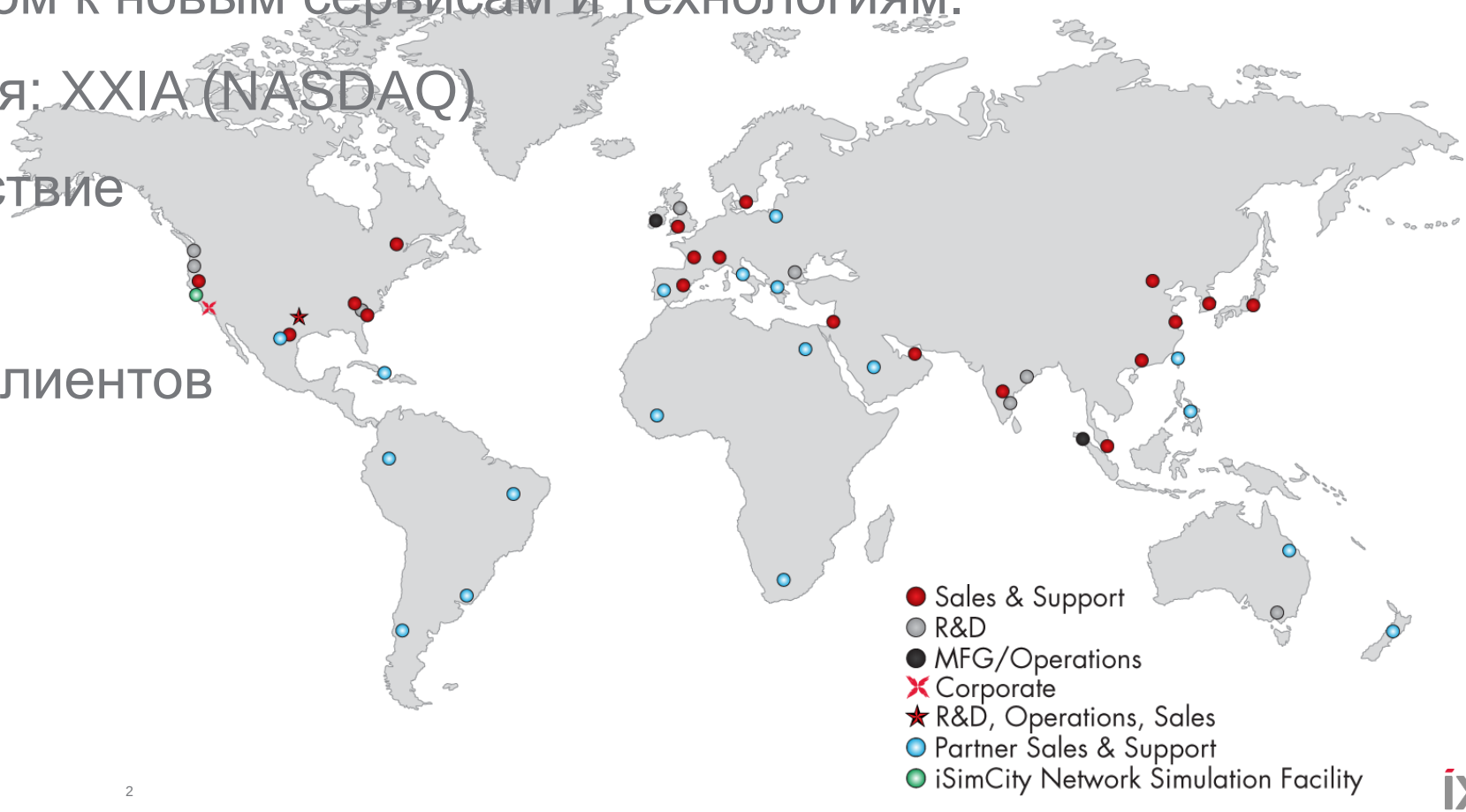
SECURITY SOLUTIONS

О КОМПАНИИ IXIA

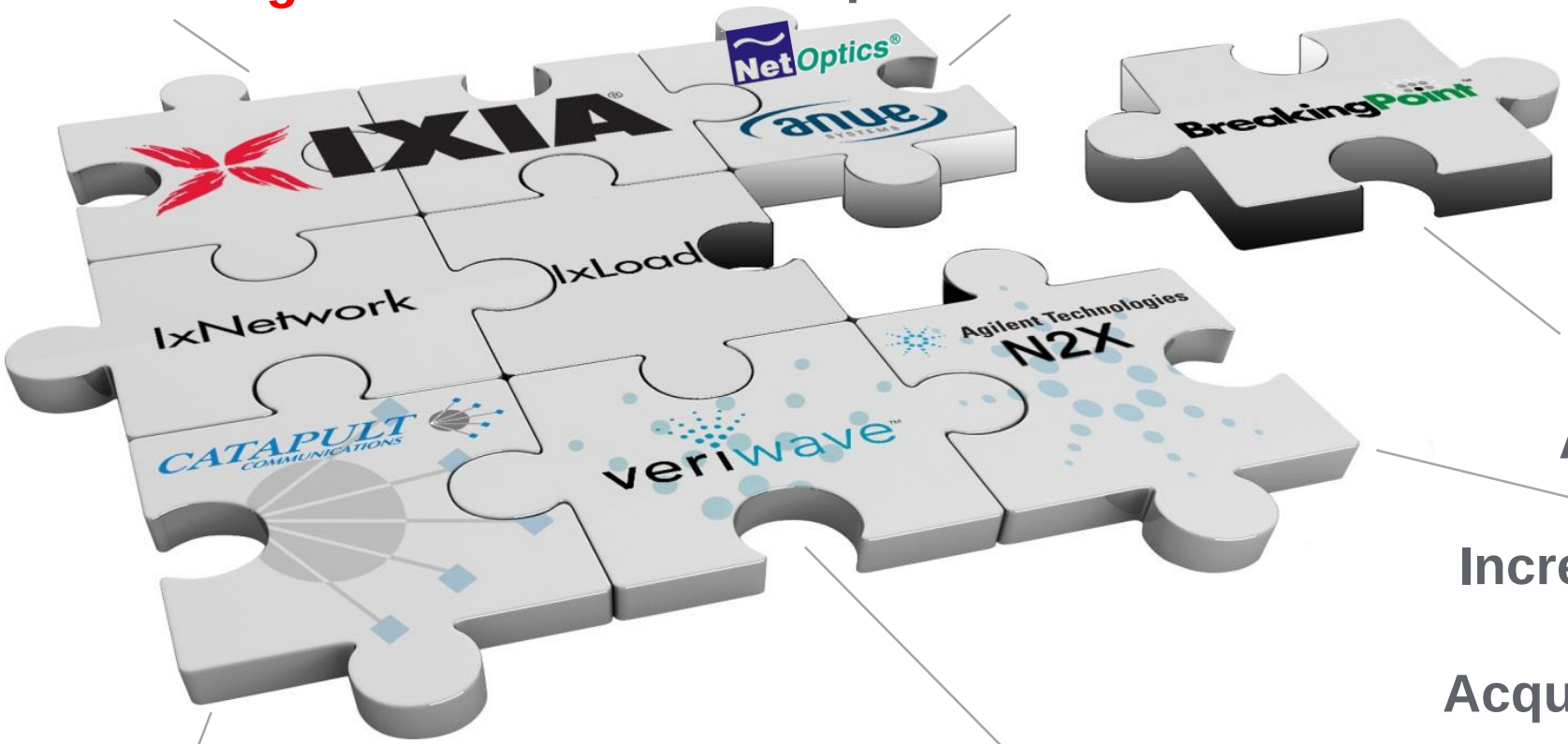
- Решения компании Ixia помогают вам уверенно развивать свой бизнес, обеспечивая ему надёжную и защищённую связь с внешним миром. Благодаря продуктам Ixia, ваши клиенты обеспечены самым быстрым и безопасным доступом к новым сервисам и технологиям.
- Публичная компания: XXIA (NASDAQ)
- Глобальное присутствие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



END-TO-END PRODUCT FAMILY

Founded in 1997
IP **Testing**

Network **Visibility**
Acquired June 2012



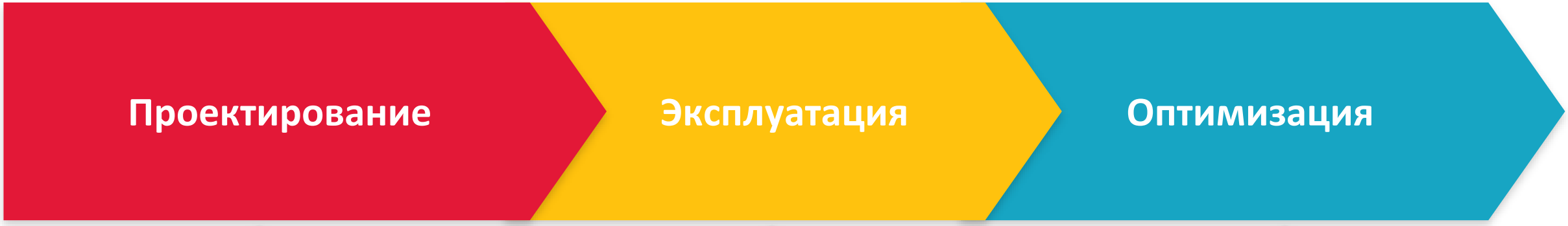
Actionable **Security**
Intelligence (ASI)
Acquired August 2012

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



Разработка проекта

Тестирование
Выбор вендора
Proof of Concept
Совместимость оборудования
Производительность
Новые технологии

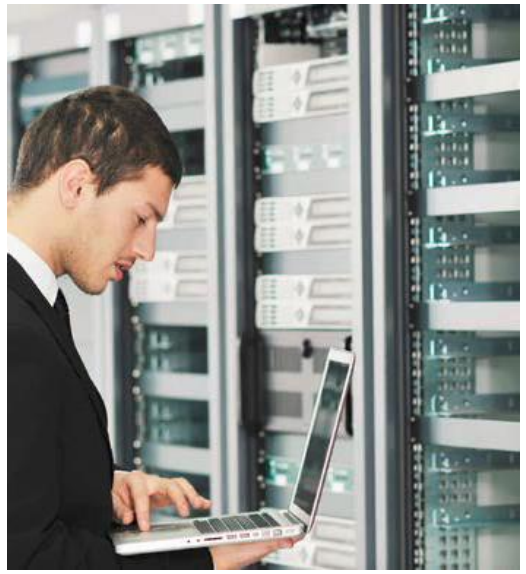
Уверенность

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

Оптимизация

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

IXIA BREAKINGPOINT



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

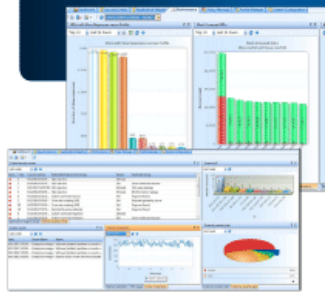
Trustwave WebDefend

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 many 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 systems 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
- Advanced Web application security detection and protection, including coverage of the OWASP Top 10 Web application attacks
- Facilitates compliance with PCI DSS requirements



Unparalleled protection against the loss of sensitive information

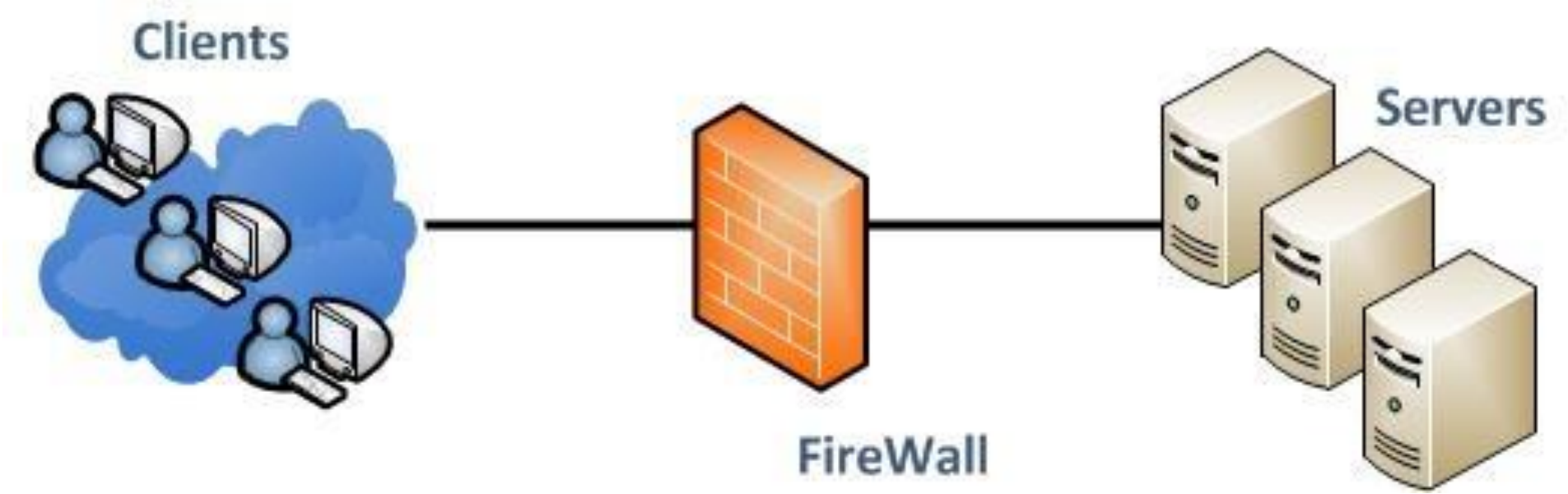
Only WebDefend uses a patent-pending profiling system and multiple, collaborative detection engines to ensure the flow of mission-critical traffic while supplying complete protection for applications to keep your confidential information safe from targeted attacks.

As of May 2013

Доверяю интегратору

ixia

МАРКЕТИНГОВЫЕ ПАРАМЕТРЫ ПРОИЗВОДИТЕЛЬНОСТИ

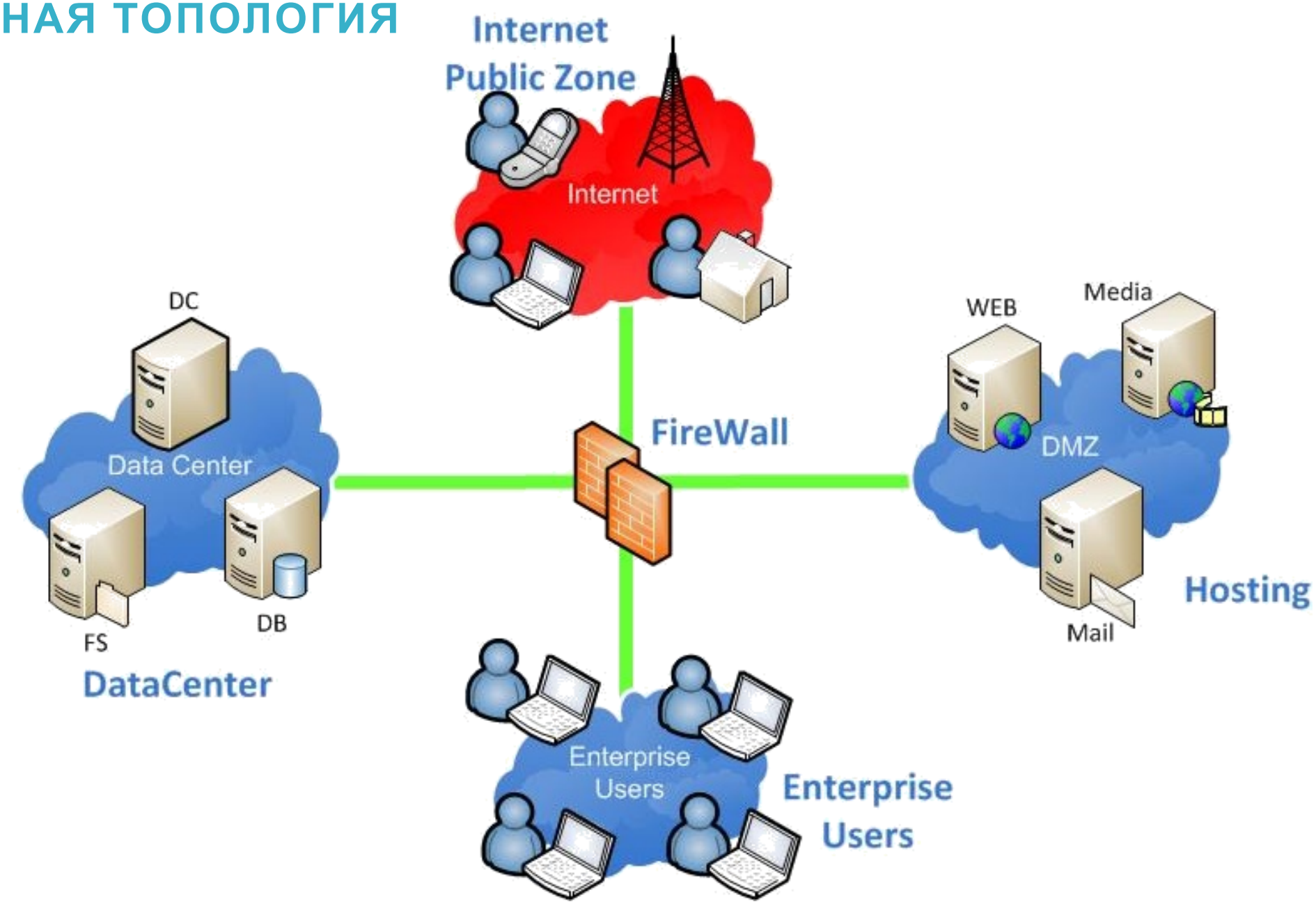


Основаны на базовой сетевой топологии

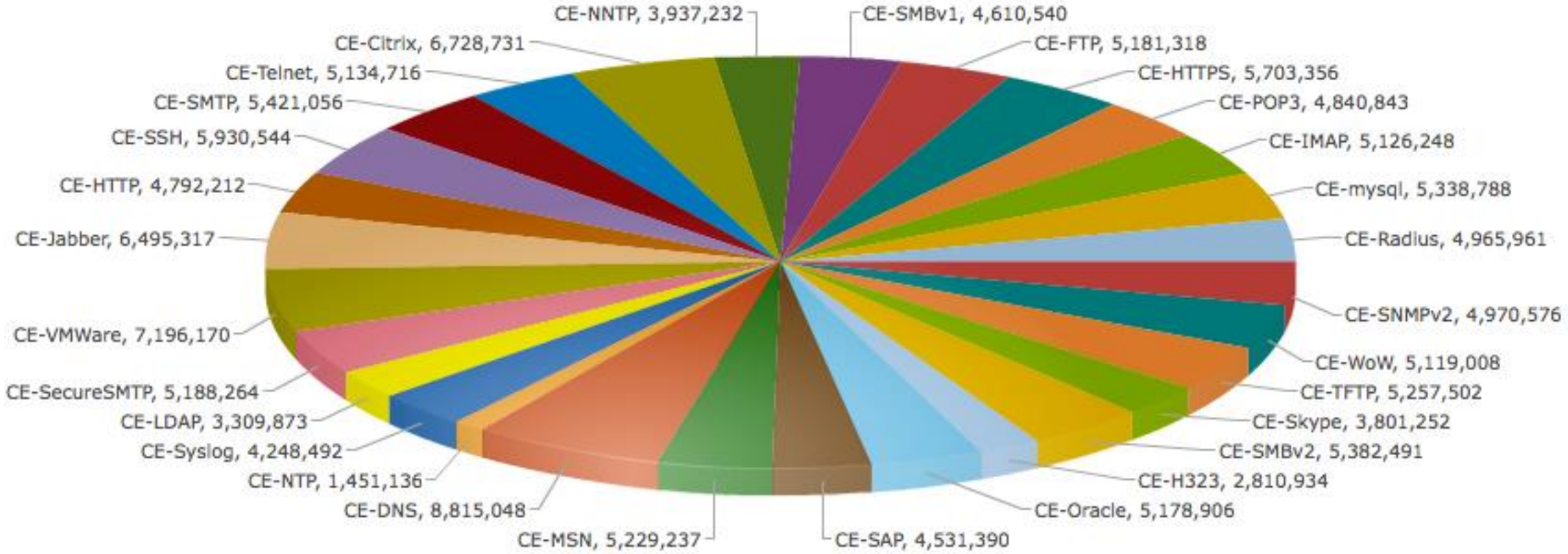
Трафик только HTTP over TCP

Упрощённые HTTP GET / HTTP Response

РЕАЛЬНАЯ ТОПОЛОГИЯ

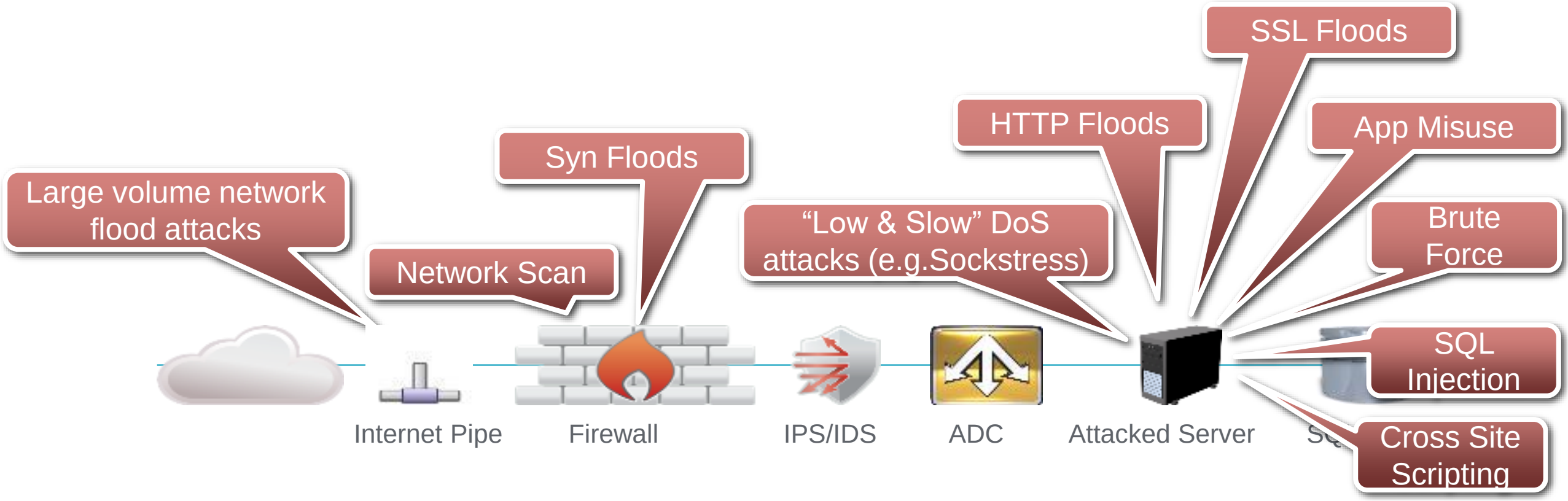


ТРАФИК РЕАЛЬНОЙ СЕТИ

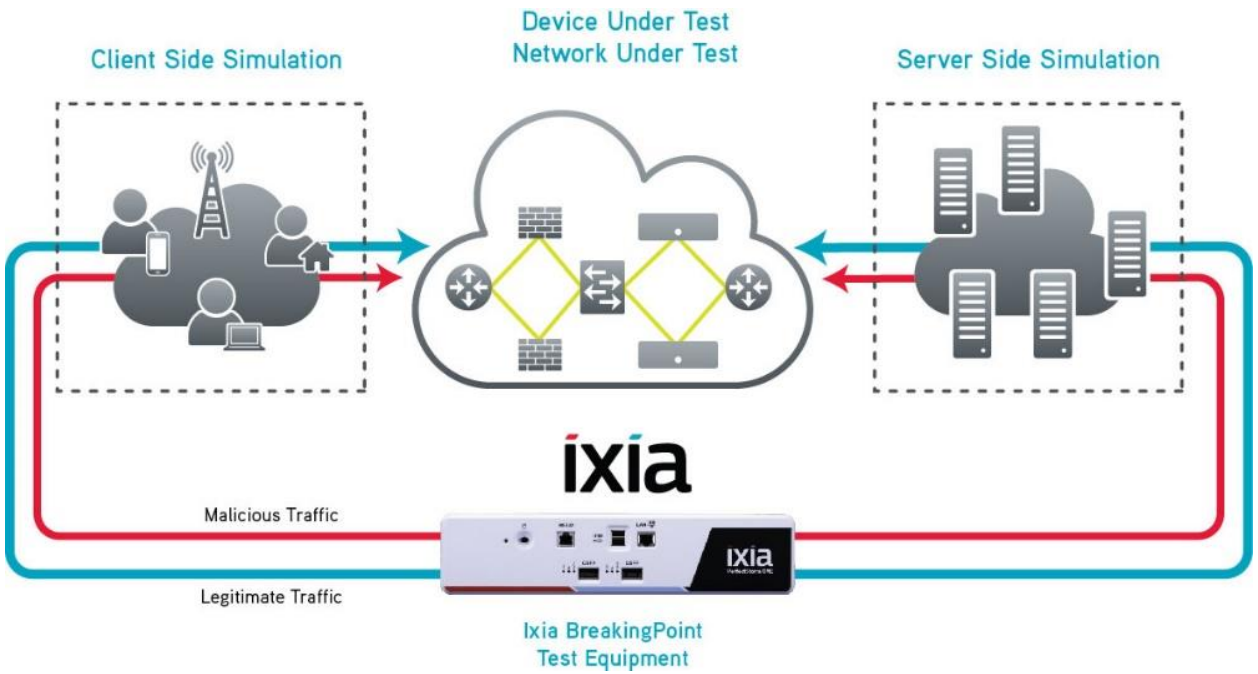


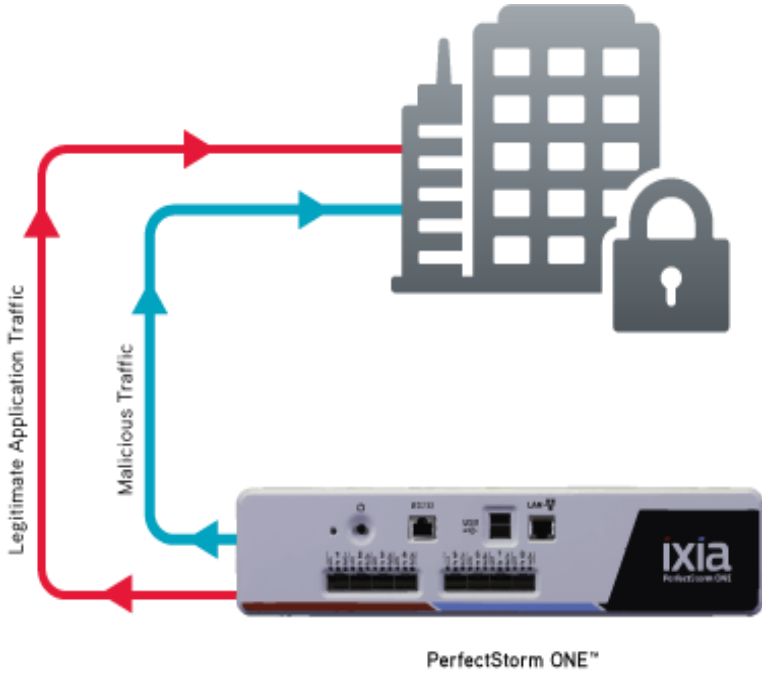
ixia

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

2-ports of 40GE with the QSFP+ interface

8-ports of 10GE with the SFP+ interface

PerfectStorm

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

PerfectStorm ONE

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

BreakingPoint VE

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

ixia

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
Winny
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

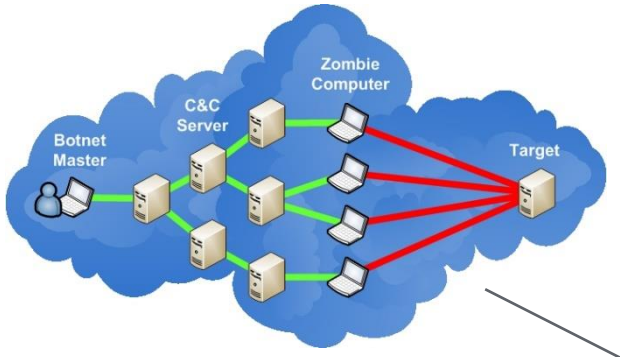
Enterprise Applications
DCE/RPC Endpoint Mapper
DCE/RPC Exchange Directory
LPD
MODBUS
SAP

Secure Data Transfer
HTTPS
SSH

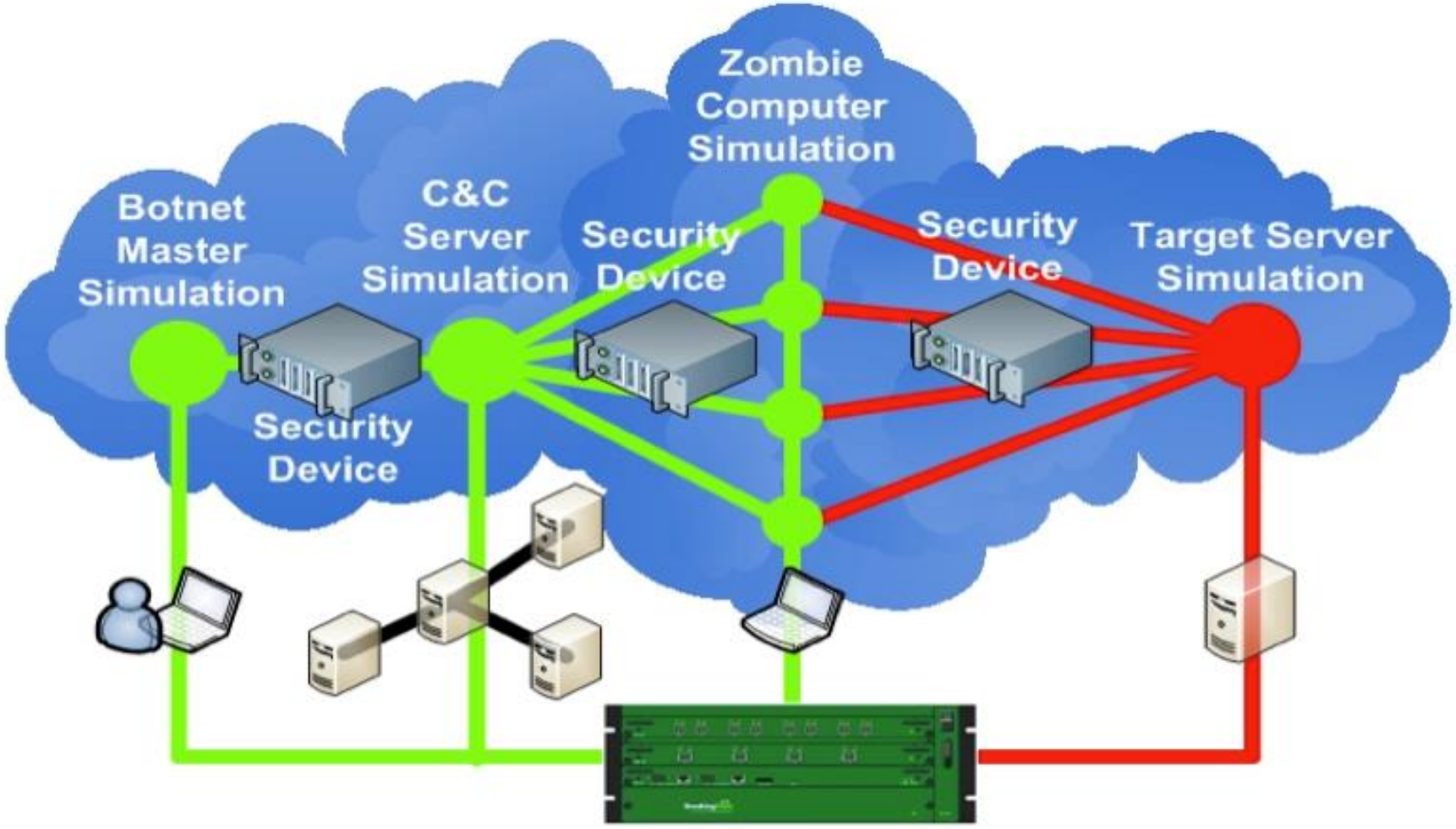
Email | Webmail
@mail.ru
AOL Webmail
Google Gmail
GMX Webmail
MSN Hotmail
Microsoft Exchange (MAPI Exchange)
IMAP
IMAPv4 Advanced
Orange WebMail
Outlook Web Access
POP3
Rediffmail WebMail
SMTP
Yahoo! Mail
Yahoo! Mail Classic

Financial
FIX
FIXT
ITCH
OUCH

IXIA BREAKINGPOINT BOTNET SIMULATION



Real Topology



- ✓ 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

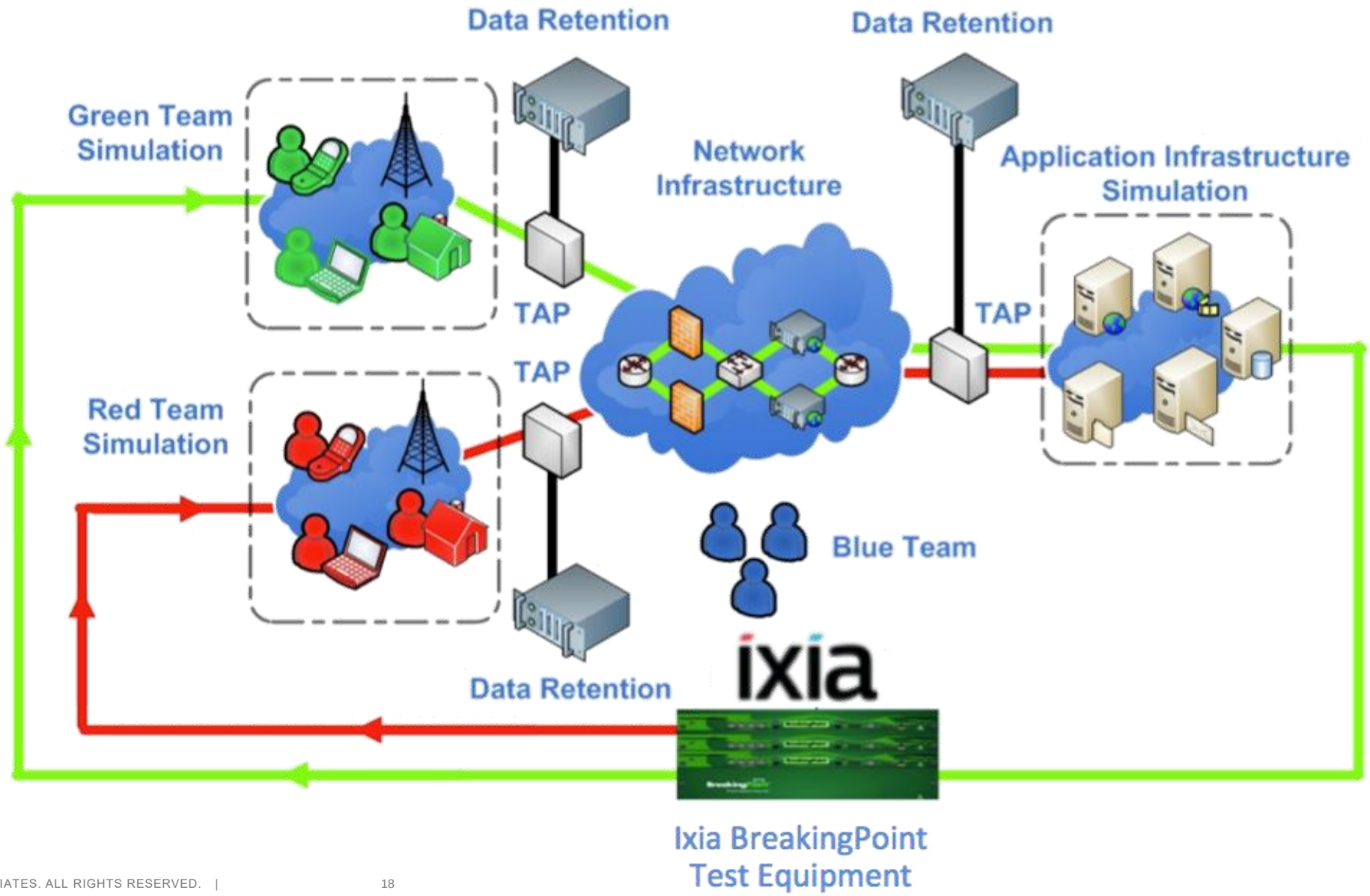
Layer 4 UDP
✓LOIC UDP53 DoS Attack
✓DDoS UDP Fragmentation
✓DDoS Non-Spoofed UDP Flood
✓DDoS UDP Flood

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

CYBER RANGE: В УЧЕНИЯХ КАК В БОЮ



ixia

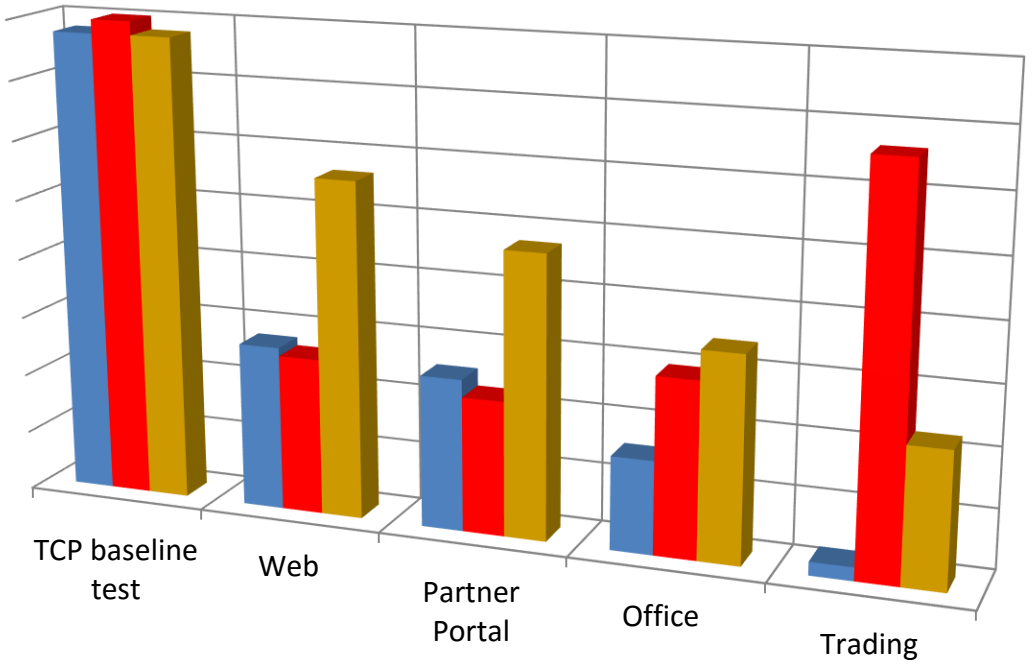
ОБОРУДОВАНИЕ, КОТОРОЕ МОЖЕТ БЫТЬ АТТЕСТОВАНО С ПОМОЩЬЮ BREAKINGPOINT

- 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

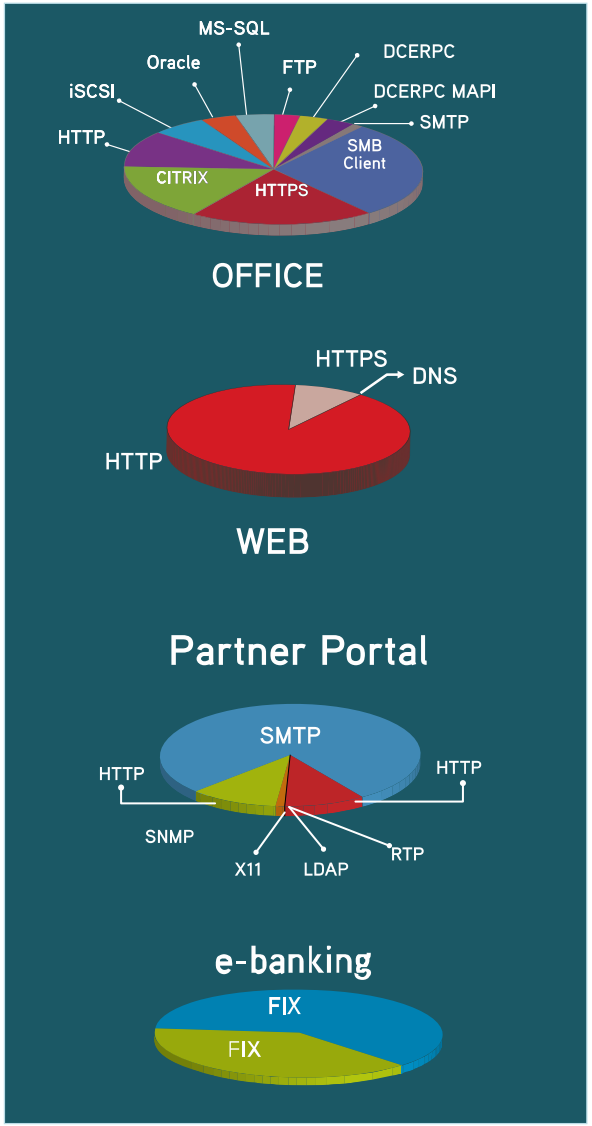
BreakingPoint™
Find it before they do.™

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
Avg Sec effectiveness *	48%	52%	28%



*BreakingPoint StrikePack 5

ixia

ГОДОВАЯ ПОДПИСКА APPLICATION & THREAT INTELLIGENCE (ATI)

Simulation and Testing

ixia

Application and Threat Intelligence

Раз в 2 недели | Новые приложения | Новые угрозы/Атаки

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

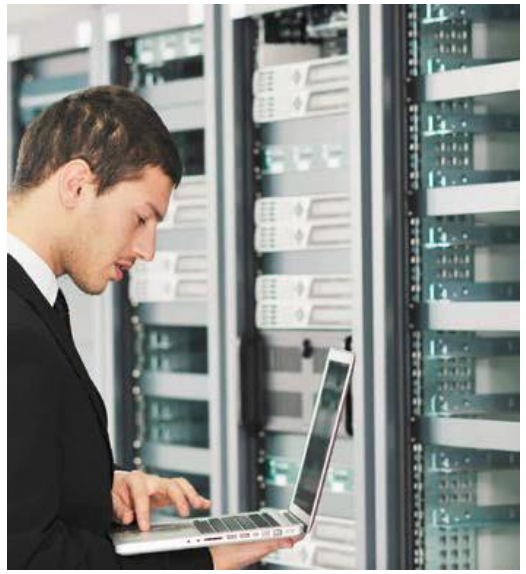
Real-World Applications

- 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

IXIA DEVELOPER



BreakingPoint

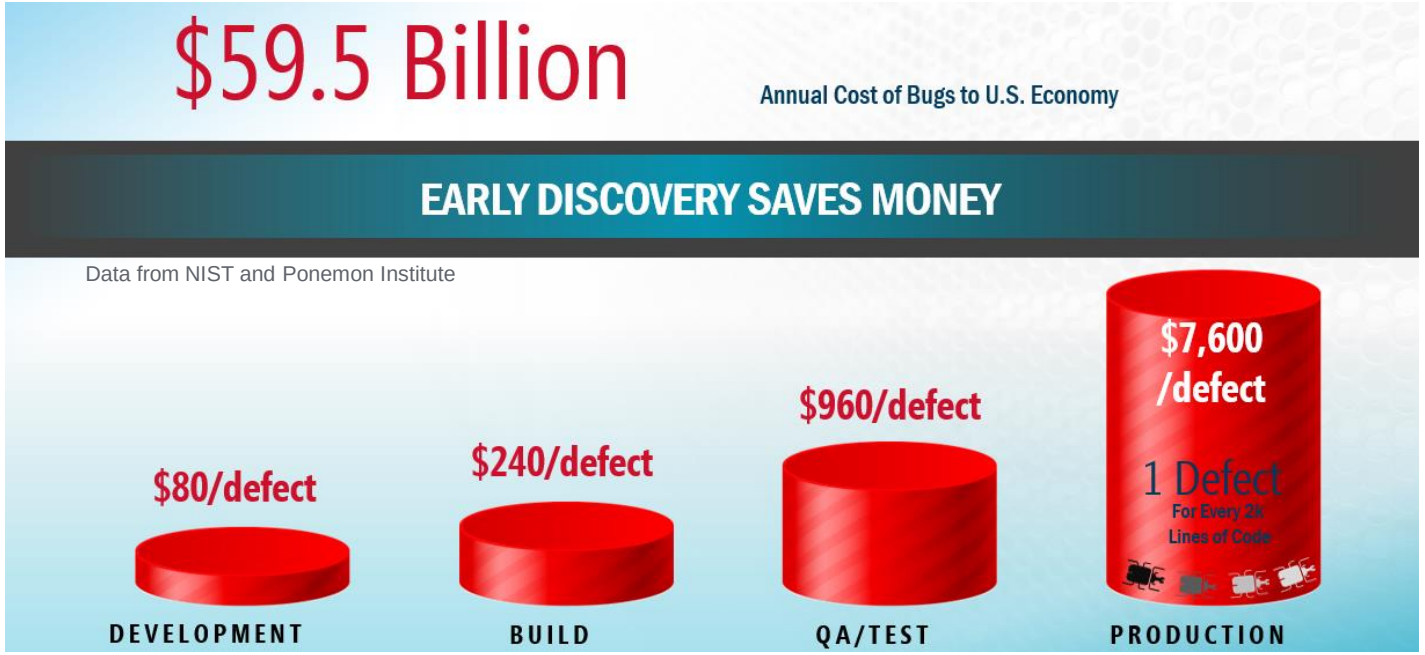
Personal edition

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



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 --intf1=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

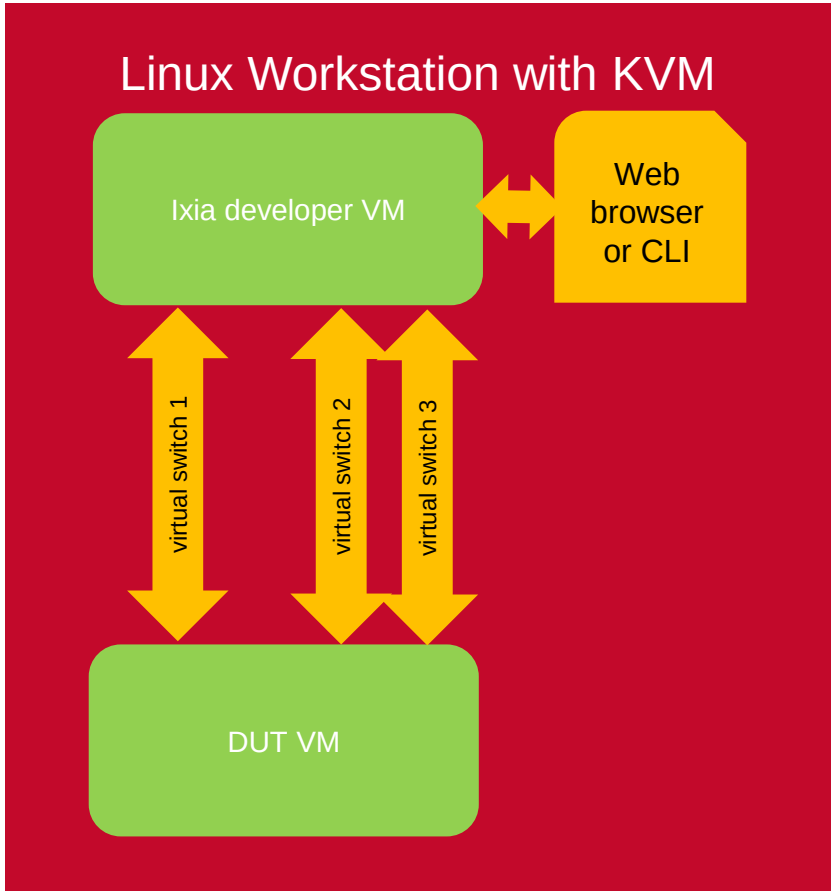
- Генерация реалистичного трафика приложений с подмешиванием атак
- Специальные функции для разработчиков: отладчик, breakpoints, захват
- Именная лицензия
- Быстрый цикл релизов
- Встроенный механизм обратной связи
- Классный HTML UI и классический CLI
- Расширяется плагинами

РАЗВОРАЧИВАНИЕ IXIA DEVELOPER

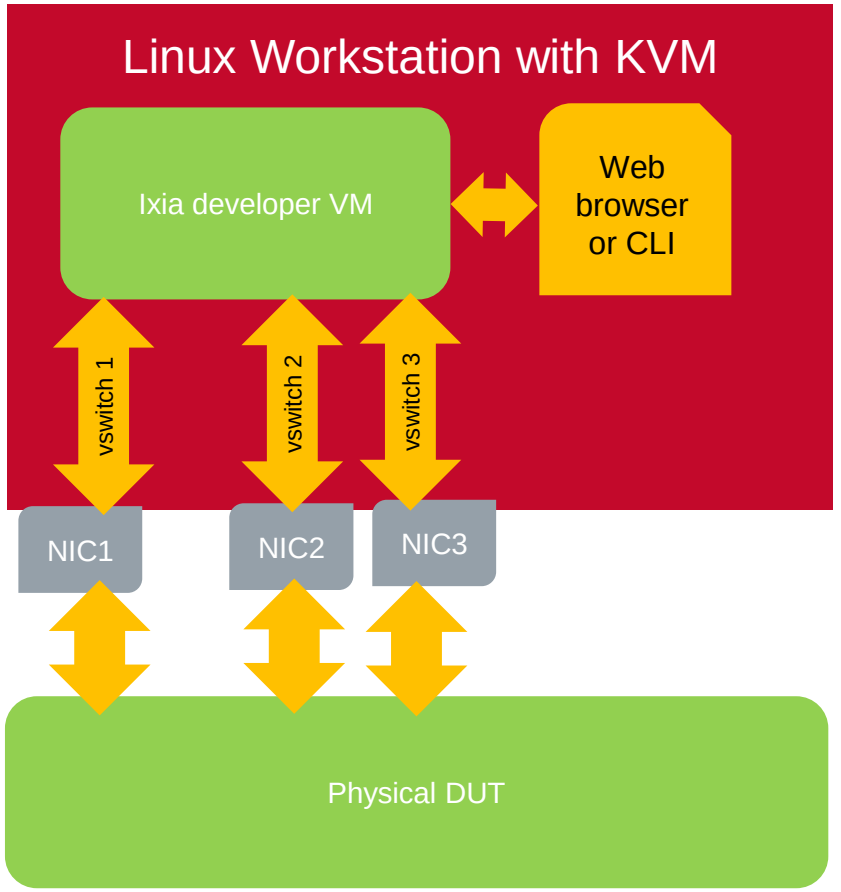
- Легкое виртуальное решение
  - одна VM (<1GB)
  - не надо разворачивать порты
  - вписывается в типовое окружение разработчика
- Быстро разворачивается
  - Менее 2 минут
- Online авторизация

VMWare ESX

СХЕМА ВЗАИМОДЕЙСТВИЯ

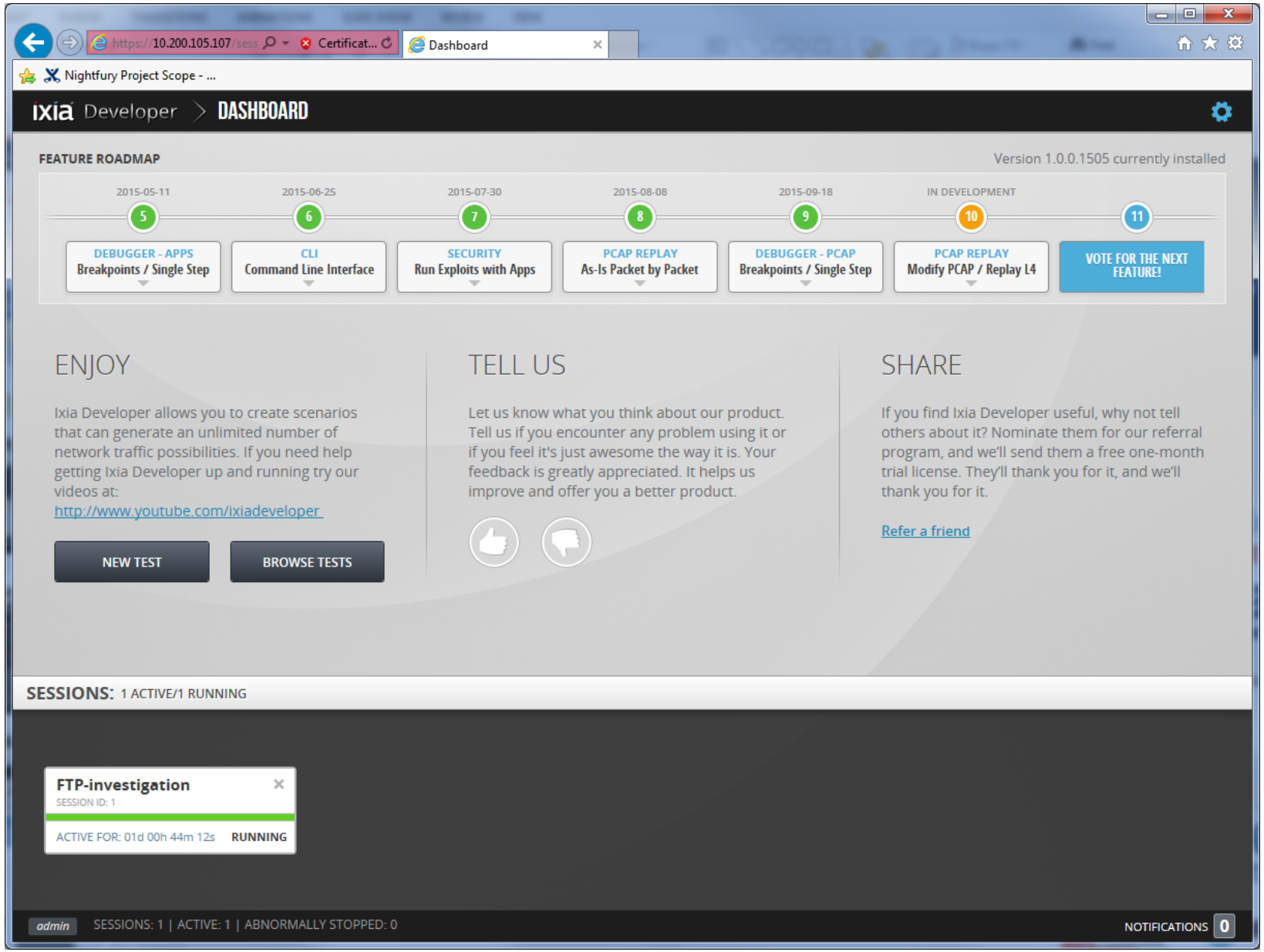


Тест внутри виртуальной среды



Тест физического устройства

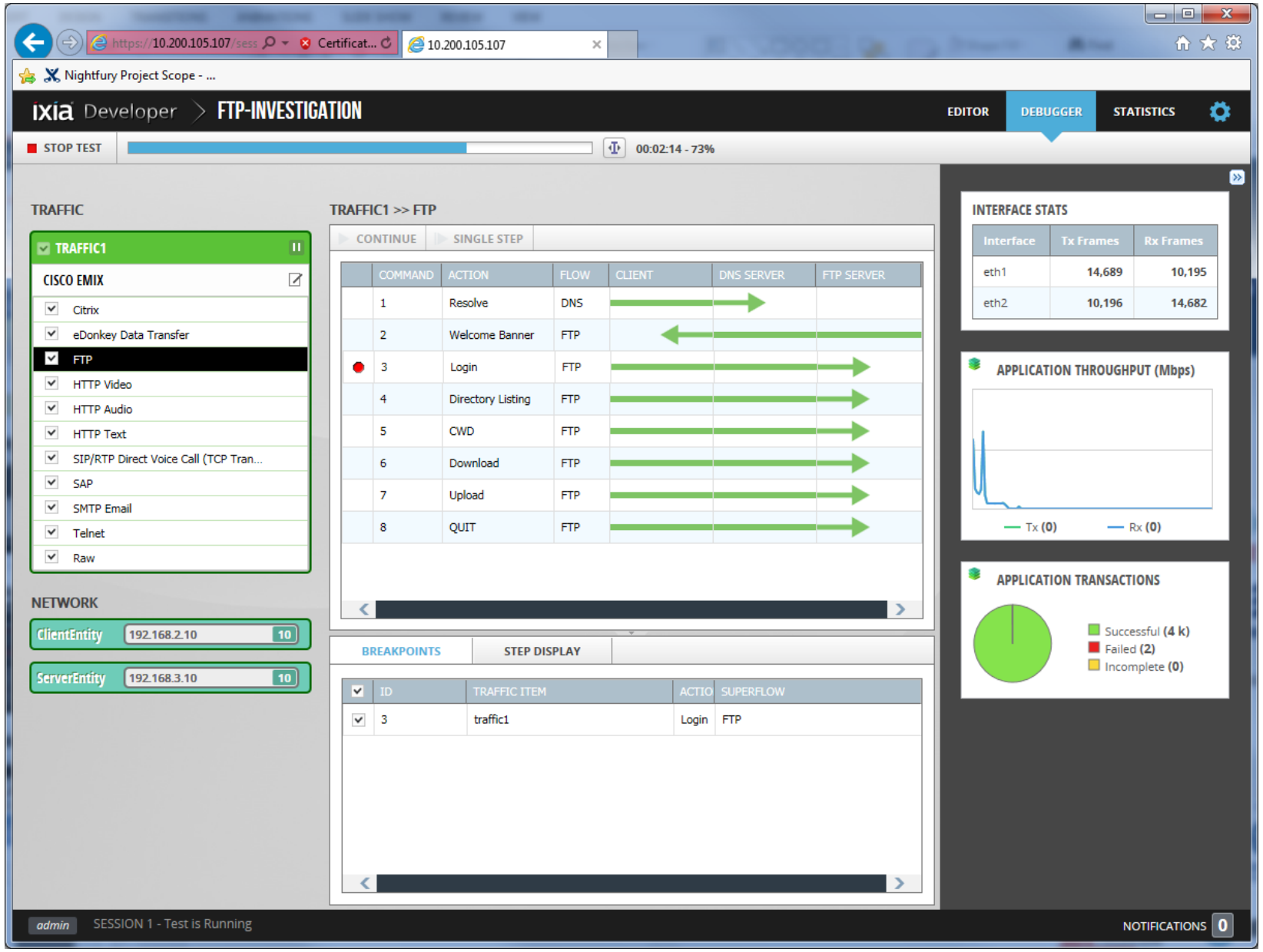
ВЗАИМОДЕЙСТВИЕ С СООБЩЕСТВОМ



ixia

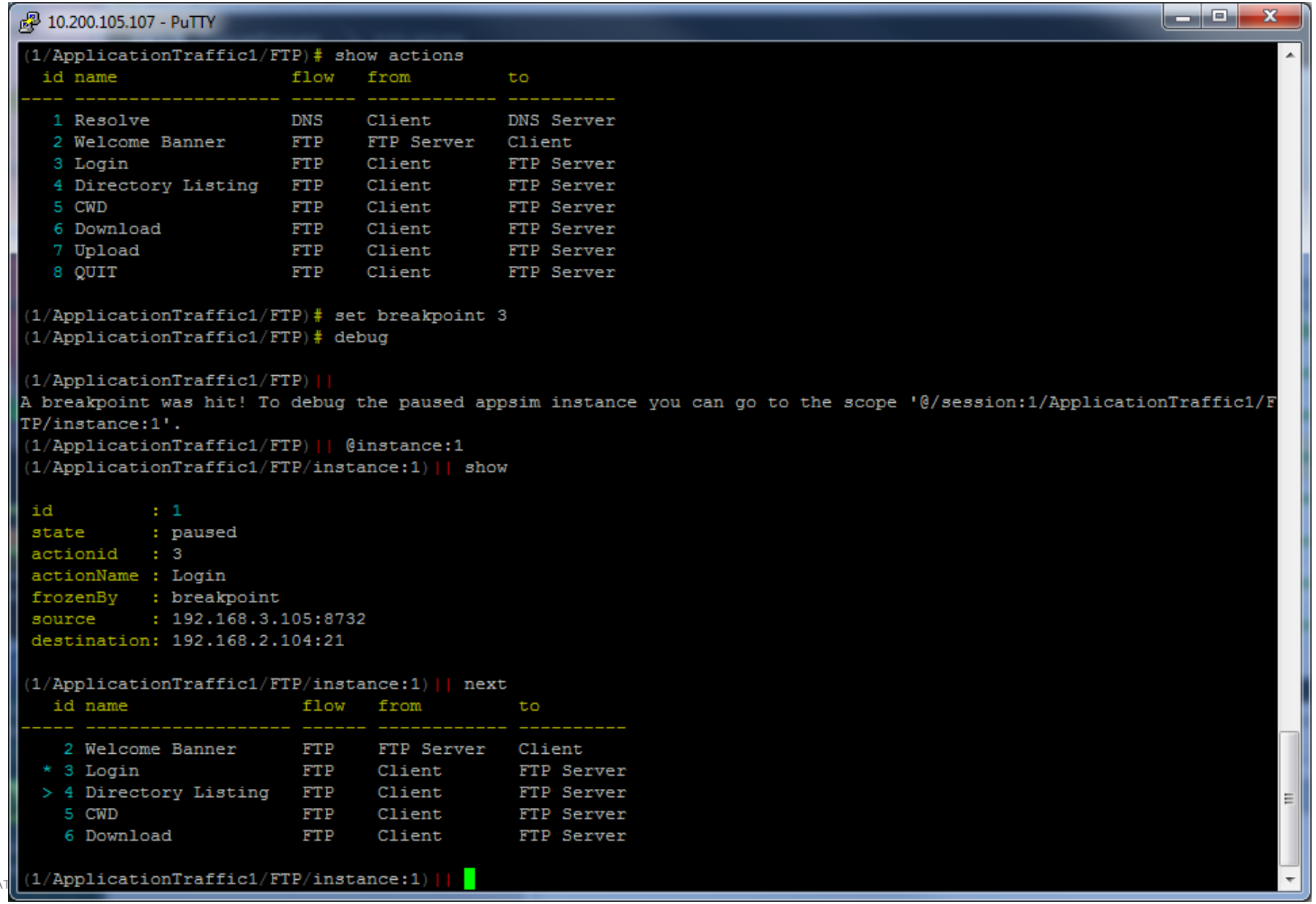
ПРОСТО!

ОТЛАДЧИК И BREAKPOINTS



ixia

ИНТУИТИВНЫЙ CLI



ixia

ЕДИНЫЙ ЦЕНТР ИССЛЕДОВАНИЙ

ATI Research Center

Security and DPI Testing

BreakingPoint

Perfect Storm

Network Assessment

IxLoad

Ixia Developer

Application Visibility

Application & Threat Intelligence Processors

Inline Security

ThreatARMOR™

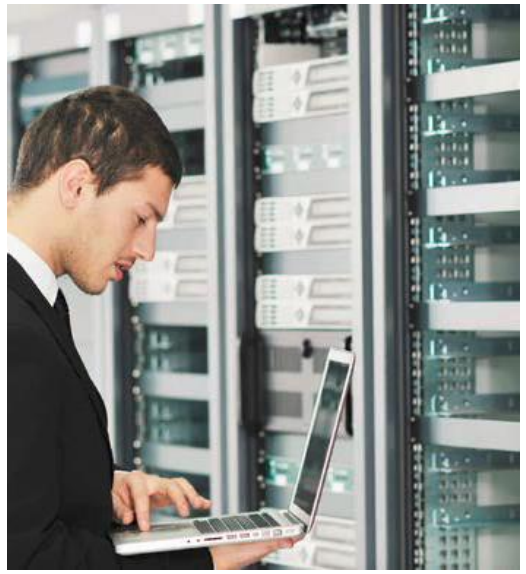
ixia

И ЭТО ТОЛЬКО НАЧАЛО ...

Ежемесячные обновления

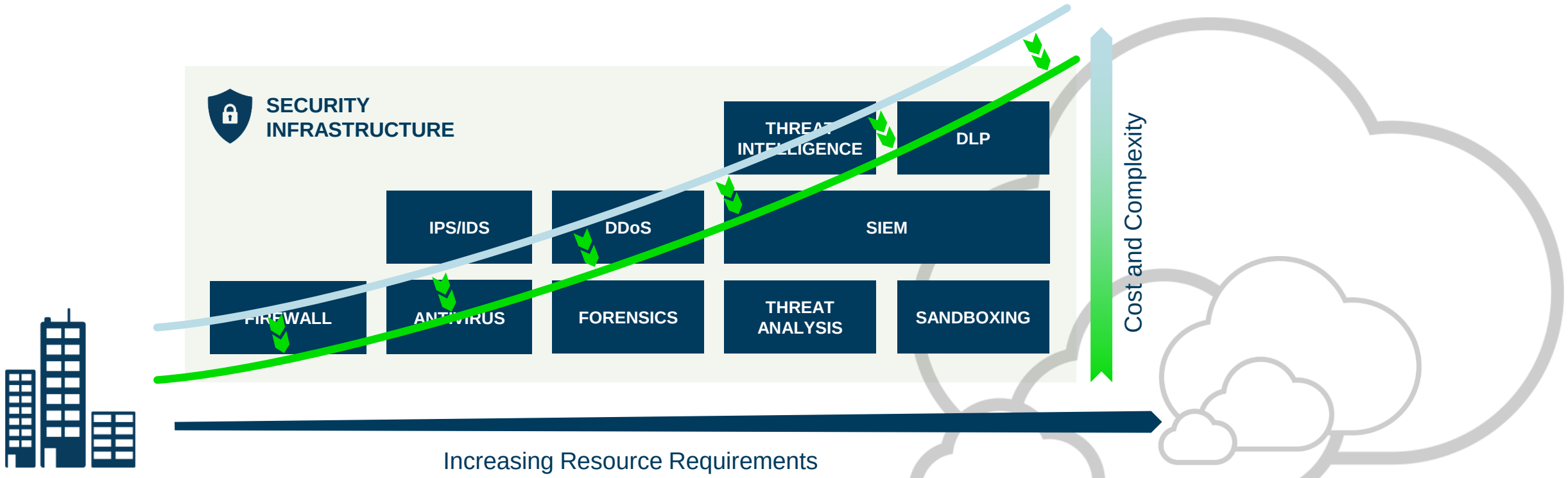
- Условные breakpoints
- Отладчик
- Произвольные статистики
- …

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

ixia

Из чего состоит трафик интернета

В КАЖДОЙ СЕТИ ЕСТЬ ДВА ТИПА ТРАФИКА

ПОДЛЕЖАЩИЙ АНАЛИЗУ:

Traffic of Possible Interest

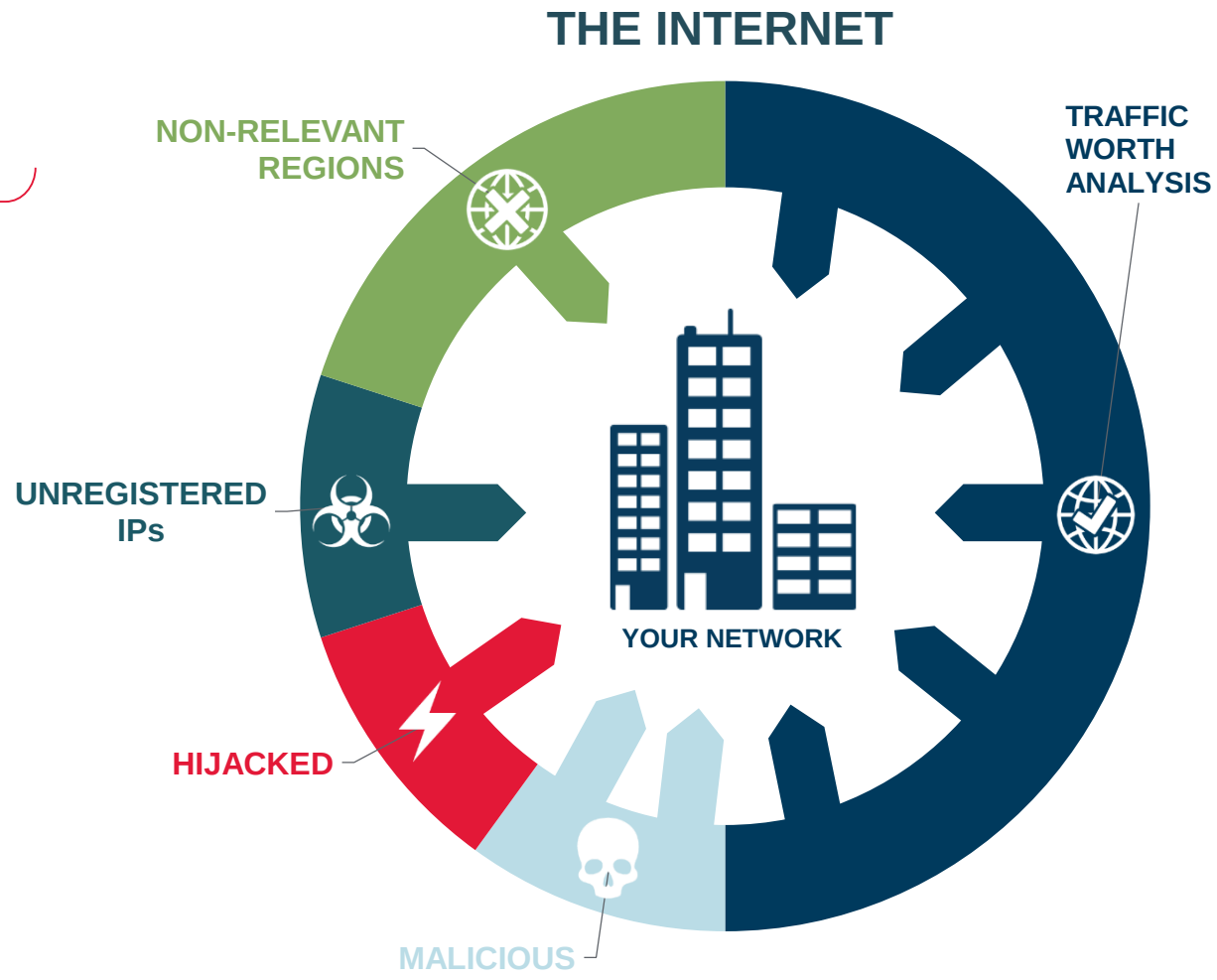
ТРАФИК, КОТОРЫЙ НЕ НУЖНО АНАЛИЗИРОВАТЬ:

KNOWN MALICIOUS

HIJACKED

UNREGISTERED IPs

UNWANTED REGIONS

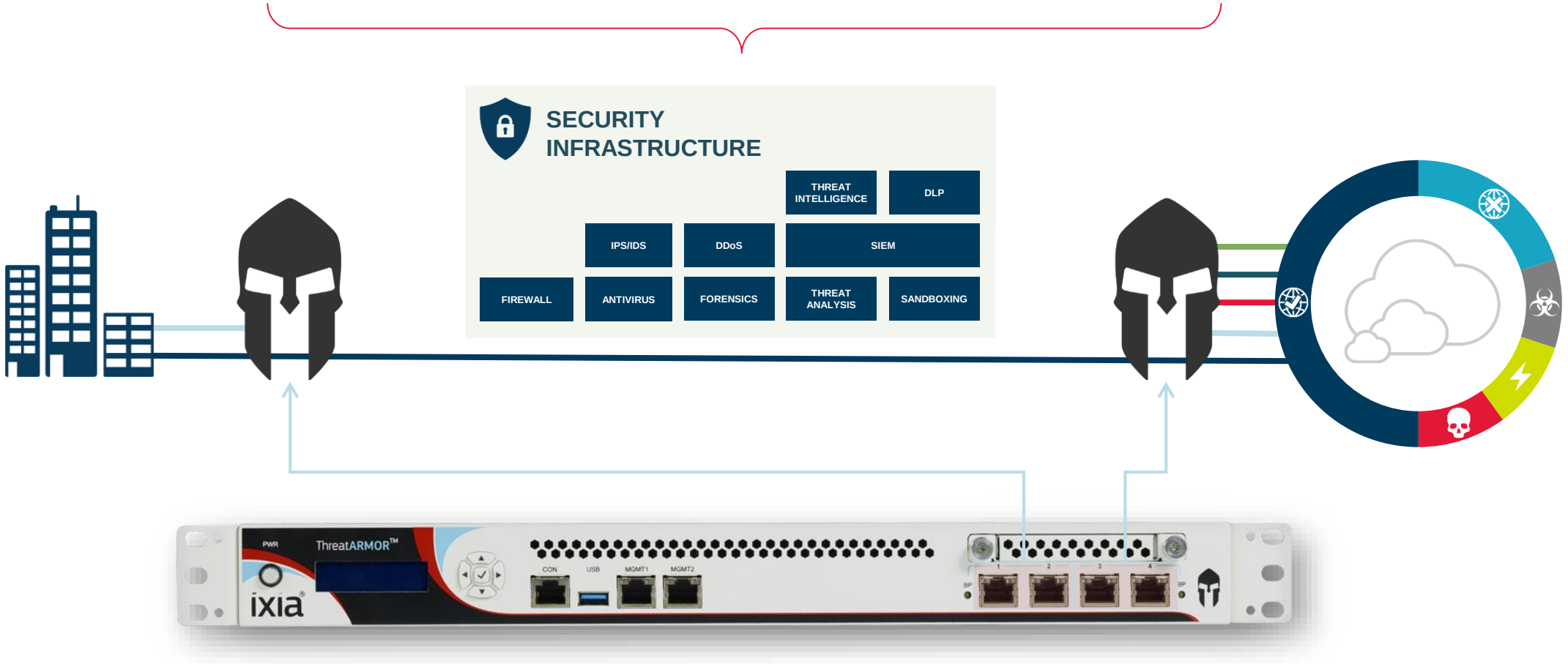


ixia

Представляем Threat**ARMOR**™ от Ixia

Threat**ARMOR – 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.

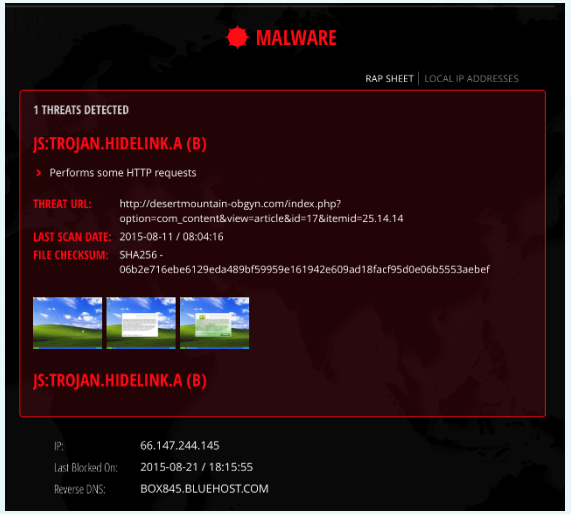
ThreatARMOR Brings Threat Intelligence to Your Network

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.

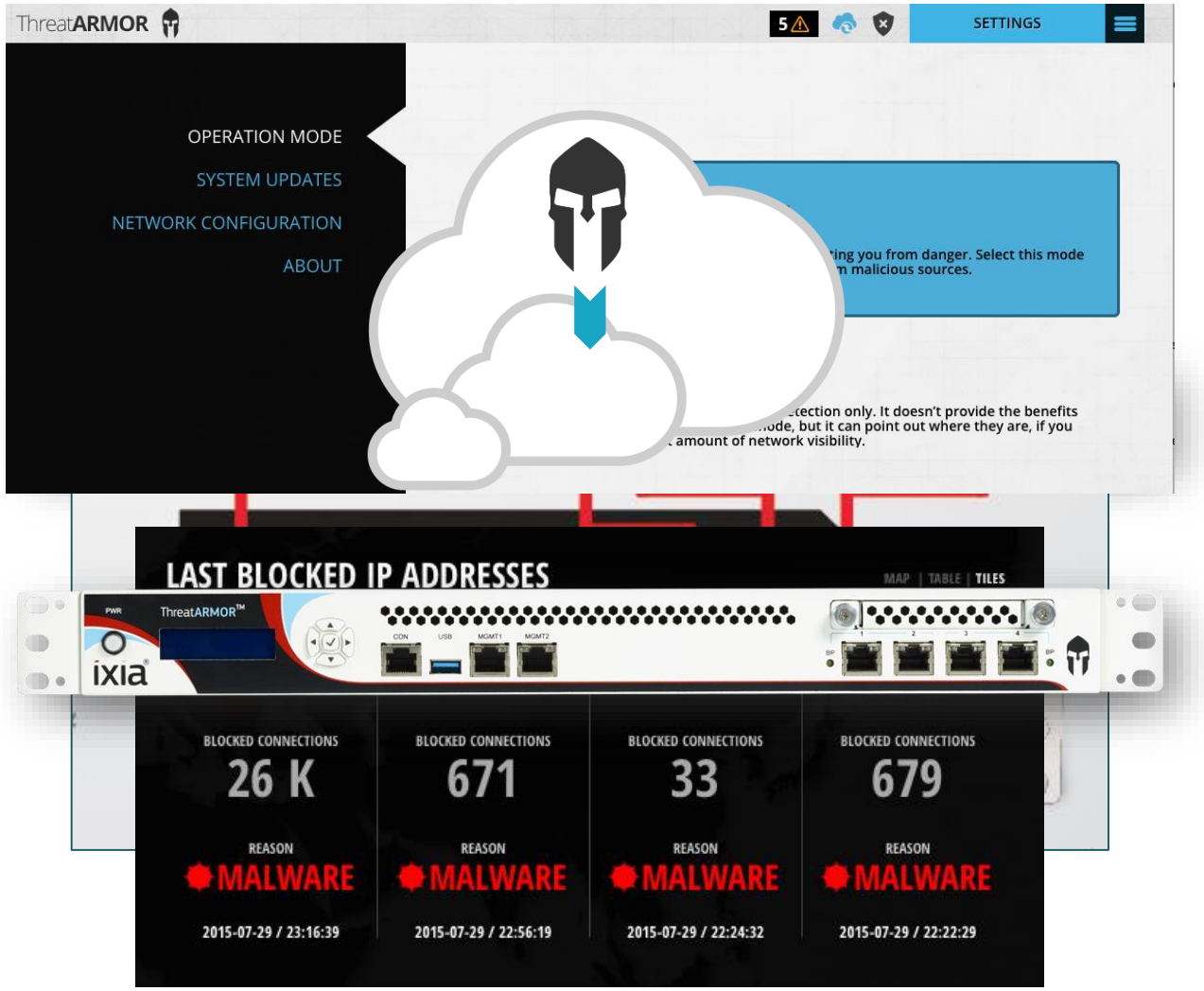
ThreatARMOR Easy Setup

EASY TO CONFIGURE

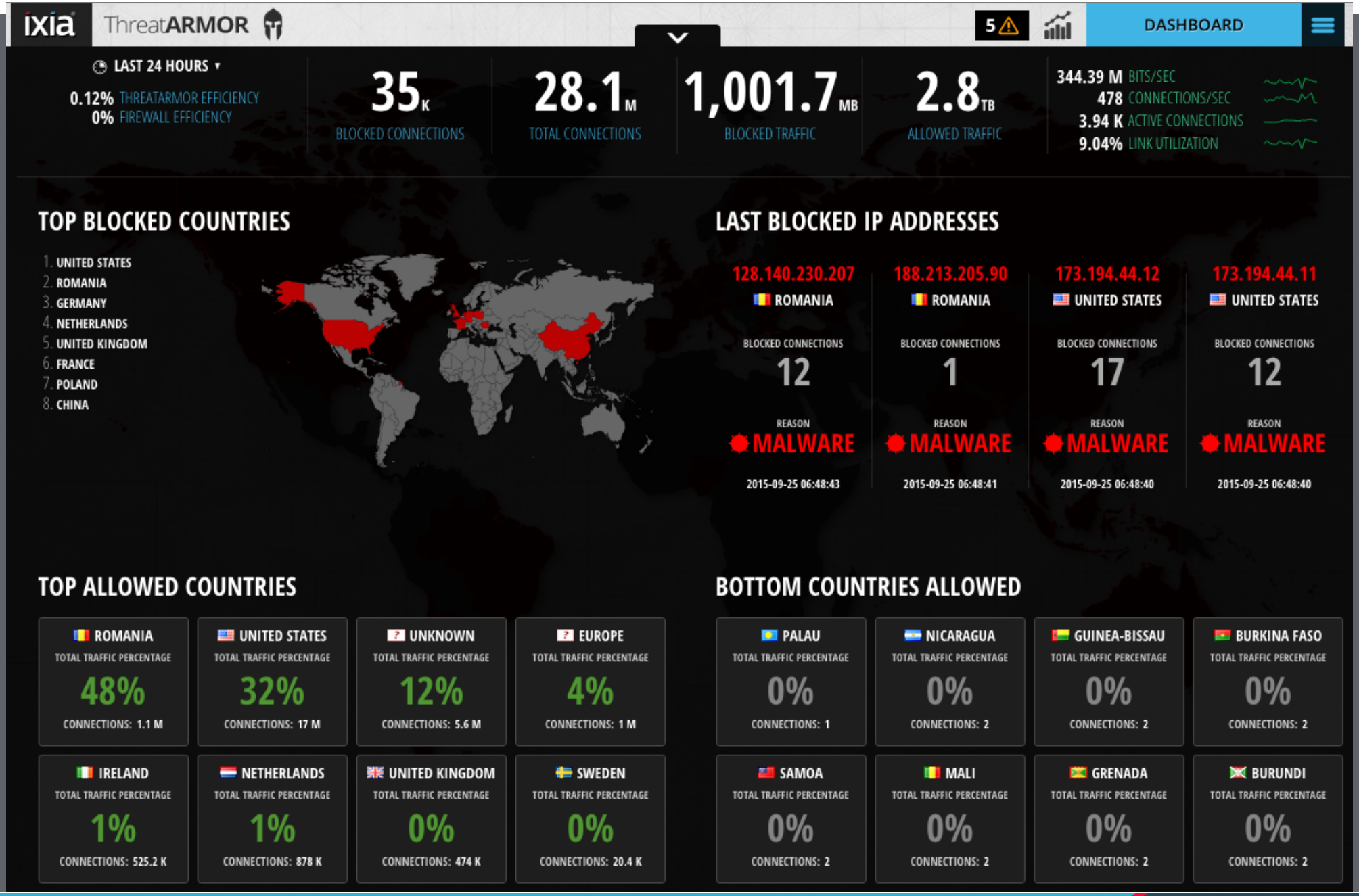
1. Connect power and Ethernet cables
2. Pick “**Report Only**” or “**Blocking Mode**”
3. Walk away, it updates automatically

Criminal site blocking is **automatic**

Geo-blocking is optional



ThreatARMOR Dashboard



ПОЧЕМУ IXIA?

Ведущие мировые корпорации и учреждения – 86 из Fortune

Финансы

Bank of America, JPMorganChase, ADP, American Express, Credit Suisse, NYSE Euronext, NASDAQ, US Bank, VISA, TD Ameritrade, E*TRADE, Fidelity Investments

Компьютеры и электроника

Apple, Microsoft, DELL, IBM, Canon, SONY, hp invent, AMCC, EMC², SAMSUNG, BROADCOM

Поставщики услуг

salesforce.com, Google, ORACLE, zynga, LinkedIn, ebay, NETFLIX, Windows Azure, amazon web services, VERITAS, YouTube

Образование

Stanford University, 東京大学 The University of Tokyo, USC University of Southern California, The University of Sydney, Harvard, University of California, Texas A&M University

Здравоохранение

BlueCross BlueShield, State Farm, Kaiser Permanente, MERCK, Johns Hopkins, Allstate, Abbott A Promise for Life, HEALTHQUEST, UCSF Medical Center

Госорганы

EUROCONTROL, NASA, U.S. Air Force, FBI, SPAWAR, Sandia National Laboratories, CIA, Department of Homeland Security, esa

Производители

BROADCOM, IBM, HUAWEI, EMC², CISCO, paloalto NETWORKS, FORTINET, f5, FireEye, ERICSSON, Alcatel·Lucent, JUNIPER NETWORKS, BROCADE, AVAYA

15 из Top 15 вендоров

Телеком операторы

at&t, vodafone, france telecom, verizon, Sprint, comcast, Telefónica, 中国移动通信 CHINA MOBILE, NTT docomo, américa móvil, TELECOM ITALIA, NTT, Deutsche Telekom

42 из Top 50 операторов

ixia

СПАСИБО

Владимир Назаренко
Директор по продажам
Ixia Украина и СНГ
+380 94 710 0942
+380 98 178 7378
vnazarenko@ixiacom.com

Узнай больше на www.ixiacom.com