ОСНОВЫ ВЫБОРА NGFW

Сравнительные характеристики и примеры тестов NSS Labs

Многие компании после покупки осознали, что в их сети скорость NGFW отличается от тех скоростей, которые указаны в рекламных брошюрах. Почему так происходит и как узнать настоящую скорость заранее? Какими критериями лучше руководствоваться при выборе NGFW?

Содержание

Основы выбора NGFW

Сейчас рекомендуется использовать многофункциональные устройства, внутри которых реализованы все необходимые сетевые и безопасные функции. Такие устройства называются UTM или NGFW. Многие, занимавшиеся подбором конкретной модели (есть даже английский термин для этого — *sizing*), часто уже после покупки осознавали, что в их сети скорость NGFW отличается от тех скоростей, которые указаны в официальных datasheet. Почему так происходит и как узнать настоящую скорость заранее?

Есть 4 способа подбора:

1. **Правильный:** самим провести тестирование NGFW на своем трафике.
2. **Легкий:** заказать тест скорости под свои параметры производителю NGFW или партнеру.
3. **Неверный:** выбрать по официальному datasheet.
4. **Быстрый:** найти результаты тестов, проведенных независимой лабораторией.

Основной список функций в современном NGFW выглядит так:

1. Маршрутизация статическая.
2. Маршрутизация динамическая (OSPF, BGP).
3. Категоризация URL и фильтрация HTTP-запросов.
4. Распознавание приложений.
5. Распознавание туннелей.
6. Распознавание пользователей.
7. Распознавание стран.
8. Распознавание типов файлов.
9. Правила безопасности по портам, приложениям, пользователям, странам, URL-категориям, расширениям файлов.
10. SSL/TLS Decryption.
11. SSH Decryption.

12. Система обнаружения вторжений (СОВ или IDS/IPS).
13. Защита от вредоносного программного обеспечения (ВПО).
14. Защита от spyware.
15. Обмен файлами и сигнатурами с внешней «песочницей».
16. Контроль соединений с бот-сетями.
17. Защита от атак по DNS.
18. Проверка индикаторов Threat Intelligence в URL, DNS, IP.
19. Функция VPN-шлюза.
20. Журналирование всех событий.
21. Встроенная единая система управления всеми этими функциями.

Современный NGFW напичкан функциями, как космический корабль. Каждая функция — это серьезная нагрузка на процессор и на оперативную память. Представьте, раньше эти функции выполняли разные устройства! Все функции влияют друг на друга, поэтому производители балансируют свою операционную систему для равномерного распределения выполняемых задач между имеющимися внутренними ресурсами. Параметры производительности при всех включенных функциях одновременно зависят от мастерства программистов и внутренней аппаратной архитектуры устройства. В целях оптимизации какие-то функции могут даже не работать, например есть устройства, в которых нет локального журналирования или встроенной системы управления.

Очень много функций у производителей реализовано в облегченном режиме: вроде бы функция есть, но она проверяет не весь трафик, а только начало; не все файлы, а только с расширением .exe; не все приложения, а только на определенных портах. У Cisco нужно смотреть на настройку intelligent application bypass, у Check Point — что такое deep scan и hold mode. У Fortinet нам нужно разбираться с отличиями в режимах инспекции: flow-mode, proxy-mode, NGFW-mode, policy-mode, profile-mode, intelligent-mode, session-limit-mode, conserve-mode, fail-open и др. У Palo Alto Networks нужно

разбираться, что такое DSRI. Весь этот «тюнинг» влияет на результаты. На результаты теста также влияет версия операционной системы, сигнатур антивируса, IPS и «песочницы». Нужен многолетний опыт хорошего инженера, чтобы во все это вникнуть, поэтому в этих тонкостях лучше всего разбираются интеграторы. И это причина, по которой лучше всего тестировать оборудование перед покупкой.

Важна не только программная, но и аппаратная часть. Специализированные графические ускорители давно есть в каждом компьютере. И в NGFW тоже используются специализированные ускорители. Они нужны для ускорения функций управления, маршрутизации, IDS/IPS, антивируса, разбора данных приложений, работы IPSEC, SSL Decryption и др. Специализированные чипы ускорения могут быть перепрограммируемыми (известны как FPGA или ПЛИС) или содержать заранее запрограммированные функции (известны как ASIC). Поскольку технологии постоянно развиваются, использовать FPGA выгоднее, поскольку вы всегда можете прошить новую микропрограмму под новую функцию. Программный код в ASIC прошивается один раз на заводе. Если используются сервера на базе процессоров Intel, в них есть только команды для ускорения работы протокола шифрования AES. Просите каждого производителя рассказать о внутренней аппаратной архитектуре решения — это важно.

Ниже приведены выдержки из результатов группового теста NGFW компанией NSS Labs, выполненного в 2018 году. Почему в 2018-м, а не в 2019-м? Потому что этот тест публично доступен по ссылке (https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2018-ngfw-comparative-report-performance.pdf) и в нем есть оценки всех международных производителей, присутствующих на рынке NGFW в России: Cisco, Check Point, Fortinet, Palo Alto Networks.

В тесте NSS Labs NGFW 2018 г. принимали участие следующие модели:

- Check Point 15600 Next Generation Threat Prevention (NGTP) Appliance vR80.20;
- Cisco Firepower 4120 Security Appliance v6.2.2;
- Fortinet FortiGate 500E V5.6.3GA build 7858;
- Palo Alto Networks PA-5220 PAN-OS 8.1.1.

Все эти компании входят в Cyber Threat Alliance, т.е. они обмениваются данными об угрозах.

Какие параметры NGFW мы должны оценивать и запрашивать у производителя:

1. **CPS (Connections Per Second)** — максимальное количество *новых* соединений, которые NGFW может принять на анализ каждую секунду. Слово *«новых»* очень важно в данном контексте. Старые обрабатываются и учитываются в следующем параметре. Важны именно *новые* соединения, возникшие в сети. Под них в NGFW выделяется *новая* память, запускаются *новые* процессы анализа. В первую очередь в этот порог упирается скорость NGFW. И именно его чаще всего упускают при выборе.

2. **CC (Concurrent Connections)** — максимальное количество одновременных соединений в секунду с включенным анализом приложений и другими функциями. Нельзя сразу подать 10 миллионов новых соединений на устройство — это лишь спровоцирует DDoS-атаку, и любое устройство умрет, если в нем нет защиты от подобного воздействия. Это число показывает, сколько одновременно различных параметров сессий и приложений умещается в оперативной памяти устройства. Максимального количества сессий можно плавно достичь, например, при подаче новых соединений каждую секунду в размере максимально заявленного CPS. Это число зависит

от объема оперативной памяти, количества/производительности процессоров и от включенного функционала.

3. **TT (Total Throughput)** — максимальная общая производительность устройства в байтах в секунду. Это суммарный объем входящего и исходящего трафика со всех интерфейсов NGFW при нужных вам функциях. Напомню, что 10-гигабитный интерфейс может одновременно передавать по 10 Гбит/с в одну и в другую сторону.

4. **Как реализовано и как выглядит журналирование**. Самый частый процесс в работе с любым firewall — это просмотр журналов. Проблемами для серьезной компании будут журналирование в текстовый файл, его полное отсутствие, журналирование только на внешние устройства, разрозненные журналы анализа для трафика, отсутствие поиска и фильтрации событий, отсутствие API и другие. Вам нужен удобный вариант, который позволит быстро найти нужную информацию о приложении или о файле и проанализировать ее. В журнале NGFW генерируется в разы больше информации о каждом соединении, чем в других сетевых устройствах: имена проходящих файлов во всех приложениях, типы файлов, названия вирусов в них, имена пользователей, названия приложений и их подфункций, страны, в которых зарегистрирован IP-адрес, названия заблокированных атак, действия с трафиком. Это бонус к привычной информации, которую мы обычно запрашиваем: IP-адреса, порты, URL-категории, зоны сети, аудит действий администраторов и событий от функций устройства.

Почему это влияет на выбор? Потому что журналирование снижает скорость устройства. Это работа со строками и на нее тратятся серьезные ресурсы. Часто производители NGFW тестируют скорость с выключенным журналированием, а после покупки устройство умирает, потому что мы лишь включили журналирование файлов.

5. **Как изменяются параметры CPS, CC, TT при включении всех функций безопасности.** Включение каждой дополнительной функции и даже одной сигнатуры IPS может значительно снизить все вышеперечисленные параметры. Включение полноценной проверки трафика всех приложений движками AV, IPS, DLP, URL-категоризация, Treat Intelligence, Anti-Bot и журналирование событий, особенно файлов, часто полностью загружает процессоры и убивает устройство. В случае неверного сайзинга мы не сможем включить все купленные (и реально нужные) функции защиты для нашей сети. Обычно измеряют в процентах от максимальной производительности в режиме «Все выключено».

Если вы раньше спрашивали: «Какая скорость у вашего NGFW?», то после прочтения данной статьи ваш вопрос будет звучать так: «Какая скорость у вашего NGFW со всей включенной защитой для HTTP-приложения с размером транзакции 44 КБ и журналированием всех событий и файлов?».

6. **Как изменяются параметры CPS, CC, TT при включении функции SSL Decryption.** SSL/TLS используется для сокрытия передаваемой информации между сервером и клиентом. Сейчас в общем объеме трафика на периметре компании SSL/TLS доходит до 80%. Большинство трафика приходится на HTTPS, но также есть SMTPS, FTPS и другие протоколы обмена. Чтобы предотвратить утечки из компании и проникновение вредоносного кода внутрь, используют механизм подмены сертификата на сетевом устройстве, которое расшифровывает трафик, проверяет его всеми имеющимися механизмами защиты и затем снова зашифровывает. Обычно проводят два теста: с включенным SSL Decryption и без него. Шифрование и расшифрование — это сложные математические преобразования данных. Нужно быть осторожным при включении режима SSL Decrypt. Учтите, что не все сервисы позволят подменить сертификат: сервера обновлений, вебинары и другие перестанут работать, — для них SSL Decryption включить нельзя, их добавляют в исключения. Исключения облегчат задачу.

Еще одна тонкость. Если мы проводим тесты, к загадочным результатам можно отнести скорость SSL Decryption с выключенными функциями безопасности. Что даст найденная скорость для оценки, подходит данная модель для защиты или нет? Мы же выполняем тест не ради теста, мы измеряем параметры функций защиты. Поэтому после извлечения расшифрованного трафика из SSL/TLS его нужно отдать на анализ движкам безопасности, а также надо включить определение приложений, ведь внутри SSL не обязательно HTTP. Да, чаще всего тестируют HTTPS. Если у вас в сети есть FTPS, SMTPS и другие протоколы, использующие SSL, их тоже нужно включить в тесты. После расшифрования SSL к полученному трафику следует применить функции безопасности: распознать приложение по контенту, проверить наличие атак сигнатурами IPS, а файлы — антивирусом, в «песочнице» или DLP, для URL в HTTP и в почтовых сообщениях проверить категорию, включить журналирование и т.д. И только после этого оценивать производительность в этом режиме. Одновременное включение SSL Decryption, антивируса и журналирования проверенных плохих и хороших файлов смертельно для любого NGFW, возможно, производителю даже придется краснеть за результат. Бывает, что у достаточно мощных устройств CPS падает до 1 соединения в секунду.

7. **Также важен профиль трафика, на котором тестировалась производительность.** Под профилем трафика мы понимаем конкретные приложения и конкретный размер транзакций в них. Например, размер файлов, которые передаем по HTTP. Именно профиль трафика определяет разницу между значениями в datasheet и реальной скоростью устройства в вашей сети. Вам нужно знать, на какой скорости будет работать выбранная модель именно в вашей сети, а не в лаборатории. И это можно определить только при тестировании на вашем реальном трафике. Данные, приведенные в datasheet, получены в лаборатории на искусственном трафике.

Если в лаборатории измеряли скорость на трафике UDP, где все пакеты одной длины, например 1500 Б, или на трафике HTTP, где все транзакции одной длины — 44 КБ, как вам это поможет? У вас в сети все IP-пакеты разные, у вас не может быть 100-процентного трафика UDP или HTTP. У вас в сети некий набор разных протоколов и приложений с пакетами и транзакциями разной длины.

Самые передовые компании оценивают скорость NGFW на смеси трафика разных приложений, допустим 30% SSL, 40% HTTP, 20% SMB, 10% FTP. Но, к сожалению, у всех эта смесь разная. К тому же для оценки скорости анализа приложений важен размер файлов, которые вы передаете. Допустим, NGFW может проверять 10 файлов по 125 МБ за 1 секунду, это создает трафик объемом 10 Гбит/с. А сможет ли при этом NGFW за 1 секунду проверить 1000 файлов по 1,25 МБ, что тоже создаст трафик 10 Гбит/с? Ниже будет показано, что нет, — чем короче размер транзакции, тем медленнее идет трафик через NGFW. Существует проект NetSecOpen (https://www.netsecopen.org/), который скоро стандартизирует методику тестирования.

Если вы изучаете официальный datasheet, внимательно читайте сноски: на каком именно трафике получены заявленные значения скорости и какие модули анализа трафика были включены.

Для примера: если одно устройство дает скорость 10 Гбит/с на HTTP 44 КБ, а другое — 10 Гбит/с на HTTP 1,7 КБ, это реально разные по скорости устройства! Устройство, которое смогло переварить трафик на таких коротких транзакциях, в 10 раз мощнее (об этом чуть ниже), хотя в сумме они дали трафик 10 Гбит/с. Но трафик-то был разный! **Чем короче транзакции приложений в сети, тем мощнее должен быть NGFW.**

Часть 1. CPS — количество новых соединений в секунду

Как вы считаете, есть ли разница в том, что ваш компьютер будет просто отправлять 200 файлов Word в сеть или перед отправкой еще открывать эти файлы в приложении Word и искать там слово «конфиденциально»? Нагрузка на память и процессоры разная: сам запуск 200 экземпляров программы Word — это тоже время. Успеет ли ваш компьютер сделать это за секунду? Или он успеет открыть только 50 файлов? Для того чтобы просто передавать 200 файлов в секунду нужны достаточные сетевые ресурсы, а вот чтобы запустить процесс анализа 200 файлов в секунду, нужен более мощный компьютер. Итак, количество новых файлов, которые мы можем взять для анализа за одну секунду, ограничено, — этот параметр очень важен, и его нужно учитывать.

После того как в первую секунду мы запустили 200 процессов анализа файлов, во вторую мы можем запустить еще 200 процессов анализа новых файлов и т.д., на каждой секунде увеличивая число анализируемых файлов до тех пор, пока не кончатся ресурсы: либо память, либо процессорная мощность, либо дисковое пространство, либо какие-то внутренние таблицы или буферы, известные только разработчикам. Так же и с сессиями, которые анализирует любой NGFW: вы не можете подать сразу 3 миллиона сессий на устройство — это будет DDoS-атака, и устройство умрет, если в нем нет защиты от них. Ниже мы обсудим еще один параметр — максимальное количество одновременных сессий. Вы можете достичь его, только плавно добавляя новые сессии. Число новых соединений, которые может обработать устройство в одну секунду, вычисляется при измерении мощности устройства и обозначается как CPS (Connections Per Second).

Вот так выглядит график количества соединений при тестировании любого сетевого устройства (рис. 1).

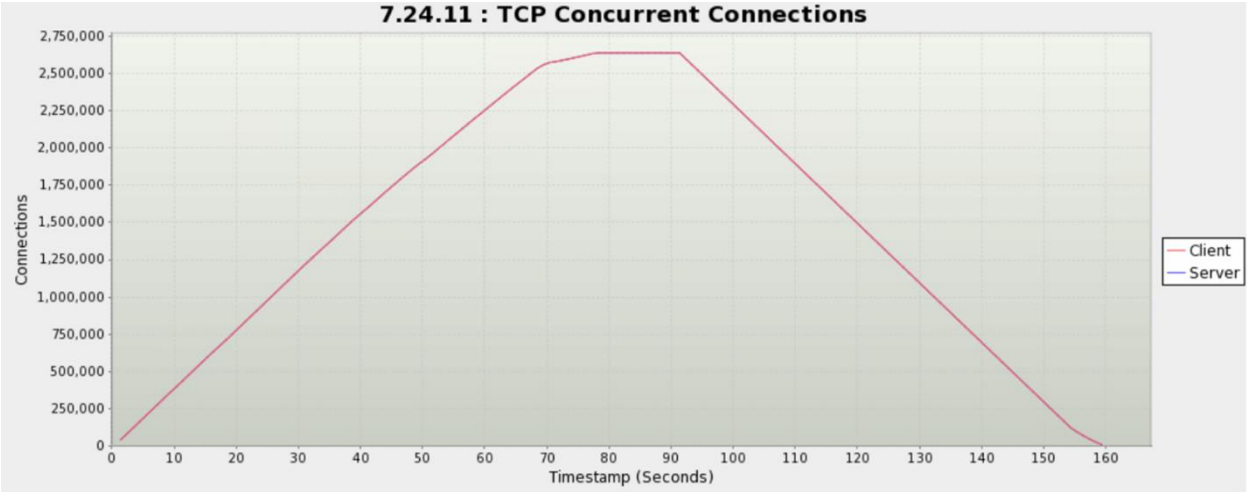


Рис. 1. Количество одновременных TCP-соединений при тестировании firewall

Проводя тест NGFW, вы постепенно подаете новые сессии, поскольку существует ограничение на количество новых сессий в секунду, которые может начать обрабатывать устройство: ему требуются время и ресурсы на каждую новую сессию, и количество новых сессий всегда ограничено. Максимальное значение CPS указывается в datasheet. CPS зависит от режима работы устройства. **Важно узнать у производителя, в каком режиме и на каком профиле трафика был измерен CPS.** Часто производители скрывают это, и заказчики вынуждены сравнивать значение CPS одного производителя, где все функции были выключены, со значениями CPS другого, где все функции были включены. Это ошибка. Давайте попробуем проанализировать CPS реальных устройств в разных режимах и разобраться, насколько режим работы устройства и профиль трафика важен при измерении CPS.

Начнем с основного режима: анализ приложений в IP-трафике. Мы знаем, что на рынке есть обычные firewall и есть NGFW. Мы вкладываем в эти понятия одно важное отличие: NGFW умеет анализировать данные приложений. Это нужно для визуализации типа приложений в нашей сети и

более удобного написания правил по типам приложений или по типам файлов, т.е. устройство работает на 7-м уровне модели OSI ISO. Для приложения Facebook мы теперь можем разрешить чаты, но запретить передачу файлов. Для приложения Gmail мы можем запретить прием файлов с расшиением .exe и отправку файлов с расширением .doc. В обычном firewall мы говорим про stateful inspection транспортного уровня протоколов TCP и UDP, или что устройство работает на 4-м уровне модели OSI ISO. А что происходит внутри приложения 7-го уровня, мы не анализируем. Можно провести аналогию с досмотром в аэропорту: мы проверяем либо паспорт, либо паспорт и содержимое багажа. Проверка багажа в NGFW называется безопасное разрешение приложений. Сейчас без этого безопасность сети немыслима.

На 3-й странице отчета NSS Labs NGFW 2018 приведено сравнение скорости устройств в режиме с инспекцией приложений и без него (рис. 2). Красным показана скорость, которую получили в режиме анализа приложения HTTP, а синим — скорость, которую получил NSS Labs с выключенным анализом приложений.

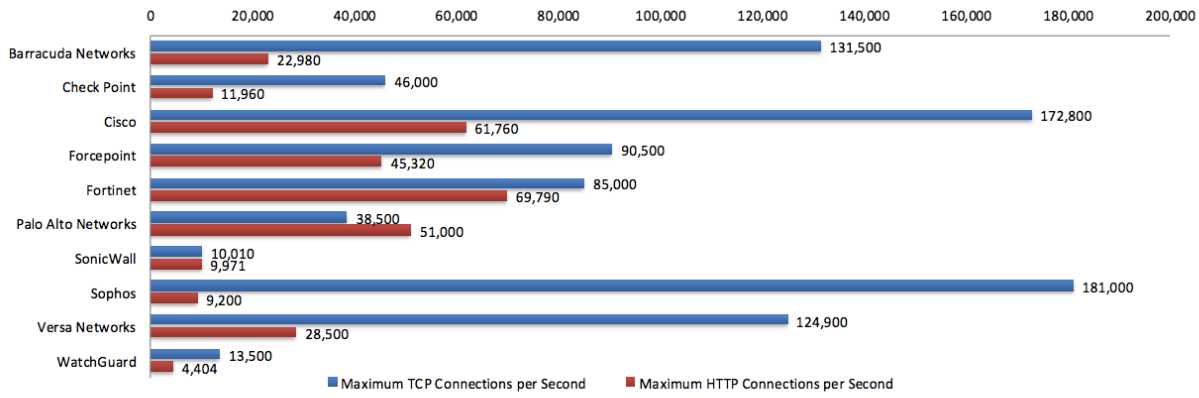


Figure 2 – Connection Dynamics

Рис. 2. Максимальные значения CPS в режиме анализа HTTP (выделено красным) и без анализа (выделено синим) (1)

Логично: когда анализ приложений выключен, скорость CPS увеличивается.

Опять же здесь важно сравнивать скорости, которые есть в datasheet и полученные при тестировании. И тут еще интереснее: данные по количеству новых соединений очень сильно отличаются. Сравните CPS 300 000 vs 11 960. Иначе говоря, в лабораторных условиях производитель смог достичь 300 000 CPS (исключим обман), а в тесте NSS не получилось, потому что трафик в лабораториях передавался разный и режим работы устройства тоже был разный.

Если включить разные функции защиты и разное число сигнатур в NGFW, в тестах получаются различные значения CPS. В этой фразе я, конечно, претендую на лавры Тони Роббинсона, но вы читаете эту статью, чтобы для вас это тоже стало банальностью.

Часто возникает удивительная ситуация: заказчик выбирает IPS нужной ему производительности, но поставщик отказывается включать все сигнатуры во время тестов. Просят использовать default-профиль, т.е. некоторую часть сигнатур (а заплатить просят за все 100%). Или бывает, что идет сравнение производительности двух IPS: в первом включено 40% сигнатур, во втором — 80%. И как оценивать их скорости? Один должен быть быстрее другого в 2 раза? Да и с сигнатурами IPS много тонкостей: сигнатура IPS одного поставщика может делать то же самое, что 300 сигнатур другого. Можно ли добавить в сравнение NSS Labs данные из официальных datasheet (рис. 13)?

Рис. 3. Пример неверного сравнения: максимальные значения CPS из теста NSS Labs в режиме анализа HTTP (выделено красным) и без анализа (выделено синим) и CPS из официальных datasheet (выделено зеленым) [(1)]

Сравнивать CPS из datasheet и CPS в тесте NSS Labs некорректно, потому что измерения были проведены с разными настройками NGFW и на разном трафике. Однако эта диаграмма (рис. 3) специально для тех, кто любит сравнивать яблоки и апельсины: 300 000, 46 000, 11 960 — это разные значения CPS, но это производительность одного и того же устройства Check Point 15600, полученная в разных условиях. Аналогично прыгает CPS в разных тестах и у других производителей. А какое число выбрать нам? Ответ: на нашем трафике с нужными нам функциями устройство покажет настоящий CPS, поэтому так важно тестировать устройство.

При выборе NGFW мы должны задать себе очень важный вопрос: какой параметр CPS достаточен для нашей сети? Нужно ориентироваться на данные CPS, которые видны на текущем сетевом оборудовании. К тому же у уже имеющегося оборудования есть параметры CPS в datasheet, можно воспользоваться ими. Если запрашивать NGFW с CPS, большим, чем у уже имеющегося текущего сетевого оборудования, это не даст прироста в

производительности сети. Значение CPS повлияет только на цену NGFW. Среднее значение CPS будет зависеть от поведения сотрудников: чем они занимаются? По статистике, в среднем сотрудник генерирует новое соединение 1 раз в 10 секунд. Соответственно, лишь 1 новое соединение в секунду нужно на каждые 10 сотрудников, 10 CPS на 100 сотрудников, 100 CPS на 1000 сотрудников и 1000 CPS на 10 000 сотрудников и т.д. Однако в сети есть еще сервера, принтеры, сетевое оборудование или оборудование, передающее голос и видео. В каждой компании будет свое значение CPS. Нам нужно оценить максимальные всплески CPS, например утром, когда все приходят на работу и почти одновременно подключаются, или после обеда, когда все возвращаются к работе, и этот CPS требуется для нашей сети.

Так ли критично ошибиться или взять устройство с меньшим CPS? Если будет всплеск и для устройства с максимальным значением 50 000 CPS сеть вдруг сгенерирует 100 000 CPS? Ничего страшного не будет, если браузер сотрудника подключится к сайту не в первую секунду, а во вторую. Но мы выше посчитали, CPS 50 000 может случиться, если в сети более 500 тысяч сотрудников идут через NGFW. Я подобных сетей не знаю. Такое может быть в телекоме, но там NGFW не рекомендуется использовать на каналах передачи данных либо им надо покупать максимальные по скорости модели, чтобы уложиться в параметр CPS, одновременно включив все функции безопасности.

Стоит ли просить в тендере устройства с CPS, большим, чем нужно реально? Да, если у вас огромный бюджет. Устройства, которые мы рассмотрели выше, дают 50 000 CPS (без инспекции трафика), и это очень много. Такие устройства сейчас используются и на периметре сети, и в ЦОД. Хотите устройства, которые дают 2 миллиона CPS, — это будет уже шасси, которое стоит миллионы долларов.

Чем больше функционала NGFW включено, тем ниже CPS

В тестах NSS Labs по NGFW используются лишь две функции: распознавание приложений и IPS. И уклон их тестов всегда в сторону IPS. Когда мы будем проводить свой тест, мы включим все нужные нам функции, и, по-хорошему, все функции NGFW важны.

Как вы видели выше в тесте NSS, анализ на уровне приложений в 2–4 раза снижает число CPS по сравнению с режимом без анализа. А что будет, если включить дополнительно анализ движком IPS, антивирусом и т.д.?

Компания bi.zone 20 ноября 2019 года провела конференцию по тестам производительности, и представитель IXIA выступил с лекцией, как измерять CPS. В его презентации были продемонстрированы результаты тестирования pfSense + Suricata. IXIA тестировала виртуальную машину с установленным firewall + IPS. Этот виртуальный firewall показал CPS 40 000 при работе в режиме роутера, а при включении satefull inspection CPS стал 12 500. При включении защиты на базе Suricata CPS упал до 2000 — в 20 раз снизился CPS при включении функционала защиты. Выступление IXIA можно посмотреть в записи по ссылке https://youtu.be/GibRXgWbaR8.

pfSense	B2B	Router mode	FW mode	IPS mode
HTTP CC	2.6M	2.6M	1.2M	270K
HTTP CPS stable	40K	40K	12.5K	2.0K
Attacks only	--	--	--	528/945
Attacks + HTTP CPS 2.0K	--	--	--	394/945

Рис. 4. Результаты тестирования pfSense + Suricata в лаборатории IXIA. Скриншот из презентации компании IXIA [(2)]

Обратите внимание на строку HTTP CPS stable и на то, как меняется CPS в разных режимах работы pfSense: при включении statefull firewall и IPS значение CPS падает в 20 раз (рис. 4).

Также из результатов данного теста видно, что число одновременных сессий упало в 10 раз — с 2 600 000 до 270 000 при включении функционала stateful inspection и IPS. Понятно почему: любой дополнительный функционал тратит оперативную память. Такие результаты будут у любого многофункционального устройства.

Чем короче транзакции у приложений, тем ниже CPS

Важно ли нашему компьютеру, сколько новых файлов он будет передавать в секунду, если это файлы разной длины? А если нужно не просто передать файлы, но и открывать их для проверки перед отправкой? Допустим, нам нужно стартовать для проверки 200 новых файлов в секунду. В первом тесте мы хотим проверить скорость, где файлы длиной 4,4 КБ, а втором — 44 КБ. Будет ли отличаться скорость проверки 200 файлов разной длины? Это, пожалуй, самый неочевидный вопрос. Лучше провести тесты.

Тесты NGFW в NSS Labs и других лабораториях показывают, что размер транзакции приложения прямо влияет на CPS. Посмотрите, это хорошо показано в результате теста NSS Labs (рис. 5). Каждый HTTP GET-запрос получал в ответ файл одной и той же длины. Были проведены последовательно тесты для файлов с размерами от 1,7 до 44 КБ. В результате теста для размера файла 44 КБ большинство производителей позволило создавать через себя 25 000 новых соединений в секунду, а для размера файла 1,7 КБ — до 60 310.

Figure 14 depicts the maximum application layer connection rates (HTTP connections per second) achieved with different HTTP response sizes (from 44 KB down to 1.7 KB).

Vendor	44 KB Response Size	21 KB Response Size	10 KB Response Size	4.5 KB Response Size	1.7 KB Response Size
Barracuda Networks	11,270	12,490	14,800	18,940	21,540
Check Point	25,000	47,491	62,800	47,600	51,200
Cisco	25,000	50,000	54,200	56,060	58,600
Forcepoint	25,000	41,000	55,310	63,730	64,340
Fortinet	19,290	29,100	42,930	51,200	60,310
Palo Alto Networks	25,000	43,160	44,670	56,570	46,900
SonicWall	2,480	3,926	5,697	7,041	8,001
Sophos	5,994	8,600	7,800	9,819	9,972
Versa Networks	5,338	7,164	10,500	16,550	22,400
WatchGuard	2,000	2,850	3,700	3,647	4,383

Figure 14 – Maximum Connection Rates per Device with Various Response Sizes

Рис. 5. Максимальный CPS в зависимости от длины транзакции HTTP (длины скачиваемого файла) (1)

Если все вышесказанное представить в виде гистограммы, видно, чем длиннее размер транзакции (в данном тесте она равна длине файла), тем меньше CPS (рис. 6).

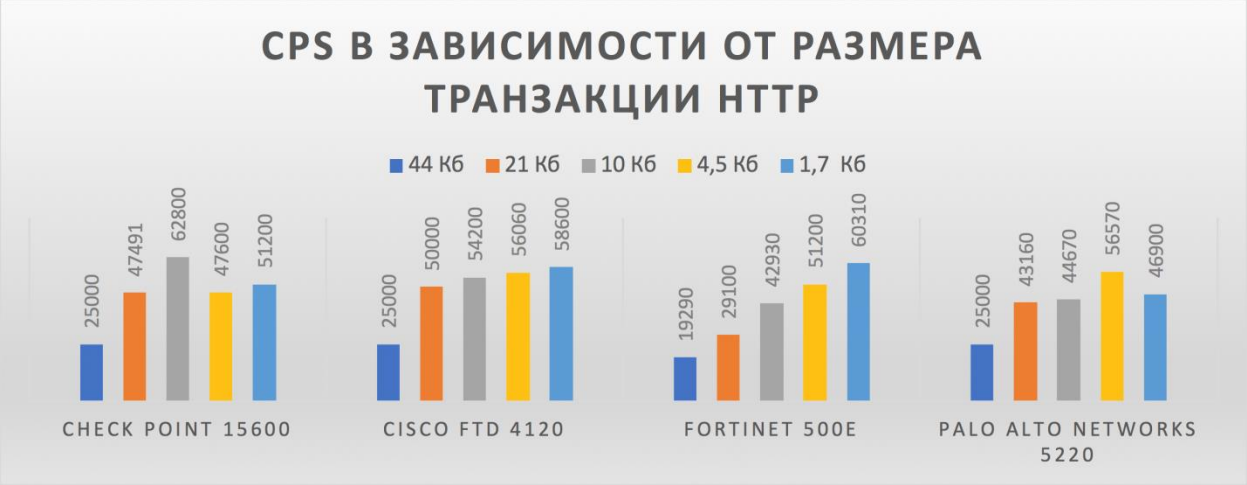


Рис. 6. Влияние размера транзакции HTTP на CPS(1)

И, кстати, давайте посчитаем, сколько это в мегабайтах в секунду: умножим размер транзакции на их количество (рис. 7).

Рис. 7. Влияние размера транзакции HTTP на количество нового трафика в секунду(1)

Интересная получилась картина: у коротких транзакций CPS больше, однако, если считать по количеству переданных байт, бóльшая разница отмечается в динамике прироста трафика: сравните 1049 vs 80 Мбайт в секунду на большом числе коротких транзакций.

А ваш IPS перестает работать при нагрузке?

В вышеупомянутом тесте IXIA выявлено, что при сильной нагрузке трафиком модуль Suricata IPS перестает блокировать атаки: число заблокированных атак упало с 528 до 394 при подаче большого объема трафика (см. рис. 4).

То же самое увидите в тестах и вы: большинство производителей IPS и потоковых антивирусов хорошо показывают себя при тестировании на одном компьютере. И это частая ошибка во время пилота — тест функционала NGFW с одного компьютера. В итоге, когда NGFW ставят в реальную сеть, с тысячью

компьютеров, срабатывает внутренняя защита, и он начинает пропускать трафик без проверки.

NGFW реально тяжело, когда в нем включают всю инспекцию приложений 7-го уровня, проверку файлов, антивирусы и другие движки защиты, поэтому вы всегда должны проверять значения CPS, CC и TT в режиме «Все включено».

Именно этим хороши тесты NSS Labs: IPS проверяется под нагрузкой и показывает, как справляется с атаками. Не понимаю, почему NSS не тестируют NGFW вместе с антивирусом. Возможно потому, что в тестах производительности с включенным потоковым антивирусом у всех все плохо.

А ваш антивирус перестает работать при нагрузке?

По моему опыту тестирования, самый ресурсоемкий программный код в UTM — антивирус. UTM нужно собрать из всех проходящих фреймов полноценный файл и проверить в нем сигнатуры или хеши из базы антивируса. Часть файлов является архивами. ZIP-архив создан так, что его можно распаковать в потоке, а RAR и 7ZIP требуют, чтобы их скачали полностью. И это, конечно же, влияет на процессоры и на память устройства. Каждый такой передаваемый архив, а их может быть несколько тысяч, создает нагрузку на NGFW.

Потоковые антивирусы делятся на два класса: проверка по хешам и проверка по сигнатурам. Хеш находит конкретную версию вируса, а сигнатура — все версии данного вируса. Проверка по хешам обычно работает медленнее, потому что в базе нужно хранить все версии каждого вида вредоносного ПО.

Следующая трудность — сами протоколы, по которым передаются файлы. Обычно антивирусом проверяют файлы внутри HTTP, SMTP, POP3, IMAP, FTP, SMB. Практика показывает, что SMB и FTP очень сложны для анализа файлов в NGFW, поэтому у многих производителей либо нет проверки файлов и работы антивируса по этим протоколам, либо анализ файлов в этих протоколах катастрофически снижает параметры CPS и TT. Это четко видно во время тестов. Самый частый протокол для тестирования антивируса — HTTP: в нем проще отследить транзакции и файлы. Во многих NGFW вы регулируете, в каких приложениях работает антивирусный движок, для каких типов файлов и для файлов какой длины он запускается. Чем больше файлов вы проверяете одновременно, тем сложнее устройству.

У некоторых производителей есть функция отключения всех проверок при перегрузке процессоров, поэтому при тестировании NGFW нужно не просто подавать файлы под максимальной нагрузкой, но и проверять в журналах, были ли найдены вирусы. Возможно, когда вы качаете один файл по SMB, вирус и обнаружится, а когда несколько человек будут качать всю папку с 2000 вирусов, часть вирусов спокойно пройдет без проверки.

Часть 2. CC —количество одновременных соединений в секунду

Память каждого многофункционального устройства делится на множество буферов разного типа. На хранение состояний соединений в каждой модели устройства любого производителя в оперативной памяти выделяется буфер определенного размера. Если этот блок памяти разделить на размер буфера, необходимый для хранения состояния каждой TCP-сессии, получится максимальное количество сессий, которые устройство может хранить в своей памяти. На состояние TCP-сессии влияет лишь информация из заголовка TCP. На состояние сессий приложения FTP уже влияет несколько TCP-сессий: как минимум сессия управления и сессии передачи файлов. На состояние сессий HTTP, RPC или SIP влияют к тому же поток данных и

команды которые идут внутри приложения. Логично, чтобы хранить состояние TCP-сессий, нужен более короткий буфер — заголовок TCP + IP составляет всего 40 Б. А если хранить состояния более высокоуровневых приложений: FTP, HTTP, SMB, RPC, SIP и других, — потребуется буфер более длинный, и тогда хранение состояния приложения 7-го уровня при том же количестве памяти уменьшит количество одновременных сессий, которые уместятся в памяти всего устройства. Это теоретическое размышление легко проверить на практике: если выключить модуль анализа приложений и сделать межсетевой экран обычным портовым firewall без анализа приложений, количество одновременных сессий увеличивается. Поэтому всегда важно спрашивать производителя, в каком режиме работы он считал количество одновременных сессий: 4-го или 7-го уровня.

В презентации компании IXIA мы уже обращали внимание на параметр CPS. Давайте теперь проанализируем параметр CC. Видно, что количество одновременных сессий в режиме без инспекции — 2 600 000, в режиме с инспекцией — 1 200 000, а в режиме IPS — уже 270 000, т.е. упало в 10 раз (см. рис. 4). Количество одновременных сессий 4-го и 7-го уровня на одном и том же устройстве обычно так и отличается — в 10 раз. В итоге для данного теста: если в вашей сети 1 миллион одновременных сессий, вы либо должны взять более мощное устройство для работы IPS, либо не включать последний. Второй вариант чаще всего и случается: при выборе отдел закупки смотрит в таблице на самое большое значение CC, а надо было смотреть на самое маленькое. И тут нужна помощь специалистов, чтобы показать, какие параметры реально важны для выбора устройства. Посмотрите в datasheet и спросите представителя производителя, в каком режиме работы измерялось число одновременных сессий. Если только на сессиях 4-го уровня, потребуйте данные для сессий 7-го уровня.

А сколько нужно вам? Посмотрите в своем текущем сетевом оборудовании — этот параметр в статистике уже есть. Но учтите, не все сетевые устройства считают трафик ICMP за сессии, а NGFW будет их считать за сессии, поскольку отслеживает эти пакеты в обе стороны. Из опыта, даже в очень больших сетях редко идут 1 000 000 одновременных соединений в секунду, а когда устройство поддерживает 3 миллиона одновременных сессий, это тройной запас. Поспрашивайте коллег, сколько одновременных сессий секунду они видят на периметре своей сети.

Часть 3. TT — максимальная пропускная способность устройства

Параметр максимальной пропускной способности считается самым главным при выборе, поскольку именно по нему измеряются все сетевые устройства, а не только NGFW. Сетевой трафик состоит из смеси отдельных транзакций разных приложений. На уровне приложений нет ограничений на длину транзакции. Это могут быть файлы длиной несколько гигабайт, идущие от сервера к клиенту, или непрерывный поток, например видео или звук. А вот нижележащие уровни стека TCP/IP фрагментируют данные приложений. Мы должны понимать, что на разбиение и сборку этих фрагментов тратятся ресурсы каждого сетевого устройства. Если смотреть на канальном уровне, каждая транзакция приложения делится на отдельные фреймы длиной 1500 Б или 9000 Б, если в сети разрешены jumbo frame. В datasheet вы можете увидеть разные значения длины: 1500, 1514, 1518. Кто-то учитывает еще длину заголовка фрейма 14 байт, кто-то и контрольную сумму FCS длиной 4 байта. Внутри ЦОД принято использовать jumbo frame, поскольку это ускоряет передачу данных по сети. Если смотреть на уровне IP, то максимальная длина IP пакета 65 535 и IP пакет уже разбивается на фреймы согласно RFC 791. Приложение в свою очередь использует TCP сегменты или UDP датаграммы для передачи внутри IP пакета. Существует много тонкостей в работе стека TCP/IP, поэтому рекомендую хорошо знать их, перед тем как вы будете оценивать производительность NGFW. Например, фреймы и пакеты имеют

свойство теряться, и TCP/IP стек повторяет их передачу, а на это нужно время, и процент потерь влияет на параметр числа переданных байт приложения в секунду. В лабораторных условиях потери можно устранить, а в реальной сети потери все равно будут.

Как меняется пропускная способность устройства NGFW, если передавать на уровне приложений данные разной длины? Что будет, если скачивать по HTTP файлы разного размера? Лучше всего это протестировать.

Тест пропускной способности для транзакций HTTP разной длины

Аналитики NSS Labs провели несколько тестов. Через каждый NGFW пересылали HTTP запросы GET и в ответ возвращали файлы длиной сначала 44 КБ, в следующем тесте 21, 10, 4,5 и 1,7 КБ в окончательном тесте. Давайте сравним результаты максимальной пропускной способности в случаях с ответами по 44 и 1,7 КБ (рис. 8). Остальные результаты вы можете посмотреть в отчете NSS.

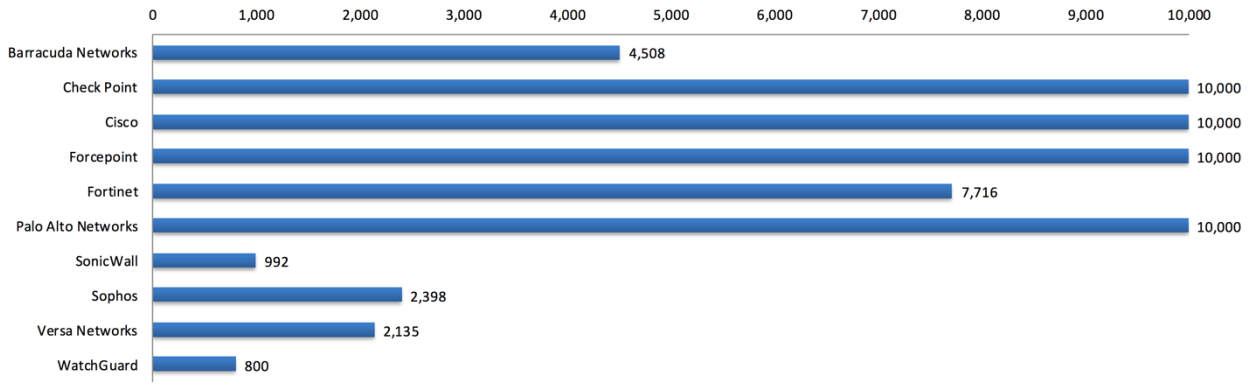


Figure 9 – Maximum Throughput per Device with 44 KB Response (Mbps)

Рис. 8. Максимальная пропускная способность при размере файлов 44 КБ[(1)]

С размером транзакции 44 КБ устройства Check Point, Cisco, Palo Alto Networks смогли достигнуть скорости 10 Гбит/с, Fortinet — 7,7 Гбит/с.

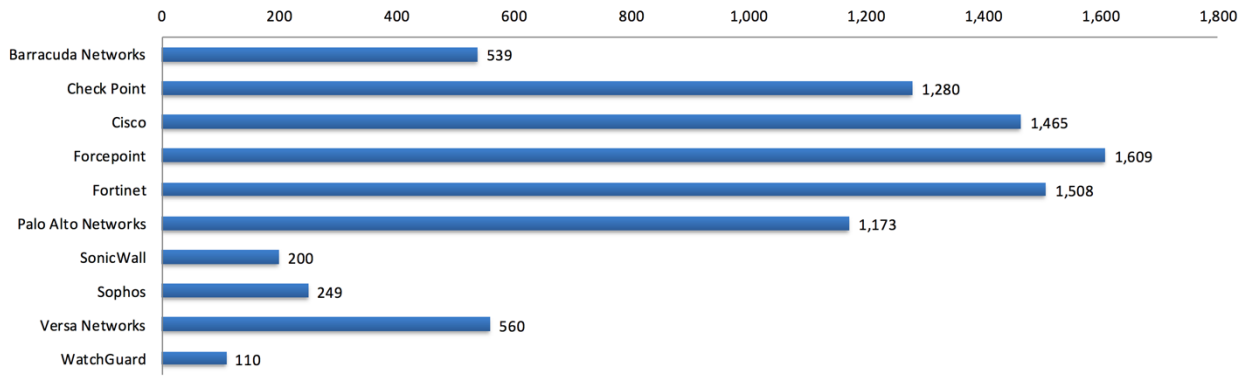


Figure 13 – Maximum Throughput per Device with 1.7 KB Response (Mbps)

Рис. 9. Максимальная пропускная способность при размере файлов 1,7 КБ(1)

С размером транзакции 1,7 КБ устройства Check Point, Cisco, Fortinet, Palo Alto Networks смогли достигнуть скорости 1,28, 1,465, 1,508 и 1,173 Гбит/с соответственно (рис. 9).

***Акцентирую ваше внимание**: 10-гигабитные устройства стали 1-гигабитными!*

Пропускная способность у каждого устройства уменьшилась на порядок!

Причина — изменение размера транзакции с 44 до 1,7 КБ. Мы уже упоминали этот тест, когда обсуждали CPS. Вы помните, что CPS при уменьшении размера транзакции увеличивается (рис. 5), но недостаточно, чтобы прокачать 10 Гбит в секунду.

Тест пропускной способности для разных профилей трафика

Но ведь у нас в сети не 100% HTTP, а сборная солянка приложений. Тест со смешанным трафиком есть у NSS. И тут цифры скачут снова между 10 и 1 Гбит/с (рис. 10, 11).

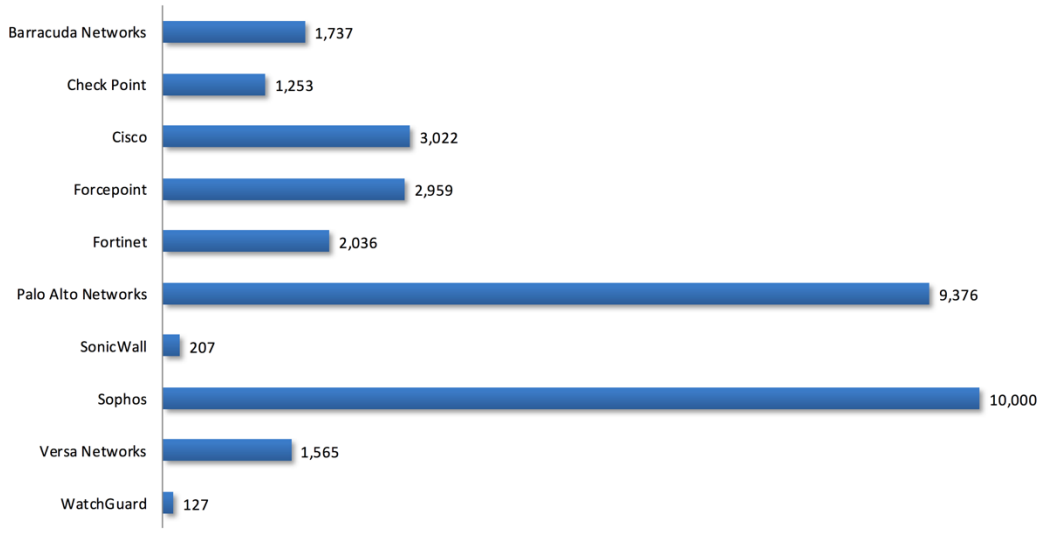


Figure 20 –Single Application Flow: Financial (Mbps)

Рис. 10. Максимальная пропускная способность для профиля трафика финансовой организации(1)

На трафике финансовых организаций почти все производители сильно снижают свою скорость. Как правило, для такого трафика характерны короткие пакеты, поэтому это выглядит логично (рис. 10). В тестах на типах трафика у NSS Labs видна какая-то аномалия с некоторыми результатами. Например, Sophos XG – в предыдущем тесте 249 Мбит/с (рис. 9), а тут 10 Гбит/с (рис.10), в то время как все другие производители просели. Не нахожу объяснения. Нужно уточнять у NSS какие были модули анализа трафика включены и какой был точно подан трафик. Это еще раз означает, что проводить собственный тест всегда достоверней.

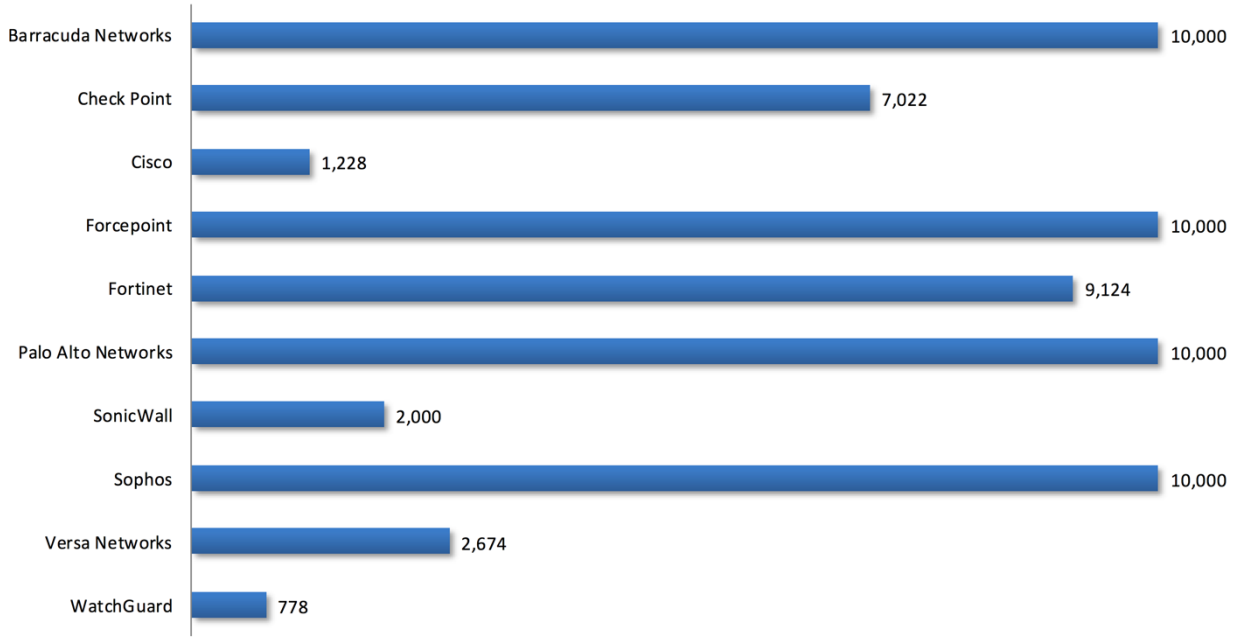


Figure 25 –Single Application Flow: Video (Mbps)

Рис. 11. Максимальная пропускная способность для профиля трафика с видеопотоком(1)

На видеотрафике все производители становятся быстрыми. При анализе этой диаграммы закрадывается подозрение, что 10 Гбит/с является максимальным не для устройства, а максимально генерируемым в тесте NSS — уж слишком много одинаково ровных результатов 10 Гбит/с. Так бывает, когда для теста используют один интерфейс со скоростью 10 Гбит/с. Устройства такой мощности лучше тестировать через интерфейсы со скоростями 40 или 100 Гбит/с либо делать EtherChannel.

Остальные тесты можно посмотреть непосредственно в самом отчете NSS Labs.

Итак, одно и то же устройство может быть как 10 Гбит/с, так и 1 Гбит/с в зависимости от типа трафика, который мы передаем через него. *Оценивайте устройства разных производителей и различные устройства одного*

производителя на одном типе трафика! Это единственно верный способ сравнить NGFW.

Часть 4. Официальные данные скорости vs реальные данные скорости

На странице 6 упомянутого отчета NSS Labs есть сравнение скоростей официальных, т.е. полученных в лаборатории производителя и опубликованных на сайте, и скоростей, измеренных в NSS Labs.

Красным показана скорость, которую производитель официально прописывает в datasheet, а синим — скорость, которую реально смогла достичь NSS Labs во время своих тестов. Анализируя данные отчета NSS, учтите, что запятая в американской нотации лишь разделяет число для удобства чтения — это не знак десятичной дроби (рис. 12).

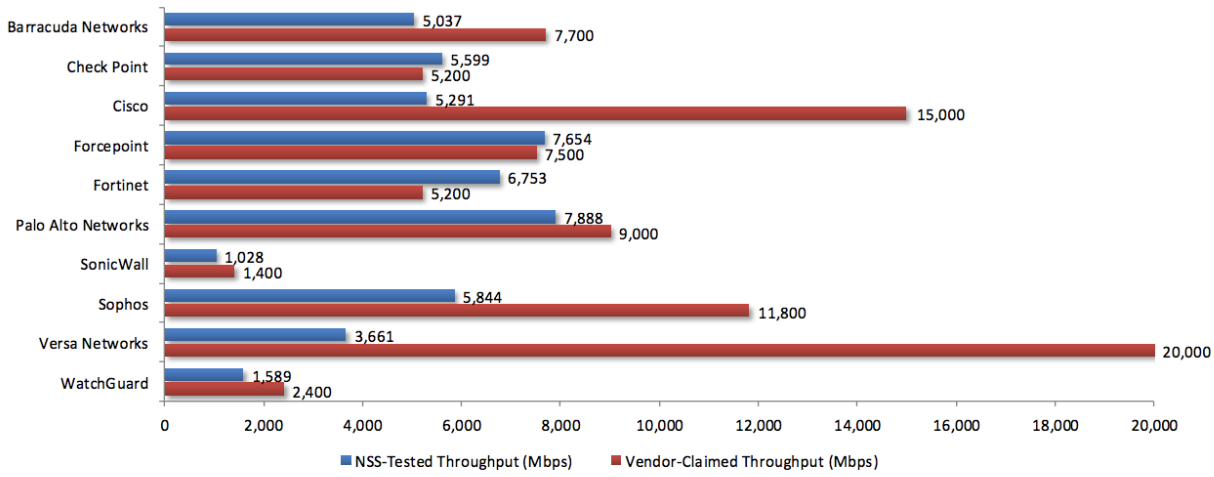


Figure 3 – Vendor-Claimed Throughput vs. NSS-Tested Throughput (Mbps)

Рис. 12. Сравнение декларируемой и измеренной пропускной способности(1)

И тут мы видим нестыковки с данными 2019 года! Давайте посмотрим какие:

- По Check Point в 2018 NSS Labs взял число из datasheet **5,599** Гбит/с, хотя в декабре 2019 года в официальном datasheet мы видим, что для модели 15600 заявлена скорость **10** Гбит/с.
- По Cisco 4120 заявленная скорость **19** Гбит/с, хотя NSS Labs пишет **15** Гбит/с.

- По Fortinet 500E заявленная скорость **5** Гбит/с, хотя NSS Labs пишет **5,2** Гбит/с.
- По Palo Alto Networks PA-5220 заявленная скорость **7,2** и **8,9** Гбит/с, хотя NSS Labs пишет **9** Гбит/с.

Кстати, интересный нюанс: нет данных, на каких приложениях получена такая скорость самим NSS Labs! Ведь, как мы увидим ниже, скорости устройства зависят от приложения, которое мы тестируем: HTTP, SMB, FTP, SSL, SIP, RTP или смесь приложений. Например, Palo Alto Networks так и пишет в сносках: если измерять TT на HTTP-ответах длиной 64 КБ, скорость устройства — 7,2 Гбит/с со всем включенным функционалом, а если измерять на смешанном трафике разных приложений, скорость увеличится — 8,9 Гбит/с. Опять же надо учитывать, что в вашей сети свой набор приложений (рис. 13).

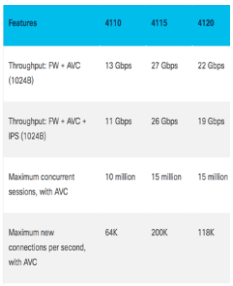
Check Point 15600


Check Point
SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY
Performance
Enterprise Testing Conditions
- 10.1 Gbps of Threat Prevention[1]
- 12.6 Gbps of NGFW[2]
- 13.5 Gbps IPS
- 41.2 Gbps of firewall throughput

Ideal Testing Conditions
- 76 Gbps of UDP 1518 byte packet firewall throughput
- 15.8 Gbps of AES-128 VPN throughput
- 300,000 connections per second, 64 byte response[3]
- 6.4/12.8/25.6M concurrent connections, 64 byte response[3]

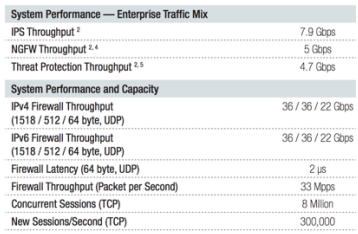
1: Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection. 2: Includes Firewall, Application Control and IPS. 3: Performance measured with default/HPP/maximum memory with R80.10.

Cisco 4120



Features	4110	4115	4120
Throughput: FW + AVC (1024B)	13 Gbps	27 Gbps	22 Gbps
Throughput: FW + AVC + IPS (1024B)	11 Gbps	26 Gbps	19 Gbps
Maximum concurrent sessions, with AVC	10 million	15 million	15 million
Maximum new connections per second, with AVC	64K	200K	118K

Fortinet 500E



System Performance — Enterprise Traffic Mix	
IPS Throughput [2]	7.9 Gbps
NGFW Throughput [2, 4]	5 Gbps
Threat Protection Throughput [2, 5]	4.7 Gbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36 / 36 / 22 Gbps
Firewall Latency (64 byte, UDP)	2 µs
Firewall Throughput (Packet per Second)	33 Mpps
Concurrent Sessions (TCP)	8 Million
New Sessions/Second (TCP)	300,000

Palo Alto Networks 5220

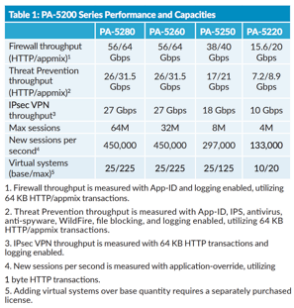


Table 1: PA-5200 Series Performance and Capacities

	PA-5280	PA-5260	PA-5250	PA-5220
Firewall throughput (HTTP/appmix)[1]	56/64 Gbps	56/64 Gbps	38/40 Gbps	15.6/20 Gbps
Threat Prevention throughput (HTTP/appmix)[2]	26/31.5 Gbps	26/31.5 Gbps	17/21 Gbps	7.2/8.9 Gbps
IPsec VPN throughput[3]	27 Gbps	27 Gbps	18 Gbps	10 Gbps
Max sessions	64M	32M	8M	4M
New sessions per second[4]	450,000	450,000	297,000	133,000
Virtual systems (base/max)[5]	25/225	25/225	25/125	10/20

1. Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.
2. Threat Prevention throughput is measured with App-ID, IPS, antivirus, anti-spyware, WildFire, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.
3. IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.
4. New sessions per second is measured with application-override, utilizing 1 byte HTTP transactions.
5. Adding virtual systems over base quantity requires a separately purchased license.

Рис. 13. Официальные данные CPS, CC и TT из datasheet Check Point, Cisco, Fortinet, Palo Alto Networks

Данные взяты из официальных datasheet (январь 2020 года):

- https://www.checkpoint.com/downloads/products/15600-security-gateway-datasheet.pdf;
- https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html;
- https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_500E.pdf;
- https://www.paloaltonetworks.com/resources/datasheets/pa-5200-series-specsheet.

Критерий выбора параметра ТТ для сравнения следующий: вам нужно выбрать такое число, которое отражает скорость устройства при всех включенных функциях. По сути, это будет минимальное число, которое отражает производитель в своих datasheet. Итак:

- Check Point — 10.1 Gbps of Threat prevention.
- Cisco — 19 Gbps Throughput: FW + AVC + IPS (1024B).
- Fortinet — 4.7 Gbps Threat Protection Throughput.
- Palo Alto Networks — 7.2/8.9 Threat Prevention throughput (HTTP/appmix).

Анализируя данные, которые показывает NSS Labs, мы понимаем, что с 2018 года все производители изменили свои официальные datasheet, причем Check Point и Cisco исправили datasheet в сторону увеличения (с 5,2 до 10,1 и с 15 до 19 Гбит/с соответственно), а Fortinet и Palo Alto Networks — в сторону уменьшения. Логика есть в уменьшении скорости: в каждый NGFW периодически добавляются новые функции безопасности, и устройство должно становиться все медленнее и медленнее. Не вижу логики увеличивать скорость в datasheet одной и той же модели. Возможно, представительства соответствующего производителя смогут это объяснить.

Если сравнивать с актуальной официальной информацией, диаграмма будет выглядеть так (рис. 14).

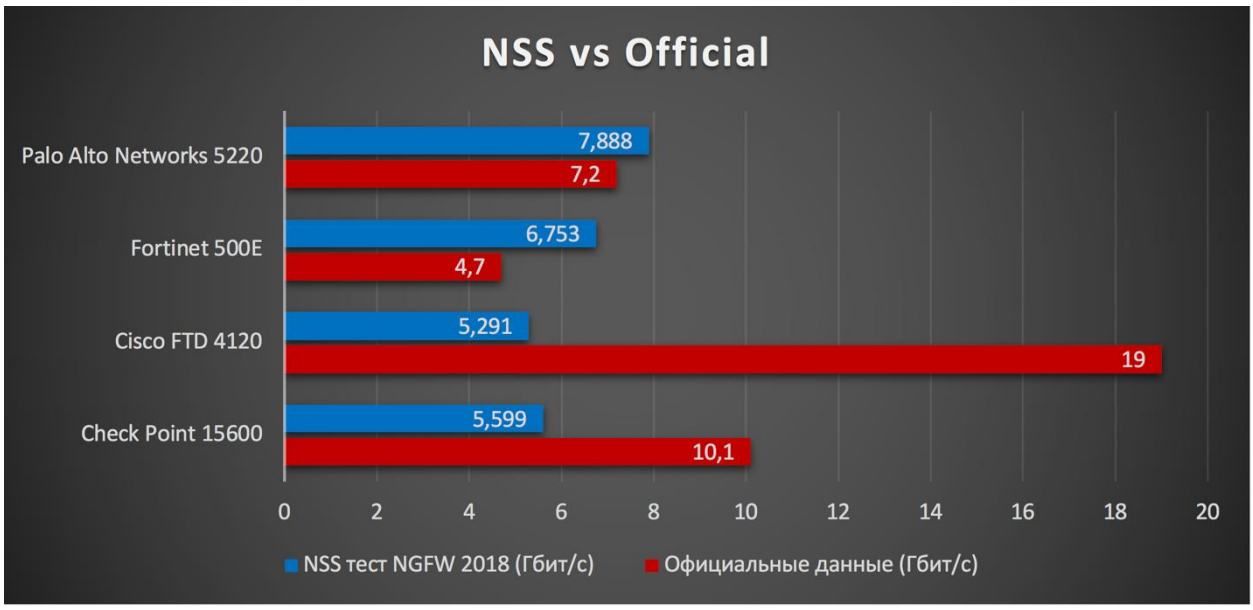


Рис. 14. Официальные значения TT из datasheet и измеренные значения TT в NSS Labs(1)

Здесь запятая — знак десятичной дроби, а все значения указаны в гигабитах в секунду.

Мы обсуждали выше, что скорости устройств, измеренных на одном профиле трафика при одинаковых выполняемых функциях, можно сравнивать. Иначе говоря, устройства друг с другом нужно сравнивать по тесту NSS (синие столбцы на рис. 14). Получается, что в тесте принимали участие более-менее одинаковые по мощности устройства от Cisco и Check Point, которые проверяют 5 Гбит/с данных приложений со всеми включенными функциями безопасности. Palo Alto Networks предоставила в тест устройство на 44% мощнее по TT, чем 5 Гбит/с. Fortinet предоставил в тест устройство на 35% мощнее по TT, чем 5 Гбит/с.

Почему удобнее сравнивать по тестам NSS?

Потому что все устройства были проверены на одном профиле трафика и в одном режиме: были включены функции определения приложений и IPS. К минусам тестов NSS Labs можно отнести то, что они никогда не тестируют потоковый антивирус, только IPS, и то, что профиль трафика, на котором они

тестируют, неизвестен. Они посылали атаки только по HTTP или были еще атаки в SMB, или RPC, или DNS? Остается только гадать. Но важно, что профиль трафика для всех тестируемых устройств был один и тот же.

А почему нельзя сравнивать скорости в разных datasheet?

Представьте, есть 4 человека: одного попросили максимально быстро перенести 1000 коробок по 1 кг, другого — 500 коробок по 2 кг, третьего — 200 коробок по 5 кг, четвертого — одну коробку в 1000 кг. И они перенесли. В сумме — 1000 кг. Можем ли мы понять, кто из них лучше? Вряд ли. Мало того, мы не знаем, как они решали эту задачу. Может быть, первый переносил сразу по 2 коробки, и задача была равносильна задаче второго, или он сразу перенес 100 коробок, и задача была равносильна четвертому.

То же самое и с datasheet разных производителей. Один измерял скорость, когда устройство проверяло трафик HTTP длиной 44 КБ, другой проверял некую сборную солянку, где HTTP было только 20% с неизвестным размером транзакций, третий проверял не только IPS, но и антивирусом, четвертый не просто проверял, а еще журналировал каждое соединение и каждый файл. И как их сравнивать? Как сравнить сладкое с зеленым? Поэтому значения, которые на рис. 14 выделены красными столбцами, сравнивать нельзя. А так хотелось в самом начале, да?

Вывод: выбирать устройство по официальным datasheet опасно, потому что реальная скорость устройства в вашей сети будет отличаться от прописанной в datasheet. Вы можете заплатить за 10 Гбит/с устройство по datasheet и в реальности получить в 2–4 раза медленнее. Тогда придется докупать еще 2–3 устройства, балансировать трафик между ними и как-то реализовывать high availability. Возможно, стоило бы купить устройство у другого производителя, пусть чуть-чуть дороже, но с реальными 10 Гбит/с.

Часть 5. Рекомендации по собственному тестированию NGFW

Выше мы уже говорили о проекте NetSecOpen (https://www.netsecopen.org/), который скоро стандартизирует методику тестирования и нам не придется делать тесты самим. Сейчас, если производитель готов предоставить нам устройство для теста, наша задача состоит из двух частей:

- подать достаточный трафик, чтобы нагрузить устройство;
- настроить устройство так, как оно будет использовано в реальной сети.

Существуют два подхода к получению тестового трафика:

1) использовать трафик из своей сети;
2) создавать генератором трафика.

Во-первых, NGFW можно подключить к SPAN порту имеющегося в сети оборудования, чтобы подать собственный трафик. SPAN позволяет забрать копию трафика с любого коммутатора сети и отправить на тестируемый NGFW.

Во-вторых, удачным решением будет использование устройств класса Network TAP, например Gigamon (https://www.gigamon.com/). Такие устройства позволяют забрать из сети и направить одинаковые копии трафика на разные NGFW одновременно, что позволяет тестировать несколько производителей и сравнивать результаты на одинаковом трафике: загрузку процессоров, памяти, обнаруженные приложения, файлы, вирусы, zero-day, бот-сети и т.д. Копия трафика не позволяет реализовать функции блокирования трафика и функцию SSL Decryption, но позволяет оценить загрузку устройства на реальном трафике.

В-третьих, есть возможность репликации трафика компании специальным программным обеспечением. Можно записать трафик компании

в моменты пиковой загрузки в виде PCAP файлов и проигрывать трафик различными утилитами, например, tcpreplay.

Есть смысл тестировать устройство на трафике из нескольких сетей компании одновременно или по очереди: периметр, ЦОД, виртуализация, контейнеризация. Хороший тестовый трафик содержит:

- атаки, которые должен ловить IPS;
- вирусы, которые должен ловить антивирус;
- приложения, которые должен обнаружить модуль анализа приложений.

Сложными приложениям для анализа являются TOR, Телеграмм, Skype и др. Также стоит пустить стандартные приложения по нестандартным портам. Повесьте RDP на порт, отличный от 3389, запустите FTP сервер на порту 25 вместо 21 и др. Протоколами для отправки вирусов и проверки работы антивируса могу быть не только HTTP, но и FTP, SMB, POP3, IMAP, их SSL версии и др. Также вы можете использовать различные утилиты для генерации атак во время теста, например Metasploit Framework.

Профессиональные лаборатории покупают специализированное оборудование компании IXIA (https://www.ixiacom.com/) для нагрузочного тестирования, поскольку на нем легко добиться повторяемости результатов на реальном трафике с нужной мощностью. Система может симулировать атаки и нелегитимные активности, а также ошибочный трафик с целью проверки эффективности работы устройств сетевой зашиты под нагрузкой - аналогично тому как это происходит в реальной жизни, но в полностью контролируемой среде лаборатории. Это позволяет максимально быстро проанализировать причинно-следственную связь различных факторов и особенностей работы конкретного производителя, модели устройства, версии программного обеспечения, архитектуры и самое главное - конкретного профиля настроек.

Итак, способ получения тестового трафика мы выбрали. Теперь на тестовом устройстве нужно включить нужный режим и нужные функции — это нагрузит тестируемый NGFW:

- анализ приложений, включая приложения на нестандартных портах и др.;
- анализ параметров приложений: URL-категорий, имен и расширений передаваемых файлов и др.;
- SSL Decryption с анализом сертификатов и приложений и распознаванием атак внутри расшифрованного трафика;
- журналирование каждого приложения и его параметров, сопоставление имени сотрудника и каждого IP-адреса, имен файлов в протоколах, найденных вирусов, zero-day, атак и других функций, которые вы будете использовать для своей защиты.

Самые запутанные настройки режимов инспекции трафика в NGFW. Во-первых, у каждого производителя есть разные варианты подключения к сети: в режиме маршрутизации, в режиме свитча, в прозрачном режиме, в режиме прокси-сервера и др. Во-вторых, есть разные варианты функционирования операционной системы, антивируса и IPS — они значительно влияют на производительность. Обычно производитель сам настраивает свои устройства и знает, какой режим включить. Мы всегда должны подробно узнавать обо всех вариантах работы: чем они отличаются?

Если мы пригласили на тест двух производителей для сравнения, это будет прекрасно. Их можно попросить проверить настройки друг друга и получить подтверждение, что установленные операционные системы актуальны, их включенные режимы равносильны (чтобы не было, что у одного производителя включено 40% сигнатур, а у другого — 100%), чтобы у обоих одновременно были включены одинаковые функции определения

приложений, обнаружения атак и журналирования. Тогда тест будет правильным и равноценным.

Теперь можно запускать тест и выбирать нужную модель.

Ссылки на источники

1. Отчет NSS Labs NGFW за 2018 год; https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/nss-labs-2018-ngfw-comparative-report-performance.pdf
2. Выступление компании IXIA на конференции bi.zone; https://youtu.be/GibRXgWbaR8

Январь 2020