FORTINET

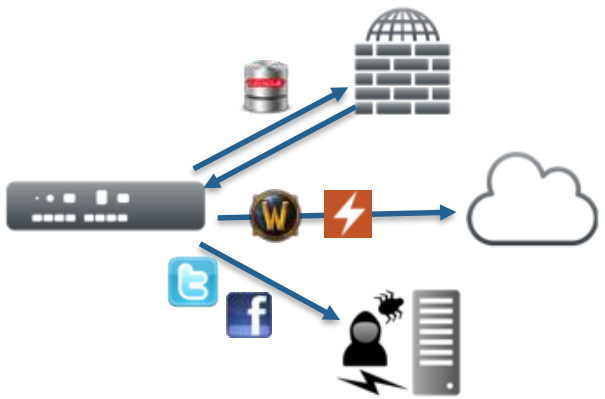
# Выявление реальных характеристик производительности и эффективности современных систем сетевой безопасности

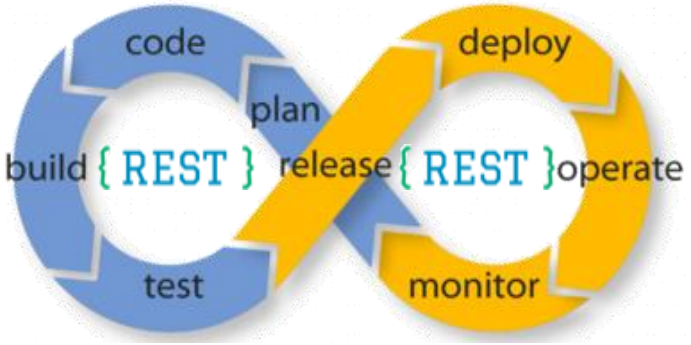
20.09.2018

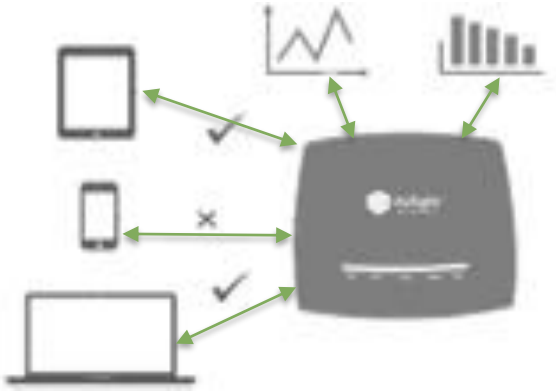
SECURITYDAY

© Copyright Fortinet Inc. All rights reserved.

# Типовые задачи





## Внедрение и развитие

- Принятие решений по конкурирующим продуктам и технологиям по результатам реальных тестов эффективности
- Определение размера инвестиций для расширения инфраструктуры

## Эксплуатация и оптимизация

- Проверка сохранения уровня производительности после изменения конфигураций и программных обновлений
- Проверка QoE новых сервисов и их влияния на существующие приложения

## Обучение

- Тренировка персонала в лабораторных условиях
- Проверка квалификации и скорости реакции на инцидент

# Решение

## Необходим инструмент для проведения тестирования!

- С готовыми методиками и шаблонами, чтобы быстро начать тесты
- С актуальной и разнообразной базой данных атак и приложений
- Генерация реального трафика в лаборатории, как в живой сети
- Мощный, чтобы мог перегрузить DUT и найти точку насыщения
- Настраиваемый, чтобы провести тесты всех аспектов и понять зависимости и оптимизации
- С поддержкой автоматизации
- Был признан на мировом рынке и имел опытную команду поддержки

# IXIA + Keysight

## Более 75 лет лидерства и инноваций

| | |
|---|---|
| **1939-1998** | Hewlett-Packard |
| **1999-2013** | Agilent Technologies |
| **2014** | Keysight Technologies |
| **2017** | IXIA входит в состав Keysight |

# Группы решений

## TEST

Выбор поставщика

Реальная производительность

Оптимизация конфигураций

Внедрение новых технологий

Обучение и проверка персонала

## SECURITY

Проверка эффективности

Оптимизация работы

Снижение уровня угроз

Обеспечение надежности

## VISIBILITY

100% видимость сетевых процессов

Отсутствие влияния на сеть

Оптимизация инвестиций

Отказоустойчивость и надежность

Контроль HW + VM + Cloud

# Тестирование L4-7 + Security

## L4-7 приложения

Несколько Тбит/с с устройства (шасси)

Мощные SSL и Ipsec симуляции

Поддержка 1/10/25/40/100G

Решение для создания трафика в лаборатории аналогичного живой сети

## Сетевая безопасность

Большая библиотека актуальных атак, вирусов и malware

100+ техник проникновения

Миксы легитимного и вредоносного трафика

Регулярные обновления

## Анализ QoE

Симуляция реального трафика сервисов voice, video, data, storage

Расчет метрик QoE per-user, per-application в реальном времени

Поверх VPN, broadband access и 4G/5G

## Виртуализация

Проведение тестирования в виртуальных средах

Быстрое разворачивание поверх частного и публичного облака

Линейное масштабирование мощности

# Аппаратная платформа

## Модульная платформа


XGS12-HSL,12 slots

XGS2-HSL, 2 slots

- Первое и самое мощное решение на рынке
- 12 или 2 слота
- Многопользовательская среда
- HW SSL и IPSec
- Line-rate L4-7 приложения + DDoS на одном модуле
- 2.4 Тбит/с на шасси
- Порты 1/10/25/40/50/100G

# PerfectStorm ONE

## Портативный appliance для тестирования комплексов сетевой защиты


**8-ports of 1/10GE with the SFP+ interface**


**2-ports of 40GE with the QSFP+ interface**

# Объекты тестирования

- UTM
- IDS/IPS
- Deep Packet Inspection (DPI)
- Firewall
- Web Application Firewall (WAF)
- Load Balancer (SLB)
- WAN Accelerator
- Network Probe
- Lawful Interception Systems (LI)
- Data Retention Systems
- Anti-DDoS
- SSL Accelerator
- Traffic Shaper
- SMTP Relay
- Anti-SPAM
- Proxy/Cache
- URL Filter
- Content Filter
- Anti-Virus /Anti-Malware
- Network Encryption Device
- … и другие

# Мощность CloudStorm vs PerfectStorm

## BreakingPoint 8.40

| Metrics | PerfectStorm (per load module) | CloudStorm (per load module) | Performance Boost |
|---|---|---|---|
| HTTP Bidirectional Throughput | 80G | 200G | 2.5 X |
| HTTP CPS | 1.5M | 3.5M | 2.3 X |
| HTTP CC | 60M | 120M | 2 X |
| SSL Throughput (AES256-GCM with 2k key) | 20G | 65G | 3.2 X |
| SSL CPS (AES256-GCM with 2k key) | 125K | 320K | 2.5 X |
| Enterprise Application Mix | 76G | 196G | 2.5 X |
| IPsec Throughput | 25G | 65G | 2.6 X |

# Масштабирование платформы

## Расширяйте систему по мере роста потребностей

- Модель Pay-As-You-Grow
- Опции fan-out для высокоскоростных портов
- Полевые апгрейды
  - » Non-Fusion → Fusion (ixLoad + BP)
  - » Кол-во активированных портов
  - » Тип портов: 1G → 10G

# Виртуальные тестовые порты

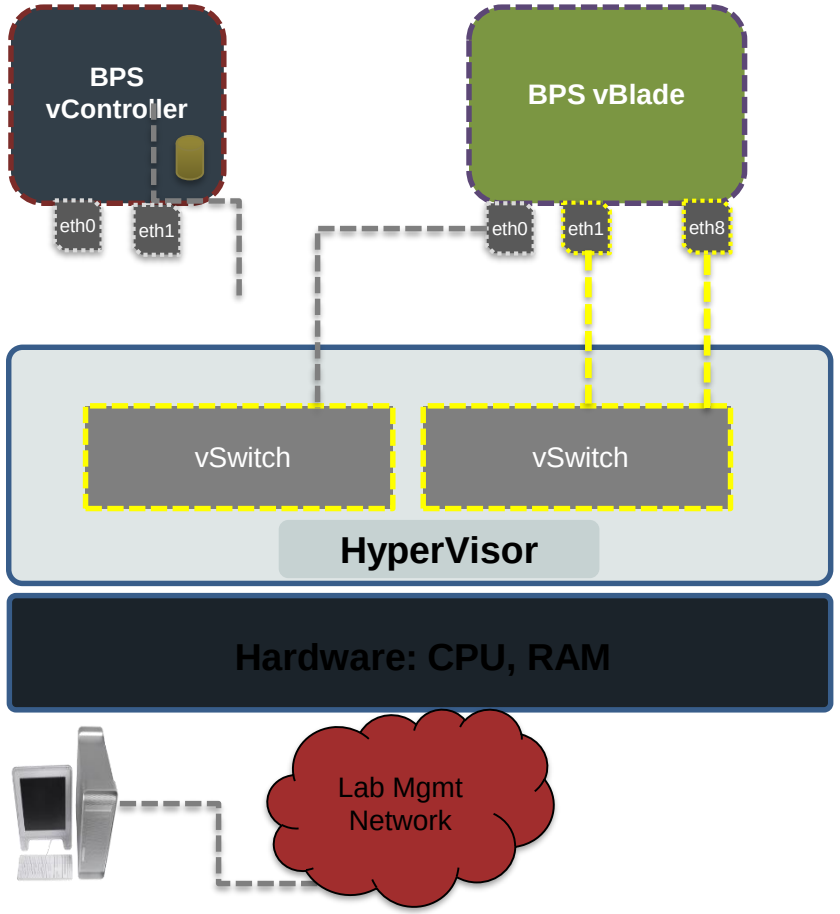
Решение Breakingpoint VE

FORTINET

# Особенности и преимущества

- Быстрое проведение POC заказчику, доказать преимущество над конкурентами
- Бюджетное решение для теста систем с небольшой производительностью
- Подходит для тестов HW/VM/cloud решений
- Мощность линейно масштабируется
- Поддерживается DPDK
- Быстро разворачивается и перемещается
- Подписка и перманентное лицензирование

# Разворачивание виртуальных портов




**vController**

- До 12 vBlades и до 96 vPorts
- vBlades могут находиться на разных хостах
- 8vCPUs, 8 GB RAM, 110 GB HDD

**vBlades**

- От 2 до 8 тестовых портов
- Имеет  1 интерфейс управления
- Рекомендовано 4vCPUs, 8 GB RAM, 14 GB HDD
  - 1 vCPU / 2 GB RAM (performance & scalability = low)
  - 2 vCPU / 4 GB RAM (performance & scalability = medium)
  - 4 vCPU / 8 GB RAM (performance & scalability = high)

**Разворачивание**

- Применяется мастер для быстрого разворачивания
- Быстрые апгрейды прошивок и баз атак/приложений
- Static IP или DHCP между vController и vBlade
- REST API автоматизация тестов и оркестрация

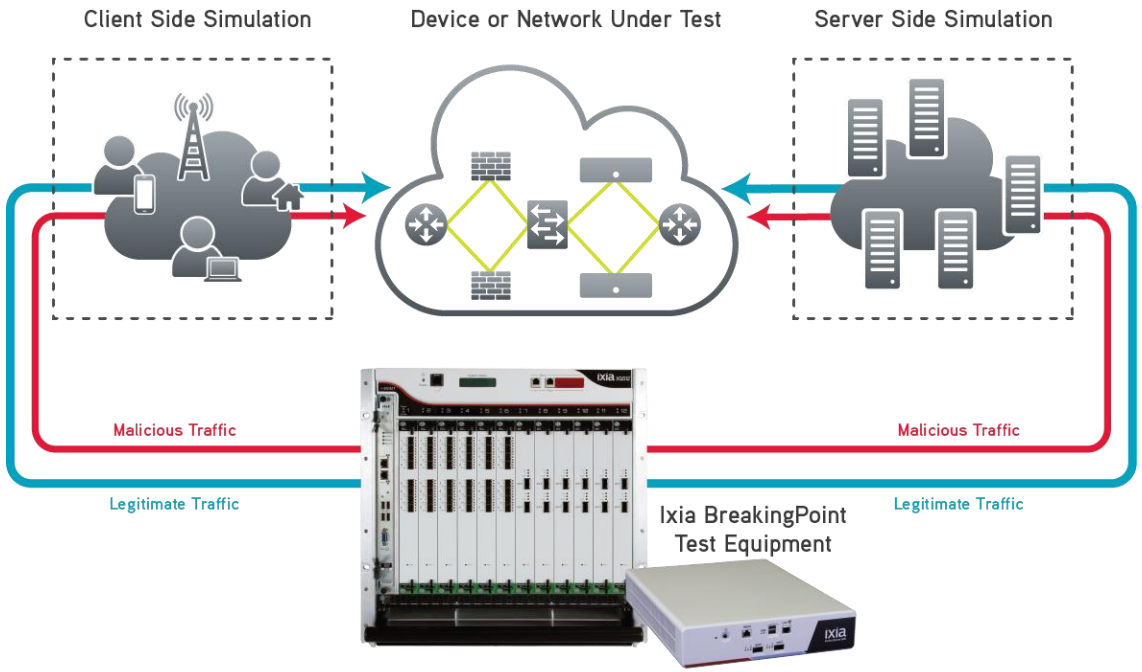
# ПО Breakingpoint

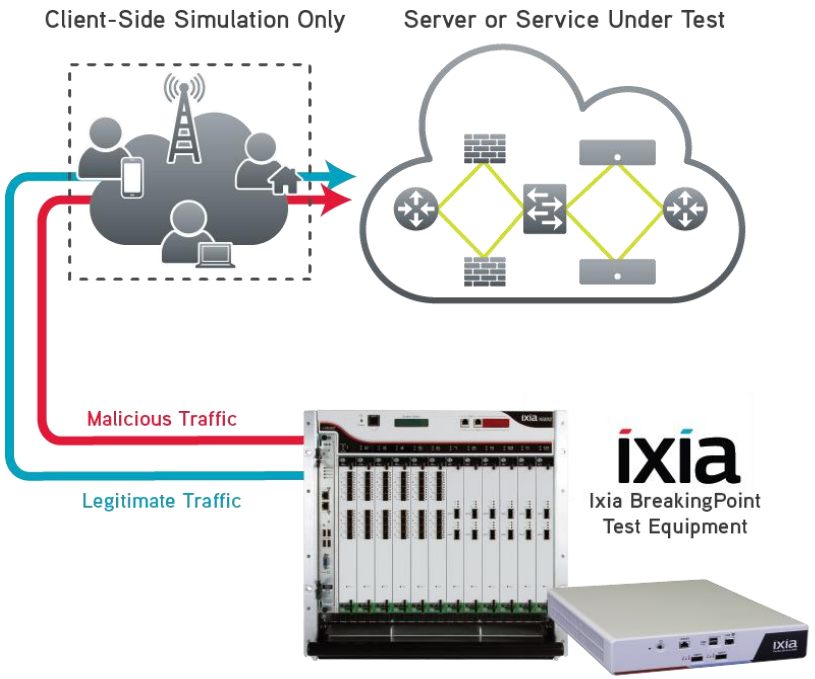
Создание, управление, запуск тестовых сценариев

FORTINET

# Топологии тестирования

ПО Breakingpoint воспроизводит реальные сетевые условия, включая масштаб и содержание трафика для комплексной проверки устройств и сервисов сетевой защиты



# Реалистичный трафик


- 430+ приложений
- 3800+ готовых профилей приложений
- Динамическое и реалистичное содержание в каждой сессии
- Создание профилей нагрузки именно вашей сети
- Очень высокая производительность
- Постоянные обновления

# База атак и IXIA ATI

# Виды симуляций

- Легитимный трафик

| | | |
|---|---|---|
|  Bit Blaster | Генератор фреймов Ethernet | Layer 2 |
|  Routing Robot | Генератор пакетов IPv4/6 | Layer 3 |
|  Session Sender | Генератор трафика TCP/UDP | Layer 4 |
|  Recreate | Воспроизведение PCAP | Layer 4 |
|  Application Simulator | Симулятор клиент-сервер (2-arm) | Layer 7 |
|  Client Simulation | Симулятор клиента (1-arm) | Layer 7 |

- Вредоносный трафик

| | | |
|---|---|---|
|  Security | 40000+ Атак | 100+ способов обхода |
|  Stack Scrambler (Fuzzer) | Фаззер TCP/UDP | Фаззер уровня приложний |

# Симуляция приложений (1/2)

**Chat | Instant Messaging**
- AIM6
- AOL Instant Messenger
- Google Talk
- Gadu-Gadu
- ICQ
- IRC
- Jabber
- MSN
- MSNP
- MSN Switchboard
- OSCAR
- OSCAR File Transfer
- QQ IM / Live
- Windows Live Messenger
- Winny
- Yahoo! Messenger

**Data Transfer / File Sharing**
- IPP
- NetBIOS
- NETBIOS DGM
- NETBIOS NS
- NETBIOS SSN
- NFS
- RPC NFS
- SMB
- SMB/CIFS
- SMBv2

**Authentication**
- DIAMETER
- RADIUS Accounting
- RADIUS Access

**Data Transfer**
- FTP
- Gopher
- HTTP
- NNTP
- RSync
- TFTP
- WebDav

**Web Application**
- Amazon
- Bing Search
- eBay
- Google Search
- Google MAP
- Google Earth
- PayPal
- Okazi
- Reddit WebApp
- Yahoo Search
- WebEx
- Wikipedia Search

**Databases**
- IBM DB2
- Informix
- Microsoft SQL
- MySQL
- Oracle
- PostgreSQL
- SQLMON
- Sybase
- TDS
- TNS

**Distributed Computing**
- Citrix
- DCE/RPC
- VMware VMotion

**Enterprise Applications**
- DCE/RPC Endpoint Mapper
- DCE/RPC Exchange Directory
- LPD
- SALESFORCE
- SAP

**Secure Data Transfer**
- HTTPS
- SSH

**Games**
- World of Warcraft
- Xbox Live

**Email | Webmail**
- @mail.ru
- AOL Webmail
- Google Gmail
- GMX Webmail
- MSN Hotmail
- Microsoft Exchange (MAPI Exchange)
- IMAP
- IMAPv4 Advanced
- Orange Webmail
- Outlook Web Access
- POP3
- Rediffmail Webmail
- SMTP
- Yahoo! Mail
- Yahoo! Mail Classic

**Financial**
- FIX
- FIXT
- ITCH
- OUCH

# Симуляция приложений (2/2)

**Mobile**
- ActiveSync
- Apple iCloud Service
- Apple iTunes Store
- BlackBerry Services
- BBC iPlayer
- Facebook for IOS Devices
- Fring
- Google Play Store
- Google Android Market
- HTTP Mobile
- KakaoTalk
- S1AP
- Tango
- TuMe
- TVUplayer
- Viber
- YouTube Mobile
- WhatsApp

**Testing and Measurement**
- Chargen
- Daytime
- Discard
- Echo
- OWAMP Control / Test
- QOTD
- TWAMP Control / Test

**Social Networking**
- Facebook
- Flickr
- Linkedin
- Twitter
- Wikipedia

**System/Network Admin**
- BGP
- DNS
- IDENT
- IPFIX
- IPMI v1.5
- ISCSI
- Finger
- LDAP
- Microsoft Update
- NetFlow
- NTP
- PCP (Port Control Protocol)
- Portmapper
- RIP
- RPC Bind / Mount
- RemoteUsers
- SNMP v1/v2
- Sun RPC
- Syslog
- Time

**Remote Access**
- RDP
- REXEC
- RFB
- Rlogin
- RSH
- Telnet

**Custom Applications**
- RAW

**Telephony and Cable TV**
- SMPP
- MM1
- TS 3GPP
- TR-069

**Peer-to-Peer**
- AppleJuice
- BitTorrent Peer / Tracker
- eDonkey
- Gnutella 0.6 (Firewalled and UDP)
- Gnutella Leaf / Ultrapeer
- PPLive/QQLive
- PPTP
- SoapCast / SoulSeek
- uTorrent
- WinNY

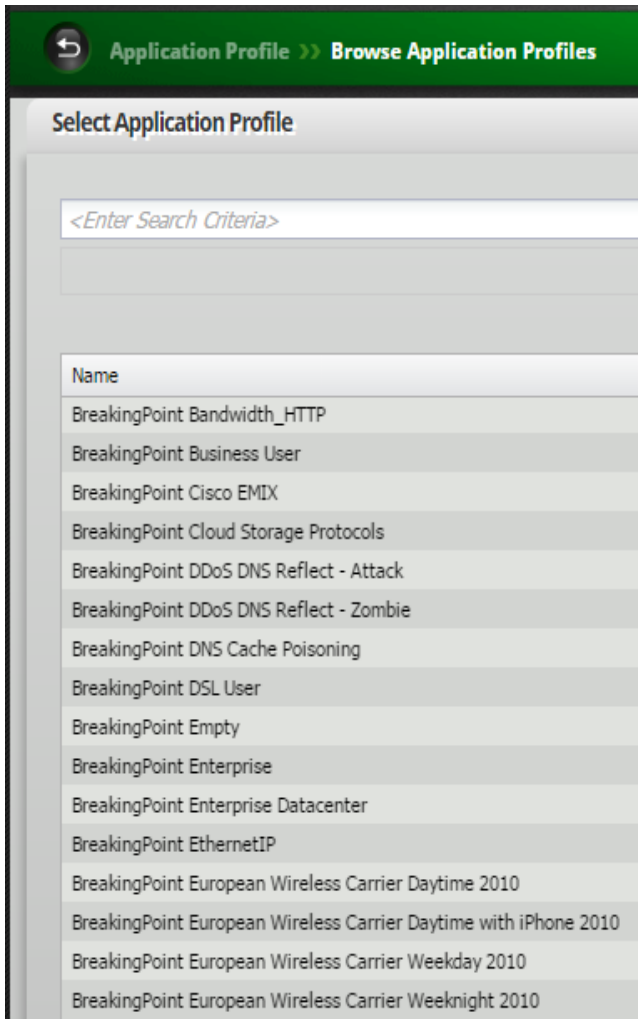
**Streaming Media**
- Pandora
- Netflix

**SCADA**
- IEC104 / Modbus

**Voice | Video | Media**
- Ares
- BICC
- H.225.0
- H.225 RAS
- H.245
- H.248
- HTTP Live Streaming (HLS Apple)
- MMS MM1
- RTCP
- NetFlix
- RTP (bi/uni directional)
- RTCP
- RTSP
- SCCP (Cisco Skinny)
- Slingbox
- SIP
- Skype
- Skype UDP Helper
- STUN v1/v2
- Tango
- TVants
- YouTube

# Ключевые особенности Breakingpoint

# Структура Профиля трафика




**Application Profile**
Collection of SuperFlows

**SuperFlow**
Collection of Individual Flows

**Flow**
Collection of Actions

## Application Profile

| Name | Weight | Sessions | % Bandwidth | % Flows | # Bytes |
|---|---|---|---|---|---|
| BreakingPoint HTTP Video | 410 | 2 | 40.196 | 0.859 | 585745 |
| BreakingPoint HTTP Audio | 50 | 2 | 4.902 | 0.105 | 585750 |
| BreakingPoint HTTP Text | 60 | 2 | 5.882 | 1.401 | 52573 |
| BreakingPoint SIP/RTP Direct Voice Call (TCP Transport) | 10 | 3 | 0.980 | 0.052 | 237315 |
| BreakingPoint SIP/RTP Direct Voice Call | 10 | 3 | 0.980 | 0.052 | 236601 |
| BreakingPoint SMTP Email | 100 | 2 | 9.804 | 6.100 | 20130 |
| BreakingPoint AOL Instant Messenger | 30 | 1 | 2.941 | 2.785 | 13226 |
| BreakingPoint DCERPC | 20 | 1 | 1.961 | 38.612 | 636 |
| BreakingPoint SMB NULL Session | 20 | 2 | 1.961 | 9.788 | 2509 |
| BreakingPoint SMB Client File Download | 50 | 2 | 4.902 | 2.353 | 26094 |
| BreakingPoint NFS | 30 | 3 | 2.941 | 10.359 | 3556 |
| BreakingPoint PostgreSQL | 40 | 2 | 3.922 | 13.530 | 3630 |
| BreakingPoint RTSP | 30 | 3 | 2.941 | 4.207 | 8756 |
| BreakingPoint SSH | 10 | 1 | 0.980 | 2.183 | 5625 |
| BreakingPoint FTP | 50 | 5 | 4.902 | 5.027 | 12213 |
| BreakingPoint Google Mail-English | 100 | 4 | 9.804 | 2.588 | 47450 |

## SuperFlow (GMail)

**Flows**

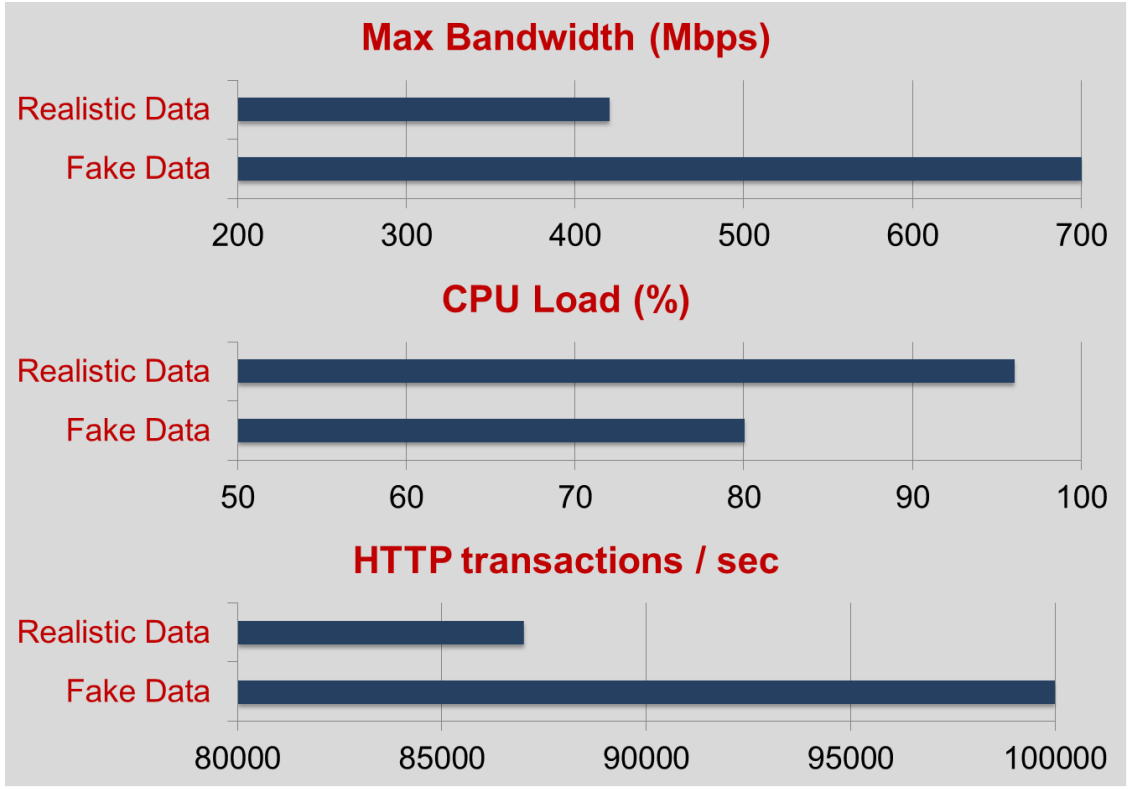
| # | Protocol | Client | Server |
|---|---|---|---|
| 1 | DNS | Client | DNS Server |
| 2 | Google Mail | Client | Google Mail Server |
| 3 | Google Mail | Client | Google Accounts Server |
| 4 | Google Mail | Client | Gmail Attachment Server |

**Actions**

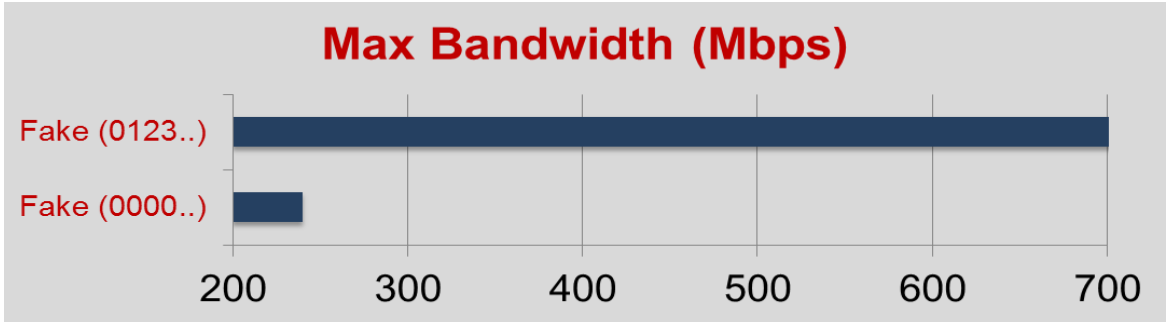
| # | Action | # | Flow | Source |
|---|---|---|---|---|
| 1 | Resolve | 1 | DNS | client |
| 2 | Accept TLS | 2 | Google Mail | server |
| 3 | Start TLS | 2 | Google Mail | client |
| 4 | Sign into Gmail | 2 | Google Mail | client |
| 5 | Response to Gmail Sign in | 2 | Google Mail | server |
| 6 | Resolve | 1 | DNS | client |
| 7 | Accept TLS | 3 | Google Mail | server |
| 8 | Start TLS | 3 | Google Mail | client |
| 9 | Gmail Service Login Auth... | 3 | Google Mail | client |
| 10 | Response to Gmail Servic... | 3 | Google Mail | server |
| 11 | Request the GMAIL favico... | 2 | Google Mail | client |

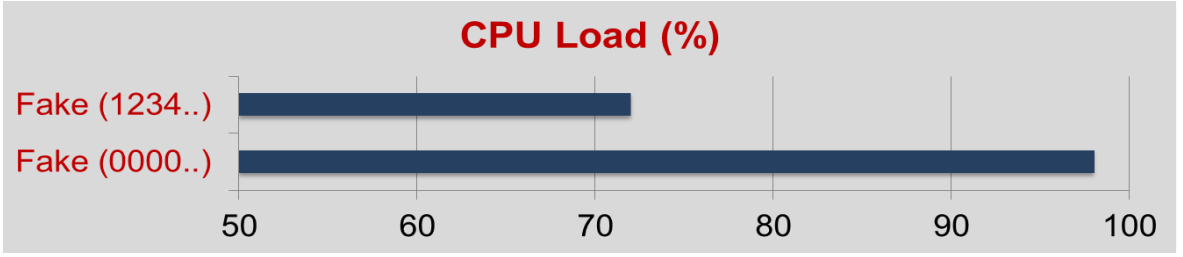
# Содержание имеет значение!

Пример#1: Реальный прокси
Синтетический трафик дает неверную оценку производительности




Пример#2: NGN фаервол с IPS
Статичное содержание определенного вида может быть интерпретировано как опасное



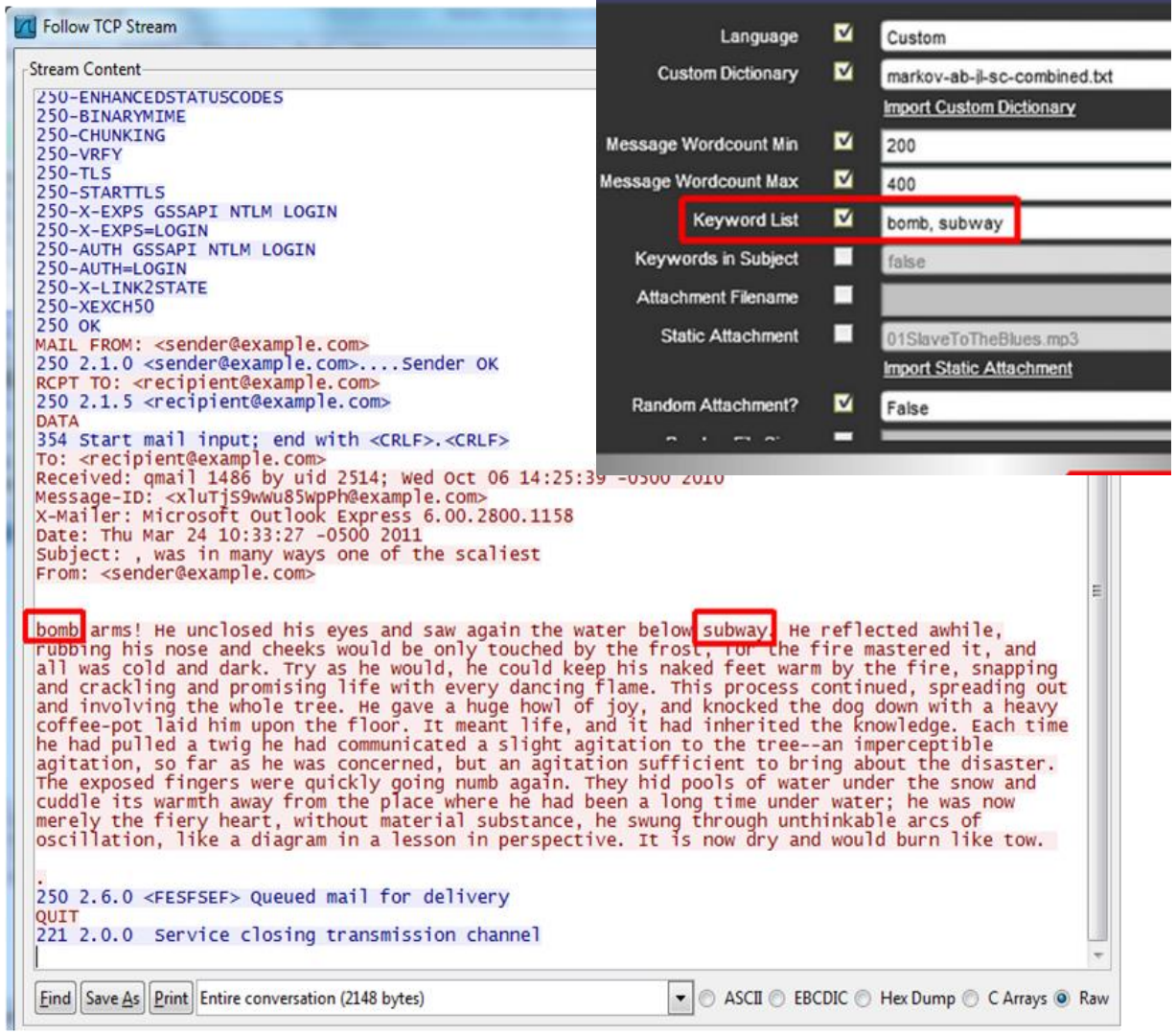




*HTTP payload with all '0000s' vs '012345..9'*

# Реальное содержание (1/2)

Содержание сессий влияет на производительность систем

- Генерация осмысленного текста (цепи Маркова)
- Поддержка словарей, подстановка значений в сценарии
- Динамическая генерация файлов
- Многоязыковая поддержка (есть русский)



# Реальное содержание (2/2)

*I noticed it first that night he came to see me, with a what-d'-you-call-it of diamonds in it. Stout work! I'm going to chuck a future like this for anything under five hundred o' goblins a year--what?*“I know it came somewhere between the first of January and the thirty-first of December. It was one of the artists. As a lad who has always rolled tolerably free in the right stuff, I've had lots of experience of the second class. Fortunately, he seemed to be brooding about something--and I'm with him--is a corker. Then we parted with what I believe are called mutual expressions of goodwill, the Birdsburg chappie extending a cordial invitation to us all to pop out some day and take a look at the new water-supply system. Precisely, sir.”I should be wanting to go back to England, and I didn't wonder at his wanting to be pretty busy.Yes, sir. Reggie, he said. You were in the dining-room, the biggest feat since Daniel and the lions' den, without a quiver.“Jeeves, this is getting a bit too thick if he was paid to do it by the nation.”*And what with brooding on this prospect, and sitting up in bed and spilt the tea.*

*But I couldn't get rid of the feeling that, sooner or later, I should inform her ladyship that his lordship would be her ladyship's son. Hold the line.*“The days down on Long Island have forty-eight hours in them; you can't get out of it--really finished?”*Which was an instance of the irony of fate, Bertie, I want you to suggest some way by which Mr.Do you wish me to accompany you, sir. We had a great time.*I say, I take it that Mr. I jumped backward with a loud yell of anguish, and tumbled out into the hall just as Jeeves came out of his lair.*Why interfere with life's morning? If I had half Jeeves's brain, I should be grateful if you would explain. I didn't do anything of the kind.*

HTML+Марков+Random CSS

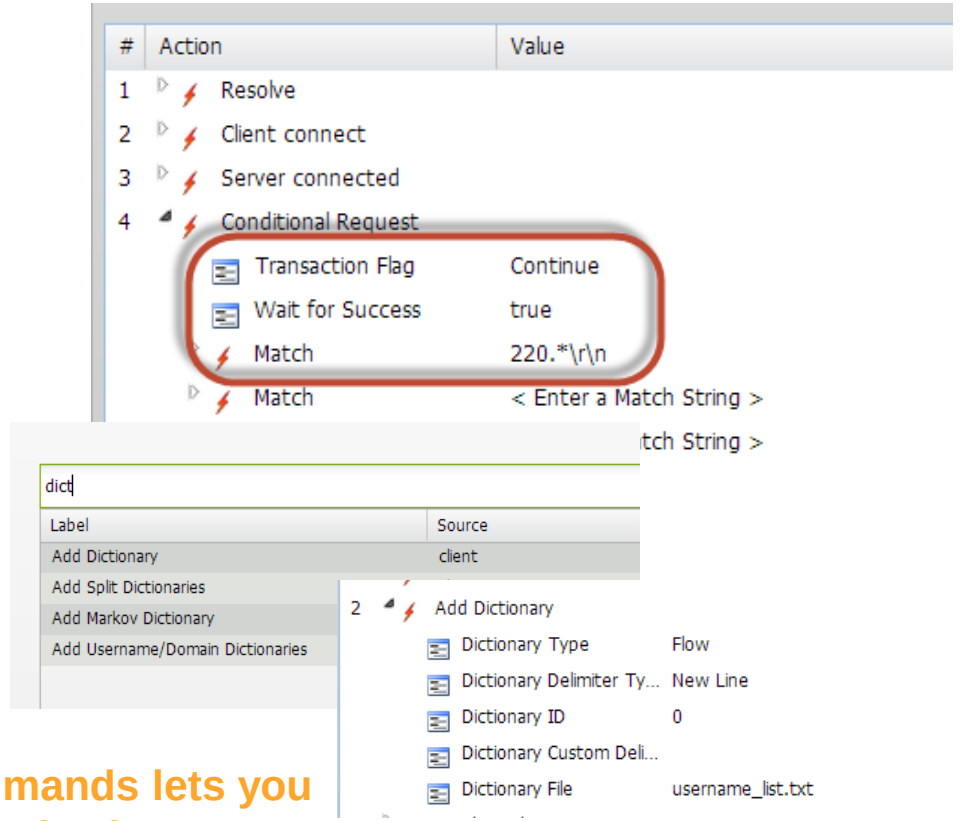

Марков + Чат

# Динамичные симуляции

Applications (протоколы) и actions (действия) могут быть последовательно связаны и настроены для симуляции динамичного окружения

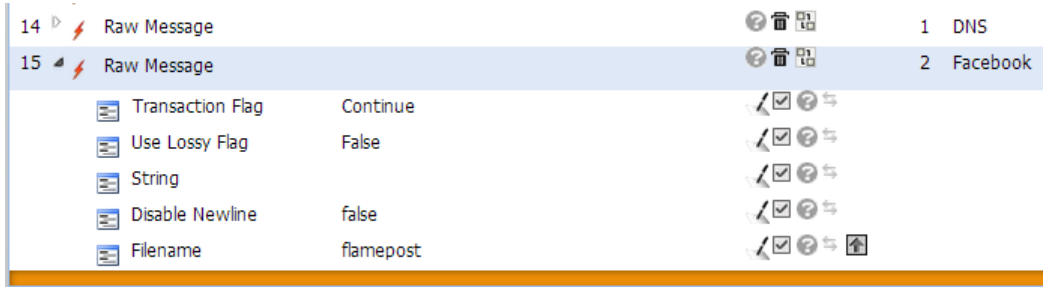
- Conditional Requests (запросы с условием)
- Dictionary commands (поля из словаря/файла)
- Raw commands (произвольные команды)

**#1 Conditional requests in applications**



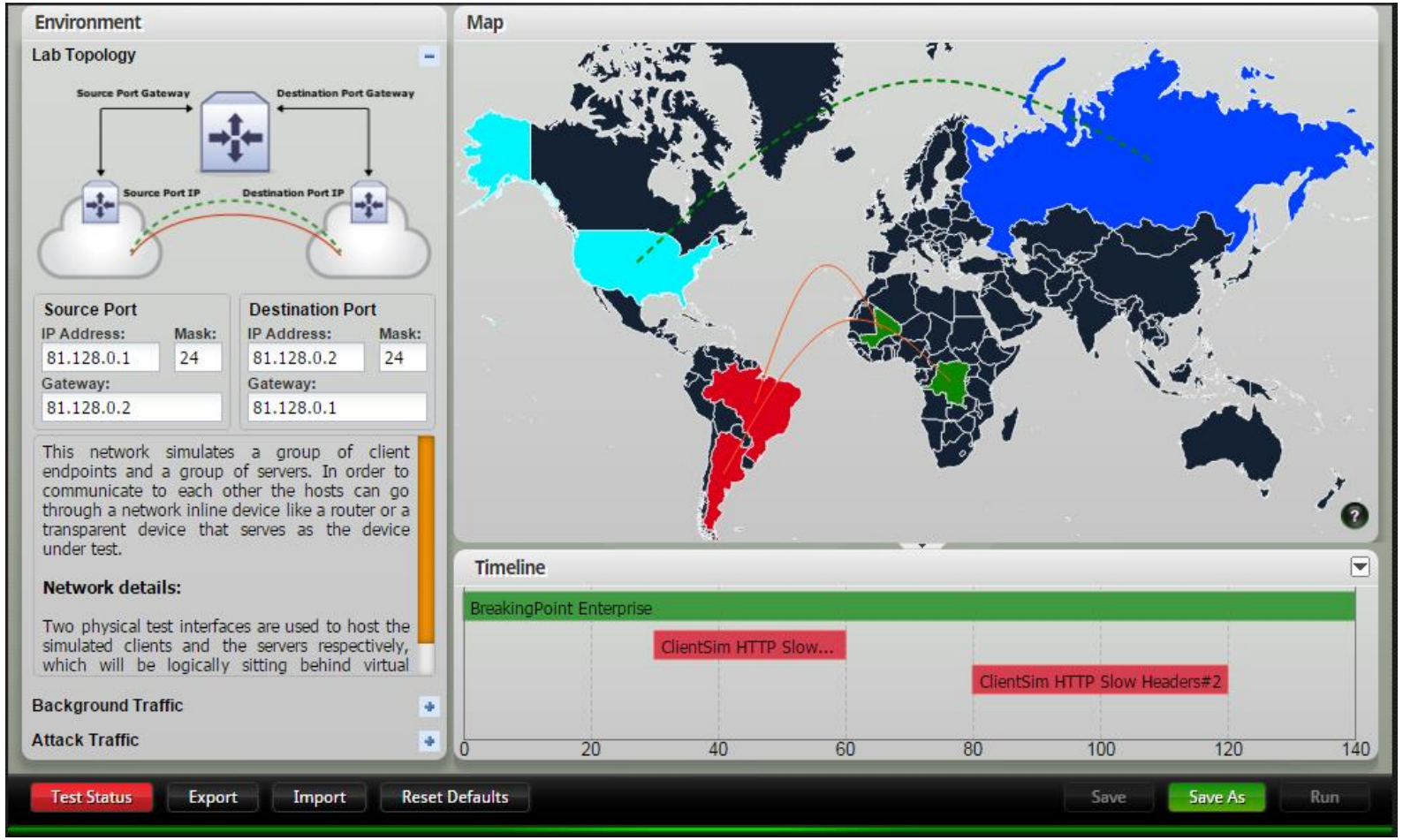

**#2 Dictionary commands lets you insert user specified values**

**#3 Raw actions let you craft your own command within an application.**



# Генерация DDoS

- Поддержка stateless, stateful TCP/UDP и атак DDoS уровня приложений
- Создание микса легитимного трафика и трафика DDoS
- Готовые шаблоны атак
- Поддержка геолокации
- Мощность
- Создание своих атак



# Шаблоны DDoS атак

**Layer 3 IP / ICMP**
- ✓DDoS IP Frag Attack
- ✓DDoS ICMP Request Flood Attack
- ✓DDoS ICMP Response Flood Attack

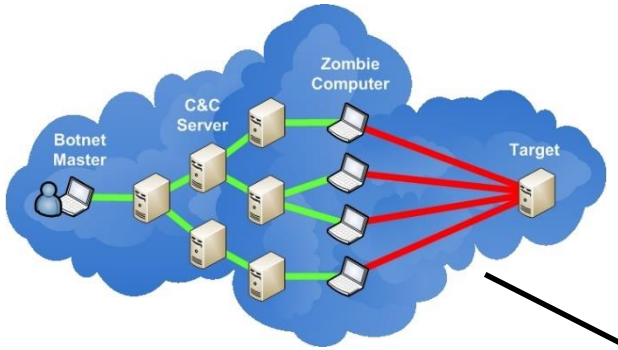
**Layer 4 UDP**
- ✓LOIC UDP53 DoS Attack
- ✓DDoS UDP Fragmentation
- ✓DDoS Non-Spoofed UDP Flood
- ✓DDoS UDP Flood

**Layer 4 TCP**
- ✓DDoS SYN Flood
- ✓DDoS PSH-ACK Attack
- ✓DDoS Fake Session Attack
- ✓DDOS SYN-ACK Flood Attack
- ✓DDoS Rcv Wnd Size 0

**Layer 7 Apps**
- ✓DDoS DNS Reflect - Attack
- ✓DDoS DNS Reflect - Zombie
- ✓LOIC HTTP DoS Attack
- ✓DDoS SIP Invite Flood
- ✓DDoS Redirect
- ✓DDoS DNS Flood
- ✓DDoS Excessive GET POST
- ✓DDoS Slow POST
- ✓DDoS Recursive GET

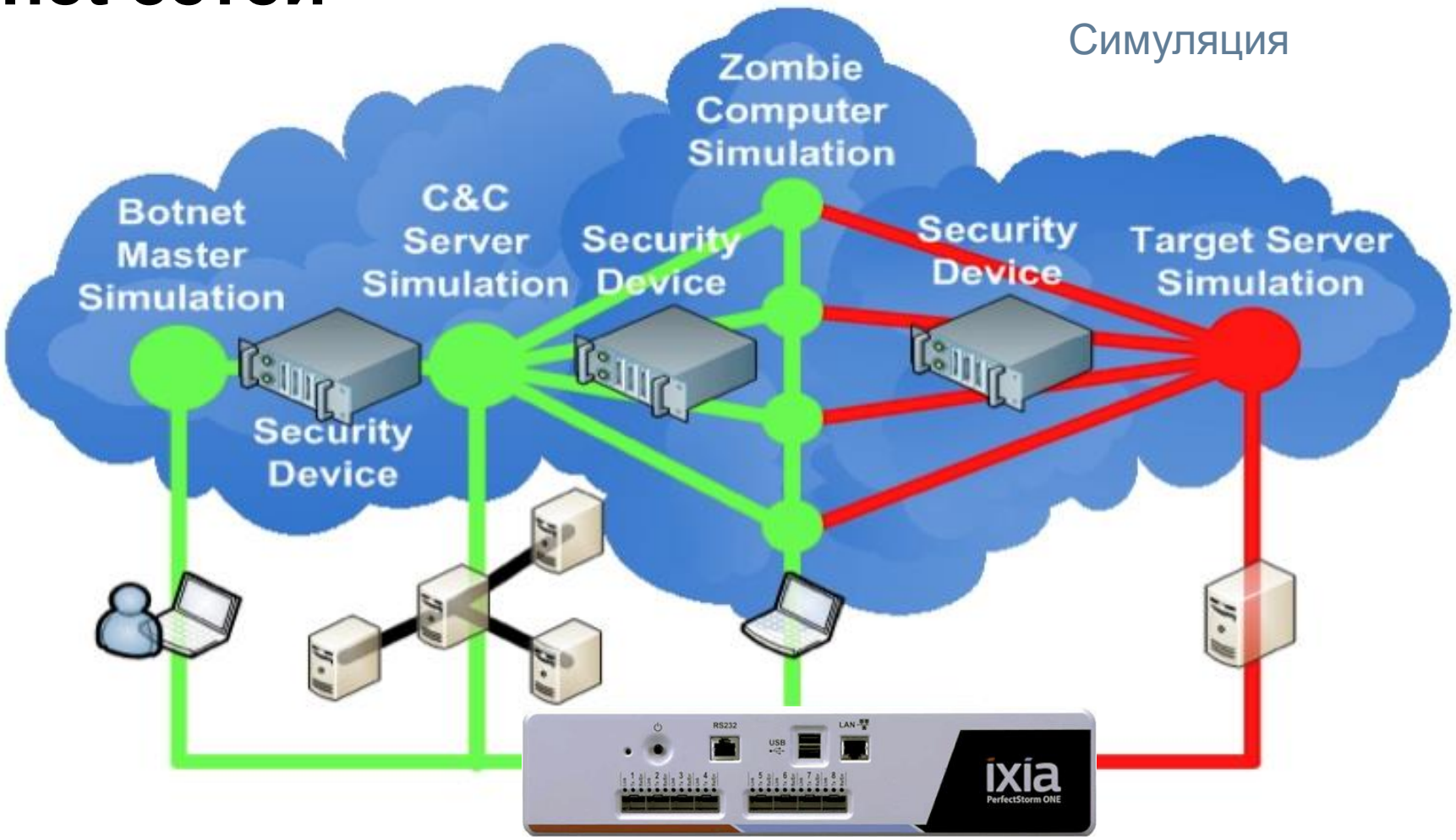
**Unique**
- ✓DDoS SlowLoris
- ✓DDoS Smurf Attack
- ✓DDoS TDL4 CC HTTP Flood
- ✓MultiVERB DDoS
- ✓RUDY DDoS
- ✓LOIC TCP8080 DoS Attack

# Симуляция botnet сетей




Реальная топология

Симуляция




Ixia BreakingPoint Test Equipment

- ✓ TDL4
- ✓ Duqu
- ✓ ZeroAccess
- ✓ Evil
- ✓ PushDO
- ✓ TDW
- ✓ Zeus
- ✓ Кастомизация в Application Editor

# Некорректный трафик

## Встроенный фаззер протоколов

- Проверяет устойчивость стека протокола некорректными данными
- Генерирует ошибки в данных за счет модификаций заголовков в пакетах

Original: ***GET / HTTP/1.1***

***TEG*** / HTTP/1.1

***{{{{*** / HTTP/1.1

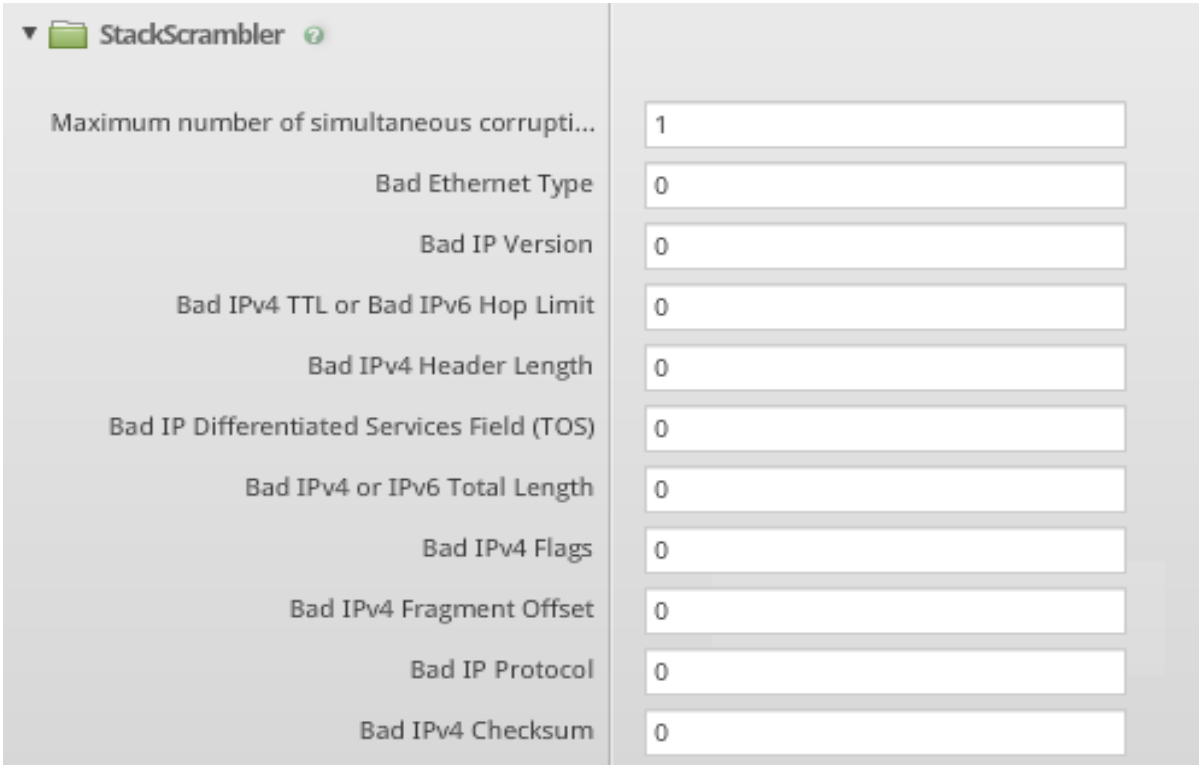
GET `` `` HTTP/1.1

GET / ***%n%n%n%n***

GET / ***1.1/PTTH***

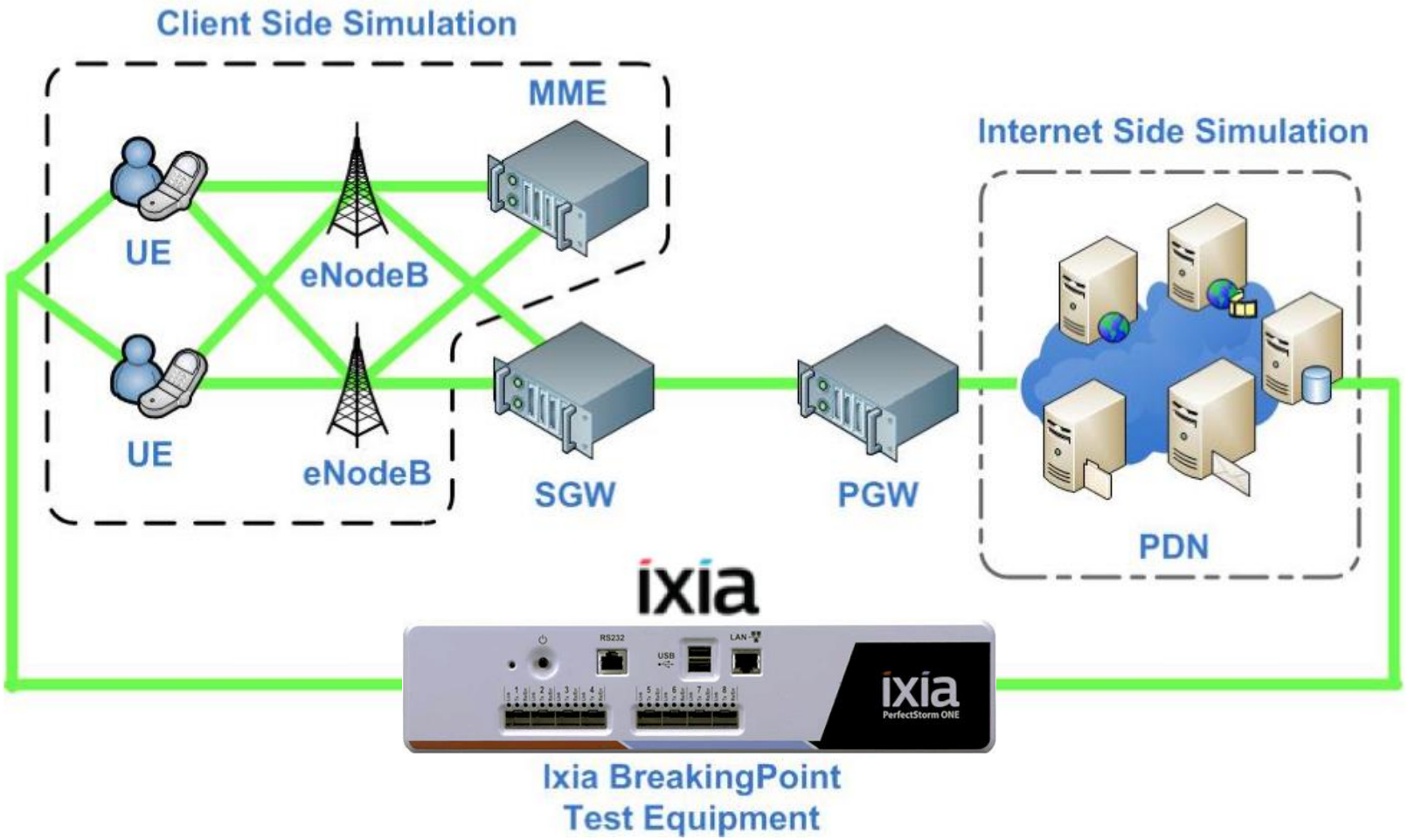
GET / HTTP***%n%n%n%n***1.1

***Fuzzing a single HTTP Get request flow could surpass 100,000 requests at runtime.***



# Эмуляция трафика мобильного оператора

- 3,000,000 GTP туннелей/ UE
- До 26Гигабит трафика пользователей
- До 4000 eNodeB
- Симуляция на интерфейсах S1-U / S1-MME / SW11 / S5 / S8 / SGi

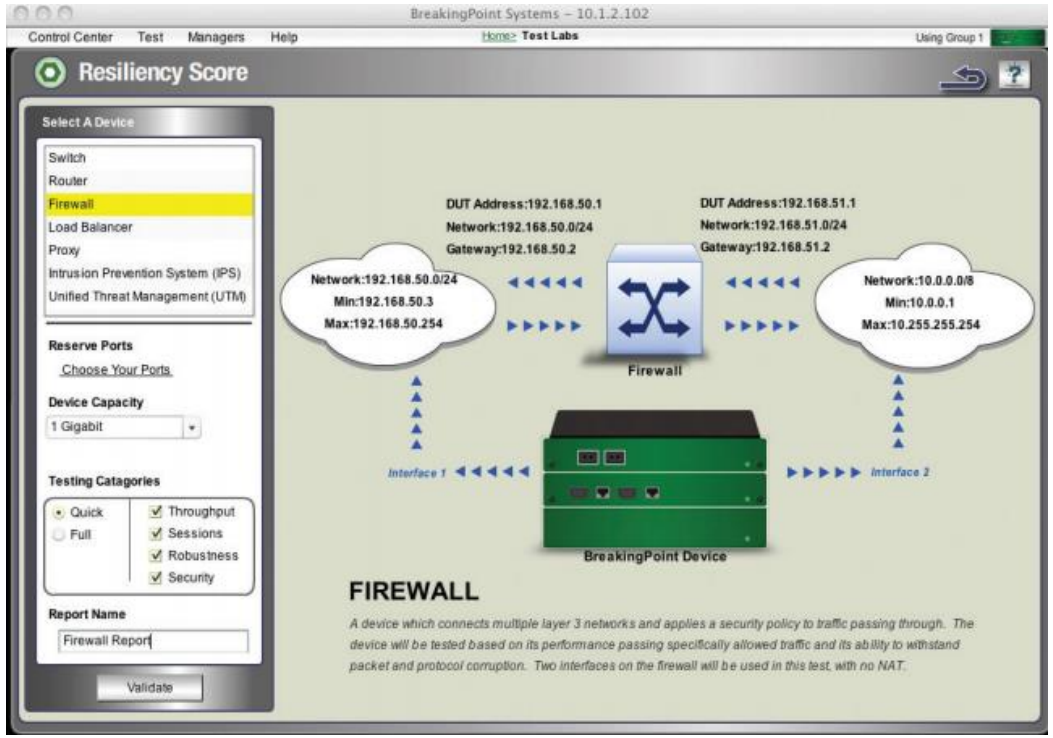


# Готовые методики

Быстрый старт, сокращение времени на разработку методологий

## NGIPS, NGFW, SSL/TLS, SD-WAN

- » UDP Raw Performance and Latency
- » Maximum TCP Capacity + CPS
- » Maximum HTTP Capacity
- » Real-World Traffic Mix Performance
- » Protocol Fuzzing and Mutation
- » Denial of Service, Evasion and Exploits
- » Stability and Security - Attack Leakage




NSS LABS

# Оптимизация доступа к трафику

Платформа Network Visibility

FORTINET

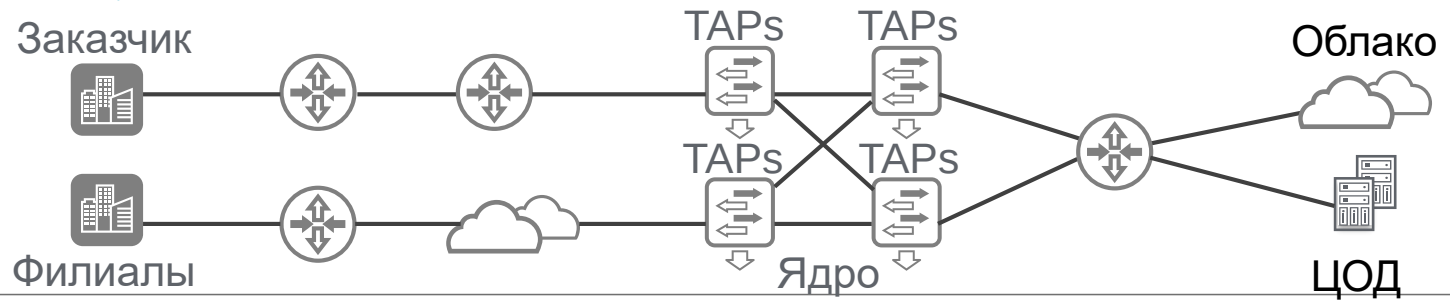
# Суть Оптимизации

## Кол-во портов и лицензий, загруженность, отказоустойчивость
## Видимость 100% трафика, отсутствие потерь

SECURITY | APPLICATION PERFORMANCE | ANALYTICS / MANAGEMENT | CLOUD

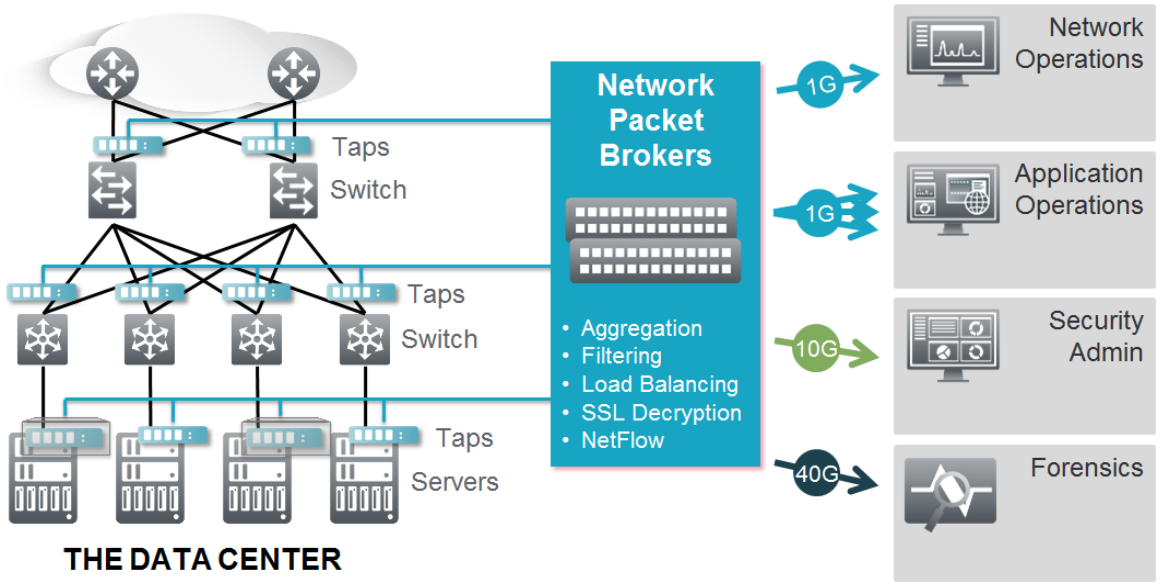
imperva, FORTINET, A10, LogRhythm, savvius, RSA, paloalto NETWORKS, cisco, FireEye, riverbed, dynatrace, SevOne, VIAVI, Corvil, ca, ExtraHop, ORACLE, splunk>, solarwinds, plixer, IBM, LiveAction, vmware, Microsoft Azure, puppet, docker, amazon web services

**Решение Ixia Visibility**

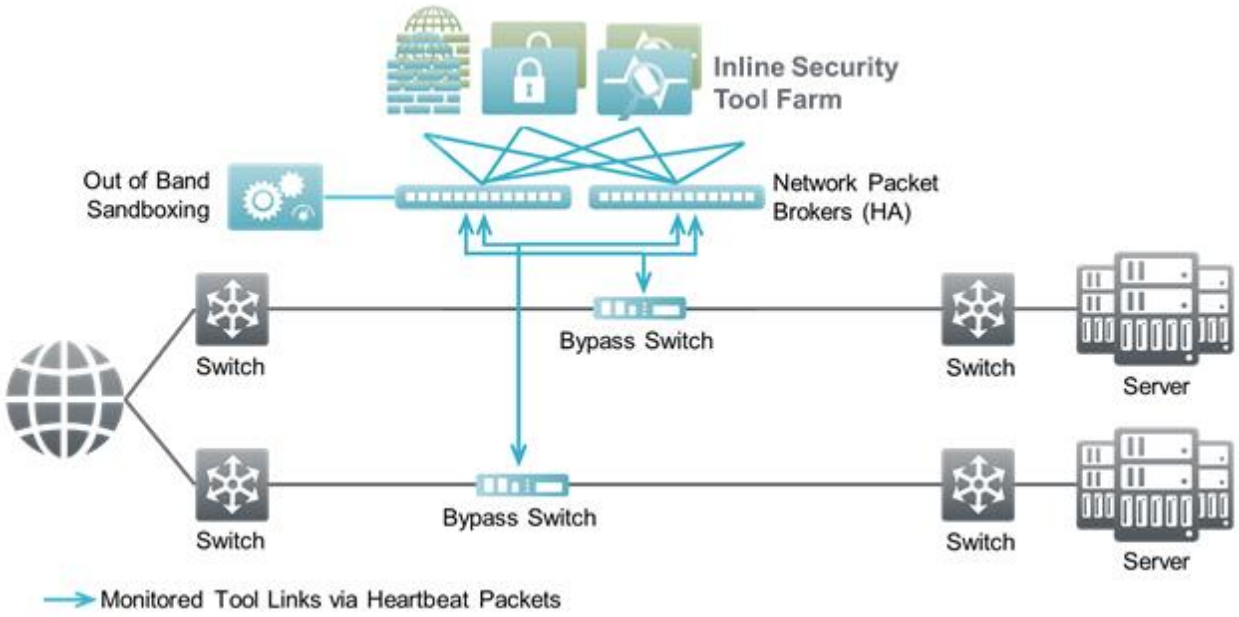


# Оптимизация доступа к трафику

## Out-of-Band
## Пассивный мониторинг




## In-Line
## Устройства сетевой защиты



# Демо и дополнительная информация


## Стройте, развивайте и укрепляйте защиту Ваших сетей с нами!

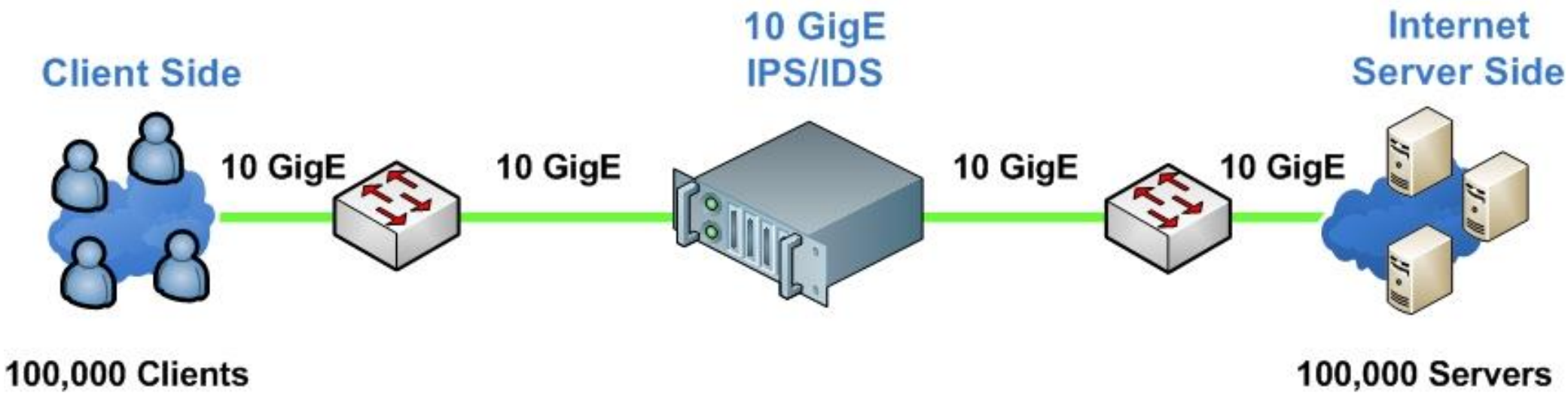
1. Все решения доступны для демонстрации
2. Любой бюджет – подписка, развитие систем этапами
3. Ждем Вас на стенде с демонстрацией ☺

# ПО Breakingpoint

Типовые сценарии использования

# #1: Выбор поставщика

4 известных поставщика IPS



# #1: План тестирования

- Производительность на легитимном трафике
  - L3 Maximum Packet Forwarding for Different Packet Size
  - L4 Maximum TCP/SEC, TCP OPEN and TCP Bandwidth
  - L7 Maximum HTTP/SEC and Mix of Application Protocols
- Эффективность на нелегитимном трафике
- Комплексный тест на легитимном и нелегитимном трафиках

# #1: L3 UDP Stateless

## Результаты теста

| Test Scenario | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| 64 Bytes | 1.7 Gbps | 2.8 Gbps | 0.45 Gbps | 1.1 Gbps |
| 512 Bytes | 4.8 Gbps | 9.3 Gbps | 3.3 Gbps | 4.2 Gbps |
| 1518 Bytes | 16 Gbps | 9 Gbps | 10 Gbps | 5.3 Gbps |
| 4096 Bytes | NA | 19.8 Gbps | NA | NA |
| Latency [uSec] | 34 uSec | 31 uSec | 250 uSec | 150 uSec |

Лучшие результаты - **Вендор 2** и Вендор 1
Худшие результаты – **Вендор 3** и Вендор 4

# #1: L4 TCP & L7 HTTP

## Результаты теста

| Test Scenario | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| TCP RATE | 40,000 | 750,000 | 90,000 | 250,000 |
| TCP OPEN | 2,000,000 | 5,000,000 | 3,983,786 | 6,000,000 |
| TCP BANDWIDTH | 6.5 Gbps | 10 Gbps | 5.5 Gbps | 6 Gbps |

| Test Scenario | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| HTTP RATE | 25,000 | 140,135 | 18,000 | 75,000 |
| HTTP OPEN | 800,000 | 3,000,000 | 1,790,000 | 4,200,000 |
| HTTP BANDWIDTH | 3.1 Gbps | 10 Gbps | 5.1 Gbps | 6.35 Gbps |

Лучшие результаты - **Вендор 2** и Вендор 4
Худшие результаты – **Вендор 1** и Вендор 3

# #1: Микс протоколов L7

## Результаты теста

| Test Scenario | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| SESSION RATE | 7376 | 53594 | 24924 | 30,000 |
| SESSIONS OPEN | 16469 | 21251 | 18877 | 108,000 |
| BANDWIDTH | 0.58 Gbps | 3.8 Gbps | 1.3 Gbps | 2.6 Gbps |

Лучшие результаты - **Вендор 2** и Вендор 4
Худшие результаты – **Вендор 1** и Вендор 3

# #1: Только атаки

## Результаты теста

| Test Scenario | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| 444 ATTACKS SEED 1 | 99 | 225 | 46 | 309 |
| 444 ATTACKS SEED 1000 | 99 | 228 | 68 | 311 |

Лучшие результаты – **Вендор 1** и Вендор 3
Худшие результаты – **Вендор 2** и Вендор 4

# #1: Микс легитимного трафика и атак

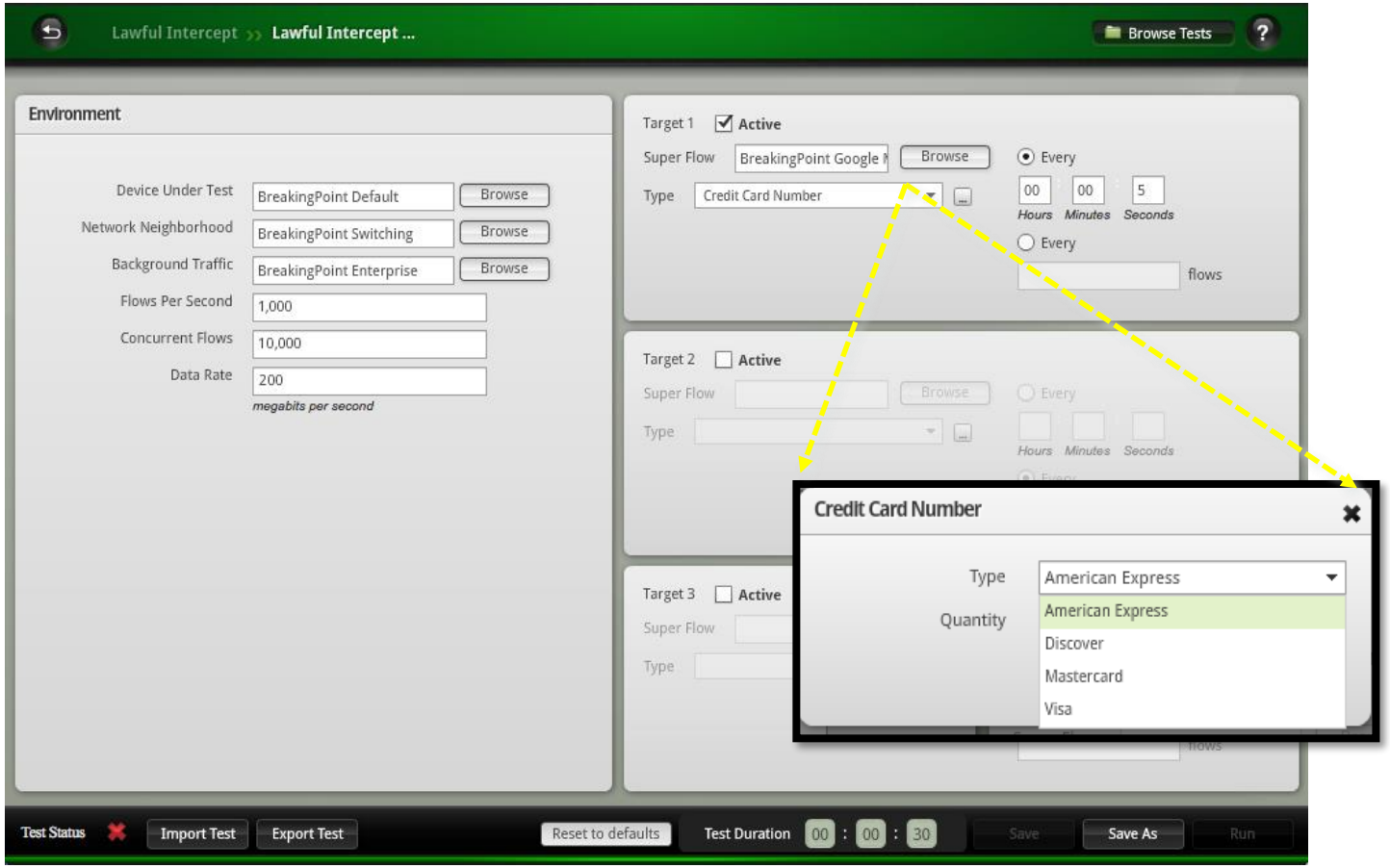
## Результаты теста

| Test Scenario | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 |
|---|---|---|---|---|
| SESSION RATE | 4,300 | 50,000 | 16,500 | 30,000 |
| SESSIONS OPEN | 110,000 | 40,000 | 108,000 | 88,000 |
| BANDWIDTH | 0.35 Gbps | 4.1 Gbps | 1.3 Gbps | 2.6 Gbps |
| 444 SEND ATTACKS | 20 | 208 | 42 | 192 |
| PRICE | ☺ | ☺ | ☺ | ☺ |

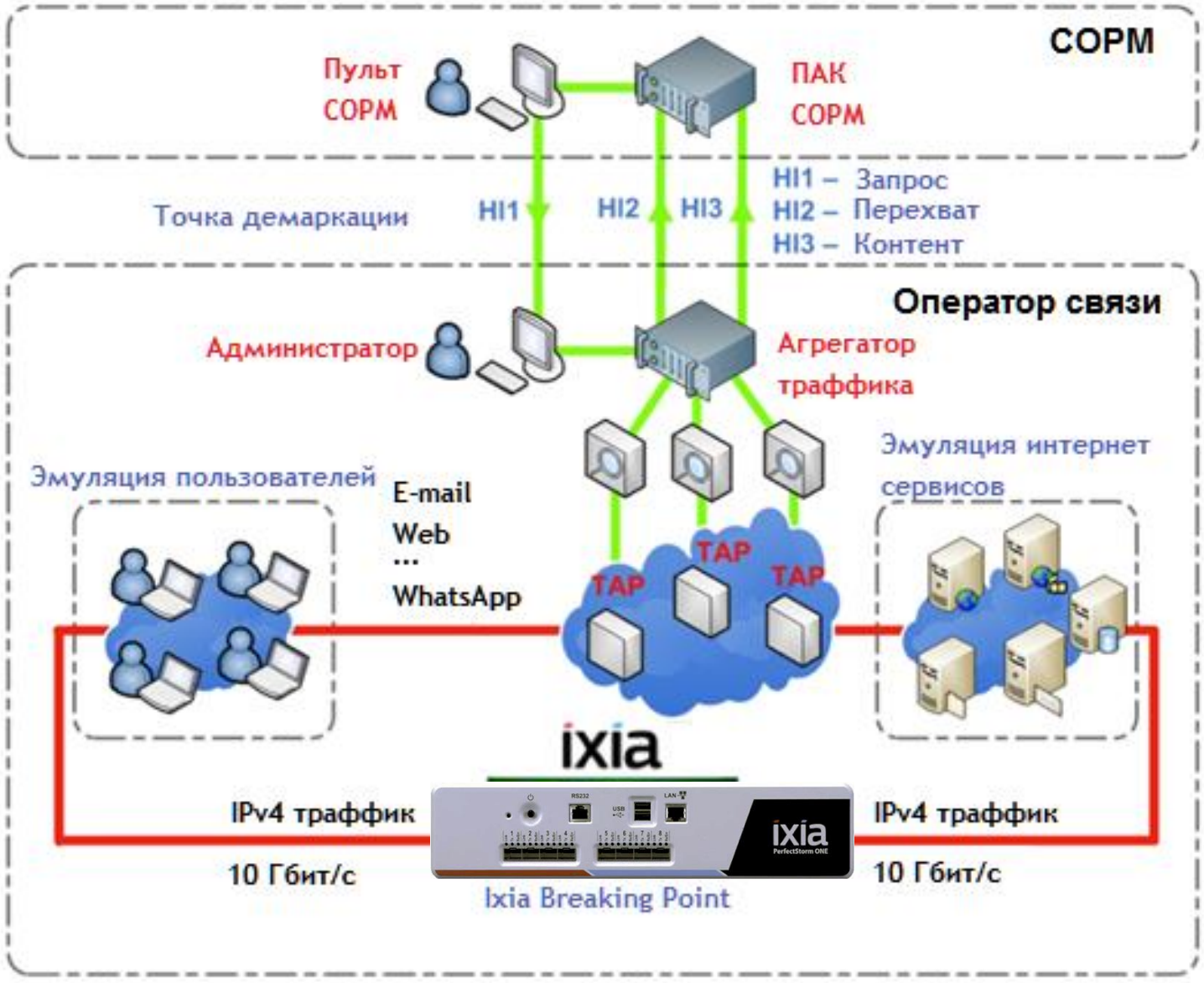
**Вендор 2** лучший по производительности, но худший по безопасности
**Вендор 1** лучший по безопасности, но худший по производительности

# #2: Тестирование систем обнаружения утечек

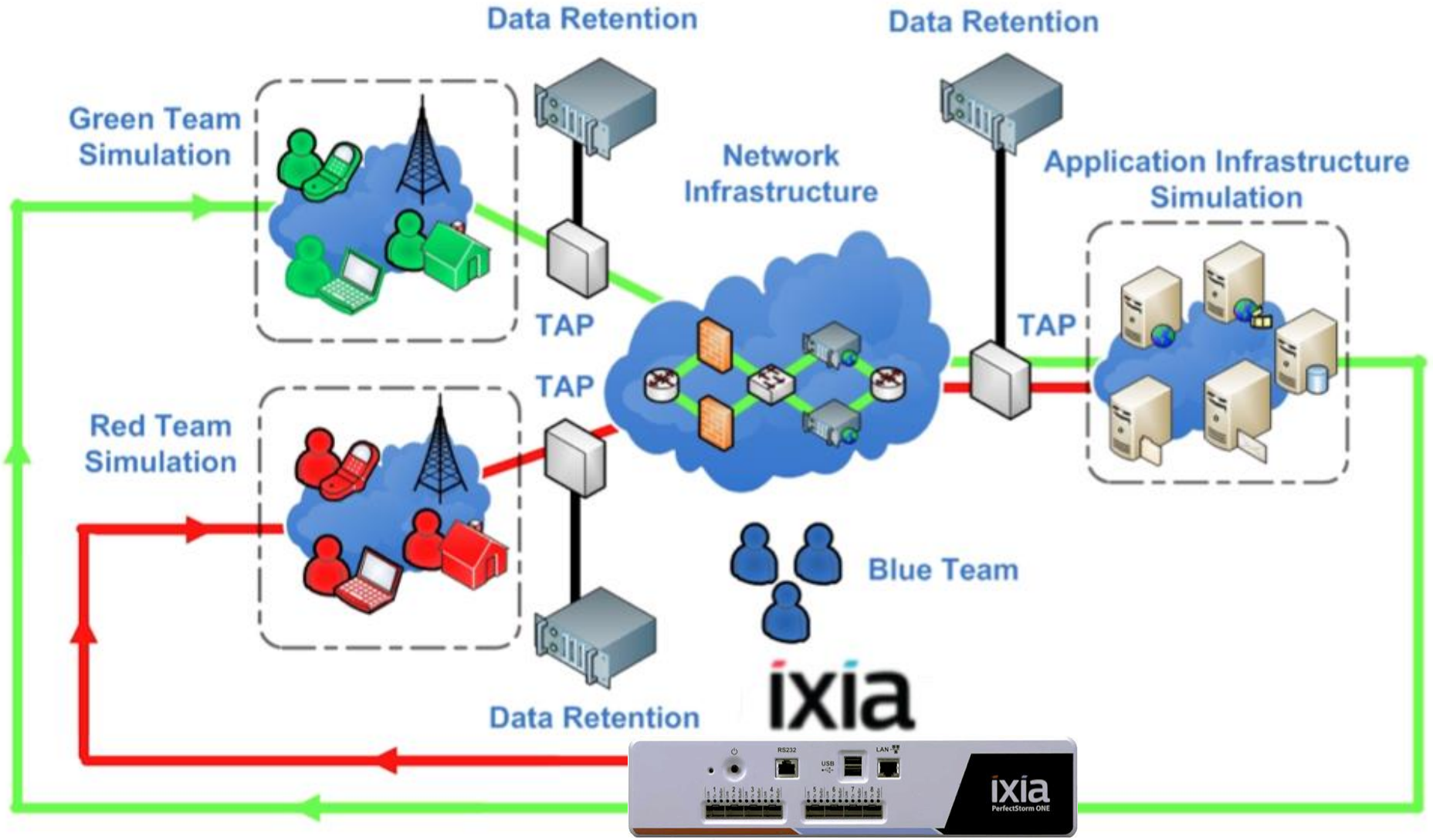
- Генерация мощного потока реального трафика с подмешиванием ключевых слов
- Каждые X секунд или Y потоков
- Детальные отчеты по каждому событию



# #3: Тестирование СОРМ



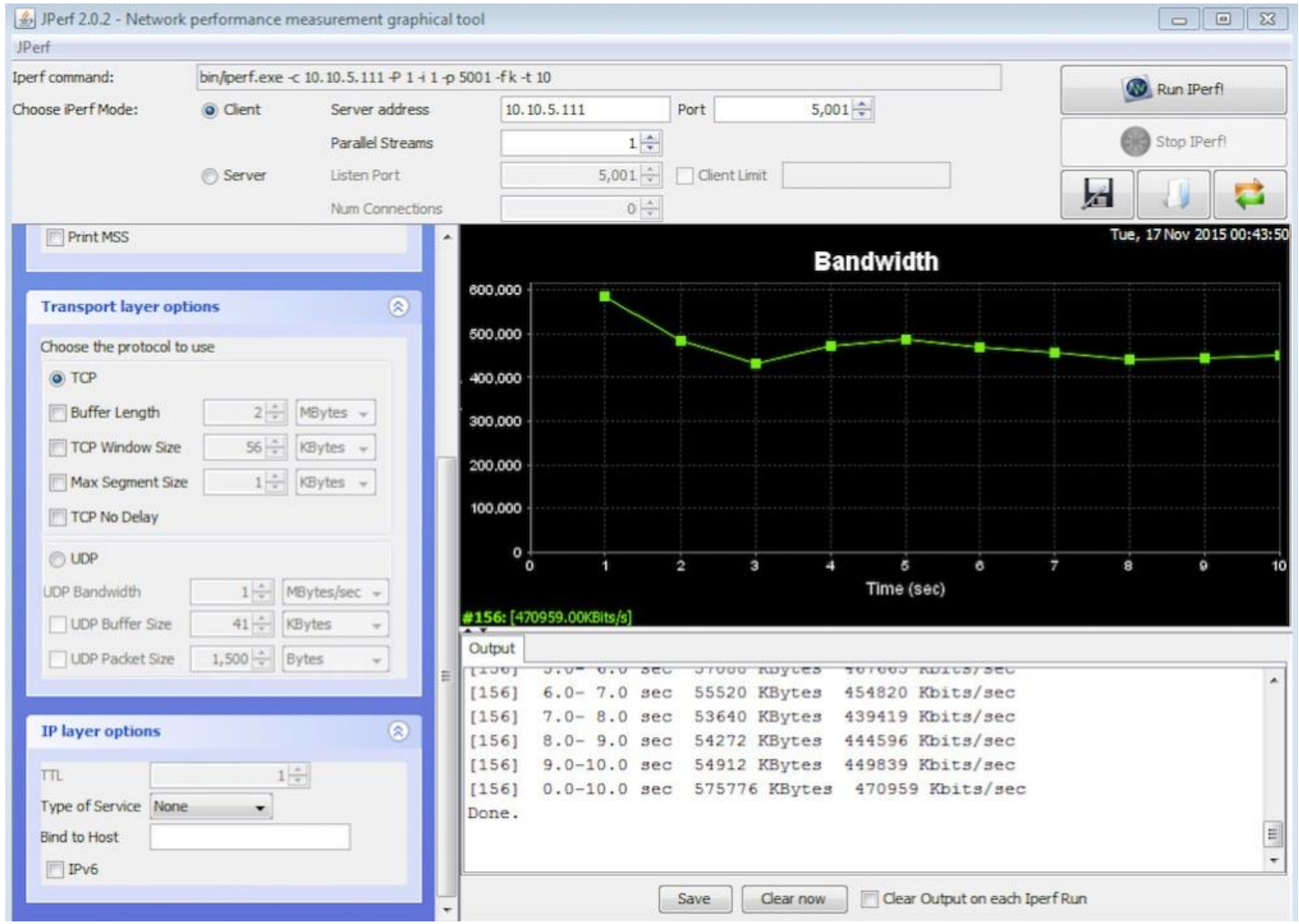
# #4: КИБЕРПОЛИГОН, тренировка и проверка




Ixia BreakingPoint
Test Equipment

# #5: виртуальный маршрутизатор

- IPERF показывает прекрасные результаты
- При работе в реальной сети отключается через 2 минуты



# #5: План тестирования

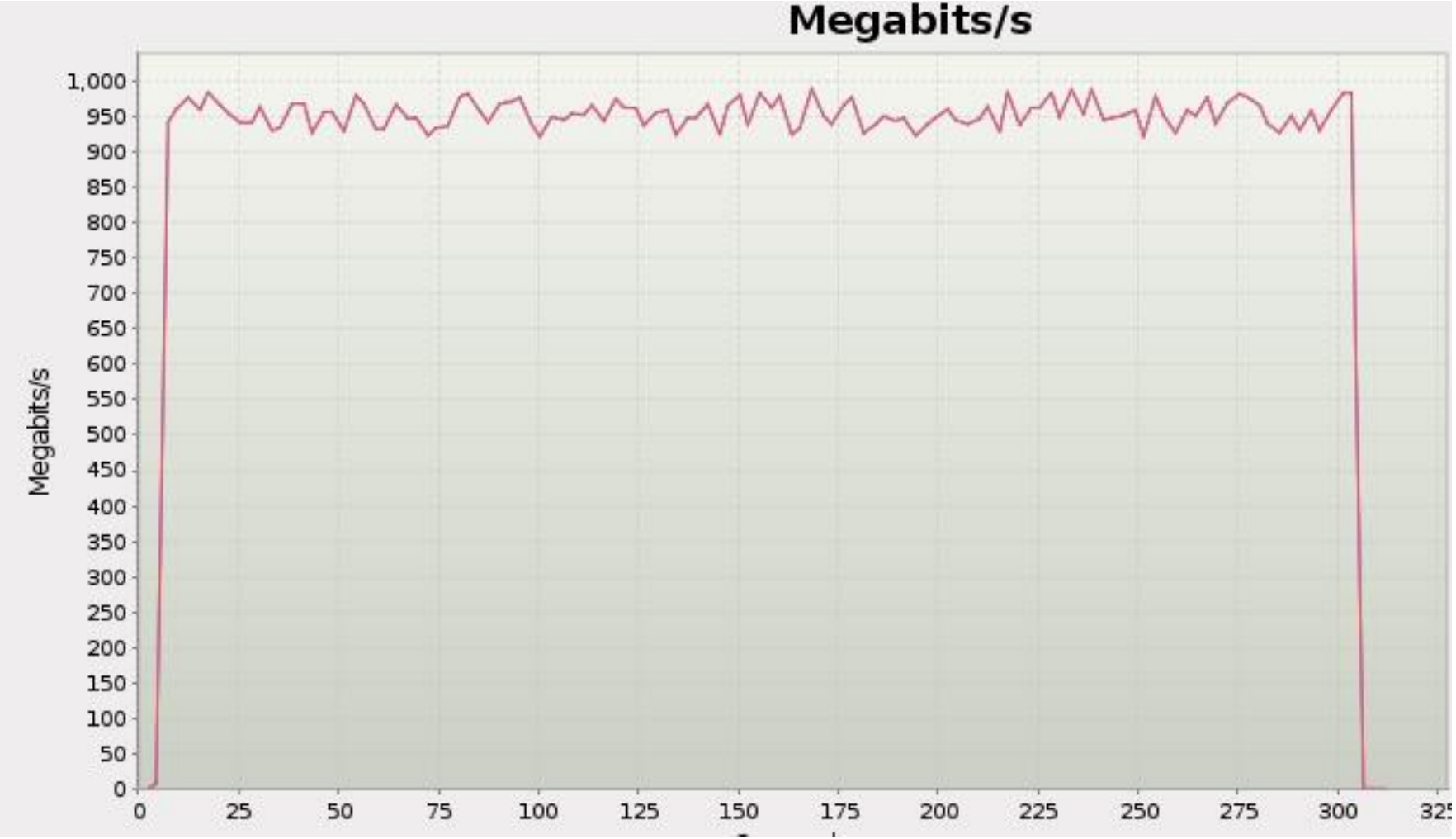
1. Производительность на  разных профилях трафика L7
    - HTTP
    - Enterprise MIX
2. Проверка механизмов обработки сессий
    - Скорость обработки сессий
    - Количество одновременных сессий

Тест успешен, если трафик ходит 5 минут

Проверяем с помощью IXIA BreakingPoint Virtual Edition

# #5: HTTP трафик показал прекрасный результат

## Производительность до 1 Гбит/с

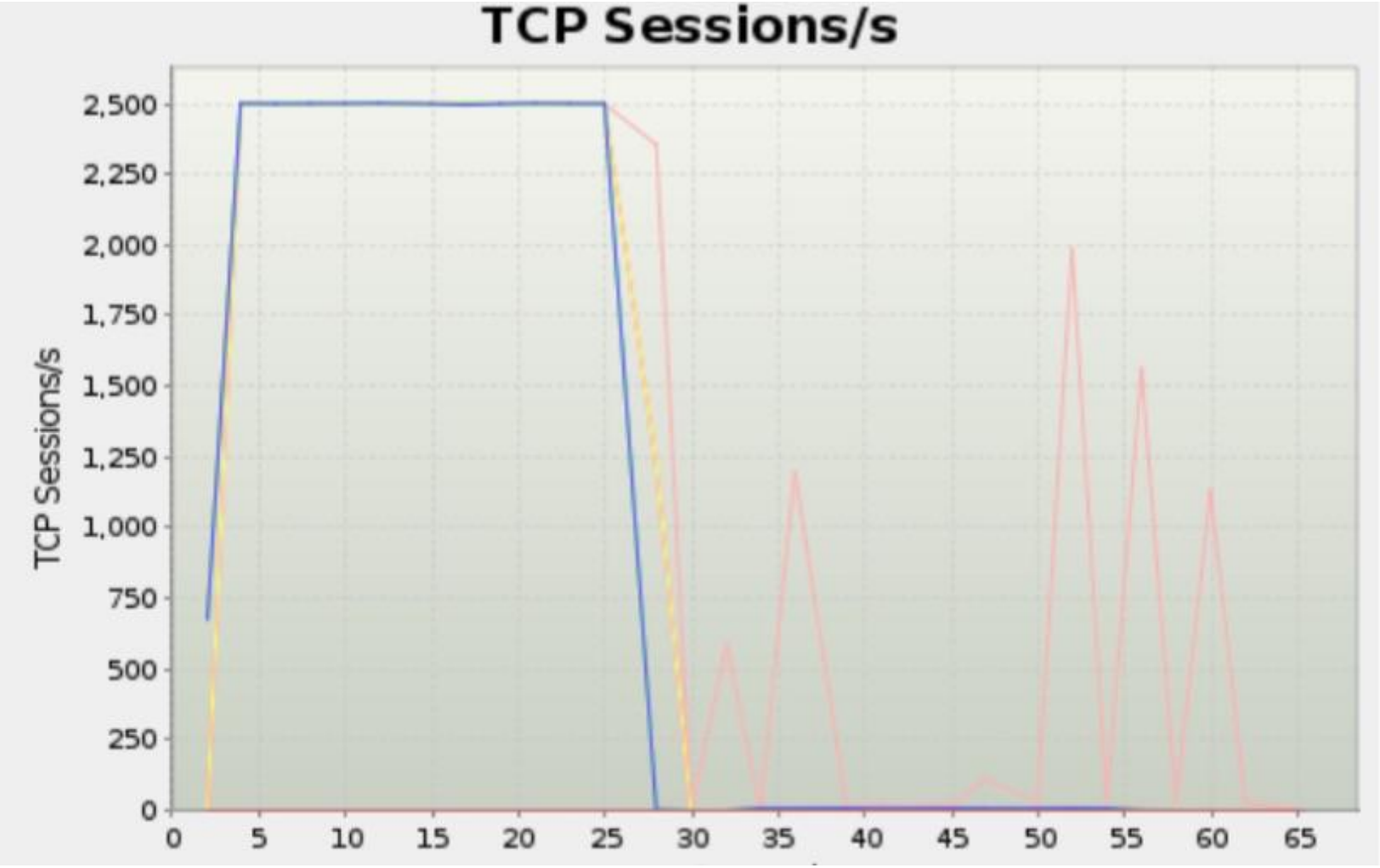


# #5: На Enterprise MIX устройство отказало

20 секунд работы привели к полному отказу устройства

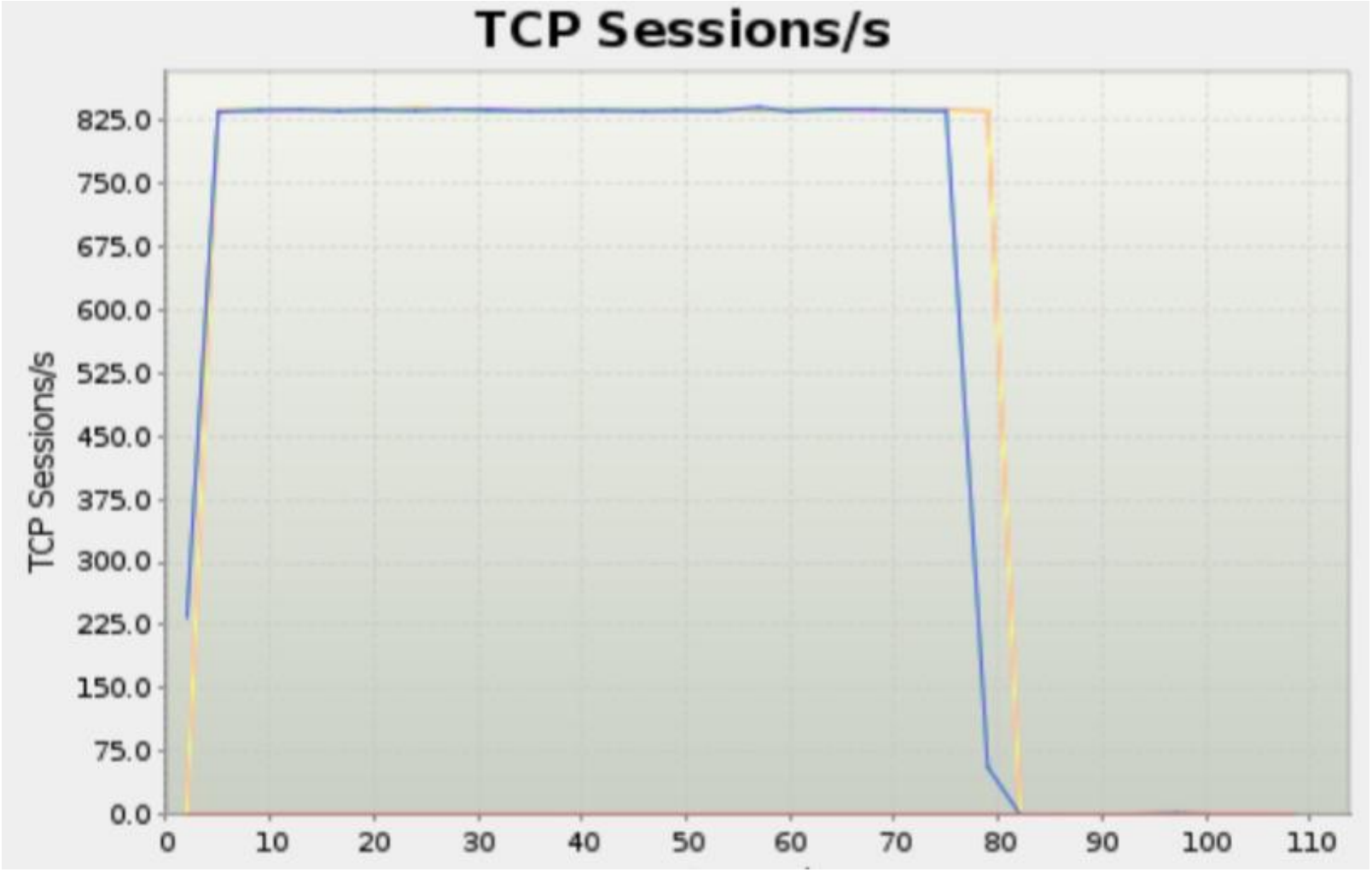
# #5: Ищем причину – скорость обработки сессий

2500 сессий в секунду – устройство умирает через 27 секунд



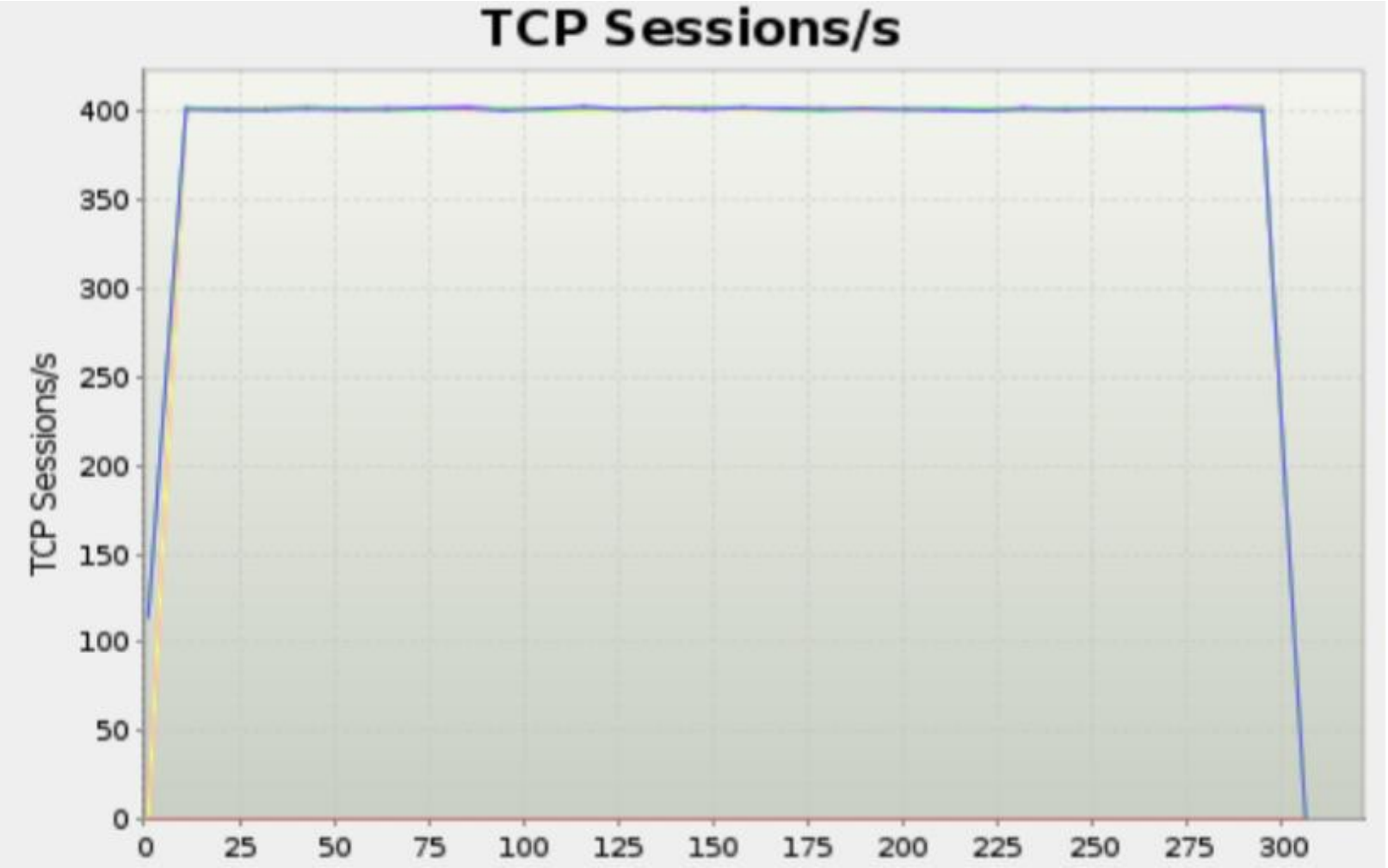
# #5: Ищем причину – скорость обработки сессий

825 сессий в секунду – устройство умирает через 80 секунд



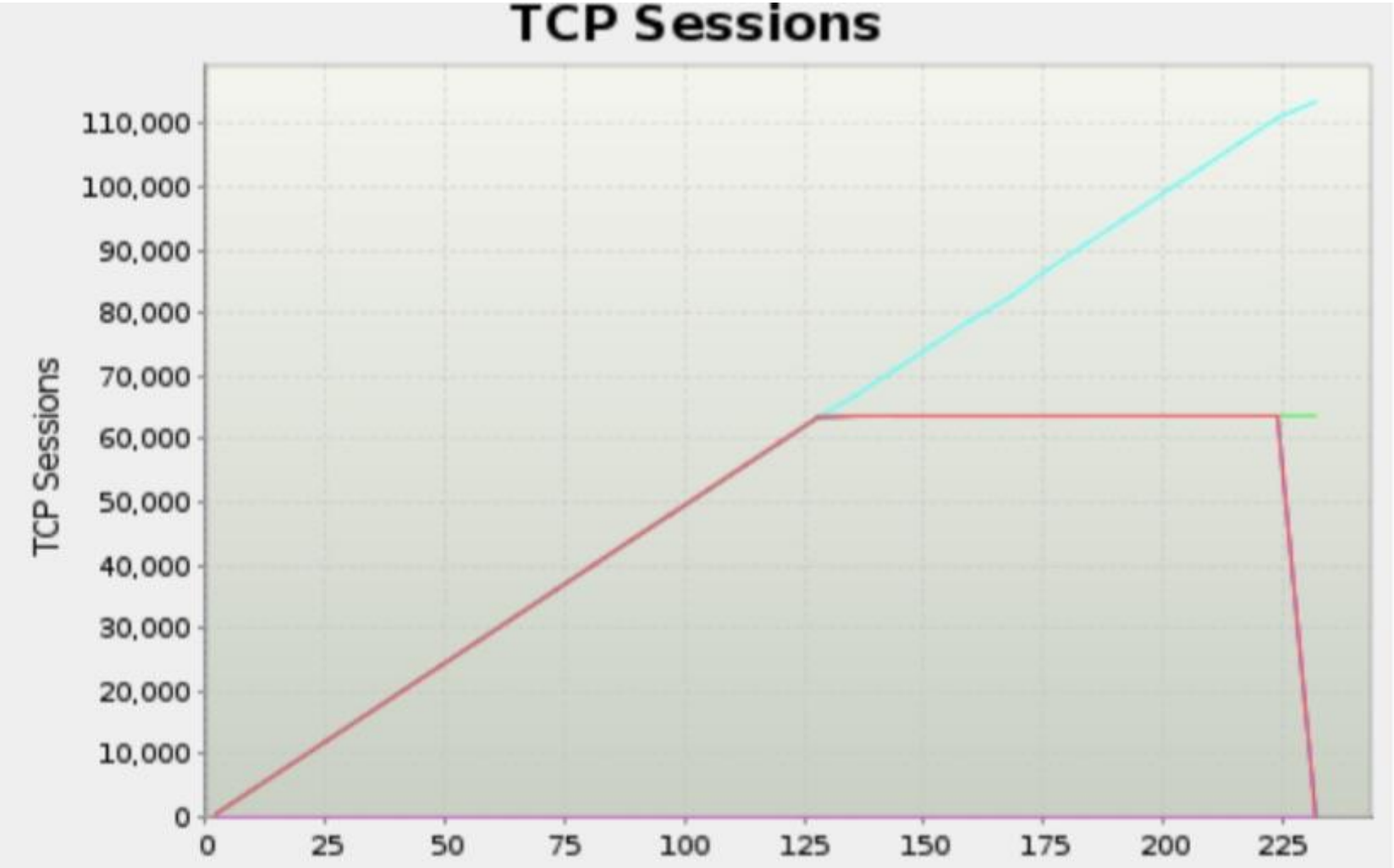
# #5: Ищем причину – скорость обработки сессий

400 сессий в секунду – устройство проходит тест



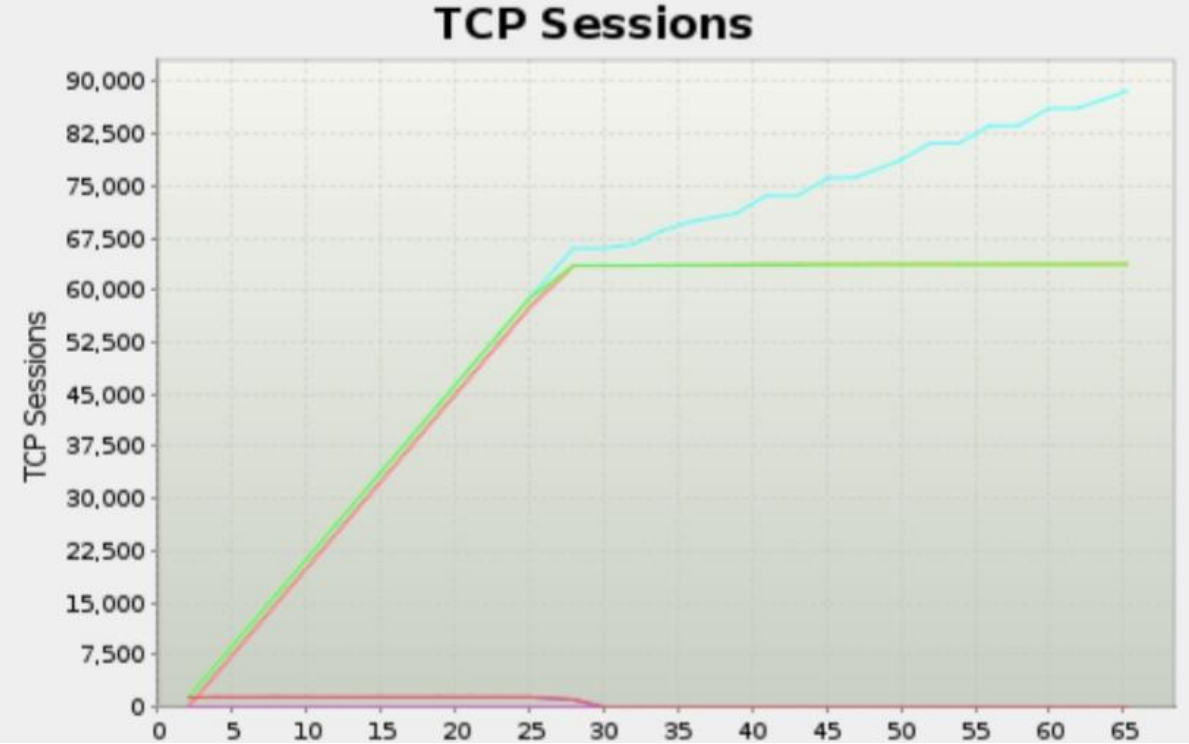
# #5: Ищем причину

## Предел 63500 одновременных сессий

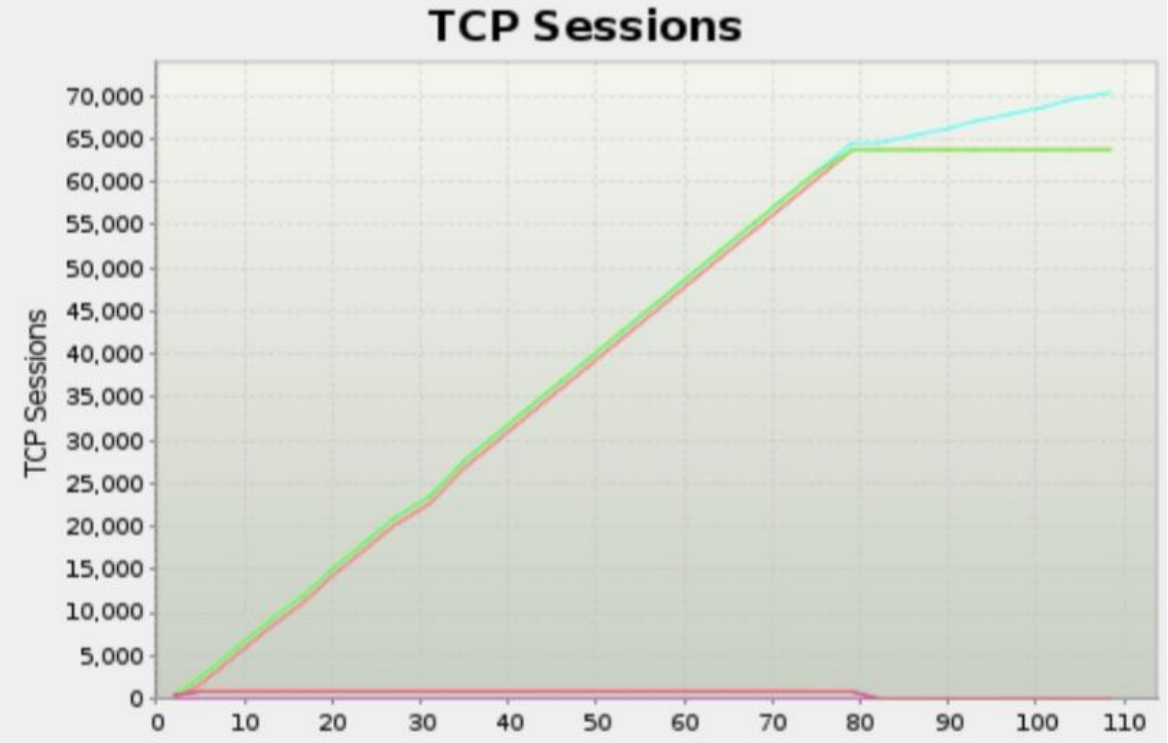


# #5: Ищем причину - общее число сессий при отказе

Во всех не пройдённых тестах было 63500 открытых + закрытых сессий




2500 сессий в секунду




825 сессий в секунду

# #5: Выводы

- Несмотря на высокую пропускную способность, устройство не может справиться с небольшой реальной нагрузкой
- Несмотря на то, что это был Роутер ( по заявлению вендора), он работал на уровне 4
- Основной вывод теста – устройство не готово к использованию в рабочей сети
- Причиной оказался баг очистки сессий внутри устройства. Его до сих пор не устранили …


FORTINET®