Решения для высоконагруженного тестирования ИТ инфраструктуры

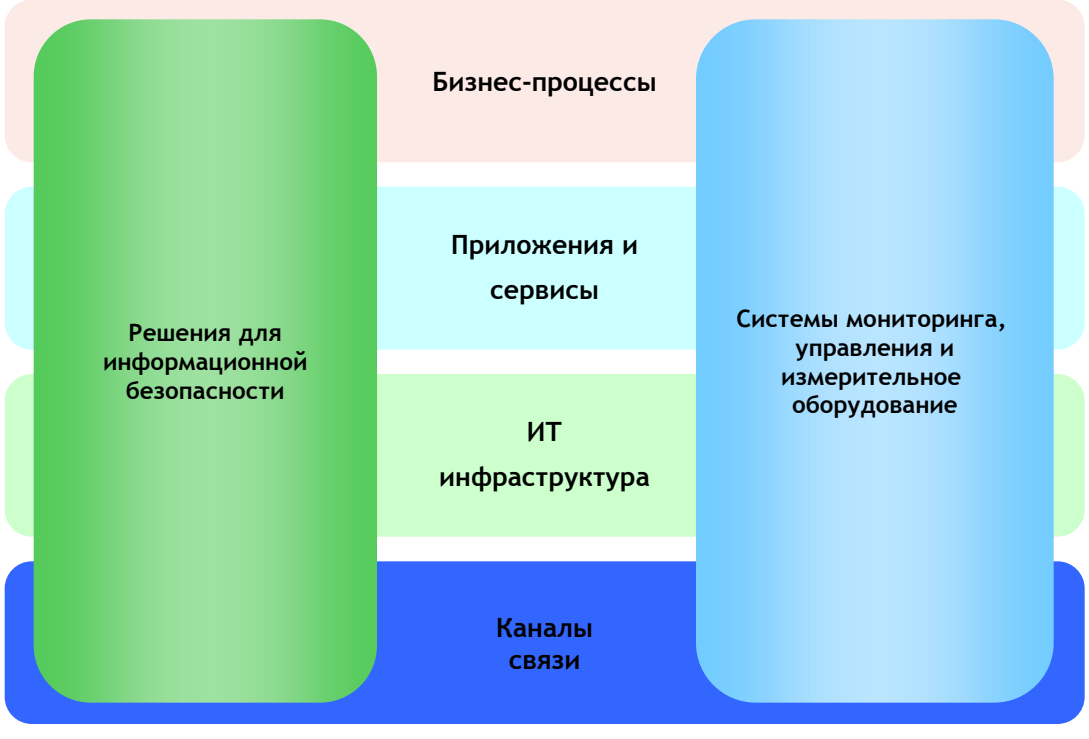
treatface

о компании

Основные факты

- Компания “Тритфейс” создана в 2010 году при поддержке крупных государственных заказчиков для разработки инфокоммуникационных решений с возможностью глубокого анализа пакетов (DPI) для закрытых государственных организаций.
- В 2011 году выпущена первая версия платформы DPI и внедрена на сети ОАО «ВымпелКом».
- В 2013 году разработана вторая версия платформы DPI, которая является одним из лучших решений на рынке средств глубокого анализа и обработки трафика.
- В начале 2014 года в деятельности компании “Тритфейс” появились новые направления, благодаря приходу в нее команд высококвалифицированных специалистов по мониторингу и тестированию сетей и приложений.
- В 2014 году внедрено решение для контроля трафика на базе платформы DPI в ОАО «Ростелеком»

Направления работы



Тестирование

Направления и цели

Зачем

- **Выбор** поставщика по реальным характеристикам
- Тонкая **оптимизация** конфигураций
- **Проверка надежности** и эффективности систем сетевой защиты под нагрузкой
- Уверенное **масштабирование** инфраструктуры
- **Соответствие** стандартам и рекомендациям
- Безопасное **внедрение** новых технологий
- **Оценка** впечатления конечных пользователей о качестве услуги и правильное планирование
- **Решение спорных** вопросов с поставщиком оборудования или канала связи
- Поиск **коренных причин** проблем на стенде

Традиционные направления

Транспорт L2-3

- HSE до 400G
- Коммутация
- Маршрутизация
- L2-3 QoS
- MPLS
- BGP
- STP
- LACP
- NFV/Openflow
- и другие

Сервисы L4-7

- Данные
- Видео
- Голос
- СХД
- Устройства stateful обработки
- Оценка QoE
- Работа сервисов под нагрузкой
- Емкость каналов связи на L4-7
- Облачные сервисы

Безопасность

- NG firewall
- WAF
- IDS/IPS
- Защита от DDoS
- Родительский контроль
- Антивирусы
- СОРМ
- Гос. реестр запрещенных ресурсов

Автоматизация

- Автоматическая сборка стендов
- Планирование ресурсов
- Реализация комплексных методологий
- Устранение рутинных процессов
- Абсолютная повторяемость экспериментов

Новые направления

Мобильные сети

- Сотовые и WiFi сети
- Доступ
- Ядро
- Femto соты
- Мобильные терминалы
- Емкость
- Биллинг
- Роуминг
- Безопасность
- QoS
- Качество речи
- И сервисов данных

Синхронизация

- PTP
- SyncE
- Масштабируемость
- Точность
- Стабильность
- Эмуляция WAN каналов
- Тестирование на соответствие RFC

NFV/SDN

- Виртуальные сетевые устройства
- Производительность
- Емкость
- Соответствие RFC
- Выбор вендора

ЦОД

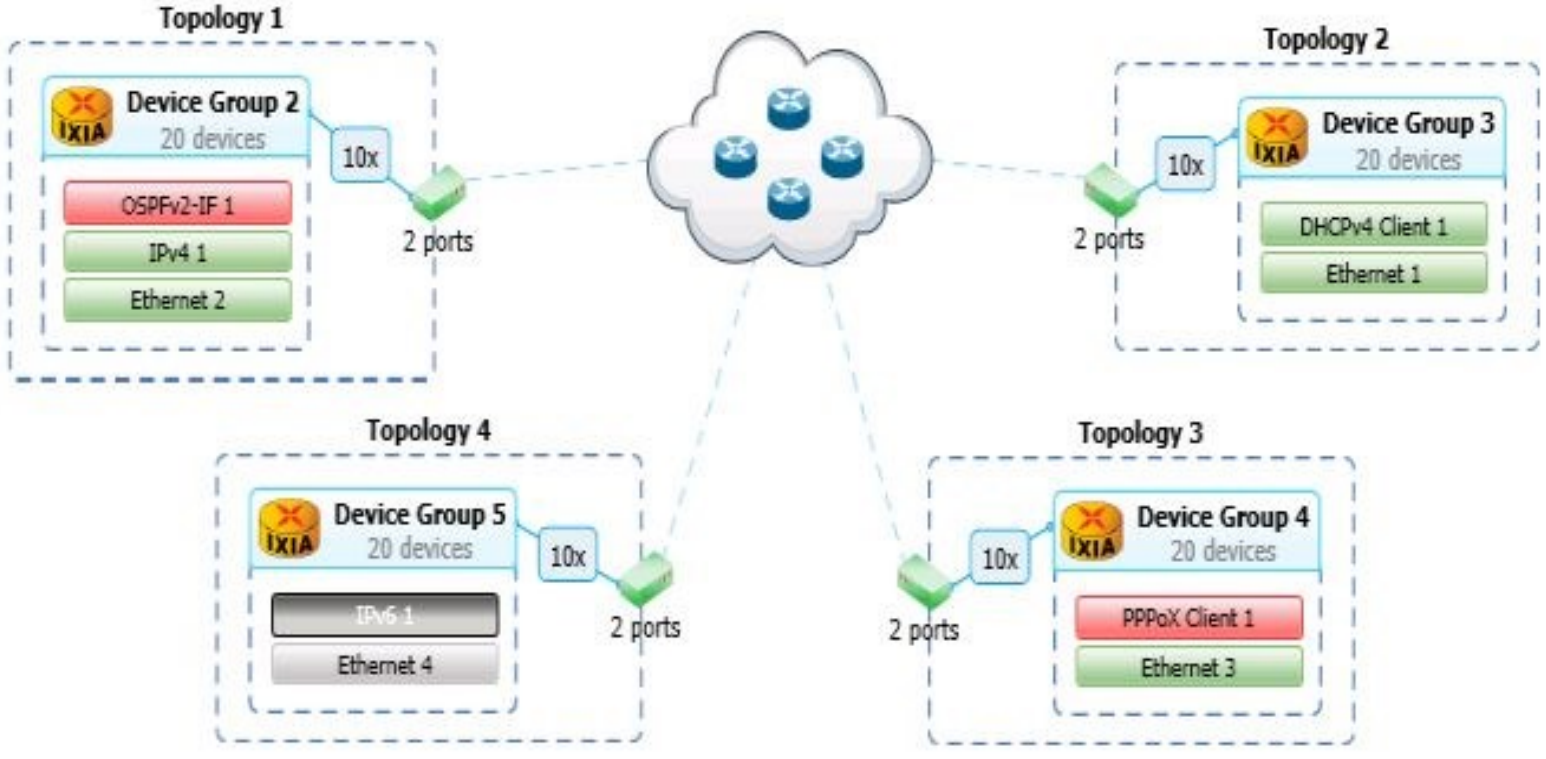
- Качество работы сервисов из облака
- Устойчивость к отказам
- Производительность СХД
- Защита от DDoS
- Переход на IPv6
- Коммутация и QoS

IXIA

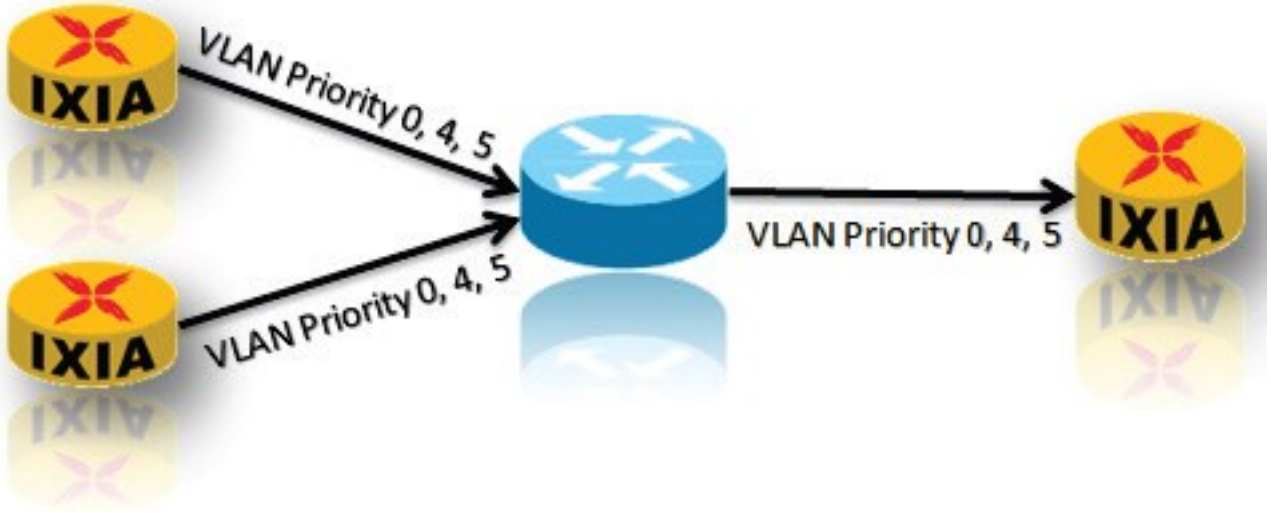
Тестирование L2-3
ПО ixNetwork

ixNetwork

Маршрутизация, коммутация, доступ, MPLS, Multicast, Carrier Ethernet, синхронизация и ЦОД



Use case #1: L2 QoS

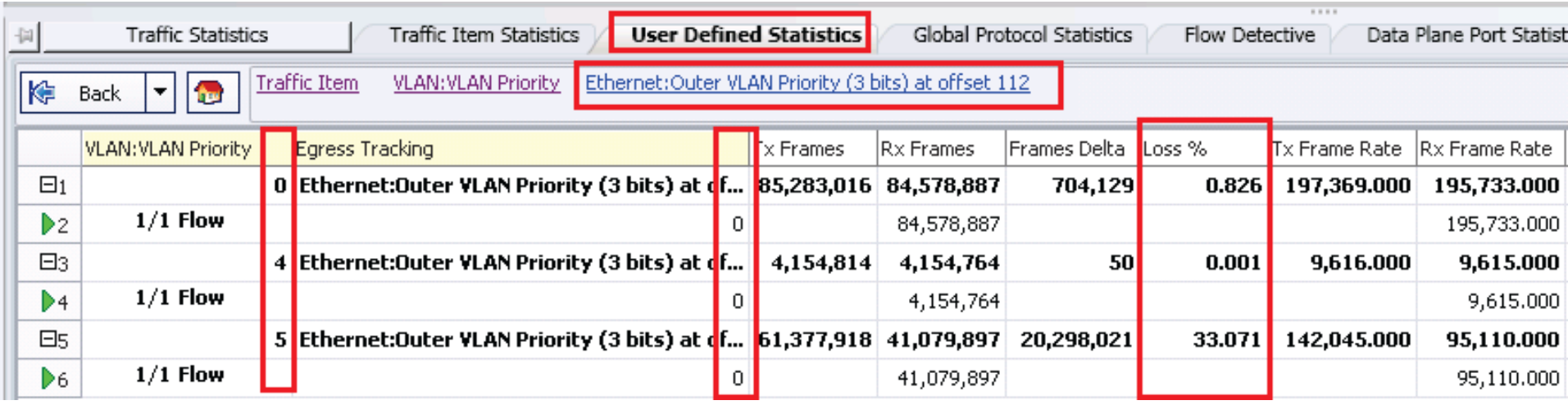


Use case #1: L2 QoS

Traffic Configuration ▸ L2-3 Flow Groups

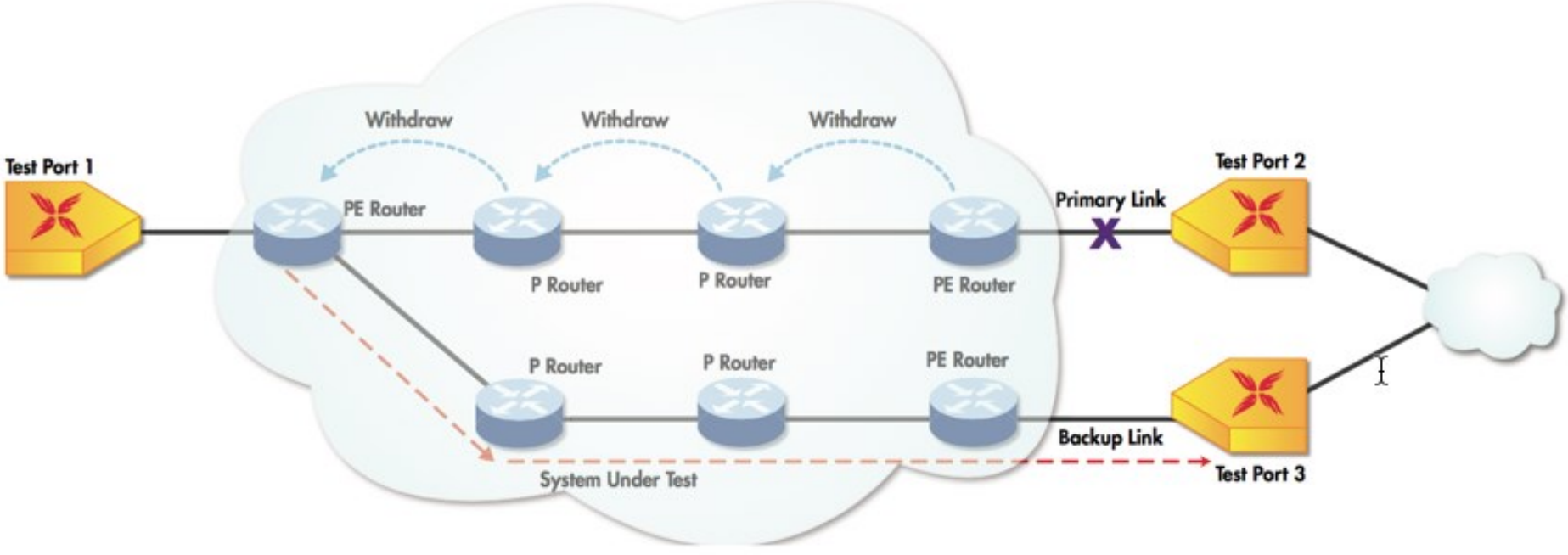
	Transmit State	Suspend	Tx Port	Encapsulation Name	Endpoint Set	VLAN:VLAN Priority	Traffic Item Name	Rx Ports
1			P1	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 0	L2QoS	P3;
2			P1	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 4	L2QoS	P3;
3			P1	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 5	L2QoS	P3;
4			P2	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 0	L2QoS	P3;
5			P2	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 4	L2QoS	P3;
6			P2	Ethernet II	EndpointSet-1	VLAN:VLAN Priority- 5	L2QoS	P3;

Use case #1: L2 QoS

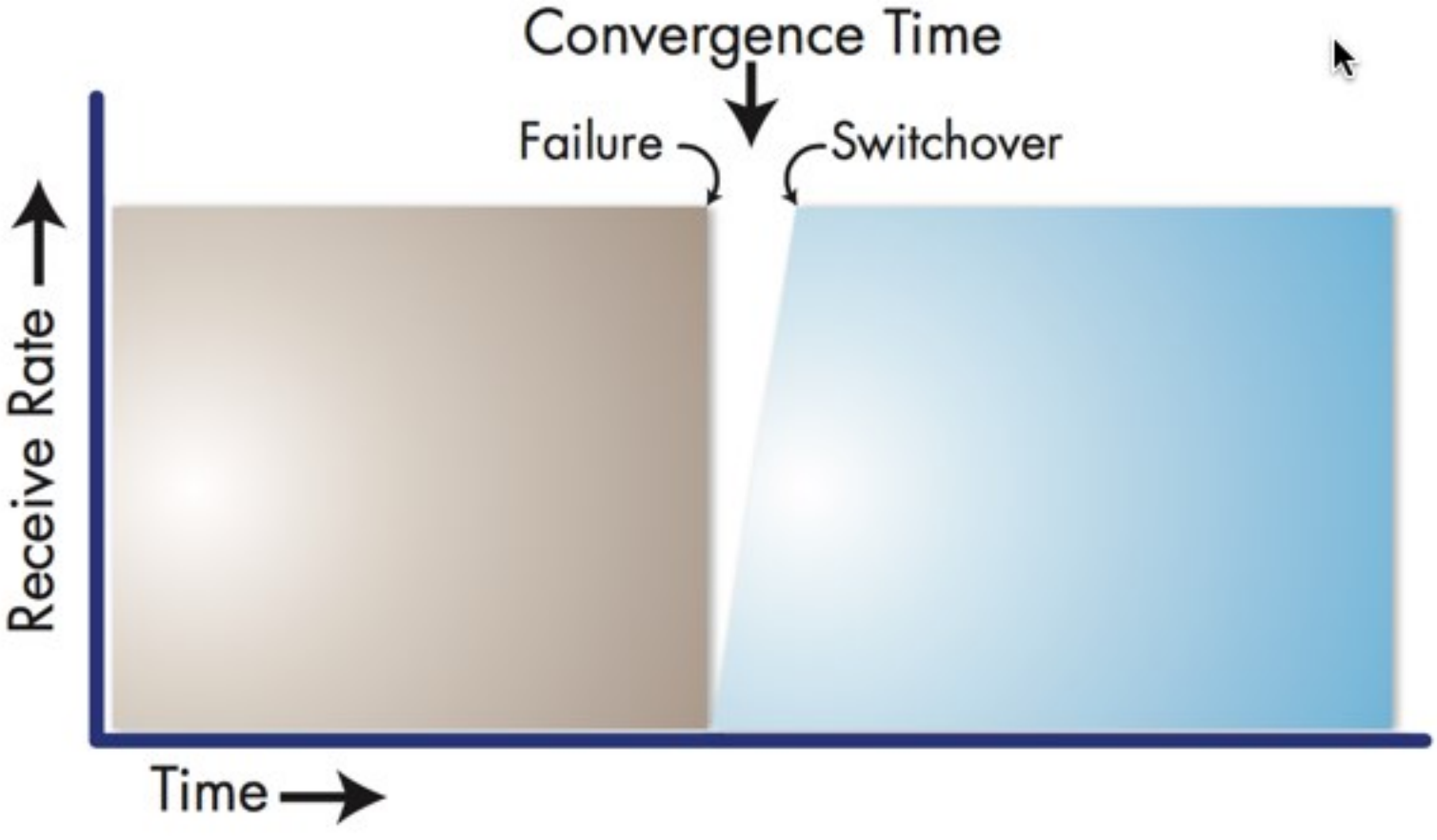


	VLAN:VLAN Priority		Egress Tracking		Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate
1		**0**	**Ethernet:Outer VLAN Priority (3 bits) at f...**		**85,283,016**	**84,578,887**	**704,129**	**0.826**	**197,369.000**	**195,733.000**
2	**1/1 Flow**			0		84,578,887				195,733.000
3		**4**	**Ethernet:Outer VLAN Priority (3 bits) at f...**		**4,154,814**	**4,154,764**	**50**	**0.001**	**9,616.000**	**9,615.000**
4	**1/1 Flow**			0		4,154,764				9,615.000
5		**5**	**Ethernet:Outer VLAN Priority (3 bits) at f...**		**61,377,918**	**41,079,897**	**20,298,021**	**33.071**	**142,045.000**	**95,110.000**
6	**1/1 Flow**			0		41,079,897				95,110.000

Use case #2: сходимость OSPF



Use case #2: сходимость OSPF



IXIA

Тестирование L4-7
ПО ixLoad

ixLoad


Генерация траффика приложений
Доставка приложений
Доставка Видео
Доставка Голоса
Проверка безопаност и

Использование

- Эмуляция клиент-серверного взаимодействия для тестирования сетевой инфраструктуры

Network Under Test

- Эмуляция клиентов для тестирования производительности конечных сер

Device Under Test

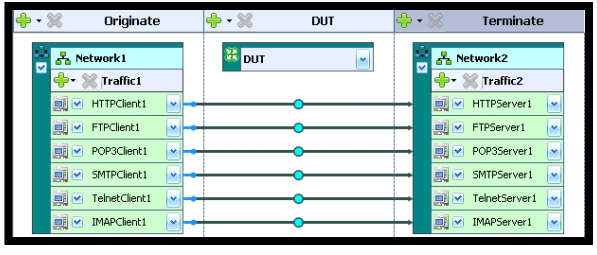
Протоколы и особенности

Протоколы

- Data → HTTP, HTTPS, FTP, Telnet, SMTP, POP3, IMAP, DDOS, DHCP, DNS, LDAP, RADIUS, TFTP, Application Replay, SQL
- VOIP → SIP, MGCP, RTP
- Video → IPTV, VoD, IGMP, RTSP, RTP, MPEG2-TS, MPEG4, H.264, VC1/WM9, OTT
- Peer-Peer → Bittorrent, eDonkey
- DHCP server

Сетевые стеки

- PPP, IPSec, DHCP (flexible option sets)
- VLAN support (802.1Q, QinQ, 802.1p)
- DSCP/TOS per protocol



Статистики

- Статистики в реальном времени
- Произвольные отчеты
- Данные по всем уровням взаимодействия L2-7 + QoE метрики

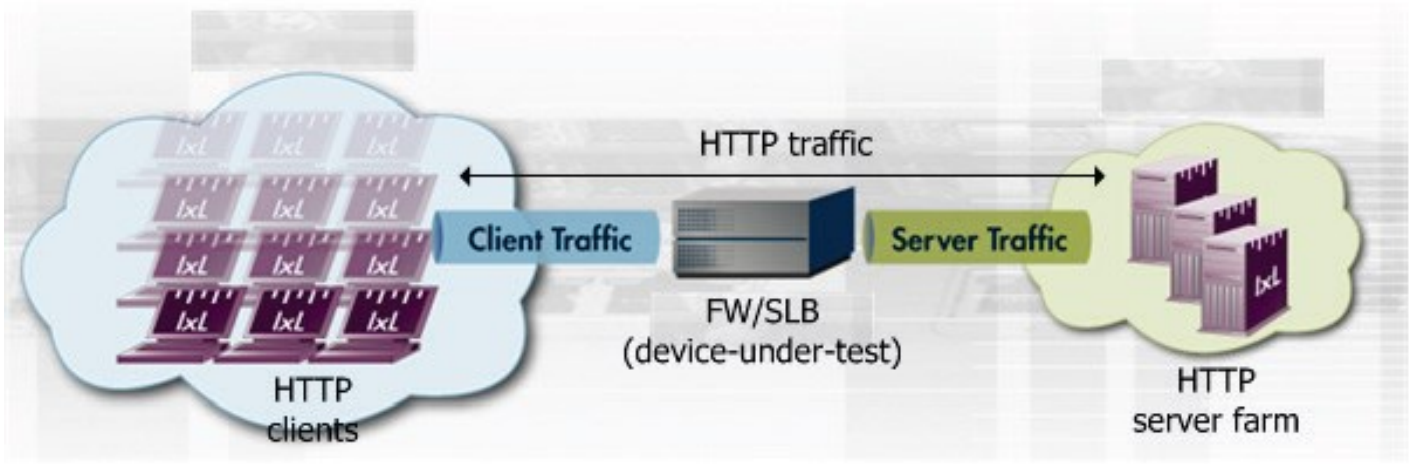
Анализ

- Захват пакетов
- Диаграммы протоколов
- Встроенный плеер аудио/видео

Автоматизация

- Полная поддержка TCL
- Test Conductor

Пример: HTTP
Одновременные соединения

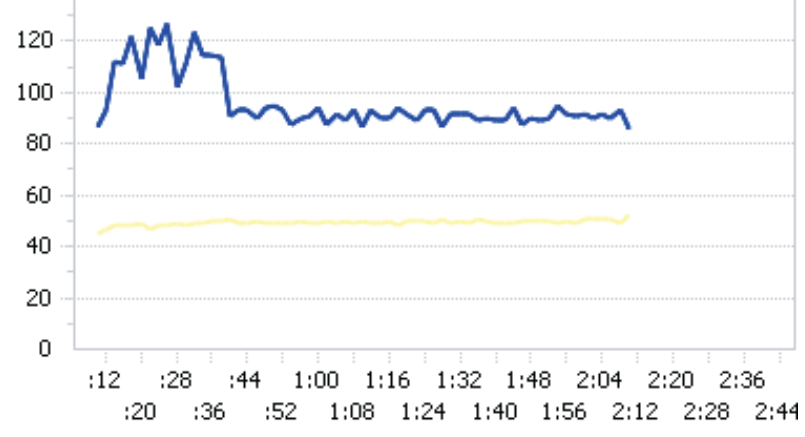


Пример: HTTP Одновременные соединения

HTTP Client - Objectives

	1:00	1:02	1:04	1:0
Simulated Users	7,500	7,500	7,500	7,5
Concurrent Connections	149,980	149,980	149,980	149,
Connection Rate	3,727	3,718	3,748	3,
Transaction Rate	3,730	3,724	3,741	3,
Connection Attempt Rate	3,726	3,724	3,742	3,

HTTP Client - Latencies



	:12	:14	:16	:18	:20	:22
Connect Time (µs)	47	48	48	48	49	47
Time To First Byte (TTFB) (µs)	93	112	111	122	106	125
Time To Last Byte (TTLB) (µs)	93	112	111	122	106	125

IXIA

Тестирование устройств защиты ПО Breakingpoint

Виды симуляций

- Легитимный трафик

Bit Blaster	Ethernet Фреймы	Layer 2
	IPv4/6 Пакеты	Layer 3
Session Sender	Сессии TCP/UDP	Layer 4
	Воссоздание PCAP файлов	Layer 4
Application Simulator	220+ Приложений Симулятор клиент-серверной модели	Layer 7
	Симулятор приложений клиента	Layer 7

- Вредоносный трафик

Security	35000+ Атак	100+ обходов
	TCP/UDP Фаззер	Фаззер приложний

Симуляция L2-L4 траффика

Модуль	Уровень	Задача
Bit Blaster	L2	Измерение характеристик коммутации
Routing Robot	L3	Измерение характеристик stateless маршрутизации
Stack Sender	**L4**	**Измерение характеристик state full маршрутизации – Connections Per Second, Concurrent Connections**
Recreate	L4	Воспроизведение PCAP файла с модификацией L2-L4 заголовков

Встроенные тесты RFC 2544

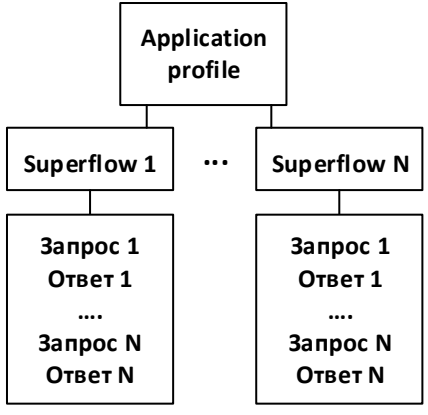
Также с помощью данных инструментов можно строить L3-L7 DDos атаки

Симуляция L7 траффика

Модуль	Уровень	Задача
Client Simulator	L7	Эмуляция клиентской стороны для тестирования сервисов
Application Simulator	**L7**	**Эмуляция клиент-серверной инфраструктуры для тестирования сетевых устройств**

Более 220 приложений.

- Создание условных запросов/ответов
- Динамическое содержимое на основе шаблонов
- Поддержка рассчитываемых полей-токенов
- Возможность написания собственных протоколов взаимодействия приложений



Симуляция атак

Модуль	Уровень	Задача
Stack Scrambler	L2-L7	Модификация служебных заголовков пакетов (Fuzzing)
Security	**L2-L7**	**Эмуляция пакетов реальных атак для тестирование средств сетевой безопасности**

Уникальное свойство платформы BreakingPoint

Более 35000 атак из публичных баз CVE, BugTraq, а также от собственного подразделения аналитиков безопасности с обновлением БД каждые 2 недели

Атаки категорированы по типу, приложениям, году выпуска.

Подходит для тестирование NGN МСЭ, IPS/IDS

[A] Analysis
[B] Backdoors
[D] Denial
[E] Exploits
[F] Fuzzers
[G] Generic
[M] Malware
[R] Recon
[S] Shellcode
[W] Worms

Симуляция DDoS атак L3-7

— **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

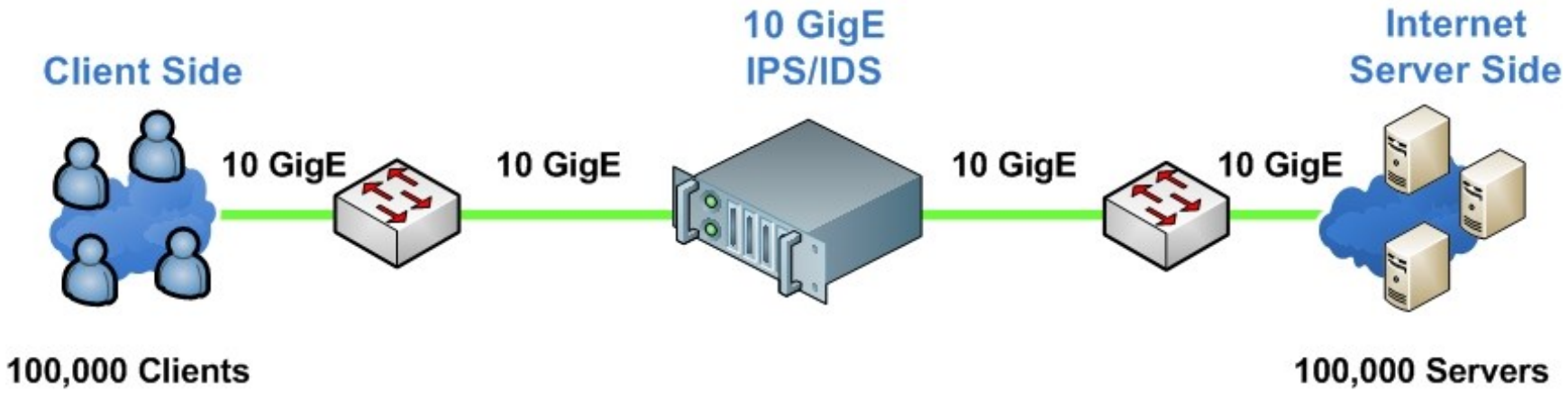
— **Layer 7 Apps**
✓ DDoS DNS Reflect - Attack
✓ DDoS DNS Reflect - Zombie
✓ LOIC HTTP DoS Attack
✓ DDoS SIP Invite Flood
✓ DDoS Redirect
✓ DDoS DNS Flood
✓ DDoS Excessive GET POST
✓ DDoS Slow POST
✓ DDoS Recursive GET

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

Пример теста

Выбор поставщика IDS

McAfee – M8000
Juniper – IDP 8200
Radware – DefensePro 8412
TippingPoint – 5100N



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

Результаты
L3 UDP Stateless Traffic

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

Результаты
L4 and L7 - TCP and HTTP

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

Результаты
L7 - Mix of Application Protocols

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

Результаты
Security test for Malicious traffic

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

Результаты
L7 – Mix of Good and Malicious Traffic

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 SEED 1	20	208	42	192

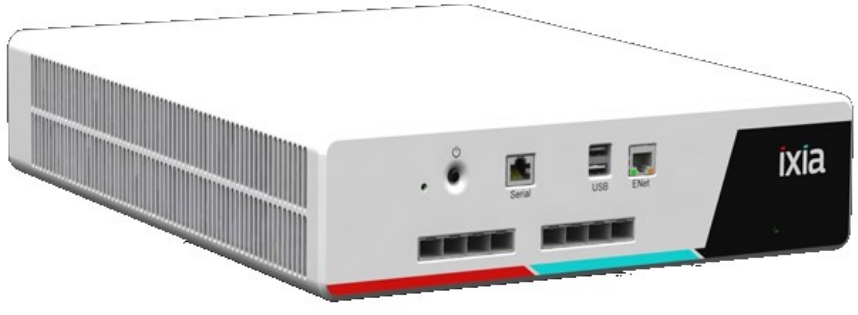
IXIA

Платформы

Аппаратные платформы

- 10/100/1000Mbps
- 10 GE
- 40 GE
- 100 GE
- 400 GE

PerfectStorm ONE

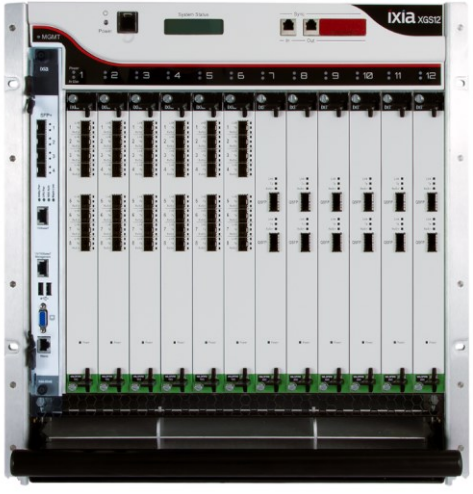


Apps	Applications	SSL Capacity
80 Gbps Throughput	60 Million Concurrent Flows	1 Million SSL Concurrent Flows

TCP Rates	SSL Rate
2 Million Connections per Second	200K SSL Connections/Second

- Портативное решение с 8 портами 1/10GE SFP+ или 2x40G
- Мощный встроенный контроллер управления
- **Высота 1.5U, 2.5”**
- Генерация трафика приложений stateful на скорости интерфейса
- Аппаратное ускорение SSL & Ipsec
- **Гибкое лицензирование по портам и полосе пропускания**

XGS-12



Applications	Connection Rate	Capacity
960	24	720
Gbps Apps Throughput	Million TCP CPS	Million HTTP CC

SSL Throughput	SSL Capacity	SSL CPS
240	12M	2.4M
Gbps SSL Throughput	Concurrent SSL Flows	SSL Connection Rate

Виртуальная платформа

Приложения	Connection Rate	Capacity
6	180	13
Gbps Apps Throughput	Thousand TCP CPS	Million HTTP CC

На каждый vContoller

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

Выводы

- Самая мощная на рынке платформа для L4-7 тестирования
- Единое решение для всех аспектов тестирования с возможностью простого масштабирования
- Оперативная реализация последних протоколов и технологий, начиная с появления RFC draft
- Удобный и понятный графический интерфейс приложений
- **Поддержка 24/7** (первая линия, IXIA Европа) и квалифицированные русскоязычные инженеры в Москве
- **Обучение на русском языке** и английском языках
- Сохранение инвестиций заказчика и соблюдение гарантийной политики (5.5 лет до EoL после EoSA)
- Возможность всегда оперативно получить **демо лицензию**, когда это требуется
- Большой демо пул модулей и систем для подмены на случай оперативной покупки/поломки или краткосрочной аренды

Спасибо!