Производительность шлюзов безопасности: «кот в мешке» или разумный расчет

При передаче данных через недоверенные сети технология IPSec VPN обеспечивает их конфиденциальность и целостность. Однако шифрование и контроль целостности – ресурсоемкие операции, при неправильном построении системы передачи данных именно они становятся узким местом. Чтобы не создавать проблем в работе ИТ-сервисов, следует уже на этапе проектирования учитывать производительность шифрующих средств.

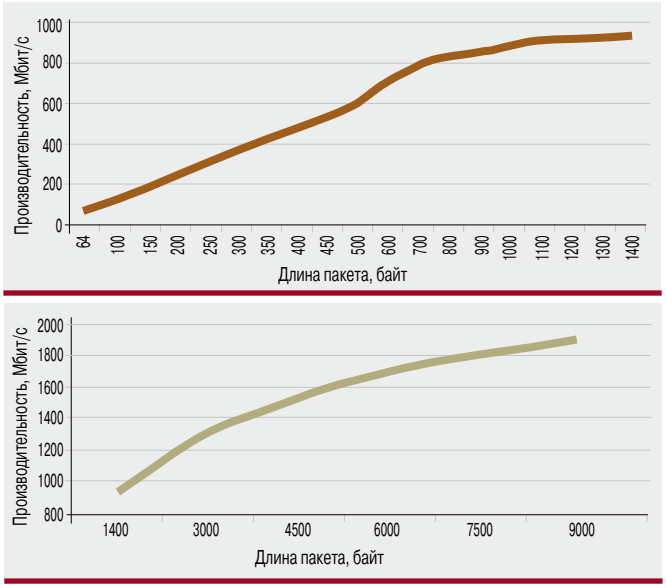
Владимир ВОРОТНИКОВ, руководитель департамента перспективных исследований и проектов, «С-Терра СиЭсПи»

Существует распространенное заблуждение, что производительность – это простое понятие, характеризуемое одним числом. На самом деле **производительность – комплексная величина, зависящая от множества факторов.** Для сетевых устройств безопасности она будет включать в себя как сетевую производительность, так и производительность шифрования. Все значения, речь о которых пойдет ниже, получены при использовании алгоритмов, описанных в ГОСТ 28147-89 и ГОСТ Р 34.11-94.

Ресурсы шлюза безопасности тратятся приблизительно в равной степени на шифрование и на дешифрование трафика. Поэтому если указана, например, производительность шифрования 500 Мбит/с, это значит, что либо шлюз шифрует поток 500 Мбит/с «в одну сторону», либо шифрует 250 Мбит/с и расшифровывает 250 Мбит/с. В любом случае перед выбором оборудования следует уточнить у вендора, какая именно производительность имеется в виду.

Еще один фактор, влияющий на производительность, – профиль трафика или, проще говоря, частота встречаемости пакетов разной длины. Это наиболее существенный параметр: **одно и то же устройство на разных профилях трафика может показывать производительность, различающуюся в десятки раз.** Например, топовые шлюзы компании «С-Терра СиЭсПи» (CSP VPN Gate 7000 HighPerformance) показывают производительность 3,5 Гбит/с на UDP-трафике с пакетами длиной 1400 байт и 150 Мбит/с на UDP-трафике с пакетами в 64 байт. Понятно, что в случае коротких пакетов узким местом становится не шифрование, а сетевая подсистема.

Производительность шлюза безопасности в зависимости от длины пакета



Измерения производительности шлюза безопасности в зависимости от длины пакета (см. рисунок) проводились на шлюзе средней производительности CSP VPN Gate 3000 от «С-Терра СиЭсПи».

Здесь важно отметить: тесты на пакетах фиксированной длины являются синтетическими. В реальной сети такой профиль трафика практически никогда не встречается. **Для того, чтобы при моделировании максимально приблизиться к условиям работы шлюзов безопасности в реальных сетях, используют смешанный трафик (IMIX).** Он неплохо соответствует среднестатистическому трафику магистральных каналов. Статистика измерений производительности шлюзов безопасности «С-Терра СиЭсПи» свидетельствует, что производительность на IMIX и на трафике UDP с пакетами длиной 450 байт примерно одинакова.

Еще один параметр, который может повлиять на производительность, – количество потоков трафика. Распространено мнение, что чем больше IPSec-туннелей, тем сложнее их обрабатывать. Это не так (по крайней мере для шлюзов безопасности «С-Терра СиЭсПи»). Плюс большого количества IPSec-туннелей в том, что обработку множества потоков легче распараллелить на многопроцессорных устройствах. Есть, конечно, верхний предел, начиная с которого производительность будет снижаться, но он обычно составляет сотни и тысячи туннелей, в зависимости от аппаратной платформы и структуры сети.

Итак, производительность – многогранное понятие, и при разных условиях у одного и того же оборудования она может отличаться на порядок. **Выбирая шлюз безопасности по производительности, старайтесь получить полную информацию:** что понимает вендор под производительностью, какова она на коротких и длинных пакетах, какова на смешанном трафике (IMIX) и что произойдет, если количество туннелей будет возрастать. Только так можно быть уверенными, что внедрение решения для защиты каналов связи пройдет прозрачно для ИТ-инфраструктуры и конечный пользователь не заметит включения шлюза безопасности в существующую сеть.

ЗАО «С-Терра СиЭсПи»
Тел./факс: (499) 940-9061,
information@s-terra.com, www.s-terra.com

Разработчик средств сетевой информационной безопасности для построения виртуальных защищенных сетей (VPN). Первый в России технологический партнер Cisco Systems.

Продукты CSP VPN сертифицированы ФСТЭК и ФСБ России. В решениях используются протокол IPSec и российские криптографические алгоритмы, сертифицированные по ГОСТ. Наряду с широкой масштабируемостью решения обладают высокой надежностью и рекордной производительностью, что обеспечивает им экономическую эффективность.