно его для "обнаружения режима" для решения вопроса.

Для сокращения количества электронных почт используйте **огонь однажды** опция для alert-frequency с итоговым интервалом 720 секунд или один раз в 12 минут.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 13000 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 720
sensor(config-sig-sig-ale-fir-yes)# summary-interval 720
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir-yes)# show settings
  fire-once
  ----------------------------------------------
     summary-key: Axxx <defaulted>
     specify-global-summary-threshold
     ----------------------------------------------
        yes
        ------------------------------------------------
           global-summary-threshold: 720 default: 240
           summary-interval: 720 default: 15
        ------------------------------------------------
     ----------------------------------------------
  ----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Дополнительные сведения

- Частота предупреждения Настройки
- Руководства по конфигурации IPS
- Cisco Systems – техническая поддержка и документация