Визитка

ВЛАДИМИР ВОРОТНИКОВ,
руководитель отдела интеграционных решений ООО «С-Терра СиЭсПи»

Производительность IPsec:
как избежать узкого места в своей сети

Шифрование передаваемых данных превратилось из экзотичной функции для «гиков» в обязательную опцию для любого пользователя

Криптозащита может быть встроена на самых разных уровнях, но здесь речь пойдет об универсальном варианте, когда шифрование работает на сетевом уровне и защищает весь трафик, независимо от применяемых пользователем приложений и, как следствие, протоколов прикладного и транспортного уровня.

С помощью набора сетевых протоколов IPsec возможно защитить как отдельное клиентское устройство, установив на него IPsec-клиент (например, С-Терра Клиент), так и весь сетевой трафик, выходящий из локальной сети, установив на выходе межсетевой экран (МЭ) или шлюз безопасности с поддержкой IPsec (например, С-Терра Шлюз).

Шифрование является ресурсоемкой операцией с точки зрения вычислений, поэтому системным администраторам и сетевым инженерам приходится заботиться не только о корректном функционировании защищенных каналов связи, но и о производительности используемого оборудования. О том, от чего зависит производительность IPsec, как подобрать оптимальную аппаратную платформу и как не превратить шифрующее устройство в узкое место сети, и пойдет речь в данной статье.

От чего зависит производительность

В общем случае производительность шлюза безопасности IPsec зависит от:

- профиля передаваемого трафика (распределение длин передаваемых пакетов, используемые протоколы, количество потоков);
- параметров аппаратной платформы, на которой работает шифрующее ПО (в первую очередь процессор и сетевая карта, затем в меньшей степени ОЗУ и внутренние шины данных).

В какой мере на производительность IPsec влияют факторы первой группы, можно почитать в [1-3]. Мы подробнее рассмотрим зависимость производительности IPsec от характеристик аппаратной платформы.

Влияние аппаратной платформы

В качестве аппаратных платформ для исследуемых продуктов были использованы серверные платформы с двумя процессорами Intel E5-2643v2, применяемые для производства шлюзов безопасности С-Терра. Шифрование данных производится по алгоритму ГОСТ 28147-89. Для шифрования трафика используется ПО «С-Терра Шлюз 4.1». Данное ПО создано российским производителем средств сетевой защиты информации, компанией ООО «С-Терра СиЭсПи».

Нижеприведенные результаты получены на модели трафика IMIX (известна также под названиями «Internet Mix» и «Смешанный трафик») [4].

Ядра двух процессоров

Результаты измерений производительности шифрования С-Терра Шлюз при последовательном использовании от 1 до 12 процессорных ядер, находящихся на двух процессорах при различных размерах пакетов (Hyper Threading выключен), показаны на рис. 1.

На графиках можно отметить несколько важных особенностей. Во-первых, линейный рост при переходе на ядра второго процессора продолжается, однако линия в точке перехода к шести ядрам претерпевает излом. Во-вторых, общая производительность для средних и маленьких пакетов сильно замедляет рост и даже переходит на спад. Причем у пакетов размером 64 байта этот процесс происходит раньше, чем, например, у пакетов размером 512 байт. Это связано с тем, что в качестве ограничения выступает ядро, балансирующее данные между процессорами, или сетевая подсистема.

Влияние Hyper Threading

Результаты измерений производительности шифрования С-Терра Шлюз на одном процессоре при включенной технологии Hyper Threading показаны на рис. 2.

На графиках (см. рис. 2) отчетливо виден излом при переходе к шестому ядру. Связан он с тем, что начинают использоваться оба виртуальных ядра (их появление как раз и вызвано включением Hyper Threading) на одном физическом ядре. В абсолютных значениях результаты, полученные при использовании Hyper Threading на одном процессоре, существенно выше результатов без Hyper Threading на одном процессоре, но ниже производительности на двух физических процессорах.

Результаты измерения производительности на двух процессорах при включенной технологии Hyper Threading показаны на рис. 3.

Как и без использования Hyper Threading, при переходе на второй физический процессор, рост производительности замедляется. При увеличении количества ядер наступает момент, когда общая производительность начинает снижаться. При этом на маленьких пакетах этот процесс начинается раньше, чем на больших. В связи с этим интересно посмотреть на производительность в пакетах в секунду (см. рис. 4).

Подведем итоги

Если узким местом является центральный процессор или внутренняя шина, то ограничение производительности возникает в значениях Мбит/с (значение пакетов/с на разных размерах пакетов при этом меняется). Характерным признаком этого является ситуация, когда результаты измерения производительности (в Мбит/с) оказываются одинаковыми для двух разных (но достаточно близких) размеров пакетов (например, 1300 и 1400 байт).

Если показатель загруженности процессора близок к 100%, то, вероятно, виноват именно процессор. Заметным признаком ограничения со стороны внутренней шины является значение производительности (в Мбит/с), равное пропускной способности шины (различная для разных шин), т.е. значению, при котором шина загружена на 100%.

Если узким местом является сетевая подсистема или модуль балансировки данных между процессорными ядрами, то, наоборот, ограничение производительности возникает в значениях пакетов/с (значения Мбит/с при этом меняются).

Анализ графиков на рис. 3, 4 позволяет разделить эти два случая. В данном случае при 20-23 используемых ядрах узким местом выступает модуль балансировки, а не сетевая подсистема, т.к. по графику на рис. 3 (11-17 ядер) видно, что сетевая подсистема способна обрабатывать большее количество пакетов в секунду.

Рекомендации

Полученные результаты полезны на этапе проектирования и внедрения системы передачи данных, элементами которой являются системы защиты. Также они важны для разработчиков средств сетевой защиты информации, каковой является и компания «С-Терра СиЭсПи», в процессе оптимизации производительности.

Оценка необходимой производительности и подбор оптимальной конфигурации оборудования для шифрования – задача многоплановая. Для получения практических навыков и опыта существуют учебные курсы, например курс «Построение защищенных виртуальных сетей на основе IPsec с использованием алгоритмов шифрования ГОСТ на базе шлюзов безопасности С-Терра СиЭсПи», проводимый в УЦ «Академия Информационных Систем». ADV

[1] Воротников В.С. Исследование параметров, влияющих на производительность в технологии IPsec. Вопросы защиты информации: Науч.-практ. журн. ФГУП «ВИМИ», 2012, вып. 4. – С. 7-8.
[2] Воротников В.С. Производительность шлюзов безопасности: «кот в мешке» или разумный расчет. ИКС, №9, 2012. – С. 57.
[3] Воротников В.С. Высокопроизводительное сертифицированное решение для защиты ЦОД. Storage News, №4, 2012. – С. 24-25.
[4] Agilent Technologies. The Journal of Internet Test Methodologies. – Сентябрь 2007 г.

Рисунок 1. Производительность на ядрах нескольких процессоров

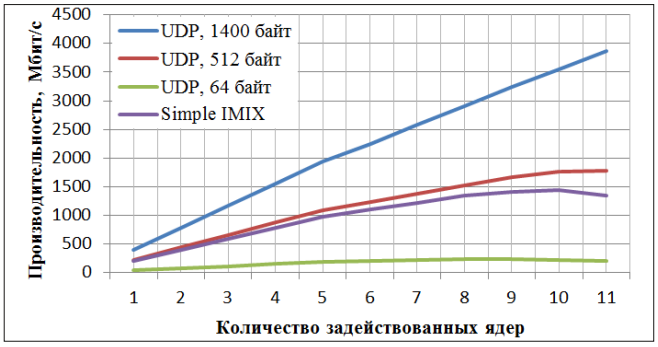

Рисунок 2. Производительность на ядрах одного процессора при использовании Hyper Threading

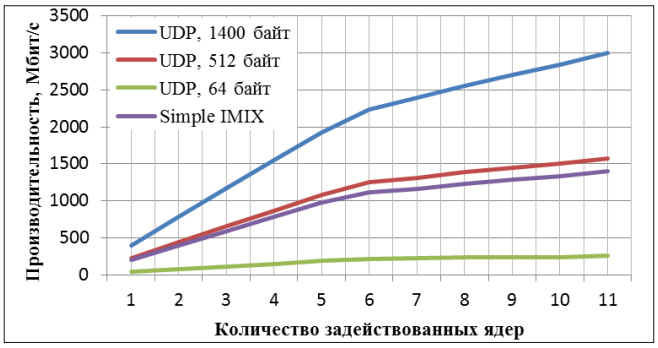

Рисунок 3. Производительность на ядрах двух процессоров при использовании Hyper Threading

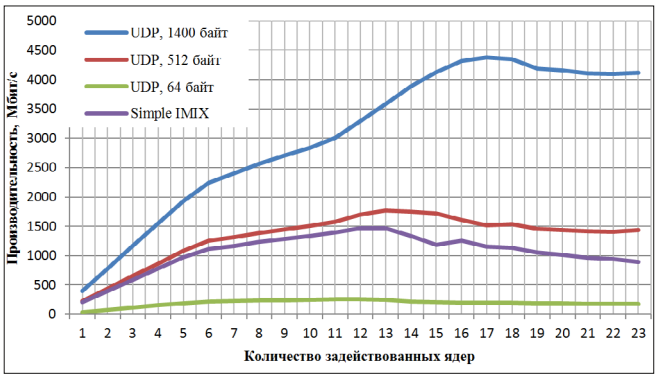

Рисунок 4. Производительность (в пакетах в секунду) на ядрах двух процессоров при использовании Hyper Threading