Содержание

Введение

Этот документ объясняет, что Суммирование События Системы предотвращения вторжений (IPS) и что причины для IP-адресов, которые обнаруживаются как 0.0.0.0:0 в событиях подписи IPS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Подпись Cisco IPS предупреждает конфигурацию
- Конфигурация объединения события IPS

> **Примечание:** Посмотрите Примеры Конфигурации объединения IPS для примеров конфигурации объединения события.

Используемые компоненты

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

- Устройство адаптивной защиты (ASA) 5500 или 5500x Модули ips
- IPS 4200, 4300, или устройства IPS серии 4500
- Расширенный сетевой модуль (NME) - Модуль ips
- Программное обеспечение IPS 7.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.

Общие сведения

Суммирование события IPS является методом, используемым для агрегации нескольк событий в одиночное предупреждение. Это приводит к сокращению громкости предупреждений, обработанных и передаваемых датчиком.

Проблема

События, генерируемые на IPS, показывают IP-адрес атакующего/жертвы как 0.0.0.0:0.

Решение

Когда IPS генерирует предупреждения подписи, он предоставляет сведения, такие как Идентификатор подписи, Метка времени, IP-адрес атакующего/жертвы, и так далее. При определенных условиях генерируемые события показывают IP-адрес атакующего/жертвы, отображенного как 0.0.0.0:0. Причина позади IP-адресов отобразилась, поскольку 0.0.0.0:0 суммирование. Для настройки, суммирование, или добавляют новую пользовательскую подпись или редактируют текущую подпись, и выберите **Alert Frequency> Summary Mode**.

Доступные опции суммирования:

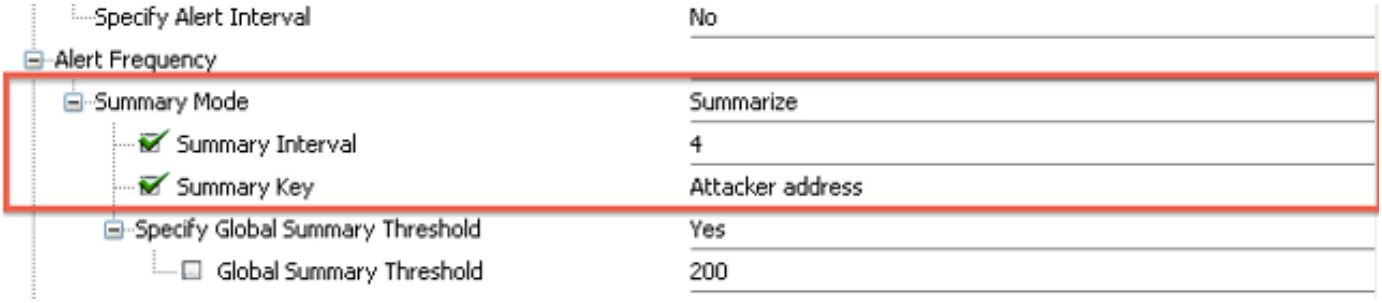
- Огонь - все - запускают предупреждение каждый раз, когда подпись инициирована.
- Огонь однажды - запускает предупреждение за набор адреса.
- Суммируйте - запускает предупреждение первоначально, подпись инициирована. Дополнительные предупреждения для той подписи суммированы на время итогового интервала.
- Глобальное суммирование - запускает предупреждение за каждый итоговый интервал.

Каково различие между Итоговым Ключевым и Глобальным Итоговым Порогом?

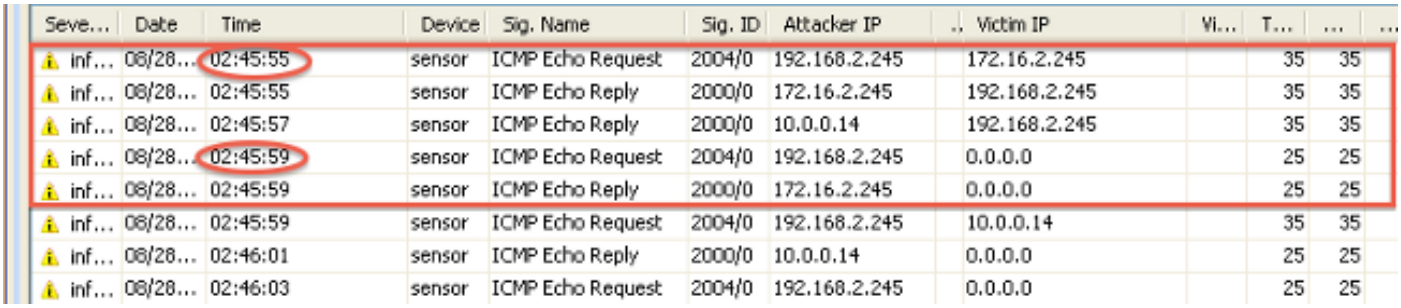
Итоговый Ключ является ключом, используемым IPS, чтобы завершить, как создать итоговое событие. По умолчанию это - адрес атакующего, что означает, что, если у вас есть один атакующий, который инициирует любую подпись, одно обычное событие и одну сводку, генерируется. Если у вас есть два атакующих, два обычных и два итоговых события генерируются для настроенного итогового интервала. Если вы установите итоговый ключ к адресу жертвы, и у вас есть два атакующих, которые предназначаются для одной жертвы, то два атакующих сделают запись только одного постоянного клиента и одного итогового события.

Итоговый Режим имеет две опции; Итоговый Интервал и Итоговый Ключ. Итоговый Интервал представлен в секундах, и он срабатывает для каждого итогового интервала. Итоговый Ключ является критерием, по которому IPS выбирает, как создать событие Summary. По умолчанию это - адрес Атакующего. Доступные опции Summary Key включают:

- Адрес атакующего (по умолчанию)
- Адрес атакующего и порт жертвы
- Атакующий и адреса жертвы
- Атакующий и адреса жертвы и порты
- Адрес жертвы



Предыдущий пример показывает подпись, суммированную с Итоговым Интервалом 4 и Итоговым Ключом как адрес атакующего. В этом сценарии подпись запускает стандартное событие первоначально, после которой точки подпись суммирована для интервала 4 секунд.



Seve...	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Vi...	T...	...	...
inf...	08/28...	02:45:55	sensor	ICMP Echo Request	2004/0	192.168.2.245	172.16.2.245		35	35	
inf...	08/28...	02:45:55	sensor	ICMP Echo Reply	2000/0	172.16.2.245	192.168.2.245		35	35	
inf...	08/28...	02:45:57	sensor	ICMP Echo Reply	2000/0	10.0.0.14	192.168.2.245		35	35	
inf...	08/28...	02:45:59	sensor	ICMP Echo Request	2004/0	192.168.2.245	0.0.0.0		25	25	
inf...	08/28...	02:45:59	sensor	ICMP Echo Reply	2000/0	172.16.2.245	0.0.0.0		25	25	
inf...	08/28...	02:45:59	sensor	ICMP Echo Request	2004/0	192.168.2.245	10.0.0.14		35	35	
inf...	08/28...	02:46:01	sensor	ICMP Echo Reply	2000/0	10.0.0.14	0.0.0.0		25	25	
inf...	08/28...	02:46:03	sensor	ICMP Echo Request	2004/0	192.168.2.245	0.0.0.0		25	25	

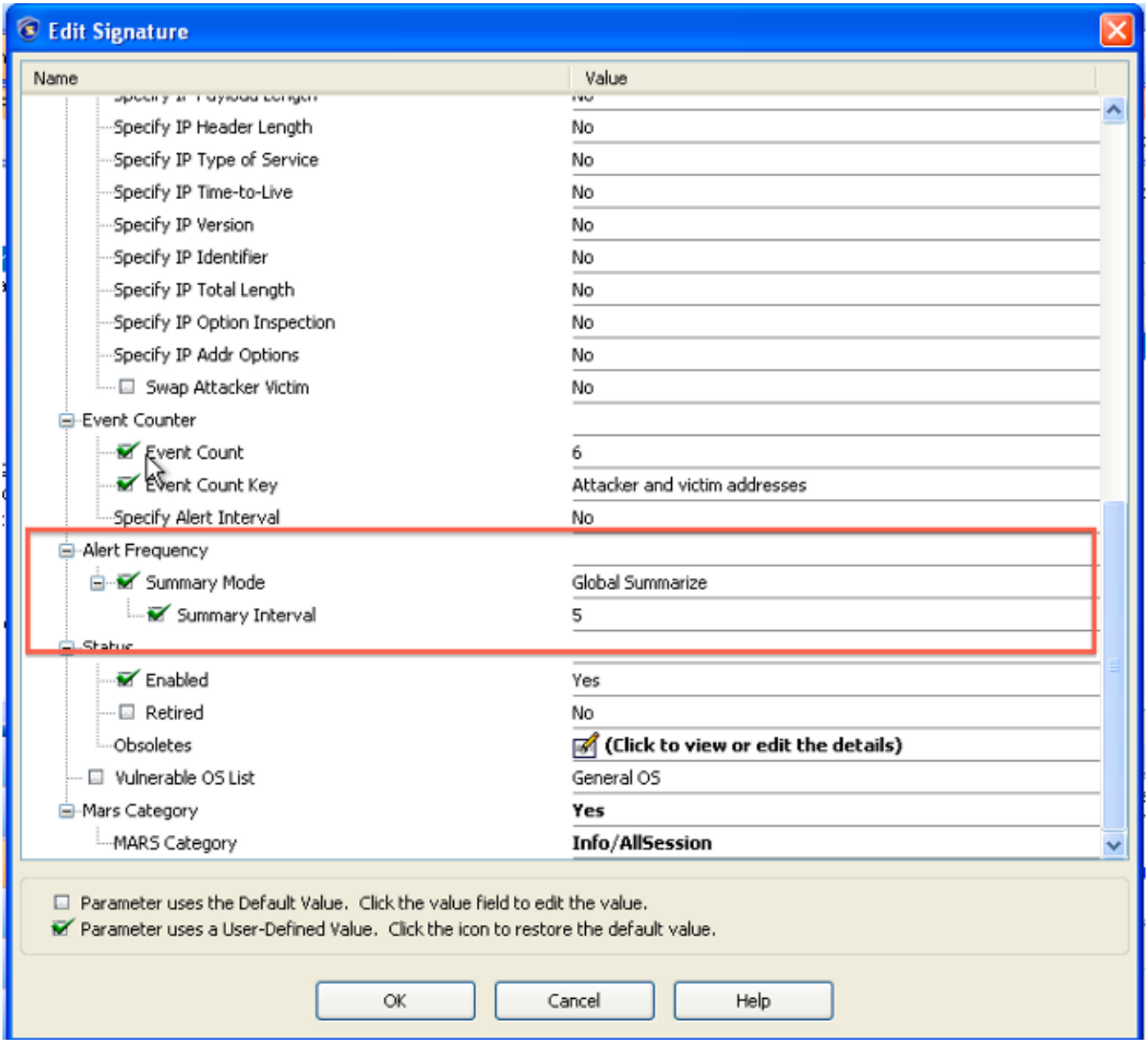
Глобальный Итоговый Порог - если глобальная сводка не задана и если существует два замеченные IP-адреса атакующего, IPS, делает запись двух стандартных событий. После периода Итогового Интервала два дополнительных итоговых события генерируются, один для каждого IP-адреса атакующего. Всего, у вас было бы 4 события зарегистрированными в заданном интервале.

С Глобальным Суммированием, включенным с Глобальным Итоговым Порогом SAID, два, и если вы повторяете предыдущий пример, тогда, IPS делает запись событий THREE: два для начальных соответствий для каждого адреса атакующего и одного итогового события для всех атакующих (два в этом случае) в заданном интервале. Теперь при увеличении масштаба количества атакующих и соответствий вы видели бы, что Глобальное Суммирование копит много событий/журналов и таким образом циклы процессора.

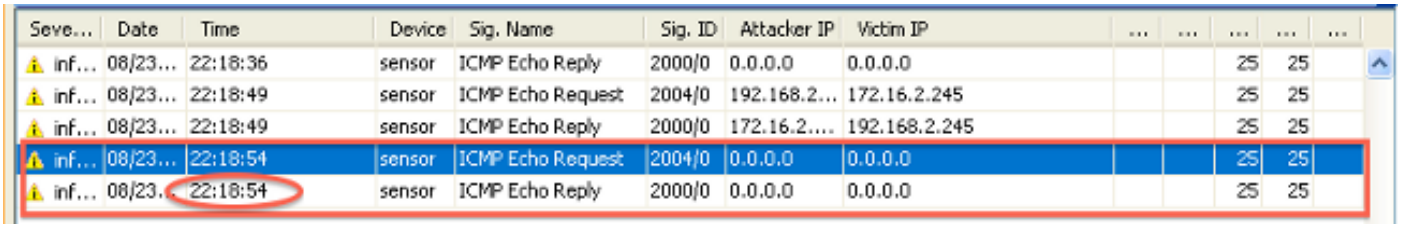
Глобальное Суммирование имеет только один подпараметр, который является "итоговым интервалом", который настроен в секундах. Когда подпись установлена в глобальный-summarizarion, она срабатывает для каждого итогового интервала. Т.е. если итоговый интервал установлен в '5', он запускает предупреждение первоначально, подпись инициирована, и после того он срабатывает для каждого итогового интервала 5 секунд.

Для редактирования подписи выберите **Configuration> Policies> Active signature** и затем ищите соответствующую подпись.

Например, ID SIG для 'запроса ICMP' является 2004. Щелкните правой кнопкой мыши подпись и выберите **Edit** для получения до диалогового окна, показанного здесь:



Во фрагменте предыдущей конфигурации итоговый режим был установлен в 'глобальный, суммируют' с итоговым интервалом 5 секунд.



Выборка предупреждений показывает подписям 'Эхо-запрос протокола ICMP' и 'Эхо - ответ ICMP', которые были суммированы и следовательно отображают IP-адреса атакующего/жертвы как '0.0.0.0'.

Не путайте глобальные события суммирования с 'событиями подписи 1102.0 (Невозможный Пакет IP)'. Хакеры могли бы попытаться уклониться от IPS с использованием всех нулей для IP - адресов источника и IP - адресов назначения и порта, который мог инициировать эту подпись, которая могла бы быть похожей на итоговое событие.

Дополнительные сведения

- Часто задаваемые вопросы подписей системы предотвращения вторжений Cisco (IPS)
- Руководство конфигурации интерфейса командой строки датчика системы предотвращения вторжений Cisco (IPS) для IPS 7.1
- Примеры конфигурации объединения IPS
- Cisco Systems – техническая поддержка и документация