



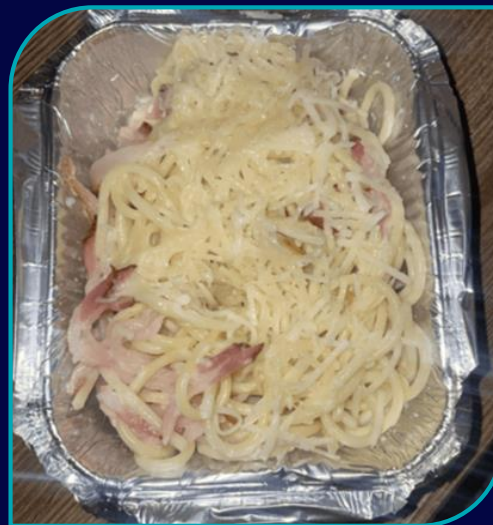


# Покупатели считают, что их вводят в заблуждение

А на сайте обещали другое



Зато порция большая



# У всех свои методики

Cisco



<sup>1</sup> Throughput measured with 1500B User Datagram Protocol (UDP) traffic measured under ideal test conditions.

[Cisco Firepower 4100 Series Data Sheet - Cisco](#)

Palo Alto



\* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.

[downloadResource \(paloaltonetworks.com\)](#)

Check Point



RFC 3511, 2544, 2647, 1242 (Lab),  
Firewall 1518B UDP (Gbps)

[Check Point 26000 Security Gateway Datasheet](#)

# Что такое «идеальные условия»

Производительность тем выше, чем легче задача



- UDP проще, чем TCP: нужно отслеживать меньше состояний
- Самый большой возможный размер пакета (обычно Jumbo frames):
  - Меньше соединений для передачи того же объема данных
  - Меньше заголовков пакетов для разбора



- Максимальное количество соединений:
  - Открыть много соединений
  - Передавать мало или совсем не передавать данных
  - Не закрывайте соединения



- Максимальное количество новых соединений в секунду:
  - Используйте много очень маленьких соединений
  - Передавать МАЛО или совсем не передавать данных
  - Закрывайте соединения как можно быстрее

# Почему никто не тестирует все варианты

Слишком долго и дорого  
–  
за это будут платить  
покупатели



- Если в продукте 26 функций, то оценка влияния каждой на производительность приводит к 67 млн. уникальных тестов.  
(с) Cisco



- Нужно быть экспертом, чтобы понимать результаты всех этих тестов.

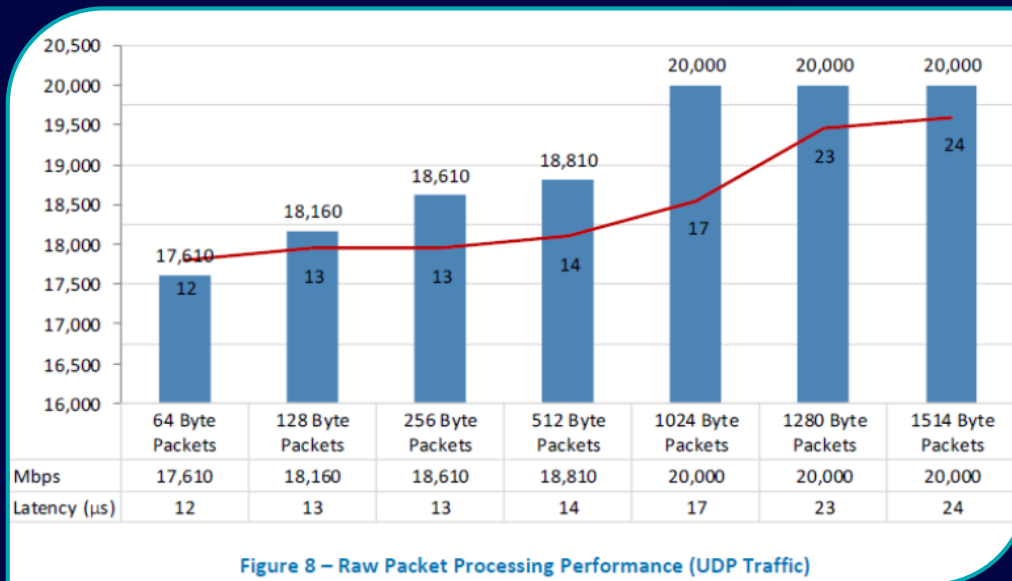


- Покупателю нужно изучить все результаты и собрать из них комбинацию своих, чтобы потом ее протестировать и понять что будет у покупателя.

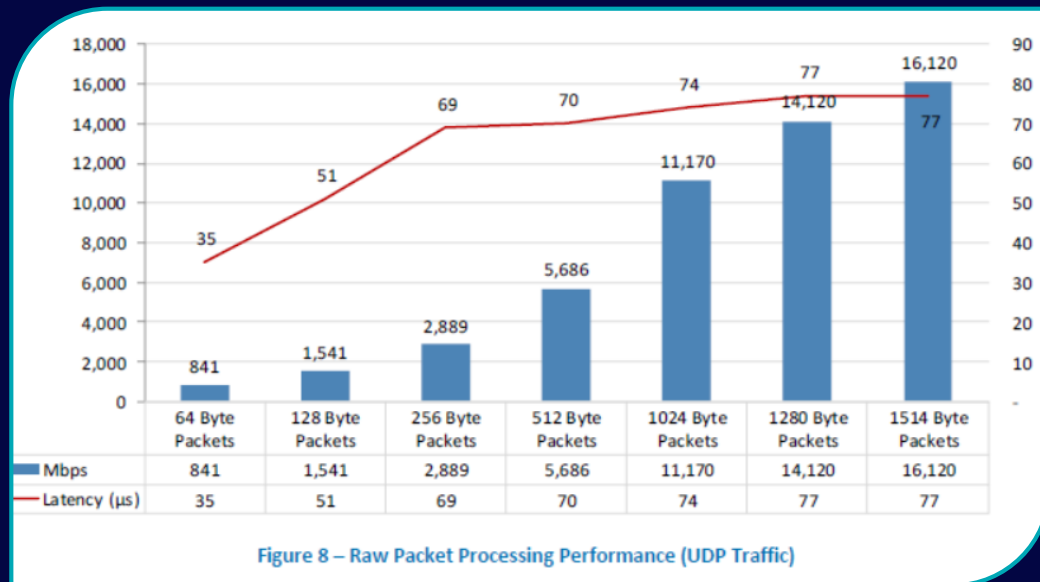


# UDP самый простой тест

Palo Alto Networks  
PA-5220 PAN-OS 8.1.6-h2



# UDP самый простой тест



Check Point Software  
Technologies 6500  
Security Gateway R80.20

# Разные приложения – разная скорость

Palo Alto Networks PA-5220 PAN-OS 8.1.6-h2

These tests measured the performance of the device with single application flows. For details about single application flow testing, see the NSS Labs Next Generation Firewall Test Methodology v9.0, available at [www.nsslabs.com](http://www.nsslabs.com).

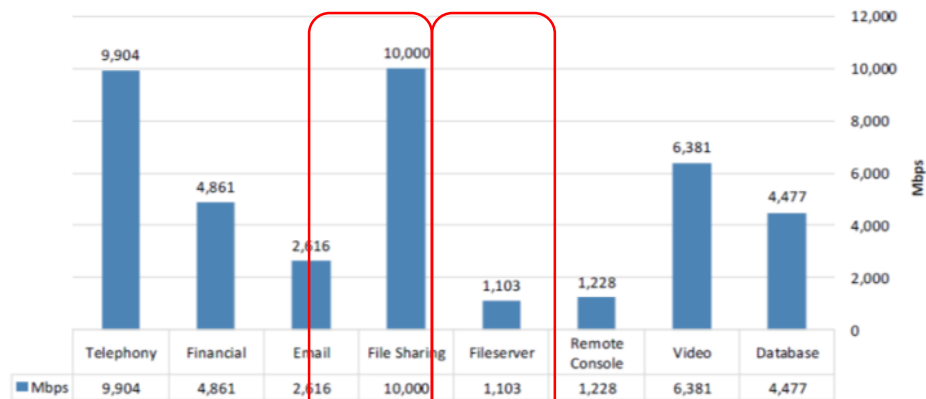


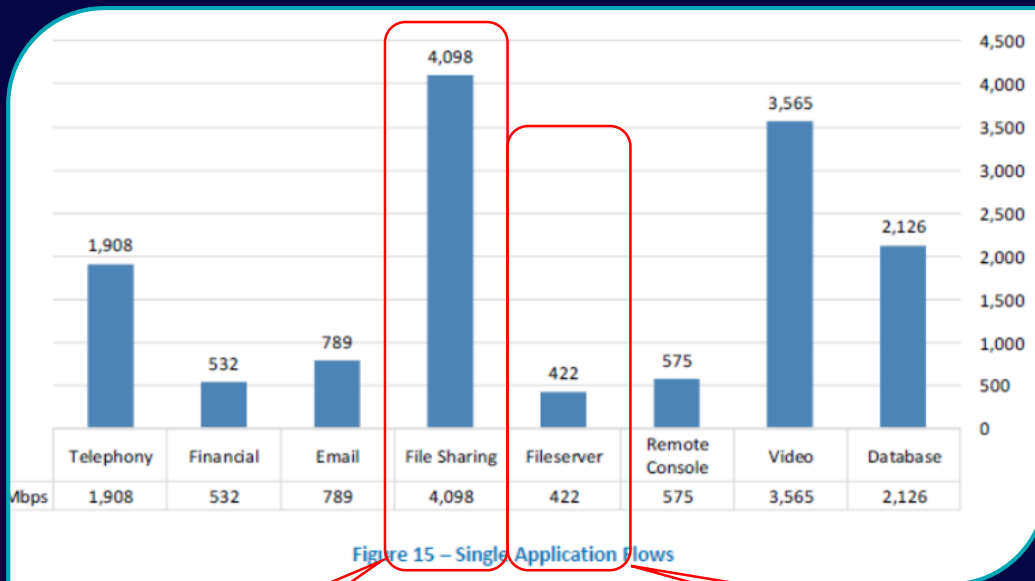
Figure 15 – Single Application Flows

FTP

SMB

# Разные приложения – разная скорость

Check Point Software Technologies 6500 Security Gateway R80.20



FTP

SMB

# Профиль трафика влияет на производительность драматически

Changing the traffic profile from HTTP to an Enterprise Mix and running it through the IPS engine:



- HTTP 44%, Bittorrent 22%, IMAP v4 16%, FTP 9%, SMTP 9%

This is Cisco's generic Multiprotocol test and is very similar to all the Internet multiprotocol standards.

# Даже HTTP у всех разный

HTTP – хороший базовый уровень для тестов “real world”

Cisco

## 1024B HTTP Test (256KB Object)

This number is to compare with other vendors at a 256KB object size. It uses a larger and commonly tested packet size for every simulated session. With the protocol overhead, the average frame size is around 1024 bytes. This represents typical production conditions for most firewall deployments.

Palo Alto  
Networks

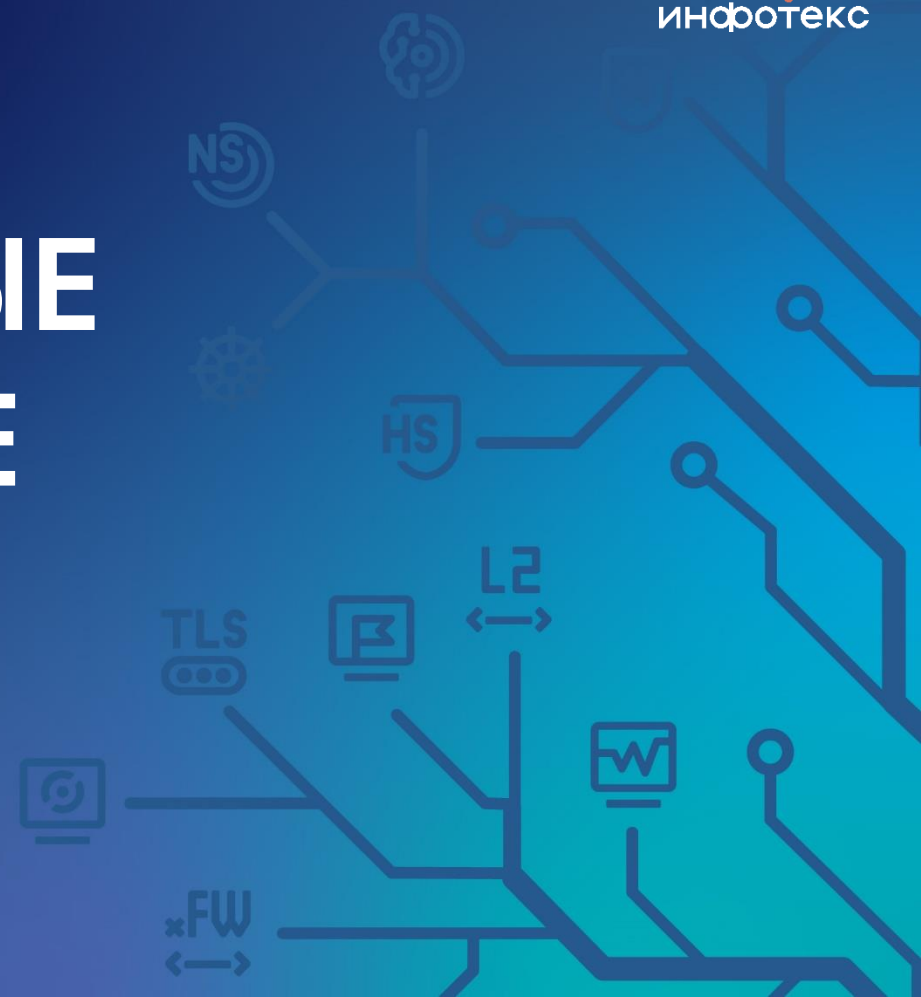
Note: Results were measured on PAN-OS 11.0.

\* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP appmix transactions.

Check Point

	Enterprise Test	Preferred Testing Conditions
Protocols	Typical blend of HTTP, SMTP, HTTPS, DNS, FTP and other protocols derived from research conducted over hundreds of customer environments	HTTP only
Content Types	Realistic blend	Page loads only

# СРАВНИТЕЛЬНЫЕ ТЕСТИРОВАНИЕ ПО МЕТОДИКЕ ИнфоТекс



# Как мы тестируем



Методики ИнфоТеКС основаны на публичных



RFC-2544, RFC 9411  
(Benchmarking Methodology for Network  
Security Device Performance)



Методики NSS Labs - NextGeneration Firewall (NGFW)

# Чем мы тестируем



Система тестирования производительности, функционала и совместимости сетей и сетевых приложений. Компактное 2-слотовое шасси Ixia XM2.



Решение PerfectStorm ONE компании Ixia представляет собой компактный программно-аппаратный комплекс (ПАК), предназначенный для тестирования систем сетевой безопасности и других сетевых средств реалистичным трафиком атак, приложений и сервисов на уровнях 4–7 модели OSI.

# Тесты по методикам и реальность

Самая жесткая методика  
по RFC 9411



Кол-во правил максимум 562

Реальный заказчик



Кол-во правил в 2022  
году было около 5 тыс.,  
а в 2023 году стало  
10 461

# Профиль трафика

## По методике NSS Labs

№	Приложение	Доля трафика, %
1.	Amazon S3	7,73
2.	AOL Instant Messenger	1,16
3.	BitTorrent	10,82
4.	Facebook	5,8
5.	<b>FTP</b>	<b>5</b>
6.	Gmail	9,66
7.	Gtalk	4,64
8.	HTTP	18,69
9.	Simulated HTTPS	9,66
10.	SMTP	1,93
11.	SSH	0,29
12.	Oracle DB	0,28
13.	Twitter	3,09
14.	Yahoo Mail	9,66
15.	YouTube	11,59

## Реальный заказчик

№	Приложение	Доля трафика, %
1.	Citrix	5,8
2.	DNS	0,3
3.	Dropbox Sync-Get	7,2
4.	HTTP Text_1	5,8
5.	HTTP VE	8,7
6.	HTTPS Dropbox	19
7.	MAX Bandwidth HTTP_	4,4
8.	RDP	0,4
9.	<b>SMB Client File Download</b>	<b>43,9</b>
10.	SNMP_1	4,5
11.		
12.		
13.		
14.		
15.		

# Журналирование

Самая жесткая методика  
по RFC 9411

Реальный заказчик



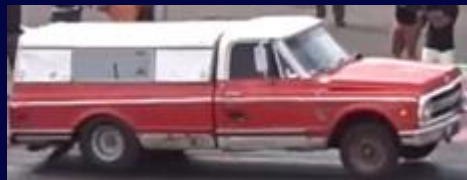
Logging and reporting  
MUST be enabled



Должно быть включено  
журналирование всего

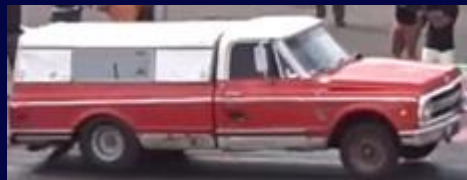


# Данные с сайта



Исполнение	Производитель А	Производитель Б
Firewall, 1518 byte UDP (Mbps)	до 45 000	До 30 000
Firewall Throughput (Packets Per Second)	4 000 000	----
Firewall, TCP Multistream (Mbps)	30 000	40 000

# Данные с сайта



Исполнение	Производитель А	Производитель Б
AppControl (Firewall+DPI) (Mbps)	7 800	32 000
NGFW Througput (Mbps)	1 531	3 900
Connections per Second	85 000	127 000
Concurrent Connections	9 900 000	16 000 000

# Казалось бы, победитель известен до старта



# Тест «Идеальные условия»

	Производитель А	Производитель Б
МЭ, 1518 байт UDP	45 Гбит/сек	38,2 Гбит/сек
МЭ (пакетов/сек)	4 млн	4,4 млн
Соединений в секунду	85 000	259 000
МЭ, TCP	30 Гбит/сек	34,5 Гбит/сек

# ТЕСТИРОВАНИЕ ПО МЕТОДИКЕ NSS LABS



# Трафик NSS Labs EMIX

Кол-во правил	Производитель А	Производитель Б
1 правило	7,2 Гбит/сек	3,3 Гбит/сек
101 правило	6,6 Гбит/сек	3,1 Гбит/сек
1001 правило	5,5 Гбит/сек	Тест не пройден



# Условия Заказчика

Кол-во правил	Производитель А	Производитель Б
1 правило	700 Мбит/сек	600 Мбит/сек
1001 правило	600 Мбит/сек	500 Мбит/сек
11001 правило	200 Мбит/сек	Тест не пройден

# Победителя определяет финиш





# Данные на сайтах верные!

## Но получены по разным методикам

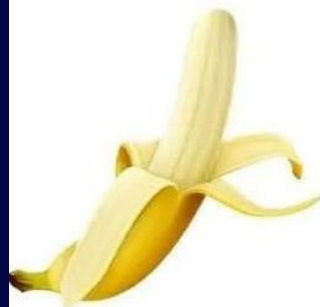
Требуйте предоставить методики измерений... если есть готовность в них разбираться, либо...

2 Результаты получены на основании методики АО «ИнфоТеКС». Результаты получены для релиза 5.6.0.»

Скорость передачи данных измерена по собственной методике, которая может быть предоставлена по запросу.

# Сравнивать нужно в равных условиях

## BANANA VS APPLE



**100 GRAMS**

- PROTEIN : 1.2GM
- CARBS : 27.2GM
- FAT : 0.3GM
- CALORIE : 116



**100 GRAMS**

- PROTEIN : 0.2GM
- FIBER : 3.2GM
- WATER : 86%
- CALORIE : 59

# Как сравнить производительность

Единый профиль трафика



Максимально идентичные  
настройки всех  
испытываемых

Единая  
методика



Единый инструмент  
нагрузочного  
тестирования

# Наши рекомендации



# Что влияет на производительность



CPU

- Elephant flows
- Распределение нагрузки между CPU
- Connection per second



Memory

- Количество политик и/или правил
- Кол-во одновременно обслуживаемых сессий



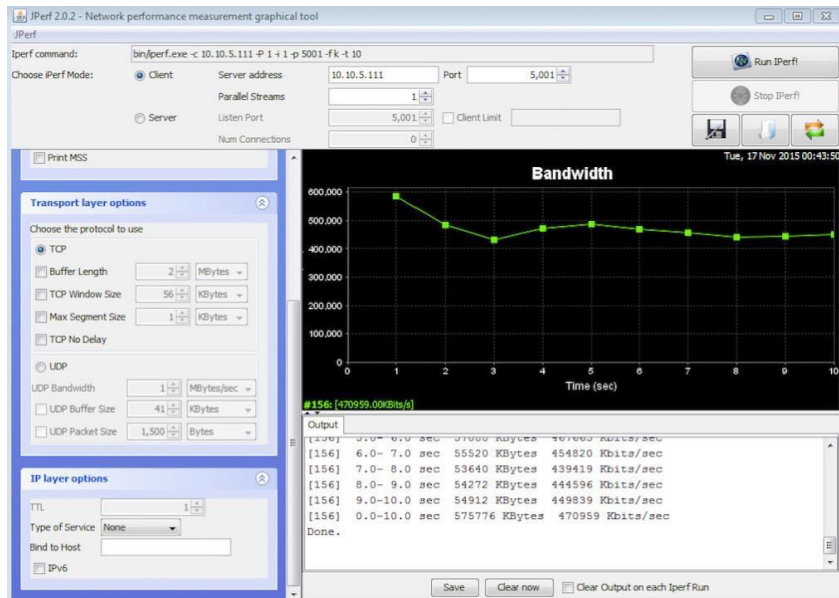
Скорость и/или  
пропускная  
способность

- Тип трафика (HTTP или EMIX)
- Включенные функции (расшифровка SSL, IPS, DPI, Антивирус и т.д.)
- Доступность свободных ресурсов: CPU, RAM



# Пилот прошел успешно

Iperf показывает прекрасные  
результаты



# А в эксплуатации

При работе в реальной сети  
отключается через 2 минуты

# Тестируем по методике

HTTP 64 Кбайт/с

Enterprise MIX NSS Labs

Скорость обработки  
сессий

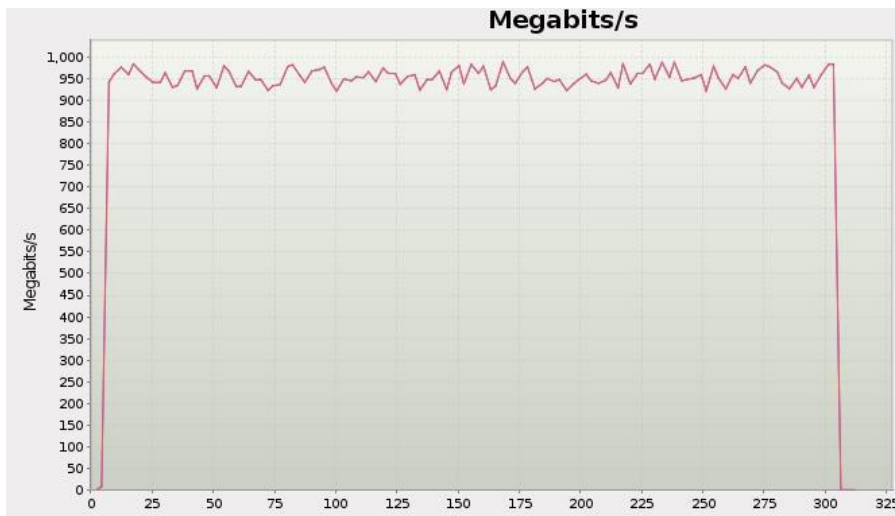
Количество  
одновременных сессий

Длительность теста 300  
секунд

Нагрузчик Ixia, Trex...

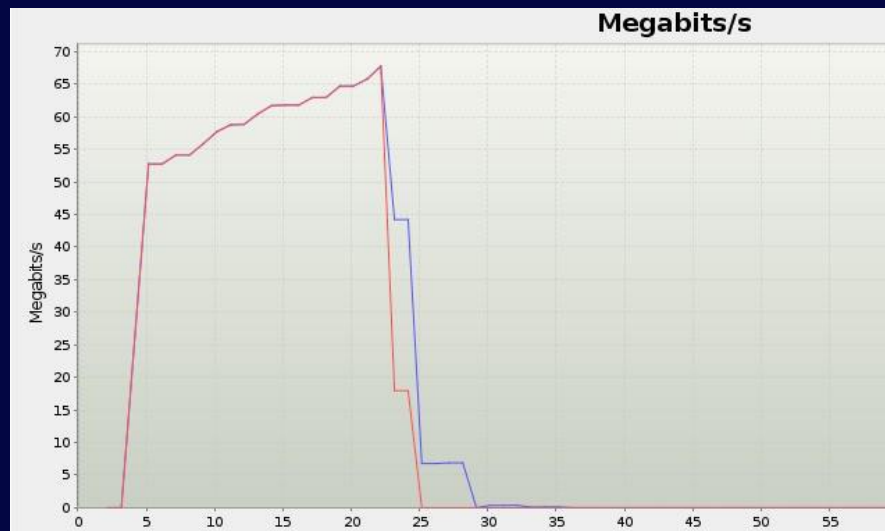
# HTTP

HTTP трафик показал прекрасный результат



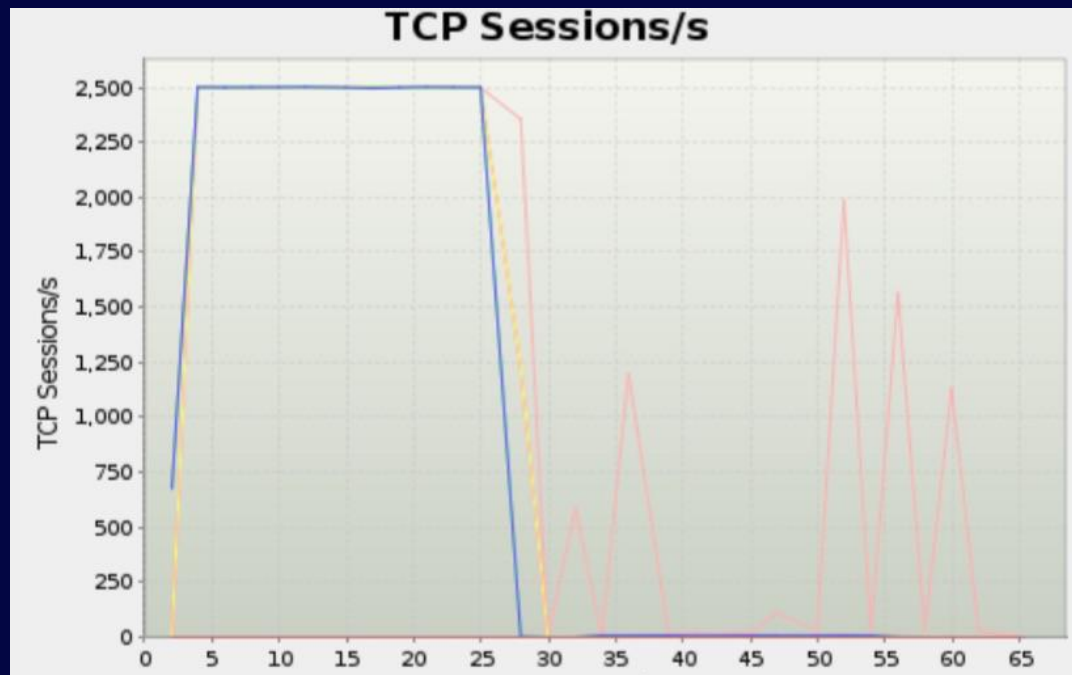
# Enterprise MIX

20 секунд работы привели к полному отказу устройства



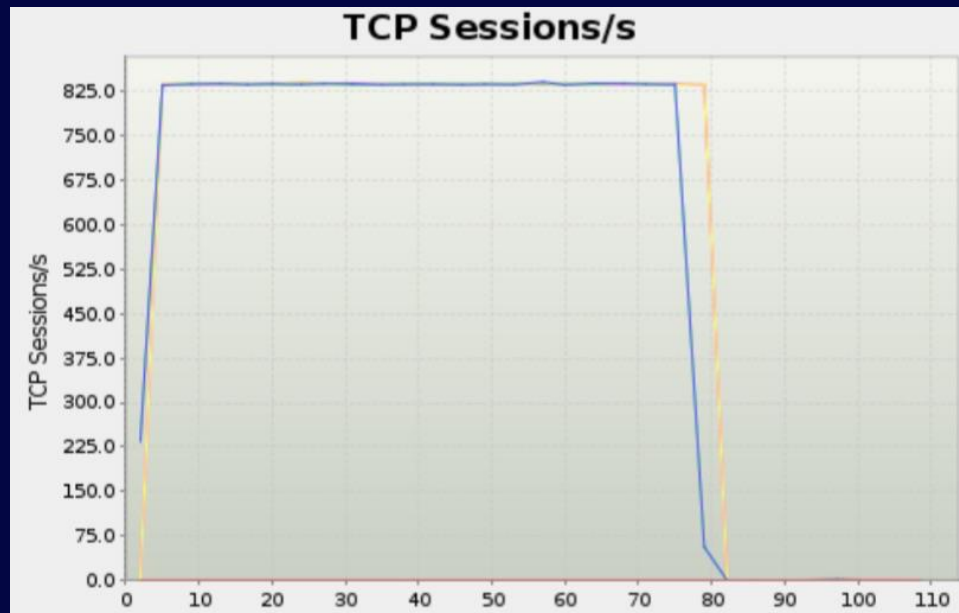
# Скорость открытия новых сессий

2500 сессий в секунду – устройство отказывает через 27 секунд



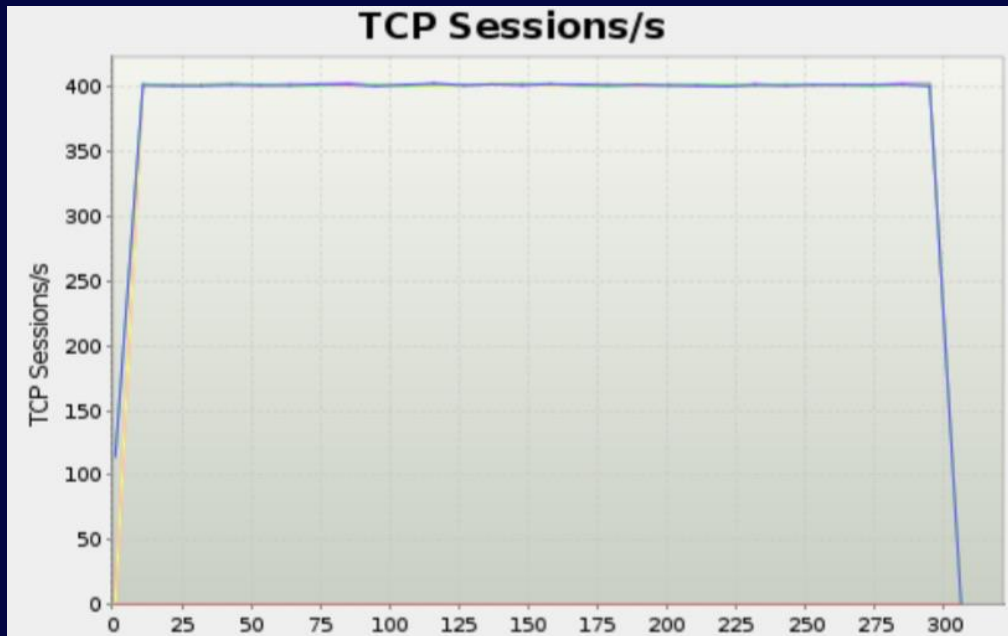
# Скорость открытия новых сессий

825 сессий в секунду – устройство отказывает через 80 секунд



# Скорость открытия новых сессий

400 сессий в секунду – устройство успешно проходит тест



# В чем причина



Количество одновременных сессий 4-го и 7-го уровня на одном и том же устройстве обычно так и отличается – в 10 раз. Второй вариант чаще всего и случается: при выборе отдел закупки смотрит в таблице на самое большое значение СС, а надо было смотреть на самое маленькое.

[Основы выбора NGFW.pdf](#)



Инфотекс

The logo for 'Инфотекс' (Infotek) features the company name in a white, sans-serif Cyrillic font. Above the letter 'о' is a stylized orange graphic consisting of a curved line that ends in a small circle. The background is a dark blue gradient with faint, light blue icons of a circuit board and various network-related symbols like 'NS', 'HS', 'L2', 'TLS', and 'xFW'.