Обработка единого потока большой сеанс (поток слона) сервисами огневой мощи

Содержание

Введение

Результат любого веб-сайта тестирования скорости пропускной способности или выходные данные любого измерительного программного средства пропускной способности (например, *iperf*) может не показать объявленную оценку пропускной способности устройств Огневой мощи Cisco. Точно так же передача очень большого файла по любому транспортному протоколу не демонстрирует объявленную оценку пропускной способности устройства Огневой мощи. Это происходит, потому что сервис Огневой мощи не использует поток одиночной сети для определения его максимальной пропускной способности. Этот документ описывает, почему единый поток не может использовать всю номинальную пропускную способность устройства Огневой мощи Cisco.

Внесенный Nazmul Rajib, и Фостером Липки, специалистами службы технической поддержки Cisco.

Обработка трафика фырканьем

Базовая технология обнаружения сервиса Огневой мощи является Фырканьем. Реализация Фырканья на устройстве Огневой мощи Cisco является одиночным процессом потока для обработки трафика. Устройство оценено для определенной оценки на основе общей производительности всех потоков, проходящих устройство. Ожидается, что устройства развернуты на Корпоративной сети, обычно около края границы, и работает с тысячами соединений.

Распределение нагрузки использования Firepower Services трафика ко многому другому Фырканью обрабатывает с одним процессом Фырканья, работающим на каждом ЦП на устройстве. Идеально, нагрузка на систему балансирует трафик равномерно через все

процессы Фырканья. Фырканье должно быть в состоянии предоставить надлежащий контекстный анализ для NGFW, IPS и контроля AMP. Гарантировать Фырканье является самым эффективным, весь трафик от единого потока с балансировкой нагрузки к одному экземпляру фырканья. Если бы весь трафик от единого потока не был сбалансирован к одиночному экземпляру фырканья, то от системы можно было уклониться путем разделения трафика таким способом, которым правило Фырканья может быть менее вероятно совпасть, или части файла не непрерывны для контроля AMP. Поэтому алгоритм балансировки нагрузки основывается на информации о соединении, которая может однозначно определить данное соединение.

Алгоритм с 2 кортежами в ASA с FirePOWER Services и NGIPS действительный

На ASA со Служебной платформой FirePOWER и NGIPS действительный, трафик является загрузкой balaned для Фырканья использования алгоритма с 2 кортежами. Точки данных для этого алгоритма:

- IP-адрес отправителя
- IP-адрес назначения

Алгоритм С 3 кортежами в Версии программного обеспечения 5.3 или Ниже на Огневой мощи и устройствах FTD

На всех предыдущих версиях (5.3 или ниже), трафик является загрузкой balaned для Фырканья использования алгоритма с 3 кортежами. Точки данных для этого алгоритма:

- IP-адрес отправителя
- IP-адрес назначения
- IP Protocol

Любой трафик с тем же источником, назначением и Протоколом "IP" с балансировкой нагрузки к одинаковому экземпляру Фырканья.

Алгоритм С 5 кортежами в Версии программного обеспечения 5.4, 6.0, и Больше на Огневой мощи и устройствах FTD

На Версии 5.4, 6.0 или больше, трафик является загрузкой balaned для Фырканья использования алгоритма с 5 кортежами. Точки данных, которые приняты во внимание, показывают ниже:

- IP-адрес отправителя
- Исходный порт
- IP-адрес назначения
- Номер порта
- IP Protocol

Цель добавить порты к алгоритму состоит в том, чтобы сбалансировать трафик более равномерно, когда существует определенный источник и целевые пары, которые составляют значительные части трафика. Путем добавления портов старшие эфемерные исходные порты должны быть другими на поток и должны добавить дополнительную энтропию, более равномерно балансирующую трафик к другим экземплярам фырканья.

Общая производительность

Общая производительность устройства измерена на основе суммарной пропускной способности всех экземпляров фырканья, работающих к их самому полному потенциалу. Методы промышленного стандарта для измерения пропускной способности для множественных соединений HTTP с помощью различных размеров объекта. Например, NSS NGFW методология тестирования измеряет общую производительность устройства с помощью 44k, 21k, 10k, 4.4k, и 1.7k объекты. Они преобразовывают в диапазон средних размеров пакета от всех 1k байтов до 128 байтов из-за других пакетов, вовлеченных в соединение HTTP.

Можно оценить оценку производительности отдельного экземпляра Фырканья путем взятия номинальной пропускной способности устройства и деления этого на количество экземпляров Фырканья, которые работают. Например, если устройство оценено в 10 Гбит/с для IPS со средним размером пакета 1k байтов, и то устройство имеет 20 экземпляров Фырканья, приблизительная максимальная пропускная способность для единственного экземпляра составила бы 500 Мбит/с за фырканье. Различные типы трафика, сетевых протоколов, размеры пакетов наряду с различиями в политике общей безопасности могут все повлиять на наблюдаемую пропускную способность устройства.

Результат тестирования программного средства третьей стороны

Когда вы тестируете с любым веб-сайтом тестирования скорости или любым измерительным программным средством пропускной способности, такой как, *iperf*, один большой поток TCP единого потока генерируется. Этот тип большого потока TCP называют **Потоком Слона**. Поток Слона является одиночным сеансом, относительно длительное сетевое подключение, которое использует большую или диспропорциональную сумму пропускной способности. Этот тип потока назначен на один экземпляр Фырканья, поэтому результат тестирования отображает пропускную способность одиночного экземпляра фырканья, не оценку суммарной пропускной способности устройства.

Исправления

Интеллектуальный обход приложения (IAB)

Версия программного обеспечения 6.0 представляет новую характеристику, названную **Интеллектуальным обходом приложения (IAB)**. Когда устройство Огневой мощи достигает предустановленного порогового значения производительности, функция IAB ищет потоки, которые соответствуют определенным критериям для интеллектуального обхода, который облегчает давление на механизмы обнаружения.

> **Совет:** Дополнительные сведения о настройке IAB могут быть найдены здесь.

Определите и доверяйте большим потокам

Большие потоки часто относятся к высокому использованию низкий инспекционный трафик значения , например, резервные копии, репликация базы данных, и т.д. Многим из этих приложений нельзя принести пользу из контроля. Для предотвращения проблем с

большими потоками можно определить большие потоки и создать правила доверия Управления доступом для них. Эти правила в состоянии однозначно определить большие потоки, позволить тем потокам проходить неосмотренный а не ограничиваться одиночным поведением экземпляра фырканья.

> **Примечание:** Для определения больших потоков для трастовых правил свяжитесь с TAC Огневой мощи Cisco.

Дополнительная документация

- Управление доступом Использование интеллектуального обхода приложения