ИНСТРУМЕНТЫ НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ В РОССИЙСКИХ ОС

Шевченко Дмитрий Александрович

студент, Российский государственный университет нефти и газа имени И. М. Губкина, РФ, г. Москва

Боготов Ислам Сергеевич

студент, Российский государственный университет нефти и газа имени И. М. Губкина, РФ, г. Москва

Уймин Антон Григорьевич

научный руководитель, Российский государственный университет нефти и газа имени И. М. Губкина, РФ, г. Москва

В современных условиях информационной безопасности основой технологического суверенитета выступает стабильная и эффективная работа сетевых систем, особенно это касается критически важных отраслей государства.

К одному из основных процессов, что обеспечивал бы надежное функционирование сетевой инфраструктуры и устойчивости к компьютерным атакам можно отнести нагрузочное тестирование сетевого стека. Проверка производительности и стабильности сетевого стека является критической необходимостью в связи с ростом числа кибератак и повышения санкционного давления.

Цель данной статьи заключается в рассмотрении некоторых инструментов, что применяются при нагрузочном тестировании сетевого стека в отечественных современных операционных системах, анализе их функциональных задач.

К основным задачам нагрузочного тестировании можно отнести:

- *Проверка пропускной способности (заключается в проверке скорости передачи данных по TCP и UDP);*
- *Тестирование устойчивости системы под некоторой нагрузкой (направлено на выявление слабых мест сетевого стека в системе при высокой нагрузке);*
- *Анализ задержек и потери пакетов (важно для измерения отклика времени и надежности передачи данных)*

По ходу работы будут изучены различные инструменты, обеспечивающие помощь специалистам при составлении оценки производительности и устойчивости сетевых компонентов системы, выявлении потенциальных уязвимостей и повышении эффективности сетевой инфраструктуры.

Как уже говорилось ранее, данная статься особенно актуальна в наше время, особенно полезна она будет различным специалистам информационной безопасности – системным администраторам и разработчикам, тесно работающим с отечественными решениями на рынке ПО.

Шевченко Д.А., Боготов И.С. ИНСТРУМЕНТЫ НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ В РОССИЙСКИХ ОС // Студенческий форум: электрон. научн. журн. 2024. № 42(309). URL: https://nauchforum.ru/journal/stud/309/157232 (дата обращения: 04.09.2025).

РАССМАТРИВАЕМЫЕ ОТЕЧЕСТВЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

На рынке ПО в России представлены различных отечественные решения, ориентированные на различные сферы, начиная от личного пользования и заканчивая государственным и корпоративным сектором.

В ходе данной работы были рассмотрены 4 отечественные операционные системы: ОС Альт, Astra Linux (Орел) и РЕД ОС, Роса Linux.

ОС Альт представляет из себя один из старейших российских дистрибутивов Linux, что поддерживается компанией «Базальт СПО».

Выпускается в различных версиях: для образовательных учреждений, корпоративного сектора, государственных структур.

Данный дистрибутив имеет сертификацию и активно используется при обучении в образовательных учреждениях.

РЕД ОС тоже представляет из себя один из дистрибутивов Linux, который был разработан компанией «Ред Софт». Активно используется как в коммерческих, так и государственных корпорациях. Имеет сертификацию ФСТЭК.

Astra Linux – одна из известных российских ОС, также основана на Linux. Активно используется в государственных учреждениях, особенно в силовых структурах. Такая система обладает своими механизмами защиты информации, обладает сертификацией ФСТЭК и Министерства обороны РФ. Если говорить о выпускаемых версиях, то они бывают различного уровня секретности и применения, начиная от базовых решений для коммерческих компаний и заканчивая такими версиями как «Орел» и «Смоленск».

Rosa Linux - линейка дистрибутивов Linux (изначально основанных на Mandriva), разработку которых ведёт российская компания «НТЦ ИТ РОСА». В линейку включены серверная версия ROSA Server и настольная версия ROSA Desktop. Для каждой из версий доступны свободно распространяемые редакции, а также построенные на их основе защищённые варианты, сертифицированные ФСТЭК России и российским Министерством обороны

Системные требования ОС и фактическая конфигурация:

Таблица 1.

Системные требования ОС и фактическая конфигурация

	Системные требования	**Фактическая конфигур**
ОС Альт (Рабочая станция версия 10.4)	Оперативная память: от 512 МБ Жёсткий диск: от 16 ГБ	Оперативная память: 1 ГБ Жёсткий диск: 25 ГБ
Astra Linux (Орел версия 2.12)	Оперативная память: от 1 ГБ Жёсткий диск: не менее 5 ГБ	Оперативная память: 1.5 Жёсткий диск: 20 ГБ
РедОС (Рабочая станция версия 7.3)	Оперативная память: от 2 ГБ Жёсткий диск: от 20 ГБ	Оперативная память: 2 ГБ Жёсткий диск: 25 ГБ
Rosa Linux (Хром 12.4)	Оперативная память: от 1.5 ГБ Жёсткий диск: от 20 ГБ	Оперативная память: от 2 Жёсткий диск: 25ГБ

КРАТКИЙ ОБЗОР НЕКОТОРЫХ ПОПУЛЯРНЫХ ИНСТРУМЕНТОВ НАГРУЗОЧНОГО ТЕСТИРОВАНИЯ СЕТЕВОГО СТЕКА

Как и в любых система Linux, в российских дистрибутивах можно использовать разные инструменты для нагрузочного тестирования сетевого стека. Ниже представлены наиболее популярные инструменты:

Iperf/Iperf3

Данный инструмент часто применяется для тестирования пропускной способности сети, поддерживает тестирование на уровнях TCP и UDP, позволяя определить скорость передачи информации между 2 узлами.

Netperf

Представляет из себя утилиту командной строки, позволяющей генерировать TCP, UDP, ICMP-пакеты для тестирования безопасности, пропускной способности сети, а также её устойчивости к сетевым атакам.

Speedtest-cli

Инструмент командной строки для измерения скорости интернет-соединения. Использует серверы Speedtest.net, что позволяют тестировать пропускную способность сети, включая скорость загрузки, выгрузки и пинг. Особенно полезен при формировании оценки качества интернет-соединения, проверки стабильности и диагностики при проблемах сети.

Tcpdump

Представляет из себя утилиту командной строки для захвата сетевого трафика и дальнейшего его анализа. Распространен при диагностике сети, мониторинге работы, изучении протоколов и проверки безопасности сети. Умеет фильтровать пакеты данных по адресам, портам и другим параметрам.

Приведем наглядную таблицу первых трех утилит:

Таблица 2.

Наглядная таблица первых трех утилит

Инструмент	**Что тестирует**	**Соответствие задача**
Iperf3 Версия 3.17.1	Пропускная способность, задержка	Высокое: подходит для тестировани способности, стабильности соед производительности сете
Hping3 Версия(3.a2.ds2-10.1)	Задержка, потери пакетов, нагрузка	Высокое: позволяет создавать касто тестировать NAT/файрволы, сетевые

Speedtest-cli Версия 2.1.3-2	Пропускная способность (скорость загрузки и выгрузки)	Среднее: удобно для тестиро пользовательской пропускной спо Интернет-сетях

Наличие утилит в российских дистрибутивах:

Таблица 3.

Наличие утилит в российских дистрибутивах

	iperf	**Hping3**	**Speedte**
Альт ОС	+	+	+
Astra Linux	+	+	+
Ред ОС	+	+	-
Роса Linux	+	+	-

ИСПОЛЬЗОВАНИЕ ДАННЫХ ИНСТУРМЕНТОВ НА ПРИМЕРЕ ALT LINUX

Iperf

Создадим сеть 10.10.10.0, где 10.10.10.1 – server_alt, 10.10.10.2 – client_alt.

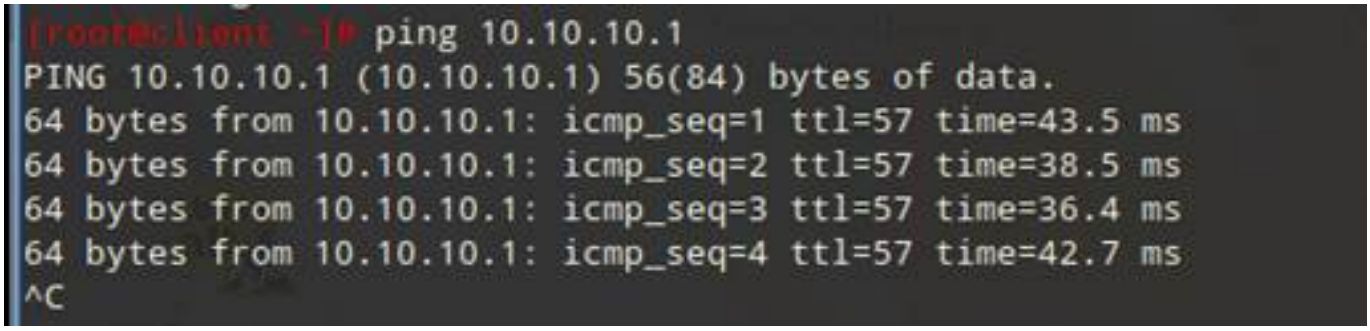

Рисунок 1. Проверка соединения между сервером и клиентом

Установим утилиту iperf3 на обе машины используя директорию apt.

apt-get install iperf3

Введем команды:

iperf3 -s (на server_alt)

iperf3 -c 10.10.10.1 (на client_alt)

Результат:

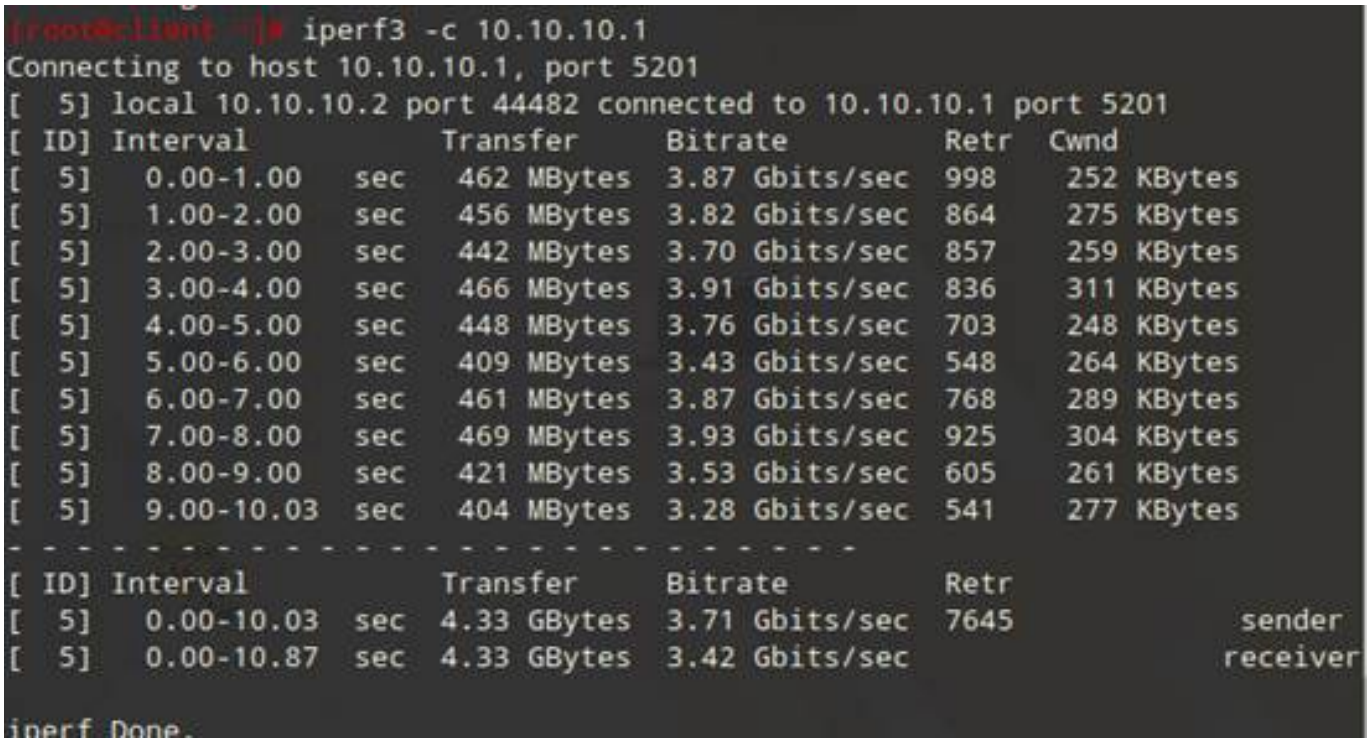

Рисунок 2. Результат выполнения работы Iperf3

Интерпретация результата по столбцам вывода:

1. **[ID]**
   - Номер потока (потоков) TCP или UDP, которые используются для передачи данных.
   - Обычно указывается [5], так как тест запускается в одном потоке, но можно настроить несколько потоков с помощью флага -P.
2. **Interval**
   - Временной интервал тестирования (в секундах).
   - Показывает начало и конец интервала (например, 0.00-1.00 означает первый промежуток времени от 0 до 1 секунды).
   - В конце выводится сводка за всё время теста, например, 0.00-10.87.
3. **Transfer**
   - Указывает общее количество данных, что было отправлено за указанный временной интервал.
   - Размеры данных указываются в MBytes или GBytes.
4. **Bitrate**
   - Средняя скорость передачи данных в указанный временной интервал.
   - Измеряется в битах в секунду (например, Gbits/sec для гигабитов в секунду).
   - Ключевая метрика для оценки пропускной способности сети.
5. **Retr (Retransmissions)**
   - Количество повторных отправок TCP-пакетов в данном временном интервале.
   - Высокие значения указывают на сетевые проблемы (потери пакетов, перегрузка, плохое соединение).
   - Применяется только для TCP.
6. **Cwnd (Congestion Window)**
   - Размер окна перегрузки TCP (указывается в KBytes).
   - Это динамический параметр, который показывает, сколько данных отправитель может передать до получения подтверждения от получателя.

    - Увеличивается при стабильной передаче и уменьшается при потере пакетов.
    - Более высокие значения Cwnd указывают на хорошую пропускную способность сети.

Hping

Вводим команду hping3 --rand-source -c 10 -p 445 10.10.10.1

--rand-source:

- Генерирует случайный IP-адрес источника для каждого отправленного пакета.
- Используется для проверки сетевых фильтров или брандмауэров, а также для симуляции атаки, где пакеты поступают с множества "поддельных" источников.

-c 10:

- Указывает количество отправляемых пакетов (в данном случае 10).

-p 445:

- Указывает целевой порт на сервере (445 — стандартно используется для SMB, общих файловых ресурсов Windows).

10.10.10.1:

- Целевой IP-адрес, на который будут отправляться пакеты.

С помощью утилиты tcpdump удостоверимся в отправке файлов на сервер (выводимые результаты рассмотрим в следующем пункте):

```
[root@server ~]# tcpdump -i enp0s8 port 445
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:46:08.746806 IP 93.248.251.118.1668 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:09.830397 IP 96-93-99-74-static.hfc.comcastbusiness.net.1669 > server.microsoft-ds: Flags [n
one], win 512, length 0
19:46:10.913984 IP mobile-107-251-236-176.mycingular.net.1670 > server.microsoft-ds: Flags [none],
 win 512, length 0
19:46:11.997835 IP 107.17.0.219.1671 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:13.081527 IP 92.222.116.72.1672 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:14.165497 IP 38.250.28.91.1673 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:15.249635 IP 225.226.168.47.1674 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:16.333719 IP 246.9.100.204.1675 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:17.417712 IP 204.174.246.91.1676 > server.microsoft-ds: Flags [none], win 512, length 0
19:46:18.501262 IP 199.110.95.176.1677 > server.microsoft-ds: Flags [none], win 512, length 0
```

Рисунок 3. Результат работы Hping

Как можно увидеть, сервер успешно получил 10 пакетов.

Tcpdump

В данном пункте подробно интерпретируем результаты работы данной утилиты.

Отметим, что каждая строка имеет следующую структуру:

<Время> IP <Источник>.<Порт> > <Назначение>.<Порт>: Flags <Флаги>, win <Окно>,

length <Длина>, где:

<Время>

- Метка времени получения пакета (с точностью до микросекунд).

IP

- Указание того, что захваченный пакет – это IP.

<Источник><Порт>

- Указывает адрес и порт отправителя пакета (например, 107.17.0.219.1671).

<Назначение><Порт>

- Указывает адрес и порт получателя пакета (в нашем случае – server.microsoft-ds)

Flags<Флаги>

- Указаны флаги заголовка TCP, что указывают на тип пакета или состояние соединения (на рисунке все пакеты не имеют специальных флагов).

win <Окно>

- Указан размер окна TCP, что показывает количество байтов, которые отправитель готов принять

length <Длина>

- Указан размер полезной нагрузки пакета в байтах (в нашем примере длина 0, а это говорит об отсутствии данных в захваченных пакетах).

В ходе анализа вывода, представленного выполнением работы утилиты tcpdump, получаем следующие выводы:

1. Имеются разные источники трафика (каждая строка имеет уникальный IP-адрес отправителя (--rand-source), как и ожидалось, это в свою очередь подтверждает спуфинг источников пакетов);
2. Данные в наших пакетах отсутствуют (на это указывает длина полезной нагрузки, равная 0, т.е. пакеты «пустые»);
3. Задано стандартное окно для пустых пакетов TCP;
4. У всех пакетов отсутствуют специальные флаги (нет специальных запросов или состояния).

Speedtest-cli

Установка утилиты происходит следующим образом:

pip3 install speedtest-cli

Т.к. утилита написана на python, то для ее работы установим python3 и pip (Python Package Installer):

apt-get install python3

curl -O https://bootstrap.pypa.io/get-pip.py

Результат работы после выполнения команды speedtest-cli:

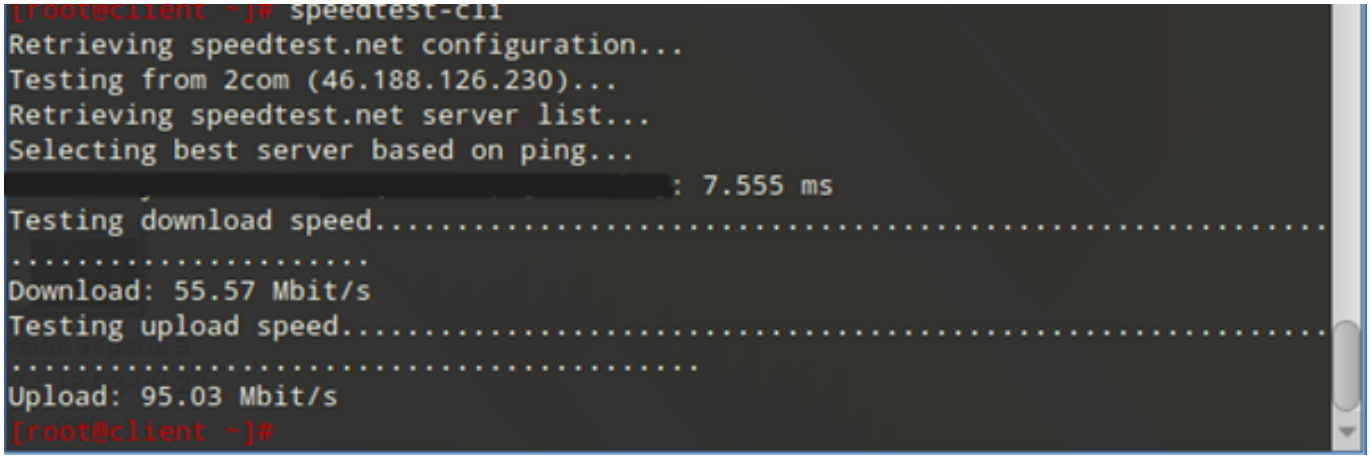

Рисунок 4. Результат выполнения Speedtest-cli

Как мы видим, представлена информация о характеристиках интернет-соединения (пинг, скорость загрузки и выгрузки данных).

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Процесс установки и вывод результатов работы инструментов нагрузочного тестирования в отечественных операционных системах схож, поэтому ниже приведем только сравнительную таблицу с основными результатами работы указанных инструментов:

Сравнительная таблица результатов работы инструментов нагрузочного тестирования сетевого стека в различных отечественных операционных системах

Таблица 4.

Сравнительная таблица результатов работы инструментов нагрузочного тестирования сетевого стека в различных отечественных операционных системах

	ОС Альт	**Astra Linux (Орел)**	**РЕД ОС**	
Iperf	Отправитель: 3.71 Гб/сек Получатель: 3.42 Гб/сек	Отправитель: 3.65 Гб/сек Получатель: 3.38 Гб/сек	Отправитель: 3.68 Гб/сек Получатель: 3.40 Гб/сек	Отправ Получа
Hping3	Все файлы отправлены/получены	Все файлы отправлены/получены	Все файлы отправлены/получены	отпра
speedtest-cli	Скачивание: 55.57 Мб/сек Отправка: 95.03 Мб/сек	Скачивание: 52.89 Мб/сек Отправка: 92.47 Мб/сек	Не поддерживается	Не п

ЗАКЛЮЧЕНИЕ

Работе сетевых систем всегда уделялось огромное внимание, но в наше время от их корректной, производительной и надежной работы зависит технологический суверенитет страны, особенно это актуально для критически важных сфер деятельности нашего государства.

В условиях мощного давления со стороны стран коллективного Запада поддержка работы сетевых систем на должном уровне выступает крайней необходимостью.

Решение данной задачи обеспечивается различными формами тестирования сетевого стека используемых систем.

Тестирование позволяет определить потенциал выстроенных сетевых систем с точки зрения безопасности, надежности и производительности.

В ходе данного исследования были рассмотрены популярные инструменты нагрузочного тестирования сетевого стека на базе отечественных решений в области операционных систем.

Мы рассмотрели цели применения различных инструментов, особенности их применения в нескольких операционных системах и проинтерпретировали результаты, что выводятся указанными утилитами.

По ходу данной работы были сделано следующее:

- Проведена проверка пропускной способности на уровне TCP;
- Протестирована устойчивость системы при некоторой нагрузке;
- Сделан анализ по задержке и потере пакетов данных;
- Проведен анализ скорости загрузки, выгрузки данных и определен пинг в сети.

Список литературы:

1. Обзор инструментария для нагрузочного и перформанс-тестирования // Хабр URL: https://habr.com/ru/companies/jugru/articles/337928/ (дата обращения: 20.11.2024).

2. Использование Hping3 в пентесте как альтернатива ping // spy-soft.net URL: https://spy-soft.net/hping3-kali-linux/?ysclid=m2qrfqa49v339667535 (дата обращения: 21.11.2024).

3. Нагрузочное тестирование сети - Справочный центр - Справочный центр Astra Linux // Справочный центр Astra Linux URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=16810141 (дата обращения: 20.11.2024).

4. Уймин, А. Г. Классификация корпоративного трафика с использованием алгоритмов машинного обучения / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2023. – № 7(600). – С. 22-29. – DOI 10.33285/2782-604X-2023-7(600)-22-29. – EDN WXXUPK.

5. Нагрузочное тестирование сети - Справочный центр - Справочный центр Astra Linux // Drach.pro URL: https://drach.pro/blog/linux/item/218-iperf-testing?ysclid=m2qr4lo7vj681819653 (дата обращения: 20.11.2024).