

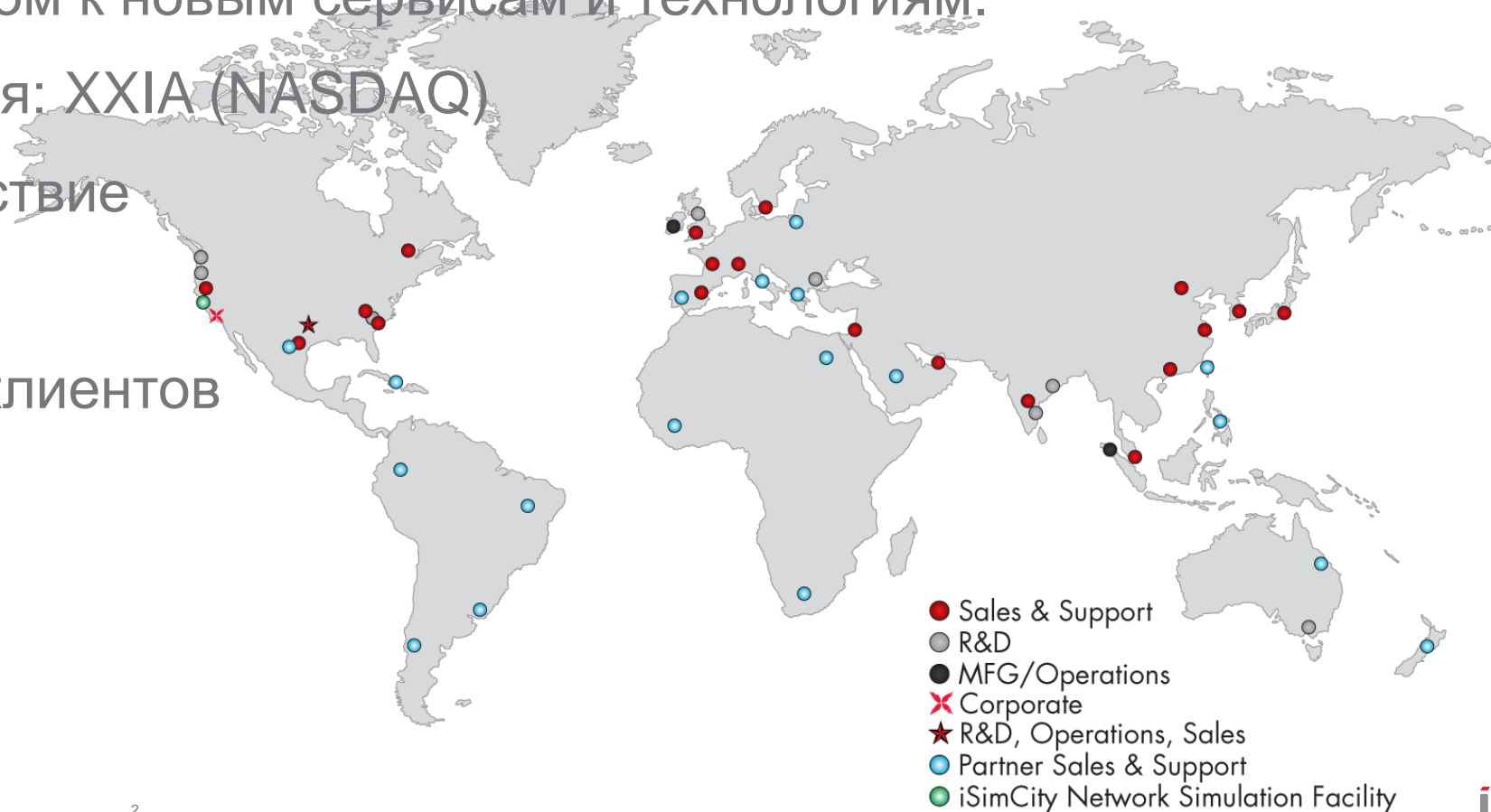
The logo for ixia is centered on a 3D cube. The cube is rendered in shades of blue, with the top and right faces being a darker blue and the left face being a lighter blue. The word "ixia" is written in a white, lowercase, sans-serif font across the front face of the cube. The letter 'i' has a small red dot, and the letter 'x' has a small blue dot. The background of the entire image is a teal color with a subtle, repeating pattern of light blue hexagons.

ixia

SECURITY SOLUTIONS

## О КОМПАНИИ IXIA

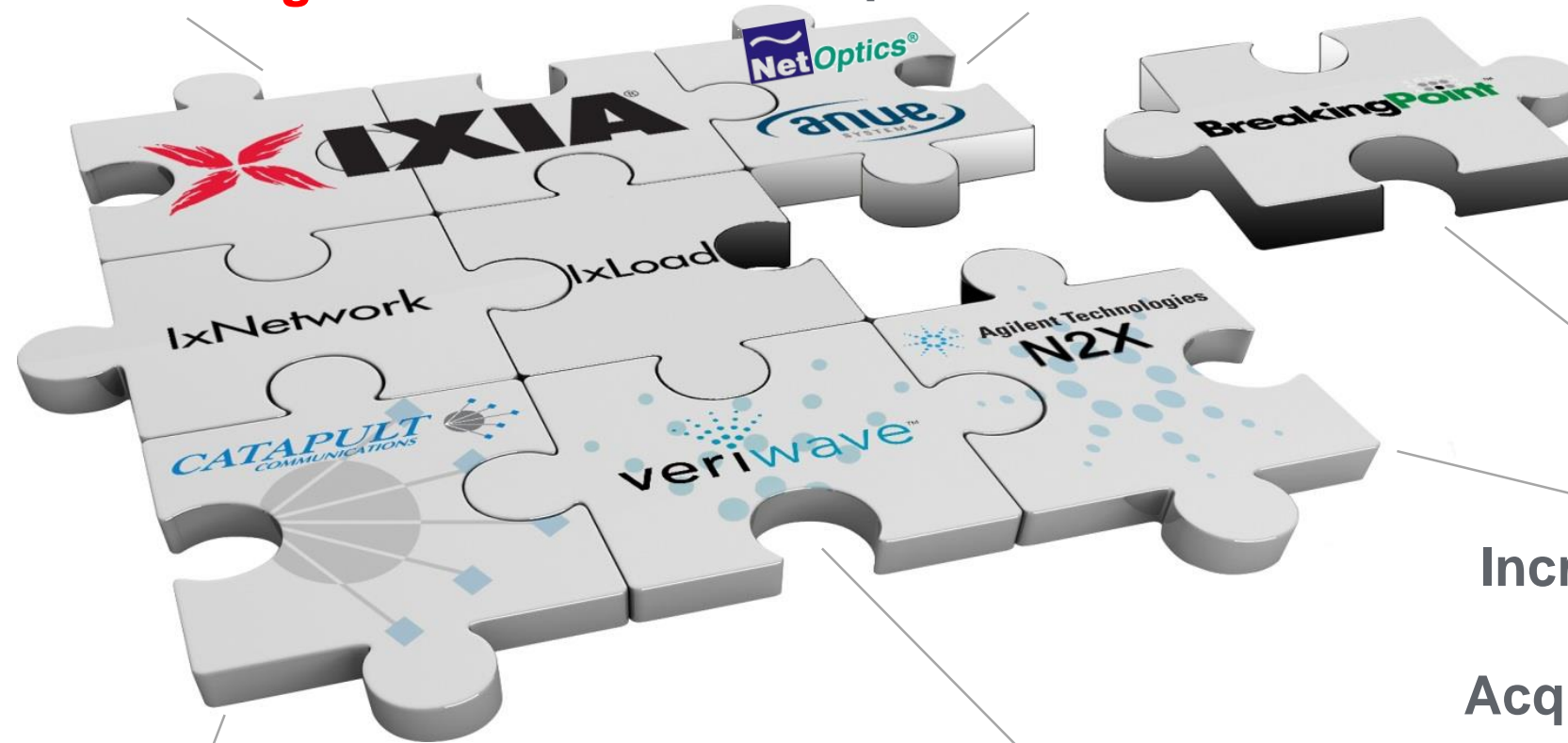
- Решения компании Ixia помогают вам уверенно развивать свой бизнес, обеспечивая ему надёжную и защищённую связь с внешним миром. Благодаря продуктам Ixia, ваши клиенты обеспечены самым быстрым и безопасным доступом к новым сервисам и технологиям.
- Публичная компания: XXIA (NASDAQ)
- Глобальное присутствие
- 1800+ сотрудников
- 2500+ постоянных клиентов



# END-TO-END PRODUCT FAMILY

Founded in 1997  
IP Testing

Network **Visibility**  
Acquired June 2012



Actionable **Security**  
Intelligence (ASI)  
Acquired August 2012

Increased Router  
Testing  
Acquired Oct 2009

Wireless Testing  
Acquired June 2009

Wi-Fi, WLAN Testing  
Acquired July 2011

# IXIA ПОМОГАЕТ НА ВСЁМ ЖИЗНЕННОМ ЦИКЛЕ ИТ

**Проектирование**

**Эксплуатация**

**Оптимизация**

## **Разработка проекта**

Тестирование  
Выбор вендора  
Proof of Concept  
Совместимость оборудования  
Производительность  
Новые технологии

## **Уверенность**

Аттестация  
производительности и  
безопасности при вводе в  
эксплуатацию новых сетей  
и услуг

## **Оптимизация**

Масштабируемость,  
Снижение стоимости и  
повышение эффективности  
систем информационной  
безопасности и мониторинга



## Тестирование и аттестация систем информационной безопасности!



# НАСКОЛЬКО ВЫ УВЕРЕНЫ В ВЫБОРЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

## Data Sheet

### Managed Web Application Firewall

Web applications are mission critical for most organizations, but many are challenged to manage the security and compliance of these applications. Further, the security threat landscape is constantly changing, increasing an organization's risk to breaches and data loss. A Web Application Firewall (WAF) helps organizations mitigate risk, as well as assist in meeting certain compliance requirements.

#### Simplified Application Protection: How Do We Do It?

Trustwave's affordable, turnkey Managed WAF solution protects against some of today's security threats and helps you meet certain requirements, such as the Payment Card Industry Data Security Standard (PCI DSS).

Trustwave security experts start by deploying Trustwave WebDefend, which features advanced, patent-pending application profiling and event correlation technology, in customer or hosted data centers. Events from WebDefend are then delivered to Trustwave's SAS-70 compliant Security Operations Center (SOC), where our security experts use Trustwave's award-winning SIEM technology to analyze protected Web application traffic in its organizational and Internet-wide context. This analysis is used to spot attacks and quickly understand and adapt to changes.

WebDefend® + Managed Security Services = Efficient, Thorough Coverage

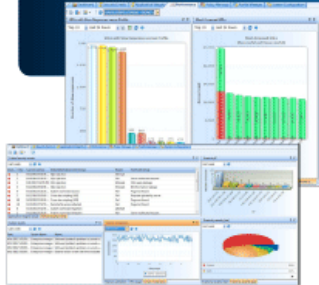
#### Trustwave WebDefend

Award-winning Trustwave WebDefend is a highly scalable Web application firewall that provides real-time, continuous security against attacks and data loss with the assurance that your Web applications operate as intended and are compliant with industry regulations.

WebDefend is integrated with our award-winning Trustwave SIEM, which serves as the nerve center to our Unified Security approach by correlating and consolidating attack information from any sources beyond Web applications to deliver simplified security and faster response to threats.

#### Key Features of Managed WAF

- Deployment and tuning of the WebDefend appliance
- Continuous system health monitoring
- 24x7x365 event monitoring and alerting, and periodic log review options
- Tuning support for scheduled changes to protected applications
- Customer access to events and reports through the MSS Portal
- A advanced Web application security detection and protection including coverage of the OWASP Top 10 Web application attacks
- Facilitates compliance with PCI DSS requirements, e.g.



Optimized protection against the size of sensitive information

Only WebDefend uses a patent-pending profiling system and multiple, collaborative detection engines to ensure the flow of mission-critical traffic while supplying complete protection for applications to keep your confidential information safe from targeted attacks.

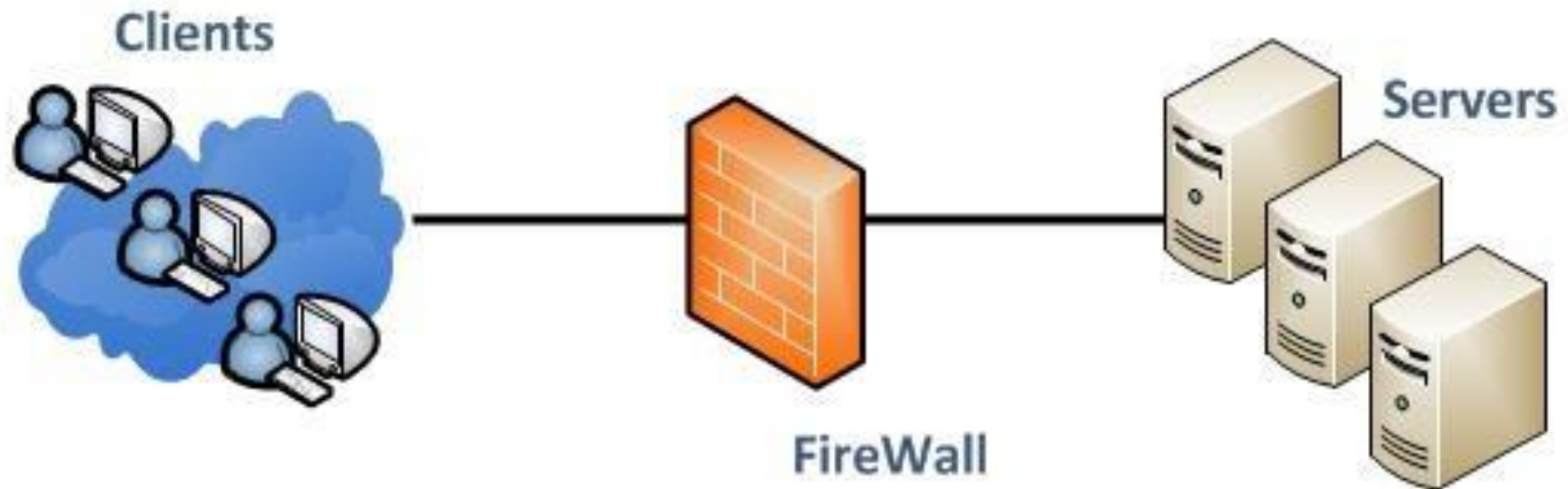


As of May 2013

Доверяю интегратору

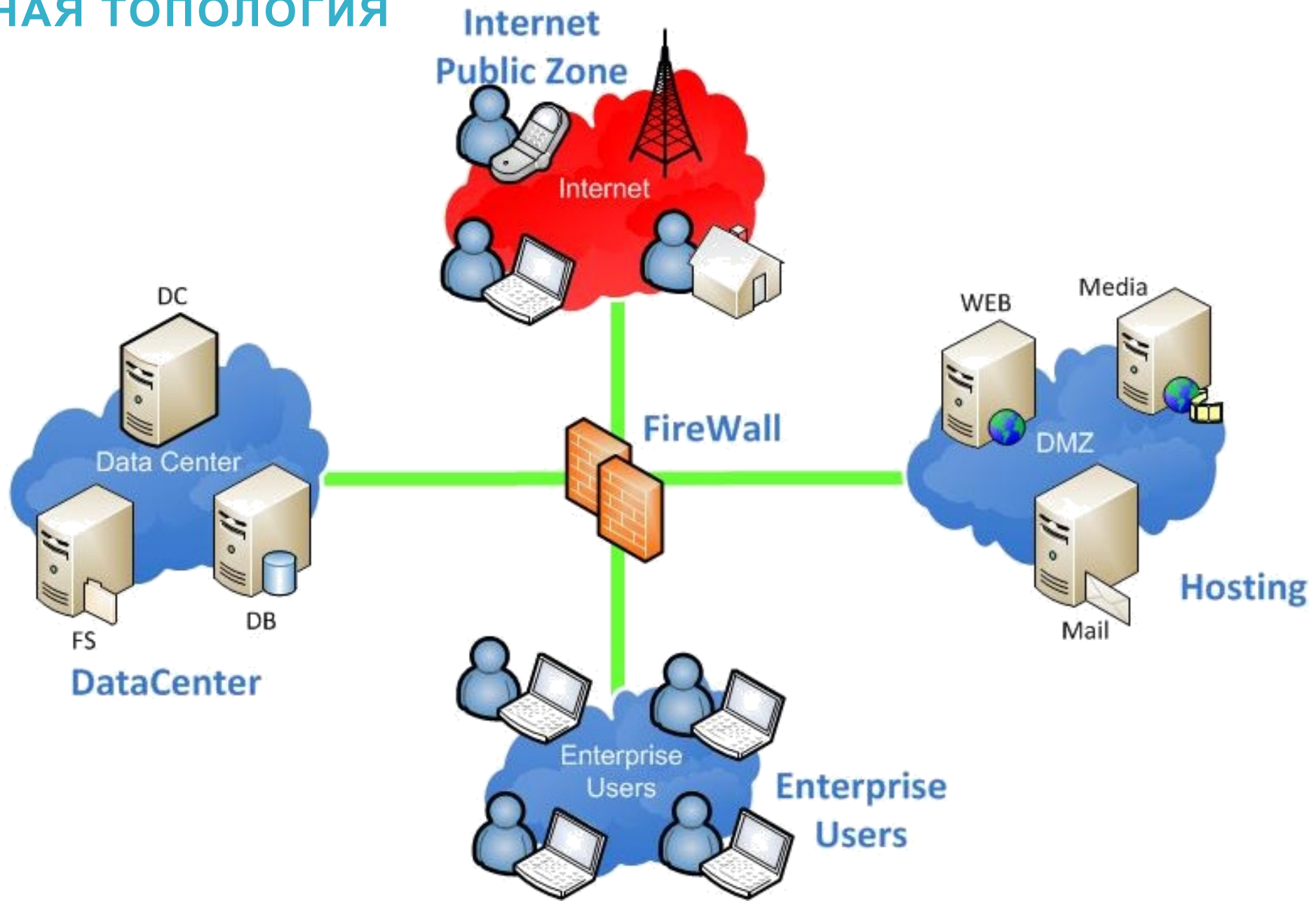


# МАРКЕТИНГОВЫЕ ПАРАМЕТРЫ ПРОИЗВОДИТЕЛЬНОСТИ



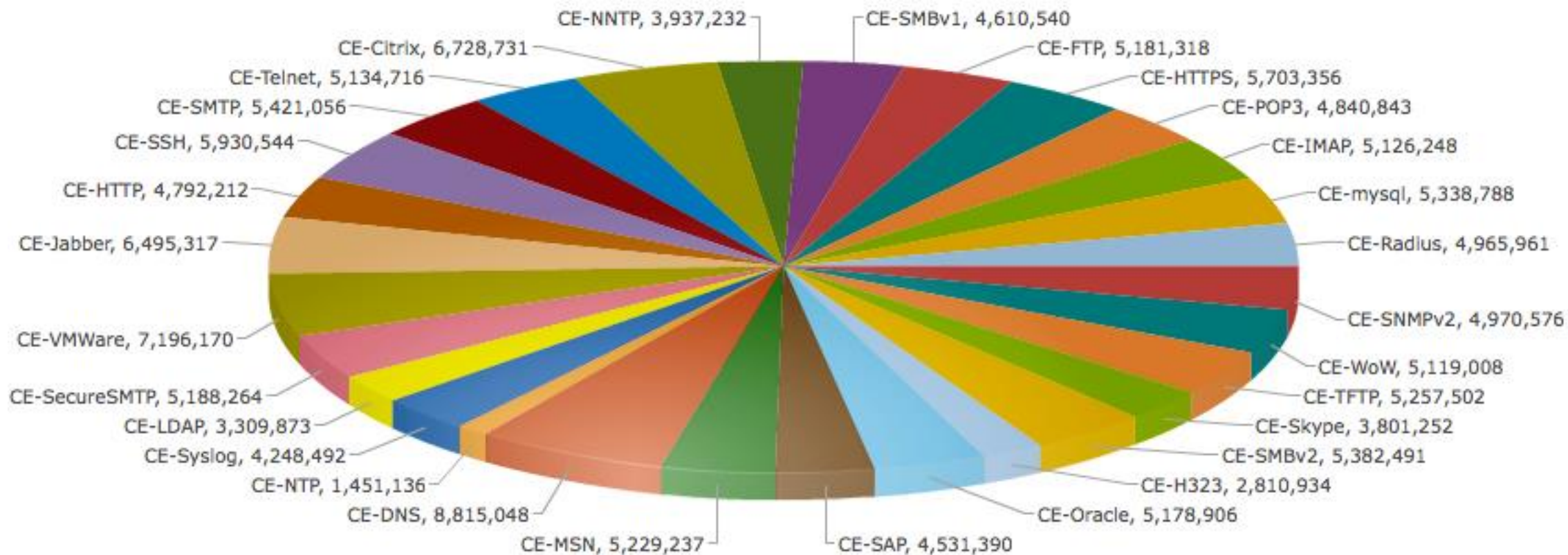
Основаны на базовой сетевой топологии  
Трафик только HTTP over TCP  
Упрощённые HTTP GET / HTTP Response

# РЕАЛЬНАЯ ТОПОЛОГИЯ

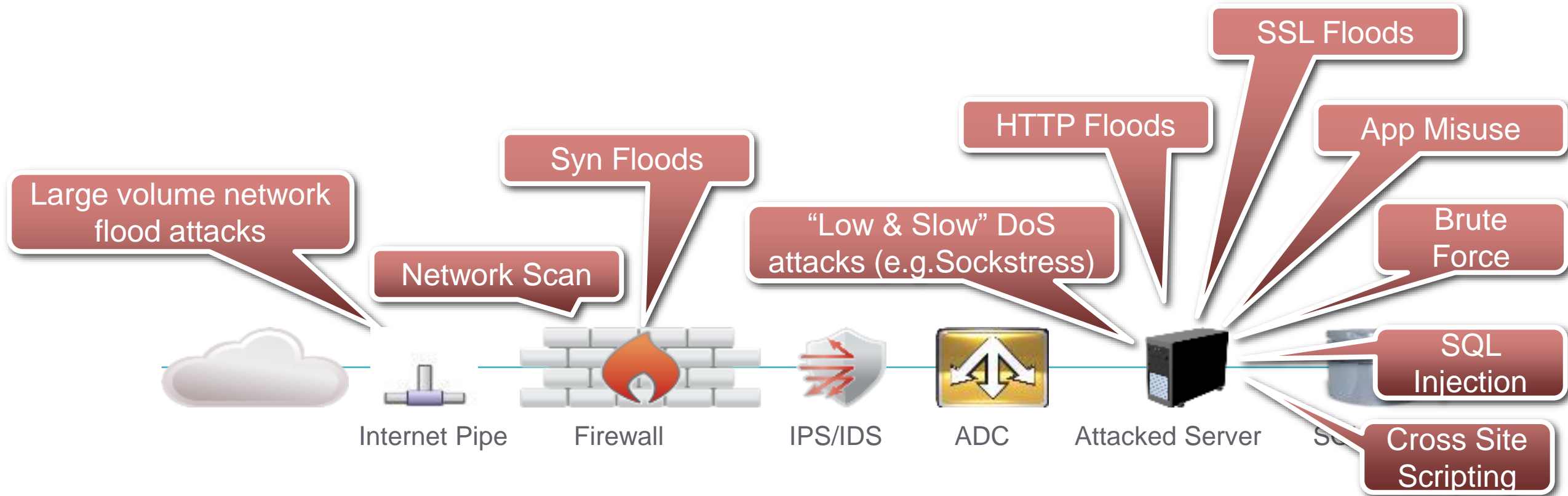




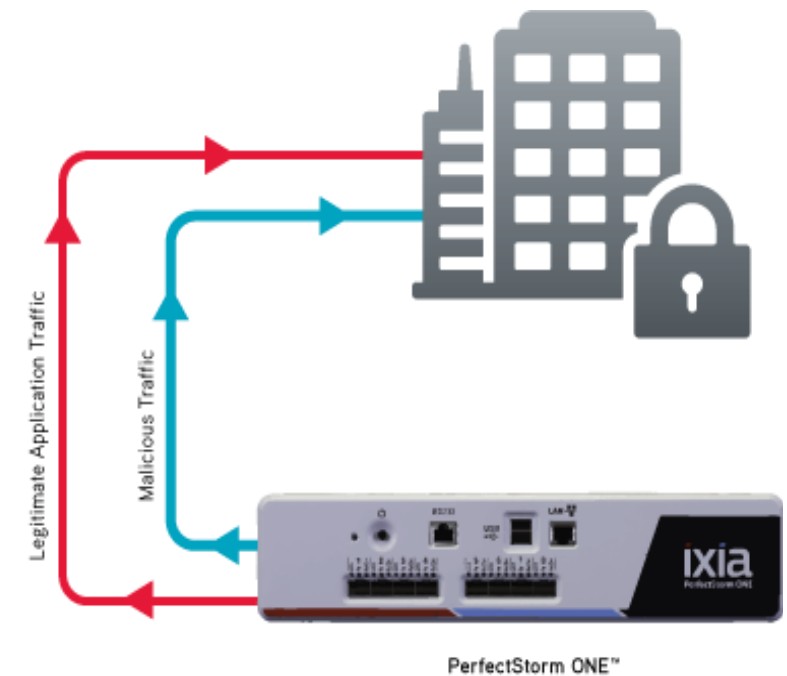
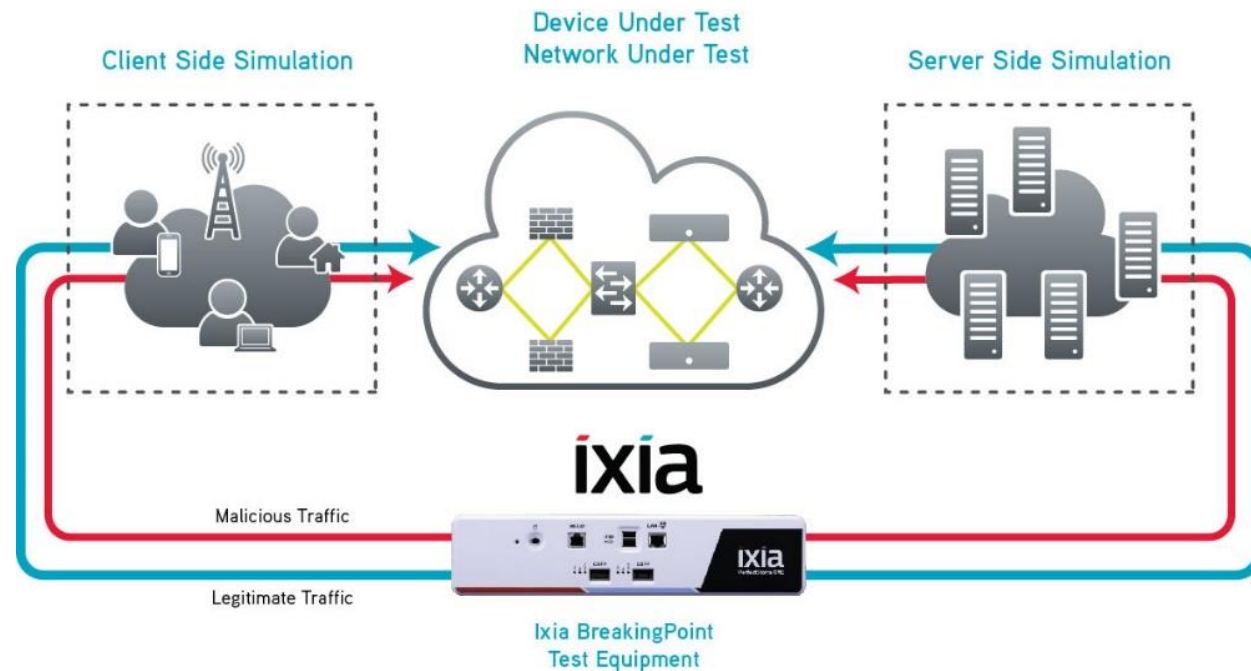
# ТРАФИК РЕАЛЬНОЙ СЕТИ



# ВРАГ НЕ СПИТ!!!



# IXIA BREAKINGPOINT



IXIA BreakingPoint – уникальный продукт, позволяющий воспроизводить реальную инфраструктуру сети с большим объёмом легитимного и вредоносного трафика L2-L7 для тестирования производительности, безопасности и стабильности сетевых элементов

# МЕТОДЫ ДОСТИЖЕНИЯ МАКСИМАЛЬНОЙ ЭФФЕКТИВНОСТИ И НАДЁЖНОСТИ СИСТЕМ БЕЗОПАСНОСТИ

## Метод

## Результат

### Производительность

Выявление скрытых недостатков, определение предельной производительности при максимальной нагрузке трафика приложений и атак.

Увеличение производительности путём оптимизации дизайна и конфигурации. Понимание предела производительности системы.

### Безопасность

Выявление уязвимостей и слабых мест в системе защиты с применением новейших методов атак, вирусов, спам-методик и актуальных версий приложений.

Уверенность, что все элементы сети защищены от новейших угроз и готовы к передаче трафика современных приложений.

### Стабильность

Эмуляция некорректной работы сети и приложений при максимальной нагрузке для оценки стабильности работы сетевых элементов.

Проактивное выявление нестабильных элементов для защиты от сбоев в работе сети и передачи трафика, которые могут привести к финансовым и имиджевым потерям.

НАДЁЖНОСТЬ

# ТЕСТОВЫЕ ПЛАТФОРМЫ



## PerfectStorm

Chassis supports up to 12 load module Scales from 80G to 960G Support 1GbE, 10GbE, 40GbE, 100GbE



2-ports of 40GE with the QSFP+ interface



8-ports of 10GE with the SFP+ interface

## PerfectStorm ONE

Appliance Scales from 4G to 80G Support 1GbE, 10GbE, 40GbE



## BreakingPoint VE

Standard x86 server & Hypervisor 1Gbps increment subscription Any Host Interfaces

# КРАТКИЙ СПИСОК ЭМУЛИРУЕМЫХ ПРИЛОЖЕНИЙ

Mobile
ActiveSync
Apple App iTunes/Store
Android Market
HTTP Mobile
BlackBerry Services
BBC iPlayer
Facebook for IOS Devices
Google Android Market
S1AP
TuMe
TVUplayer
Viber
YouTube Mobile
WhatsApp

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

Custom Applications
RAW
SCADA
IEC104

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

Social Networking
Facebook
Flickr
Linkedin
Twitter
Wikipedia

Telephony and Cable TV
SMPP
MM1
TR-069

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

Streaming Media
Pandora
Netflix

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

# КРАТКИЙ СПИСОК ЭМУЛИРУЕМЫХ ПРИЛОЖЕНИЙ. ЧАСТЬ 2

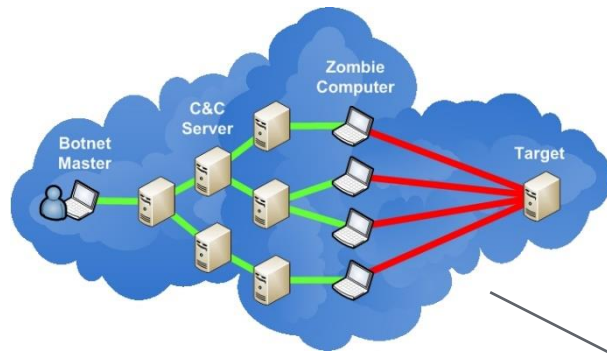
Chat   Instant Messaging
AIM6
AOL Instant Messenger
Google Talk
Gadu-Gadu
ICQ
IRC
Jabber
MSN
MSNP
MSN Switchboard
OSCAR
OSCAR File Transfer
QQ IM / Live
Windows Live Messenger
Winy
Yahoo! Messenger
Web Application
Bing Search
eBay
Google Search
Google MAP
Google Earth
Paypal
Reddit WebApp
Yahoo Search
WebEx

Authentication
DIAMETER
RADIUS Accounting
RADIUS Access
Data Transfer
FTP
Gopher
HTTP
NNTP
RSync
TFTP
WebDav
Data Transfer / File Sharing
IPP
NetBIOS
NETBIOS DGM
NETBIOS NS
NETBIOS SSN
NFS
RPC NFS
SMB
SMB/CIFS
SMBv2
Games
World of Warcraft
Xbox Live

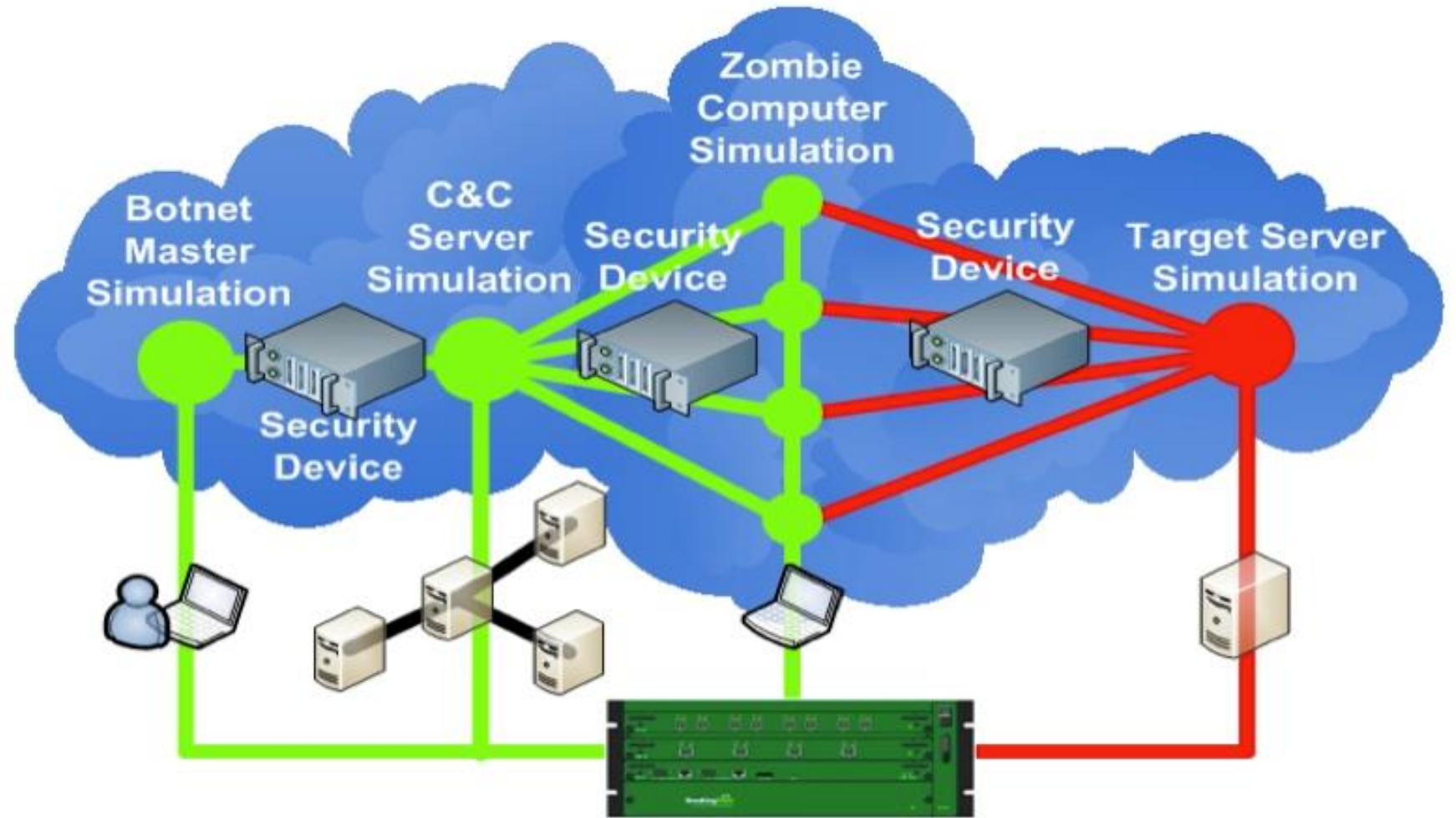
Databases
IBM DB2
Informix
Microsoft SQL
MySQL
Oracle
PostgreSQL
SQLMON
Sybase
TDS
TNS
Distributed Computing
Citrix
DCE/RPC
VMware VMotion
Enterprise Applications
DCE/RPC Endpoint Mapper
DCE/RPC Exchange Directory
LPD
MODBUS
SAP
Secure Data Transfer
HTTPS
SSH

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

# IXIA BREAKINGPOINT BOTNET SIMULATION



Real Topology



Ixia BreakingPoint Test Equipment

- ✓ TDL4
- ✓ Duqu
- ✓ ZeroAccess
- ✓ Evil
- ✓ PushDO
- ✓ TDW
- ✓ Zeus
- ✓ Customization in Application Editor



# BREAKINGPOINT DDOS SIMULATION

## 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

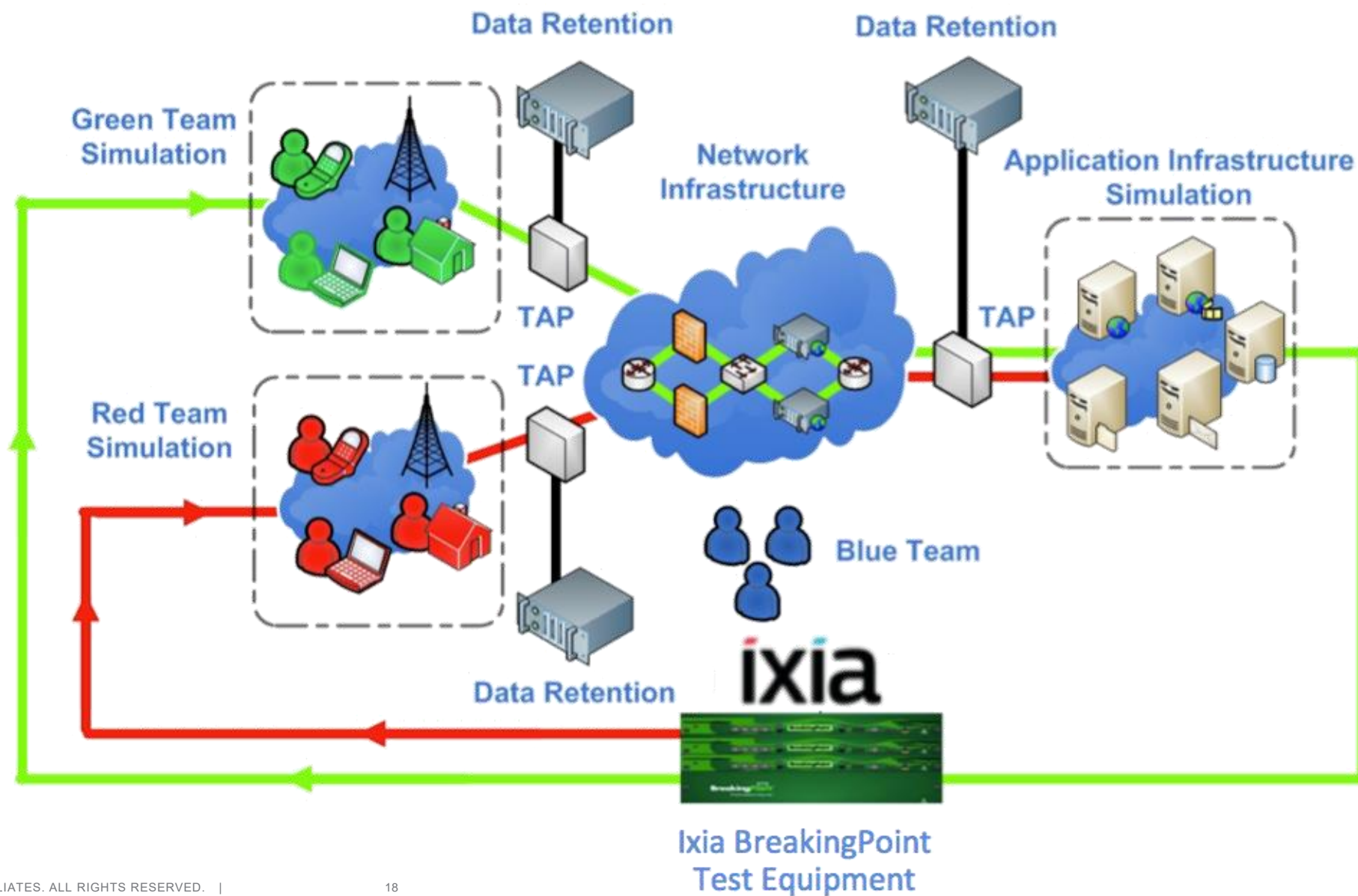
## Layer 7 Apps

- ✓ 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

# СYBER RANGE: В УЧЕНИЯХ КАК В БОЮ



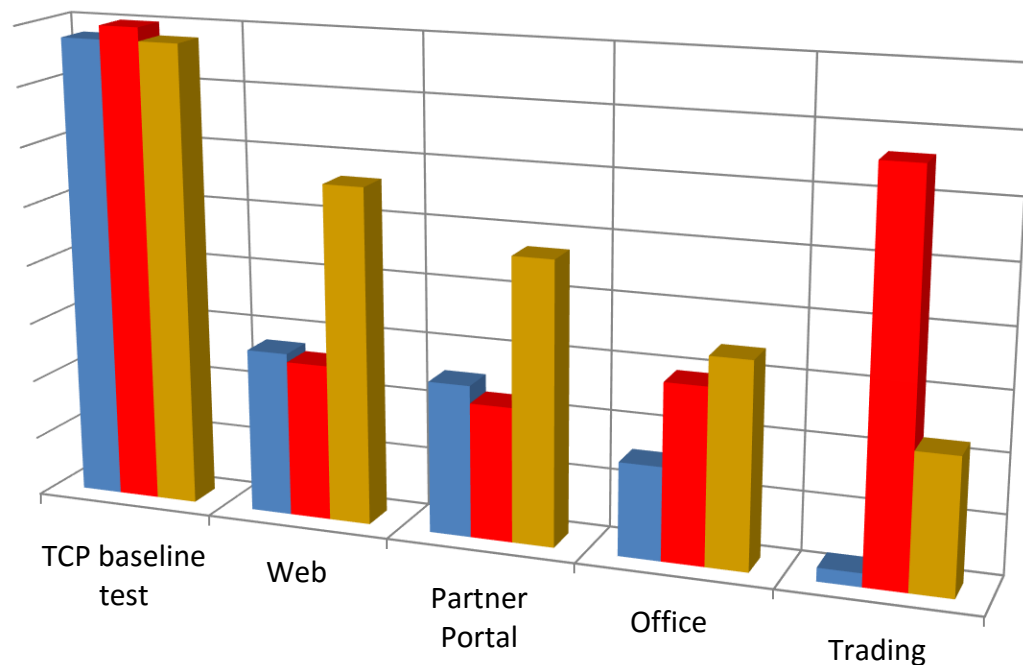
# ОБОРУДОВАНИЕ, КОТОРОЕ МОЖЕТ БЫТЬ АТТЕСТОВАНО С ПОМОЩЬЮ BREAKINGPOINT

- UTM
- IDS/IPS
- QoS Deep Packet Inspection
- Firewall
- Web Application Firewall
- Load Balancer
- WAN Accelerator
- Network Probe
- Lawful Interception Systems
- 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 многое, многое другое



# ПРИМЕР – ВЫБОР NGFW

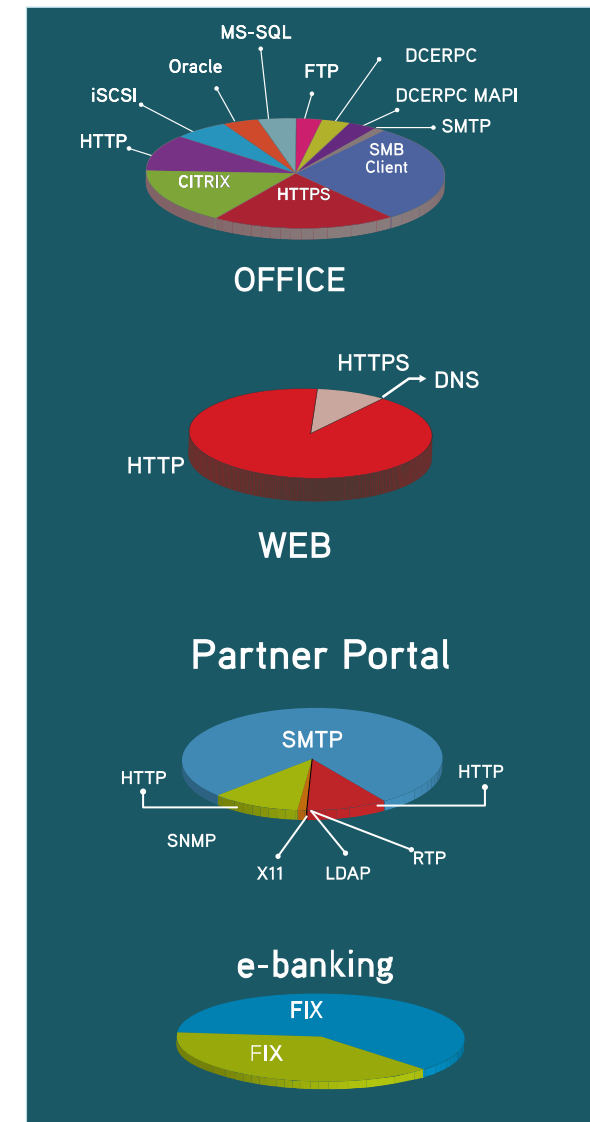
- Внедрение корпоративного NGFW в банке
- Задача: выбрать вендора
- Компания имеет 4 типовых сценария
- Все вендоры NGFW заявили производительность 1Gbps



■ Vendor A    ■ Vendor B    ■ Vendor C

	Vendor A	Vendor B	Vendor C
Avg Sec effectiveness *	48%	52%	28%

\*BreakingPoint StrikePack 5



# ГОДОВАЯ ПОДПИСКА APPLICATION & THREAT INTELLIGENCE (ATI)

## Simulation and Testing

# ixia



## Application and Threat Intelligence



## Real Attacks

- 6,000+ live security attacks
- 36,000+ pieces of live malware
- 180+ evasions
- DDoS and botnet simulation
- Custom attacks
- Research and frequent updates

## Real-World Applications

- 300+ application protocols
- Social, peer-to-peer, voice, video
- Web, enterprise applications, gaming
- Mobile
- Storage workloads
- Custom applications
- Frequent updates

## Unprecedented Performance

- 960 Gbps blended application traffic
- 720M concurrent HTTP sessions
- 24M HTTP sessions/second
- 12M CC SSL sessions/second

Раз в 2 недели

Новые приложения

Новые угрозы/Атаки

# IXIA DEVELOPER



## **BreakingPoint Personal edition**



# РЕАЛЬНОСТЬ КОМПАНИИ-РАЗРАБОТЧИКА

## Различные модели разработки – одинаковые проблемы



# РЕЗУЛЬТАТ – ПЛОХАЯ ЭФФЕКТИВНОСТЬ

- Бюджет найден поздно, а поздно найденные баги очень дорого исправлять
- Баги обычно сложно анализировать инструментами, ориентированными на QA



**\$59.5 Billion**

Annual Cost of Bugs to U.S. Economy

## EARLY DISCOVERY SAVES MONEY

Data from NIST and Ponemon Institute

**\$80/defect**

**DEVELOPMENT**

**\$240/defect**

**BUILD**

**\$960/defect**

**QA/TEST**

**\$7,600  
/defect**

**1 Defect  
For Every 2k  
Lines of Code**

**PRODUCTION**



# ЧТО ЕСЛИ БЫ МЫ СМОГЛИ

- *увеличить эффективность ?*
  - легкое решение, доступное всем
  - находить баги раньше
  - расследовать проблемы быстрее
  - радоваться богатым возможностям генератора трафика
  - никакого дорогого железа
- *дать ощущение разработчикам, что они часть сообщества ?*
  - прямой канал для отзывов
  - прозрачный roadmap, на который вы можете повлиять
  - внесите свой вклад!



# НО ЕСТЬ ЖЕ БЕСПЛАТНЫЕ ИНСТРУМЕНТЫ...

Здорово, если они работают, но ...

- Ограниченная поддержка или ее отсутствие
- Ограниченная функциональность
- Редкие обновления
- Часто требуется пересобрать и адаптировать



```
root@bt: /pentest/sniffers/tcpreplay
File Edit View Terminal Help
root@bt: /pentest/sniffers/tcpreplay# ./tcpreplay --intf=eth0 test.pcap
sending out eth0
processing file: test.pcap
Actual: 263 packets (196705 bytes) sent in 7.72 seconds.      Rated: 2
5479.9 bps, 0.19 Mbps, 34.07 pps
Statistics for network device: eth0
  Attempted packets:      263
  Successful packets:    263
  Failed packets:         0
  Retried packets (ENOBUFS): 0
  Retried packets (EAGAIN): 0
root@bt: /pentest/sniffers/tcpreplay#
```

```
C:\Windows\System32\cmd.exe - server.bat
C:\Iperf>iperf -l 8942 -p 5001 -w 1048576 -M 8942 -s -i 5
Server listening on TCP port 5001
TCP window size: 1.00 MByte

[1868] local 192.168.2.1 port 5001 connected with 192.168.2.20 port 53925
[ ID] Interval          Transfer      Bandwidth
[1868] 0.0- 5.0 sec      376 MBytes    631 Mbits/sec
[1868] 5.0-10.0 sec     568 MBytes    953 Mbits/sec
[1868] 10.0-15.0 sec     579 MBytes    972 Mbits/sec
[1868] 15.0-20.0 sec     582 MBytes    977 Mbits/sec
[1868] 20.0-25.0 sec     581 MBytes    976 Mbits/sec
[1868] 25.0-30.0 sec     576 MBytes    967 Mbits/sec
[1868] 30.0-35.0 sec     585 MBytes    981 Mbits/sec
[1868] 35.0-40.0 sec     582 MBytes    976 Mbits/sec
[1868] 40.0-45.0 sec     579 MBytes    972 Mbits/sec
[1868] 45.0-50.0 sec     583 MBytes    979 Mbits/sec
[1868] 50.0-55.0 sec     584 MBytes    980 Mbits/sec
[1868] 55.0-60.0 sec     583 MBytes    978 Mbits/sec
[1868] 60.0-65.0 sec     467 MBytes    783 Mbits/sec
[1868] 65.0-70.0 sec     585 MBytes    981 Mbits/sec
[1868] 70.0-75.0 sec     589 MBytes    988 Mbits/sec
[1868] 75.0-80.0 sec     582 MBytes    977 Mbits/sec
```

# ПРЕДСТАВЛЯЕМ IXIA DEVELOPER!

Легкий тестовый инструмент разработчика, который станет незаменимой частью жизненного цикла

- Генерация реалистичного трафика приложений с подмешиванием атак
- Специальные функции для разработчиков: отладчик, breakpoints, захват
- Именная лицензия
- Быстрый цикл релизов
- Встроенный механизм обратной связи
- Классный HTML UI и классический CLI
- Расширяется плагинами



# РАЗВОРАЧИВАНИЕ IXIA DEVELOPER

- Легкое виртуальное решение
  - одна VM (<1GB)
  - не надо разворачивать порты
  - вписывается в типовое окружение разработчика
- Быстро разворачивается
  - Менее 2 минут
- Online авторизация



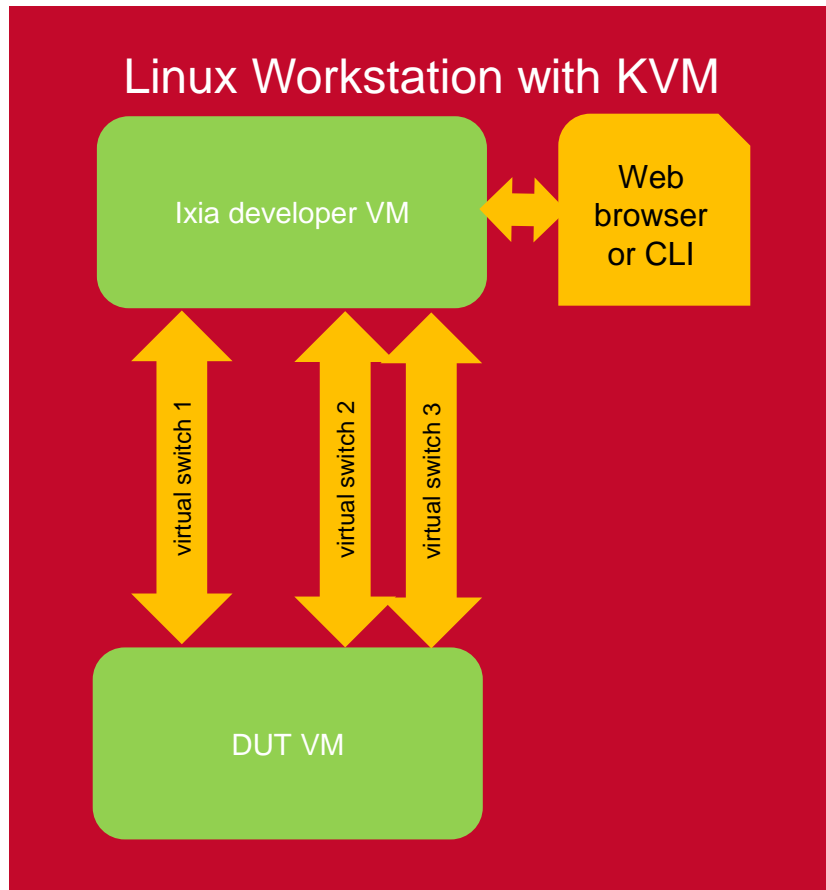
VMWare ESX



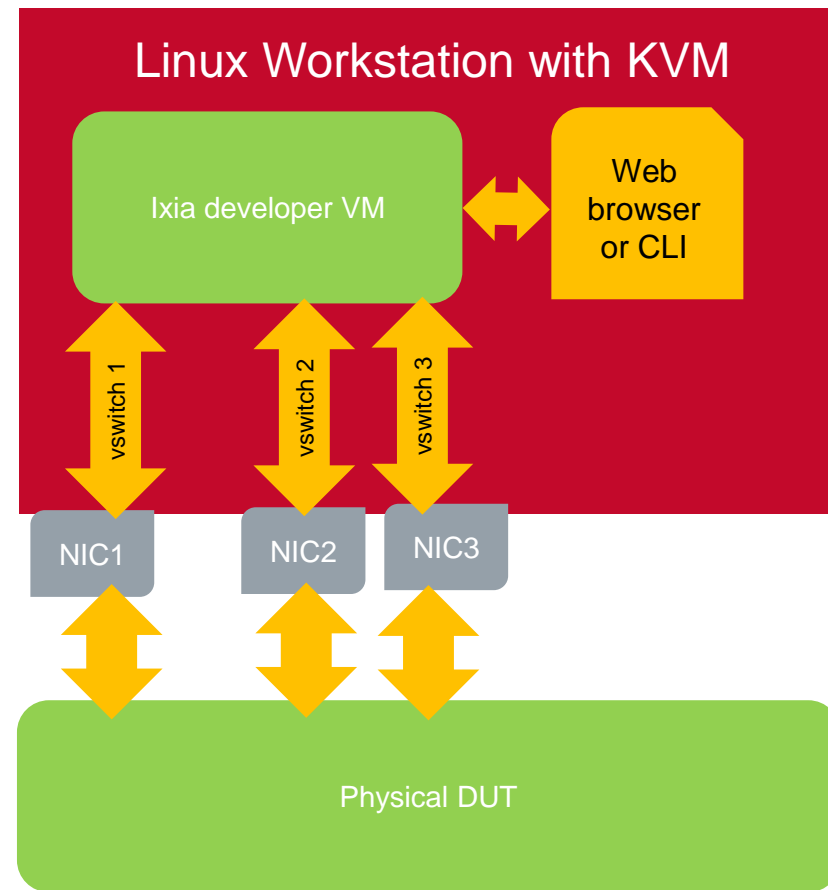
VMware Fusion



# СХЕМА ВЗАИМОДЕЙСТВИЯ



Тест внутри виртуальной среды



Тест физического устройства

# ВЗАИМОДЕЙСТВИЕ С СООБЩЕСТВОМ

The screenshot displays the Ixia Developer Dashboard. At the top, the browser address bar shows the URL `https://10.200.105.107/`. The dashboard header includes the Ixia logo, 'Developer', and 'DASHBOARD'. A settings gear icon is visible in the top right corner.

The main section is titled 'FEATURE ROADMAP' and includes the text 'Version 1.0.0.1505 currently installed'. A horizontal timeline shows feature milestones from 2015-05-11 to 2015-09-18, with a final 'IN DEVELOPMENT' phase. Below the timeline are feature cards: 'DEBUGGER - APPS Breakpoints / Single Step', 'CLI Command Line Interface', 'SECURITY Run Exploits with Apps', 'PCAP REPLAY As-Is Packet by Packet', 'DEBUGGER - PCAP Breakpoints / Single Step', and 'PCAP REPLAY Modify PCAP / Replay L4'. A 'VOTE FOR THE NEXT FEATURE!' button is also present.

Below the roadmap are three columns: 'ENJOY' with a video link, 'TELL US' with thumbs up/down icons, and 'SHARE' with a 'Refer a friend' link. At the bottom, a 'SESSIONS' section shows '1 ACTIVE/1 RUNNING' and a session card for 'FTP-investigation' (SESSION ID: 1) that is 'RUNNING' and 'ACTIVE FOR: 01d 00h 44m 12s'.

The footer contains the text '© 2016 IXIA AND/OR ITS AFFILIATES. ALL', a user profile 'admin', session statistics 'SESSIONS: 1 | ACTIVE: 1 | ABNORMALLY STOPPED: 0', and a 'NOTIFICATIONS 0' badge.

# ПРОСТО!

The screenshot displays the Ixia Developer interface for an FTP-INVESIGATION test. The interface is divided into several sections:

- Header:** Includes the Ixia logo, "Developer > FTP-INVESIGATION", and navigation tabs for "EDITOR", "DEBUGGER", and "STATISTICS".
- Traffic Configuration:**
  - TRAFFIC 1 (CISCO EMIX (11 APPS)):** A green panel showing a pie chart with categories: Raw (17%), HTTP Video (17%), Citrix (15%), and All Other (51%). Below it is a "TIMELINE and CONSTRAINTS" graph showing a ramp up from 0:00:00 to 0:02:00, a steady state from 0:02:00 to 0:01:00, and a ramp down. Parameters include 10 sessions, 10000 sessions/s, and 10000 Mb/s.
  - SECURITY TRAFFIC 2 (CLIENTSIDE STRIKES):** An orange panel showing a pie chart for "Exploits" with categories: Exploits: Browser (853), Exploits: Office Document (425), Exploits: Clientside (416), and All Other (904). Below it, "NUMBER OF STRIKES" is 2598.
- Network Topology:** A central "NETWORK" section showing a "ClientEntity" (192.168.2.10) connected to a server icon, which is connected to a "ServerEntity" (192.168.3.10).
- Interface Stats:** A table showing traffic for eth1 and eth2.

Interface	Tx Frames	Rx Frames
eth1	12,329	7,919
eth2	8,325	11,441
- Application Throughput:** A line graph showing throughput in Mbps. The legend indicates Tx (1.357) and Rx (1.361) Mbps.
- Application Transactions:** A pie chart showing transaction status: Successful (3 k), Failed (0), and Incomplete (1).
- Strikes:** A pie chart showing strike status: Blocked (43) and Allowed (234).

At the bottom, the status bar shows "admin SESSION 1 - Test is Stopping" and "NOTIFICATIONS 0".

# ОТЛАДЧИК И BREAKPOINTS

The screenshot displays the Ixia Developer FTP-DEBUGGER interface. The browser address bar shows `https://10.200.105.107/`. The page title is "Nightfury Project Scope - ...". The interface includes a navigation bar with "EDITOR", "DEBUGGER" (active), and "STATISTICS" tabs. A "STOP TEST" button and a progress indicator (00:02:14 - 73%) are visible.

**TRAFFIC**

**TRAFFIC1**

- CISCO EMIX
- Citrix
- eDonkey Data Transfer
- FTP**
- HTTP Video
- HTTP Audio
- HTTP Text
- SIP/RTP Direct Voice Call (TCP Tran...
- SAP
- SMTP Email
- Telnet
- Raw

**NETWORK**

ClientEntity: 192.168.2.10 (10)

ServerEntity: 192.168.3.10 (10)

**TRAFFIC1 >> FTP**

CONTINUE SINGLE STEP

COMMAND	ACTION	FLOW	CLIENT	DNS SERVER	FTP SERVER
1	Resolve	DNS	→		
2	Welcome Banner	FTP	←		
3	Login	FTP	→		
4	Directory Listing	FTP	→		
5	CWD	FTP	→		
6	Download	FTP	→		
7	Upload	FTP	→		
8	QUIT	FTP	→		

**BREAKPOINTS** STEP DISPLAY

ID	TRAFFIC ITEM	ACTIO	SUPERFLOW
3	traffic1	Login	FTP

**INTERFACE STATS**

Interface	Tx Frames	Rx Frames
eth1	14,689	10,195
eth2	10,196	14,682

**APPLICATION THROUGHPUT (Mbps)**

Tx (0) Rx (0)

**APPLICATION TRANSACTIONS**

- Successful (4 k)
- Failed (2)
- Incomplete (0)

admin SESSION 1 - Test is Running NOTIFICATIONS 0



# ИНТУИТИВНЫЙ CLI

```
10.200.105.107 - PuTTY
(1/ApplicationTraffic1/FTP)# show actions
  id name          flow  from      to
-----
  1 Resolve        DNS   Client    DNS Server
  2 Welcome Banner FTP   FTP Server Client
  3 Login          FTP   Client    FTP Server
  4 Directory Listing FTP   Client    FTP Server
  5 CWD            FTP   Client    FTP Server
  6 Download       FTP   Client    FTP Server
  7 Upload         FTP   Client    FTP Server
  8 QUIT           FTP   Client    FTP Server

(1/ApplicationTraffic1/FTP)# set breakpoint 3
(1/ApplicationTraffic1/FTP)# debug

(1/ApplicationTraffic1/FTP) ||
A breakpoint was hit! To debug the paused appsim instance you can go to the scope '@/session:1/ApplicationTraffic1/FTP/instance:1'.
(1/ApplicationTraffic1/FTP) || @instance:1
(1/ApplicationTraffic1/FTP/instance:1) || show

  id      : 1
  state   : paused
  actionid : 3
  actionName : Login
  frozenBy : breakpoint
  source  : 192.168.3.105:8732
  destination: 192.168.2.104:21

(1/ApplicationTraffic1/FTP/instance:1) || next
  id name          flow  from      to
-----
  2 Welcome Banner FTP   FTP Server Client
  * 3 Login          FTP   Client    FTP Server
  > 4 Directory Listing FTP   Client    FTP Server
  5 CWD            FTP   Client    FTP Server
  6 Download       FTP   Client    FTP Server

(1/ApplicationTraffic1/FTP/instance:1) ||
```

# ATI Research Center

Security and  
DPI Testing



BreakingPoint



Perfect Storm

Network Assessment



IxLoad



Ixia  
Developer

Application  
Visibility



Application & Threat  
Intelligence  
Processors

Inline Security



ThreatARMOR™

# И ЭТО ТОЛЬКО НАЧАЛО ...

Ежемесячные обновления

- Условные breakpoints
- Отладчик
- Произвольные статистики
- ...



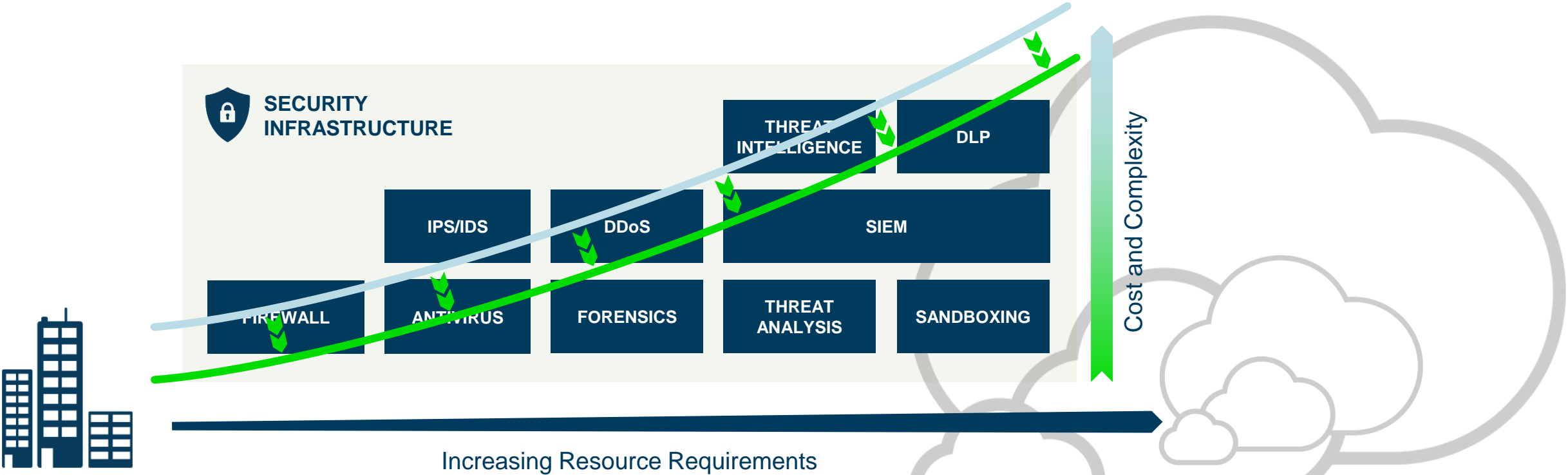
# IXIA TREATARMOR



**Дополнительный уровень защиты  
корпоративных сетей**



# Инвестиции в безопасность постоянно растут



**SECURITY INNOVATION TRACKS THREAT INNOVATION**  
**BUT WHAT IF YOU COULD SHRINK THE INTERNET?**  
 More protection. More complexity. More maintenance. More to manage.

FEWER  
ATTACKERS

FEWER SIEM  
ALERTS

SMALLER ATTACK  
SURFACE

SECURITY INFRASTRUCTURE  
can focus on what's important

# Из чего состоит трафик интернета

**В КАЖДОЙ СЕТИ ЕСТЬ  
ДВА ТИПА ТРАФИКА**

**ПОДЛЕЖАЩИЙ  
АНАЛИЗУ:**

Traffic of Possible Interest

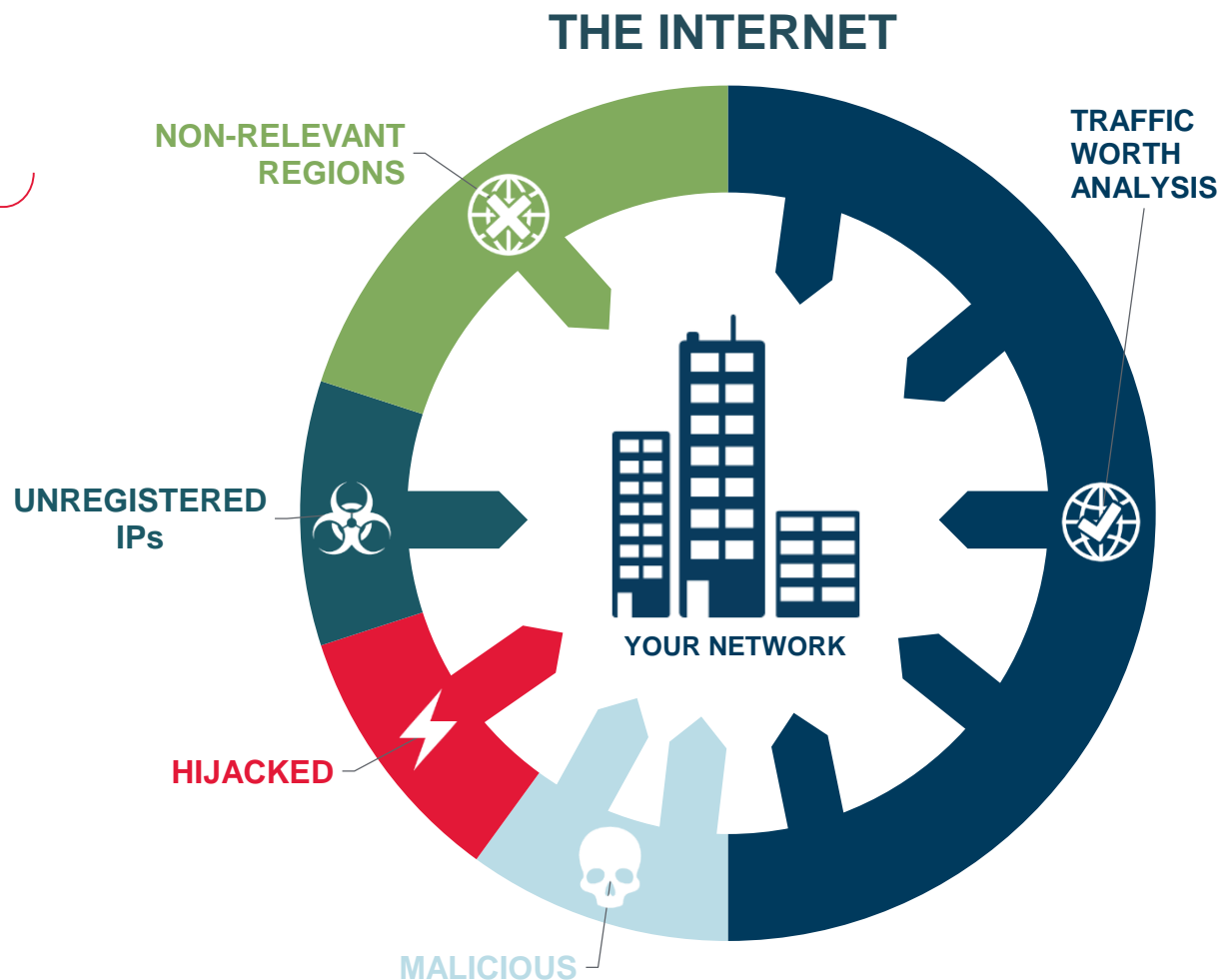
**ТРАФИК, КОТОРЫЙ НЕ  
НУЖНО АНАЛИЗИРОВАТЬ:**

KNOWN MALICIOUS

**HIJACKED**

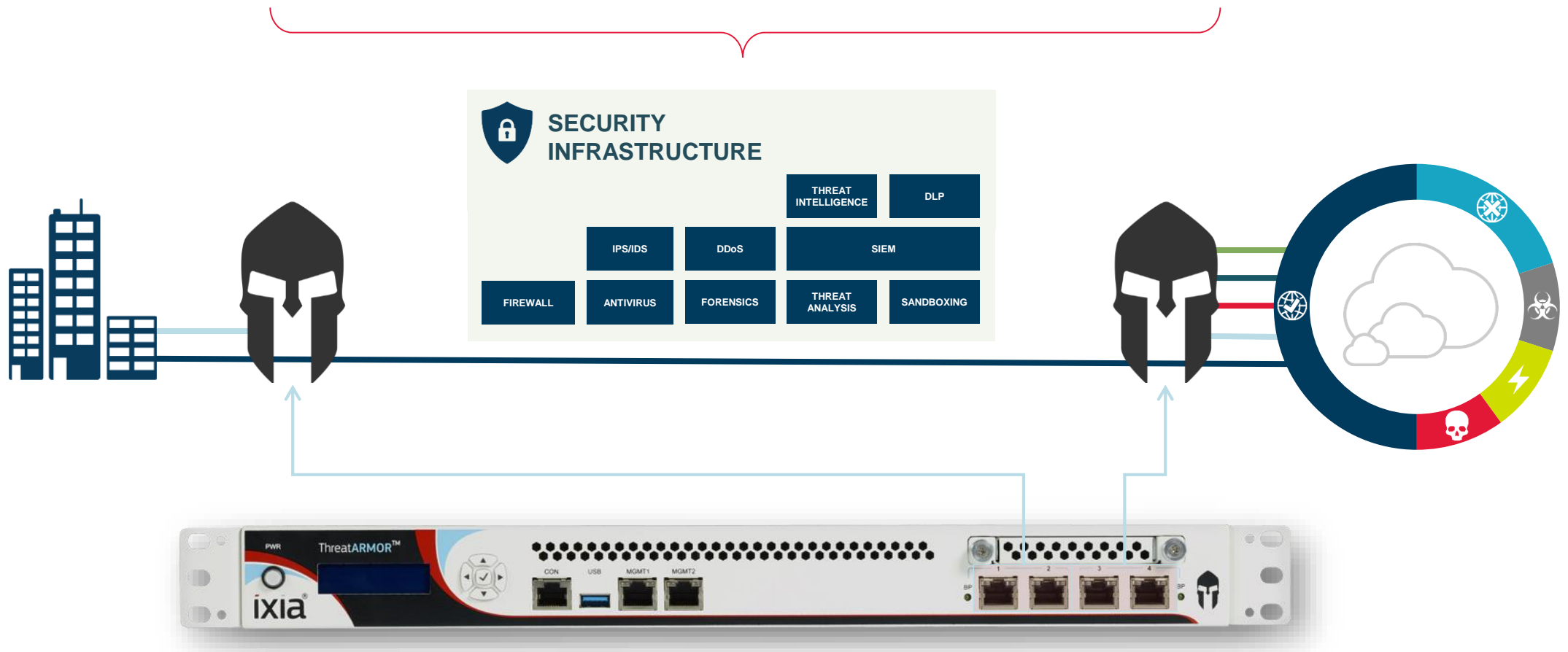
UNREGISTERED IPs

UNWANTED REGIONS



# Представляем ThreatARMOR™ от Ixia

ThreatARMOR – новый передовой рубеж защиты.  
Блокирует нежелательный трафик - входящий и исходящий.



# Разве мой Firewall этого не делает?

Next-gen firewalls are **really good** at DPI, **content inspection**, and **threat detection**, but they're **really bad** at **large-scale IP address blocking**.

---

## Why would you want to **block a lot of IPs**?

18% of DDoS attacks come from China

Russia, Ukraine, Pakistan, China, and Turkey are in the top 10 Botnet C&C countries

China, Brazil, Russia and India together account for 26% of web application attacks

---

## THE PROBLEM WITH MASSIVE-SCALE BLOCKING

COUNTRY	IP RANGES
Russia	5,632
China	2,659
Pakistan	231
Turkey	644
Ukraine	2,528

CATEGORY	# OF IP ADDRESSES
Malicious Sites	> 1,000,000
Hijacked IP's	> 16,000,000
BOGONs	> 800,000,000

**MOST NGFWs RUN OUT OF CAPACITY AT AROUND 10,000 RULES.**



# ThreatARMOR Brings Threat Intelligence to Your Network

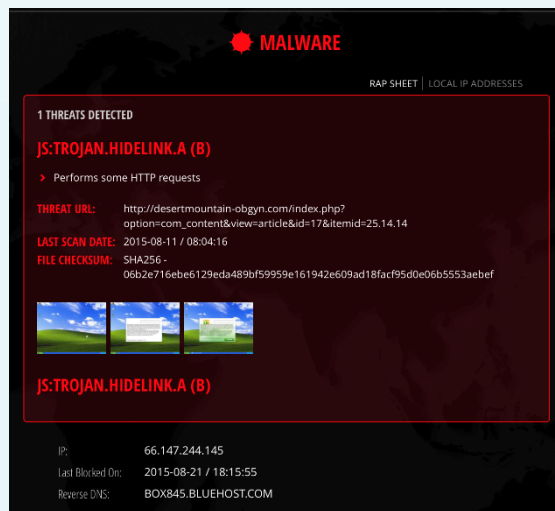
## IXIA ATI Research Center

Professional-grade Threat Intelligence  
used by industry leaders



## ThreatARMOR Rap Sheets

Clear proof for every  
blocked site.



## ThreatARMOR Appliance

Set, Select and Forget.  
Auto-updates every 5 min.  
Maximum reliability.



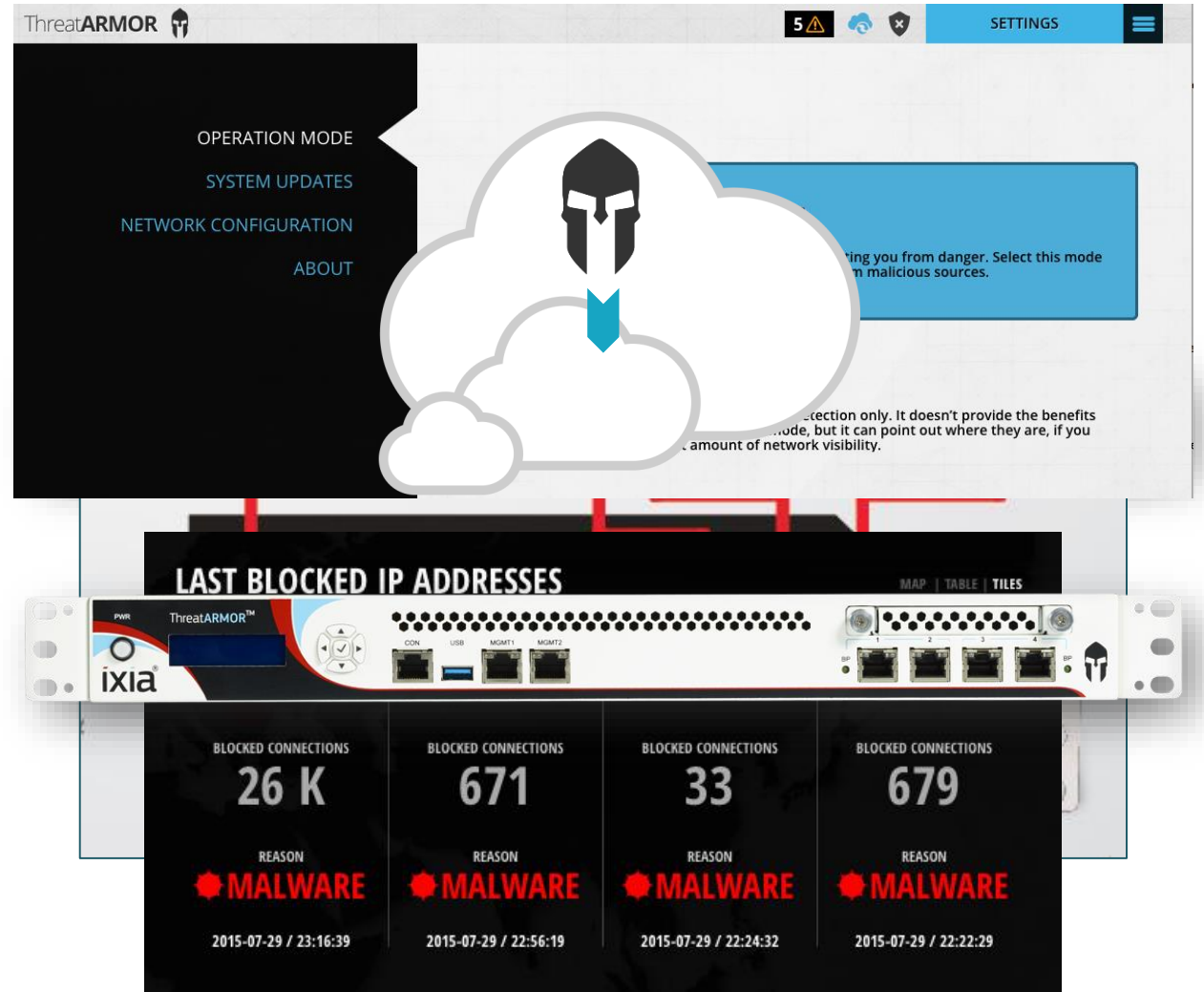
# ThreatARMOR Easy Setup

## EASY TO CONFIGURE

1. Connect power and Ethernet cables
2. Pick “**Report Only**” or “**Blocking Mode**”
3. Walk away, it updates automatically

Criminal site blocking is **automatic**

Geo-blocking is optional



# ThreatARMOR Dashboard



ThreatARMOR



DASHBOARD



LAST 24 HOURS ▾

0.12% THREATARMOR EFFICIENCY  
0% FIREWALL EFFICIENCY

35<sub>K</sub>

BLOCKED CONNECTIONS

28.1<sub>M</sub>

TOTAL CONNECTIONS

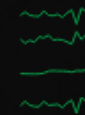
1,001.7<sub>MB</sub>

BLOCKED TRAFFIC

2.8<sub>TB</sub>

ALLOWED TRAFFIC

344.39 M BITS/SEC  
478 CONNECTIONS/SEC  
3.94 K ACTIVE CONNECTIONS  
9.04% LINK UTILIZATION



## TOP BLOCKED COUNTRIES

1. UNITED STATES
2. ROMANIA
3. GERMANY
4. NETHERLANDS
5. UNITED KINGDOM
6. FRANCE
7. POLAND
8. CHINA



## LAST BLOCKED IP ADDRESSES

128.140.230.207

ROMANIA

BLOCKED CONNECTIONS

12

REASON

MALWARE

2015-09-25 06:48:43

188.213.205.90

ROMANIA

BLOCKED CONNECTIONS

1

REASON

MALWARE

2015-09-25 06:48:41

173.194.44.12

UNITED STATES

BLOCKED CONNECTIONS

17

REASON

MALWARE

2015-09-25 06:48:40

173.194.44.11

UNITED STATES

BLOCKED CONNECTIONS

12

REASON

MALWARE

2015-09-25 06:48:40

## TOP ALLOWED COUNTRIES

ROMANIA TOTAL TRAFFIC PERCENTAGE <b>48%</b> CONNECTIONS: 1.1 M	UNITED STATES TOTAL TRAFFIC PERCENTAGE <b>32%</b> CONNECTIONS: 17 M	UNKNOWN TOTAL TRAFFIC PERCENTAGE <b>12%</b> CONNECTIONS: 5.6 M	EUROPE TOTAL TRAFFIC PERCENTAGE <b>4%</b> CONNECTIONS: 1 M
IRELAND TOTAL TRAFFIC PERCENTAGE <b>1%</b> CONNECTIONS: 525.2 K	NETHERLANDS TOTAL TRAFFIC PERCENTAGE <b>1%</b> CONNECTIONS: 878 K	UNITED KINGDOM TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 474 K	SWEDEN TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 20.4 K

## BOTTOM COUNTRIES ALLOWED

PALAU TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 1	NICARAGUA TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2	GUINEA-BISSAU TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2	BURKINA FASO TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2
SAMOA TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2	MALI TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2	GRENADA TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2	BURUNDI TOTAL TRAFFIC PERCENTAGE <b>0%</b> CONNECTIONS: 2

# ПОЧЕМУ IXIA?

## Ведущие мировые корпорации и учреждения – 86 из Fortune

### Финансы



### Компьютеры и электроника



### Поставщики услуг



### Образование



### Здравоохранение



### Госорганы



## Производители



15 из Top 15 вендоров

## Телеком операторы



42 из Top 50 операторов

# СПАСИБО

Владимир Назаренко  
Директор по продажам  
Ixia Украина и СНГ  
+380 94 710 0942  
+380 98 178 7378  
[vnazarenko@ixiacom.com](mailto:vnazarenko@ixiacom.com)

Узнай больше на [www.ixiacom.com](http://www.ixiacom.com)