Содержание

Введение

Система FireSIGHT генерирует события, когда она обнаруживает новый хост на вашем отслеживаемом сегменте сети. Это может обнаружить операционную систему или сервис неправильно, или с меньшей уверенностью. Если событие отмечено как *Неизвестное*, это означает, что трафик проанализирован, но операционные системы не совпадают ни с одним из известных отпечатков пальца. Этот документ предоставляет чек-листа и рекомендации минимизировать *Неизвестные события*.

Предварительные условия

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Система FireSIGHT, устройства FirePOWER и виртуальные устройства NGIPS
- Версия программного обеспечения 5.2 или 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.

Устранение неполадок контрольных списков

Если ваша Система FireSIGHT генерирует события, которые находятся в ожидании или в неизвестном состоянии, можно выполнить действия ниже, чтобы начать решать эту проблему:

> **Примечание:** *Неопознанные* хосты не являются тем же как *Неизвестными хостами*. *Неопознанные* хосты являются хостами, о которых система еще не собрала

достаточно информации для определения их операционных систем.

Чек-лист устранения неполадок	Рекомендации
1. Какая версия VDB установлена на Центре управления FireSIGHT?	Последняя версия VDB имеет большую информацию об отпечатке пальца. Всегда рекомендуется установить послед версию на Центре управления FireSIGHT.
2. Каков предел хоста вашей лицензии FireSIGHT? Сколько хостов было обнаружено FireSIGHT?	Если предел хоста превышает, Система FireSIGHT сокраща самые старые данные, поскольку входят новые данные. Ког предел хоста достиг, можно настроить Системную политику отбрасывания новых хостов.
3. Сколько переходов далеко хосты расположены от управляемого устройства FireSIGHT?	Выше счетчик переходов между хостами и управляемым устройством, еще дальше хост от устройства, и таким образ увеличенная вероятность трафик модифицировался и не позволит точную идентификацию.
4. Есть ли какие-либо встроенные устройства между хостами и управляемое устройство?	Присутствие любого встроенного устройства; такой как межсетевой экран, устройство NAT, балансировщик загрузк прокси-сервер могут модифицировать исходный TCP или информацию о IP - заголовке, которая может также быть причинами не распознанного или неопознанного сбора свед от хостов.
5. Управляемые устройства контролируют трафик в какой-либо асинхронной сети маршрутизации?	Если FireSIGHT Системные мониторы асинхронный трафик маршрутизации, это может не быть в состоянии видеть завершенный сеанс.
6. Там какие-либо нестандартные порты используются для каких-либо сервисов? Там какие-либо пользовательские декодеры настроены для адресации к нестандартным портам?	Неправильно настроенный пользовательский декодер може конфликтовать с декодерами по умолчанию.

Дополнительные данные

Если все вышеупомянутые рекомендации будут придерживаться, но все еще существуют неизвестные, или неопознанные найденные хосты в состоянии ожидания, то мы должны будем проанализировать следующий data:

1. Полный трафик сеанса

Полный трафик сеанса от хостов, которые определены неправильно или отмечены как неизвестные или в состоянии ожидания.

2. Устранение проблем файлов

Устранение проблем файлов от Центра управления FireSIGHT и управляемого устройства.

Карта сети или топология, показывая местоположение управляемого устройства были бы полезны.

3. Захват пакета (PCAP)

Пакеты, полученные управляемым устройством, могут быть другими, чем пакеты, инициируемые на хостах. Если какой-либо заголовок, модифицирующий встроенное устройство, существует между хостами и управляемым устройством, это происходит. Поэтому лучше перехватить PCAP от обоих концов - хосты и управляемые устройства, который позволяет сравнивать заголовки от двух PCAPs. Любое несоответствие между пакетами может вызвать ошибочное дешифрирование сервисов или хостов.