ГРУППА КОМПАНИЙ | СПБ

Фортикс

Методика нагрузочного тестирования программно-аппаратного комплекса «Фортикс»

версия 1.0

Москва 2026 г.

Оглавление

ОБЩИЕ СВЕДЕНИЯ О ПРОДУКТЕ 3
1. Цели и задачи 4
1.1. Цель тестирования 4
1.2. Программа тестирования 4
2. Оборудование для тестирования 5
3. Схемы стендов и конфигурации устройств 6
3.1. Сетевые топологии и план IP-адресации 6
3.2. Конфигурация устройств 8
3.3. Конфигурация генераторов трафика 10
4. Нагрузочное тестирование 11
4.1 Тестирование в режиме маршрутизации 11
4.2. Нагрузочное тестирование в режиме СКЗИ 12
4.3. Нагрузочное тестирование в режиме МЭ + Контроль приложений (DPI) 12
4.4. Нагрузочное тестирование в режиме СКЗИ+ МЭ + Контроль приложений (стресс-тест) 13
Приложение №1 14
Приложение №2 16
Приложение №3 18
Приложение №4 21
Приложение №5 22

ОБЩИЕ СВЕДЕНИЯ О ПРОДУКТЕ

ПАК «Фортикс» предоставляет функциональные возможности маршрутизатора, СКЗИ, средства межсетевого экранирования и отказоустойчивого кластера, реализованные в программном обеспечении (далее по тексту – ПО) ПАК «Фортикс».

Подробное описание функциональных возможностей ПАК «Фортикс», модельный ряд и документация на изделие представлены на сайте ООО «Защищенные телекоммуникационные системы» и доступны по адресу: https://zts.ru/products/fortics/.

1. Цели и задачи

1.1. Цель тестирования

Определение производительности модельного ряда ПАК «Фортикс» в смоделированных лабораторных в условиях приближенных реальным, для оценки возможности применения ПАК «Фортикс» в средних и крупных компаниях, центрах обработки данных в качестве оборудования для маршрутизации IP-пакетов, средства криптографической защиты информации и межсетевого экрана.

В процессе тестирования ПАК «Фортикс» моделируются различные сценарии использования оборудования:

- работа устройств режиме СКЗИ или МЭ с разным количеством IP-туннелей или правил фильтрации.
- работа в нескольких режимах одновременно («стресс тест») с большим количеством IP-туннелей, правил МЭ, включенными опциями журналирования IP-пакетов и контролем приложений (DPI).

Для имитации реальной активности работы систем и приложений, используемых в корпоративных сетях, применяется подготовленный профиль EMIX-трафика. Профиль EMIX-трафика представлен в приложении 5.

1.2. Программа тестирования

Перечень тестов для тестирования приведен в таблице 1.

Таблица 1. Программа тестирования

№ п/п	Режим работы	Тесты	Описание теста
1.	**Маршрутизация**	Max HTTP concurrent connection (CC)	Определение максимального количества поддерживаемых TCP-сессий в режиме маршрутизации
		Max HTTP connection peer second (CPS)	Определение максимального количества новых TCP-сессий в режиме маршрутизации
2.	**СКЗИ**	EMIX – трафик 1 туннель	Определение максимальной пропускной способности в режиме туннелирования
		EMIX – трафик 100 туннелей	Определение максимальной пропускной способности в режиме туннелирования
3.	**МЭ + Контроль приложений (DPI)**	- EMIX-трафик	Определение максимальной производительности в режиме МЭ
		- HTTP CPS	
		- HTTP CC	
		- HTTP транзакции переменной длины (1 kb, 64kb)	
4.	**СКЗИ +МЭ + Контроль приложений (стресс-тест)**	EMIX - трафик 100 туннелей	Определение максимальной производительности в режиме туннелирования и межсетевого экранирования

2. Оборудование для тестирования

Нагрузочное тестирование проводится с применением специализированных программных генераторов трафика Trex, развернутых в среде виртуализации Proxmox. Для автоматизации процесса тестирования на Trex используется набор скриптов от Олега Каштанова. Ссылка на Github: https://github.com/OlegKashtanov/ngfw trex perf.

На программном генераторе Trex генерируется и отравляется на объект тестирования сформированный профиль EMIX-трафика, запускаются автоматизированные тесты для измерения показателей пропускной способности, потери соединений, максимального значения новых TCP-соединений (CPS), максимального значения поддерживаемых (конкурентных) TCP-соединений (CC).

Характеристики аппаратной платформы для виртуализации и используемое ПО приведены в таблице 2.

Таблица 2. Используемые аппаратные средства и ПО

Тип	Характеристики
Аппаратная платформа тип 1	128 Гбайт ОЗУ 2 x Intel(R) Xeon(R) Gold 6134 @ 3.20GHz Количество ядер/потоков 8/16 2 x Intel X710 (2 интерфейса) Proxmox VE 9.0.3
Аппаратная платформа тип 2	64 Гбайт ОЗУ Intel(R) Core(R) I9 13900H @ 3.20GHz Количество ядер/потоков 14/20 Intel X710 (2 интерфейса) Intel E810 (2 интерфейса) Proxmox VE 9.0.3
Виртуальная машина (ВМ) Trex №1	ОЗУ: 45 GB vCores: 16 Сетевая карта: PCI Passthrough X710_0 PCI Passthrough X710_1
ВМ Trex №2, №3	ОЗУ: 45 GB vCores: 6 Сетевая карта: PCI Passthrough X710_0 PCI Passthrough X710_1
ПО ВМ Trex	ОС Linux Debian 13 Trex 3.02
ПО ВМ Grafana	ОС Linux Debian 13 Grafana 12.3.1, InfluxDB 1.6.7

Для графического представления результатов, полученных на генераторе трафика Trex, используется средство визуализации Grafana с дашбордом Trex. Дашборд доступен по ссылке: https://grafana.com/grafana/dashboards/22 905-cisco-trex/.

3. Схемы стендов и конфигурации устройств

3.1. Сетевые топологии и план IP-адресации

Принципиальная схема для проведения нагрузочного тестирования ПАК «Фортикс» режимах маршрутизации и МЭ на генераторе трафика TRex представлена на рисунке 1.

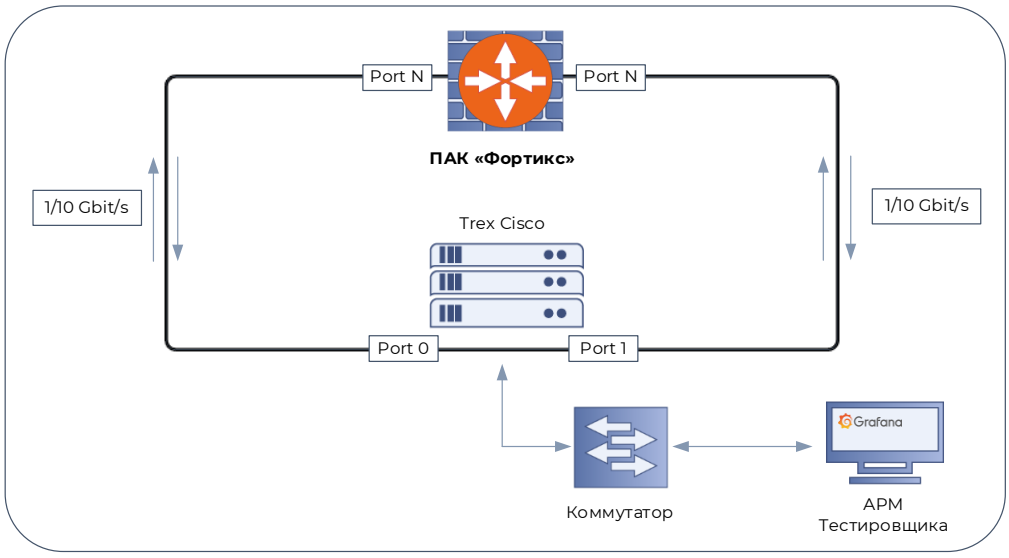


Рисунок 1. Схема для проведения нагрузочного тестирования ПАК «Фортикс» в режимах маршрутизации и МЭ на генераторе трафика TRex

Принципиальная схема для проведения нагрузочного тестирования ПАК «Фортикс» режиме СКЗИ на генераторе трафика TRex представлена на рисунке 2.

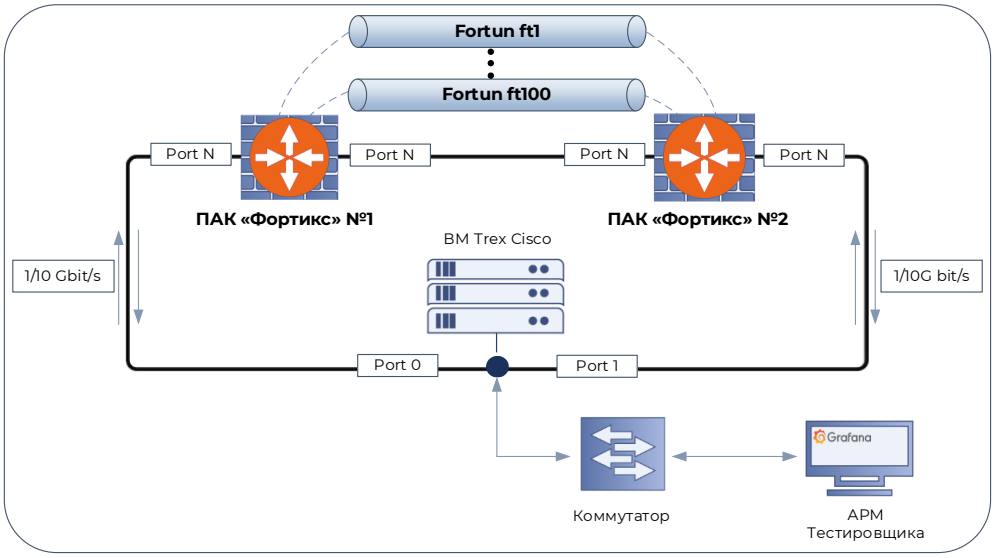


Рисунок 2. Схема для проведения нагрузочного тестирования ПАК «Фортикс» в режиме СКЗИ на генераторе трафика TRex

Принципиальная схема для проведения нагрузочного тестирования старших моделей ПАК «Фортикс» режиме маршрутизации и МЭ на двух генераторах трафика TRex представлена на рисунке 3.

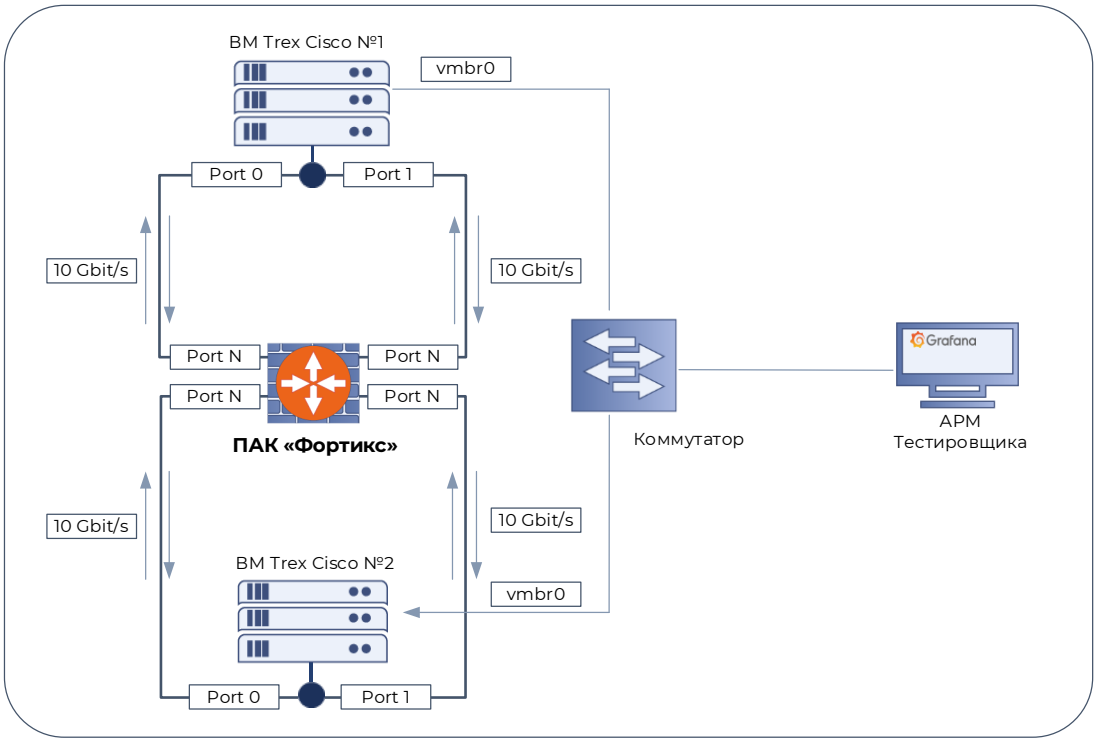


Рисунок 3. Схема для проведения нагрузочного тестирования старших моделей ПАК «Фортикс» в режиме маршрутизации и МЭ на двух генераторах трафика TRex

План IP-адресации представлен в таблице 3.

Таблица 3. План IP-адресации

№ п/п	Адресация	Назначение
1	16.0.0.1-16.0.255.249	Адреса, используемые генератором трафика в качестве клиентов в ВМ Trex №1
2	48.0.0.1-48.1.255.199	Адреса, используемые генератором трафика в качестве серверов в ВМ Trex №1
3	17.0.0.1-17.0.255.249	Адреса, используемые генератором трафика в качестве клиентов в ВМ Trex №2
4	49.0.0.1-49.1.255.199	Адреса, используемые генератором трафика в качестве серверов в ВМ Trex №2
5	192.168.1.1/24	IP-адрес сервера виртуализации Proxmox №1
6	192.168.1.2/24	IP-адрес сервера виртуализации Proxmox №2
7	99.99.99.1/24	IP-адрес первого интерфейса ВМ Trex №1
8	99.99.99.254/24	IP-адрес шлюза по умолчанию для первого интерфейса ВМ Trex №1
9	98.98.98.1/24	IP-адрес первого интерфейса ВМ Trex №2

№ п/п	Адресация	Назначение
10	98.98.98.254/24	IP-адрес шлюза по умолчанию первого интерфейса ВМ Trex №2
11	100.100.100.1/24	IP-адрес второго интерфейса ВМ Trex №1
12	100.100.100.254/24	IP-адрес шлюза по умолчанию второго интерфейса ВМ Trex №1
13	101.101.101.1/24	IP-адрес второго интерфейса ВМ Trex №2
14	101.101.101.254/24	IP-адрес шлюза по умолчанию второго интерфейса ВМ Trex №2
15	192.168.1.22/24	IP-адрес ВМ Trex №1
16	192.168.1.23/24	IP-адрес ВМ Trex №1
17	192.168.1.8/24	IP-адрес АРМ Тестировщика
18	192.168.1.28/24	IP-адрес ВМ Grafana

3.2. Конфигурация устройств

3.2.1. Конфигурация устройств ПАК «Фортикс» для оценки производительности в режиме маршрутизации

Для оценки производительности ПАК «Фортикс» в режиме маршрутизации на каждом из устройств ПАК «Фортикс» предварительно проводятся следующие настройки:

- настраивается IP-адресация на требуемом количестве интерфейсов;
- включается пересылка IP-пакетов (IP forwarding) между интерфейсами;
- устанавливается значение таймера tcp-fin-wait – 30 сек;
- устанавливается максимальный размер очереди сетевого интерфейса max-backlog – 65535;

Максимальное количество записей conntrack для старших моделей с ОЗУ 32 Гбайт – 70 000 000 записей. Для средних и младших моделей с ОЗУ 16 Гбайт – 30 000 000.

Пример конфигурации в режиме маршрутизации для работы с двумя генераторами трафика TRex представлен в приложении №2.

3.2.2. Конфигурация устройств ПАК «Фортикс» для оценки производительности в режиме СКЗИ

Для оценки производительности СКЗИ на паре устройств ПАК «Фортикс» предварительно проводятся следующие настройки:

- генерируются и сохраняются в постоянной памяти ключи доступа (КД);
- на одном из устройств генерируется матрица симметричных ключей;
- ключ шифрования матрицы и матрица сохраняются на USB-накопитель;
- ключевые строки матрицы экспортируются на USB-накопитель;
- ключевые строки с USB-накопителей импортируются на два устройства;
- на каждом устройстве создаются туннельные L3 интерфейсы fortun;
- на каждом устройстве добавляется статические маршруты до конечных адресов через туннельные интерфейсы fortun tun1 – tun N;
- увеличиваются MTU на интерфейсах fortun 1500 байт и ethernet 1600 байт соответственно.

Максимальное количество настраиваемых VPN-туннелей fortun:
- 100 туннелей для моделей 7314R, 6216R, 3308R;
- 30 туннелей для модели 2304R(RM2).

Для моделей 6216R и 7314R при работе с одним интерфейсом fortun дополнительно настраиваются следующие параметры:
- smp-affinity – балансировка шифрования по ядрам процессора. Значения **0-11** для модели 7314R, **0-8** для модели 6216R;
- rps – распределение по ядрам процессора на приеме. Значения **23-47** для модели 7314R,
8-15 для модели 6216R;

Пример конфигурации с настройкой VPN-туннелей fortun и статической маршрутизацией представлен в приложении 3.

3.2.3. Конфигурация устройств ПАК «Фортикс» для оценки производительности в режиме МЭ + Контроль приложений (DPI)

Для оценки производительности в режиме межсетевого экрана настраивается отдельный фильтр в цепочке **forward**, содержащий требуемое количество правил. Для обеспечения работы трассировщика соединений conntrack в фильтре настраиваются разрешающие правила с критериями отбора по состоянию соединения *established, related*. После создания фильтра он применяется в точке перехвата (hook) **after-zone.** Дополнительно производится конфигурация фильтра межсетевого экрана на требуемое количество правил с режимом инспектирования пакетов DPI (анализ IP-пакетов L7). Для всех правил фильтра кроме правила с именем «conntrack» включается журналирование. Для двух последних разрешающих правил журналируются только первые 100 байт IP-пакета – параметр snaplen 100.

Под критерии отбора DPI попадает трафик приложения Citrix, используемого в профиле EMIX.

Максимальное количество правил в фильтре определяется моделью устройства:
- Фортикс 3308R, Фортикс 6216R, Фортикс 7314R – 1000;
- Фортикс 2304R (RM2) – 250 правил L3, L4 без DPI.

Пример конфигурации фильтра на 1000 правил представлен в приложении №1.

3.2.4. Конфигурация устройств ПАК «Фортикс» для оценки производительности в режиме СКЗИ + МЭ + Контроль приложений (стресс-тест)

Для оценки производительности в режиме межсетевого экрана настраивается отдельный фильтр в цепочке **forward**, содержащий требуемое количество правил. Для обеспечения работы трассировщика соединений conntrack в фильтре настраиваются разрешающие правила с критериями отбора по состоянию соединения *established, related*. После создания фильтра он применяется в точке перехвата (hook) **after-zone.** Дополнительно производится конфигурация фильтра межсетевого экрана на требуемое количество правил с режимом глубокого инспектирования пакетов DPI (анализ IP-пакетов L7). Для всех правил фильтра кроме правила с именем «conntrack» включается журналирование. Для двух последних разрешающих правил журналируются только первые 100 байт IP-пакета – параметр snaplen 100.

Под критерии отбора DPI попадает трафик приложения Citrix, используемого в профиле EMIX.

Максимальное количество правил в фильтре зависит от модели устройства:

- Фортикс 3308R, Фортикс 6216R, Фортикс 7314R – 1000;
- Фортикс 2304R (RM2) – 250 правил L3, L4 без DPI.

Порядок настройки СКЗИ идентичен изложенному в п.3.2.2.

3.3. Конфигурация генераторов трафика

3.3.1. Конфигурация генераторов трафика Trex

Параметры конфигурационного файла trex_cfg.yaml для ВМ Trex №1 и ВМ Trex №2 приведены в приложении 4.

Команда для запуска сервиса Trex: *./t-rex-64 -c 14 -i --astf --tso-disable --lro-disable --iom 0 –queue-drop;*

Команда для запуска окна мониторинга Trex (консоли): *./trex-console -t* .

Размер страницы hugepages=2048.

3.3.2. Средства мониторинга ПАК «Фортикс»

Для оценки нагрузки на ПАК «Фортикс» используется встроенная служба мониторинга sysmon. Переключение между отображением текущей информации производится с помощью клавиши <Space>.

Sysmon используется как вспомогательный инструмент для мониторинга нагрузки в следующих тестах:

- HTTP CPS, HTTP CC – отслеживание доступного объема ОЗУ;
- EMIX – нагрузка на CPU в режиме СКЗИ;
- EMIX – запросы прерываний (IRQ) в нескольких одновременных режимах («стресс-тест»).

Для проверки состояния таблицы conntrack используется команда *show conntrack*. Для отображения общего количества записей в таблице conntrack используется команда *show conntrack | grep total:*.

4. Нагрузочное тестирование

4.1 Тестирование в режиме маршрутизации

4.1.2 HTTP CPS

Последовательность действий:

1. Собрать схему сети в соответствии с рисунком 3.
2. Запустить сервис Trex и открыть окно мониторинга. Дополнительно открыть службу sysmon на ПАК «Фортикс».
3. Запустить скрипт из каталога */opt/ngfw/trex_profiles/http_max_cps.py* с начальным целевым показателем 40000 соединений (параметр *-m*), временем выхода на целевой показатель 120 секунд (параметр ramp_up), длительность после достижения целевого показателя - 240 секунд (параметр -d).
4. В окне мониторинга консоли Trex зафиксировать текущее значение CPS (*total_cps:)*, отсутствие потери пакетов (*drop_rate:*) и отсутствия переполнения очереди tx (*queue_full:*). Убедиться что тест пройден – «result:»«Passed».
5. Увеличивать параметр -m до появления потери пакетов не более 0.1%. Зафиксировать полученный результат. В окне службы «sysmon» следить за свободным размером ОЗУ. При остатке размера ОЗУ менее 300 Мб остановить выполнение теста и уменьшить параметр -m.
6. Очистить таблицу conntrack выполнив команду *do clear conntrack*.
7. Повторно выполнить тест не менее трех раз. Убедиться в стабильности полученного значения.

4.1.3 HTTP CC

Последовательность действий:

1. Собрать схему сети в соответствии с рисунком 3 или 5 (в зависимости от модели аппаратной платформы).
2. Запустить сервисы Trex на двух и более ВМ (количество ВМ зависит от модели аппаратной платформы ПАК «Фортикс») и открыть окно мониторинга. Для моделей ПАК «Фортикс» 7314R и 6216R получение максимального целевого показателя HTTP CC возможно на трех ВМ с сервисами Trex.
3. Запустить скрипт из каталога */opt/ngfw/trex_profiles/max_cc.py* с показателем 32 000 новых соединений секунду (параметр -m), временем выхода на целевой показатель 100 секунд (параметр -d), поддержанием соединений после достижения целевого показателя 300 секунд (параметр --cc-dur), задержкой между HTTP-транзакциями (параметр delay) 26 секунд и количеством транзакций 15 (параметр flow_size). При использовании двух и более ВМ скрипты должны запускаться одновременно.
4. Увеличивать параметры *-d* и *delay* до появления потери пакетов не более 0.1%. В окне службы «sysmon» следить за свободным размером ОЗУ. При уменьшении в процессе тестирования объема ОЗУ менее 800 Мб остановить выполнение теста и уменьшить параметр -m. Зафиксировать полученный результат. Параметр delay рассчитывается по формуле: delay = (d + cc-dur) / flow_size.
5. В случае резкого увеличения значения счетчика *queue_full* принудительно остановить тестирование. При тестировании моделей

ПАК «Фортикс» с интерфейсами 1Гбит/с необходимо подключить дополнительный коммутатор и изменить схему подключения – BM Trex подключается к коммутатору на скорости 10Гбит/с, ПАК «Фортикс» на скорости 1 Гбит/с.

6. В окне мониторинга зафиксировать текущее значение установленных соединений, отсутствии потери пакетов (drop_rate:) и и отсутствия переполнения очереди *tx* (*queue_full:*). Убедиться, что тест пройден – «result:»«Passed».
7. Очистить таблицу conntrack выполнив команду *do clear conntrack*.
8. Повторно выполнить тест не менее трех раз. Убедиться в стабильности полученного значения.

4.2. Нагрузочное тестирование в режиме СКЗИ

4.2.1 EMIX 1 туннель

Последовательность действий:

1. Собрать схему сети в соответствии с рисунком 4.
2. Запустить сервис Trex и открыть окно мониторинга.
3. Запустить скрипт из каталога /opt/ngfw/trex_profiles/emix.py с начальным значением параметра -m 1.2, длительностью 120 секунд (параметр -d).
4. В окне мониторинга зафиксировать текущее значение пропускной способности «*total_rx:*» и отсутствие потери пакетов «*drop_rate:*». Убедиться что тест пройден – «result:»«Passed».
5. Увеличивать параметр -m до появления потери пакетов не более 0.1%. Зафиксировать полученный результат.
6. В окне службы «sysmon» дополнительно следить за загрузкой CPU. Загрузка на CPU по параметру SYS 99% на каждое ядро свидетельствует о достижении максимальной нагрузки на устройство.
7. Повторно выполнить тест не менее трех раз. Убедиться в стабильности полученного значения.

4.2.2 EMIX 100 туннелей

Последовательность действий идентична п. 4.2.1.

4.3. Нагрузочное тестирование в режиме МЭ + Контроль приложений (DPI)

4.3.1 EMIX-трафик

Последовательность действий идентична п. 4.2.1.

4.3.2 HTTP CPS

Последовательность действий идентична п. 4.1.2.

4.3.3 HTTP CC

Последовательность действий идентична п. 4.1.3.

4.3.4 HTTP транзакции 1kb.

Последовательность действий:

1. Собрать схему сети в соответствии с рисунком 3. Для старших моделей собрать схему сети в соответствии с рисунком 5.
2. Запустить сервисы Trex на двух и более ВМ (количество ВМ зависит от модели аппаратной платформы ПАК «Фортикс») и открыть окно мониторинга.
3. Запустить скрипты из каталогов */opt/ngfw/trex_profiles/tcp_http_16KB.py* с начальным значение множителя 5000 (параметр -m), длительностью 300 секунд (параметр -d), размер ответа от сервера 1kb (параметр response_size_kb), количеством HTTP-транзакций в сессии 20 (параметр flow_size).
4. В окне мониторинга зафиксировать текущее значение пропускной способности (total_rx:) и отсутствие (наличие) потери пакетов (drop_rate:). Убедиться что тест пройден – «result:»«Passed».
5. Увеличивать параметр -m до появления потери пакетов не более 0.1%. Зафиксировать полученный результат.
6. Повторно выполнить тест не менее трех раз. Убедиться в стабильности полученного значения.

4.3.5 HTTP транзакции 16kb

Последовательность действий:

1. Собрать схему сети в соответствии с рисунком 3. Для старших моделей собрать схему сети в соответствии с рисунком 5.
2. Запустить сервисы Trex на двух и более ВМ (количество ВМ зависит от модели аппаратной платформы ПАК «Фортикс») и открыть окно мониторинга.
3. Запустить скрипты из каталога */opt/ngfw/trex_profiles/tcp_http_16KB.py* с начальным значение множителя 300 (параметр -m), длительностью 300 секунд (параметр -d), количеством HTTP-транзакций в сессии 20 (параметр flow_size).
4. В окне мониторинга зафиксировать текущее значение пропускной способности «total_rx:» и отсутствие потери пакетов «drop_rate:». Убедиться что тест пройден – «result:»«Passed».
5. Увеличивать параметр -m до появления потери пакетов не более 0.1%. Зафиксировать полученный результат.
6. Повторно выполнить тест не менее трех раз. Убедиться в стабильности полученного значения.

4.4. Нагрузочное тестирование в режиме СКЗИ+ МЭ + Контроль приложений (стресс-тест)

4.4.1 EMIX-трафик

Последовательность действий идентична п. 4.2.1

Приложение №1

Конфигурация ПАК «Фортикс» в режиме межсетевого экрана

Листинг 1 – Структура фильтра на 1000 правил ПАК «Фортикс» в режиме МЭ и контроля приложений (DPI)

```
firewall ipv4 netfilter {
 application appaname1_APP protocol protocol_name
 . . .
 application appaname100_APP protocol protocol_name
 filter test {
 rule conntrack {
  state established
  state related
  accept
 }
 rule 1 {
  log prefix X
  ndpi proto appaname1_APP
  drop
 }
 . . .
 rule 50 {
  log prefix X
  ndpi proto appanameN_APP
  drop
 }
 rule 51 {
  log prefix X
  from address 1.1.1.1/32
  drop
 }
 . . .
 rule 500 {
  log prefix X
  from address n.n.n.n/32
  drop
 }
 rule 501 {
  log prefix X
  from address 192.0.2.120/32
  to-port udp X
  drop
 }
 . . .
 rule 950 {
  from address n.n.n.n/32
  to-port udp X
  drop
 }
 rule 951 {
 ndpi proto citrix_APP
 log prefix citrix snaplen 100
 accept
 }
 . . .

 rule 998 {
```

```
  ndpi proto citrix_APP
  log prefix citrix_APP snaplen 100
  accept
  }
  rule 999 {
  accept
  from {
     address 48.0.0.0/8
     address 49.0.0.0/8
   }
   to {
      address 17.0.0.0/8
      address 16.0.0.0/8
  }
   log prefix EMIX_ALLOW_NET_1 snaplen 100
  }
 rule 1000 {
   accept
   to {
      address 48.0.0.0/8
      address 49.0.0.0/8
  }
   from {
      address 17.0.0.0/8
      address 16.0.0.0/8
  }
   log prefix EMIX_ALLOW_NET_2 snaplen 100
  }
}
 forward after-zone filter test
}
```

Приложение №2

Конфигурация ПАК «Фортикс» в режиме маршрутизации

Листинг 1 – Пример конфигурации четырех интерфейсов ПАК «Фортикс» для работы с двумя генераторами трафика Trex

```
interface {
  ether enX {
    enable
    ipv4 {
      address 99.99.99.254/24
      neighbor 99.99.99.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
    }
  }
  ether enX {
    enable
    ipv4 {
      address 100.100.100.254/24
      neighbor 100.100.100.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
    }
  }
  ether enX {
    enable
    ipv4 {
      address 98.98.98.254/24
      neighbor 98.98.98.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
  }
  ether enX {
    enable
    ipv4 {
      address 101.101.101.254/24
      neighbor 101.101.101.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
  }
}
```

Листинг 2 – Пример настройки маршрутизации ПАК «Фортикс» для работы с двумя генераторами трафика Trex

```
router unicast ipv4 {
      to 16.0.0.0/8 via gw 99.99.99.1
      to 48.0.0.0/8 via gw 100.100.100.1
      to 17.0.0.0/8 via gw 98.98.98.1
      to 49.0.0.0/8 via gw 101.101.101.1
  }
}
```

Приложение №3

Конфигурация ПАК «Фортикс» в режиме СКЗИ

Листинг 1 – Пример конфигурации интерфейсов ПАК «Фортикс» для работы с двумя генераторами трафика Trex на 1 VPN-туннеле

```
interface ether enX {
    enable
    ipv4 {
      address 99.99.99.254/24
      neighbor 99.99.99.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
    }
  }
  ether enX {
    enable
    ipv4 {
      address 98.98.98.254/24
      neighbor 98.98.98.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
    }
  }
  ether enX {
    mtu 1600
    enable
    ipv4 {
      address 10.10.10.1/24
    }
    device ring {
        rx 4096
        tx 4096
      }
    }
}
  fortun ft1 {
      enable
      mtu 1500
      rps 8-15
      ipv4 {
        local 10.10.10.1
        remote 10.10.10.2
      }
      mode tun
      id 1
      keepalive
      forsec-key {
        serial XXXXXX
        local-cn 2
        remote-cn 1
      }
      encryption
      smp-affinity 0-7
    }
}
```

Листинг 2 – Пример настройки маршрутизации ПАК «Фортикс» для работы с двумя генераторами трафика Trex на 1 VPN-туннеле

```
router {
  unicast ipv4 {
     to 16.0.0.0/8 via gw 99.99.99.1
     to 48.0.0.0/8 via interface ft1
     to 17.0.0.0/8 via gw 98.98.98.1
     to 49.0.0.0/8 via interface ft1
  }
```

Листинг 3 - Пример конфигурации интерфейсов ПАК «Фортикс» для 100 VPN-туннелей

```
interface ether enX {
    enable
    ipv4 {
      address 99.99.99.254/24
      neighbor 99.99.99.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
    }
  }
  ether enX {
    enable
    ipv4 {
      address 98.98.98.254/24
      neighbor 98.98.98.1 mac XX:XX:XX:XX:XX:XX
    }
    device ring {
      rx 4096
      tx 4096
    }
  }
  ether enX {
    mtu 1600
    enable
    ipv4 {
      address 10.10.10.1/24
    }
    device ring {
       rx 4096
       tx 4096
     }
    }
  fortun ft1 {
     enable
     mtu 1500
     ipv4 {
       local 10.10.10.1
       remote 10.10.10.2
     }
     mode tun
     id 1
     keepalive
     forsec-key {
       serial XXXXXX
       local-cn 2
       remote-cn 1
     }
```

```
    encryption
  }
.
.
.
 fortun ft100 {
      enable
      mtu 1500
      ipv4 {
        local 10.10.10.1
        remote 10.10.10.2
      }
      mode tun
      id X
      encap {
        sport 604
        dport 604
      }
      keepalive
      forsec-key {
        serial XXXXXX
        local-cn 2
        remote-cn 1
      }
      encryption
    }
}
```

Листинг 4 - Пример настройки маршрутизации ПАК «Фортикс» для 100 туннелей

```
router unicast ipv4 {
 to 16.0.0.0/8 via gw 99.99.99.1
 to 17.0.0.0/8 via gw 98.98.98.1

 to 48.0.0.0/21 via interface ft1

 . . .
 to 48.1.52.0/22 via interface ft50

 . . .
 to 48.1.252.0/22 via interface ft100

 . . .
 to 49.0.0.0/21 via interface ft1

 . . .
 to 49.1.52.0/22 via interface ft50

 . . .
 to 49.1.252.0/22 via interface ft100
}
```

Приложение №4

Конфигурационные файлы trex_cfg.yaml для генераторов трафика TRex №1 и TRex №2

Листинг №1 – Конфигурация генератора трафика TRex №1

```
- version: 2
  interfaces: ['00:10.0', '00:10.1']
  port_info:
      - ip: 99.99.99.1
        default_gw: 99.99.99.254
      - ip: 100.100.100.1
        default_gw: 100.100.100.254

  platform:
      master_thread_id: 0
      latency_thread_id: 1
      dual_if:
        - socket: 0
          threads: [2,3,4,5,6,7,8,9,10,11,12,13,14,15]

  memory:
      dp_flows: 40000000
```

Листинг №2 – Конфигурация генератора трафика TRex №2

```
- version: 2
  interfaces: ['00:10.0', '00:11.0']
  port_info:
      - ip: 101.101.101.1
        default_gw: 101.101.101.254
      - ip: 102.102.102.1
        default_gw: 102.102.102.254

  platform:
      master_thread_id: 0
      latency_thread_id: 1
      dual_if:
        - socket: 0
          threads: [2,3,4,5]

  memory:
      dp_flows: 40000000
```

Приложение №5

Профиль EMIX-трафика

name	cps	f-pkts	f-bytes	Mb/sec	MB/sec	c-flows	PPS
http_get.pcap	102	44	38182	29.71	3.71	45	4488
http_post.pcap	102	54	48900	38.05	4.76	55	5508
https.pcap	33	96	92387	23.26	2.91	32	3168
http_browsing.pcap	179	37	34721	47.42	5.93	66	6623
exchange.pcap	64	43	10192	4.98	0.62	28	2752
email_pop1.pcap	1	20	5763	0.05	0.01	0	24
email_pop2.pcap	1	114	102429	0.94	0.12	1	137
email_pop4_29.pcap	1	30	15870	0.15	0.02	0	36
oracle.pcap	20	302	58547	8.93	1.12	60	6040
rtp_160_0.pcap	1	84	97484	0.52	0.07	1	59
rtp_160_1.pcap	1	1244	1138480	6.08	0.76	9	871
rtp_250k_1_0.pcap	0	108	147128	0.56	0.07	1	54
rtp_250k_2_0.pcap	0	1920	1767018	6.74	0.84	10	960
smtp_1.pcap	2	22	5794	0.08	0.01	0	41
smtp_2.pcap	2	35	18624	0.26	0.03	1	65
smtp_3.pcap	2	110	97424	1.38	0.17	2	204
video_call_0.pcap	3	2325	2551177	58.39	7.30	70	6975
video_rtp_1588_0.pcap	7	1558	123704	6.98	0.87	115	11529
citrix_0.pcap	11	272	86729	7.28	0.91	30	2992
dns_0.pcap	498	2	178	0.68	0.08	10	996
sip_0.pcap	7	7	2723	0.15	0.02	1	52
rtsp_0.pcap	1	20	4038	0.04	0.00	0	24
sum	**1040**	**8447**	**6447492**	**242.63**	**30.33**	**536**	**53596**