ixia
A Keysight Business

РЕШЕНИЯ ДЛЯ КИБЕРБЕЗОПАСНОСТИ И ТЕСТИРОВАНИЯ ПРИЛОЖЕНИЙ

APPLICATIONS + SECURITY HARDWARE PLATFROM

CloudStorm™

- 2.4 Terabit Platform – 200G per load module
- Highest SSL and IPsec performance with strong encryption
- Linerate 100G Apps + DDoS
- QSFP28, 100/50/40/25/10GE capable

PerfectStorm™

- 960 Gigabit Platform – 80G per load module or appliance
- Full crypto - SSL and IPsec
- Expand at your own pace with field-upgrades
- 100G CXP, 40G QSFP and 10/1 SFP+ with fan-out and small port count options

CLOUDSTORM™

Cloud-scale Applications & Security Test Platform

XGS12-HSL,12 slots

XGS2-HSL, 2 slots

- 12-slot or 2-slot easily manageable multi-user system
- Full crypto - SSL and IPSec
- Line-rate apps + DDoS on a single module
- Complete feature parity with PerfectStorm
- 5-speeds supported – 10G/40G/25G/50G/100G with speed-down and fan-outs

CloudStorm Fusion	CloudStorm Non-Fusion
• BreakingPoint • IxLoad	• IxLoad
• XGS12-HSL Chassis • XGS2-HSL Chassis	• XGS12-HSL Chassis • XGS2-HSL Chassis

ixia
A Keysight Business

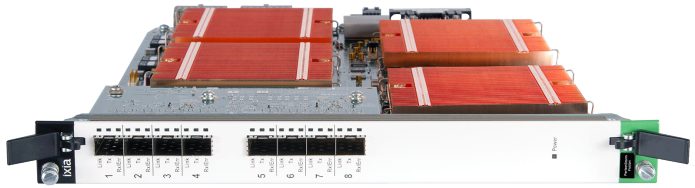
PERFECTSTORM™

Unified Applications & Security Test Platform

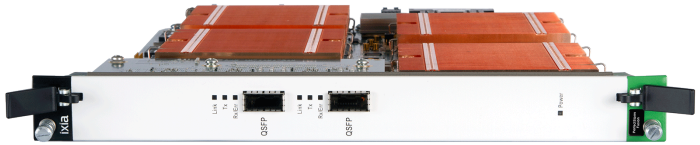
XGS12,12 slots

XGS2, 2 slots

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



2-ports of 40GE with QSFP+ interface



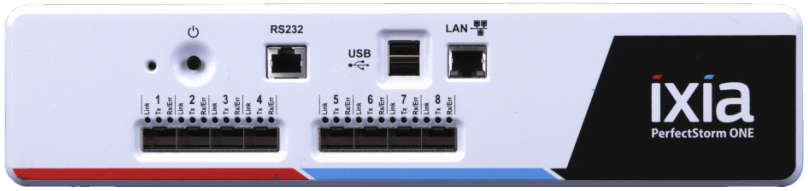
1-port of 100GE with CXP interface

- 12-slot or 2-slot easily manageable multi-user system
- Industry's leading performance - 80Gbps of application and 20Gbps of SSL, 40Gbps of IPsec performance per card
- Flexible fanout options

PerfectStorm Fusion	PerfectStorm Non-Fusion
• BreakingPoint • IxLoad	• IxLoad
• XGS12-HS/HSL Chassis • XGS2-HS/HSL Chassis	• XGS12-SD/HS/HSL Chassis • XGS2-SD/HS/HSL Chassis

PERFECTSTORM ONE™

Портативный ПАК для тестирования комплексов сетевой защиты



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

2-ports of 40GE with QSFP+ interface

- Increased portability, reduced footprint and power consumption (1.5U)
- Industry's leading performance - 80Gbps of application and 20Gbps of SSL and 40Gbps of IPsec performance per appliance
- Flexible fan-out options

PerfectStorm ONE Fusion	PerfectStorm ONE Non-Fusion
• BreakingPoint • IxLoad	• IxLoad

ixia
A Keysight Business

CLOUDSTORM VS PERFECTSTORM

BreakingPoint 8.50

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

This is a subset of the performance matrix; subject to change

ixia
A Keysight Business

МАСШТАБИРУЕМОСТЬ

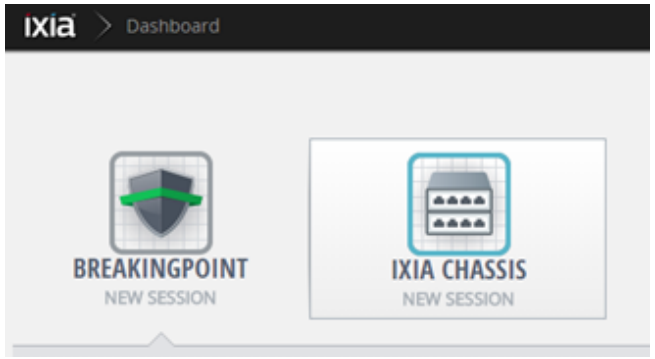
Развивайте системы Perfect Storm согласно ваших потребностей

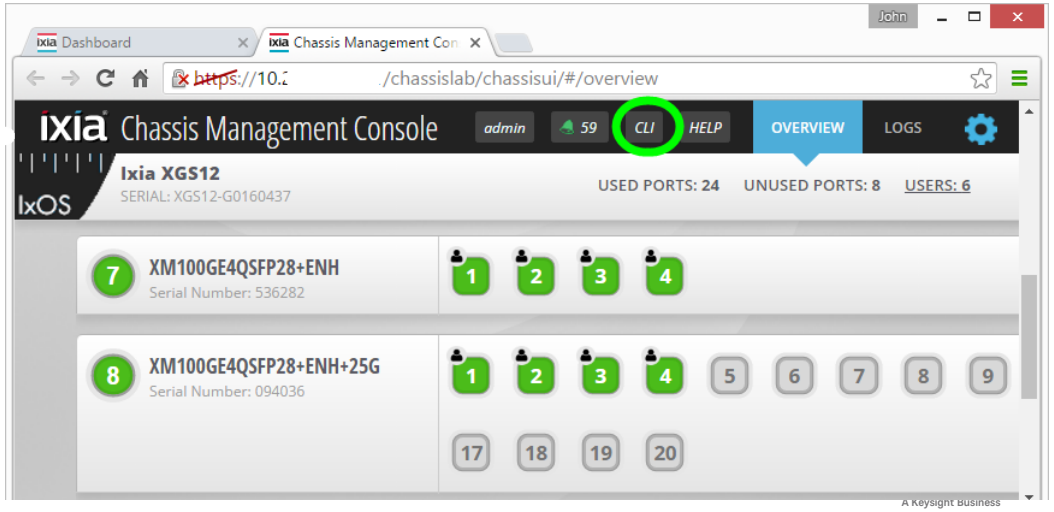
- Модель Pay-as-you-grow для уменьшения CAPEX
- In-field апгрейды для
  - Non-Fusion ➔ Fusion
  - Low port counts ➔ Fully populated systems
  - Low speed ➔ High speed (1G→10G)
- Гибкие встроенные опции fan-out

NATIVE IXOS

Новая упрощенная архитектура

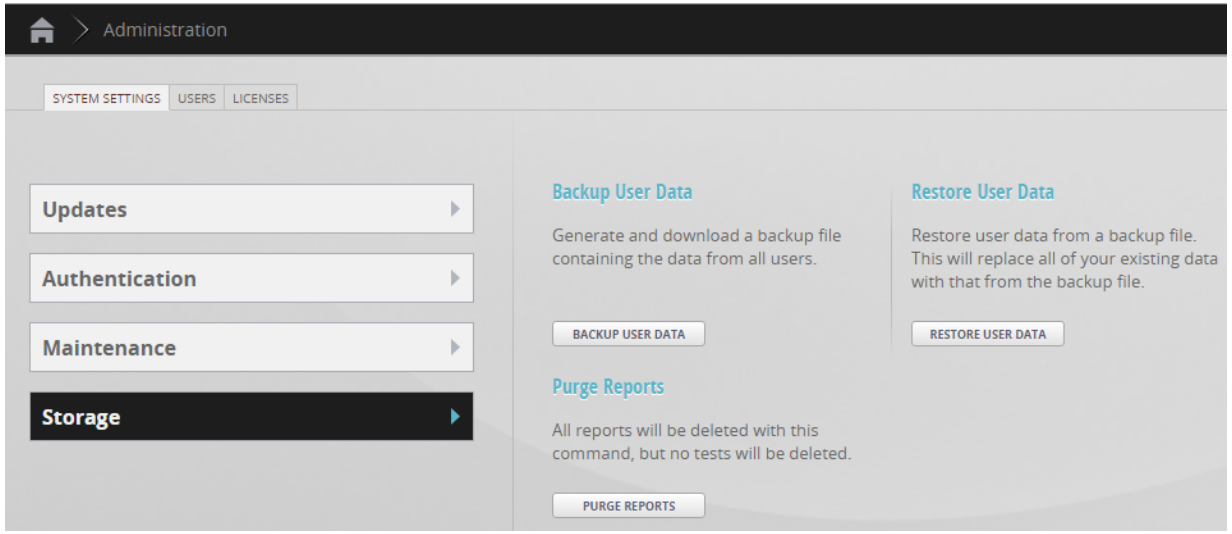
- Linux-only environment on PerfectStorm ONE, XGS12-HSL and XGS2-HSL chassis – Windows-free environment
- Single management IP
- New IxServer HTML5 WebUI
- New Chassis CLI
- Faster system bootup & test initialization
- Existing units are field upgradable
- Supports CloudStorm, PerfectStorm, Multis, Novus and Xcellon-Ultra NP variants, other load modules will only be supported on the Windows based chassis





NATIVE IXOS – УЛУЧШЕНИЯ BREAKINGPOINT

- Более высокая масштабируемость и улучшенная стабильность для более интенсивных конфигураций BPS
- Новый механизм Backup/Restore для BPS
  - Local computer
  - NFS Share
  - USB Drive



ixia
A Keysight Business

ПРОИЗВОДИТЕЛЬНОСТЬ NATIVE IXOS

ixia

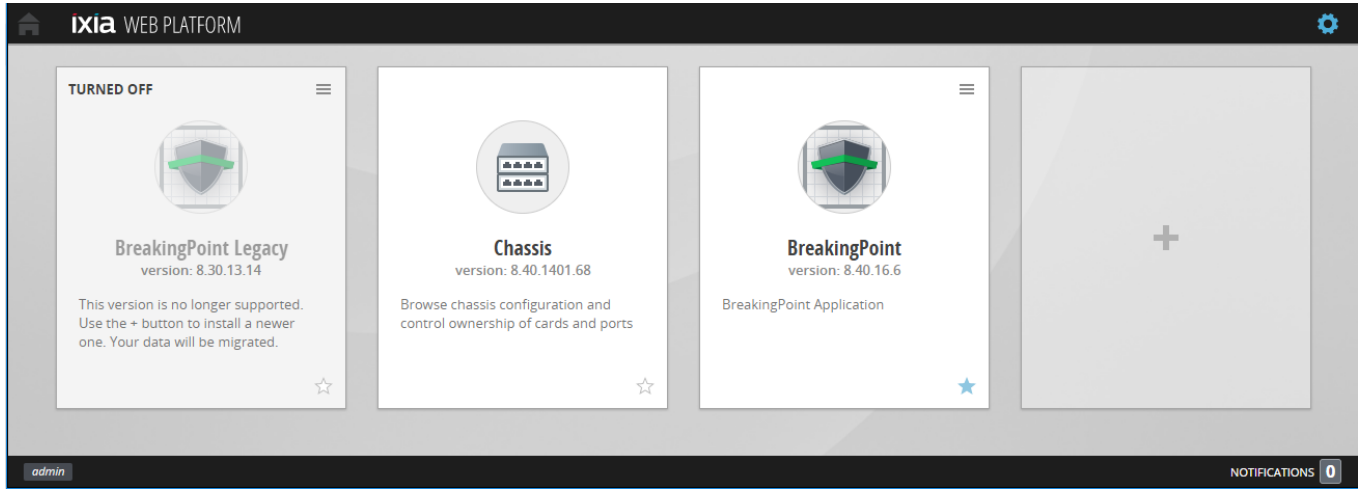
HSL OVER HS PERFORMANCE IMPROVEMENTS

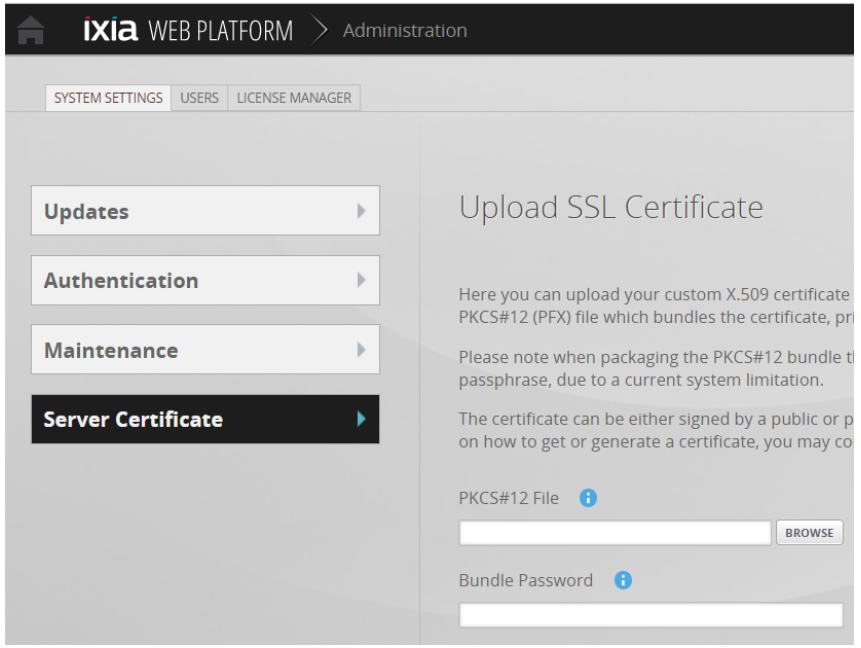
XGS Chassis family

ixia
A Keysight Business

НОВАЯ WEB-ПЛАТФОРМА

- Новый workflow - Разделение Шасси и ПО BreakingPoint (начиная с версии 8.40)
  - Загрузка пользовательских сертификатов X.509 SSL для web-сервера
  - Управление пользователями и лицензированием доступно глобально из web-платформы
  - Избранные (“★“) приложения для прямого доступа без логина



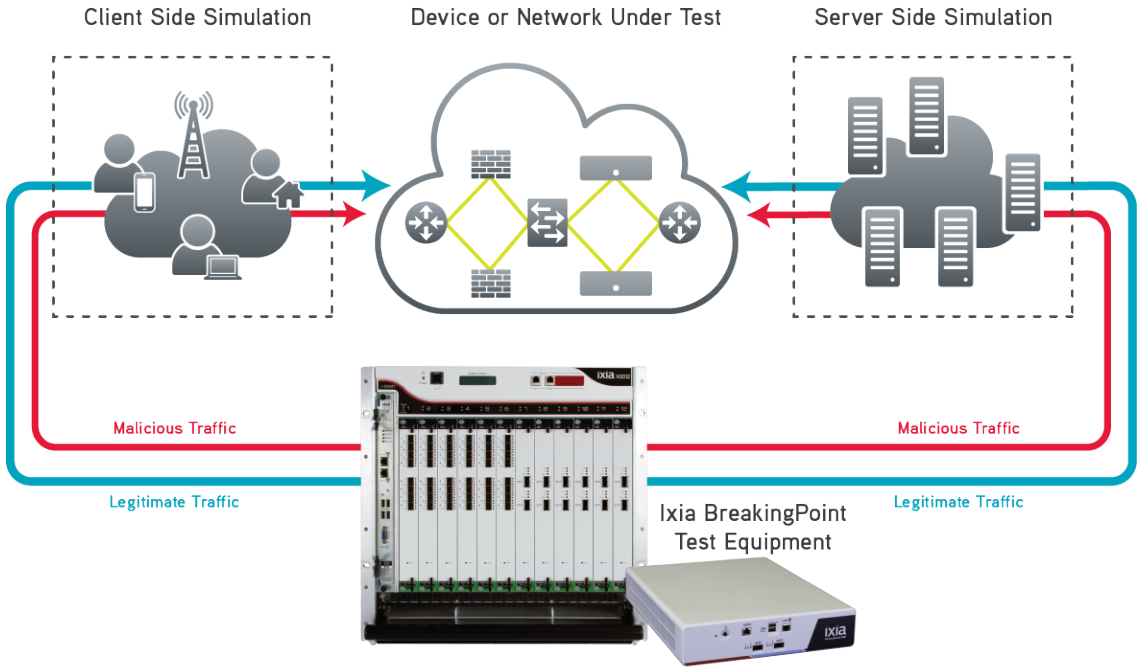


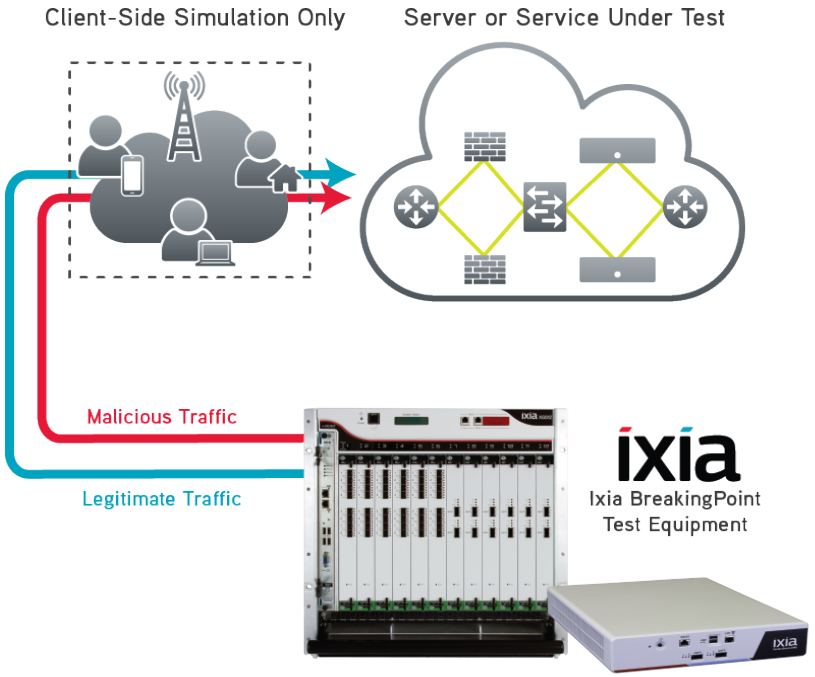
ixia
A Keysight Business

ОБЗОР ПО BREAKINGPOINT

ТОПОЛОГИИ ТЕСТИРОВАНИЯ

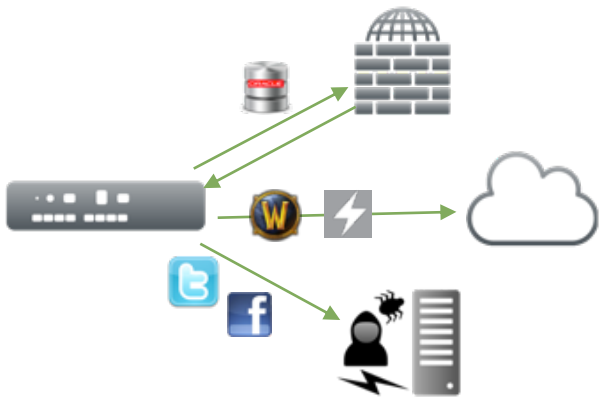
ПО Breakingpoint воспроизводит реальные сетевые условия, включая масштаб и содержание трафика для комплексной проверки устройств и сервисов сетевой защиты

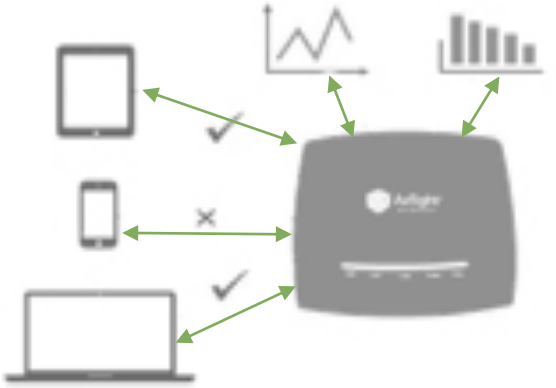




ixia
A Keysight Business

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

ixia
A Keysight Business

РЕАЛИСТИЧНЫЙ ТРАФИК

- 360+ 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

DDOS and botnet simulation

Identify unknown applications

Detect traffic geo-location

7000+ exploits

30,000+ malware

100+ evasions

ATI RESEARCH CENTER

IXIA INTELLIGENCE

- Ixia engineers
- Security vendors
- Packet broker flows
- NEM Interactions

SECURITY RESEARCH LABS

GLOBAL NETWORK OF HONEYPOTS AND WEB CRAWLERS

BIG DATA SOURCES

- Billions of IPs and URLs
- Millions of SPAM
- Open source data sets
- Network intrusions

26 biweekly updates | NEW applications | NEW DDoS/APT

ixia
A Keysight Business

ПРИМЕНЕНИЕ ATI

Security and DPI Testing

BreakingPoint

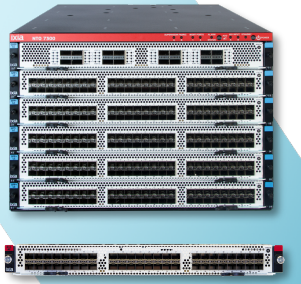
Network Assessment

Perfect Storm

IxLoad

IxChariot

Application Visibility



Application & Threat Intelligence Processors

Inline Security

ThreatARMOR™

Equipment Manufacturers

Enterprise Networks

Service Providers

ixia
A Keysight Business

КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ

Полная проверка периметра безопасности вашей сети

Largest Collection of Exploits, Malware

- 7,000+ exploits
- 30,000+ malware
- Mobile malware
- Strike fuzzing
- Unique attack payloads in each transaction

Most Complete Set of Evasions

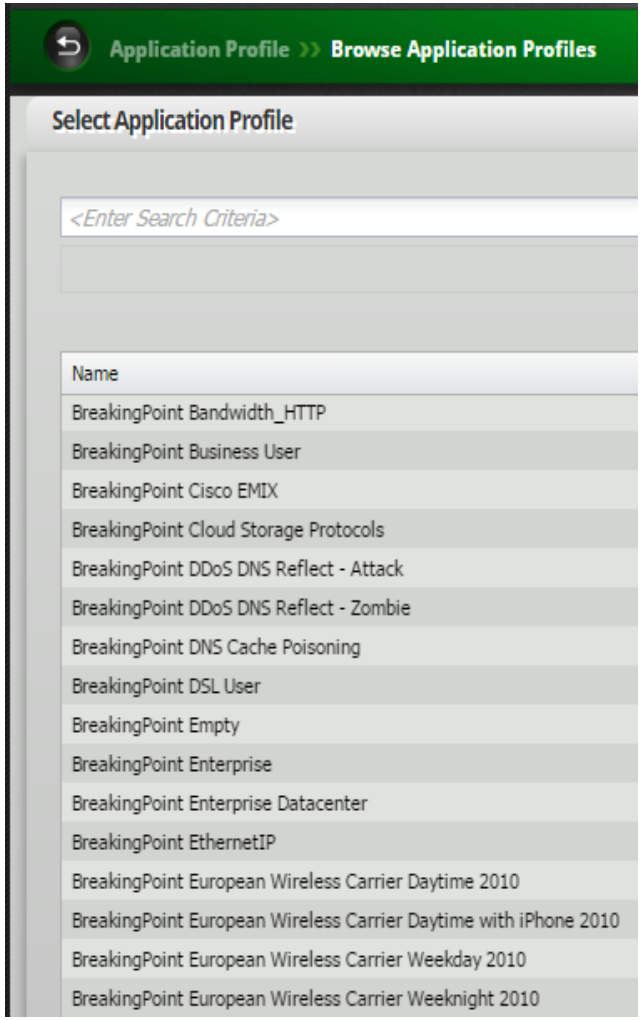
- 100+ evasion techniques
- Validate against malware polymorphism

DDoS, Botnet, and APT Simulation

- Botnets emulating zombie to C&C communication
- Volumetric, protocol, and application-layer DDoS attacks

ixia
A Keysight Business

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

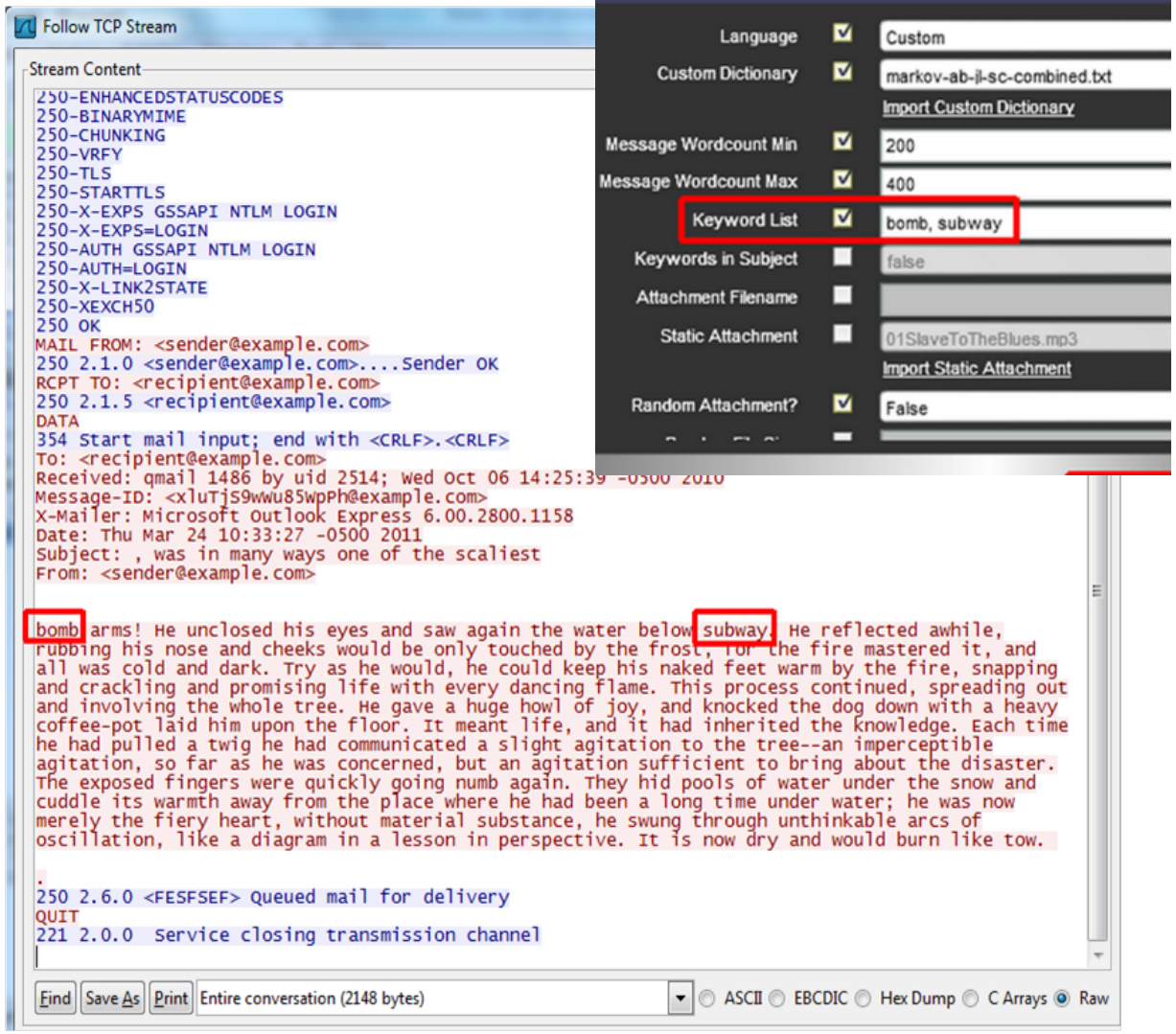
#	Action	#	Flow	Source
1	Resolve	1	DNS	client
2	Accept TLS	2	Google Mail	server
3	Start TLS	2	Google Mail	client
4	Sign into Gmail	2	Google Mail	client
5	Response to Gmail Sign in	2	Google Mail	server
6	Resolve	1	DNS	client
7	Accept TLS	3	Google Mail	server
8	Start TLS	3	Google Mail	client
9	Gmail Service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

ixia
A Keysight Business

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)



ixia
A Keysight Business

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

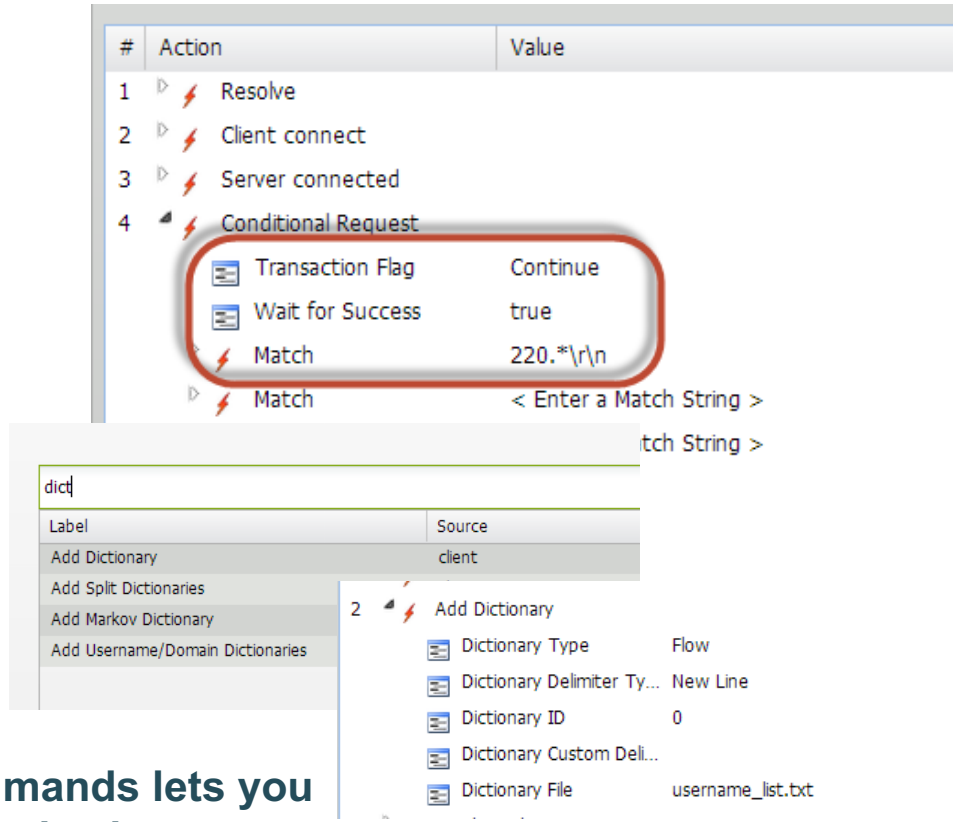
ixia
A Keysight Business

ДИНАМИЧНЫЕ СИМУЛЯЦИИ

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

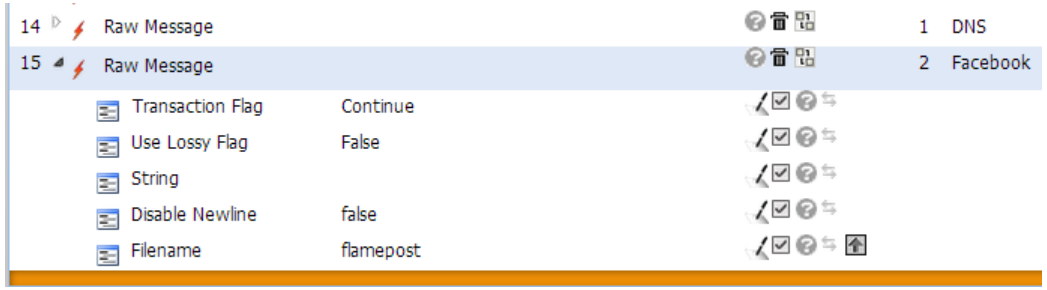
- Conditional Requests (запросы с условием)
- Dictionary commands (поля из словаря/файла)
- Raw commands (произвольные команды)

#1 Conditional requests in applications



#2 Dictionary commands lets you insert user specified values

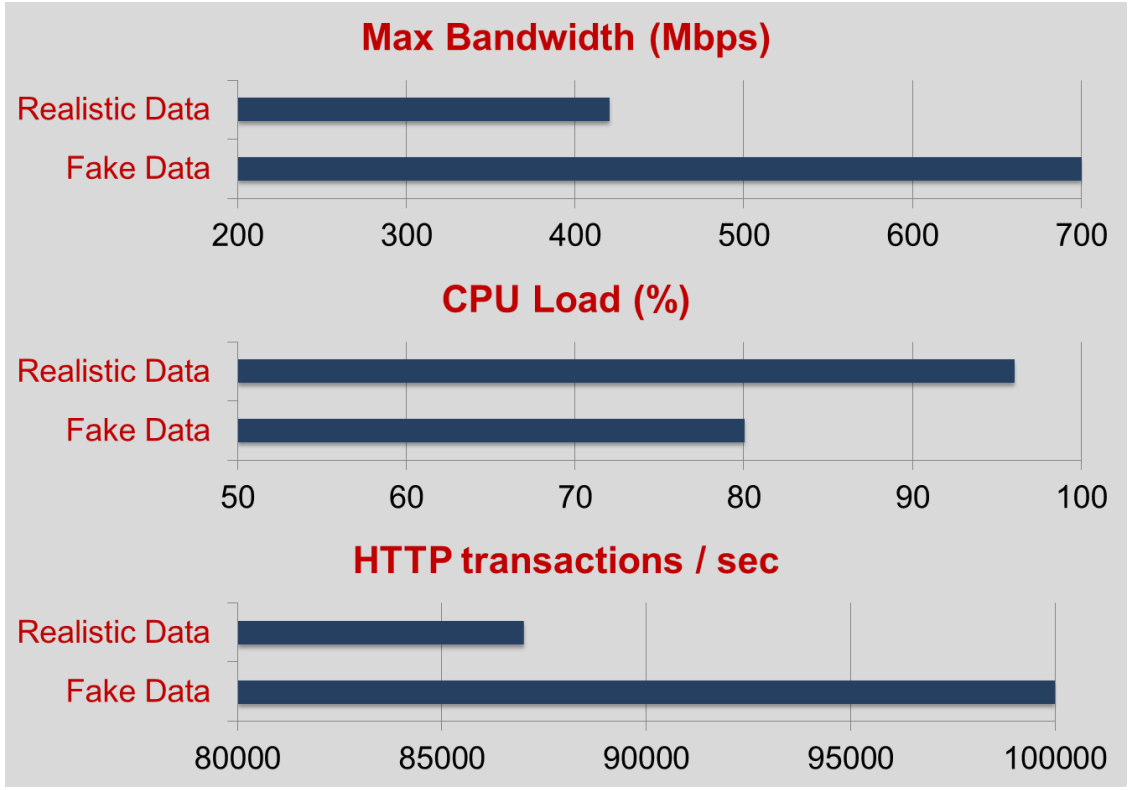
#3 Raw actions let you craft your own command within an application.



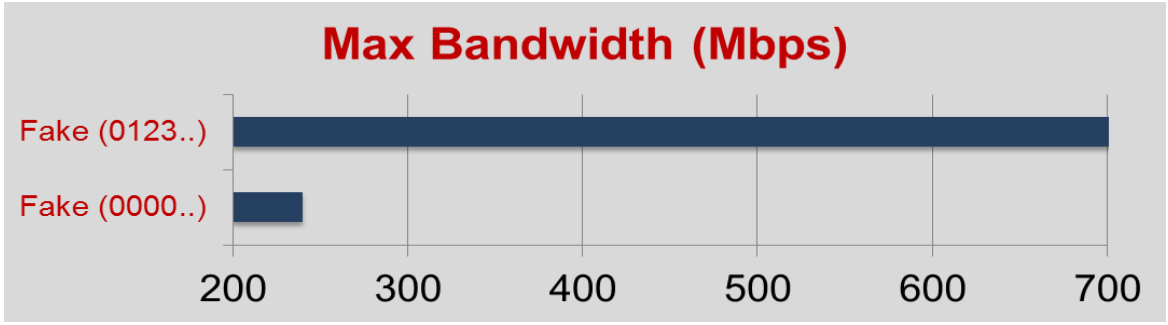
ixia
A Keysight Business

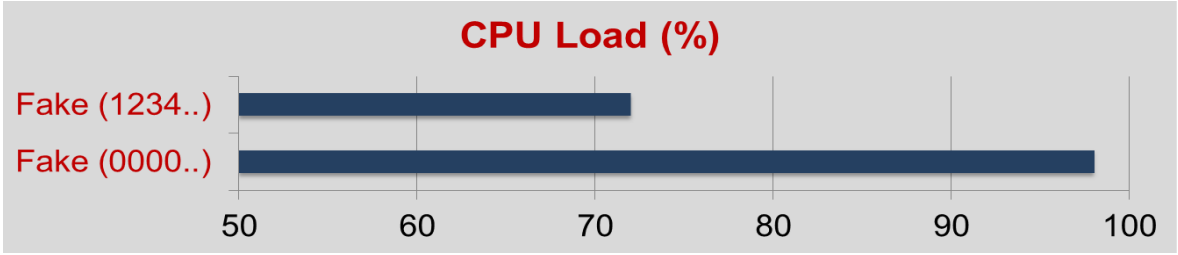
СОДЕРЖАНИЕ ИМЕЕТ ЗНАЧЕНИЕ!

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



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



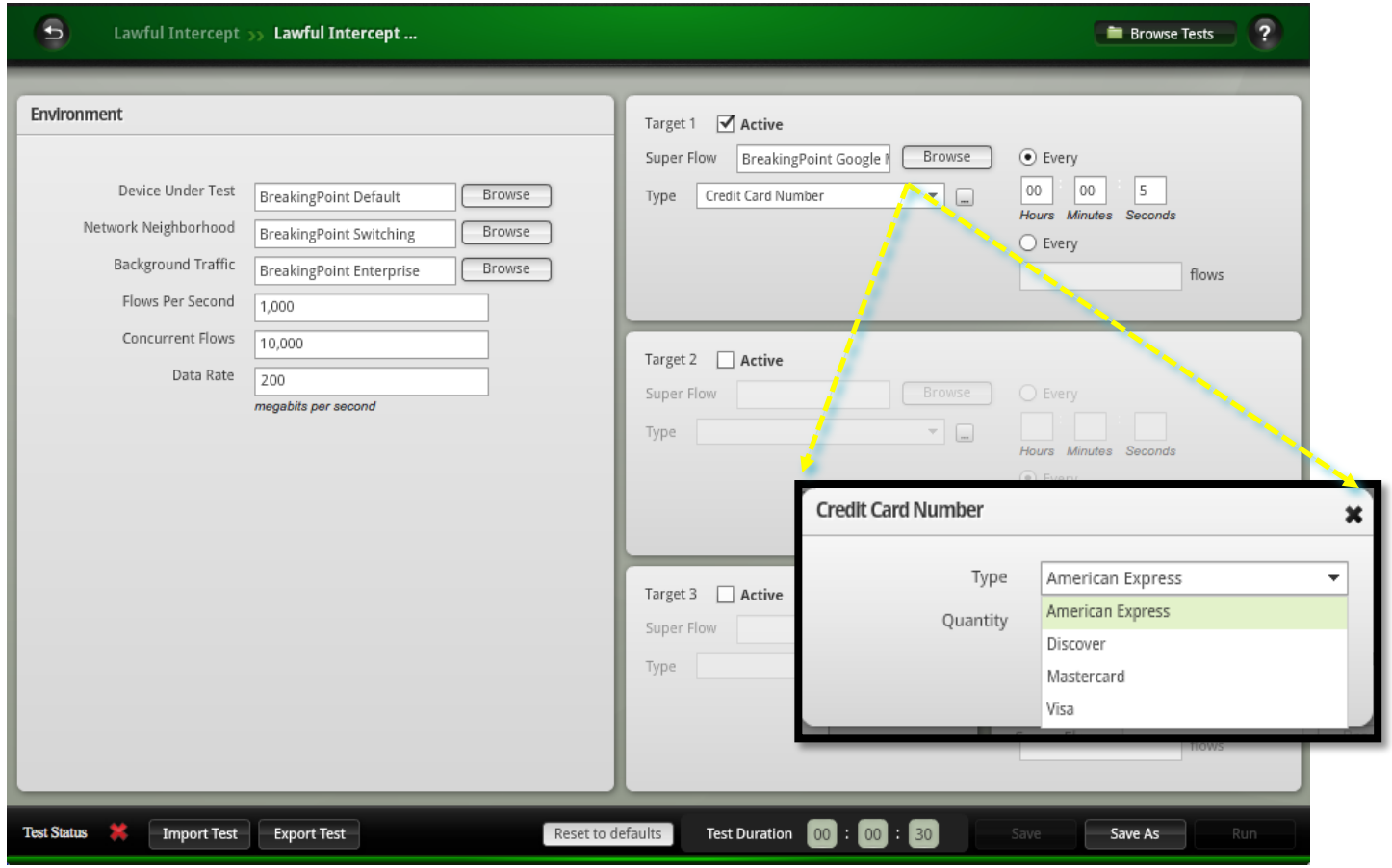


HTTP payload with all '0000s' vs '012345..9'

ixia
A Keysight Business

#2: ТЕСТИРОВАНИЕ СИСТЕМ DLP

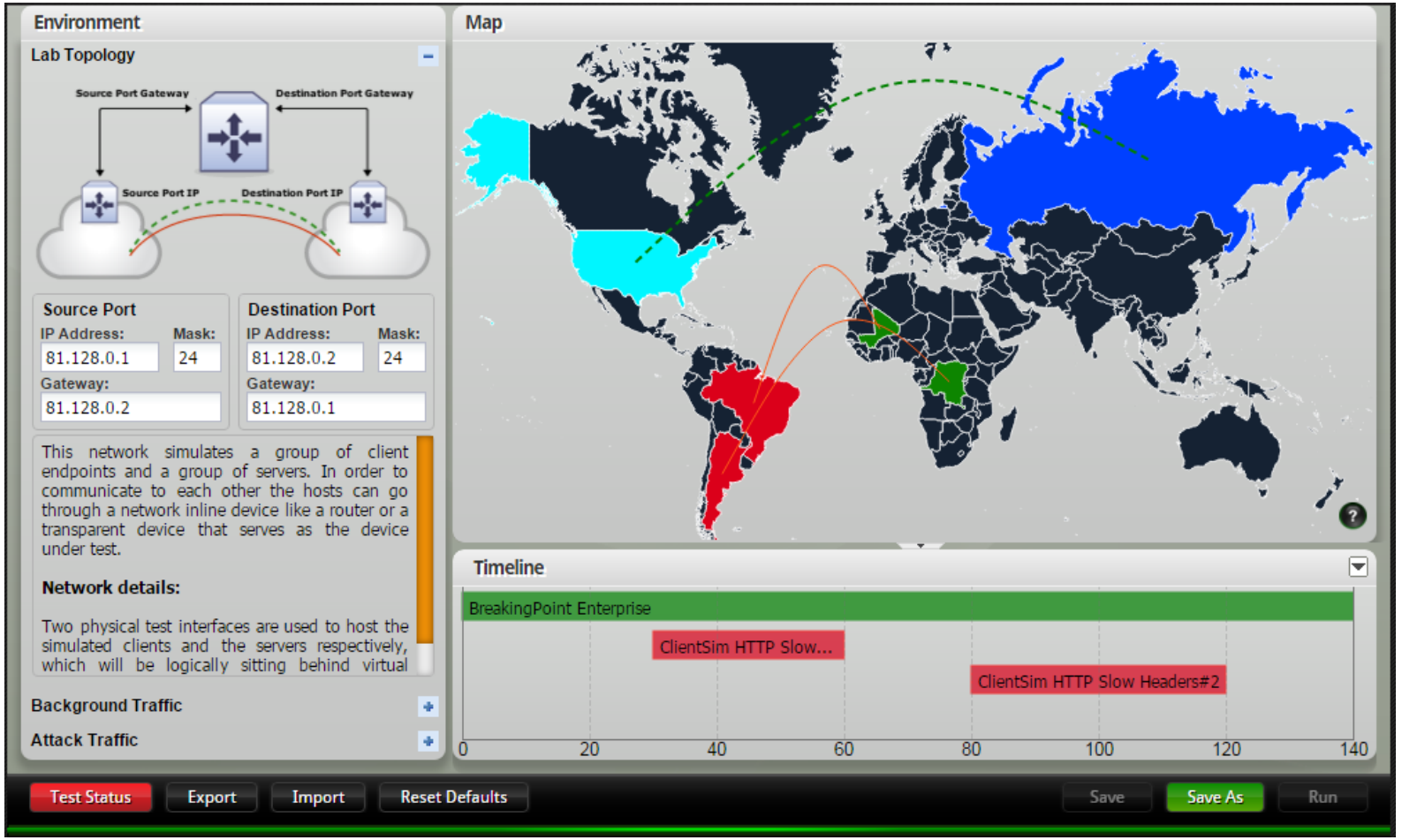
- Генерация мощного потока реального трафика с подмешиванием ключевых слов
- Каждые X секунд или Y потоков
- Детальные отчеты по каждому событию



ixia
A Keysight Business

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



ixia
A Keysight Business

ОТКАЗОУСТОЙЧИВОСТЬ СЕТИ

Fuzzing Application Protocols

- Validates integrity of protocol stacks and robustness of your devices with malformed packets
- Generates corrupt data by modifying part of the packet
  - Random or user-defined payload
  - Data rates: constant, range, random
  - Bad IP version, checksum, options; bad TCP options, urgent pointer, etc.
  - Pseudo random number generator (PRNG) seed for repeatable testing

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

TEG / HTTP/1.1

{{{{ / HTTP/1.1

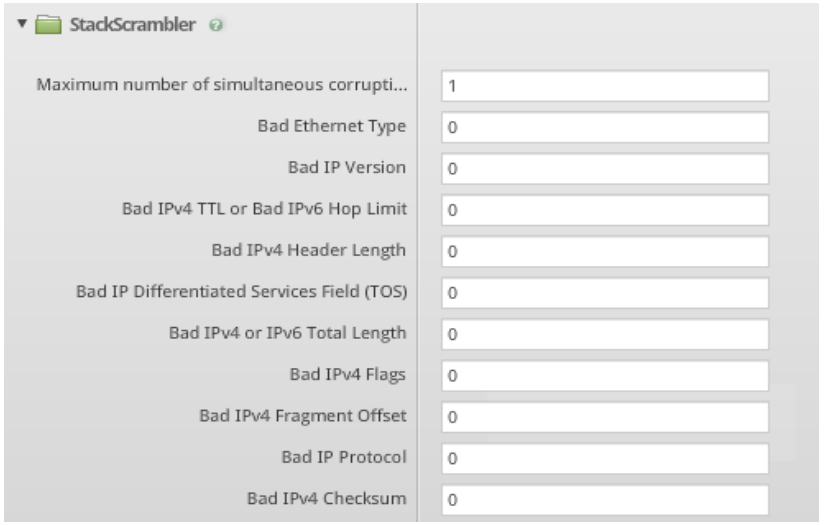
GET `` HTTP/1.1

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

GET / ***1.1/PTTH***

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

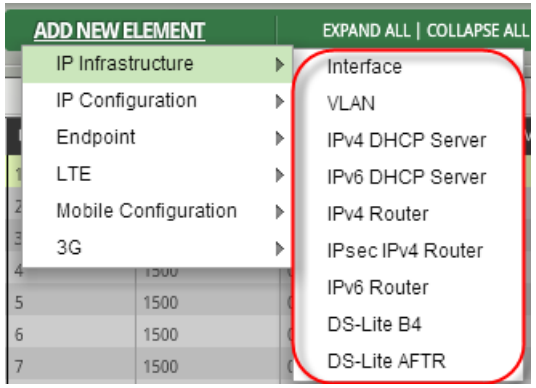
Fuzzing a single HTTP Get request flow could surpass 100,000 requests at runtime.

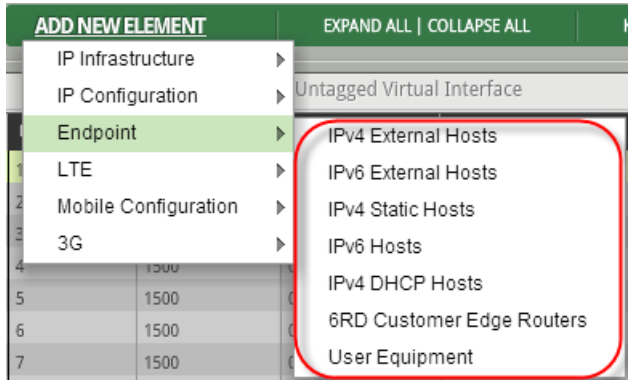


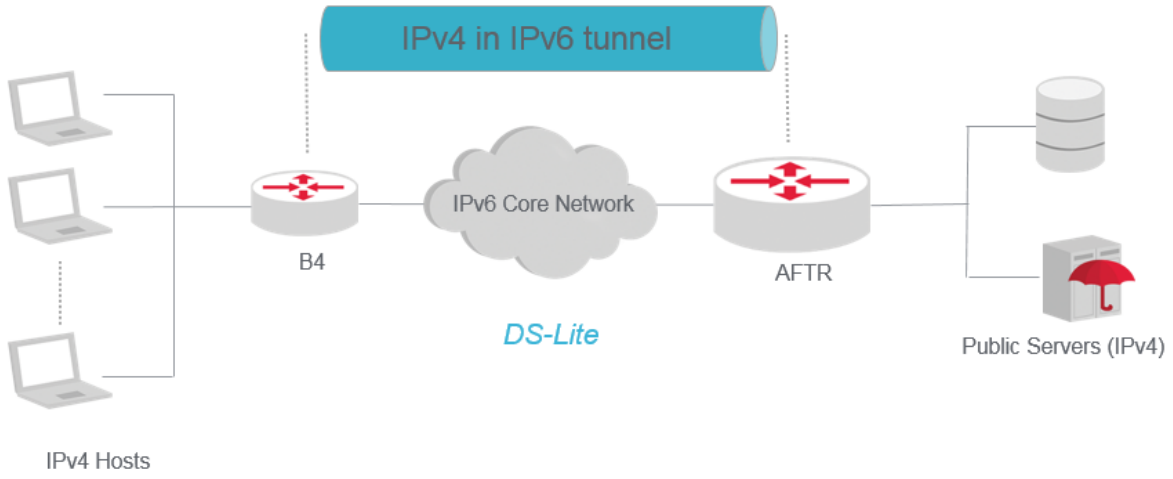
ixia
A Keysight Business

ШИРОТА СИМУЛЯЦИИ СЕТЕВОГО ДОСТУПА

- Subscriber network connection emulation across multiple underplaying infrastructures
  - DHCPv4/6
  - VLAN (802.1Q, QinQ)
  - Virtual Router instances
  - GTPv1/v2
- Extend application and security validation in the context of IPv6 readiness
  - Integrate with IPv6 transitioning technologies:
    - DS-Lite, 6rd
    - DHCP-PD
    - SLAAC

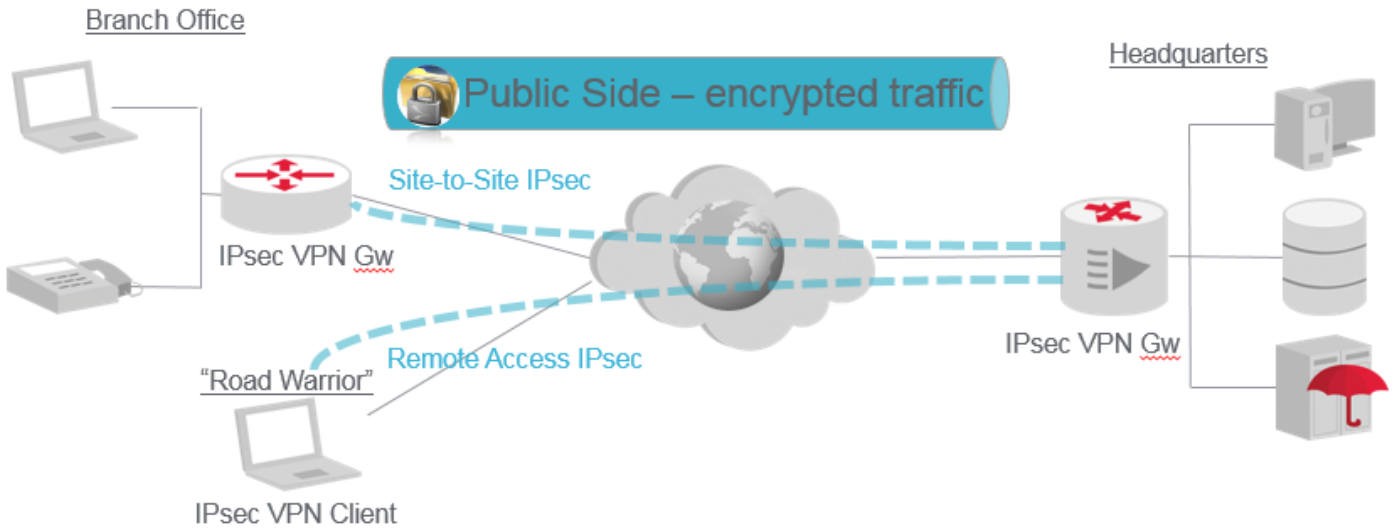






ТЕХНОЛОГИИ IPSEC VPN

- Реалистичная эмуляция IPsec с учетом отраслевых сценариев
  - Site-to-site и remote access VPN
  - Приложения, инкапсулированные в IPsec
  - Fuzzing поверх IPsec
  - Унифицированное тестовое решение для брандмауэров, UTM и интегрированных устройств безопасности



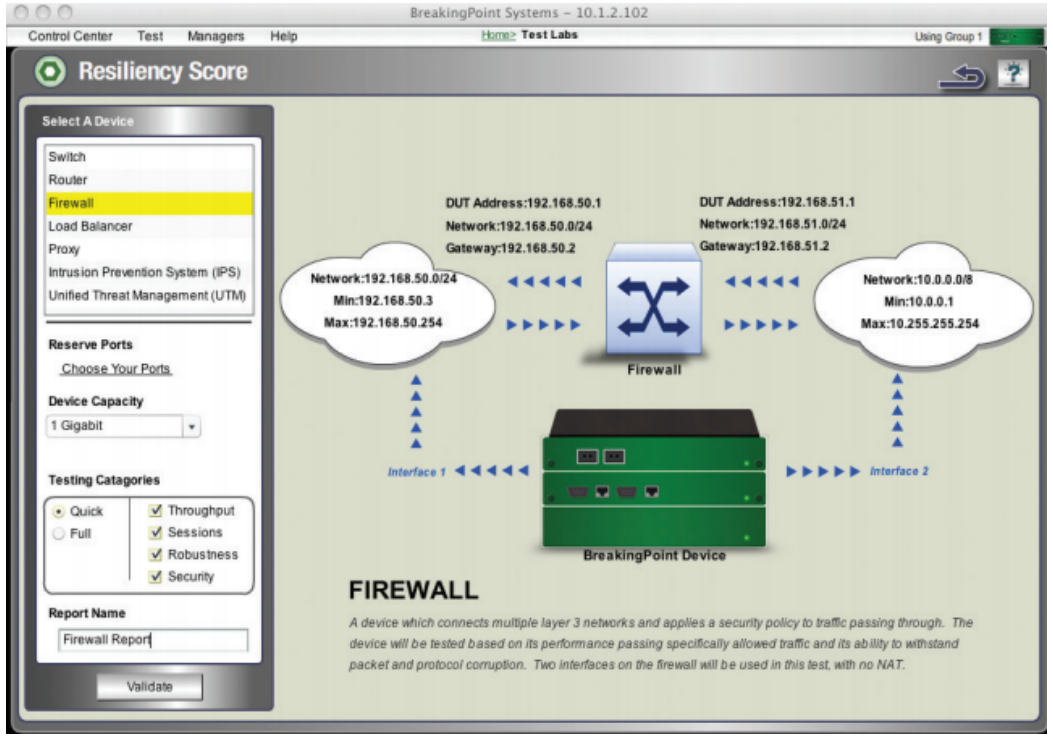
ixia
A Keysight Business

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



ixia
A Keysight Business

BREAKINGPOINT – ПРЕИМУЩЕСТВА

- Поддерживается на физических, виртуальных и публичных облачных платформах
- Пользовательский интерфейс HTLM5 (установка программного обеспечения клиента не требуется)
- Более быстрое тестирование, лучшая производительность
- Лицензирование по принципу «Все включено»
- REST API и TCL API для автоматизации и оркестрации
- Встроенная отчетность и статистика в реальном времени
- Поддержка авторизации с помощью TACACS+
- Единственное решение на рынке, соединяющее производственную сеть и лабораторию (с TrafficREWIND)

DEMO
BREAKINGPOINT
DDOS ATTACK

CUSTOMER USE CASE
VALIDATE DDOS MITIGATION – FINANCIAL EXCHANGE

Customer

- World's leading derivatives marketplace
- 3 billion in contracts annually

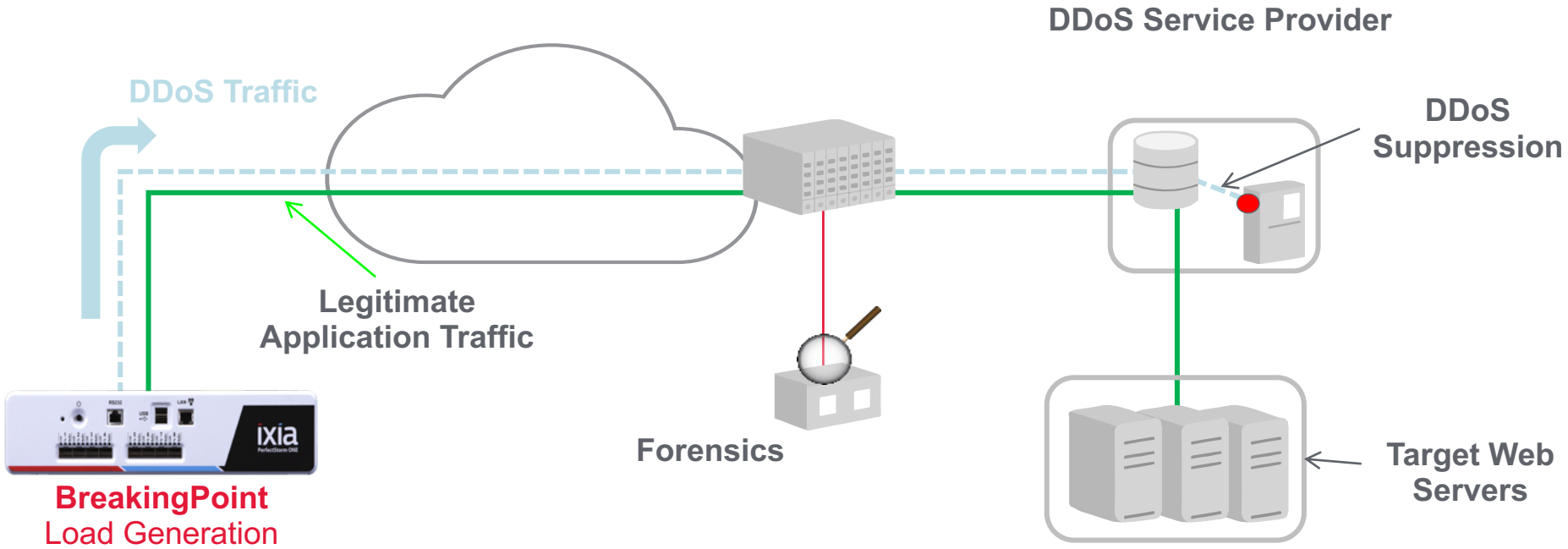
Need

- Validate DDoS mitigation service provider
- Reduce mitigation time
- Improve cyber attack readiness

Results

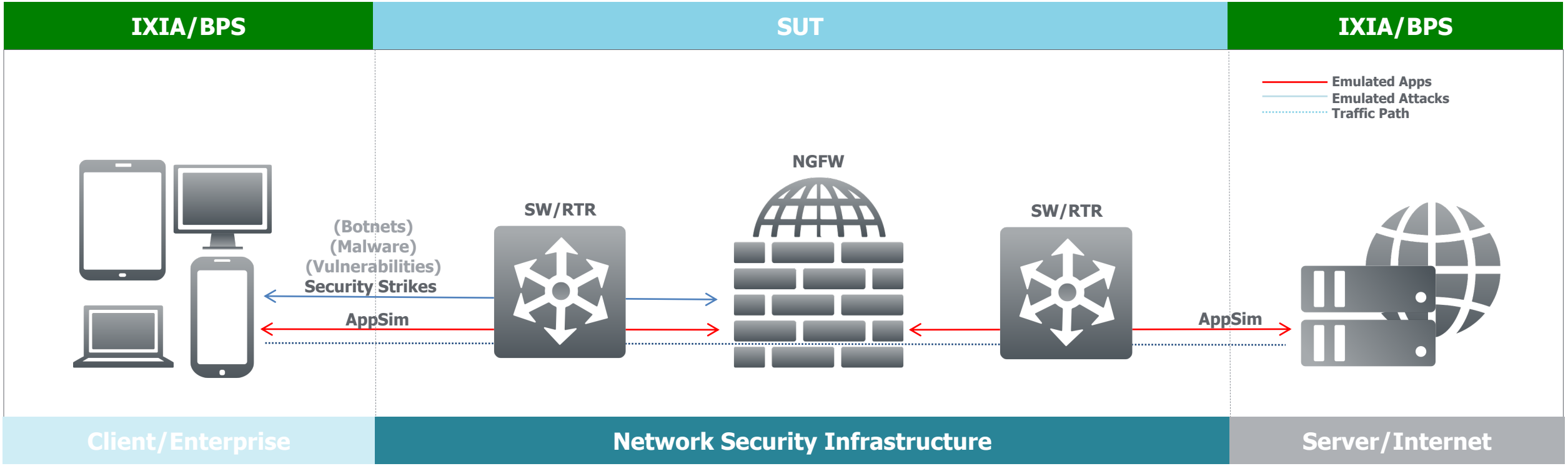
- 10x Improvement of DDoS protection activation speed
- Improved cyber resiliency and readiness

CUSTOMER USE CASE
VALIDATE DDOS MITIGATION – FINANCIAL EXCHANGE



CUSTOMER USE CASES

ТЕСТИРОВАНИЕ – NGFW/IPS/DPI/UTM

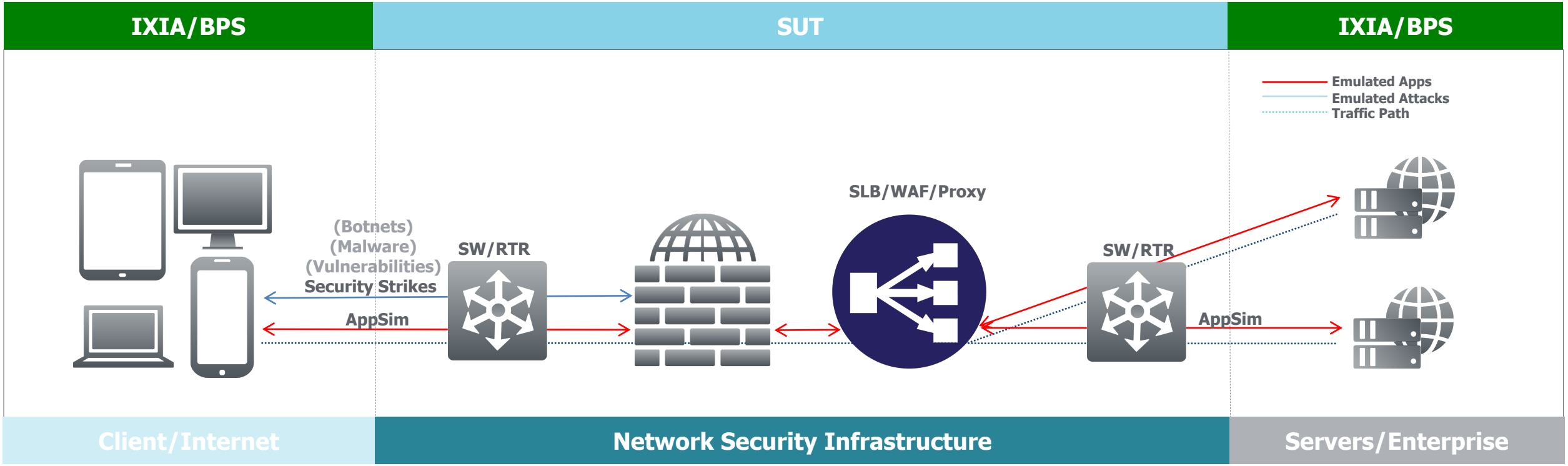


Test Methodologies

Internet scale | Realistic application mix | Variety of security attacks | Up-to-date ATI | Dual-stack | Mobile transport

ixia
A Keysight Business

ТЕСТИРОВАНИЕ – SLB/WAF/PROXY

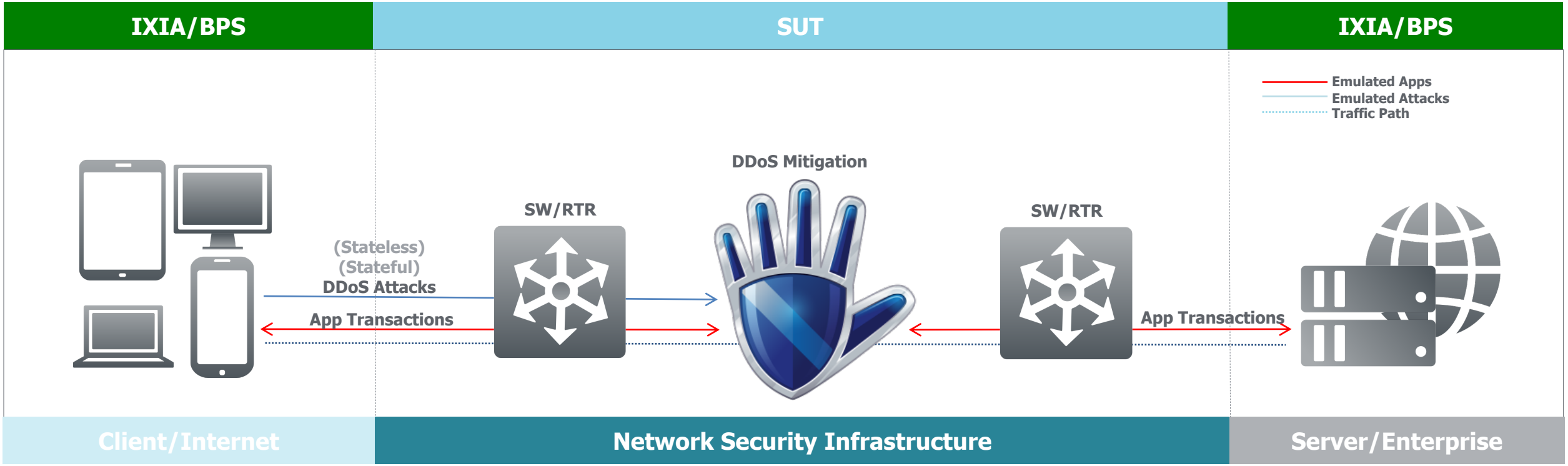


Test Methodologies

Performance | ClientSim | ServerSim | Up-to-date ATI | Security | Dual-stack

ixia
A Keysight Business

ТЕСТИРОВАНИЕ – DDOS MITIGATION

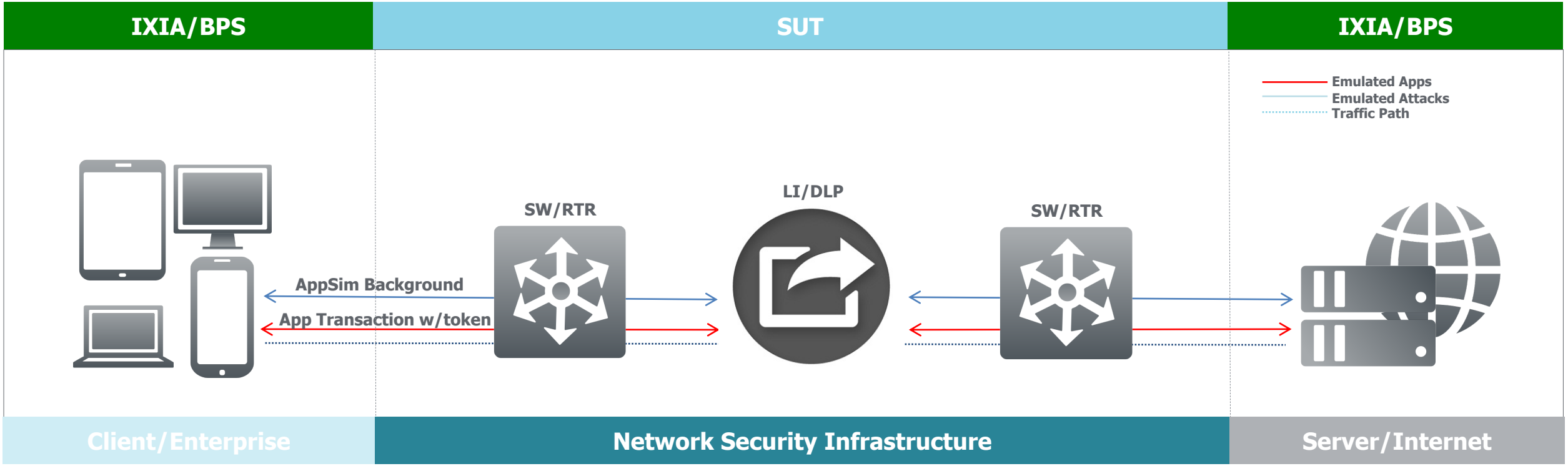


Test Methodologies

Large scale distributed DoS attacks | Legit application transactions | Up-to-date ATI | Easy-to-use DDoS Lab

ixia
A Keysight Business

ТЕСТИРОВАНИЕ – LAWFUL INTERCEPTION (LI)/DLP

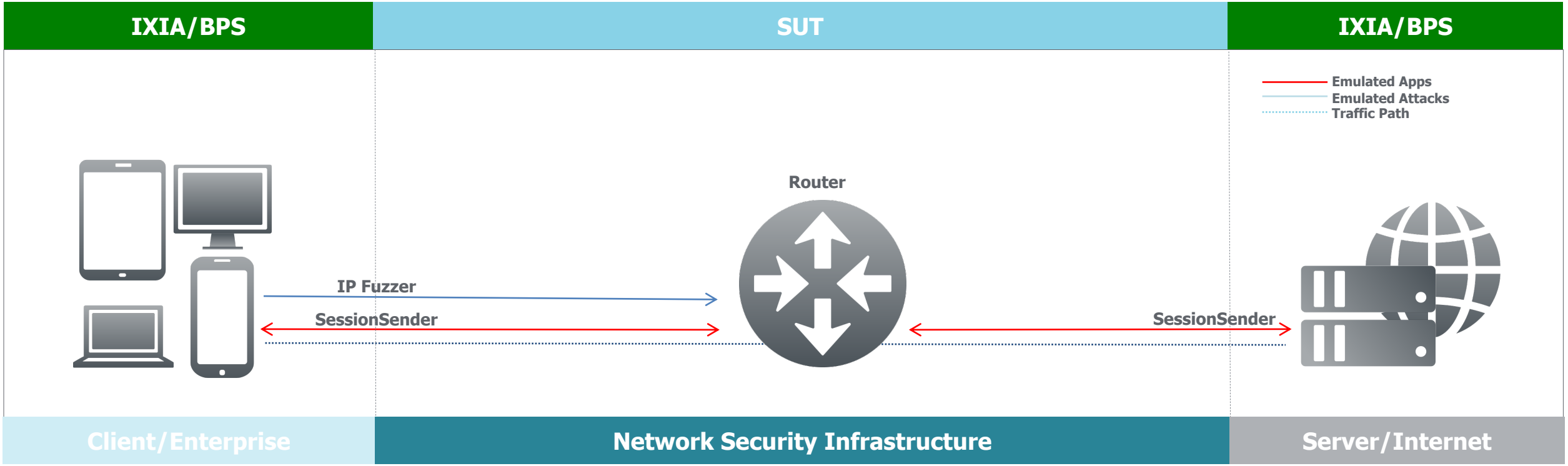


Test Methodologies

“Needle in a Haystack” | Up-to-date ATI | Dual-stack | Mobile transport

ixia
A Keysight Business

ТЕСТИРОВАНИЕ – ROUTER

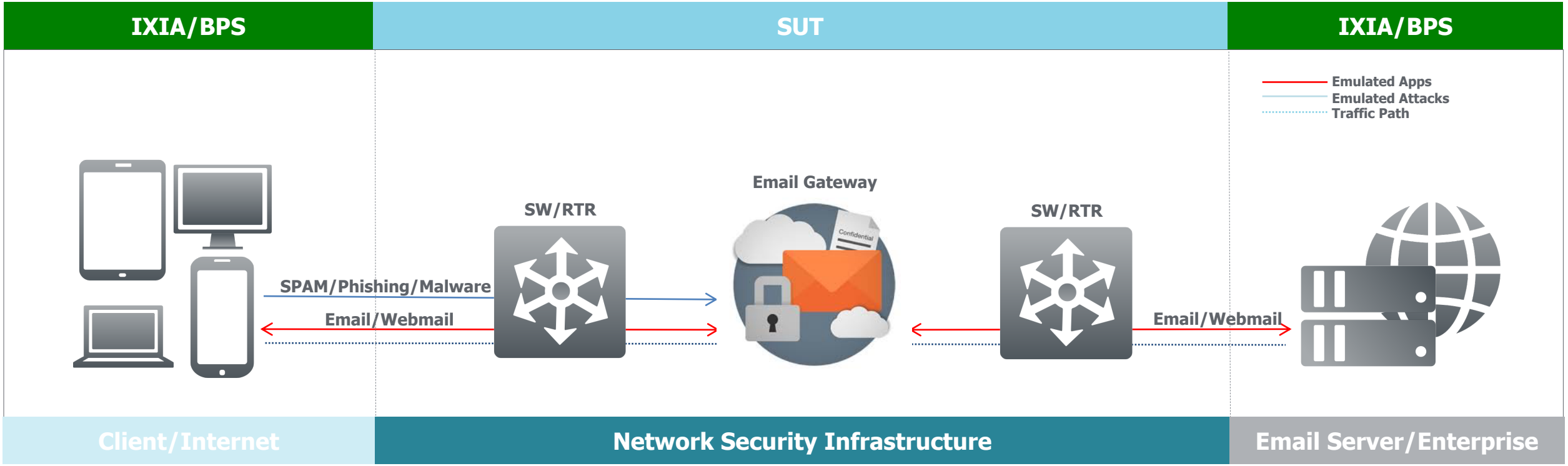


Test Methodologies

Internet scale | IP Fuzzer | Session Sender | Dual-stack

ixia
A Keysight Business

ТЕСТИРОВАНИЕ – EMAIL SECURITY



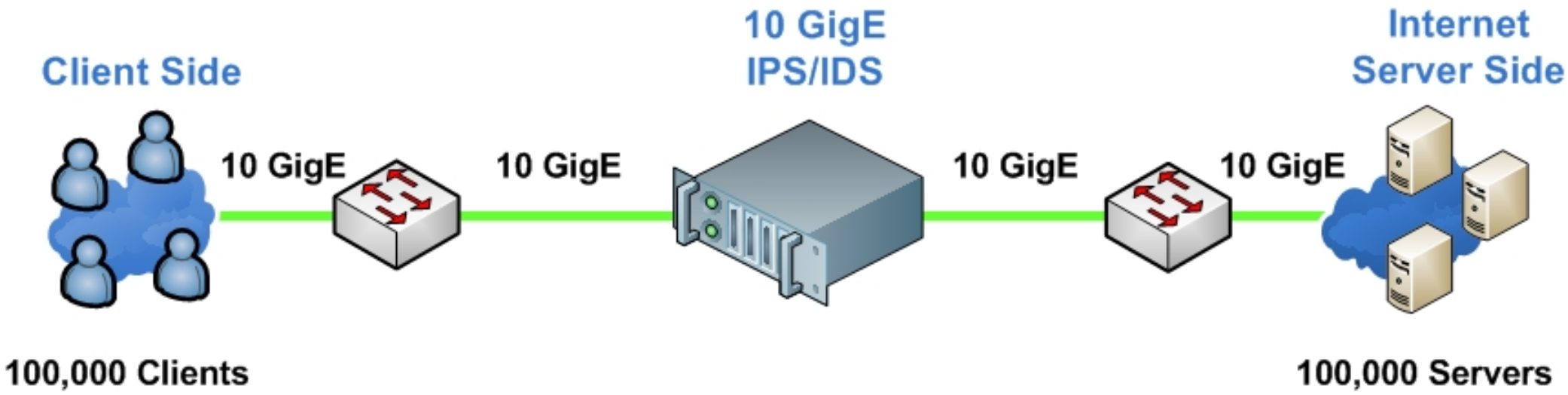
Test Methodologies

Performance | Markov | SPAM | Phishing | Malware | Dual-stack

ixia
A Keysight Business

#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

45

#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

47

#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

48

#1: МИКС ЛЕГИТИМНОГО ТРАФИКА И АТАК

Результаты теста

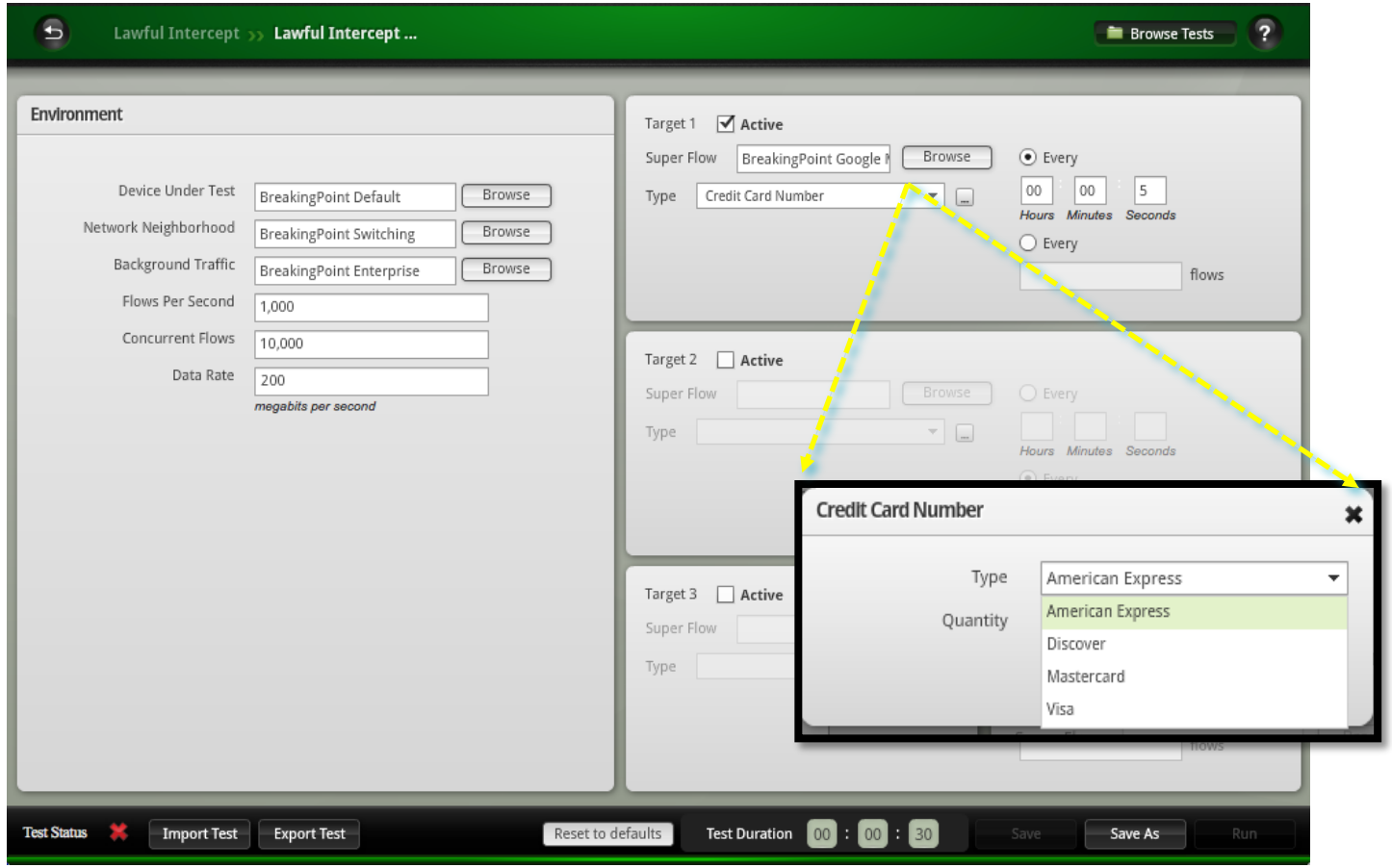
Test Scenario	Vendor 1	Vendor 2	Vendor 3	Vendor 4
SESSION RATE	4,300	50,000	16,500	30,000
SESSIONS OPEN	110,000	40,000	108,000	88,000
BANDWIDTH	0.35 Gbps	4.1 Gbps	1.3 Gbps	2.6 Gbps
444 SEND ATTACKS	20	208	42	192
PRICE	☺	☺	☺	☺

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

49

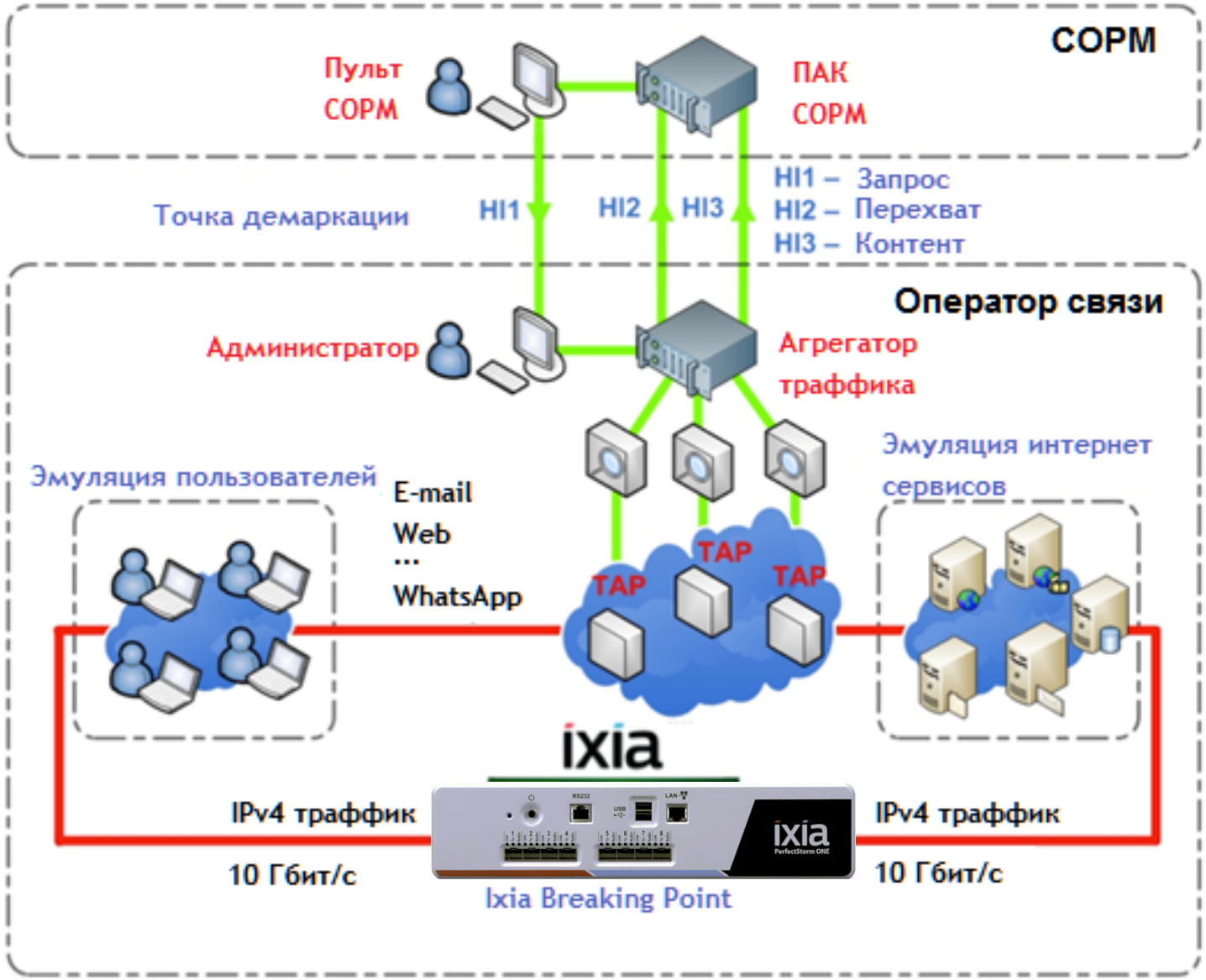
#2: ТЕСТИРОВАНИЕ СИСТЕМ DLP

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



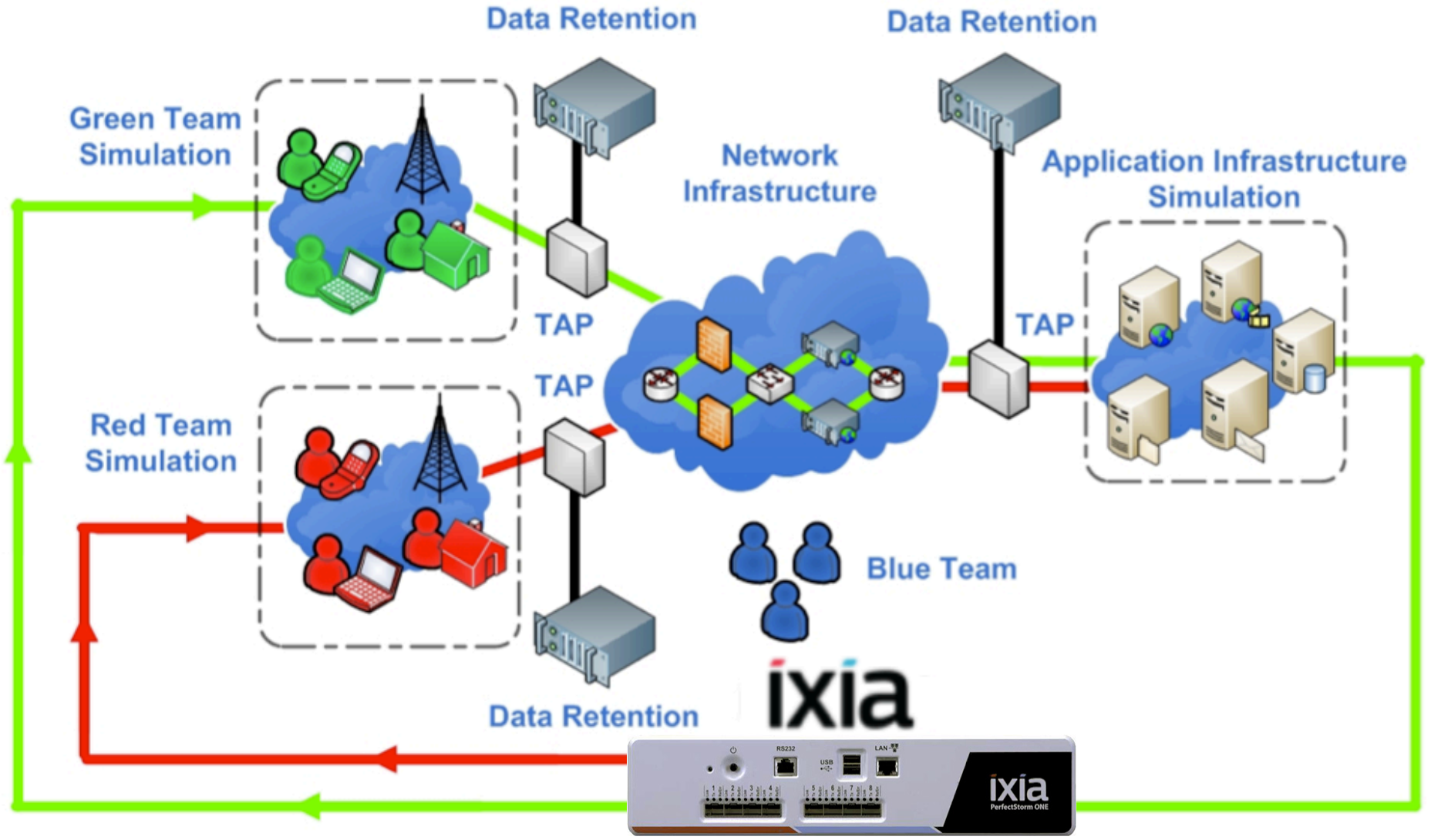
ixia
A Keysight Business

#3: ТЕСТИРОВАНИЕ СОРМ



ixia
A Keysight Business

#4: КИБЕРПОЛИГОН, ТРЕНИРОВКА И ПРОВЕРКА

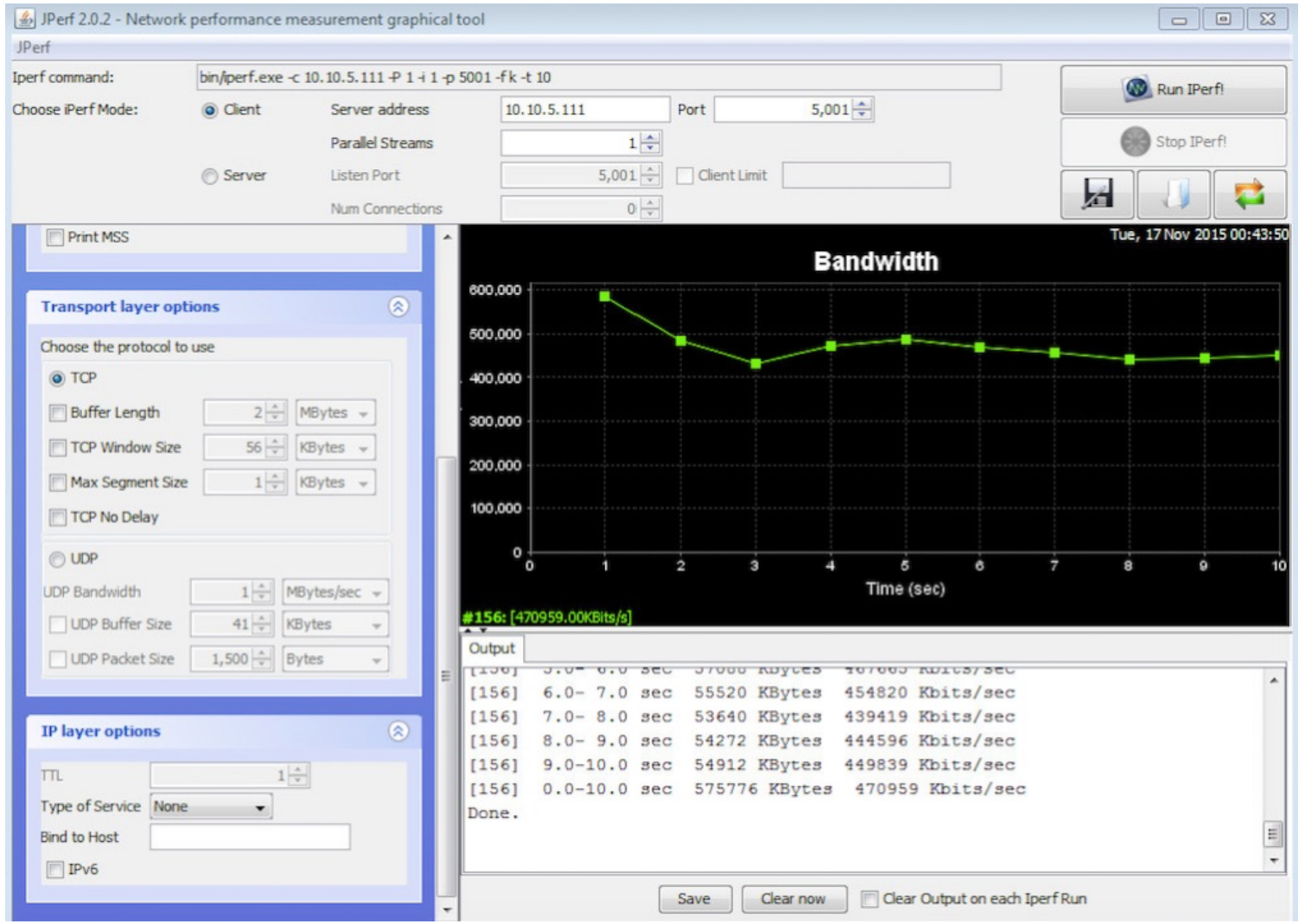


Ixia BreakingPoint Test Equipment

ixia
A Keysight Business

#5: ВИРТУАЛЬНЫЙ МАРШРУТИЗАТОР

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



ixia
A Keysight Business

#5: ПЛАН ТЕСТИРОВАНИЯ

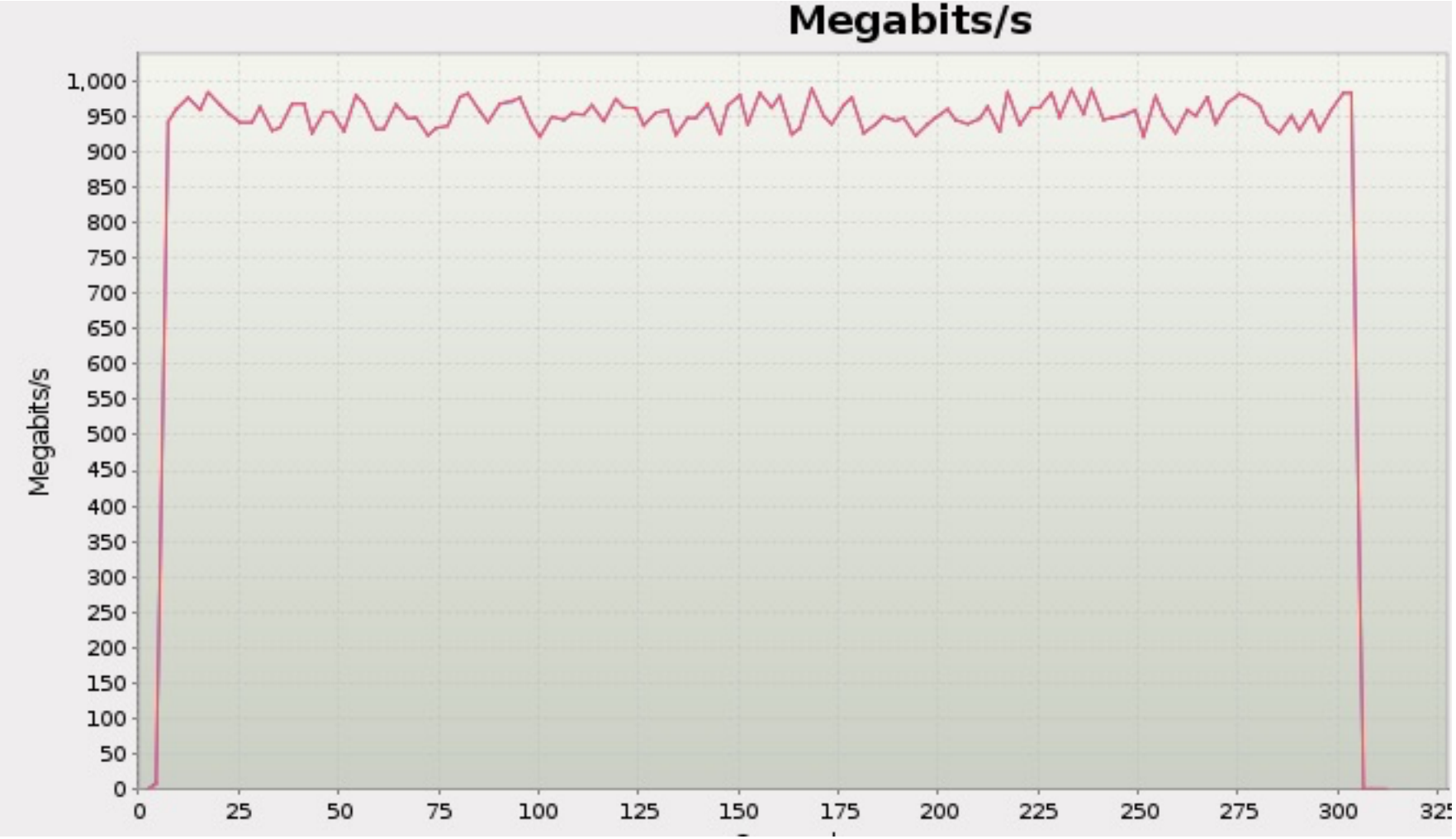
1. Производительность на разных профилях трафика L7
   - HTTP
   - Enterprise MIX
2. Проверка механизмов обработки сессий
   - Скорость обработки сессий
   - Количество одновременных сессий

Тест успешен, если трафик ходит 5 минут

Проверяем с помощью IXIA BreakingPoint Virtual Edition

#5: HTTP ТРАФИК ПОКАЗАЛ ПРЕКРАСНЫЙ РЕЗУЛЬТАТ

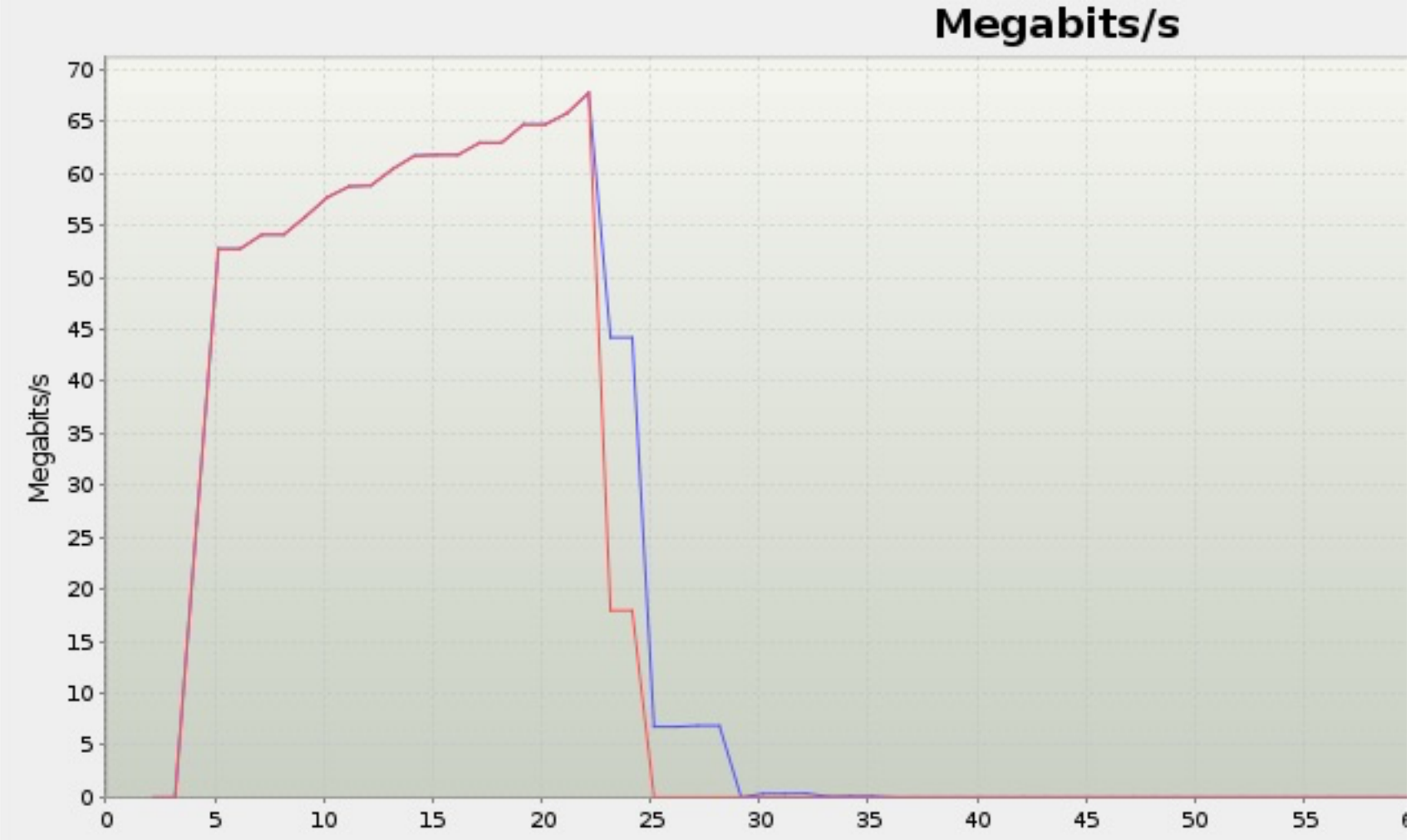
Производительность до 1 Гбит/с



ixia
A Keysight Business

#5: НА ENTERPRISE MIX УСТРОЙСТВО ОТКАЗАЛО

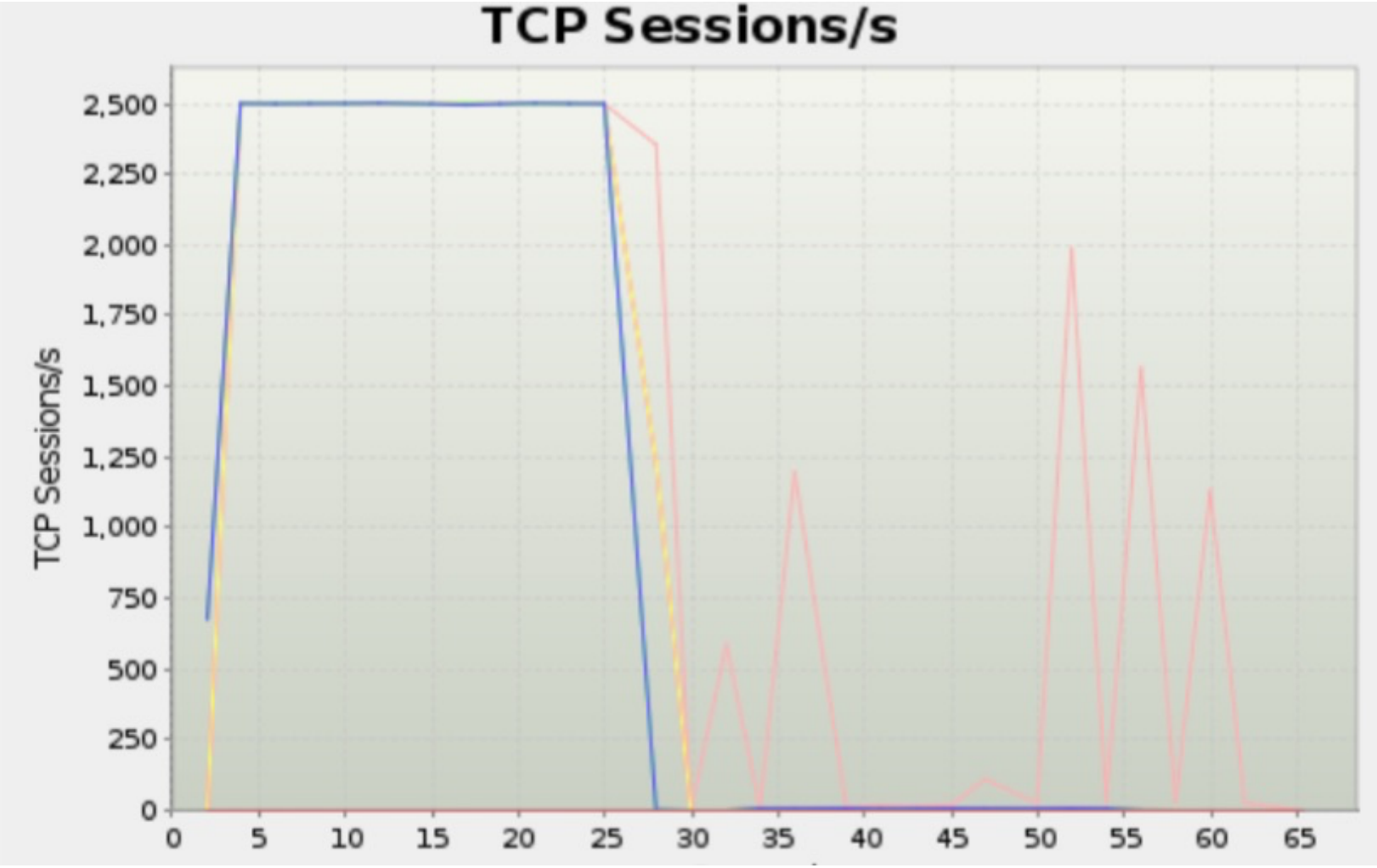
20 секунд работы привели к полному отказу устройства



ixia
A Keysight Business

#5: ИЩЕМ ПРИЧИНУ – СКОРОСТЬ ОБРАБОТКИ СЕССИЙ

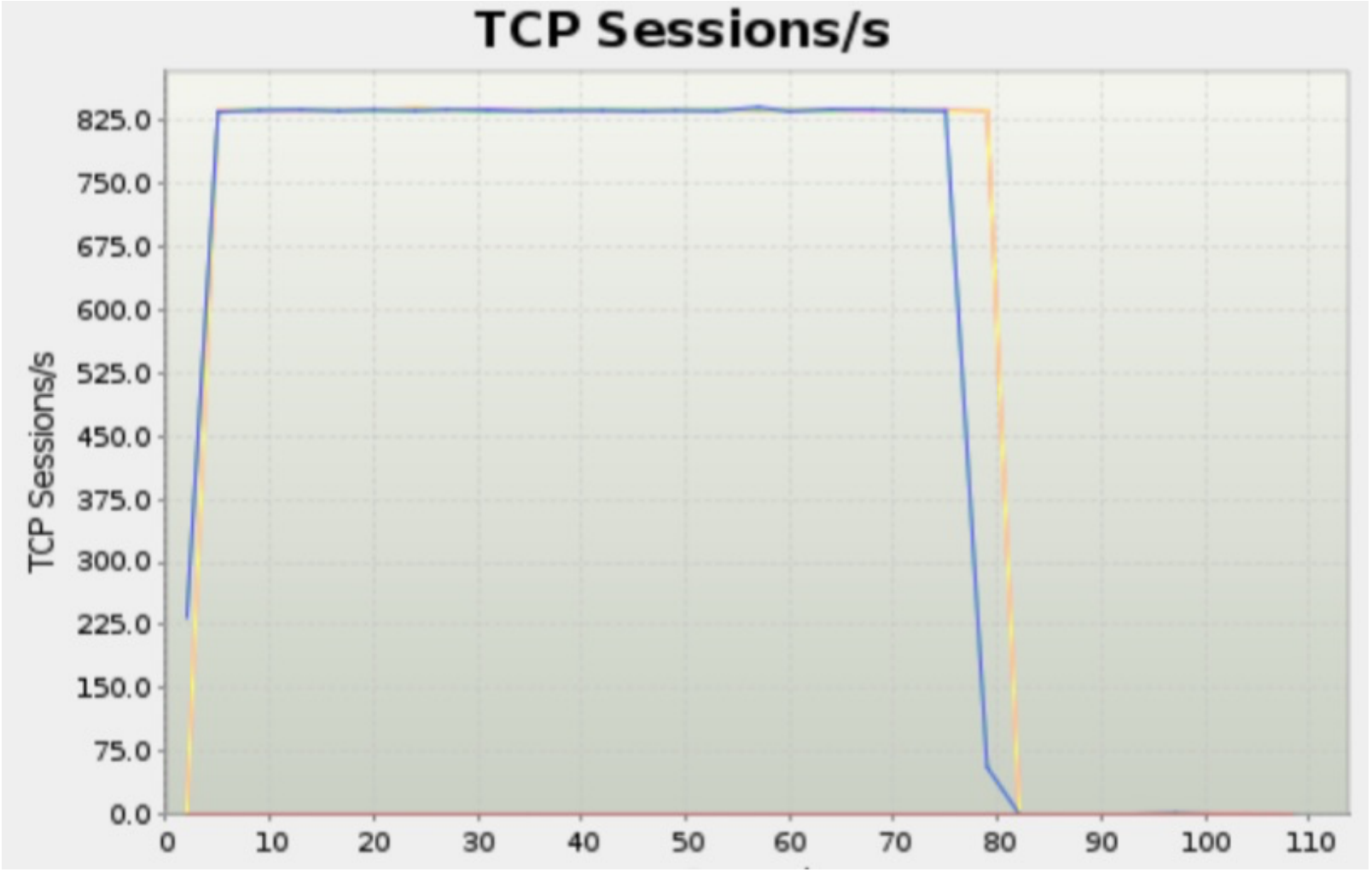
2500 сессий в секунду – устройство умирает через 27 секунд



ixia
A Keysight Business

#5: ИЩЕМ ПРИЧИНУ – СКОРОСТЬ ОБРАБОТКИ СЕССИЙ

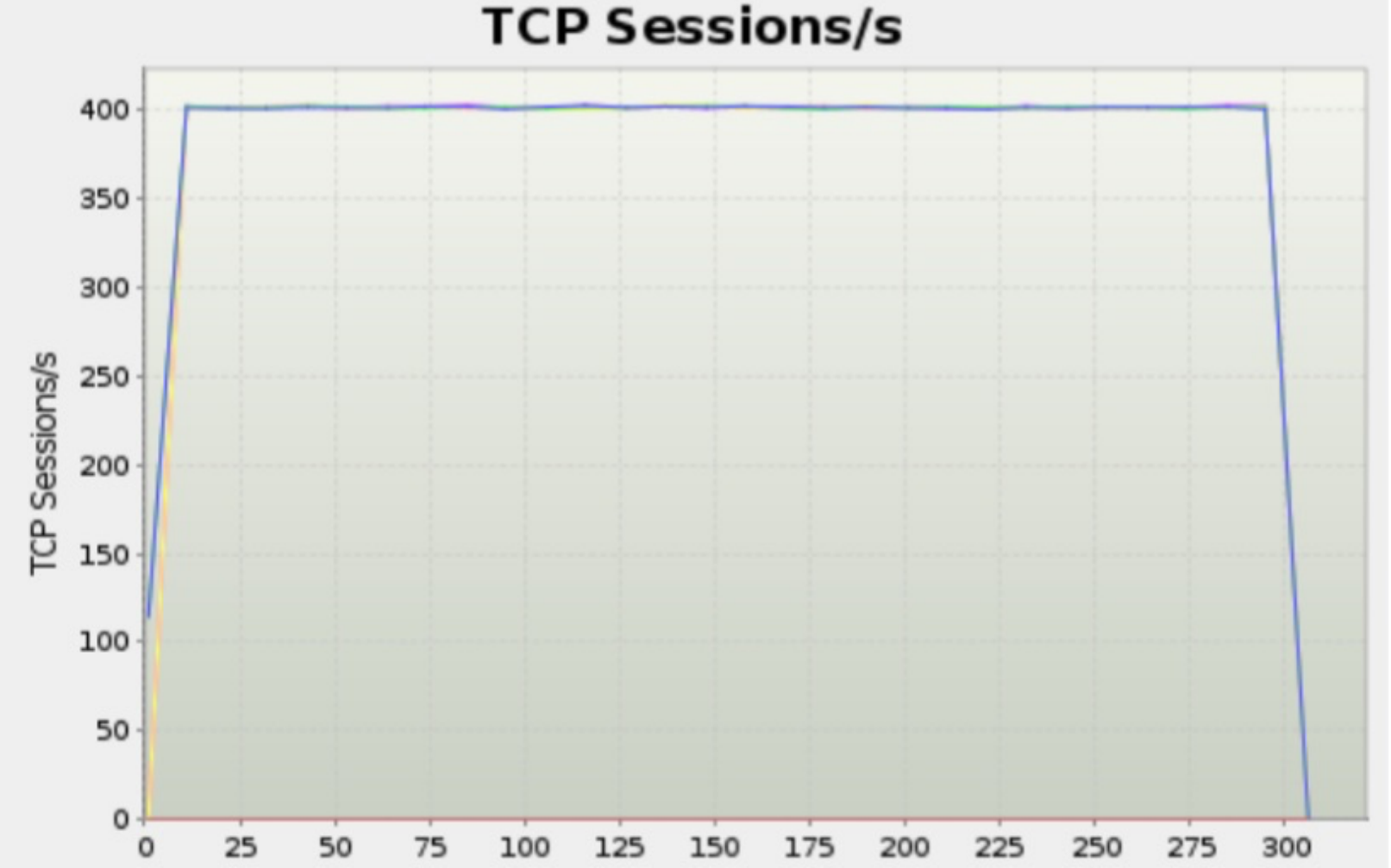
825 сессий в секунду – устройство умирает через 80 секунд



ixia
A Keysight Business

#5: ИЩЕМ ПРИЧИНУ – СКОРОСТЬ ОБРАБОТКИ СЕССИЙ

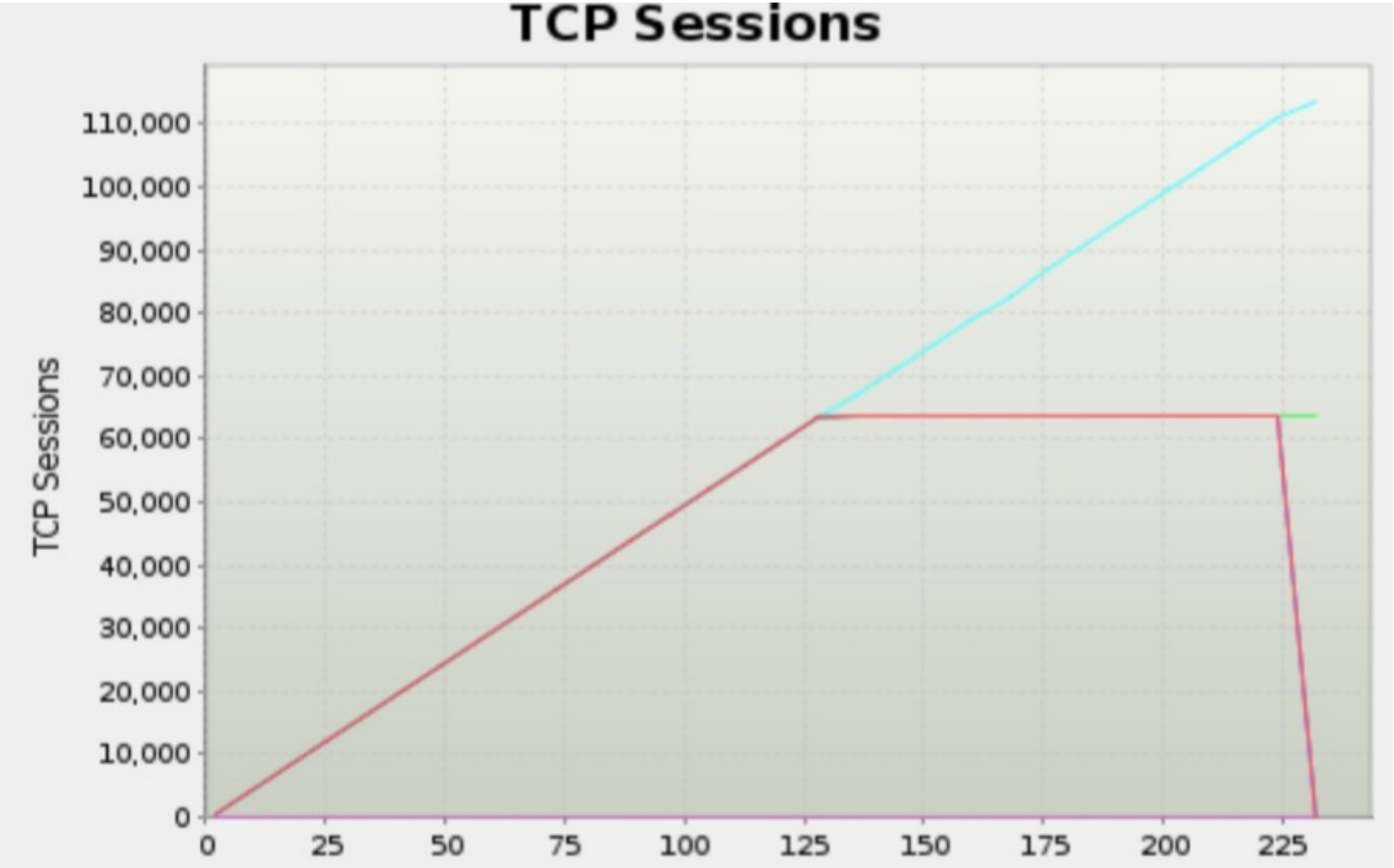
400 сессий в секунду – устройство проходит тест



ixia
A Keysight Business

#5: ИЩЕМ ПРИЧИНУ

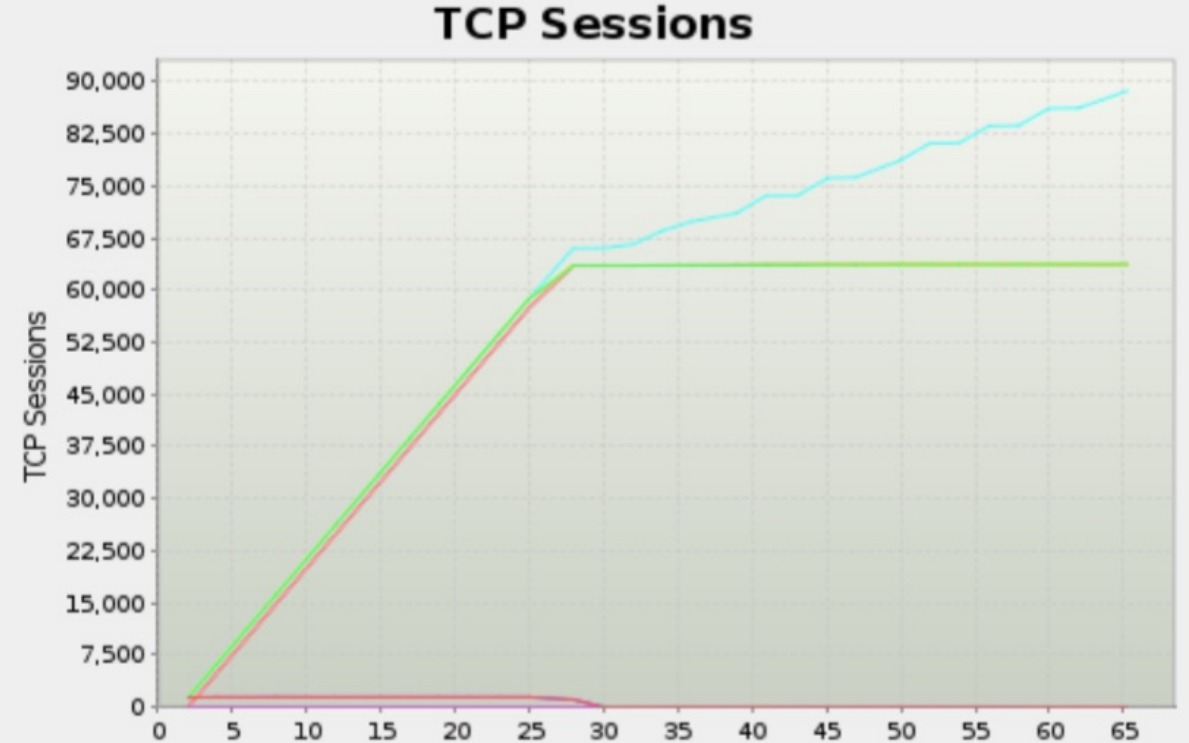
Предел 63500 одновременных сессий



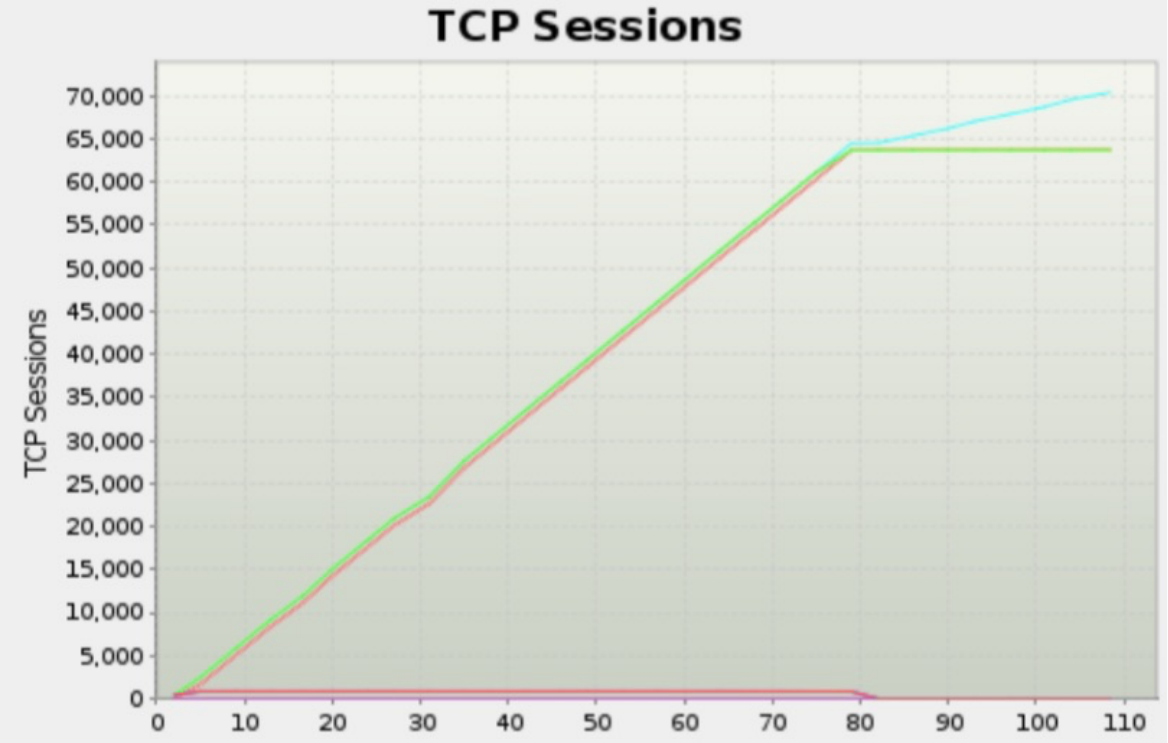
ixia
A Keysight Business

#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

ixia
A Keysight Business

#5: ВЫВОДЫ

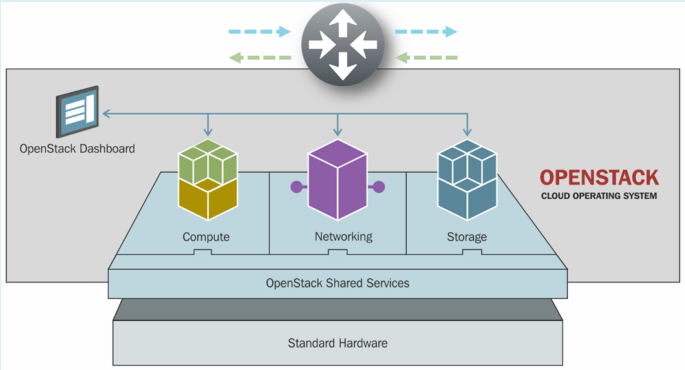
- Несмотря на высокую пропускную способность, устройство не может справиться с небольшой реальной нагрузкой
- Несмотря на то, что это был Роутер (по заявлению вендора), он работал на уровне 4
- Основной вывод теста – устройство не готово к использованию в рабочей сети
- Причиной оказался баг очистки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

BREAKINGPOINT VIRTUAL EDITION (VE) ОБЗОРНАЯ ЧАСТЬ

РЕШАЕМЫЕ ЗАДАЧИ

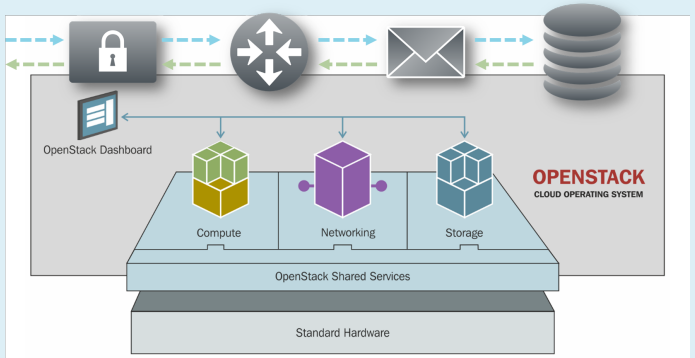
Тестирование VNF, NFV, цепочек сервисов

- Тестирование производительности



Обеспечение качества сервиса

- Подтверждение производительности и качества



SDDC (Software Defined Data Center)

- Гибкая, основанная на ПО модель развертывания будет расти вместе с вашим дата-центром
- Train your people and improve cyber resiliency and readiness

ixia
A Keysight Business

BREAKINGPOINT VE

Мощь и гибкость лидирующего приложения для решения задач в области безопасности

- Самостоятельный продукт Ixia
- Гибкая система лицензий по функционал и уровням производительности
- Возможности строить тестовые окружения любого масштаба любое время, везде
- Простая и быстрая модель развертывания
- Единый интерфейс управления физическими и виртуальным портами для тестов
- REST API для автоматизации и оркестрации

ixia
A Keysight Business

BPS-VE – СЦЕНАРИИ РАЗМЕЩЕНИЯ

Размещение на одном хосте

- vController и vBlade находятся на одном физическом (возможно применять до 12 vBlades с одним vController)
- vController реализован как виртуальная машина
- vBlades тоже виртуальные машины, ОС - Linux

Размещение на нескольких хостах

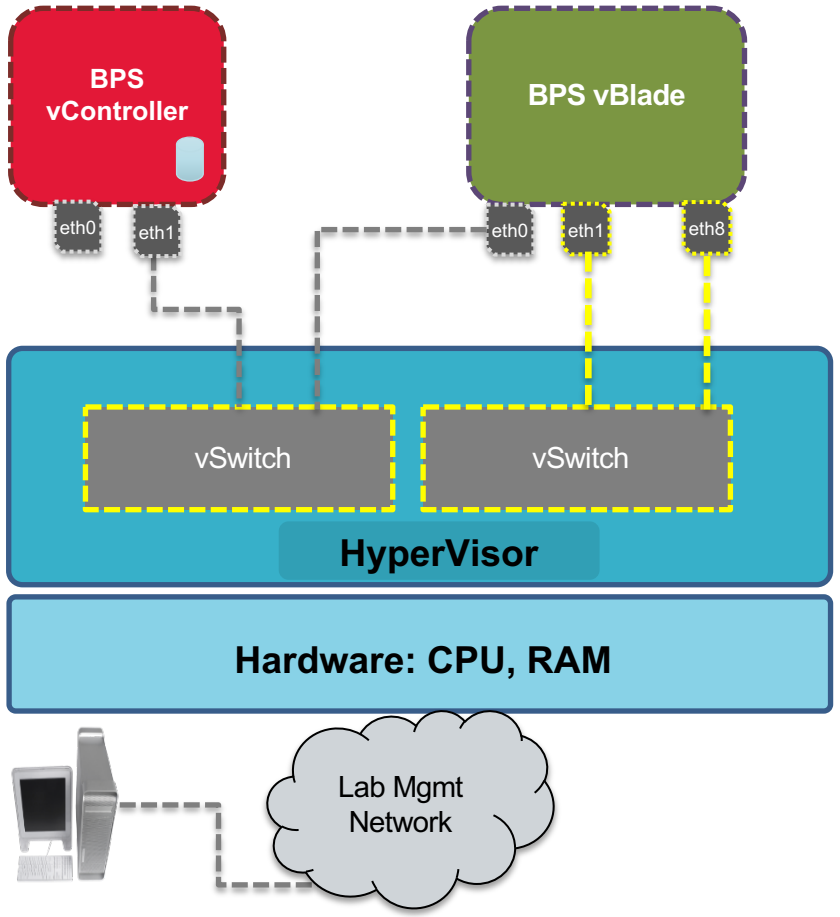
- vController находится на одном хосте (возможно с несколькими vBlades)
- Другие хосты несут на себе только vBlades

Важно

Трафик генерируется и терминируется всегда на одном vBlade (аналогично аппаратной реализации)

ixia
A Keysight Business

МОДЕЛЬ РАЗВЕРТЫВАНИЯ



vController – виртуальный контроллер системы

- Поддерживает до 12 vBlades и до 96 vPorts
- Управляет vBlades на различных физических серверах
- Требует минимум 8vCPUs, 8 GB RAM, 110 GB HDD

vBlades – виртуальные модули тестирования

- Каждое vBlade может нести от 2 до 8 интерфейсов
- Каждое vBlade имеет интерфейс управления
- Рекомендовано 4vCPUs, 8 GB RAM, 14 GB HDD
  - 1 vCPU / 2 GB RAM (для базовой производительности)
  - 2 vCPU / 4 GB RAM (для повышенной производительности)
  - 4 vCPU / 8 GB RAM (для максимальной производительности)

Развертывание

- Автоматизация развертывания виртуальных компонентов
- Возможность обновлять ПО без повторного развертывания
- Статическая или динамическая адресация
- Поддержка REST API для автоматизации

ixia
A Keysight Business

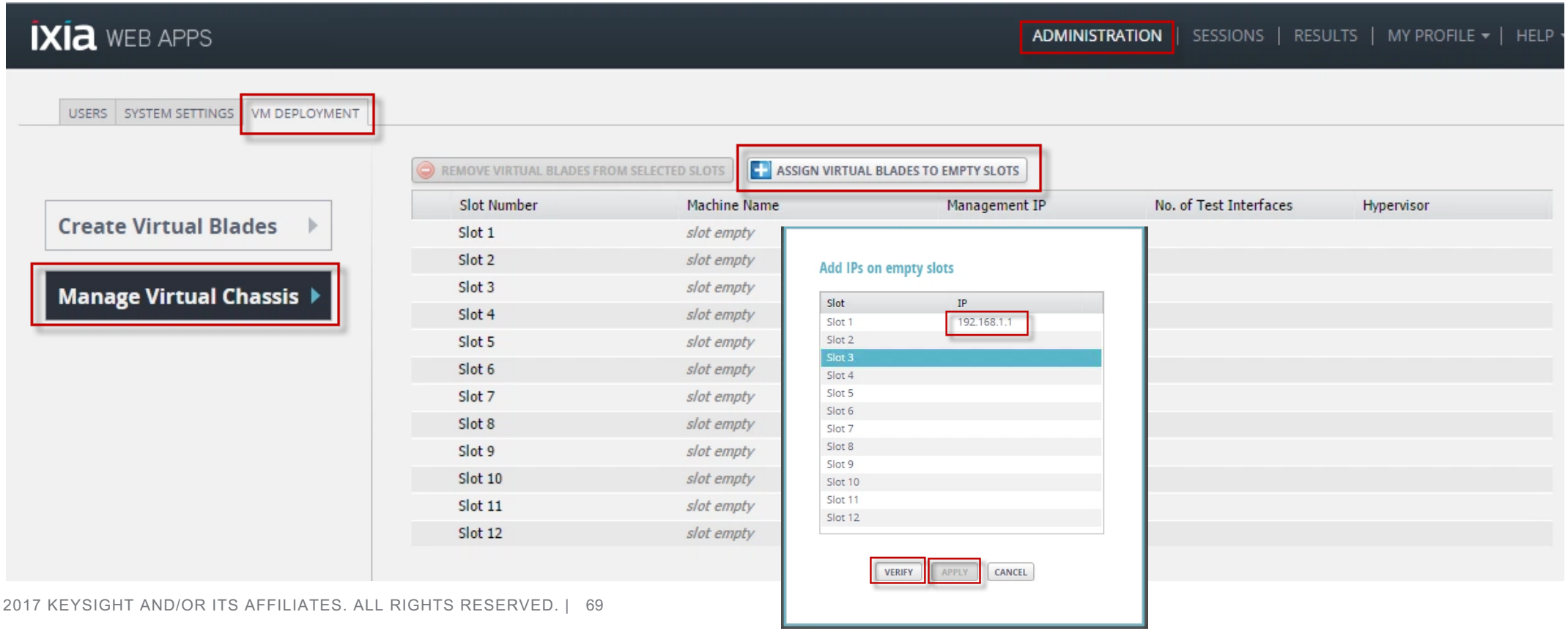
ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ

<table>
<tr><th>Категории</th><th colspan="3">Одобренные</th><th>Совместимые</th></tr>
<tr><td>Hypervisor
и
Host OS</td><td colspan="3">• VMware vSphere ESXi 6.X
• KVM over CentOS 7.X
• KVM over 16.04 LTS</td><td>• VMware vSphere ESXi 5.X
• KVM over CentOS 6.X
• KVM over Ubuntu 14.04 LTS
• KVM over RHEL 6.X
• KVM over RHEL 7.X</td></tr>
<tr><td>Управление и оркестрация</td><td colspan="3">OpenStack Mitaka and Liberty (vanilla distribution)</td><td>• VMware vCenter 5.X
• VMware vCenter 6.X
• Other OpenStack-based platforms (vanilla distributions)
• Other OpenStack-based platforms (vendor-specific distributions)</td></tr>
<tr><td rowspan="4">Сетевые соединения vNIC-драйвера</td><td rowspan="2">Virtual Switch</td><td>Performance Acceleration Enabled (DPDK)</td><td>VMXNET3 (VMware)</td><td rowspan="4">N/A</td></tr>
<tr><td>Performance Acceleration Disabled (DPDK)</td><td>VMXNET3 (VMware)
VIRTIO (KVM)</td></tr>
<tr><td>PCI Pass-Through</td><td colspan="2">Intel 01G igb (VMware)
Intel 10G ixgbe (VMware)</td></tr>
<tr><td>SR-IOV</td><td colspan="2">Intel 01G igb (VMware)
Intel 10G ixgbe (VMware)</td></tr>
<tr><td>Типы виртуальных коммутаторов</td><td colspan="3">• Virtual Standard Switch (only on VMware)
• Linux Bridges (only on KVM)
• Open Virtual Switch (only on OpenStack)</td><td>• Virtual Distributed Switch (only on VMware)
• Open Virtual Switch (only on KVM)
• Linux Bridges (only on OpenStack)</td></tr>
<tr><td colspan="5">Нельзя использовать аппаратные и виртуальные порты в одном тесте</td></tr>
<tr><td colspan="5">Нельзя проводить тестирование между распределенными портами</td></tr>
</table>

BPS-VE ЛЕГКОСТЬ РАЗВЕРТЫВАНИЕ

Модель подключения/настройки достаточно гибкая и простая

- vController и vBlade также представлены раздельными OVA или QCOW2 образами
- Возможно подключать и отключать vBlade с vController через web GUI или REST API
- Настраиваемая статичная или DHCP связанность между vController и vBlade



ixia
A Keysight Business

ЛИЦЕНЗИРОВАНИЕ

- All-inclusive лицензия открывает весь функционал
- Все выходящие новые функции доступны в рамках лицензии
- Типы лицензий:

1G-Tier	10G-Tier
○ 1Gbps of throughput	○ 10Gbps of throughput
○ 2M concurrent Superflows	○ 20M concurrent Superflows
○ Single security and security NP component	○ Two security and security NP component

- Возможность перемещать лицензии между инсталляциями или использовать единый сервер лицензий
- Лицензии блокируются при активном тесте

ixia
A Keysight Business

ПРОИЗВОДИТЕЛЬНОСТЬ

Производительность – с применением vSwitch			
	Стандартная реализация	DPDK (Data Plane Development Kit) (базис – пропускная способность)	DPDK (Data Plane Development Kit) (базис – балансирование трафика)
HTTP Throughput	9.6 Gbps	19Gbps	9.6Gbps
HTTP CPS	110K	170K	170K
HTTP CC	4M	4M	4M

Производительность – с применением SRIoV		
	Стандартная реализация	DPDK (Data Plane Development Kit)
HTTP Throughput	9 Gbps	20 Gbps
HTTP CPS	110K	235K
HTTP CC	4M	4M

Производительность – с применением PCI-Passthrough		
	Стандартная реализация	DPDK (Data Plane Development Kit)
HTTP Throughput	9 Gbps	20 Gbps
HTTP CPS	80K	240K
HTTP CC	4M	4M

Данные приведены относительно системы:

- VMware ESXi-6.0
- CPU: Intel® Xeon® CPU E3-1285 v4 @ 3.50 GHz (4 cores @ 3.50 GHz)
- vBlade: 4 vCPUs, 8 GB RAM
- vController: 8 vCPUs, 8 GB RAM
- 1 vBlade with 2 ports deployed

BPS-VE – ФАКТЫ

Session Sender
AppSim
ClientSim
Security
Security NP
Stack Scrambler
DDoS
Recreate
Routing Robot
RFC 2544 Lab
Lawful Intercept Lab
Multicast Lab

IPv4/IPv6 hosts

External Hosts

Virtual Routers

VLAN

DHCPv4

VMware ESX 5.5
KVM over CentOS 6.5, 7.0
KVM over Ubuntu 14.04 LTS
OpenStack

Deployment &
Discovery Tools
OVA support

vChassis with VM cards distributed across multiple physical hosts

vBlades with 8-ports for test traffic

Centralized or Local Licensing Server

Subscription Licenses

Firmware Upgrades

Flexible Licensing (floating)

Performance based with one 1/10 Gbps as license unit

Frequent Updates
Every 2 weeks

Real Attacks
6,000+ exploits
35,000+ malware
180+ evasions
DDoS and botnets

Real-World Apps
300+ applications
Web, Mail, Social,
peer-to-peer,
voice, video
enterprise apps

ixia
A Keysight Business

BPS-VE 8.40 – ТАБЛИЦА ФУНКЦИОНАЛА

Network Neighborhood	VM
IPv4/IPv6 Static Hosts	✓
IPv4/IPv6 External Hosts	✓
VLAN	✓
IPv4/IPv6 Router	✓
DHCPv4 (client/server)	✓
IPv4 DNS	✓
IPv6 DNS	✓
IPsec IKEv1/IKEv2	NS
LTE (IPv4)	✓
LTE (IPv6)	NS
6rd	NS
DSLite	NS
DHCPv6 (client/server)	NS
IPv6 SLAAC	NS

BPS Test Component	VM
Application Simulator	✓
Client Simulation	✓
Security	✓
Security NP	✓
Session Sender	✓
Stack Scrambler	✓
SSL/TLS	✓
Hardware-based packet capture	SW 1GB
Impairment	NS
Bit Blaster	✓
Routing Robot	✓
Recreate	✓
SCTP	✓

Breaking Point Labs	VM
Session Sender Lab	✓
RFC 2544 Lab	✓
Multicast Lab	✓
Lawful Intercept Lab	✓
Device Validation Lab	NS
MultiBox testing	NS
Resiliency Score	NS
Data Center Resiliency	NS
LTE Lab	NS
DDoS Lab	✓

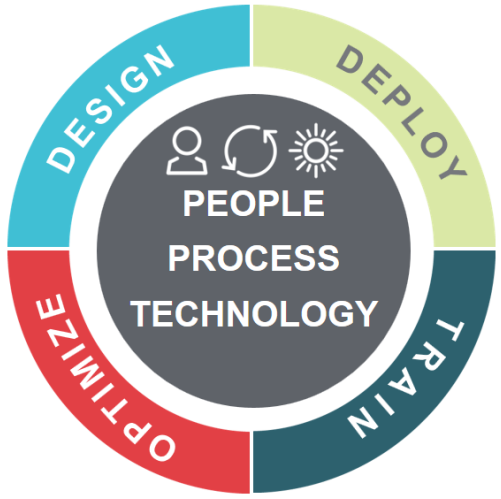
See disclaimer on slide 2 of this presentation

ixia
A Keysight Business

ixia

BreakingPoint Cloud

BreakingPoint Cloud является SaaS платформой кибербезопасности позволяющей моделировать уязвимости и векторы угроз. Анализирует вашу облачную или гибридную IT безопасность, чтобы вы могли заранее принять меры для укрепления своих критических участков.



ixia
A Keysight Business

BPS-VE – ЭТО УДОБНО

Легкий доступ к BPS технологиям:

- Доступная точка входа для начинающих пользователей
- Подписка OPEX основана на существующих IT проектах
- Улучшенное лицензирование в линейке 1Gbps

Гибкое и простое развертывание

Критично для тестирования NFV

Elasticity to build test beds at any scale, at any time, anywhere

- Масштабирование в рамках 1/10 Gbps
- Удобная модель лицензирования
- Можно распределять лицензии по группам пользователей

ixia
A Keysight Business

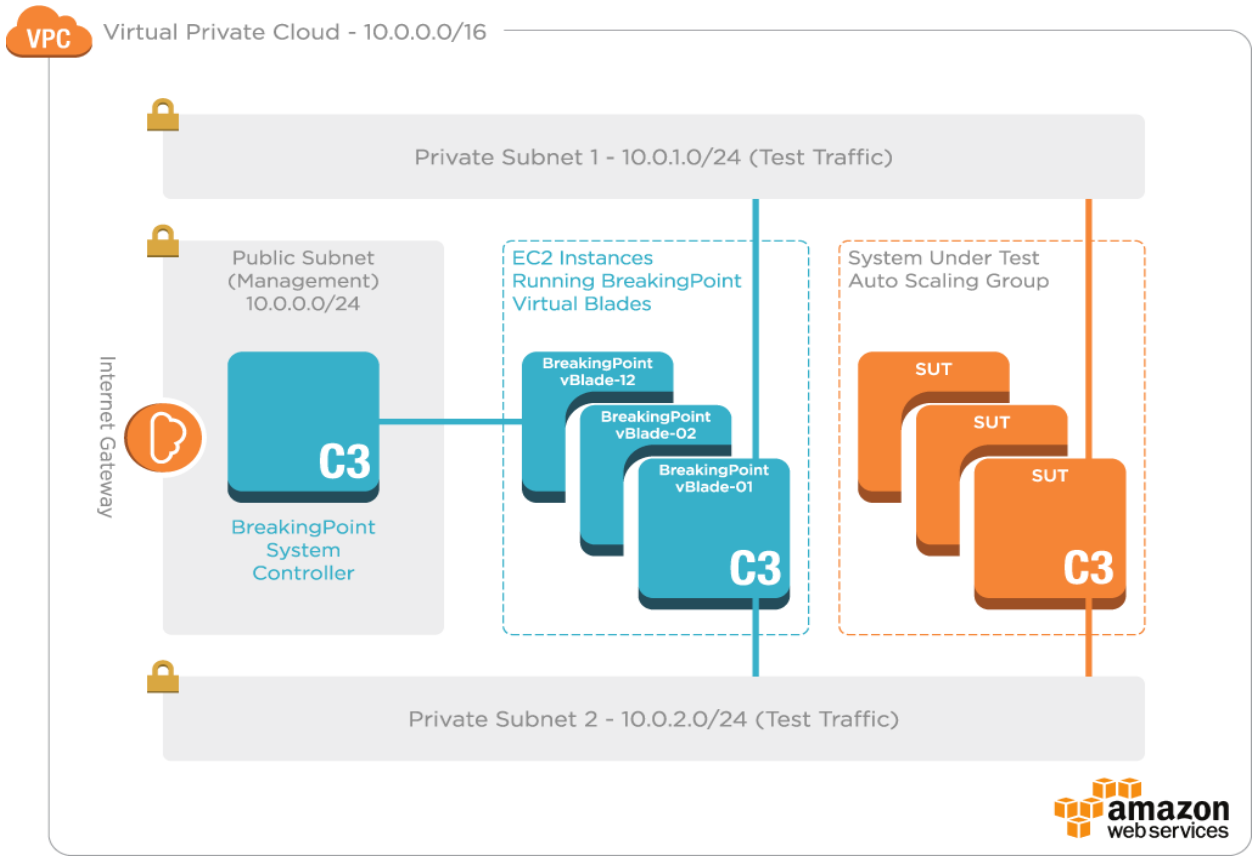
BREAKINGPOINT B AWS

BREAKINGPOINT B AWS

- Гибкость и мощность лидирующего приложения в области кибербезопасности сейчас доступна на AWS
- Вы можете использовать существующие лицензии
  - 1Gbps уровня лицензирования
  - 10Gbps уровня лицензирования
- Вы можете перенести свои методики в облачную платформу

РАЗВЕРТЫВАНИЕ В AWS

- BreakingPoint Amazon Machine Images (AMIs) доступны в Community
  - Отдельные AMIs для System Controller и vBlades
  - Просто ищите по слову Ixia
- Варианты развертывания
  - Вручную (через EC2 Launch wizard)
  - Через оркестрацию (CloudFormation Templates)
    - vBlades автоматически подключатся к Controller
  - Через полную автоматизацию (AWS SDK scripts)



ixia
A Keysight Business

ИСПОЛЬЗУЙТЕ СВОИ ЛИЦЕНЗИИ

- All-inclusive лицензия открывает весь функционал
- Все выходящие новые функции доступны в рамках лицензии
- Типы лицензий:

1G-Funtional Tier – 939-9600	10G-Performance Tier – 939-9610
○ 1Gbps of throughput	○ 10Gbps of throughput
○ 2M concurrent Superflows	○ 20M concurrent Superflows
○ Single security and security NP component	○ Two security and security NP component

ixia
A Keysight Business

ДАННЫЕ ПО ПРОИЗВОДИТЕЛЬНОСТИ

Примеры к BPS на AWS

AWS Instance	Performance Metric	Test Component	Release 8.40 Performance Acceleration OFF	Release 8.40 Performance Acceleration ON	Comments
R4.4xlarge	Throughput (HTTP) - unidir	AppSim	3.8 Gbps	5.35 Gbps	Elastic Network Adapter (ENA)
R4.4xlarge	Throughput (HTTP) - bidir	AppSim	5.2 Gbps	8.5 Gbps	Elastic Network Adapter (ENA)
R4.4xlarge	Throughput (SSL) MTU 1500	AppSim	2.5 Gbps	5 Gbps	Elastic Network Adapter (ENA)
M4.16xlarge	Throughput (HTTP) - unidir	AppSim	4 Gbps	5.3 Gbps	Elastic Network Adapter (ENA)
M4.16xlarge	Throughput (HTTP) - bidir	AppSim	6.2 Gbps	7.75 Gbps	Elastic Network Adapter (ENA)
M4.16xlarge	Throughput (SSL) MTU 1500	AppSim	2.4 Gbps	3.6 Gbps	Elastic Network Adapter (ENA)

ДАННЫЕ ПО ПРОИЗВОДИТЕЛЬНОСТИ

Примеры к BPS на AWS (продолжение)

AWS Instance	Performance Metric	Test Component	Release 8.40 Performance Acceleration OFF	Release 8.40 Performance Acceleration ON	Comments
I3.8xlarge	Throughput (HTTP) - unidir	AppSim	5.3 Gbps	7.5 Gbps	Elastic Network Adapter (ENA)
I3.8xlarge	Throughput (HTTP) - bidir	AppSim	7 Gbps	9.9 Gbps	Elastic Network Adapter (ENA)
C4.4xlarge	Throughput (HTTP) - unidir	AppSim	4 Gbps	4 Gbps	SR-IOV
C4.4xlarge	Throughput (HTTP) - bidir	AppSim	4.5 Gbps	4.5 Gbps	SR-IOV
C4.4xlarge	Throughput (SSL) MTU 1500	AppSim	2.5 Gbps	2.5 Gbps	SR-IOV

BPS 8.50 ТАБЛИЦА ФУНКЦИОНАЛА НА AWS

Network Neighborhood	
IPv4/IPv6 Static Hosts	✓
IPv4/IPv6 External Hosts	✓
VLAN	NS
IPv4/IPv6 Router	✓
DHCPv4 (client/server)	NS
IPv4 DNS/IPv6 DNS	✓
IPsec IKEv1/IKEv2	NS
LTE (IPv4)	NS
LTE (IPv6)	NS
6rd	NS
DSLite	NS
DHCPv6 (client/server)	NS
IPv6 SLAAC	NS

BPS Test Component	
Application Simulator	✓
Client Simulation	✓
Security	✓ (1)
Security NP	✓ (1)
Session Sender	✓
Stack Scrambler	✓ (2)
SSL/TLS	✓
Packet capture	SW 1GB
Impairment	NS
Bit Blaster	NS
Routing Robot	Limited
Recreate	✓ Replay without modification (3)
SCTP	✓
BreakingPoint Labs	NS

(1) Некоторые атаки могут быть заблокированы AWS

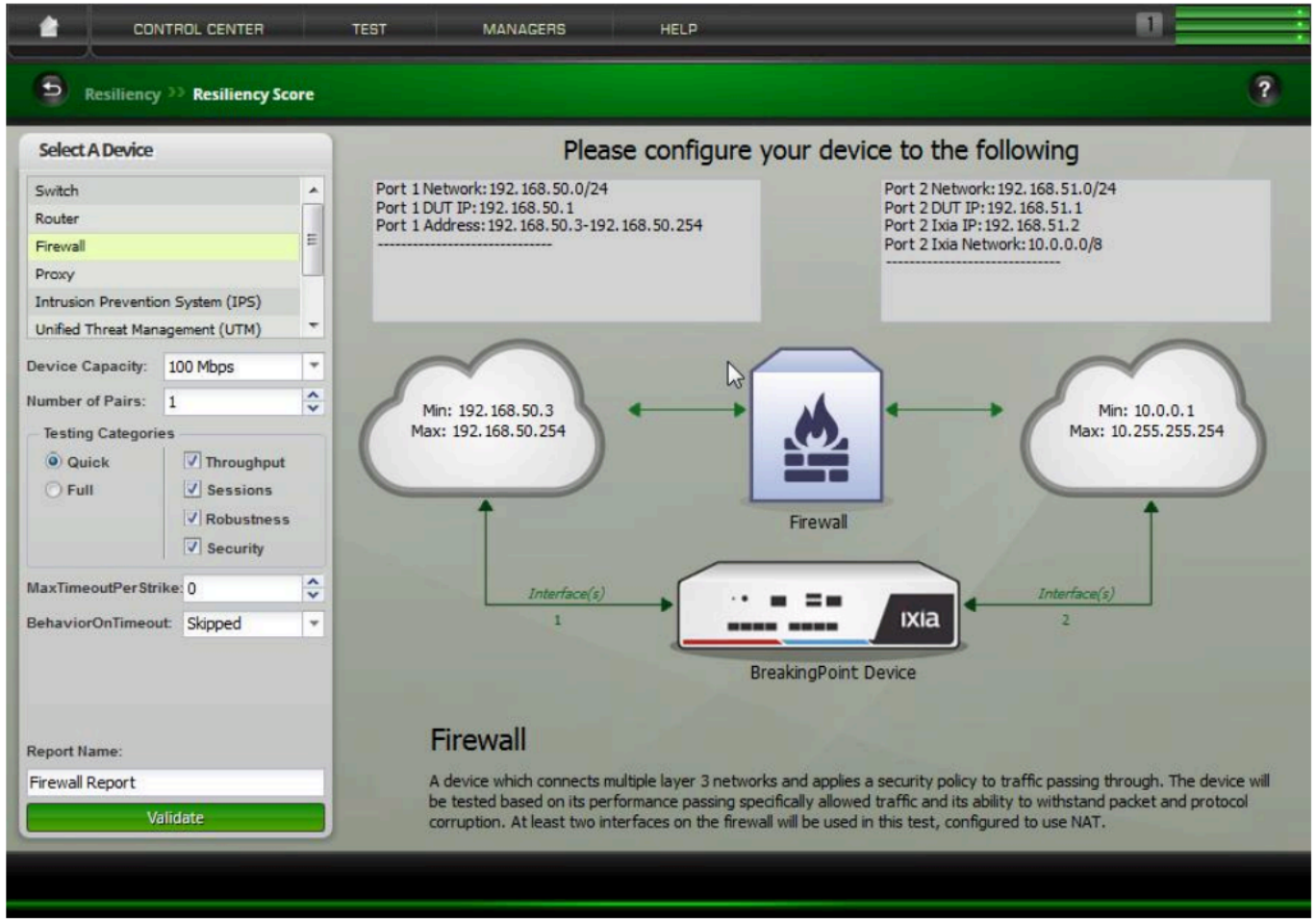
(2) Некоторые некорректные паттерны IP пакетов несовместимы с AWS (трафик может теряться)

(3) AWS требует чтобы BPS использовал MAC адреса, относящиеся к интерфейсам, с которых происходит рассылка трафика.

ixia
A Keysight Business

ЛОКАЛЬНОЕ ТЕСТИРОВАНИЕ

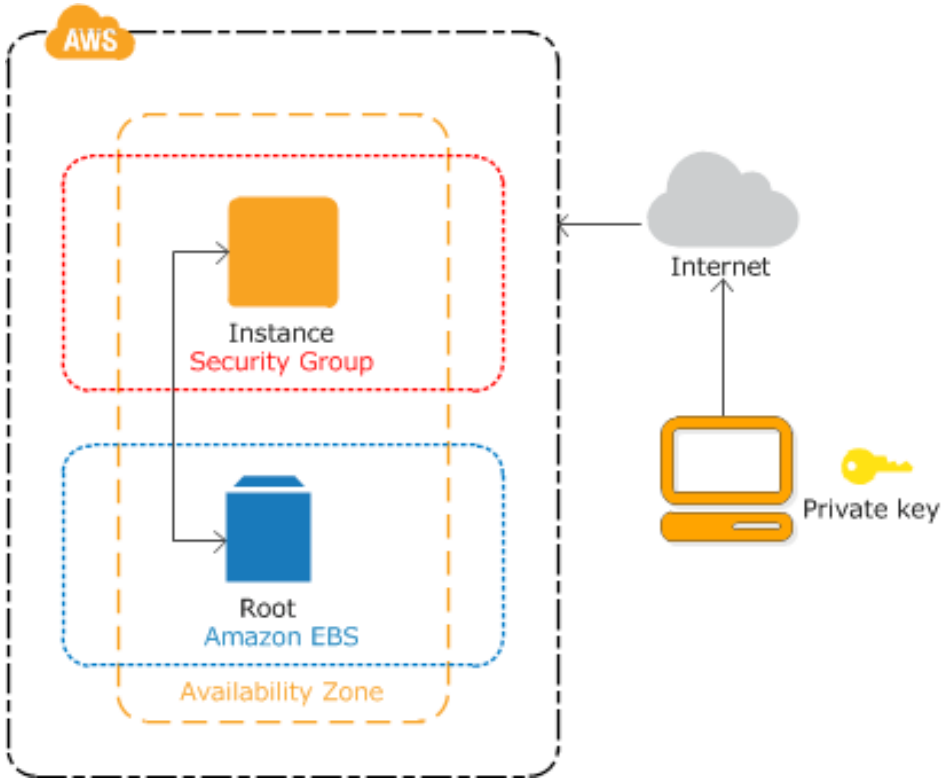
- Развертывание BPS внутри сети
- Тестирование устройства по методике Two-Arm
- Достаточно развернуть vController и vBlade с двумя интерфейсами



ixia
A Keysight Business

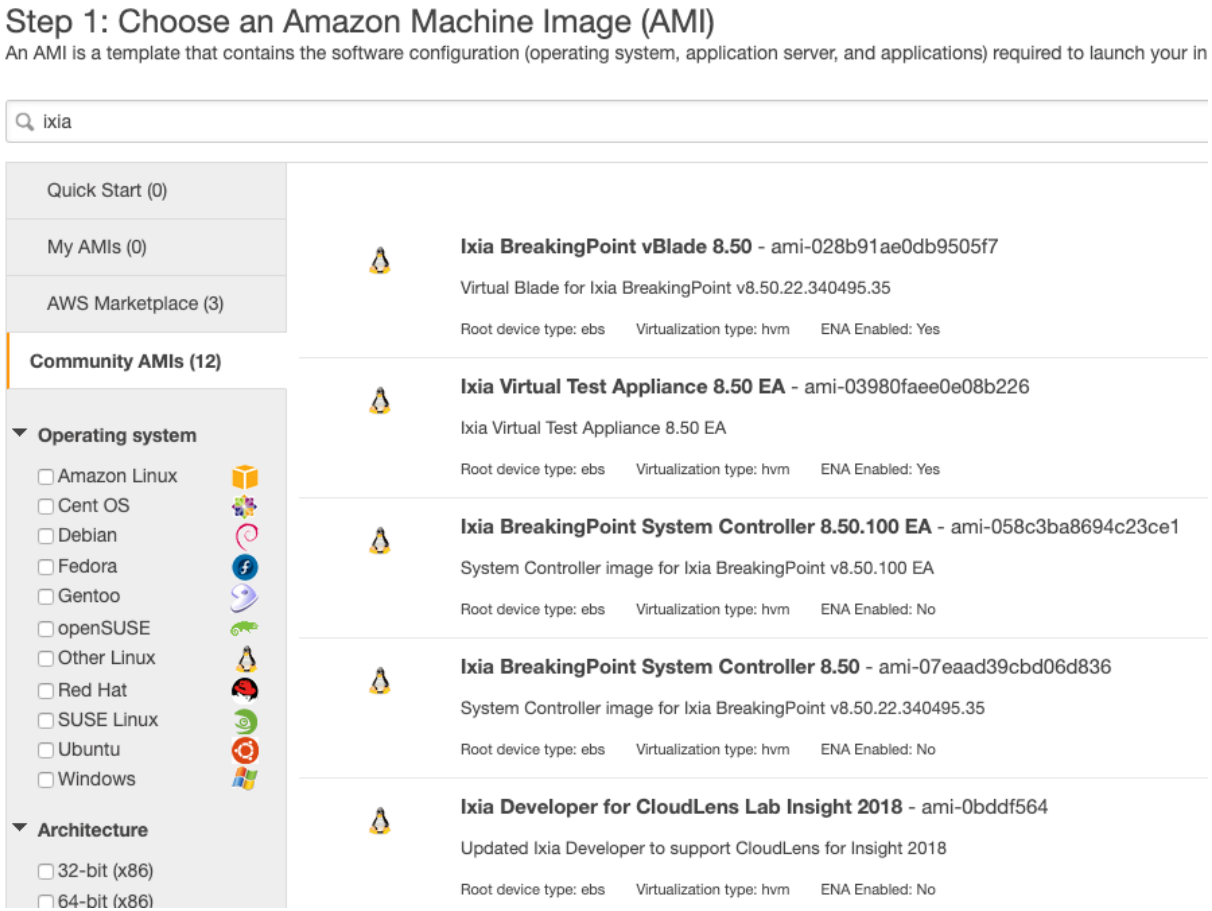
ПОСТРОЕНИЕ ОБЛАКА AMAZON

- 16 регионов по миру
- 1-3 зон доступности в каждом регионе
- Возможность оперировать собственными как внешними так и внутренними адресациями, маршрутизацией
- API, CLI, VPN, разграниченный доступ
- Безопасный доступ к собственным ресурсам с возможностью шаринга



BPS В ОДНОМ РЕГИОНЕ

- Развертывается прямо из Amazon market
- Время развертывания несколько минут
- Для коммутации достаточно добавить vController и vBlade в друг-другу в ACL



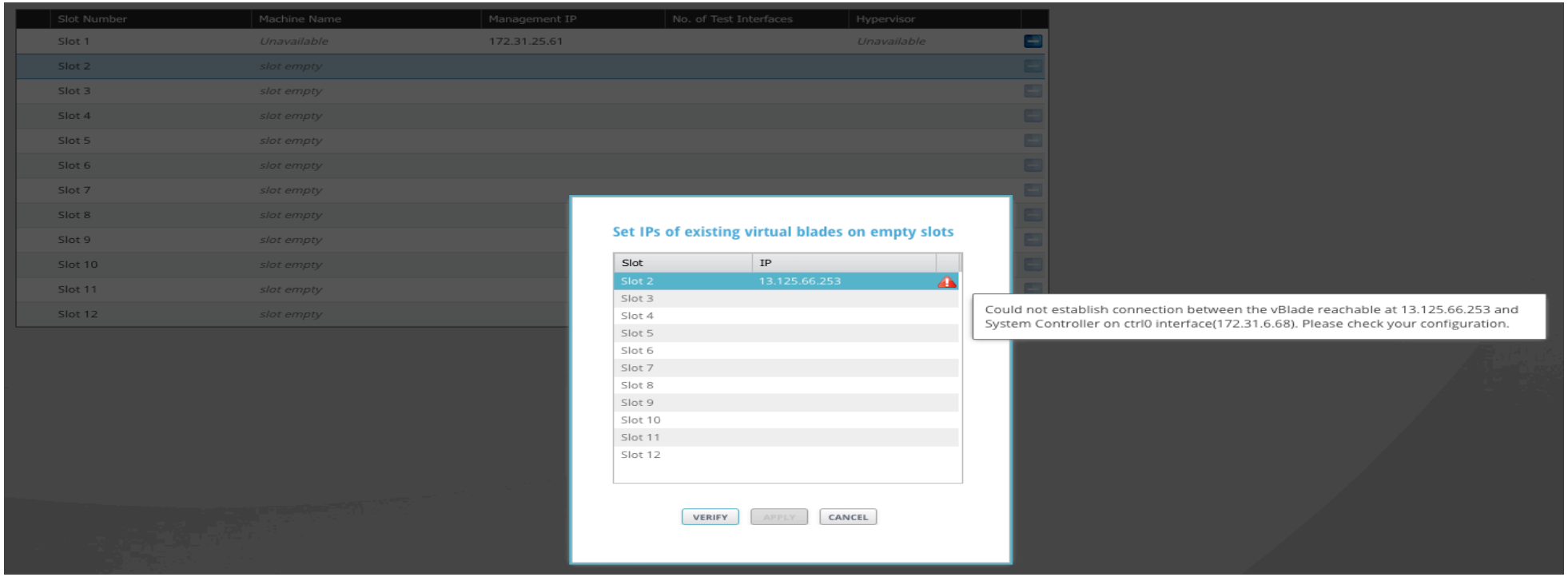
ixia
A Keysight Business

ДЕТАЛИ РАЗВЕРТЫВАНИЯ ONE REGION

- Размер виртуальной машины для vController - t2.small или больше (у нас t2.large)
- Размер виртуальной машины для vBlade - t2.xlarge или больше
- Первый интерфейс vBlade – менеджмент, публичный адрес ему не нужен
- Для нескольких портов на vBlade добавляем дополнительные интерфейсы через Amazon GUI
- Для доступа к vController достаточно открыть для вашего внешнего адреса HTTP (TCP443)
- Для коммутации vBlade к vController необходимо их добавить друг к другу в Security Group и коммутировать по внутренним адресам (Private IPs)

BPS С РАСПРЕДЕЛЕНИЕМ ПО РЕГИОНАМ

- Развертывание такое же не сложное, как в одном регионе
- В нужных нам регионах поднимаем дополнительные vBlade и устанавливаем соединения с vController



ixia
A Keysight Business

ДЕТАЛИ РАЗВЕРТЫВАНИЯ DISTIBUTED №1

- Мы хотим D – Distribution. По умолчанию Amazon выделяет 5 Elastic IPs на регион – мы хотим больше и пишем запрос в саппорт
- Адреса добавляются к vBlade парами: приватный-публичный, все их нужно прописать в Neighborhood
- Amazon использует NAT 1в1, но BPS так vBlade на подключает
- Нужно устанавливать через VPC пиринговые соединения между регионами
- **VPC-сети в регионах не должны перекрываться!**

ДЕТАЛИ РАЗВЕРТЫВАНИЯ DISTIBUTED №2

- В Security Groups vBlade и vController добавляем **сабнеты** друг друга
- vController и vBlade должны «видеть» друг друга по всем портам (и ICMP)
- Крайне желательно давать понятные дескрипшены объектов
- На менеджмент-интерфейсе vBlade Elastic IP (публичный адрес) не нужен
- Не нужно держать про запас не подключенные к интерфейсу Elastic IPs - это стоит дополнительных денег
- Не забываем про ACL (Security Groups) и все входящие соединения делаем только для себя
- Пароль по умолчанию на BPS admin:admin лучше все-таки сменить

ИТОГ

- Решением BreakingPoint по тестированию систем защиты можно использовать через сеть Интернет для создания распределенной сложной нагрузки
- Решение просто в развертывании, использовании и масштабировании
- Хорошо подходит в качестве инструмента периодического контроля за состоянием политик защиты
- Подробные отчеты по результатам тестирования со всех точек
- Можно использовать именно когда это необходимо

BREAKINGPOINT HA AZURE

BREAKINGPOINT НА AZURE

- Гибкость и мощность лидирующего приложения в области кибербезопасности сейчас доступна на AWS
- Вы можете использовать существующие лицензии
  - 1Gbps уровня лицензирования
  - 10Gbps уровня лицензирования
- Вы можете перенести свои методики в облачную платформу
- Решение сейчас в стадии испытаний, но возможно к использованию

РАЗВОРАЧИВАНИЕ НА AZURE

- BPS Azure Virtual Hard Disk Images (VHDs)
    - System Controller VHD для Hyper-V
    - Virtual Blade VHD для Hyper-V

- BPS Варианты развертывания
    - Вручную (через Azure Portal)
    - Через оркестрацию (Azure Resource Manager ARM Templates)
        - vBlades автоматически подключатся к Controller
    - Через полную автоматизацию(Azure PowerShell scripts)

ИСПОЛЬЗУЙТЕ СВОИ ЛИЦЕНЗИИ

- All-inclusive лицензия открывает весь функционал
- Все выходящие новые функции доступны в рамках лицензии
- Типы лицензий:

1G-Funtional Tier – 939-9600	10G-Performance Tier – 939-9610
○ 1Gbps of throughput	○ 10Gbps of throughput
○ 2M concurrent Superflows	○ 20M concurrent Superflows
○ Single security and security NP component	○ Two security and security NP component

ixia
A Keysight Business

BPS 8.50 ТАБЛИЦА ФУНКЦИОНАЛА НА AZURE (БЕТА)

Network Neighborhood	
IPv4/IPv6 Static Hosts	✓
IPv4/IPv6 External Hosts	✓
VLAN	NS
IPv4/IPv6 Router	✓
DHCPv4 (client/server)	NS
IPv4 DNS/IPv6 DNS	✓
IPsec IKEv1/IKEv2	NS
LTE (IPv4)	NS
LTE (IPv6)	NS
6rd	NS
DSLite	NS
DHCPv6 (client/server)	NS
IPv6 SLAAC	NS

BPS Test Component	
Application Simulator	✓
Client Simulation	✓
Security	✓ (1)
Security NP	✓ (1)
Session Sender	✓
Stack Scrambler	✓ (2)
SSL/TLS	✓
Packet capture	SW 1GB
Impairment	NS
Bit Blaster	NS
Routing Robot	Limited
Recreate	✓ Replay without modification (3)
SCTP	✓
BreakingPoint Labs	NS

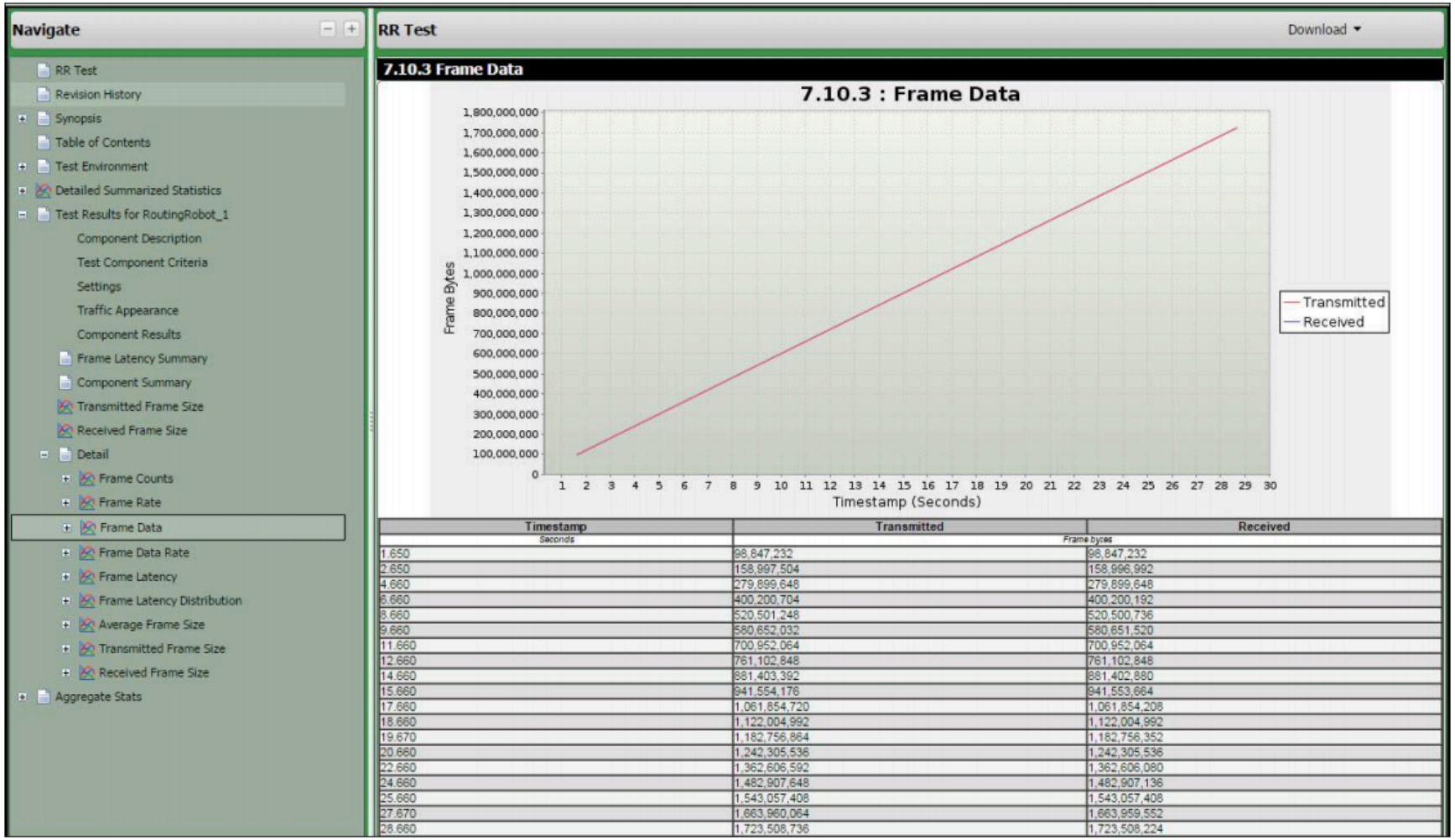
1) Некоторые атаки могут быть заблокированы Azure

(2) Некоторые некорректные паттерны IP пакетов несовместимы с Azure (трафик может теряться)

(3) Azure требует чтобы BPS использовал MAC адреса, относящиеся к интерфейсам, с которых происходит рассылка трафика.

ixia
A Keysight Business

СПАСИБО



Timestamp (Seconds)	Transmitted (Frame bytes)	Received (Frame bytes)
1.650	98,847,232	98,847,232
2.650	158,997,504	158,996,992
4.660	279,899,648	279,899,648
6.660	400,200,704	400,200,192
8.660	520,501,248	520,500,736
9.660	580,652,032	580,651,520
11.660	700,952,064	700,952,064
12.660	761,102,848	761,102,848
14.660	881,403,392	881,402,880
15.660	941,554,176	941,553,664
17.660	1,061,854,720	1,061,854,208
18.660	1,122,004,992	1,122,004,992
19.670	1,182,756,864	1,182,756,352
20.660	1,242,305,536	1,242,305,536
22.660	1,362,606,592	1,362,606,080
24.660	1,482,907,648	1,482,907,136
25.660	1,543,057,408	1,543,057,408
27.670	1,663,960,064	1,663,959,552
28.660	1,723,508,736	1,723,508,224

ixia
A Keysight Business


ixia
A Keysight Business