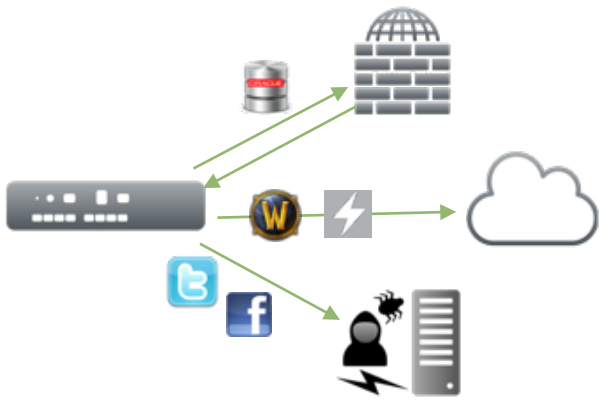
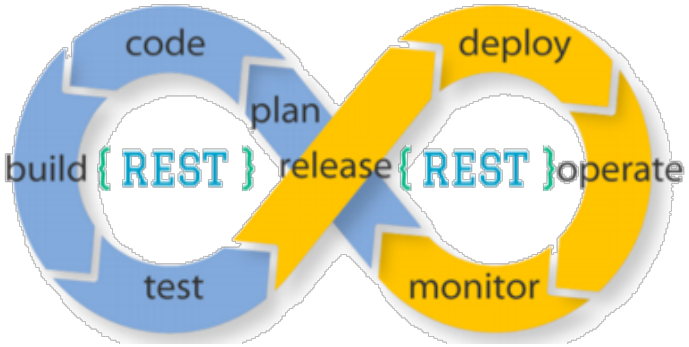
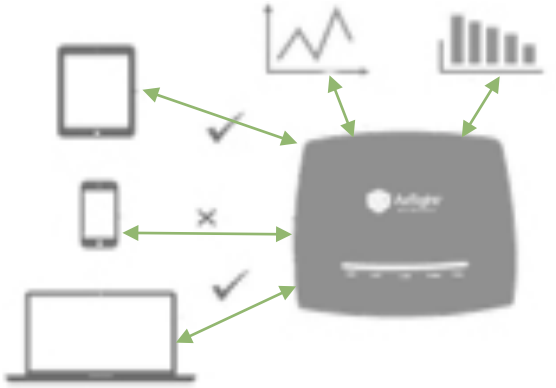

ixia

ПЛАТФОРМА PERFECTSTORM:
ТЕСТИРОВАНИЕ УСТРОЙСТВ И СЕРВИСОВ СЕТЕВОЙ ЗАЩИТЫ

ТИПОВЫЕ ЗАДАЧИ







Проверка перед внедрением

- Принятие решений по конкурирующим продуктам и технологиям по результатам реальных тестов эффективности.
- Определение правильного размера инвестиций в расширение инфраструктуры.

Эксплуатация

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

Обучение & оптимизация

- Оптимизация конфигурации систем защиты за счет оценки влияния изменений на конечную политику безопасности.
- Тренировка персонала и проверка скорости реакции на инцидент.

ixia

ОТВЕТ

Необходим инструмент для проведения тестирования!

- С готовыми методиками и шаблонами, чтобы быстро начать тесты.
- С актуальной базой данных атак.
- Чтобы генерировал трафик пользователей 1 в 1, без синтетики.
- Мощный, чтобы мог перегрузить DUT и найти точку насыщения.
- Настраиваемый, чтобы провести тесты всех аспектов и понять зависимости и оптимизации вендора под трафик.
- С поддержкой автоматизации для периодического проведения типовых тестов.
- Был признан на мировом рынке и имел опытную команду поддержки.

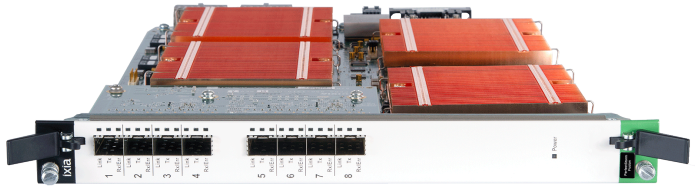
Платформа PerfectStorm™

Аппаратная часть и модули нагрузки

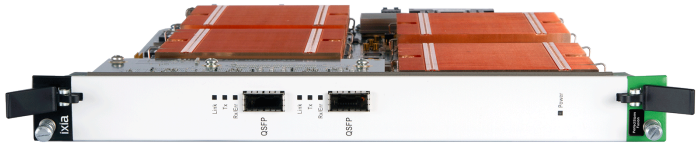
XGS12,12 слотов

XGS2, 2 слота

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



2-ports of 40GE with the QSFP+ interface



1-Port of 100GE with CXP interface

- Самая высокая производительность на рынке.
- Реальный и динамичный трафик, как в живой сети.
- Многопользовательский режим.
- 2 форм-фактора шасси.
- Поддержка IxLoad и BreakingPoint.

PerfectStorm Fusion	PerfectStorm Non-Fusion
BreakingPoint & IxLoad	IxLoad
XGS12/2-HS Chassis	XGS12/2-SD/HS Chassis

ixia

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

ixia

ЕДИНОЕ РЕШЕНИЕ

Xcellon-Ultra NP

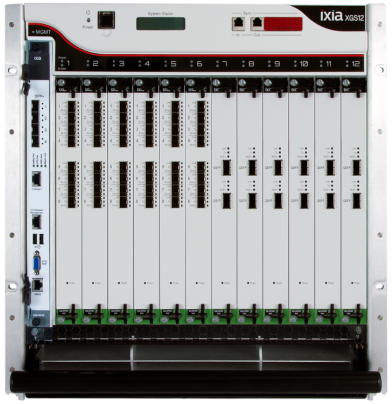
Scalable Layer 2-7 Performance Testing Within XM Chassis

Xcellon-Ultra XTS

Ultra-high Encrypted IPsec Performance

Breakingpoint Firestorm

Ultra-high Apps & Security Performance



ПРОИЗВОДИТЕЛЬНОСТЬ PerfectStorm™ BREAKINGPOINT

BreakingPoint KPI	PerfectStorm
Application Throughput	80 Gbps
Application Flow Rate (open)	2M flows/sec
TCP CPS (sustain)	1.5 M CPS
Concurrent Application Flows	60 M
SSL Throughput	20 Gbps
SSL CC	1 M
SSL Handshakes per second	190 K
IPsec Throughput	25 Gbps
IPsec Tunnels	500K tunnels
IPsec Tunnel Rate	2000/sec
SCTP Throughput	14 Gbps

Данные на модуль в two-arm-режиме, клиенты и серверы симулируются в рамках одного модуля.

ixia

ПРОИЗВОДИТЕЛЬНОСТЬ PerfectStorm™ IXLOAD

IxLoad KPI	PerfectStorm
Application Throughput (AppLib)	64 Gbps
HTTP Uni/Bi-directional Throughput	40 Gbps /76 Gbps
HTTP CPS	1.5 M CPS
HTTP TPS	5.5 M TPS
HTTP CC	30 M
SSL Throughput	20 Gbps
SSL CC	1 M
IPTV/OTT Throughput	20 Gbps
IPTV/OTT Sim Users	150,000
SIP/RTP active calls	96,000
SIP/SRTP active calls	24,000

Данные на модуль в two-arm-режиме, клиенты и серверы симулируются в рамках одного модуля.

МОДУЛЬ CXP 100G (PS100GE1NG)

Модуль с поддержкой fan-out-технологии для разветвления портов

- 1 порт 100GbE CXP (native).
- 2 порта 40GbE QSFP+ (через fan-out-кабель).
- 8 портов 10GbE SFP+ (через fan-out-кабель).

ПРОИЗВОДИТЕЛЬНОСТЬ НА ШАССИ

Applications

960

Gbps
Apps Throughput

Connection Rate

24

Million
TCP CPS

Capacity

720

Million
HTTP CC

SSL Throughput

240

Gbps
SSL Throughput

SSL Capacity

12M

Concurrent
SSL Flows

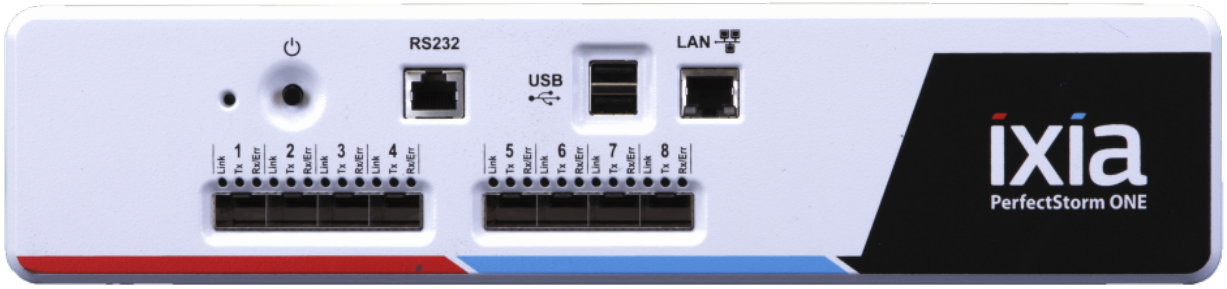
SSL CPS

2.4M

SSL
Connection Rate

PerfectStorm ONE™

Готовый appliance для тестирования комплексов сетевой защиты



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

2-ports of 40GE with the QSFP+ interface

МАСШТАБИРОВАНИЕ

Расширяйте систему по мере роста потребностей

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

ПОДДЕРЖКА МОДУЛЕЙ НАГРУЗКИ

PerfectStorm

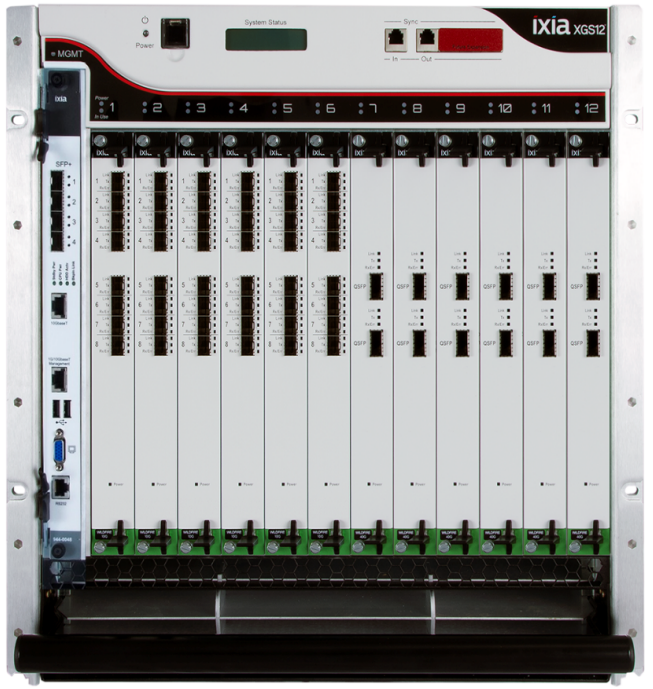
ixia IxLoad

BreakingPoint Find it before they do.™

XM-модули

ixia IxNetwork

ixia IxLoad



ixia

ВИРТУАЛЬНЫЕ ПОРТЫ

ВИРТУАЛЬНЫЕ ТЕСТОВЫЕ ПОРТЫ

Автоматизированное разворачивание для Vmware и KVM

Приложения	Connection Rate	Capacity
18	540	40
Gbps Apps Throughput	Thousand TCP CPS	Million HTTP CC

На каждый vController

- Гибкое лицензирование по полосе пропускания.
- Простое и неограниченное масштабирование физических ресурсов.

ixia

ЛИЦЕНЗИРОВАНИЕ

Общее описание:

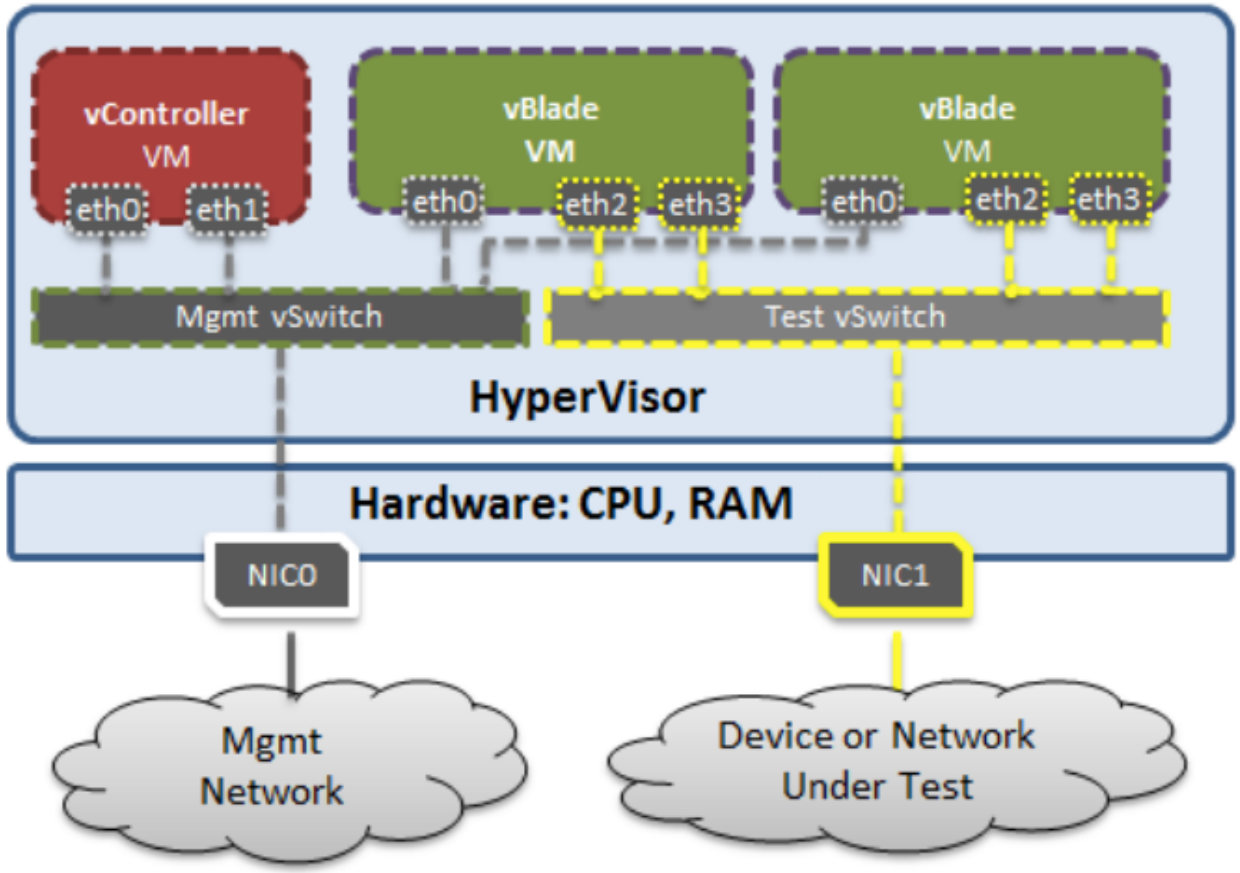
- Подписка позволяет работать с системой в течении года, получая все необходимые обновления софта и новых атак.

Особенности:

- Лицензируется исключительно полоса пропускания генерируемого трафика с шагом в 1 Гбит/с Simplex-трафика на 1 год при использовании 1 интерфейса.
- Лицензия может быть использована различными vController.
- Для увеличения требуемой полосы пропускания достаточно закупить новые лицензии.

АРХИТЕКТУРА ВИРТУАЛЬНЫХ ПОРТОВ

- До 12 виртуальных vBlade на vController.
- До 8 виртуальных интерфейсов на vBlade.
- До 96 виртуальных интерфейсов на vContoller.
- vBlade можно разворачивать на разных хостах.



СИСТЕМНЫЕ ТРЕБОВАНИЯ

Программные:

- Среда виртуализации: Vmware ESX 5.5 или KVM.
- Сервис DHCP.

Аппаратные:

- Серверы с архитектурой Intel x86-64.
- Виртуальная машина vController – 8 GB RAM, 8 vCPU, 100 GB Hard Disk.
- Виртуальная машина vBlade – 8 GB RAM, 4 vCPU, 10GB Hard Disk.

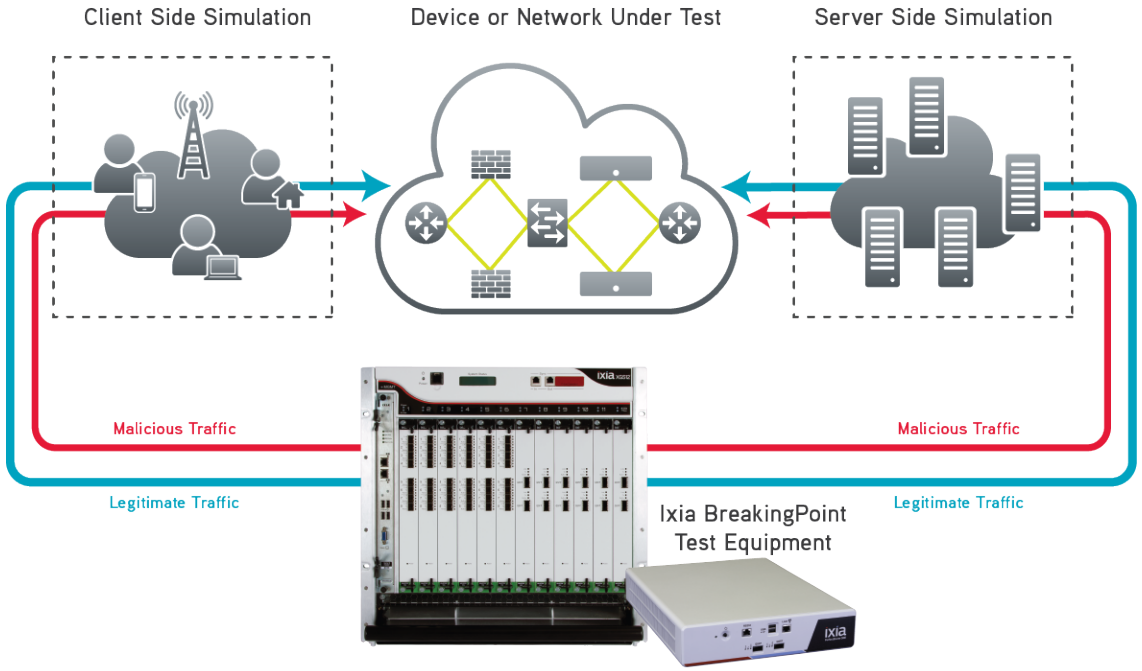
ПРЕИМУЩЕСТВА

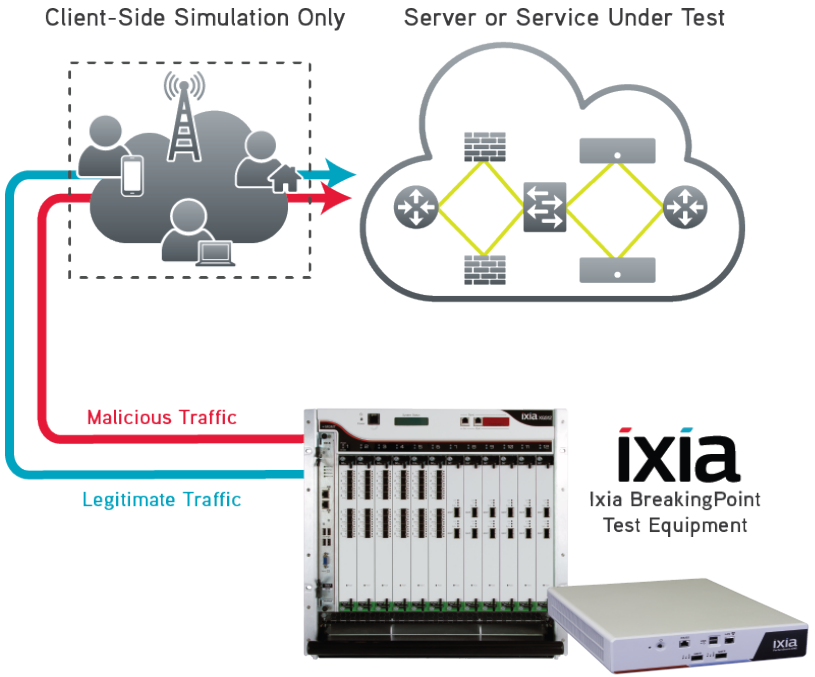
- Быстрое проведение POC заказчику, доказать преимущество над конкурентами.
- Бюджетное решение для теста систем с небольшой производительностью.
- Небольшие расходы OPEX с привязкой к проектам.
- Проверка готовности к миграции ЦОД.
- Тестирование виртуальных устройств и частного/гибридного облака.
- Обучение и проверка готовности персонала.

ПО УПРАВЛЕНИЯ:
BREAKINGPOINT

ТОПОЛОГИИ ТЕСТИРОВАНИЯ

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





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	36000+ Атак	100+ способов обхода
Stack Scrambler (Fuzzer)	Фаззер TCP/UDP	Фаззер уровня приложений

ТРАФИК РЕАЛЬНЫХ ПРИЛОЖЕНИЙ И АТАК

- Встроенная библиотека профилей различных сетевых сервисов и атак для моделирования динамической природы трафика.
- Обновление каждые 2 недели.

BreakingPoint 3.5.1:

- 36895 атак (malware и эксплоиты)
- 3409 готовых superflow
- 295 сервисов/протоколов

В 2015 году добавлено:

- 42 приложения
- 143 superflows
- 549 эксплоитов
- 250 ботнетов
- 450 malware
- Ежемесячные обновления для Evergreen Applications

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

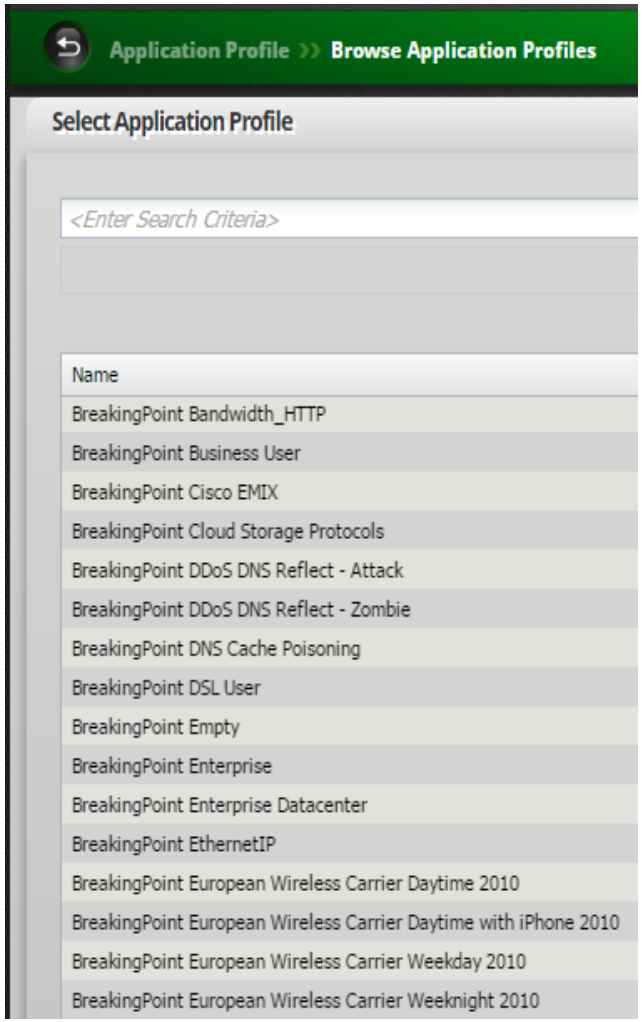
Streaming Media
Pandora
Netflix

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

BREAKINGPOINT:
ОСОБЕННОСТИ

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

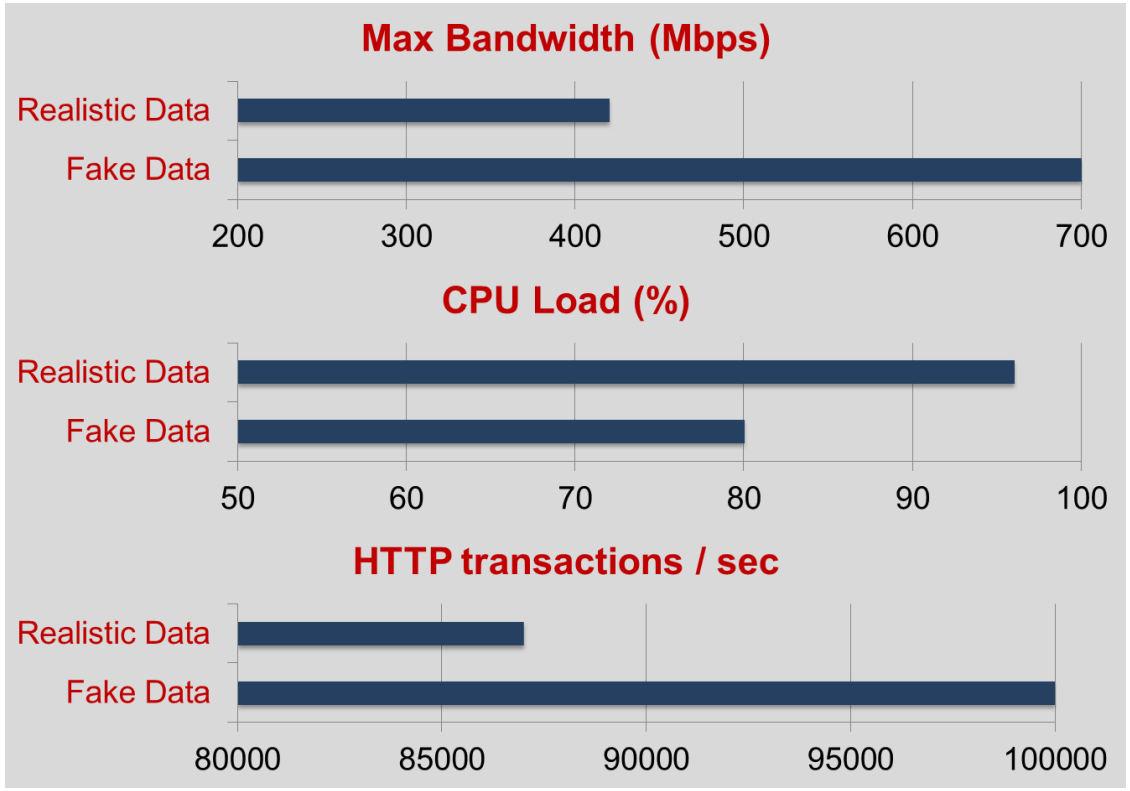
#	Protocol	Client	Server
1	DNS	Client	DNS Server
2	Google Mail	Client	Google Mail Server
3	Google Mail	Client	Google Accounts Server
4	Google Mail	Client	Gmail Attachment Server

Actions

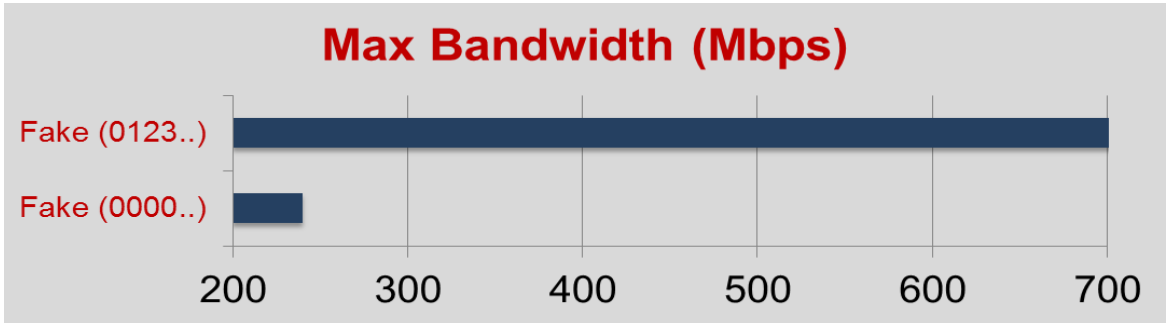
#	Action	#	Flow	Source
1	Resolve	1	DNS	client
2	Accept TLS	2	Google Mail	server
3	Start TLS	2	Google Mail	client
4	Sign into Gmail	2	Google Mail	client
5	Response to Gmail Sign in	2	Google Mail	server
6	Resolve	1	DNS	client
7	Accept TLS	3	Google Mail	server
8	Start TLS	3	Google Mail	client
9	Gmail Service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

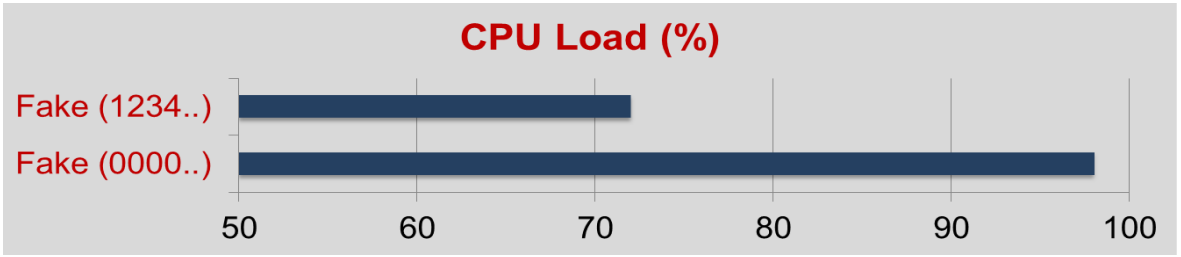
СОДЕРЖАНИЕ ИМЕЕТ ЗНАЧЕНИЕ!

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



Пример#2. NGN-файрвол с IPS.
Статичное содержание определенного вида может быть интерпретировано как опасное.



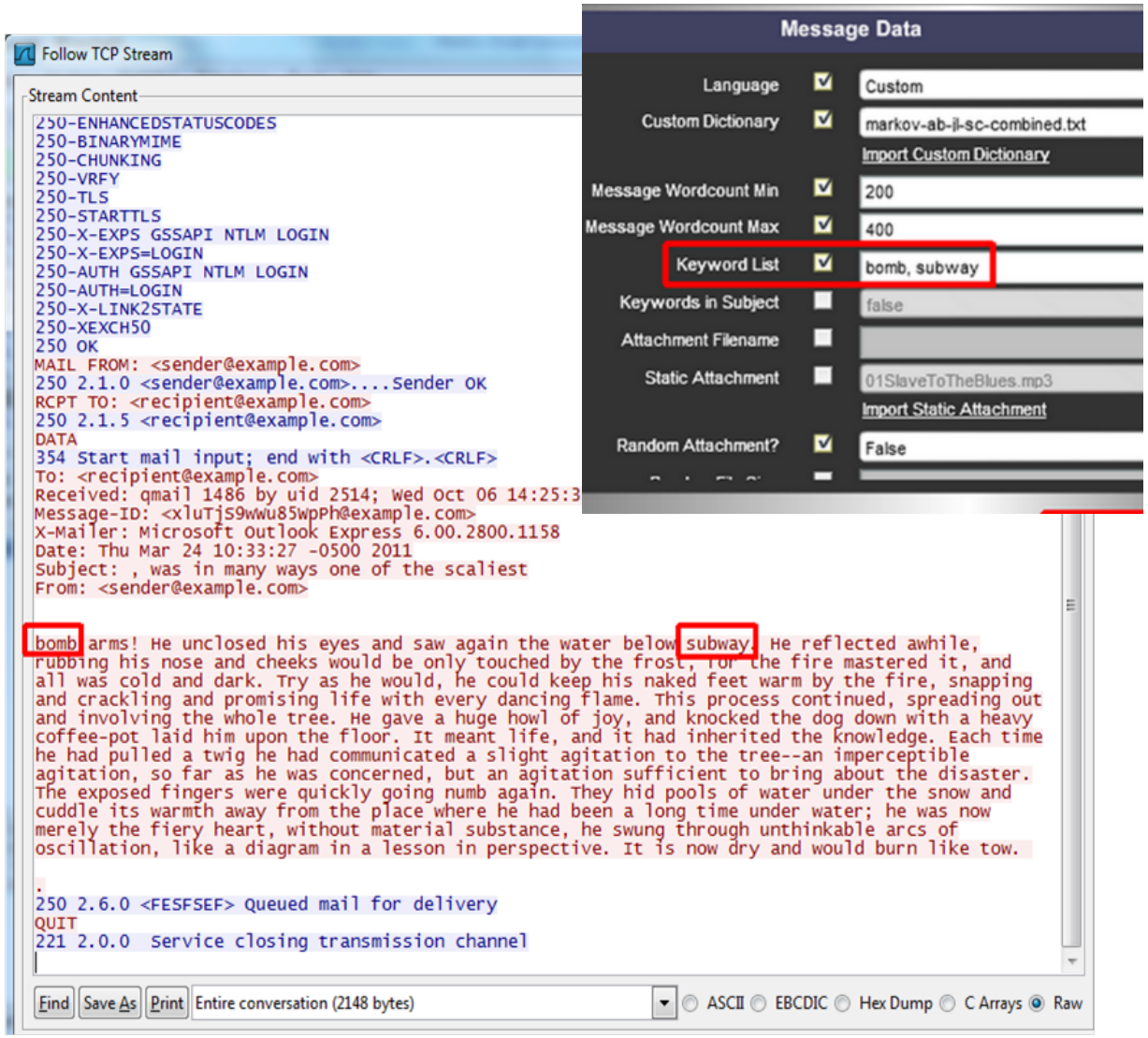


HTTP payload with all ‘0000s’ vs ‘012345..9’

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).



Марков в email с ключевым словом target.

ixia

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

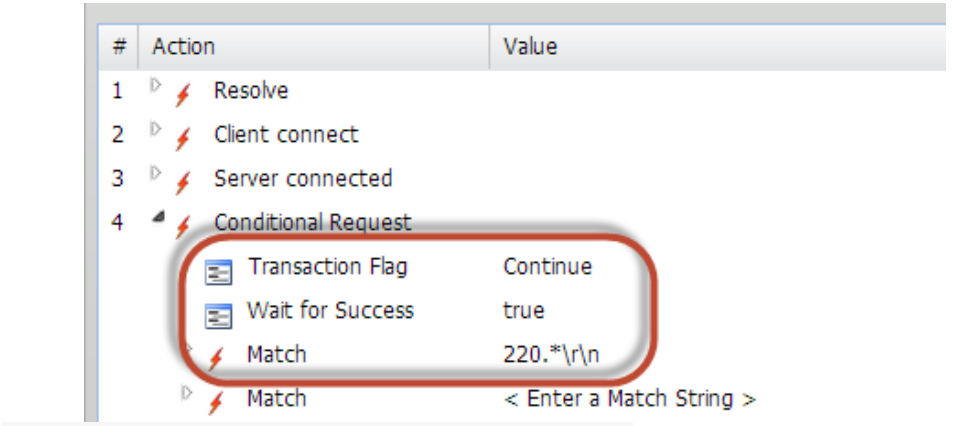
ixia

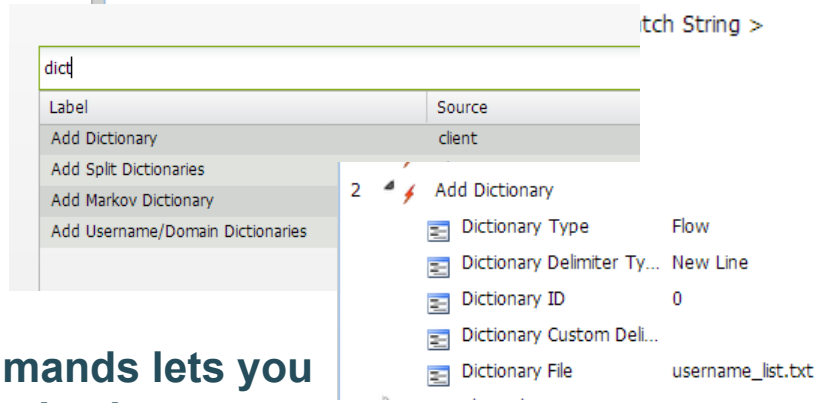
ДИНАМИЧНЫЕ СИМУЛЯЦИИ

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).

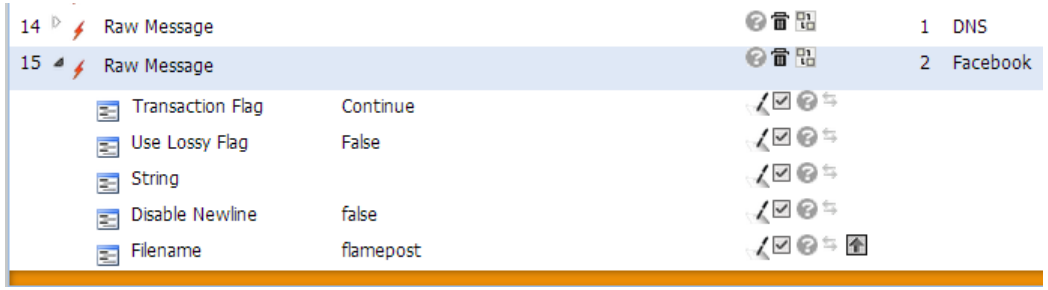
#1 Conditional requests in applications





#2 Dictionary commands lets you insert user specified values

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



ixia

КАСТОМИЗАЦИЯ

Если не хватает функционала “из коробки”

Включено в стандартную лицензию:

- Воспроизведение трафика из ранее захваченного.
- Raw – создание собственных сообщений внутри протокола.
- Загрузка своих malware.

Custom Application Toolkit (опция):

- Свои протоколы и exploit.
- XML-шаблоны, вставки на Ruby.
- Любые транзакции поверх TCP и UDP.

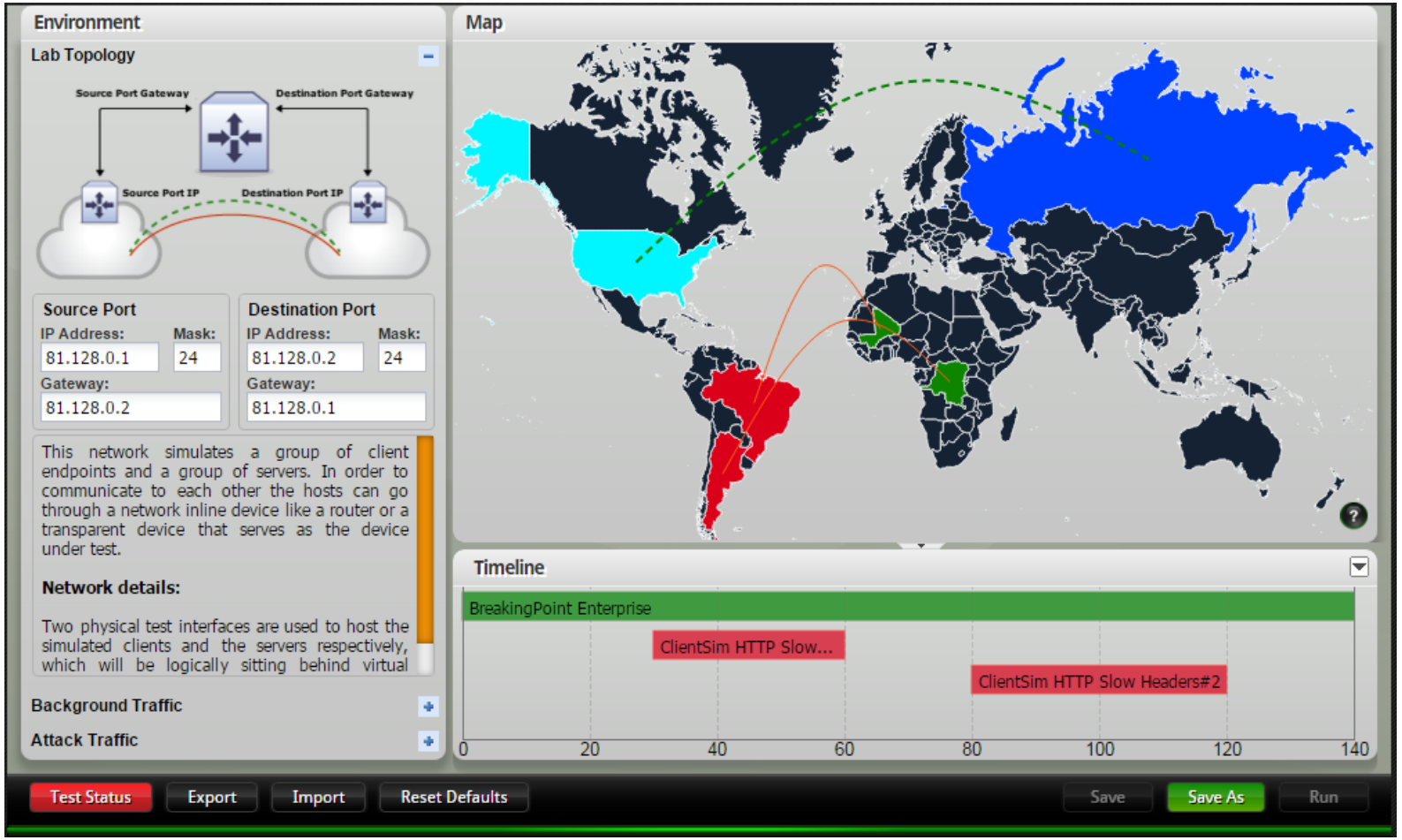
```
<application sport="0" dport="554">
  <conf>
    <dblock store="SessionID_Value" type="text_rand_numeric" min="2
  </conf>
  <client>
    <dblock type="ascii">DESCRIBE rtsp://10.0.0.3/sample_300kbit.mp
    <dblock type="ascii">CSeq: 1\r\n</dblock>
    <dblock type="ascii">Accept: application/sdp\r\n</dblock>
    <dblock type="ascii">Bandwidth: 384000\r\n</dblock>
    <dblock type="ascii">Accept-Language: nl-NL\r\n</dblock>
    <dblock type="ascii">User-Agent: QuickTime/7.6.4 (qtver=7.6.4;o
    <dblock type="ascii">\x0d\x0a</dblock>
  </client>

  <server>
    <dblock type="ascii">RTSP/1.0 200 OK\r\n</dblock>
    <dblock type="ascii">Server: QTSS/6.0.3 (Build/526.3; Platform/
    <dblock type="ascii">Cseq: 1\r\n</dblock>
    <dblock type="ascii">Last-Modified: Sat, 17 May 2008 10:39:24 G
    <dblock type="ascii">Cache-Control: must-revalidate\r\n</dblock
    <dblock type="ascii">Content-length: 1263\r\n</dblock>
    <dblock type="ascii">Date: Thu, 12 Nov 2009 10:04:24 GMT\r\n</d
    <dblock type="ascii">Expires: Thu, 12 Nov 2009 10:04:24 GMT\r\n
    <dblock type="ascii">Content-Type: application/sdp\r\n</dblock>
    <dblock type="ascii">x-Accept-Retransmit: our-retransmit\r\n</d
    <dblock type="ascii">x-Accept-Dynamic-Rate: 1\r\n</dblock>
    <dblock type="ascii">Content-Base: rtsp://10.0.0.3/sample_300kb
    <dblock type="ascii">\r\n</dblock>
    <dblock type="ascii">v=0\r\n</dblock>
    <dblock type="ascii">o=StreamingServer 3467009064 1211020764000
    <dblock type="ascii">s=/sample_300kbit.mp4\r\n</dblock>
    <dblock type="ascii">u=http:///\r\n</dblock>
    <dblock type="ascii">e=admin@\r\n</dblock>
    <dblock type="ascii">c=IN IP4 0.0.0.0\r\n</dblock>
    <dblock type="ascii">b=AS:258\r\n</dblock>
    <dblock type="ascii">t=0 0\r\n</dblock>
    <dblock type="ascii">a=control:*\r\n</dblock>
```


ixia

ГЕНЕРАЦИЯ АТАК 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

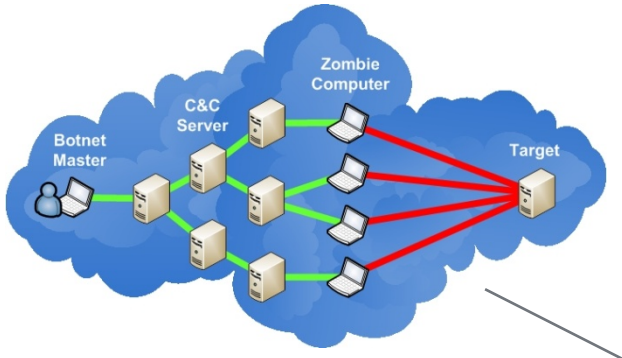
Layer 4 TCP
- ✓DDoS SYN Flood
- ✓DDoS PSH-ACK Attack
- ✓DDoS Fake Session Attack
- ✓DDOS SYN-ACK Flood Attack
- ✓DDoS Rcv Wnd Size 0

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

ixia

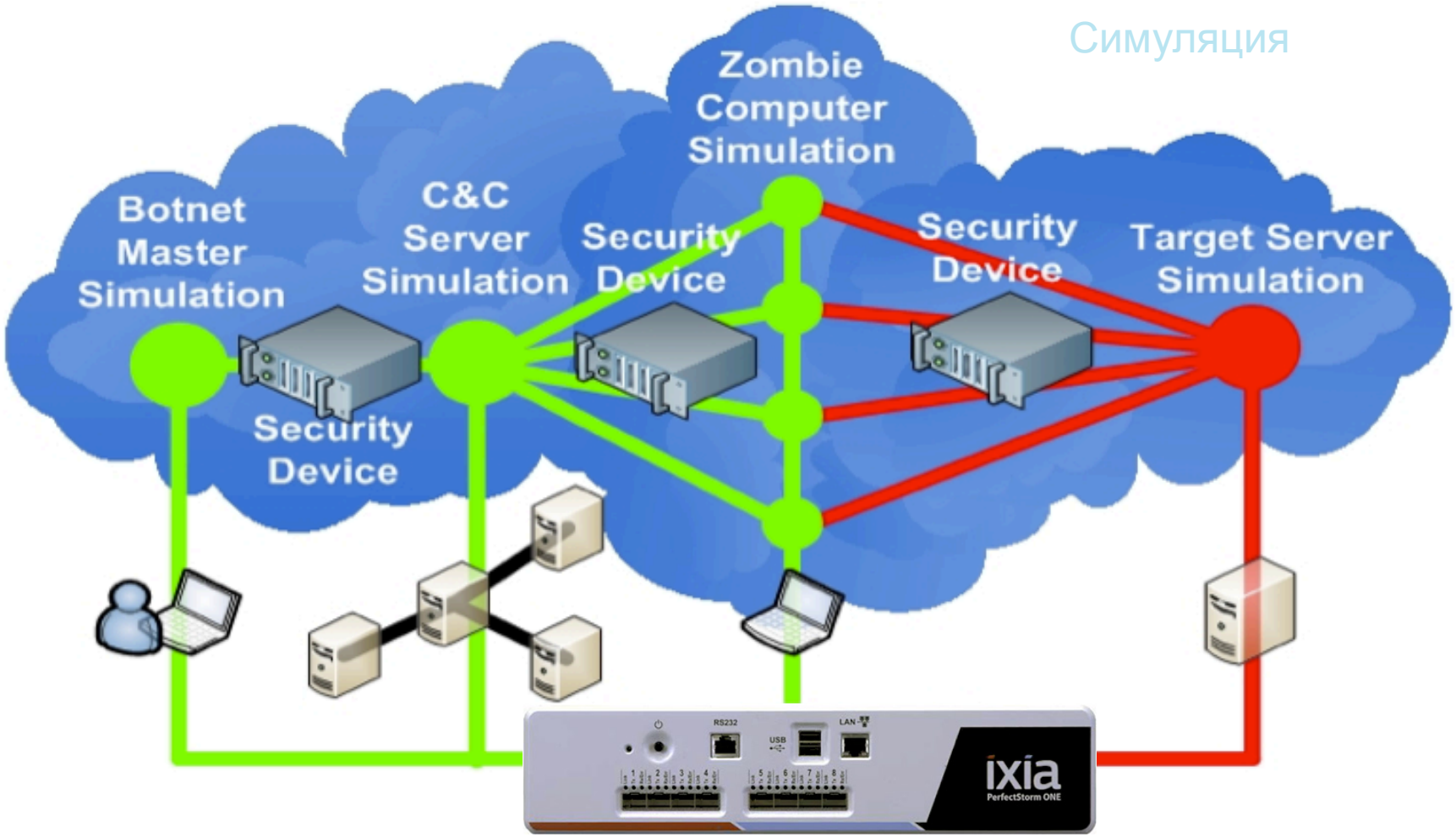
СИМУЛЯЦИЯ BOTNET-СЕТЕЙ



Реальная топология

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

Симуляция



Ixia BreakingPoint Test Equipment

ixia

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

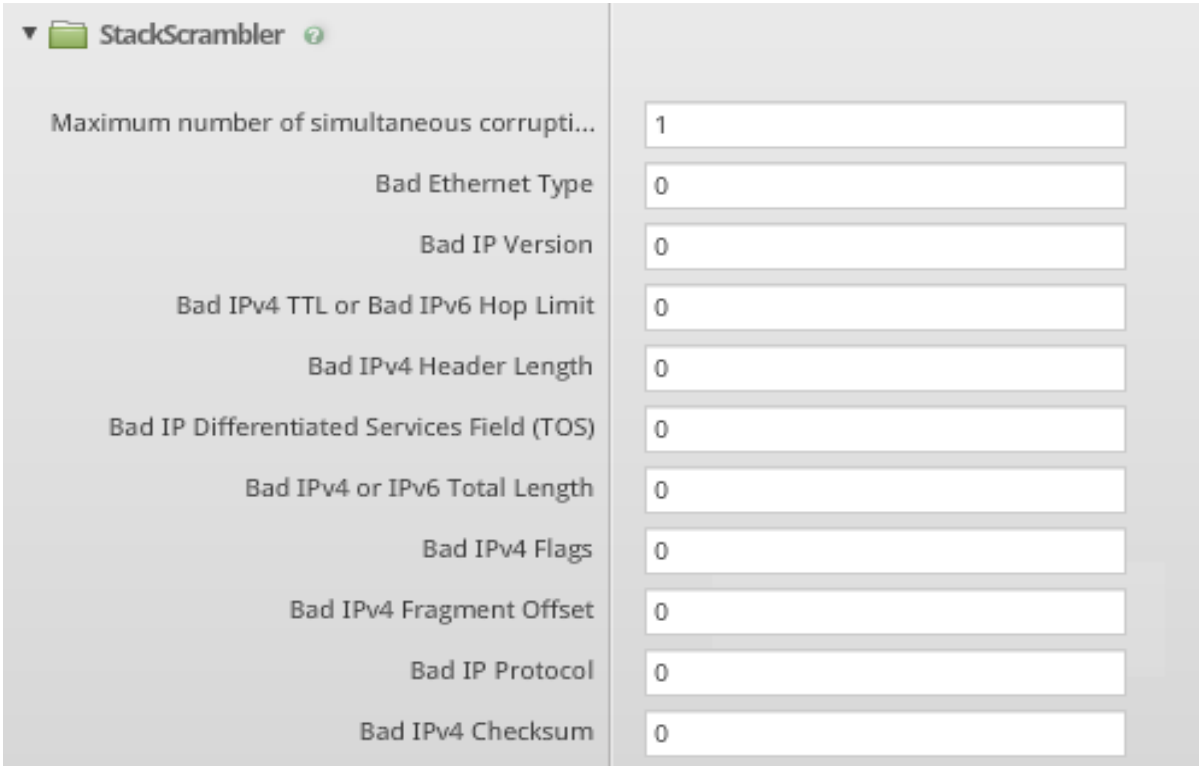
GET `` `` HTTP/1.1

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.

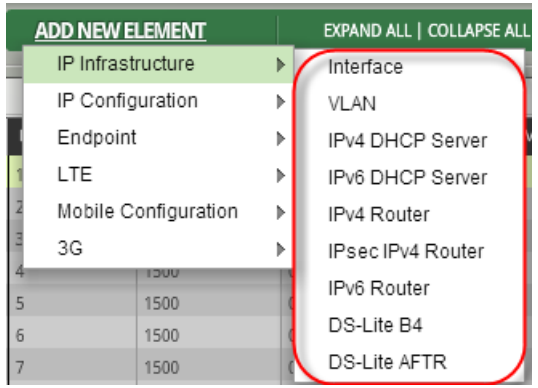


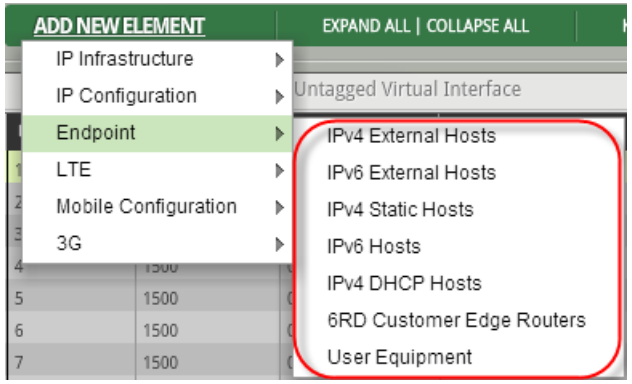
ixia

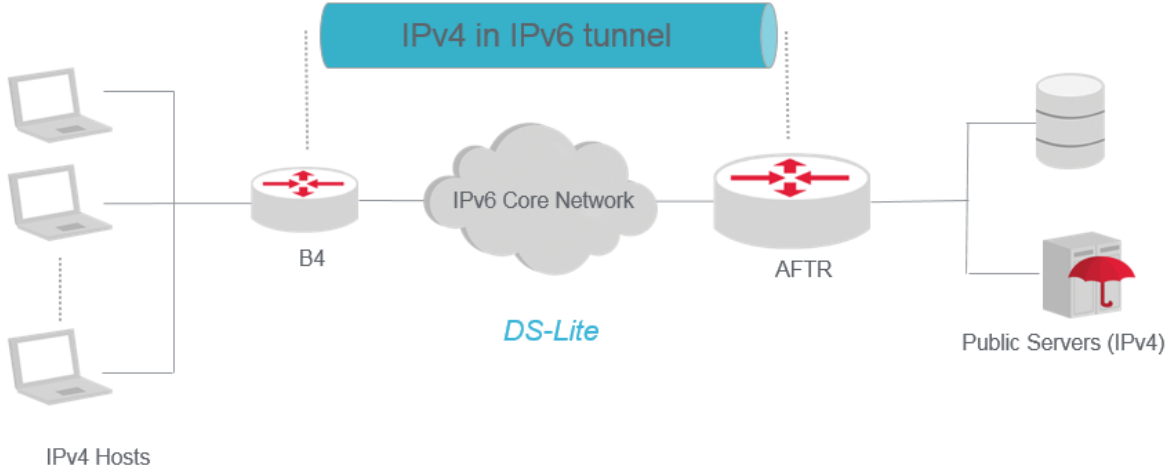
СЕТЕВОЙ УРОВЕНЬ

- Эмуляция активности клиентов поверх:
  - DHCPv4/6
  - VLAN (802.1Q, QinQ)
  - Virtual Router instances
  - GTPv1/v2

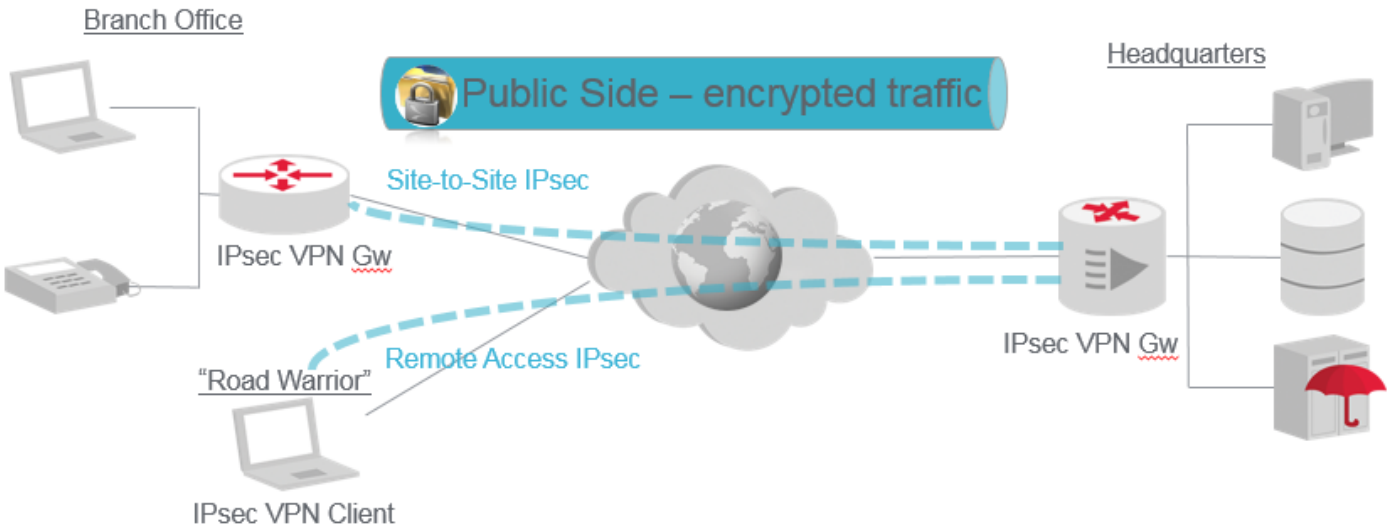
- Готовность к переходу на IPv6:
  - DS-Lite, 6rd
  - DHCP-PD
  - SLAAC







ТЕСТИРОВАНИЕ IPSEC



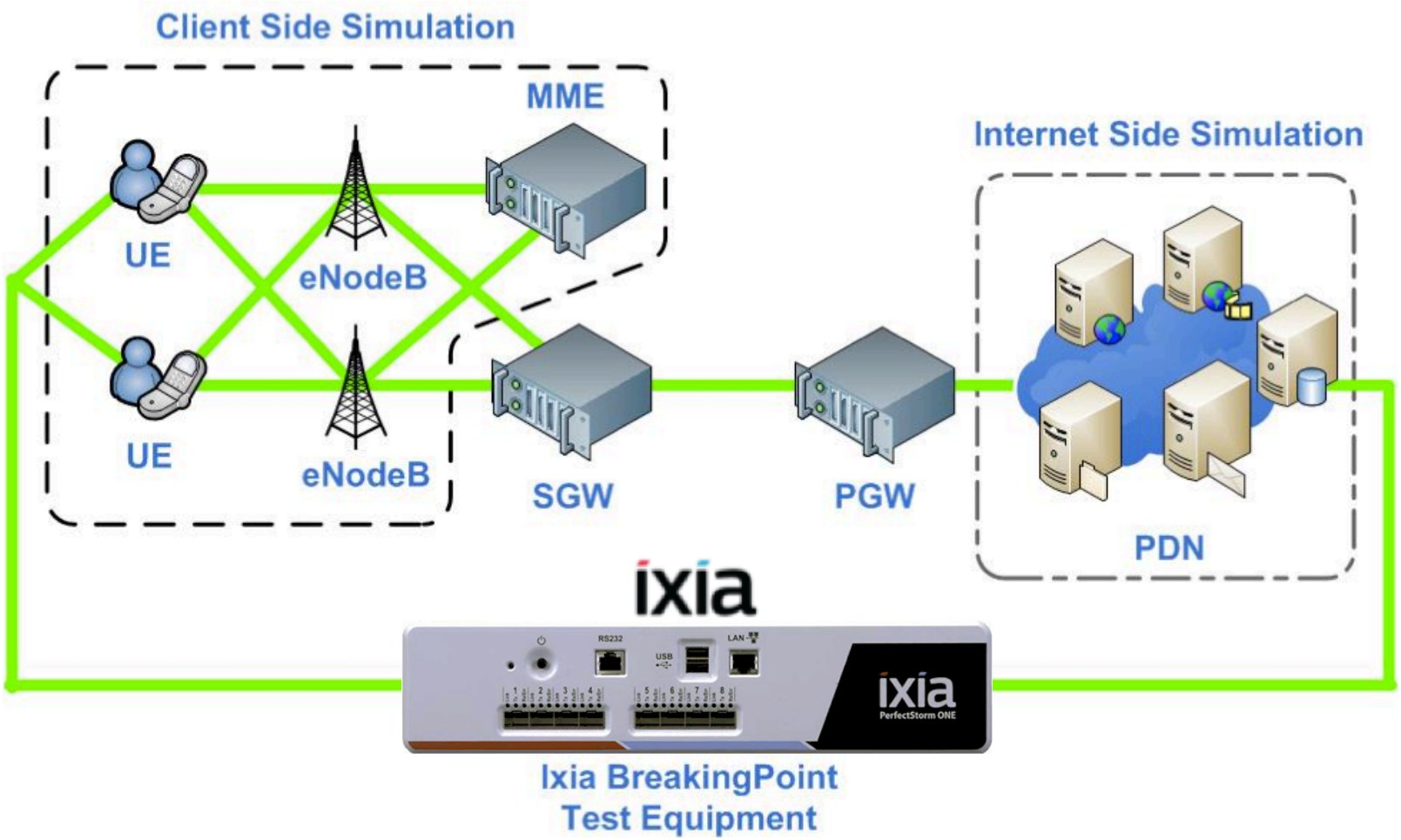
Эмуляция IPsec и трафика поверх:

- Site to Site и Remote Access.
- Генерация трафика приложений и атак.
- Фаззер поверх Ipsec.
- Универсальное решение для тестирования файрволов, UTM и других интегрированных решений сетевой защиты.

ixia

ЭМУЛЯЦИЯ ТРАФИКА МОБИЛЬНОГО ОПЕРАТОРА

- 3 млн GTP- туннелей/UE.
- До 26 гигабит трафика пользователей.
- До 4000 eNodeB.
- Симуляция на интерфейсах S1-U/S1-MME/SW11/S5/S8/SGi.



ixia

ГОТОВЫЕ МЕТОДИКИ

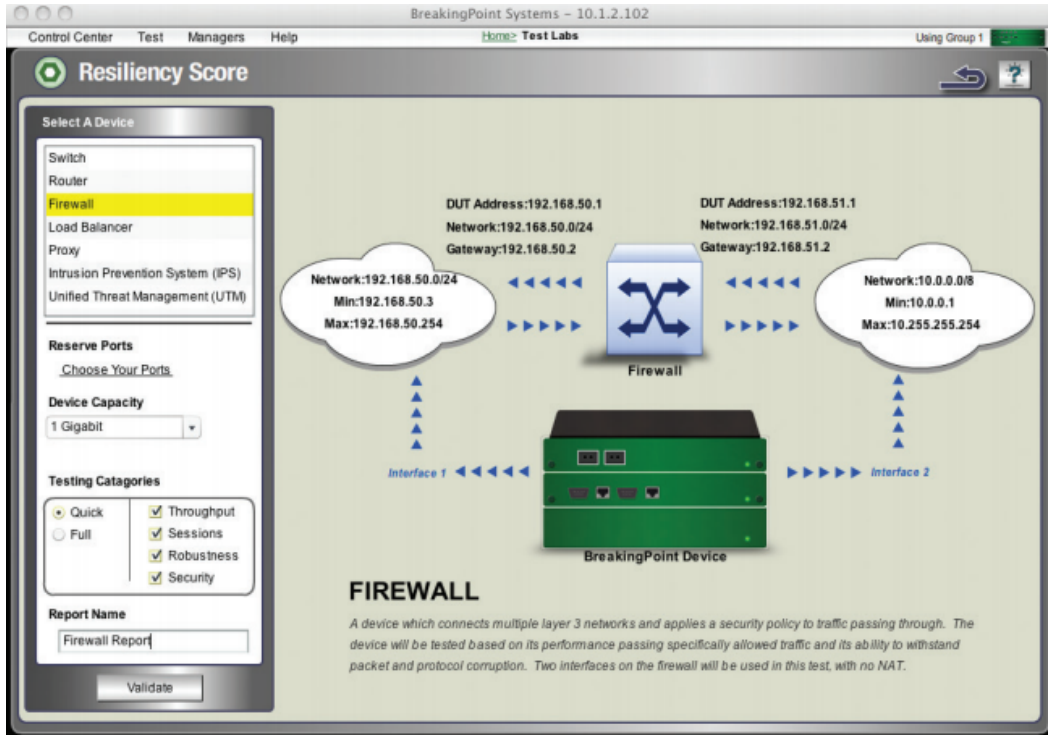
Быстрый старт, сокращение времени на разработку методологий

Network Intrusion Prevention System (IPS), Test Methodology v.7.2

- UDP Raw Performance and Latency
- Maximum Capacity (Per-Second)
- Maximum Capacity
- Maximum HTTP Capacity
- Real-World Traffic Mix Performance
- Protocol Fuzzing and Mutation

Next Generation Firewall, Test Methodology v.6

- Simple and Complex Policies
- Denial of Service, Evasion and Exploits
- Raw Performance with UDP and Latency Testing
- Maximum Capacity (Per Second) Testing
- Maximum HTTP Capacity Testing
- Real-World Traffic Mix Performance
- Stability and Security - Attack Leakage
- Protocol Fuzzing and Mutation



ПРОЧИЕ ОСОБЕННОСТИ

- Поддерживается на физической и виртуальных платформах.
- Не требует инсталляции ПО на клиента – интерфейс HTLM5.
- Минимум опций, в лицензию включено все.
- Автоматизация через REST API и TCL API.
- Поддержка TACACS+.

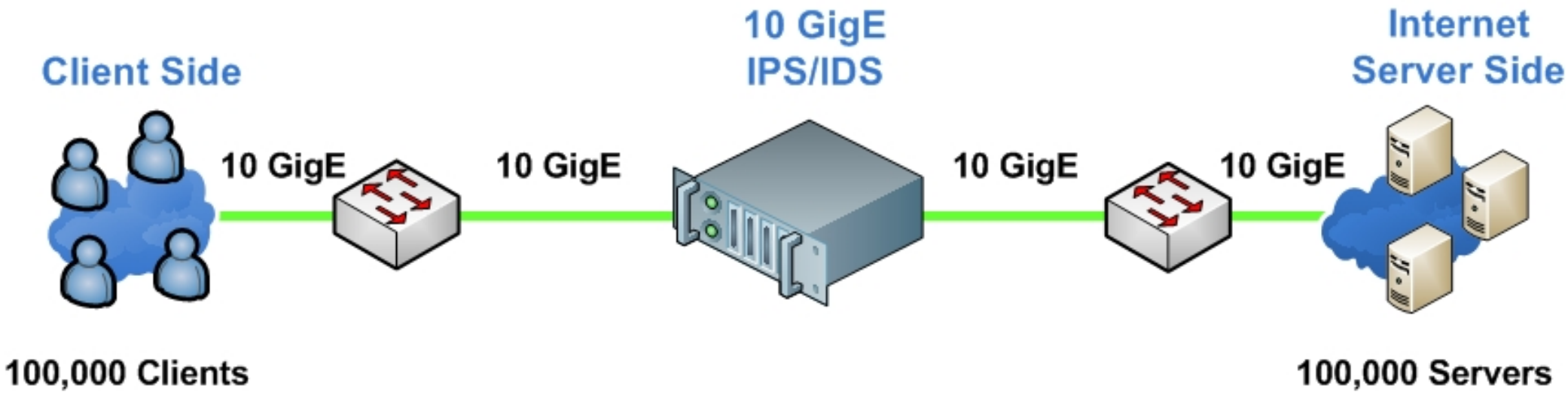
ПО BREAKINGPOINT:

ТИПОВЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

ixia

#1: ВЫБОР ПОСТАВЩИКА

4 известных поставщика IPS



ixia

#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 трафике.

#1: L3 UDP STATELESS TRAFFIC

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 AND L7 – TCP AND 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: SECURITY TEST FOR MALICIOUS TRAFFIC

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: SECURITY TEST FOR MALICIOUS TRAFFIC

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

49

#1: L7 – MIX OF GOOD AND MALICIOUS TRAFFIC

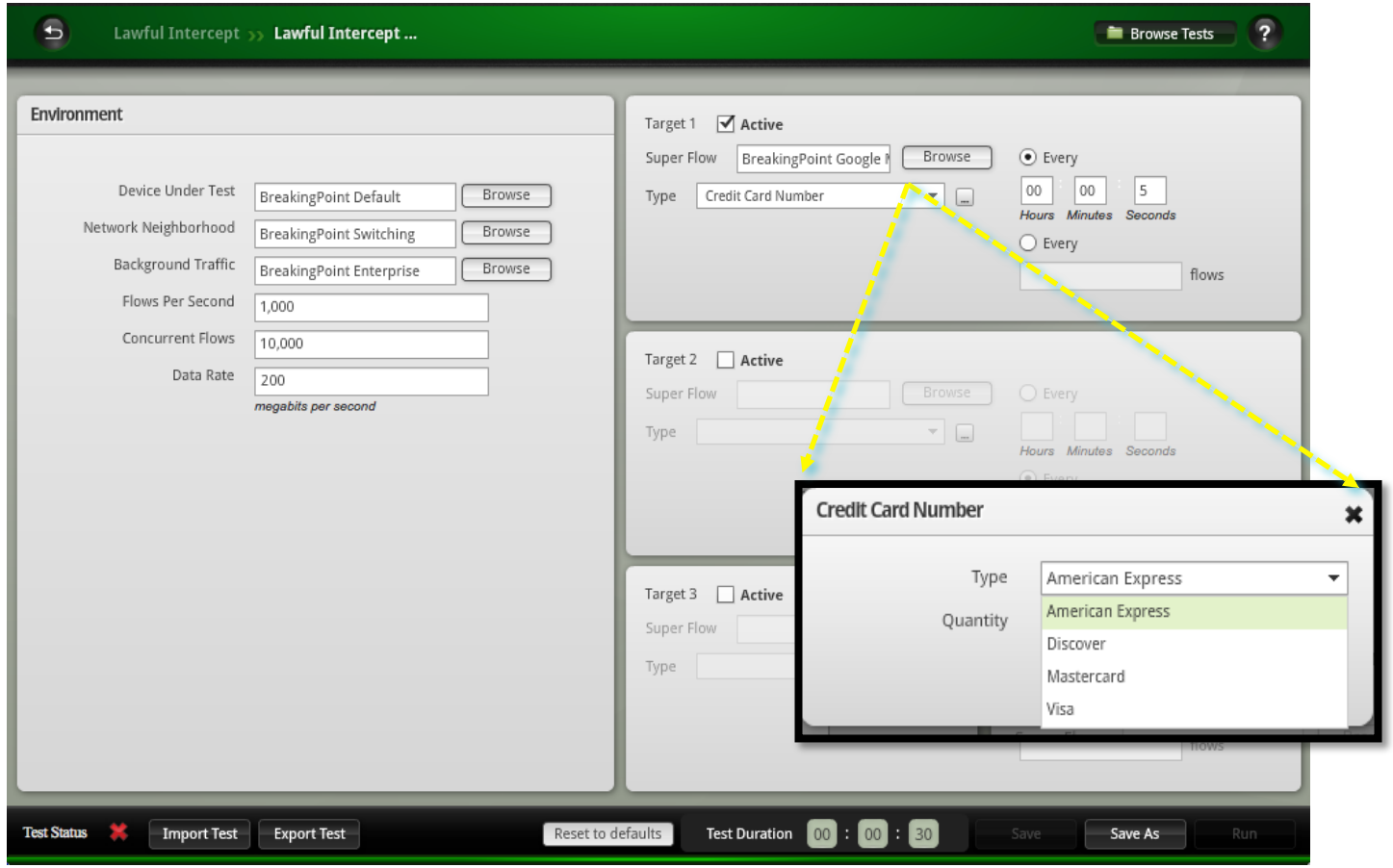
Результаты теста

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.

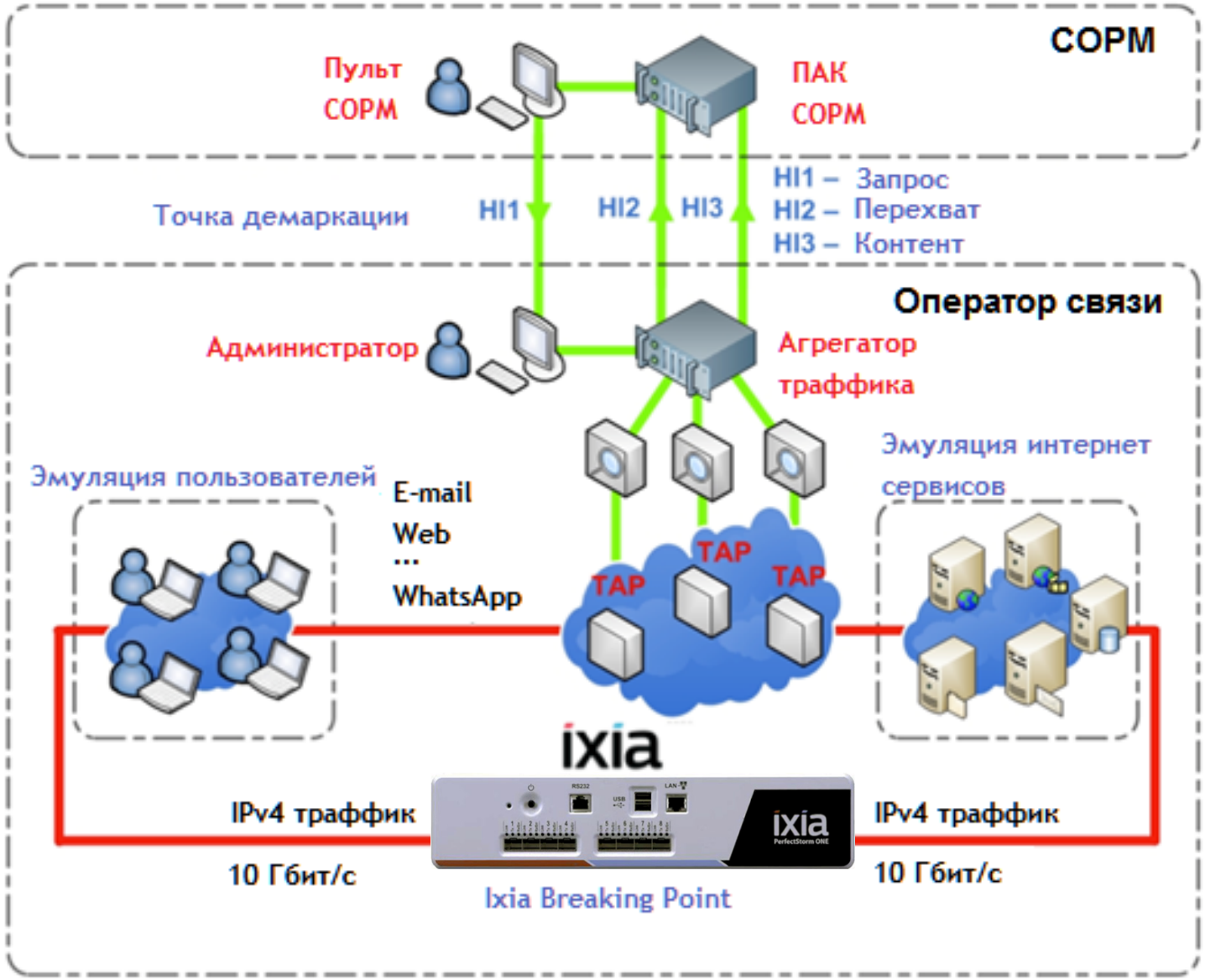
#2: ТЕСТИРОВАНИЕ СИСТЕМ ОБНАРУЖЕНИЯ УТЕЧЕК

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



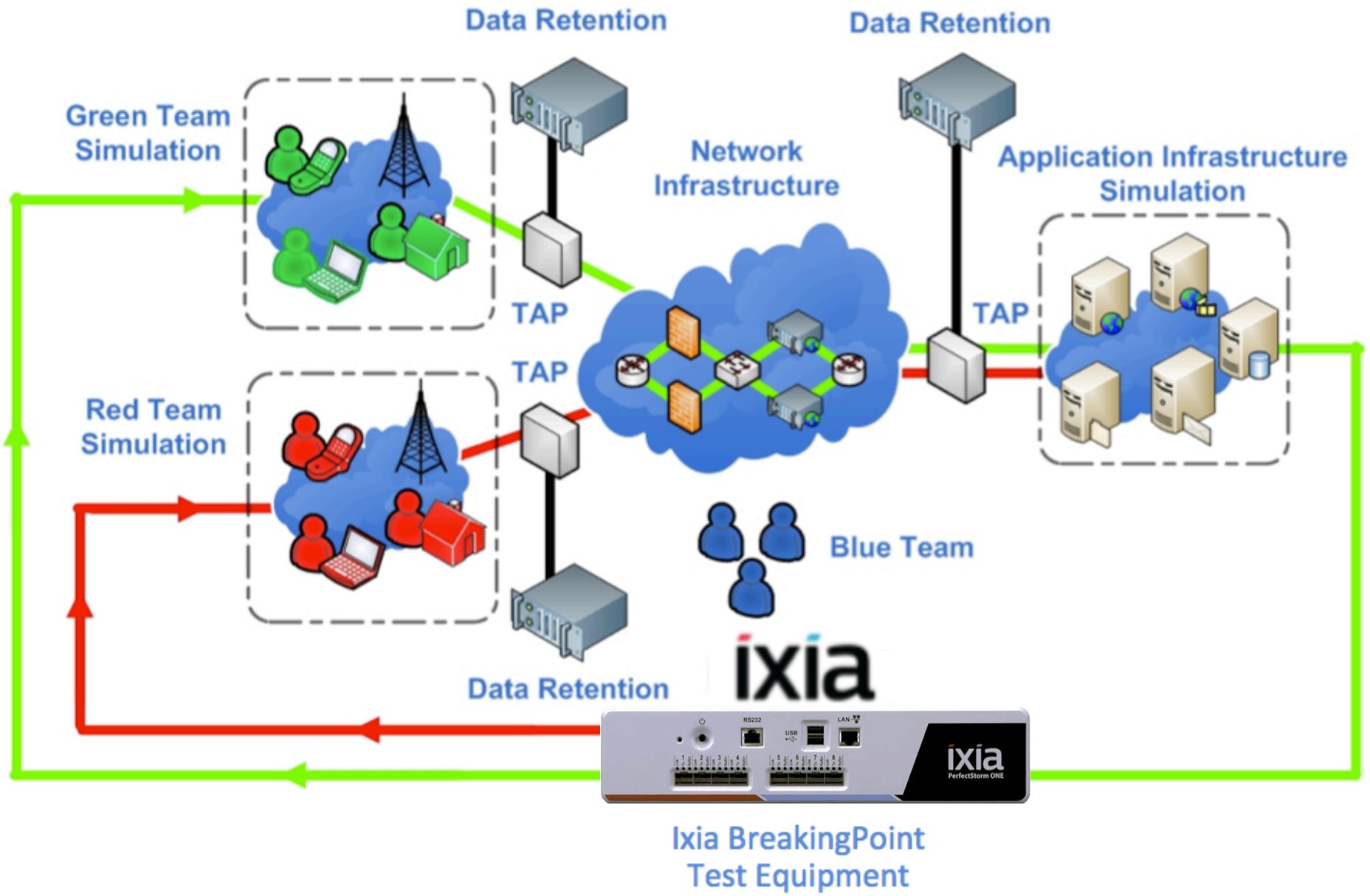
ixia

#3: ТЕСТИРОВАНИЕ СОРМ



ixia

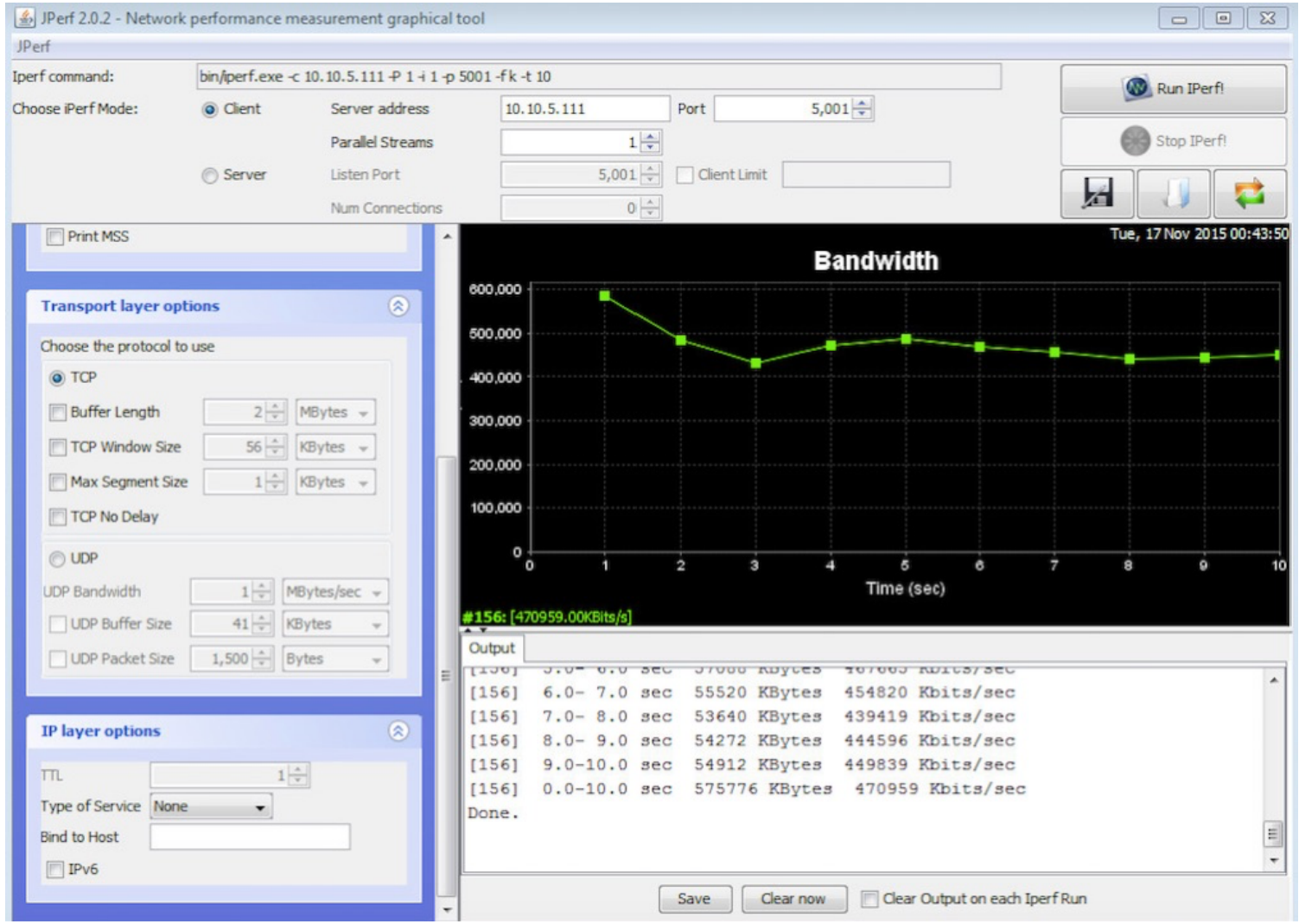
#4: КИБЕРПОЛИГОН, ТРЕНИРОВКА И ПРОВЕРКА



ixia

#5: ВИРТУАЛЬНЫЙ МАРШРУТИЗАТОР

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



#5: ПЛАН ТЕСТИРОВАНИЯ

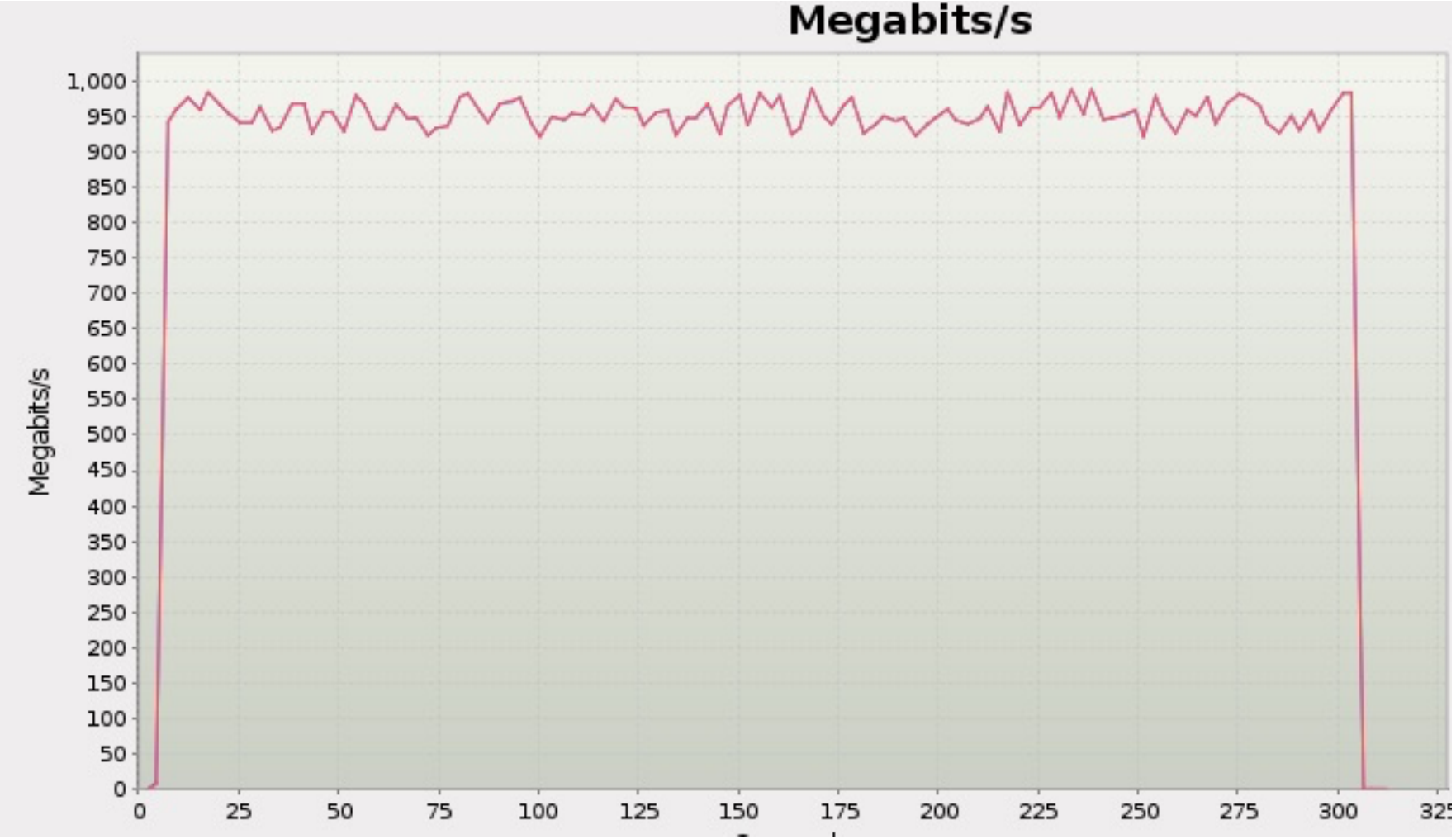
1. Производительность на разных профилях трафика L7:
   - HTTP,
   - Enterprise MIX.
2. Проверка механизмов обработки сессий:
   - Скорость обработки сессий.
   - Количество одновременных сессий.

Тест успешен, если трафик ходит 5 минут.

Проверяем с помощью IXIA BreakingPoint Virtual Edition.

#5: HTTP ТРАФИК ПОКАЗАЛ ПРЕКРАСНЫЙ РЕЗУЛЬТАТ

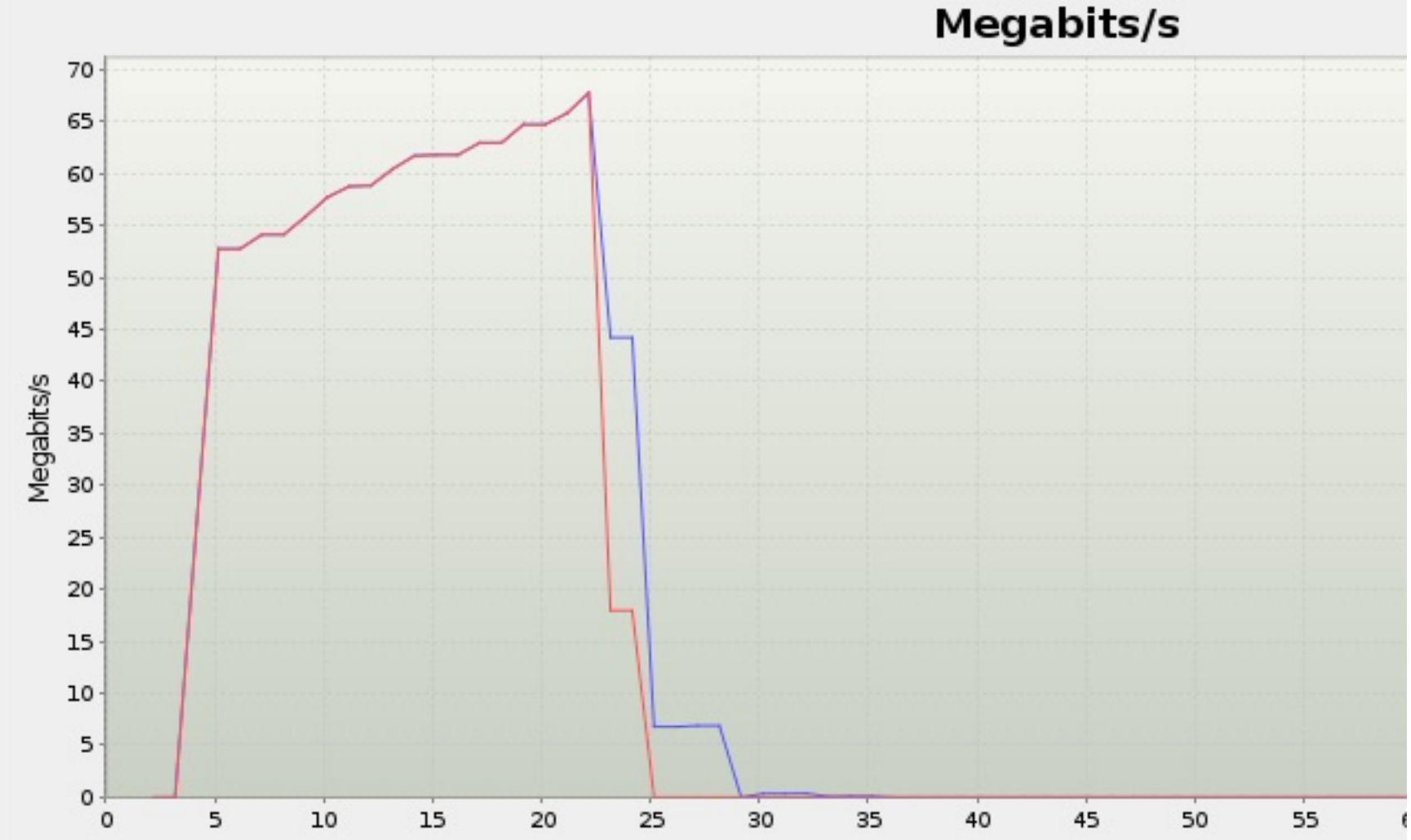
Производительность до 1 Гбит/с



ixia

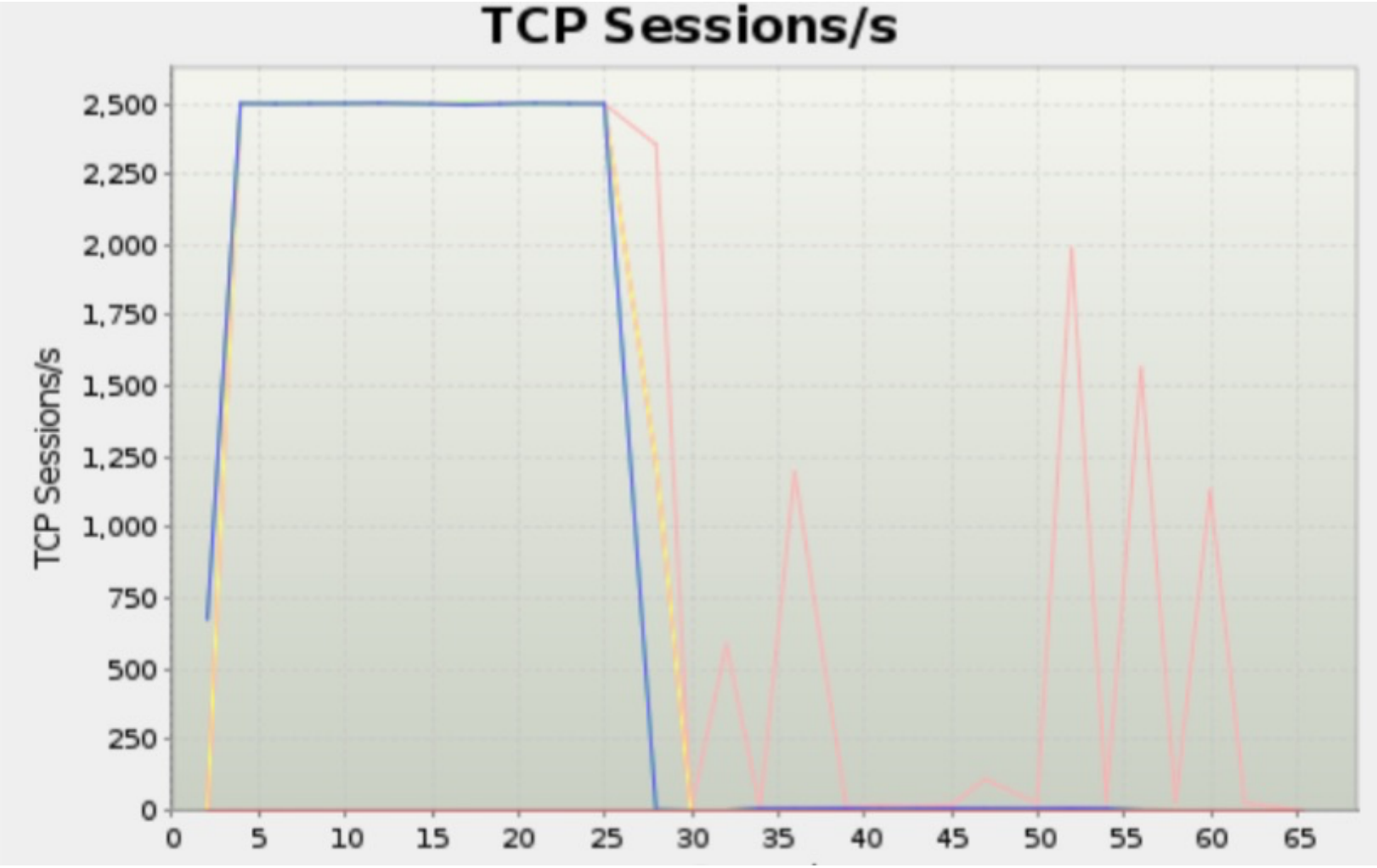
#5: НА ENTERPRISE MIX УСТРОЙСТВО ОТКАЗАЛО

20 секунд работы привели к полному отказу устройства



#5: ИЩЕМ ПРИЧИНУ – СКОРОСТЬ ОБРАБОТКИ СЕССИЙ

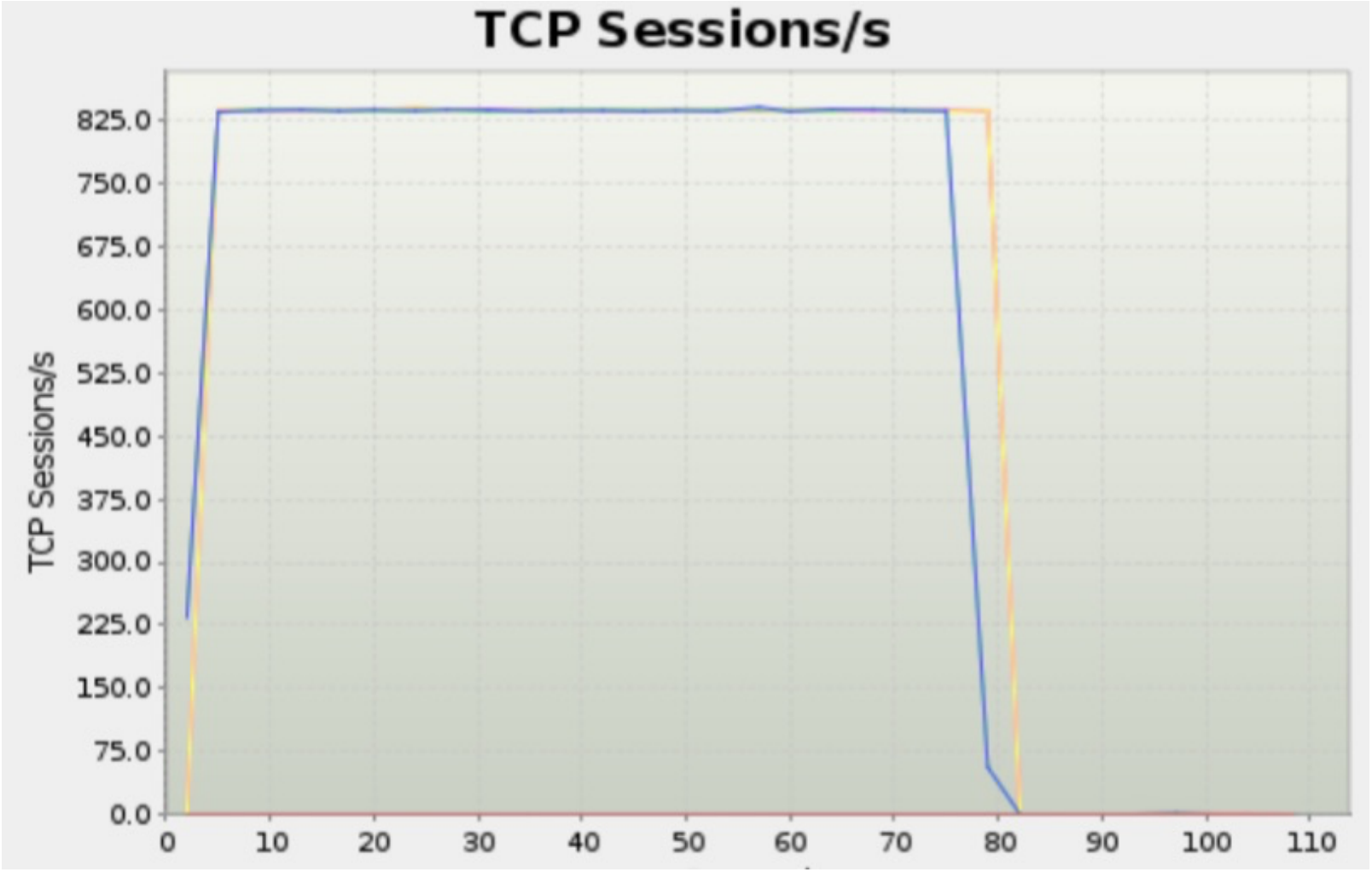
2500 сессий в секунду – устройство умирает через 27 секунд



ixia

#5: ИЩЕМ ПРИЧИНУ – СКОРОСТЬ ОБРАБОТКИ СЕССИЙ

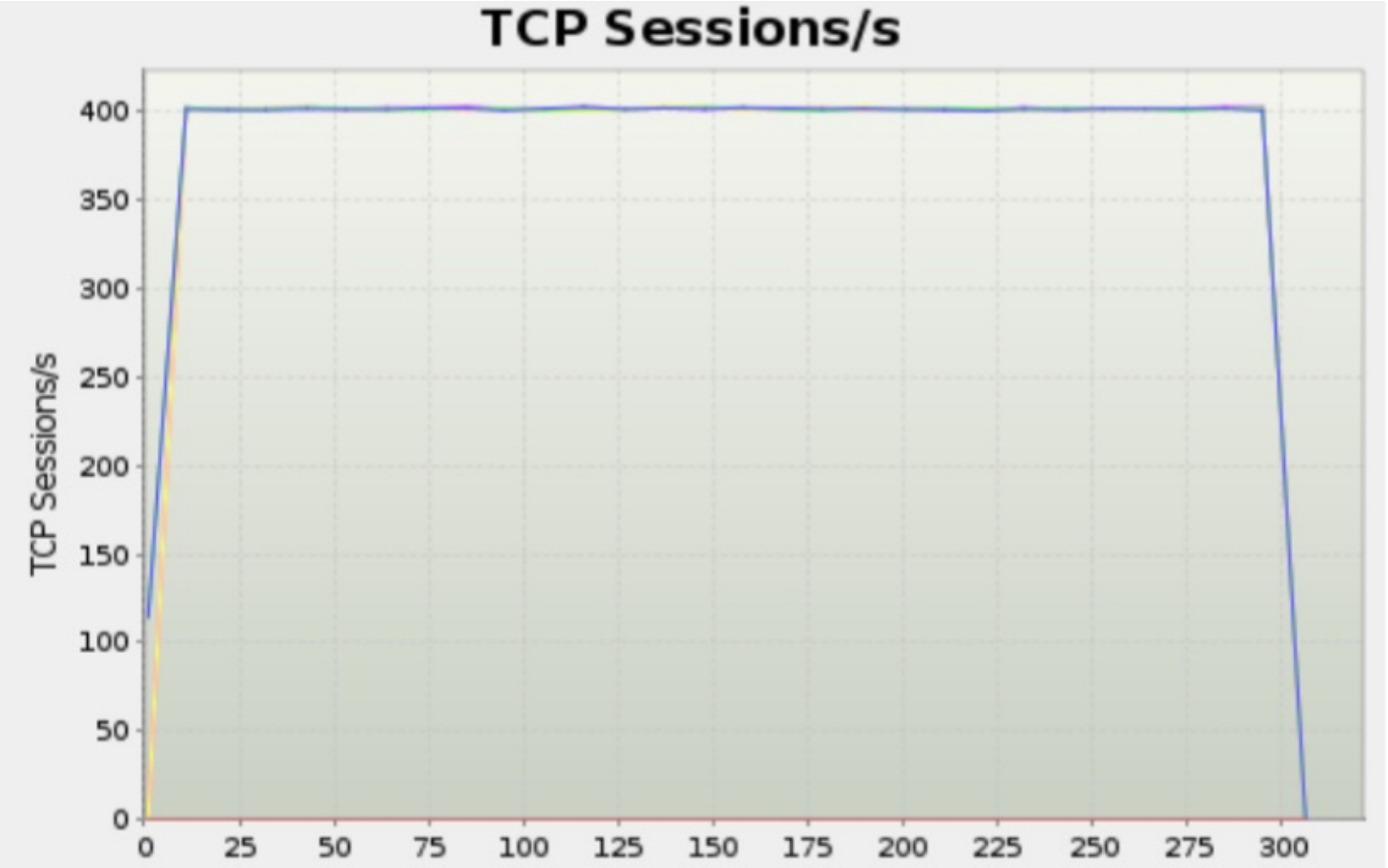
825 сессий в секунду – устройство умирает через 80 секунд



ixia

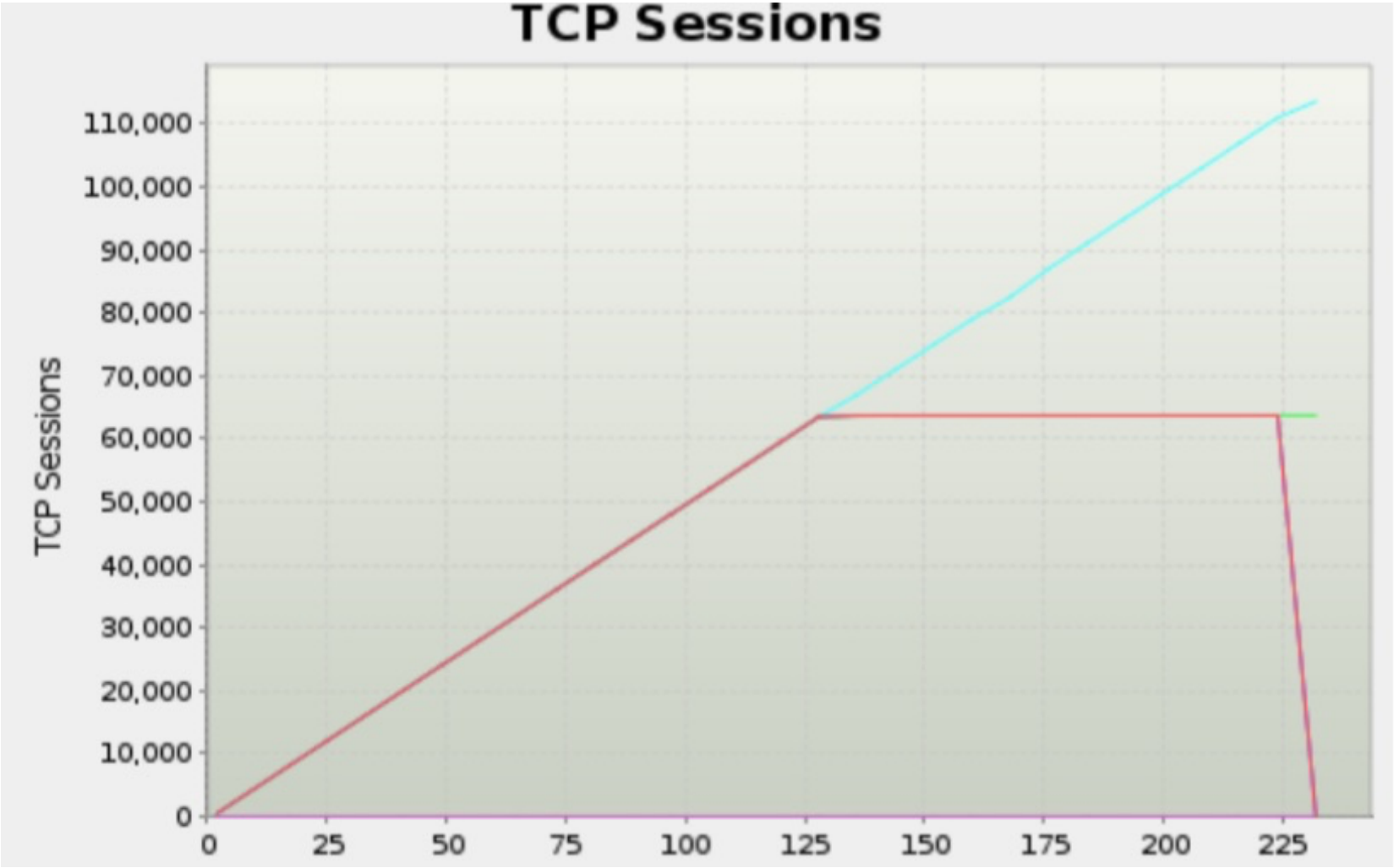
#5: ИЩЕМ ПРИЧИНУ – СКОРОСТЬ ОБРАБОТКИ СЕССИЙ

400 сессий в секунду – устройство проходит тест



#5: ИЩЕМ ПРИЧИНУ

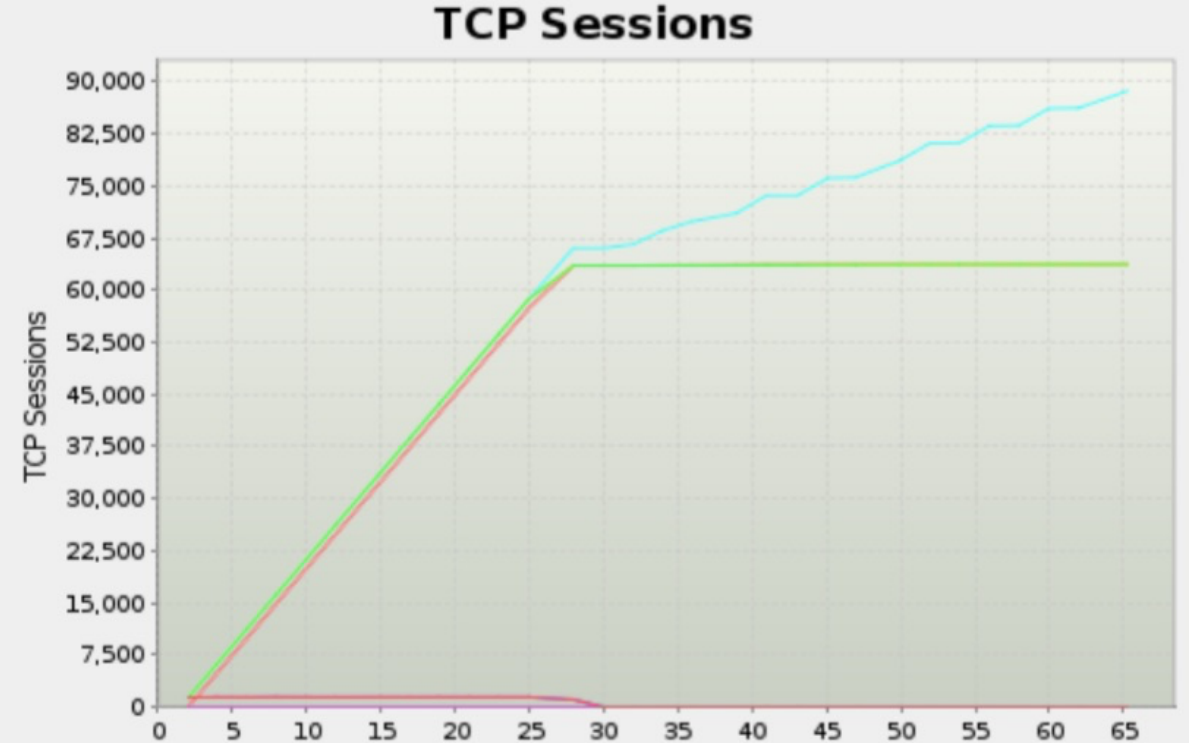
Предел 63 500 одновременных сессий



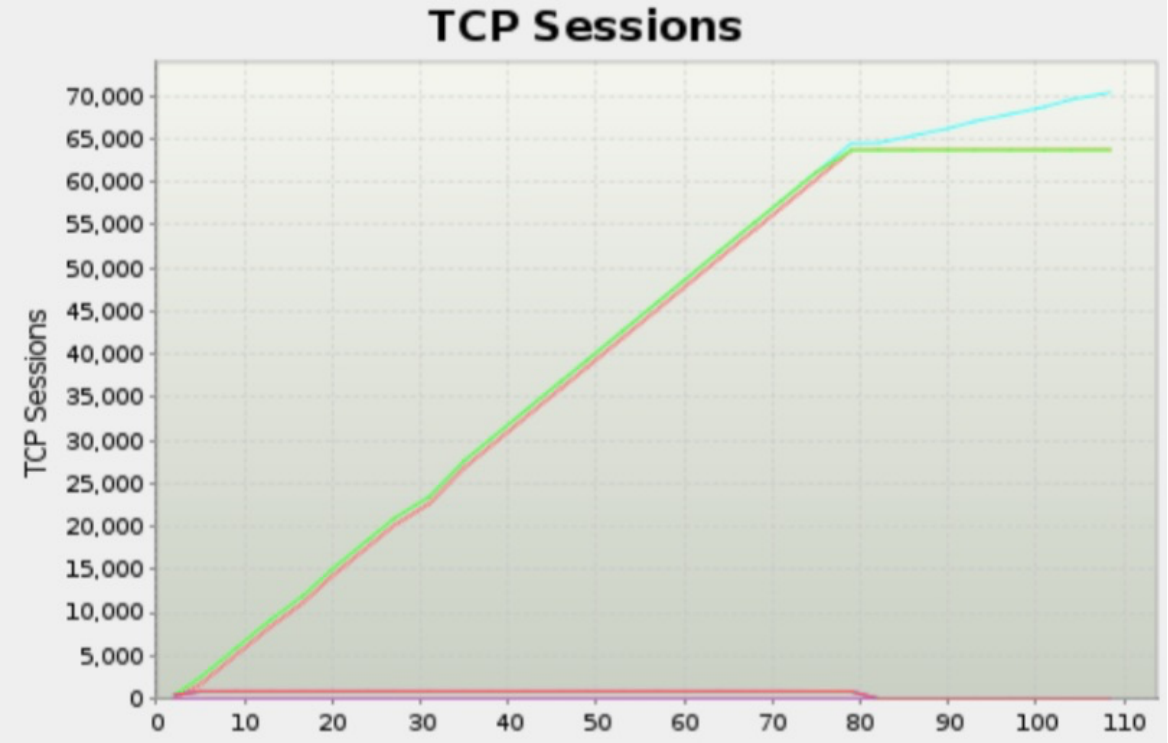
ixia

#5: ИЩЕМ ПРИЧИНУ – ОБЩЕЕ ЧИСЛО СЕССИЙ ПРИ ОТКАЗЕ

Во всех не пройдённых тестах было 63 500 открытых + закрытых сессий



2500 сессий в секунду



825 сессий в секунду

ixia

#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…


ixia