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 FTP или HTTP - 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 использует 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.

Мера Firepower Services максимальная пропускная способность устройства путем распределения нагрузки трафика ко многим другим рабочим процессам для фырканья - один процесс фырканья для каждого ЦП на устройстве. Однако сервисы Огневой мощи балансируют нагрузку трафика равномерно на на пакет за пакетом через все экземпляры Фырканья. Фырканье должно быть в состоянии повторно собрать соединения. Если Фырканье doesnot повторно собирает эти сеансы, от системы предотвращения вторжений можно было бы уклониться путем фрагментации пакетов таким способом, которым правило Фырканья может быть менее вероятно совпасть. Для каждого отдельного экземпляра Фырканья, чтобы быть в состоянии повторно собрать трафик, сервис Огневой мощи должен передать весь трафик от любых соединений до того же экземпляра Фырканья. Поэтому алгоритм балансировки нагрузки основывается на информации о соединении, которая может однозначно определить данное соединение.

Алгоритм с 3 кортежами в версии программного обеспечения 5.3 или ниже

На всех предыдущих версиях (5.3 или ниже), Фырканье использует алгоритм 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 Версии 5.4, 6.0 или больше, Firepower Services использует алгоритм 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 основывается на объединенной способности всех экземпляров фырканья, работающих к их самому полному потенциалу. Можно оценить оценку производительности отдельного экземпляра Фырканья путем взятия оценки устройства и деления, что количеством экземпляров Фырканья, которые работают.

Например, 8250 устройств оценены в 10 Гбит/с для IPS и имеют 22 экземпляра выполнения Фырканья. Поэтому одиночное пороговое значение производительности Фырканья было бы экземпляром на 10,000 Мбит/с / 22 = экземпляр 454 Мбит/с за фырканье. Теперь некоторые устройства могут немного недооцененный, поэтому одиночный экземпляр Фырканья может обработать немного больше, чем этот алгоритм дал бы вам. 8250 устройств являются одним из них, обычно это достигает пика в экземпляре 500 Мбит/с за фырканье.

Другим примером был бы ASA 5516 с сервисами Огневой мощи. ASA 5516 оценен в максимальной пропускной способности 450 Мбит/с с 1500 пакетами в 1 байт для Видимости Приложения и Контроля (AVC) и IPS. ASA 5516 имеет 3 экземпляра выполнения фырканья. Максимум на пропускную способность экземпляра составил бы приблизительно 150 Мбит/с.

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 обычно относятся к большим передачам файла, например, резервным копиям, репликации базы данных, и т.д. Многим из этих передач файла нельзя принести пользу из контроля. Для предотвращения проблем с большими передачами файла можно определить большие потоки и создать правила доверия Управления доступом для них. Эти правила в состоянии однозначно определить большие потоки, позволить Фырканью передавать те потоки, неосмотренные 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