



ул. Ольховская, д. 4, корп. 2

г. Москва, 105066

+7 499 110-25-34

info@bi.zone

www.bi.zone

# Отчет о тестировании NGFW "Континент 4" для ООО "Код Безопасности" в 2025

# Оглавление

Термины и сокращения .....	3
Введение .....	4
Цели тестирования .....	5
Описание платформы .....	6
Материально-техническое обеспечение испытаний: .....	7
Схема .....	8
Список проводимых тестов.....	9
Общая таблица результатов .....	10
Итоги тестирования .....	12
1.1 Пропускная способность межсетевого экрана (UDP 1500).....	12
1.2.1 Пропускная способность межсетевого экрана (Arpmix) .....	13
1.2.2 Пропускная способность межсетевого экрана (Arpmix, без логирования)...	14
2.1 Пропускная способность контроля приложений .....	16
2.2 Пропускная способность контроля приложений (без логирования) .....	17
3.1 Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 47% - COB, атаки, подмешанные в легитимный трафик) .....	18
3.2 Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 65% - COB, атаки, подмешанные в легитимный трафик) .....	20
3.3 Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 90% - COB, атаки, подмешанные в легитимный трафик) .....	21
Приложение 1.....	23
О компании BI.ZONE .....	24
О компании «Код Безопасности» .....	25

# Термины и сокращения

Сокращение	Определение
HTTP	HyperText Transfer Protocol — протокол прикладного уровня передачи данных
NGFW	Next-Generation Firewall — система межсетевого экранирования нового поколения
TCP	Transmission Control Protocol — сетевой протокол управления передачей
TLS	Transport Layer Security — безопасность транспортного уровня
UDP	User Datagram Protocol — протокол передачи сетевых датаграмм
МСЭ	Межсетевой экран
СОБ	Система обнаружения вторжений

---

# Введение

В настоящем документе приведен отчет о результатах тестирования межсетевого экрана (далее - МСЭ), проведенного ООО «БИЗон» (далее — Исполнитель) для ООО "Код Безопасности" (далее — Заказчик) в феврале 2025 г.

---

## Цели тестирования

В ходе тестирования проверялись функциональные возможности и технические характеристики МСЭ Заказчика. Испытания проводились на тестовом стенде Исполнителя. По результатам тестов фиксировались значения измеряемых характеристик.

# Описание платформы

Тестирование выполнялось на специальном лабораторном стенде Исполнителя с использованием ПО генератора трафика Ixia Breaking Point на базе аппаратной платформы семейства PerfectStorm.

На Ixia формировался трафик и направлялся на тестируемое устройство в соответствии с методикой тестирования. Отфильтрованный трафик передавался тестируемым устройством на выделенные интерфейсы Ixia. На генераторе трафика производилась оценка работы тестируемого устройства.

Для эмуляции протоколов и приложений использовался набор Application Mix (Arpmix) на генераторе трафика Breaking Point в пропорциях, представленных на рис. 1.

Name	Weight	Seed	Sessions	% Bandwidth*	% Flows	# Bytes
Bandwidth HTTP 100k	70	Generated	1	35.65	30.30	335,586
TLSv1.2 HTTP Standard Response Size 100KB	30	Generated	1	15.28	12.99	115,385
Webex IR	40	Generated	2	10.19	17.32	7,862
Remote Desktop Protocol-moex	20	Generated	1	10.19	8.66	5,097
TLSv1.2 HTTP Standard Response Size 10KB	20	Generated	1	10.19	8.66	12,494
SSH	10	Generated	1	5.09	4.33	9,726
BreakingPoint SMTP Email SV	10	Generated	1	5.09	4.33	20,235
DNS	6	Generated	1	3.06	2.60	257
RTSP	10	Generated	3	1.70	4.33	7,925
SMBv2 File Download_SV	3	Generated	1	1.53	1.30	117,412
FTP	10	Generated	5	1.02	4.33	12,250
LDAP	2	Generated	1	1.02	0.87	812

Рис. 1. Профиль тестового трафика, согласованный с Заказчиком.

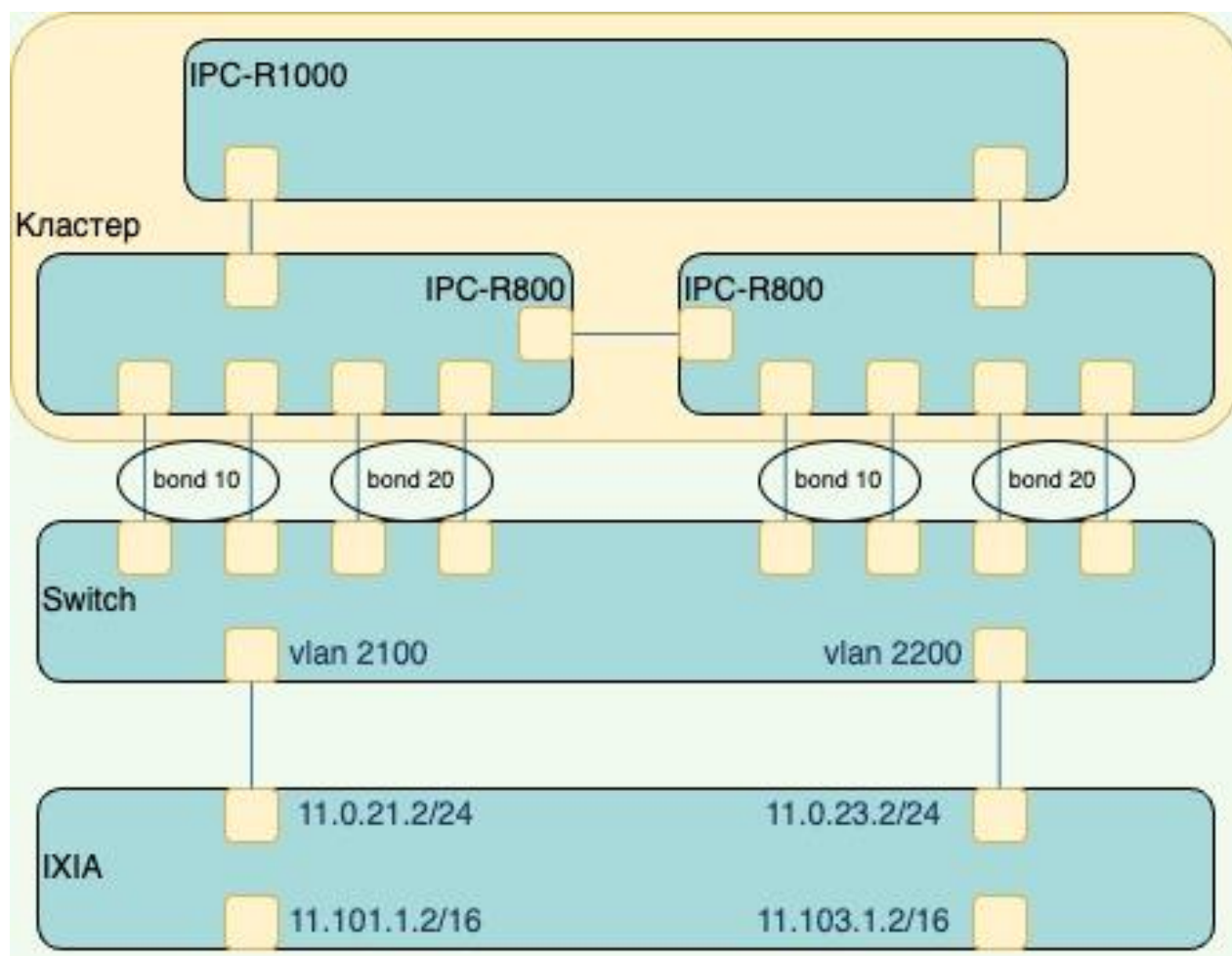
---

# Материально-техническое обеспечение испытаний:

- Шасси генератора трафика Ixia XGS2-HSL с управляющим ПО Ixia Breaking Point.
- Модуль нагрузки Ixia PerfectStorm.
- Сетевое оборудование для обеспечения связности объектов тестового стенда: Huawei S6730-H.
- ЦУС - Платформа IPC-R1000 "Континент 4".
- Кластер - Платформа IPC-R800 "Континент 4".

# Схема

Схема состояла из двух IPC-R800 объединенных в кластер под управлением IPC-R1000. Использовались четыре интерфейса 10 GE, объединенных в два bond-интерфейса. Тестовый трафик запускался с генератора трафика из сетей 11.101.1.2/16 и 11.103.1.2/16 через два интерфейса 100 GE. Во время тестирования, часть ресурсов NGFW использовалась для организации кластера.



# Список проводимых тестов

Тестируемое оборудование было протестировано при работе в следующих режимах:

1. Пропускная способность межсетевого экрана (UDP 1500 и Arpmix).
2. Пропускная способность контроля приложений (Arpmix).
3. Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений (Arpmix) с различным распределением по компонентам:
  - 3.1 100% - контроль приложений, 47% - СОВ.
  - 3.2 100% - контроль приложений, 65% - СОВ.
  - 3.3 100% - контроль приложений, 90% - СОВ.

Для тестов п.п 3, к тестовому трафику добавлялись атаки. На NGFW для прохождения тестов было настроено 300 правил с логированием. Правила фильтрации для прохождения тестов приведены в Приложении 1.

# Общая таблица результатов

По итогу каждого проведенных испытаний была заполнена таблица результатов (табл. 1):

N п/п	Тест	Максимальная пропускная способность	Максимальная загрузка одного из ядер NGFW/Средняя нагрузка на все ядра NGFW	Пропускная способность, заявленная Заказчиком
1.1	Пропускная способность межсетевого экрана (UDP 1500)	37,440 Мбит/с	100%/74,4%	24,000 Мбит/с
1.2.1	Пропускная способность межсетевого экрана (Arpmix)	13,408 Мбит/с	92.9%/68,7%	13,000 Мбит/с
1.2.2	Пропускная способность межсетевого экрана (Arpmix, без логирования)	16,008 Мбит/с	98,7%/65,2%	
2.1	Пропускная способность контроля приложений	13,419 Мбит/с	87,7%/83,25%	
2.2	Пропускная способность контроля приложений (без логирования)	16,012 Мбит/с	98,7%/67,7%	
3.1	Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 47% -	5,810 Мбит/с	100%/96,9%	3,800 Мбит/с

---

СОВ, атаки подмешанные в  
легитимный трафик)

---

3.2	Пропускная способность контроля приложений и системы обнаружения/предотвращен ия вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 65% - СОВ, атаки подмешанные в легитимный трафик)	6,046 Мбит/с	100%/99,2%	3,800 Мбит/с
-----	--	--------------	------------	--------------

---

3.3	Пропускная способность контроля приложений и системы обнаружения/предотвращен ия вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 90% - СОВ, атаки подмешанные в легитимный трафик)	2,363 Мбит/с	97,3%/92,4%	3,800 Мбит/с
-----	--	--------------	-------------	--------------

---

# Итоги тестирования

## 1.1 Пропускная способность межсетевое экрана (UDP 1500)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 37,440 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 100%, среднее значение нагрузки всех ядер составило 74,4%.

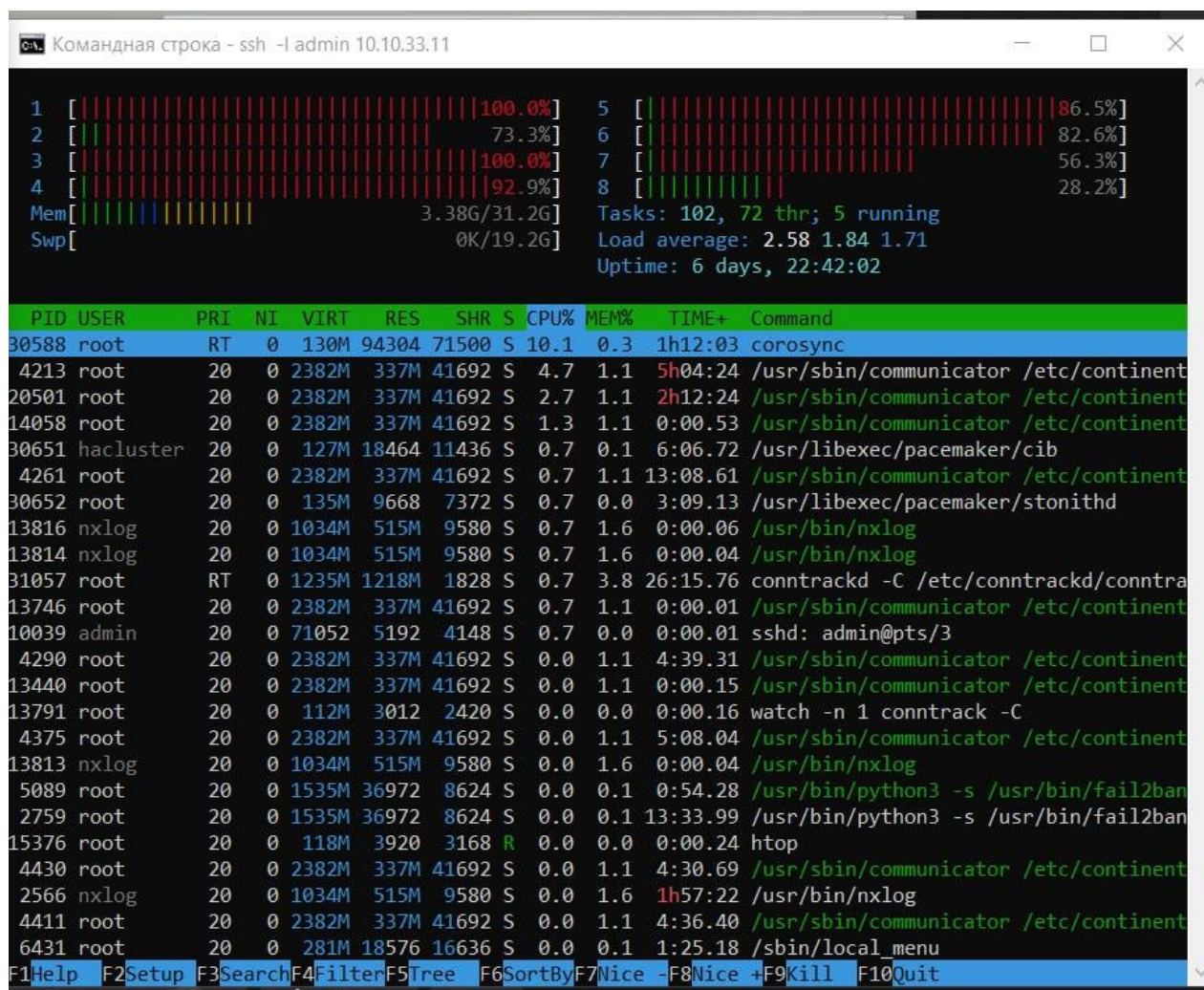


Рис. 2. Вывод нагрузки на ядра Устройства, во время прохождения теста.

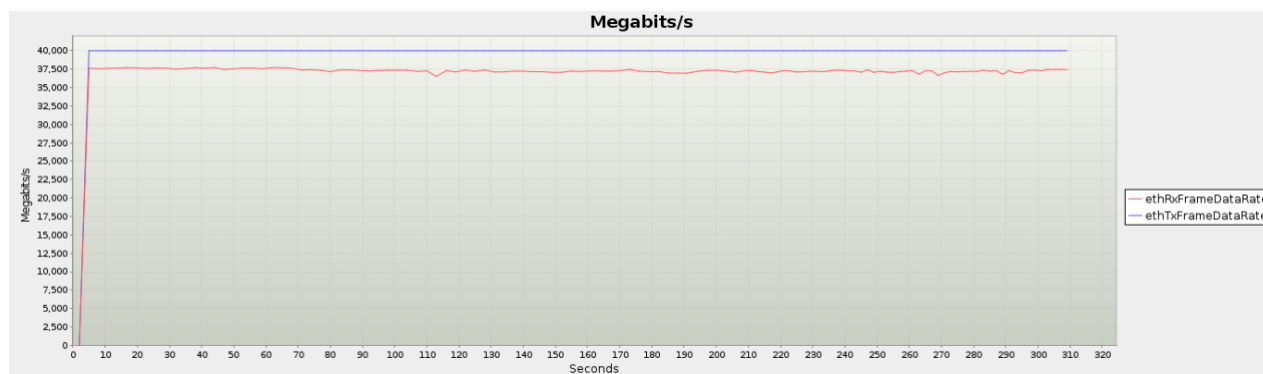


Рис. 3. График пропускной способности, зафиксированной на генераторе трафика. В режиме МСЭ Устройство обрабатывает без ошибок в среднем 37 Гбит/с UDP-трафика.

## 1.2.1 Пропускная способность межсетевое экрана (Armitix)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 13,408 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 92,9%, среднее значение нагрузки всех ядер составило 68,7%.

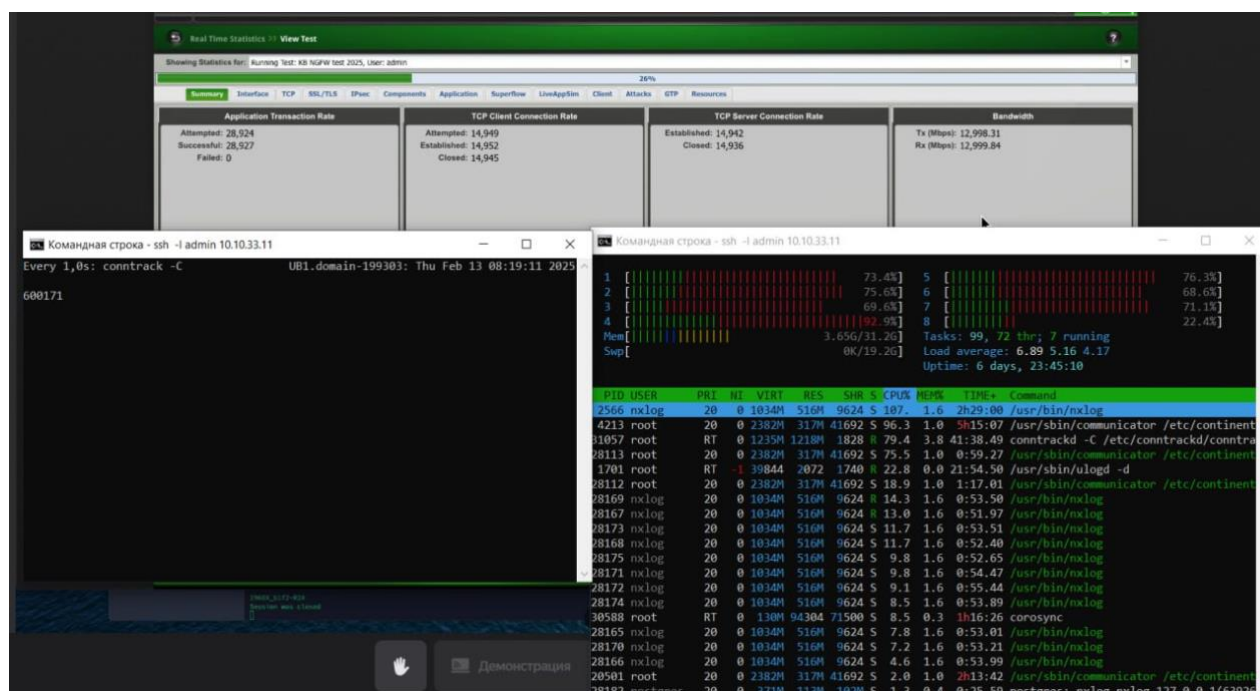


Рис. 4. Вывод нагрузки на ядра и вывод команды `conntrack -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

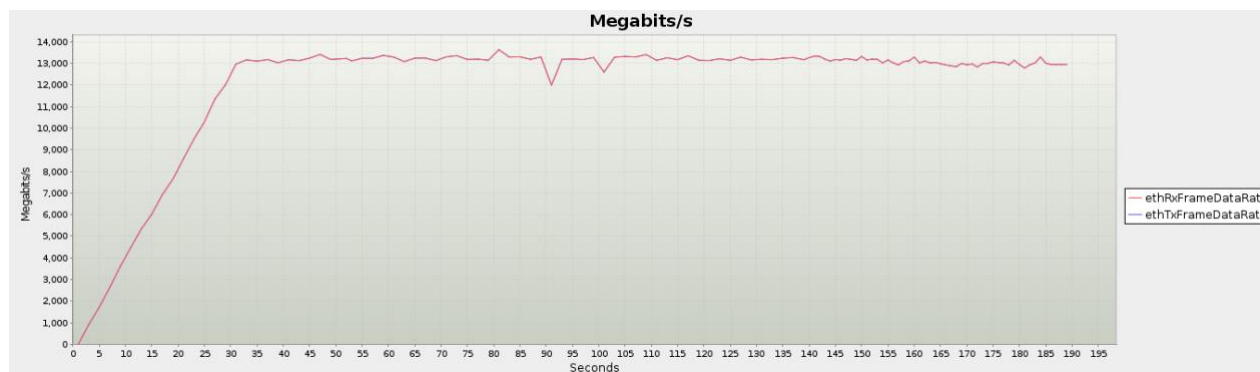


Рис. 5. График пропускной способности, зафиксированной на генераторе трафика.

В режиме МСЭ с включенным логированием Устройство обрабатывает без ошибок в среднем 13 Гбит/с трафика.

## 1.2.2 Пропускная способность межсетевого экрана (Armitix, без логирования)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 16,008 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 98,7%, среднее значение нагрузки всех ядер составило 65,2%.

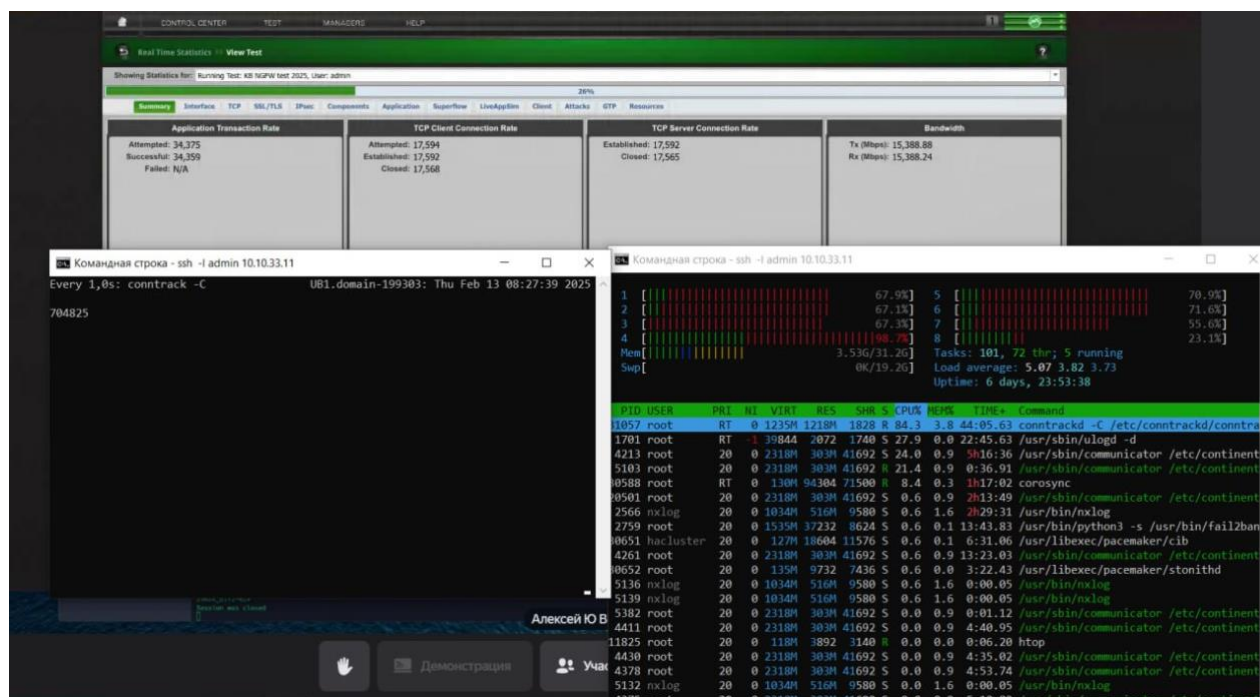


Рис. 6. Вывод нагрузки на ядра и вывод команды `conntrack -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

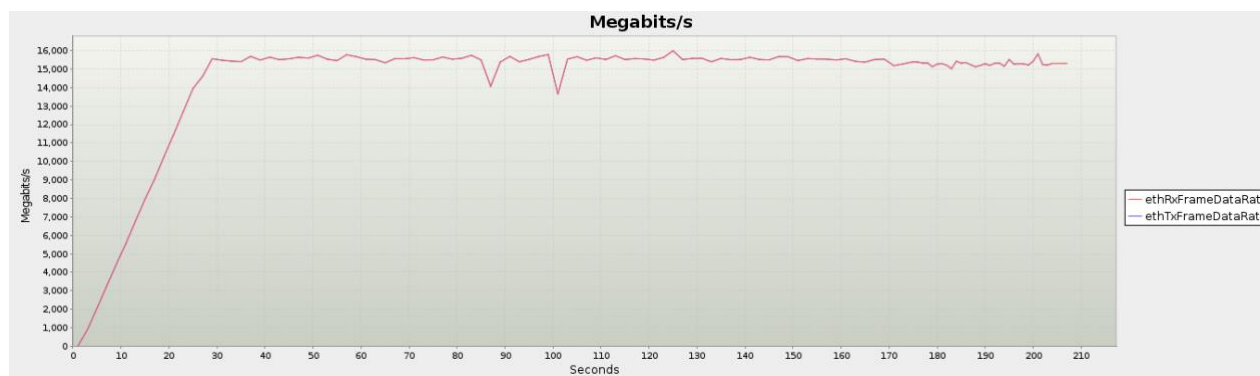


Рис. 7. График пропускной способности, зафиксированной на генераторе трафика. В режиме МСЭ с выключенным логированием Устройство обрабатывает без ошибок в среднем 15,5 Гбит/с трафика.

## 2.1 Пропускная способность контроля приложений

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 13,419 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 87,7%, среднее значение нагрузки всех ядер составило 83,25%.

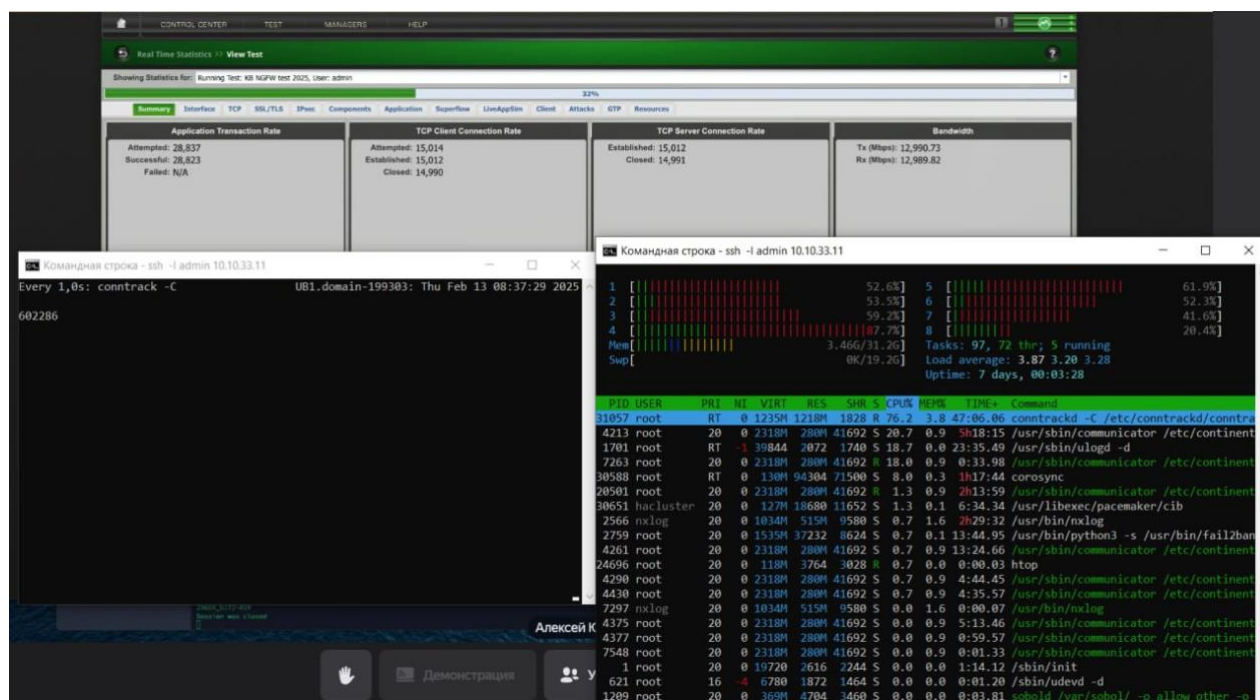


Рис. 8. Вывод нагрузки на ядра и вывод команды `contrackd -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

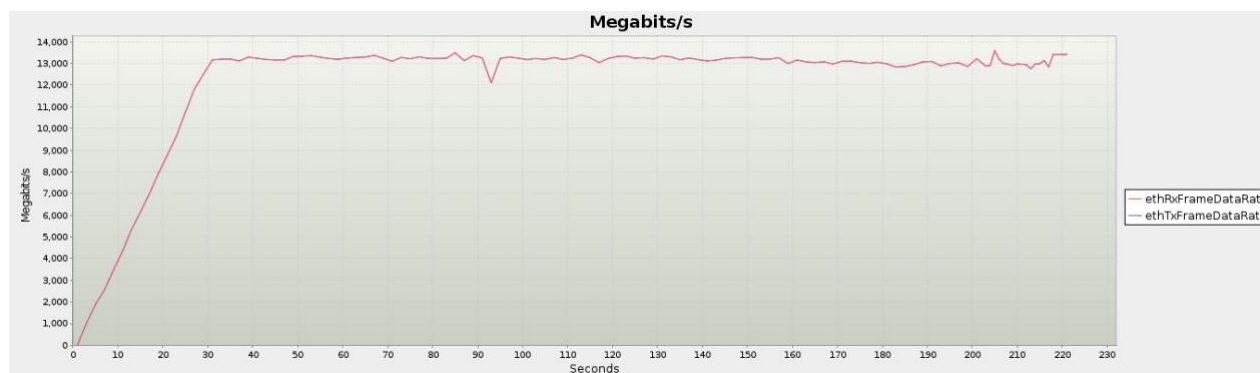


Рис. 9. График пропускной способности, зафиксированной на генераторе трафика.

В режиме контроля приложений с включенным логированием, Устройство обрабатывает без ошибок в среднем 13 Гбит/с трафика.

## 2.2 Пропускная способность контроля приложений (без логирования)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 16,012 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 98,7%, среднее значение нагрузки всех ядер составило 67,7%.

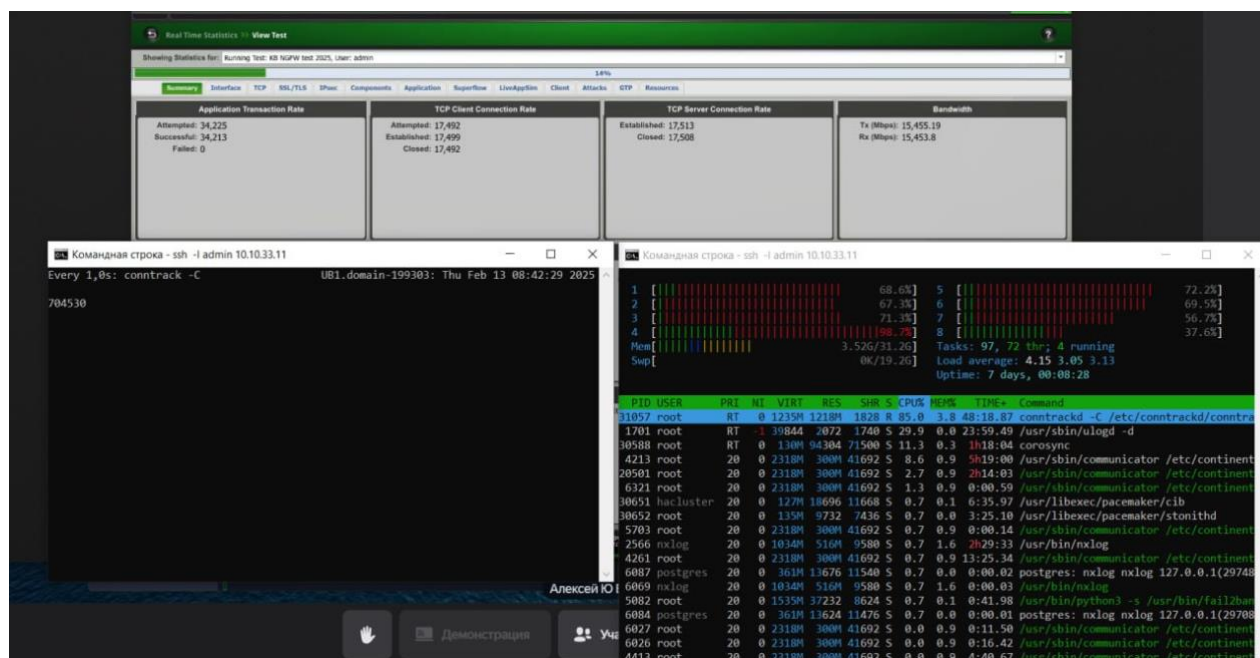


Рис. 10. Вывод нагрузки на ядра и вывод команды `conntrack -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

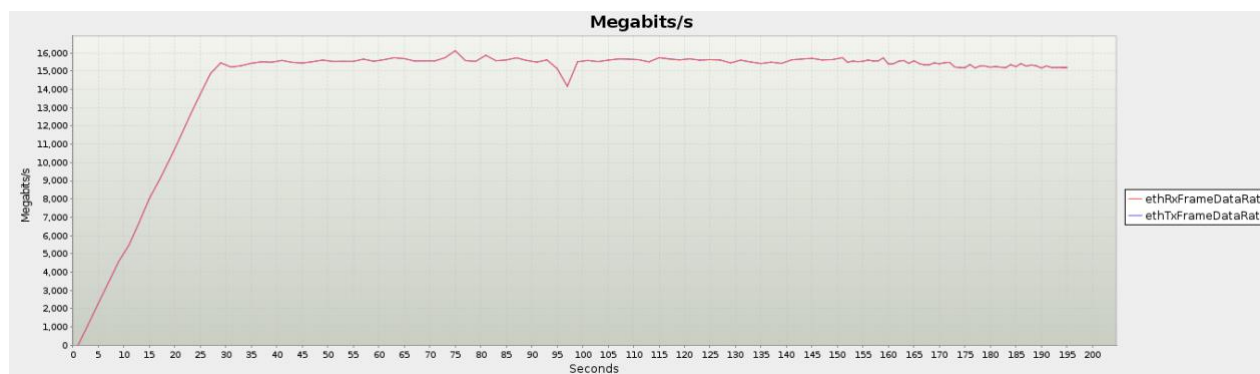


Рис. 11. График пропускной способности, зафиксированной на генераторе трафика.

В режиме контроля приложений с выключенным логированием Устройство обрабатывает без ошибок в среднем 15,5 Гбит/с трафика.

### 3.1 Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 47% - СОВ, атаки, подмешанные в легитимный трафик)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 5,810 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 100%, среднее значение нагрузки всех ядер составило 96,9%.

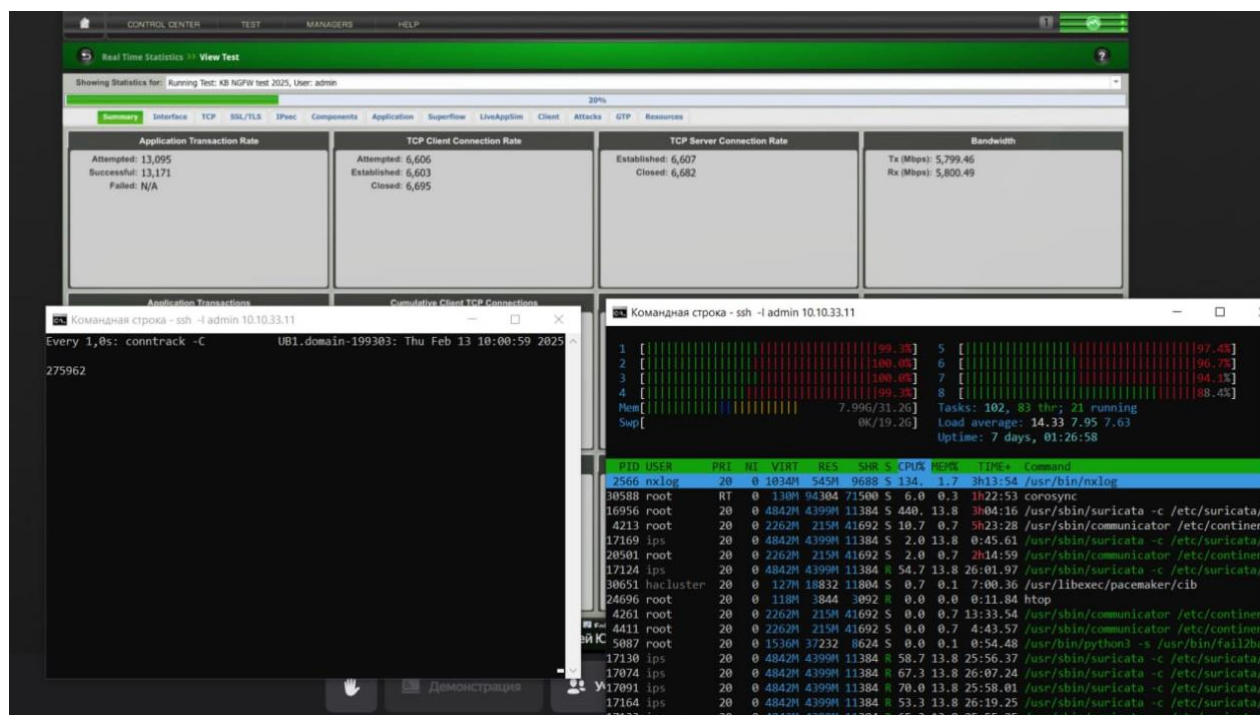


Рис. 20. Вывод нагрузки на ядра и вывод команды `conntrack -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

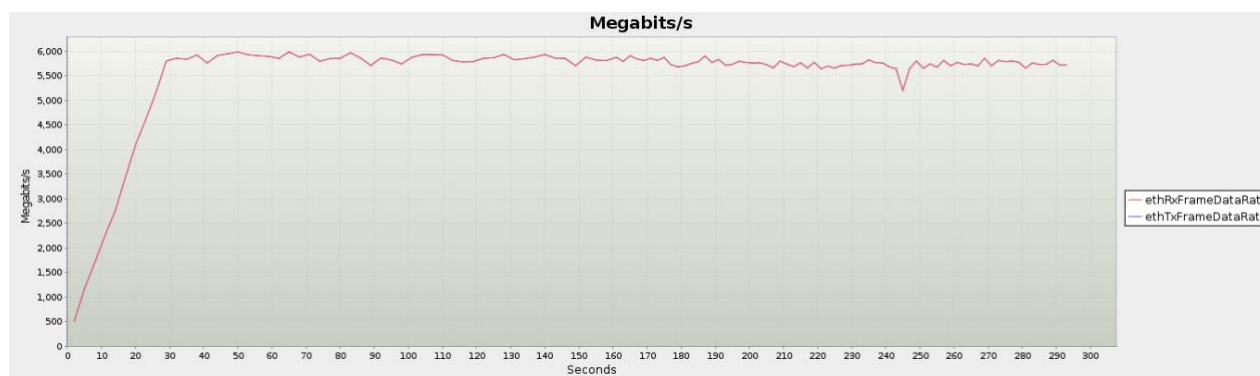


Рис. 21. График пропускной способности, зафиксированной на генераторе трафика.

В режиме DPI и 47% СОВ с атаками, подмешанными в трафик, Устройство обрабатывает без ошибок в среднем 5,5 Гбит/с трафика.

## 3.2 Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 65% - СОВ, атаки, подмешанные в легитимный трафик)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 6,046 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 100%, среднее значение нагрузки всех ядер составило 99,2%.

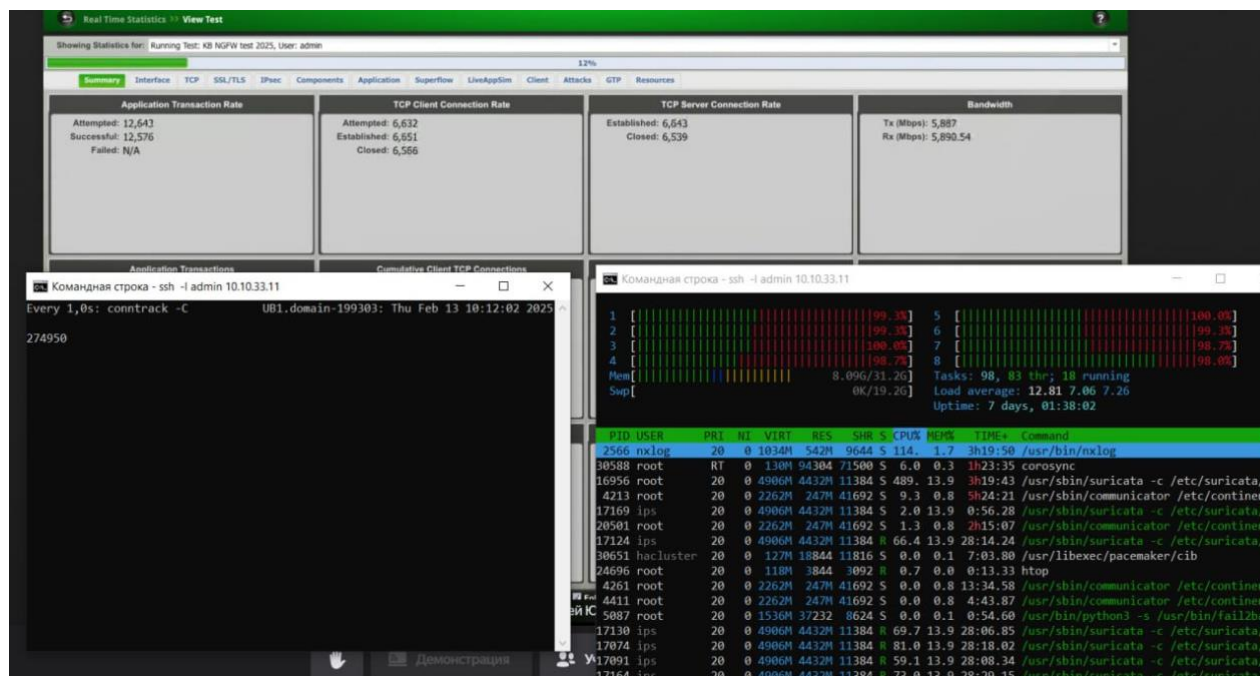


Рис. 22. Вывод нагрузки на ядра и вывод команды `conntrack -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

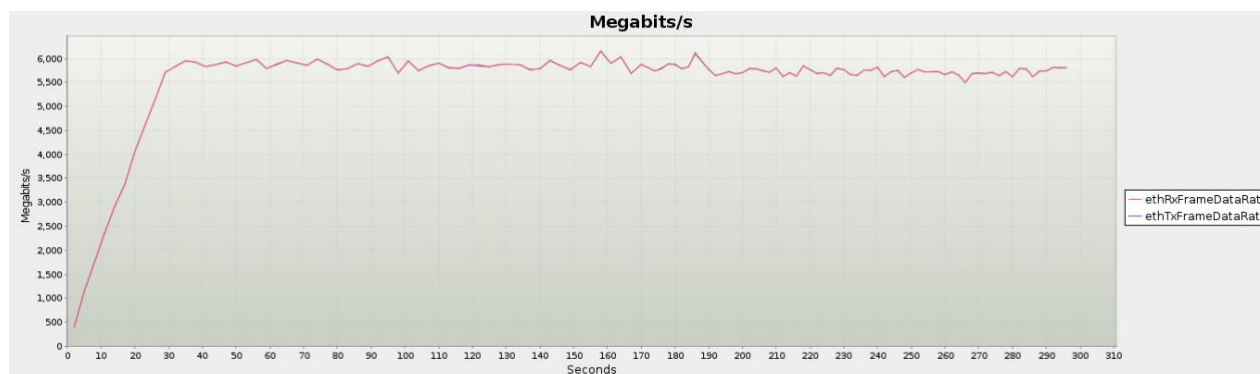


Рис. 23. График пропускной способности, зафиксированной на генераторе трафика.

В режиме DPI и 65% COB с атаками, подмешанными в трафик, Устройство обрабатывает без ошибок в среднем 5,4 Гбит/с трафика.

### 3.3 Пропускная способность контроля приложений и системы обнаружения/предотвращения вторжений на разных наборах сигнатур с различным распределением по компонентам (100% - контроль приложений, 90% - COB, атаки, подмешанные в легитимный трафик)

Максимальное значение пропускной способности, зафиксированное на генераторе трафика - 2,363 Мбит/с.

Максимальное зафиксированное значение нагрузки на ядро составило 97,3%, среднее значение нагрузки всех ядер составило 92,4%.

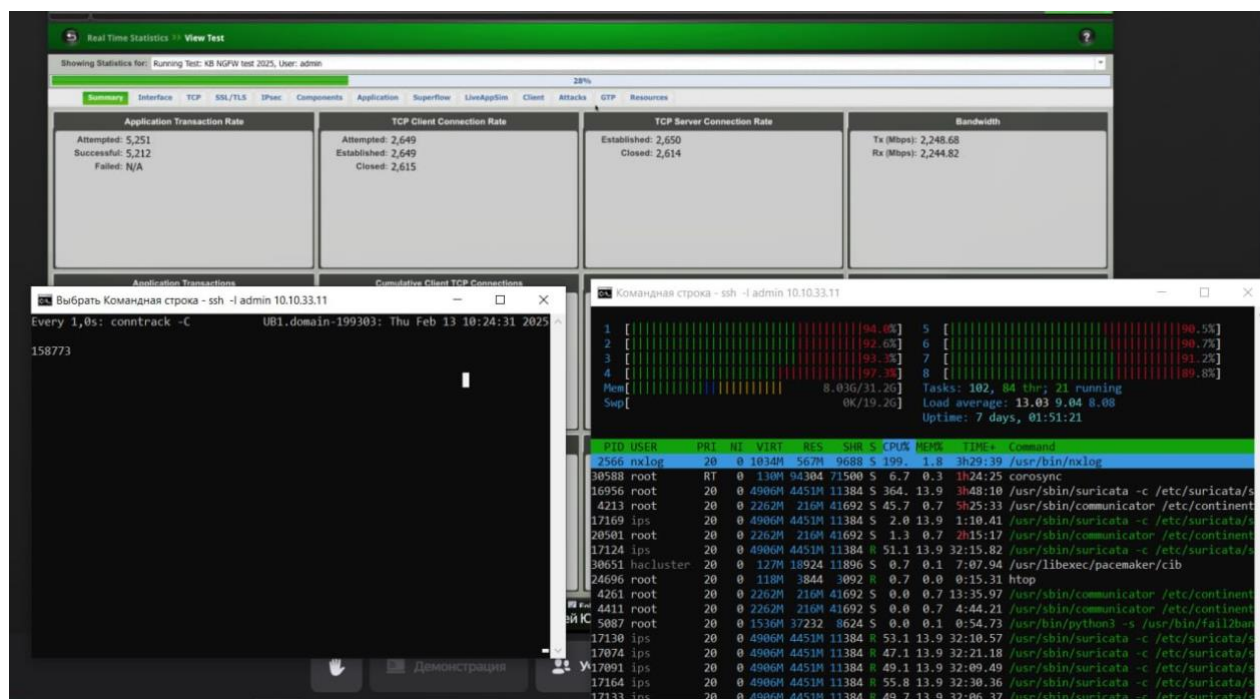


Рис. 24. Вывод нагрузки на ядра и вывод команды `conntrack -C` на Устройстве, а также значений (transaction rate, connection rate со стороны клиента и сервера, bandwidth) на Генераторе трафика во время прохождения теста.

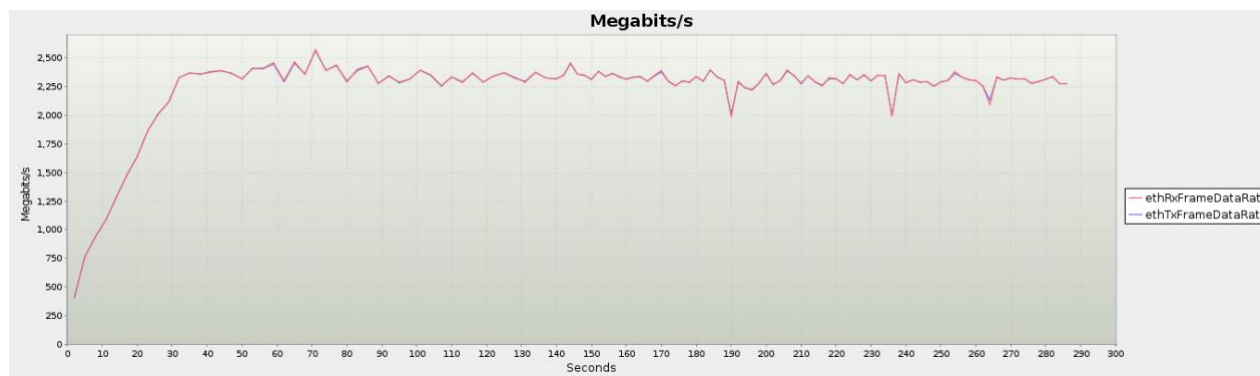


Рис. 25. График пропускной способности, зафиксированной на генераторе трафика. В режиме DPI и 90% COB с атаками, подмешанными в трафик, Устройство обрабатывает без ошибок в среднем 2,1 Гбит/с трафика.

# Приложение 1.

296	Rule 296	<input checked="" type="checkbox"/> 16.93.0.0/16	<input checked="" type="checkbox"/> 48.215.0.0/16	10851	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
297	Rule 297	<input checked="" type="checkbox"/> 16.37.0.0/16	<input checked="" type="checkbox"/> 48.72.0.0/16	↑ 5709	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
298	Rule 298	<input checked="" type="checkbox"/> 16.94.0.0/16	<input checked="" type="checkbox"/> 48.45.0.0/16	↑ 35614	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
299	Rule 299	<input checked="" type="checkbox"/> 16.213.0.0/16	<input checked="" type="checkbox"/> 48.201.0.0/16	↑ 46798	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
312												
300	<input checked="" type="checkbox"/> (1)(1)(1)	* Любой	* Любой	↑ HTTP	* Любое	<input checked="" type="checkbox"/> Фильтр...	<input checked="" type="checkbox"/> any http ass	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
301	<input checked="" type="checkbox"/> (1)(1)	* Любой	* Любой	↑ TLS	* Любое	<input checked="" type="checkbox"/> Фильтр...	<input checked="" type="checkbox"/> any https ass	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
302	<input checked="" type="checkbox"/> (1)	* Любой	* Любой	* Любой	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
303	<input checked="" type="checkbox"/> (1)	* Любой	* Любой	* Любой	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust

Рис. 26. Правила фильтрации на NGFW для теста с UDP трафиком.

297	Rule 297	<input checked="" type="checkbox"/> 16.37.0.0/16	<input checked="" type="checkbox"/> 48.72.0.0/16	↑ 5709	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
298	Rule 298	<input checked="" type="checkbox"/> 16.94.0.0/16	<input checked="" type="checkbox"/> 48.45.0.0/16	↑ 35614	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
299	Rule 299	<input checked="" type="checkbox"/> 16.213.0.0/16	<input checked="" type="checkbox"/> 48.201.0.0/16	↑ 46798	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
312												
300	<input checked="" type="checkbox"/> (1)(1)(1)	* Любой	* Любой	↑ HTTP	* Любое	<input checked="" type="checkbox"/> Фильтр...	<input checked="" type="checkbox"/> any http ass	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
301	<input checked="" type="checkbox"/> (1)(1)	* Любой	* Любой	↑ TLS	* Любое	<input checked="" type="checkbox"/> Фильтр...	<input checked="" type="checkbox"/> any https ass	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
302	<input checked="" type="checkbox"/> (1)	* Любой	* Любой	* Любой	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
303	<input checked="" type="checkbox"/> (1)	* Любой	* Любой	* Любой	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust

Рис. 27. Правила фильтрации на NGFW контроля приложений. Тестирование производительности контроля приложений, трафик Armitix.

298	Rule 298	<input checked="" type="checkbox"/> 16.94.0.0/16	<input checked="" type="checkbox"/> 48.45.0.0/16	↑ 35614	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
299	Rule 299	<input checked="" type="checkbox"/> 16.213.0.0/16	<input checked="" type="checkbox"/> 48.201.0.0/16	↑ 46798	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	- Нет	* Везде
312												
300	<input checked="" type="checkbox"/> (1)(1)(1)	* Любой	* Любой	↑ HTTP	* Любое	<input checked="" type="checkbox"/> Фильтр...	<input checked="" type="checkbox"/> any http ass	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
301	<input checked="" type="checkbox"/> (1)(1)	* Любой	* Любой	↑ TLS	* Любое	<input checked="" type="checkbox"/> Фильтр...	<input checked="" type="checkbox"/> any https ass	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
302	<input checked="" type="checkbox"/> (1)	* Любой	* Любой	* Любой	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	- Выкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust
303	<input checked="" type="checkbox"/> (1)	* Любой	* Любой	* Любой	* Любое	<input checked="" type="checkbox"/> Пропуст...	* Не задан	<input checked="" type="checkbox"/> Вкл	* Всегда	<input checked="" type="checkbox"/> Лог	- Нет	<input checked="" type="checkbox"/> clust

Рис. 28 Правила фильтрации на NGFW. Тестирование производительности контроля приложения и системы обнаружения/предотвращения вторжений, трафик Armitix.

# О компании VI.ZONE

VI.ZONE — компания по управлению цифровыми рисками, которая помогает организациям безопасно развивать бизнес в киберпространстве. VI.ZONE разрабатывает собственные продукты для обеспечения устойчивости ИТ-инфраструктур любого размера и оказывает широкий спектр услуг по киберзащите: от расследования инцидентов и мониторинга угроз до создания стратегий по кибербезопасности и комплексного аутсорсинга профильных функций.

С 2016 года компания реализовала более 1600 проектов в сферах финансов, телекоммуникаций, энергетики, авиации и многих других, защитив свыше 800 клиентов в 10 странах мира. Мы активно сотрудничаем с такими международными организациями, как Интерпол, Международный Комитет Красного Креста, SWIFT, CyberPeace Institute, Всемирный экономический форум, а квалификация наших экспертов подтверждена сертификатами мирового уровня.

**АССОЦИАЦИЯ  
БАНКОВ  
РОССИИ****Geneva Dialogue**  
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

## О компании «Код Безопасности»

Российский разработчик программных и аппаратных средств, обеспечивающих защиту информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Компания основана в 2008 году и ведет свою деятельность на основании девяти лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации. Более 60 действующих сертификатов, выданных этими органами, подтверждают высокое качество продуктов и позволяют использовать их в информационных системах с самыми жесткими требованиями к безопасности. Продукты компании применяются для защиты конфиденциальной информации, коммерческой тайны, персональных данных и сведений, составляющих государственную тайну.

Свыше 900 авторизованных партнеров компании поставляют ее продукты и обеспечивают их качественную поддержку во всех регионах России и в странах СНГ. Более 32 000 государственных и коммерческих организаций доверяют продуктам «Кода Безопасности» и используют их для защиты рабочих станций, серверов, виртуальных инфраструктур, мобильных устройств и сетевого взаимодействия всех компонентов информационных систем.