ixia

Представление ThreatARMOR

Владимир Дегтярский,
«Тритфейс»

ThreatARMOR

- Определение поверхности и направленности атак сети
- Виды киберугроз
- ThreatARMOR на страже вашей сети

ixia

Поверхность атаки сети

- Подверженность сети кибератакам
- Угроза взлома вашей сети
- Угроза кражи данных

Ваша сеть подвергается огромному количеству кибератак

ixia

Направленность атак

Два типа трафика передается на каждую сеть:

НЕНУЖНЫЙ:

Вредоносный трафик

Перехват сессий

Незарегистрированные IP

Нежелательные регионы

Ваша сеть

НУЖНЫЙ:

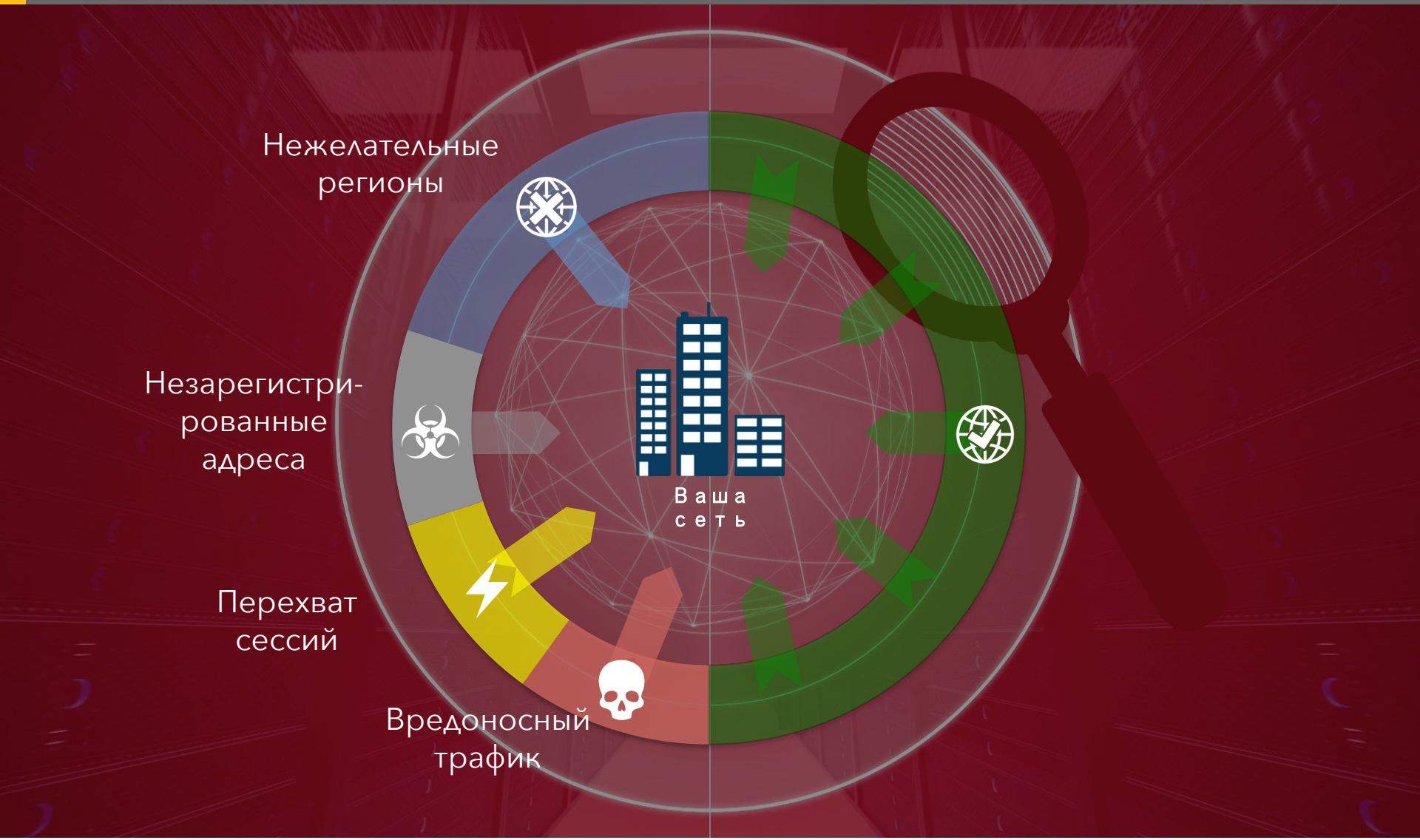
Трафик возможного интереса:

Бизнес-трафик.

Трафик клиента.

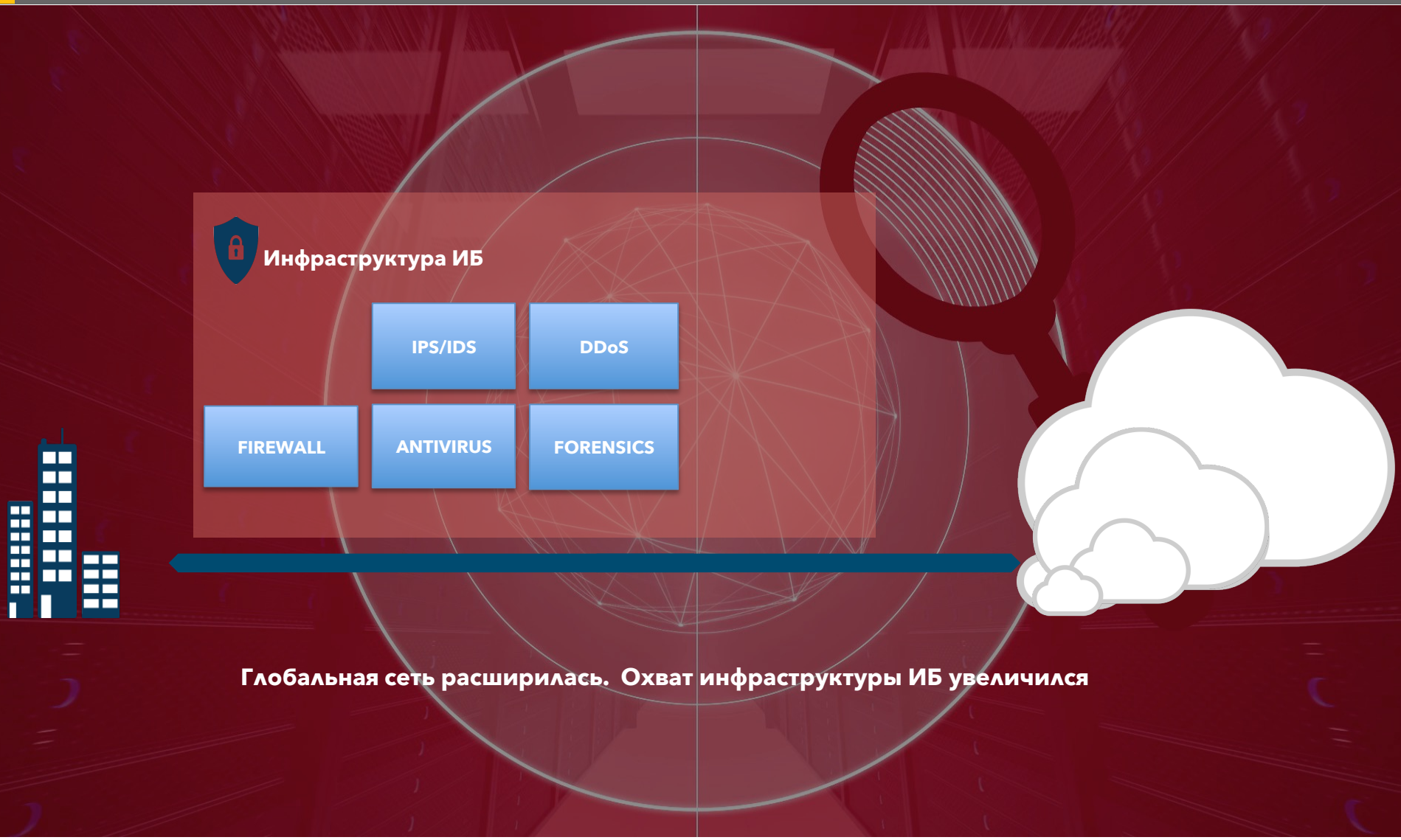
ixia

Направленность атак



ixia

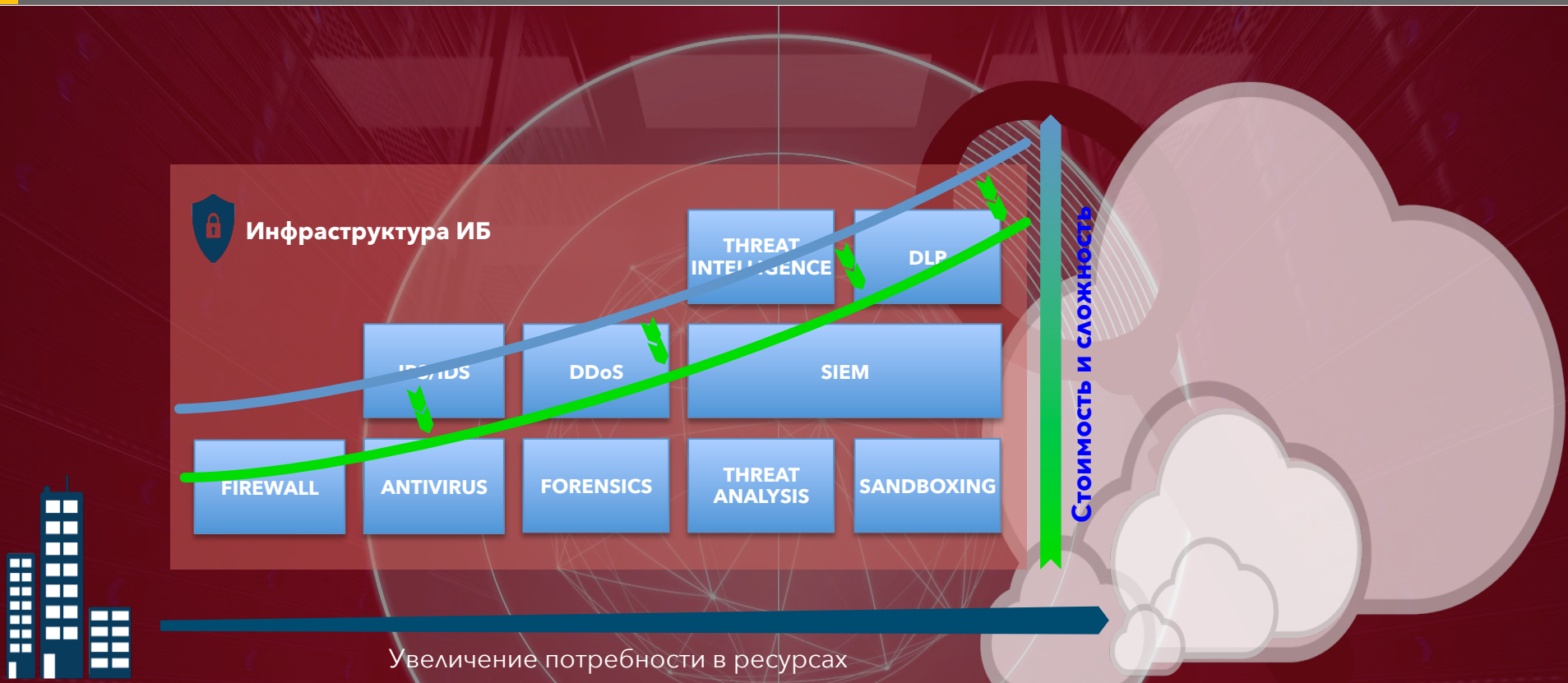
Расширение требований безопасности



Глобальная сеть расширилась. Охват инфраструктуры ИБ увеличился

ixia

Расширение требований безопасности



Новшества технологий безопасности обусловлены развитием угроз.

Больше защиты. Больше сложности. Больше обслуживания. Больше управления.

Что, если бы вы смогли сократить трафик из Интернета?

Сокращение числа атакующих	**Уменьшение числа уведомлений SIEM**	**Уменьшение поверхности атак**	**Инфраструктура безопасности** с фокусировкой на важном

ixia

Разве файрвол не делает этого?

Межсетевые экраны следующего поколения (NGFW) оптимизированы для проверки контента и обнаружения угроз, но они не так хороши в **блокировке большого количества IP-адресов.**

Страна	Диапазоны IPv4
Россия	5 632
Китай	2 659
Украина	2 528
Турция	644
Пакистан	231

Категория	**Кол-во адресов IPv4**
Вредоносный трафик	> 1 000 000
Перехват сессий	> 16 000 000
BOGON	> 800 000 000

Зачем вам нужно блокировать большое количество IP?

18% DDoS-атак происходят из **Китая.**

Китай, Бразилия, Россия и Индия вместе генерируют 26% атак на Web-приложения.

Россия, Украина, Пакистан, Китай и Турция
входят в ТОП 10 стран по количеству **контроллеров ботнетов.**

ixia

Как много гео-IPv4-адресов?

	A	B	C	D
1	IPv4 start range	IPv4 end range	Country code	Country
2	1.0.0.0	1.0.0.255	AU	Australia
3	1.0.1.0	1.0.3.255	CN	China
4	1.0.4.0	1.0.7.255	AU	Australia
5	1.0.8.0	1.0.15.255	CN	China
6	1.0.16.0	1.0.31.255	JP	Japan
7	1.0.32.0	1.0.63.255	CN	China
8	1.0.64.0	1.0.127.255	JP	Japan
9	1.0.128.0	1.0.255.255	TH	Thailand
10	1.1.0.0	1.1.0.255	CN	China
11	1.1.1.0	1.1.1.255	AU	Australia
12	1.1.2.0	1.1.63.255	CN	China
13	1.1.64.0	1.1.127.255	JP	Japan
14	1.1.128.0	1.1.255.255	TH	Thailand
15	1.2.0.0	1.2.2.255	CN	China
16	1.2.3.0	1.2.3.255	US	United States
17	1.2.4.0	1.2.127.255	CN	China
18	1.2.128.0	1.2.255.255	TH	Thailand
19	1.3.0.0	1.3.255.255	CN	China
20	1.4.0.0	1.4.0.255	AU	Australia
21	1.4.1.0	1.4.127.255	CN	China
22	1.4.128.0	1.4.255.255	TH	Thailand
23	1.5.0.0	1.5.255.255	JP	Japan
24	1.6.0.0	1.7.255.255	IN	India
25	1.8.0.0	1.8.255.255	CN	China
26	1.9.0.0	1.9.255.255	MY	Malaysia
27	1.10.0.0	1.10.9.255	CN	China

GeoIPCountryWhois.csv

ixia

Ботнет - где?

Тор 5 стран с наибольшим количеством зараженных хостов

Страна	Кол-во ботов
1. Индия	1 120 000
2. Вьетнам	1 010 000
3. Китай	771 000
4. Россия	511 000
5. Бразилия	433 000

Источник: Spamhaus (Март 2016).
https://www.spamhaus.org/statistics/botnet-cc/

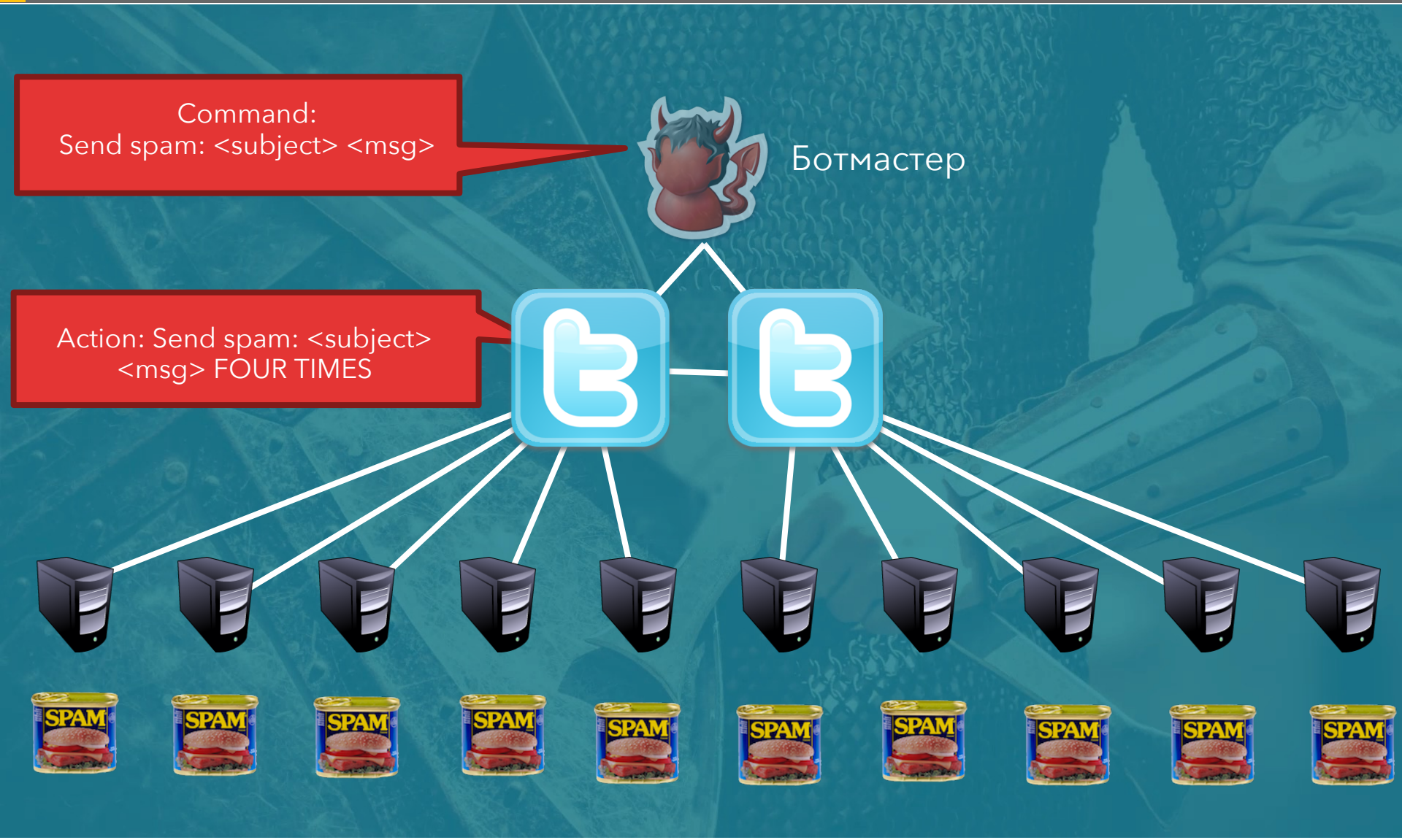
Тор 5 стран с наибольшим количеством C&C-серверов

Страна	C&C-серверы
1. США	631
2. БВО	237
3. Нидерланды	154
4. Россия	125
5. Германия	95

Источник: McAfee.

ixia

Ботнет – C&C-архитектура



ixia

Пример фишинговой страницы

Is Your Credit Card Stolen? Check for free!

Free! Check if your credit card has been stolen!

If you fear your credit card info has been stolen, enter it here and you can find out for **free**. Avoiding fraud has never been easier!

About

Credit card issuer: Select card issuer

Credit card number:

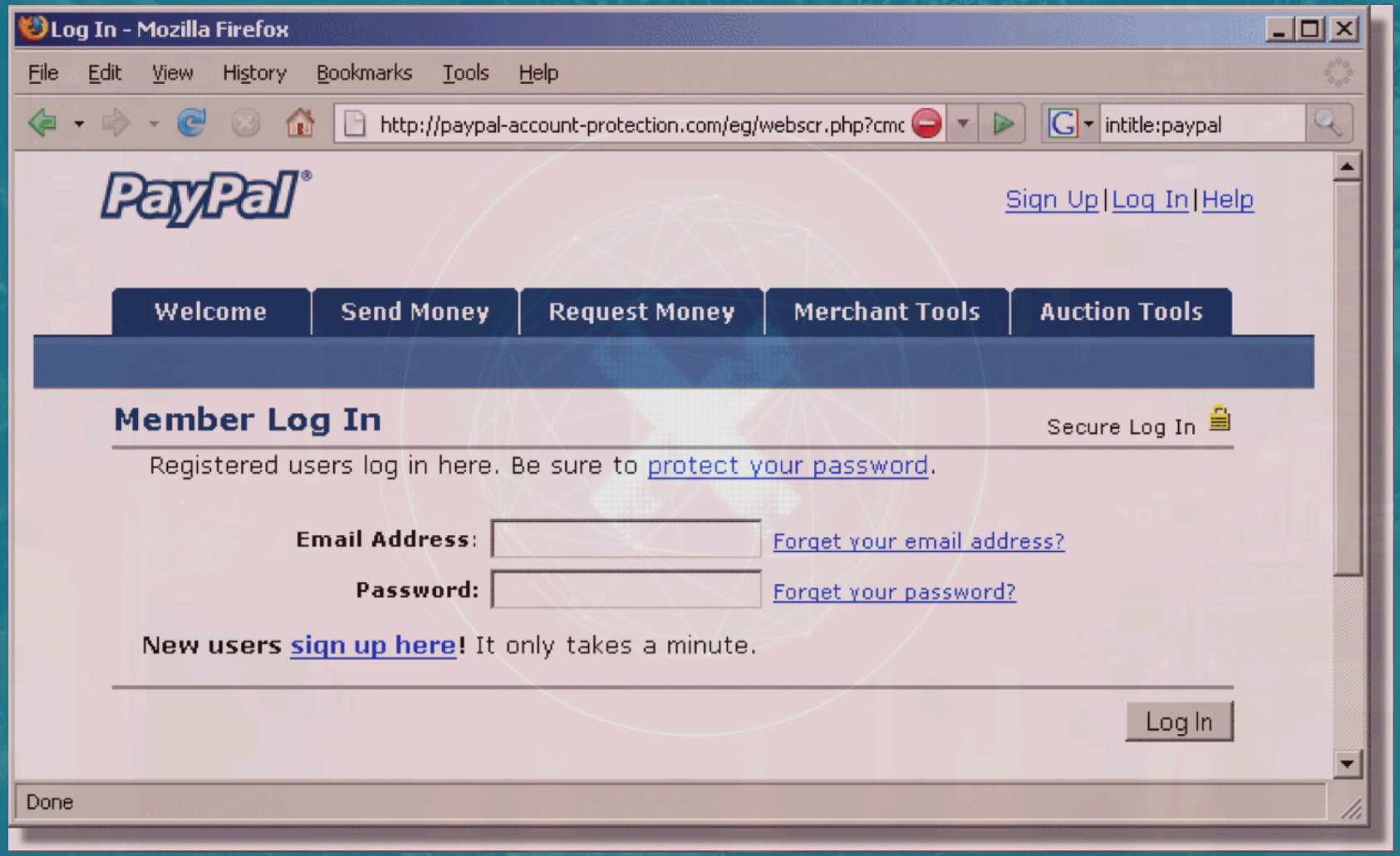
Name on credit card:

Expiration Date: 01 / 2010

Check if my credit card is stolen

Verified Secure

Пример фишинговой страницы № 2



ixia

ThreatARMOR™

ThreatARMOR выступает на первой линии защиты вашей сети.

Блокировка нежелательного входящего трафика и предотвращение исходящих вредоносных коммуникаций.

ixia

ThreatARMOR™

NOT IPS

NOT FIREWALL

NOT ANTIVIRUS

ixia

Преимущества ThreatARMOR

Высокая производительность

- Сфокусирован только на блокировке IP.
- Справляется с задачей на скорости линии.
- Масштаб без влияния на производительность при блокировке от одного IP-адреса до миллиарда IP-адресов.

Высокая отказоустойчивость

- Максимальная надежность.
- Резервируемые блоки питания.
- Встроенный байпас.
- SSD-диск с возможностью замены в полевых условиях.

ixia

Влияние на IT-безопасность

21 000 часов в год тратится на обработку ложно-позитивных сообщений о киберугрозах.

Ponemon Institute, 2015

ThreatARMOR устраняет **33%** ненужных ложно-позитивных сообщений, экономя **6 300 часов** для предприятия.

Средняя ЗП сотрудников IT Security = **$100K.**

Payscale (US Based Median), 2015

157

недель сэкономлено

$300K+

Экономия операционных расходов

ixia

ThreatARMOR привносит опыт команды Threat Intelligence в вашу сеть

IXIA ATI Research Center

Профессиональная база Threat Intelligence, используемая лидерами отрасли.

ThreatARMOR Rap Sheets

Доказательство каждого заблокированного сайта.

ThreatARMOR Appliance

Установите, настройте и забудьте.

Автообновление каждые 5 мин.

Максимальная надежность.

Получение информации об угрозах

ixia

Детальные отчеты

IP:185.68.16.161

RAP SHEET | LOCAL IP ADDRESSES

THREA

JS:IFRAME-BND [TRJ]

THREAT URL	http://chuguevnews. 02&id=935:2014-02-
LAST SCAN DATE	2016-01-10 15:46:51
FILE CHECKSUM	SHA256 - fecdbcc77c324650fb
PAGE TITLE	Home | chuguevnev

JS:IFRAME-BND [TRJ]

THREAT URL	http://chuguevnews. 17-35?tmpl=compor
LAST SCAN DATE	2016-01-10 15:39:20
FILE CHECKSUM	SHA256 - 9b470f11291dcb18a 9

Reverse DNS: 185.68.16.161

IP:202.97.174.82

RAP SHEET | LOCAL IP ADDRESSES

THR

COMMUNICATED WITH WIN32/TROJANDOWNLOAD

LAST SCAN DATE	2016-01-06 00:53:40
FILE CHECKSUM	SHA256 - 79938cad61289bca

COMMUNICATED WITH A V WIN32/TROJANDOWNLOAD

LAST SCAN DATE	2015-12-07 07:36:03
FILE CHECKSUM	SHA256 - a15e9de35a616186

Reverse DNS: 202.97.174.82

IP:205.203.0.1

HIJACKED

RAP SHEET | LOCAL IP ADDRESSES

THIS IP IS HIJACKED

HIJACKED INFO

This particular network range has been hijacked. A hijacked range is a netblock brought back from the dead, often by a spammer. The original owner of the block may have left it derelict for any number of reasons. For more information about these types of IP ranges please visit http://www.spamhaus.org/faq/section/DROP%20FAQ#258

LAST SCAN DATE	2015-12-30 06:28:54
MORE INFO AT	http://www.spamhaus.org/sbl/sbl.lasso?query=SBL104616
ASN	9737 TOTNET-TH-AS-AP TOT Public Company Limited,TH
ASN REGISTRAR	apnic
ASN DESCRIPTION	TOTNET-TH-AS-AP TOT Public Company Limited,TH
ASN REGISTRATION DATE	2011-04-08
ASN (AUTONOMOUS SYSTEM NUMBER)	9737

Reverse DNS: 205.203.0.1

Last Blocked On: 2016-01-08 13:28:34

ixia

Детальные отчеты (продолжение)

IP:221.146.224.75

RAP SHEET | LOCAL IP ADDRESSES

THREATS DETECTED: 1 EXPLOIT

PERFORMED THE FOLLOWING EXPLOIT: SSH-BRUTEFORCE

LAST SCAN DATE 2016-01-08 16:02:24

Reverse DNS: 221.146.224.75

Last Blocked On: 2(

IP:95.173.185.143

PHISHING

RAP SHEET | LOCAL IP ADDRESSES

THREATS DETECTED: 2 PHISHING

HTML/PHISHING.DHL.B TROJAN

THREAT URL http://sanalkoyum.com/wp-content/post%20dhl/express/tracking.html

LAST SCAN DATE 2016-01-10 06:07:20

FILE CHECKSUM SHA256 - d5156ced298eaa043540d3264c97221fbd7ded243f562d3d26ce4d2d203d76fd

PAGE TITLE TRADE FILE

HTML/PHISHING.DHL.B TROJAN

THREAT URL http://sanalkoyum.com/wp-includes/dhl/dhl/tracking.html

LAST SCAN DATE 2016-01-07 06:20:25

FILE CHECKSUM SHA256 - d5156ced298eaa043540d3264c97221fbd7ded243f562d3d26ce4d2d203d76fd

PAGE TITLE TRADE FILE

Reverse DNS: NS481.WEBEMPRESA.EU

Last Blocked On: 2016-01-08 13:28:34

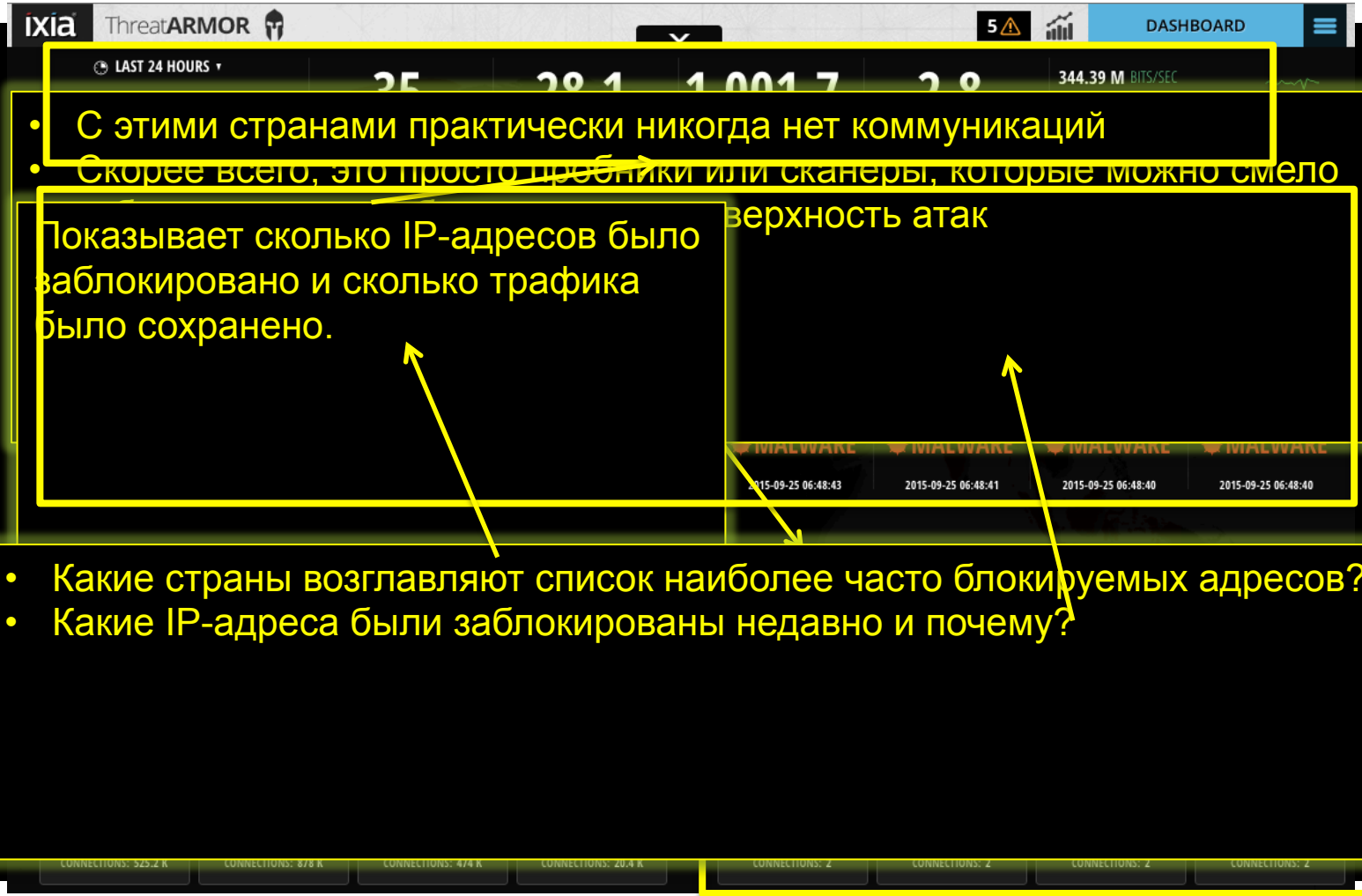
ixia

«Белый» список

- Alexa и Quantcast топ **10 000**:
  - Включая Facebook, Google, YouTube, Wikipedia и т. д.
- Облачные сервисы:
  - Amazon AWS, Microsoft Azure, Salesforce.
- Интернет инфраструктура:
  - DNS серверы, NTP серверы, и т. д.

ixia

ThreatARMOR Dashboard



- С этими странами практически никогда нет коммуникаций
- Скорее всего, это просто пробники или сканеры, которые можно смело верхность атак

Показывает сколько IP-адресов было заблокировано и сколько трафика было сохранено.

- Какие страны возглавляют список наиболее часто блокируемых адресов?
- Какие IP-адреса были заблокированы недавно и почему?

ixia

ThreatARMOR простота установки

Легко сконфигурировать

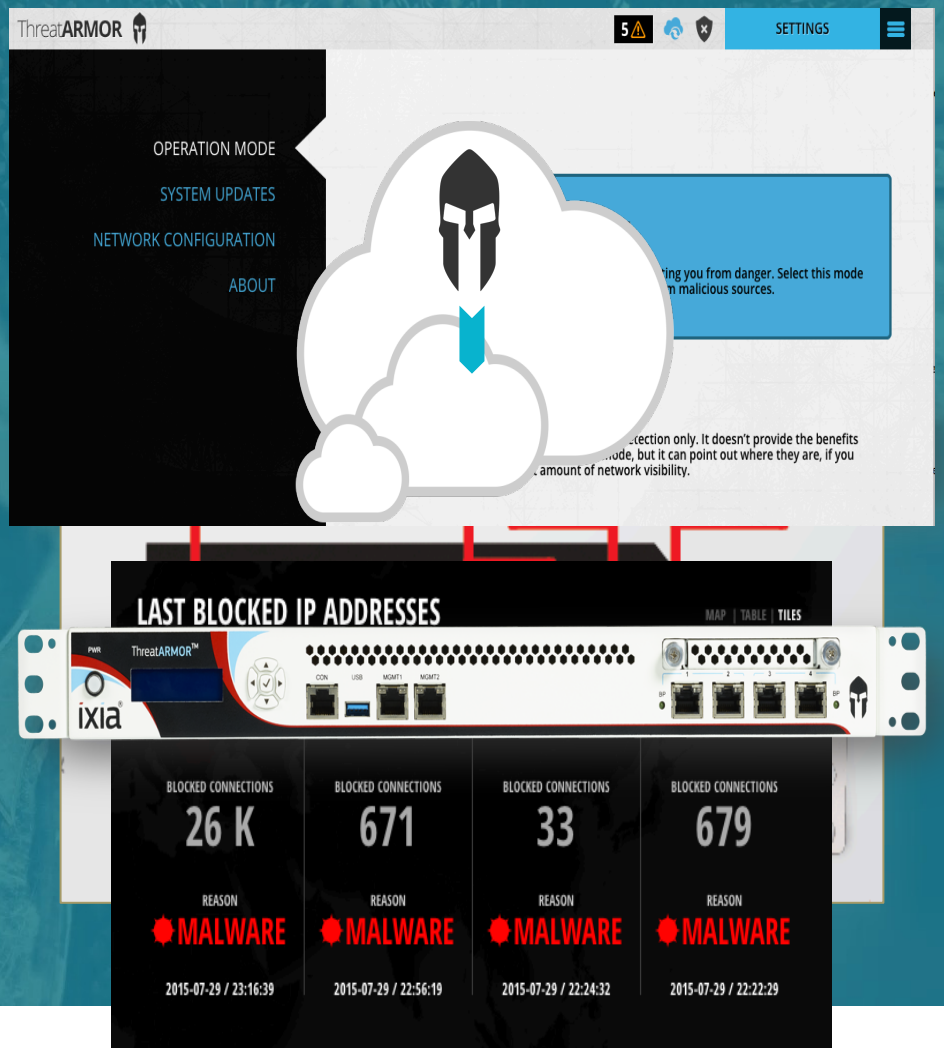
1. Подсоедините питание и Ethernet-кабели.

2. Выберите режим Reporting или Blocking.

3. Продолжайте работать в привычном режиме! (Обновляется автоматически.)

Блокировка опасных сайтов – **автоматическая**

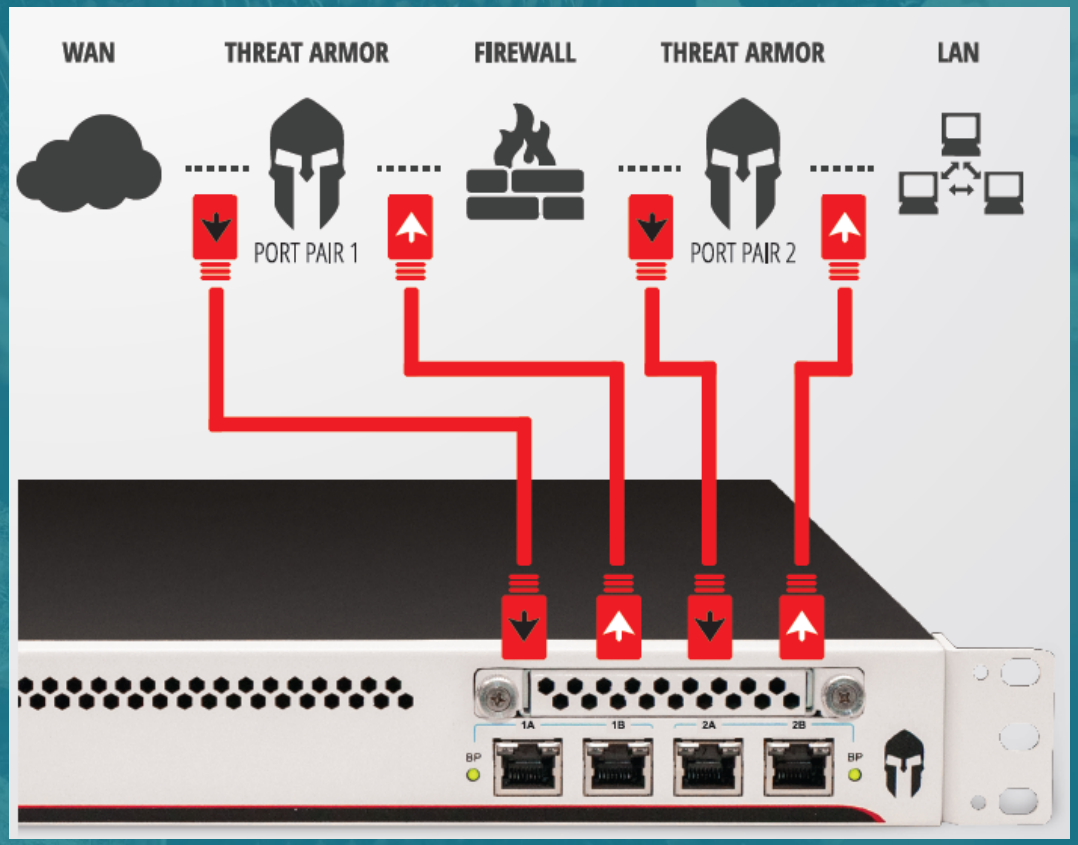
Геоблокировка – **опциональная**



ixia

Threat**ARMOR**™: inline-установка

В соответствии с топологией справа на обеих сторонах файрвола и устройств безопасности вставьте Ethernet-кабели из вашей сети в **пару портов 1 для WAN** и **пару портов 2 для LAN**.

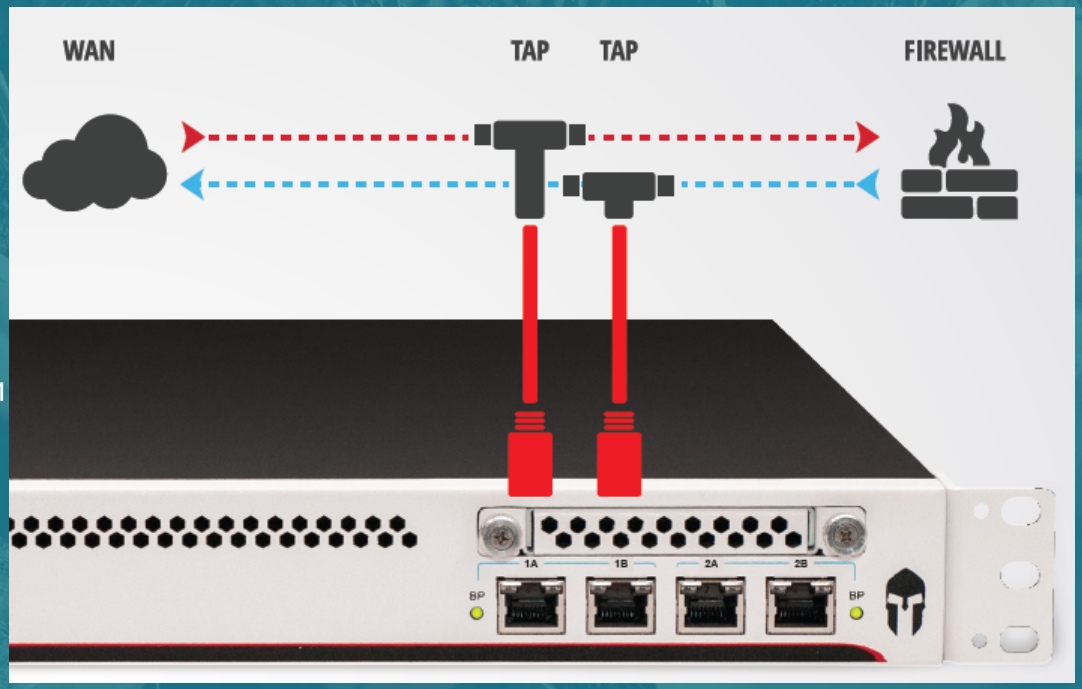


ixia

ThreatARMOR™: offline-установка.

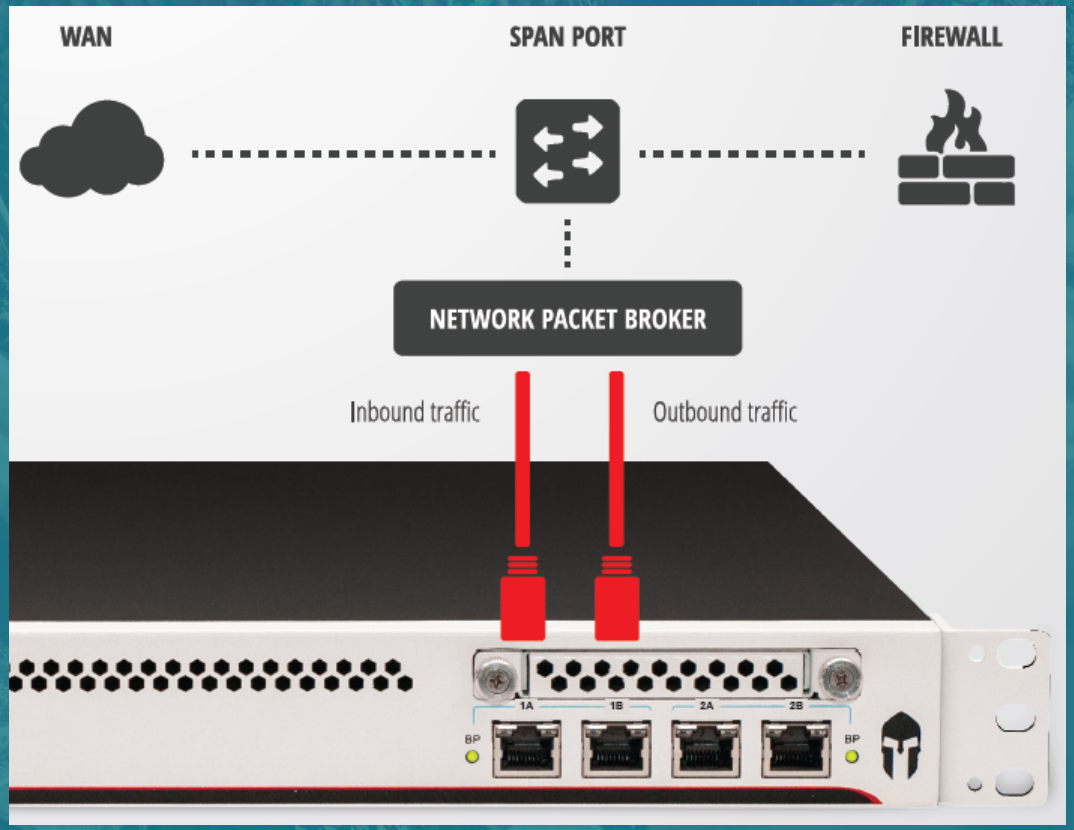
TAP

В соответствии с топологией справа подключите сетевой ответвитель к линку между файрволом и WAN, а затем подсоедините ответвитель к **паре портов 1.**



ixia

Threat**ARMOR**™: offline-установка. SPAN



В соответствии с топологией справа SPAN-порт коммутатора, который зеркалирует весь трафик между файрволом и WAN, подсоедините к **паре портов 1** через брокер сетевых пакетов NTO. Используйте NTO для перенаправления **исходящего трафика (Source= Firewall) на порт 1A** и **входящего трафика (Destination= Firewall) на порт 1B.**

ixia

Резюме

Threat**ARMOR :** перестаньте анализировать трафик, который вам известен

Блокируйте нежелательные входящие или исходящие активности.

Получайте больше от вашей команды IT-безопасности и устройств безопасности.

Получайте выгоду от профессиональной команды Ixia Application and Threat Intelligence.

ixia

TEST. VISIBILITY. SECURITY.

Спасибо!

ixia