Мониторинг и анализ Производительности Сети

riverbed

Network Performance Monitoring
(он всё ещё актуален? или уже устарел)

riverbed®

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

5% всего «бардака» случается из-за сети – а вот остальные 95% кроются в самих приложениях и настройках их серверов...

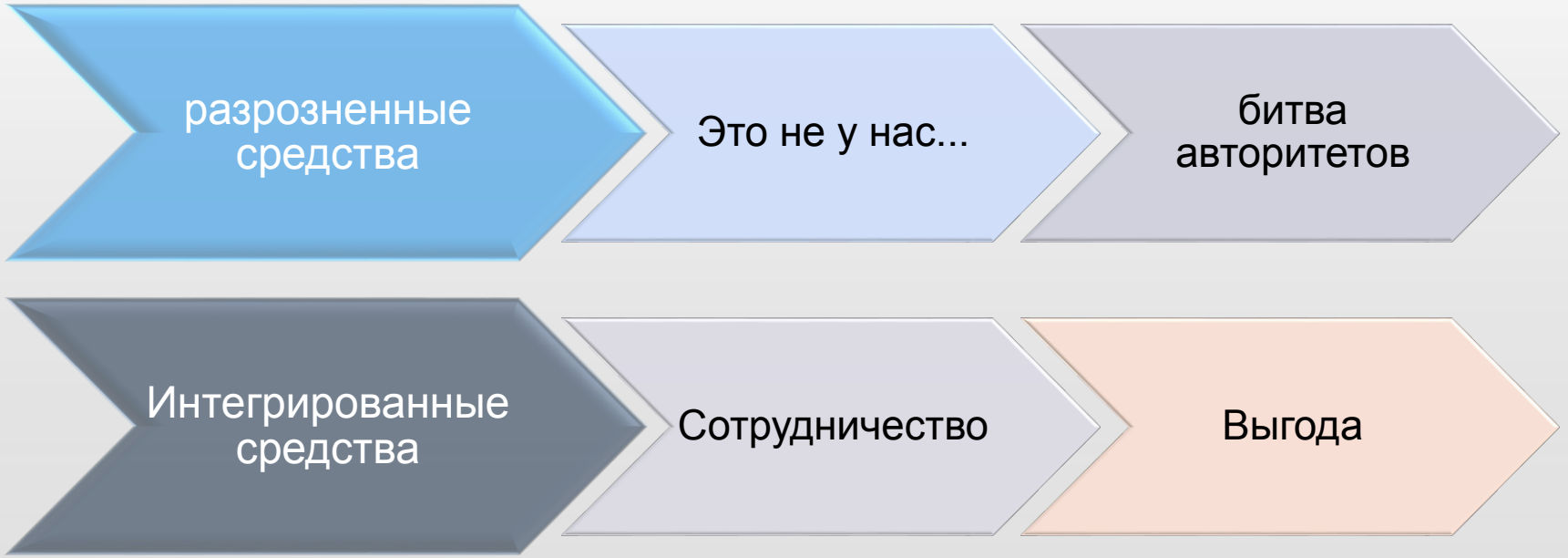
так говорят клиенты у которых внедрена всесторонняя концепция мониторинга

Признаки «Взрослых» Клиентов

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

Выросли из состояния “Это не у нас, смотрите у Вас...”

Network team – не «мальчик для битья», а разведчик...
выполняющий быстрое и точное сужение домена поиска проблемы.

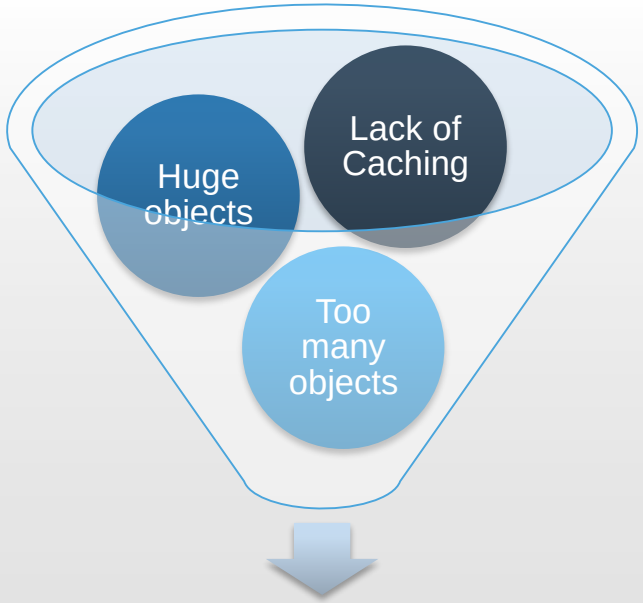


Роль Network team: помимо предоставления сервиса «всё работает», контроль состояния «всё работает быстро»

Что прикладники хотят знать про сеть?

...кроме отмазки что у нас всё нормально?

это проблемы вообще среди всех приложений или КОНКРЕТНО с моим приложением и ЭТИМ клиентом



Неэффективно но «быстро»...

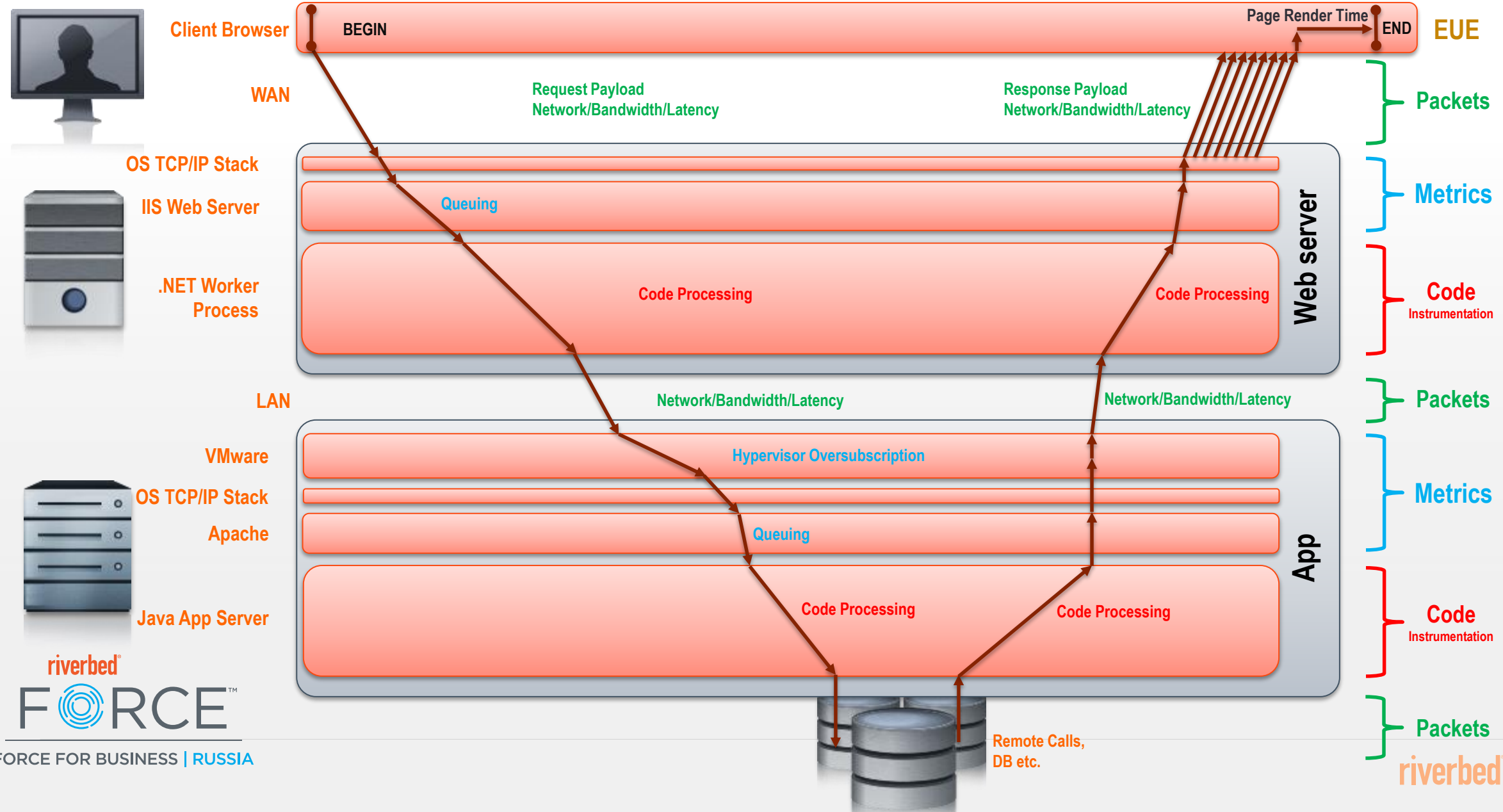
как скрестить ужа с ежом?

riverbed FORCE™

FORCE FOR BUSINESS | RUSSIA

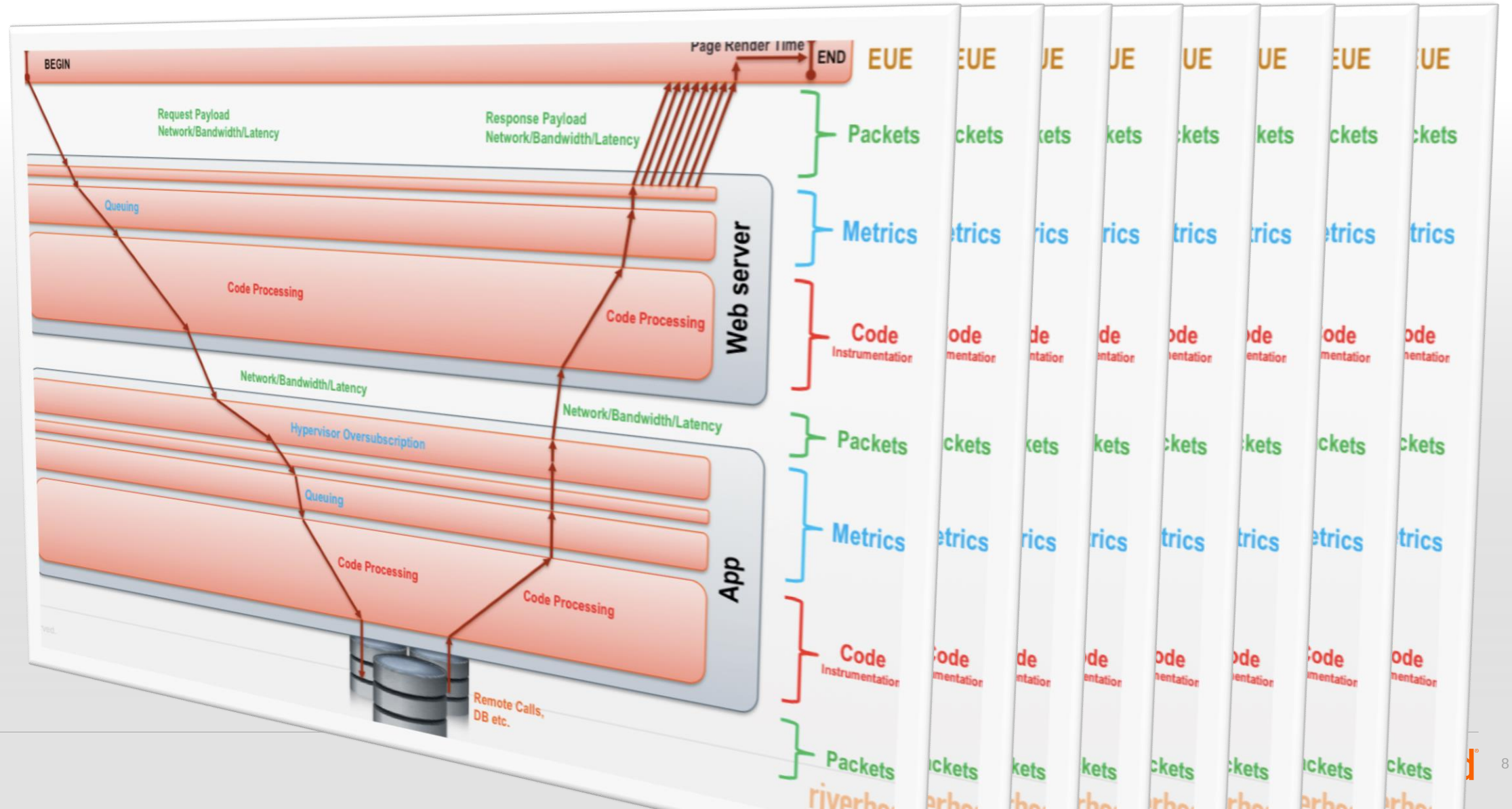
riverbed®

Анатомия транзакции



И это всё в больших масштабах...

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA



Идеальная интеграция

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

1. Корреляция всех метрик и объектов.

   по времени

2. Контекстный переход из NPM в анализ транзакций

   по запрашиваемым URL (NPM➔APM)

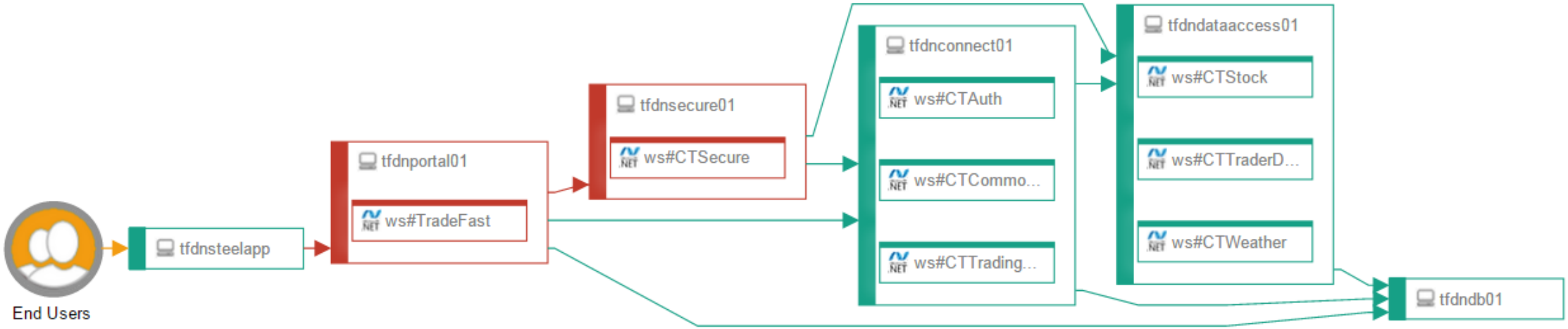
3. Конкретизация из анализа транзакций в производительность сети (APM➔NPM)

   по запрашиваемым URL (APM➔NPM)

Portal: инфраструктурная топология

красивая картинка для отдела эксплуатации

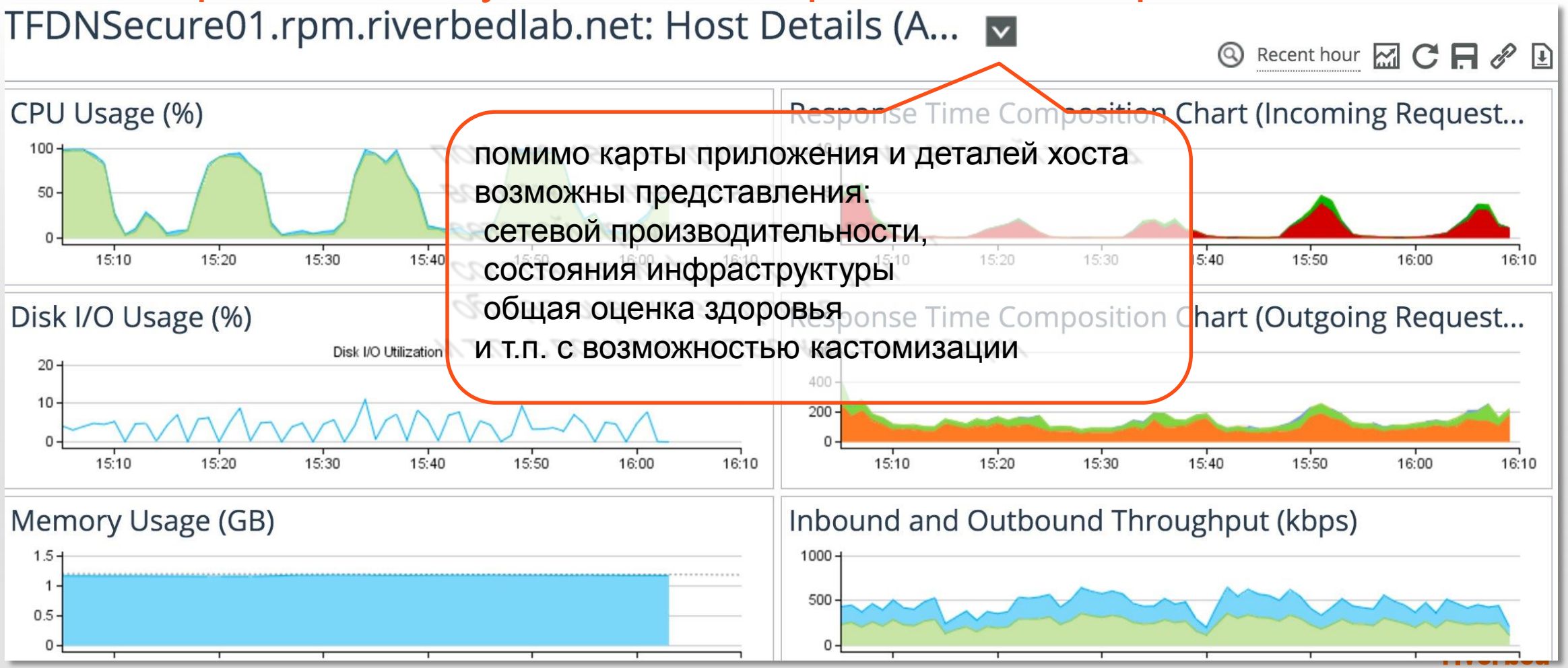
- Цвет определяется метриками объектов
- Метрики объектов берутся из средств NPM и APM одновременно



Portal: контекстная корреляция

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

при подключении к порталу всех источников автоматически и «из коробки» доступны комбинированные метрики

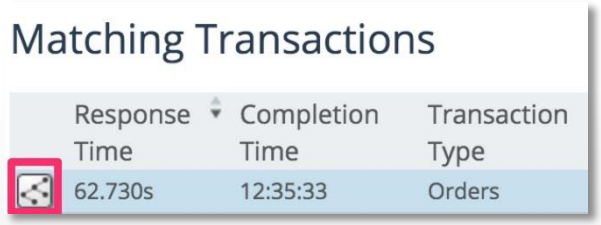


Интеграция: хочу видеть NPM из средств APM

у каждой транзакции есть кнопка...

... “View Transaction Details”:

нас интересует раздел Resources



OVERVIEW | URLS | TOP CALLS | CALL TREE | EXCEPTIONS | SQL | ENVIRONMENTAL PERFORMANCE | AJAX | RESOURCES | ANALYSIS OPERATORS | HELP

⊞ AJAX (no data)

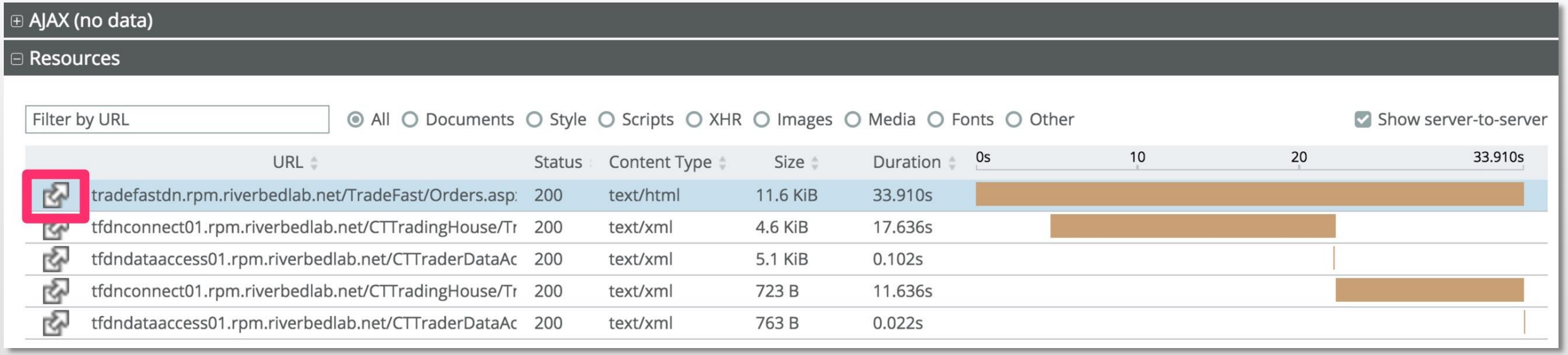
⊟ Resources

Filter by URL | All | Documents | Style | Scripts | XHR | Images | Media | Fonts | Other | Show server-to-server

URL	Status	Content Type	Size	Duration	0s 100 200 300 470.786s
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.120s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.092s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.102s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.098s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.102s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.093s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.153s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.134s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.122s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.102s	
tfdndataaccess01.rpm.riverbedlab.net/CTStock/Se	200	text/xml	1.5 KiB	0.084s	

Интеграция: хочу видеть NPM из средств APM
и даже ещё глубже

- кнопка launch выдаст пакеты в AppResponse



riverbed FORCE™
FORCE FOR BUSINESS | RUSSIA

и вот как это работает...

riverbed FORCE™

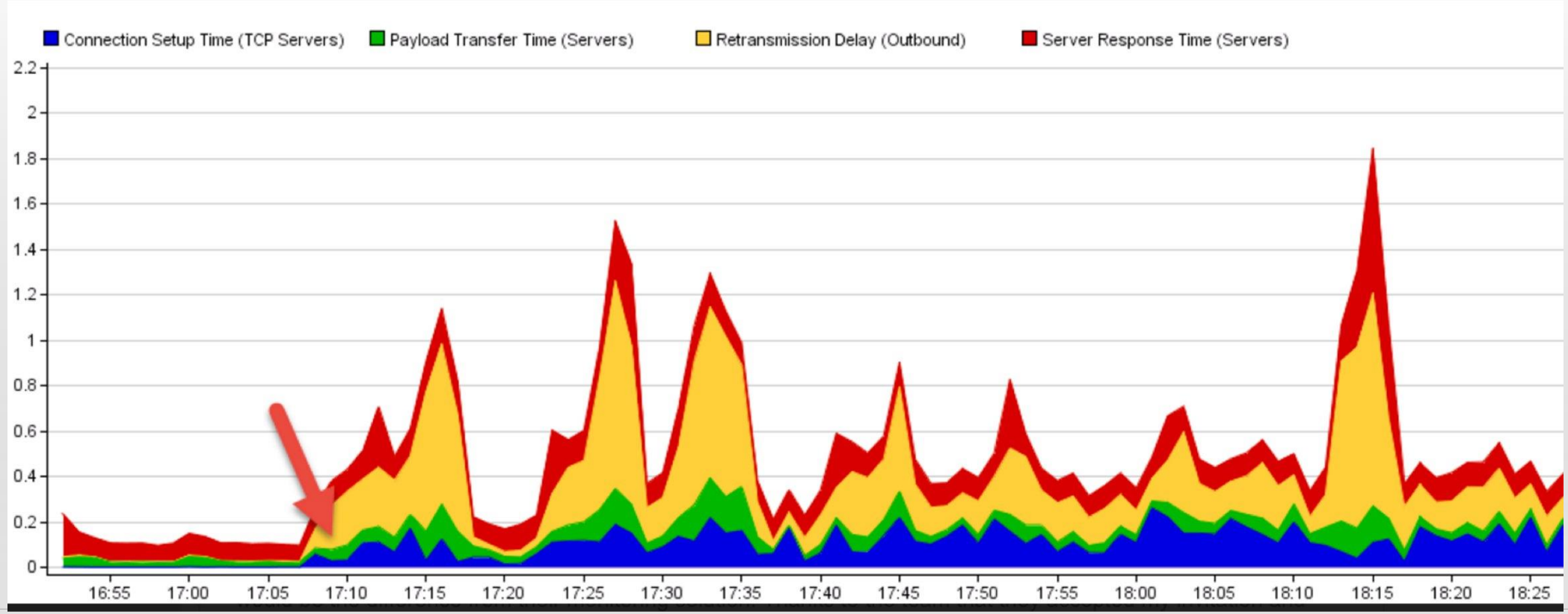
FORCE FOR BUSINESS | RUSSIA

riverbed®

Вот если бы у всех был SteelCentral

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

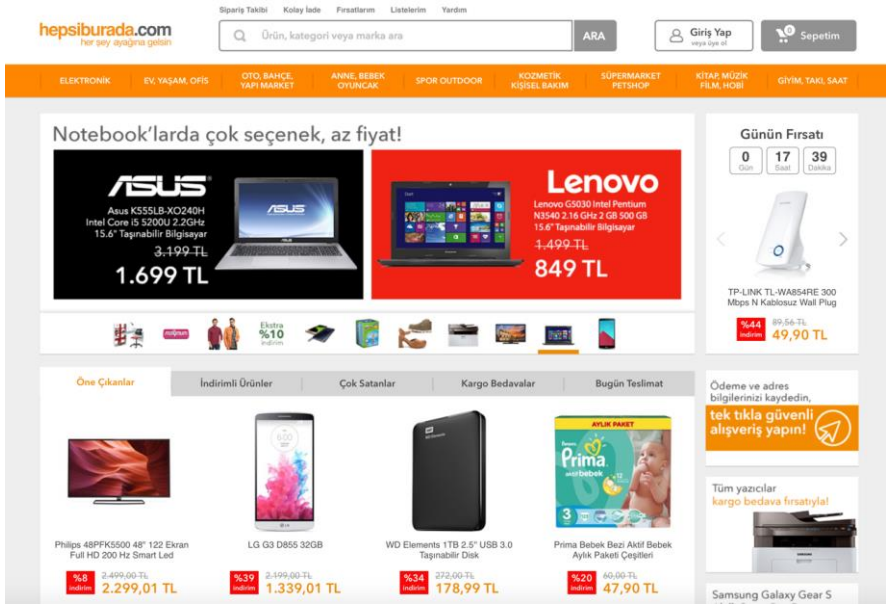
- Slides are in Appendix B of this presentation




«хардкорщикам» посвящается...

У каждого свой Mediamarkt...

- Начиная с 1998 заказчик является самым крупным представителем e-commerce в своём регионе
- 18 Место среди всех розничных сетей Европы
- 4 Миллиона подписчиков, 8.5 Миллионов посетителей, 27 тысяч заказов ежедневно.
- .Net ~~наше~~ их всё, около 800 серверов приложений
- В 2013 году несмотря на старания конкурентов ~~dynatrace, AppDynamics~~ был выбран Riverbed
- интегрированность NPM и APM было решающим фактором
- AppInternals 80 agents + AppResponse 4200
- + Transaction Analyzer + Portal



С чего всё началось

- В конце 2013 года компания решила трансформировать свой ecommerce бизнес и заказала программное решение у крупного разработчика софта (+3000 программистов)

- Кому интересно разработка стоила $6 миллионов
- Непосредственно у заказчика работали 112 разрабов одновременно.

- Через год работа была готова и заказчик приступил к...

- нагрузочному тестированию...

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

...Наш код идеален. Наш инструмент контроля явно указывает на причину проблемы в вашем поисковом движке, который криво написан и требует замены!!!

Мистер: Сами вы программировать не умеете

Архитектор кода приглашённый по контракту

А что если ваш инструмент APM ВРЁТ?!!

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

- упал предмет на вентилятор… Партнёром разработчика был dynaTrace

- dynaTrace убедительно указывал в сторону SDL Fredhooper Search Engine, которая под нагрузкой показывала замедление всех вовлечённых транзакций.

- На CIO давили юристы под угрозой неустоек подталкивая к подписанию «кривого софта»

- Но у CIO был отчёт Riverbed AppResponse о производительности Fredhooper поэтому он сопротивлялся..

суперсекретный слайд

«Старая» .Net разработка
Сервера **Front и Back-end**

Riverbed

Fredhooper поисковик

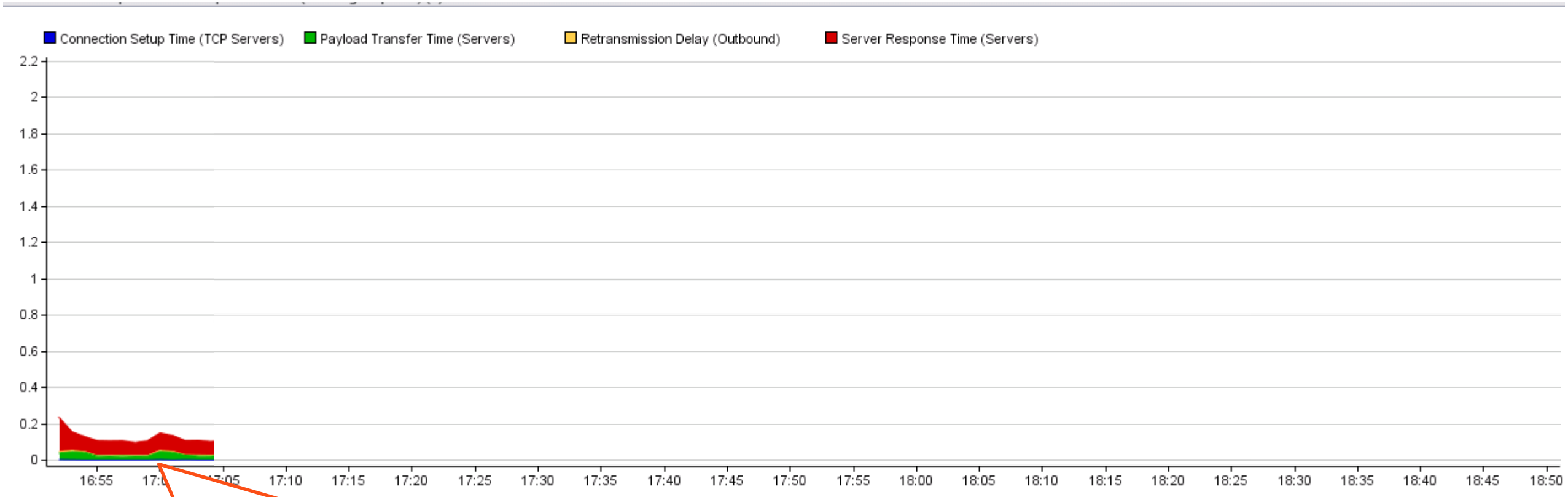
БД Сервера

«Заморский продукт»
.Net Application Servers

dynaTrace

что же видел Riverbed и не видел Dynatrace?!!

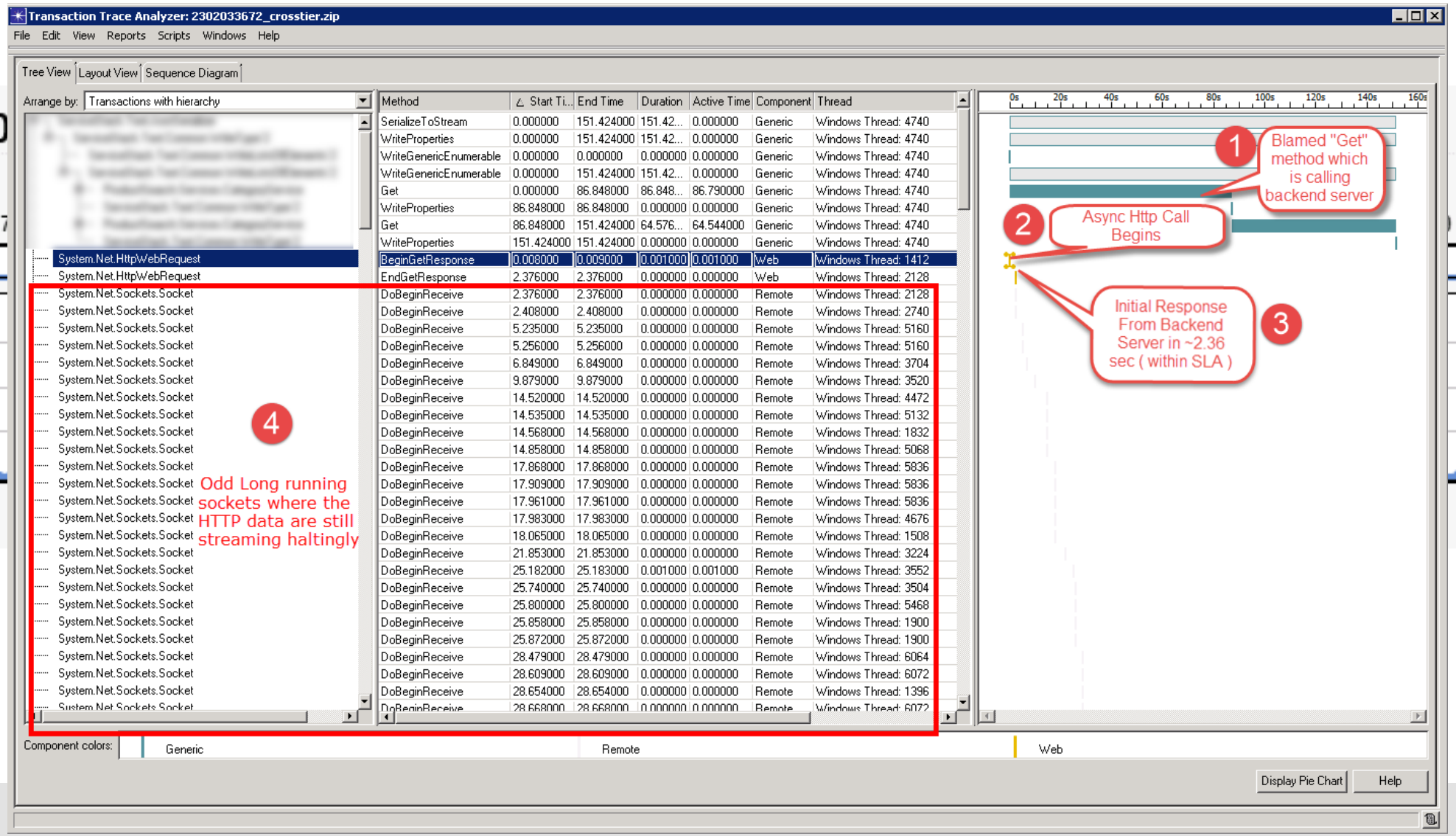
ПАКЕТЫ



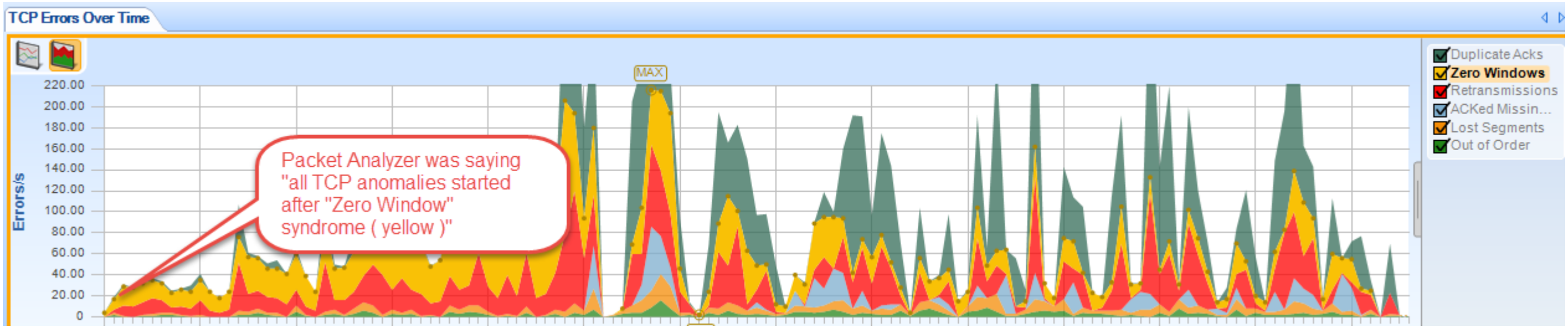
Так выглядело время отклика при эксплуатации поисковика старым приложением

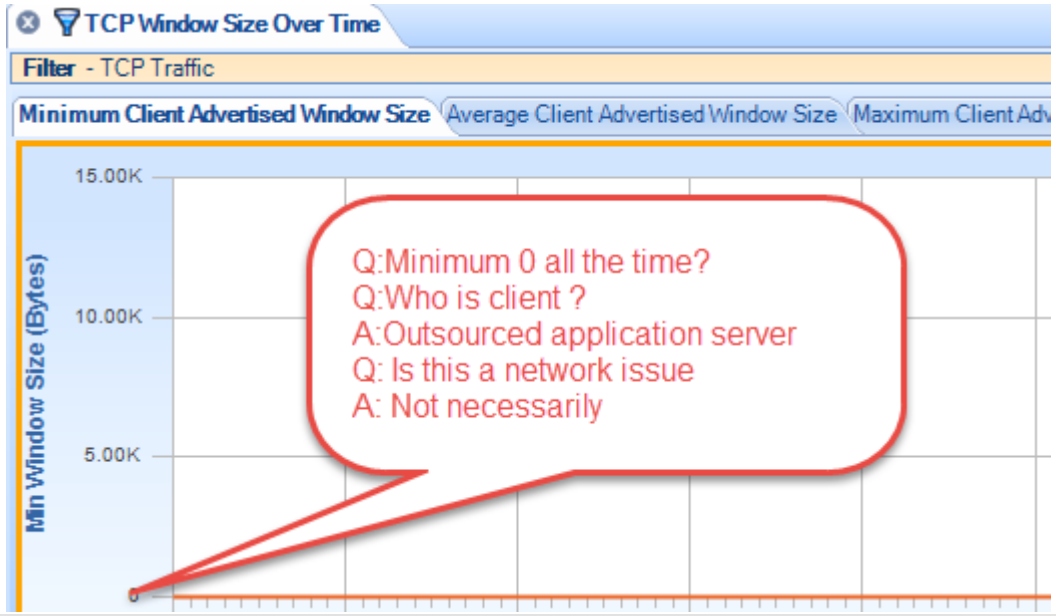
что увидел Riverbed APM (когда уломали...)

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA



исследуем отобранные пакеты в Packet Analyzer





проблема на уровне TCP (что опять сеть? не совсем)

И уж точно не на стороне Search Engine

Клиент (Новая разработка) постоянно сообщал о полном TCP буфере через ACK’s... всё время.

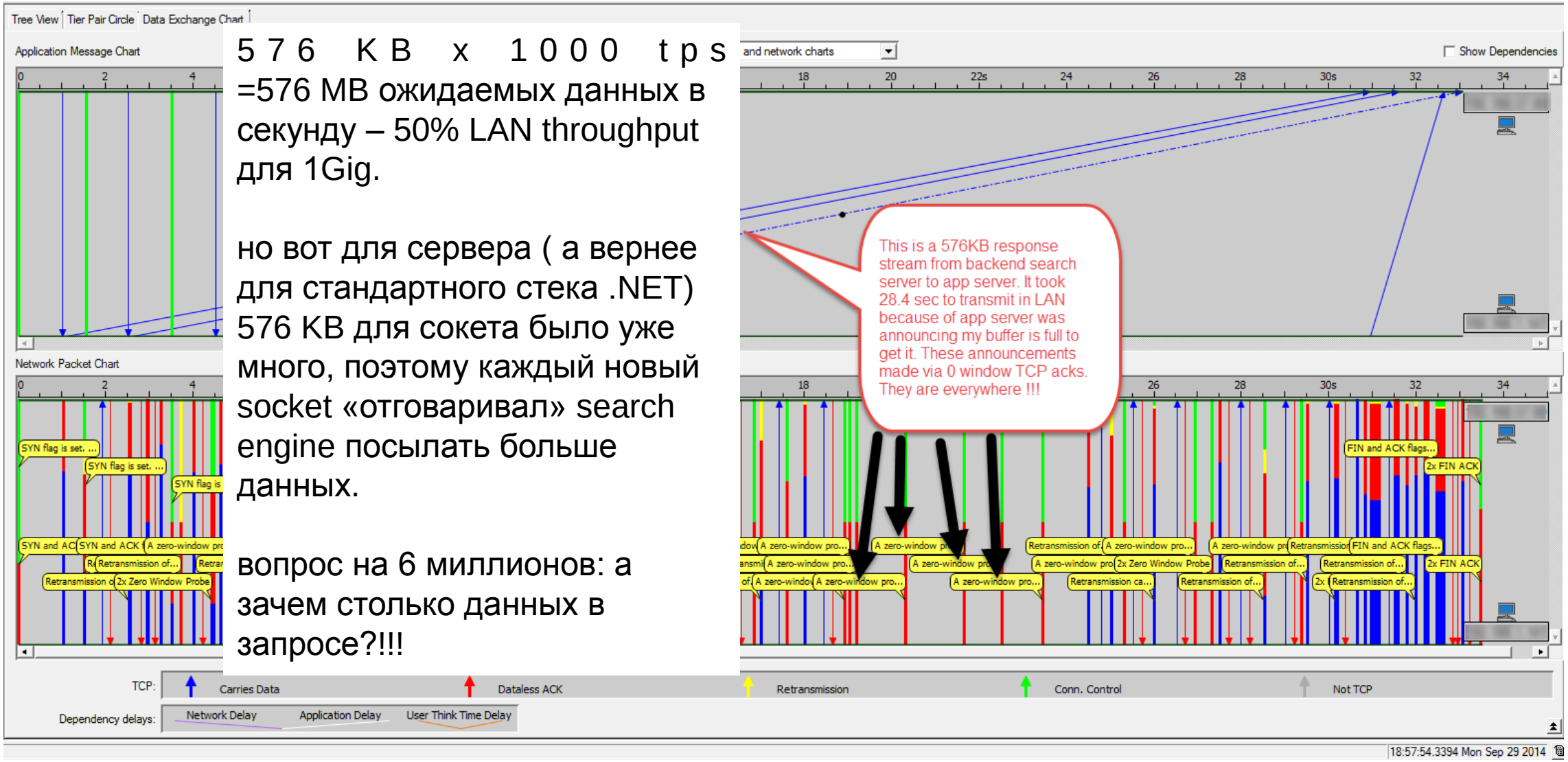
пора убедить разработчика используя Transaction Analyzer…

все что Transaction Analyzer знает о пакетах

5 7 6 K B x 1 0 0 0 t p s =576 MB ожидаемых данных в секунду – 50% LAN throughput для 1Gig.

но вот для сервера (а вернее для стандартного стека .NET) 576 KB для сокета было уже много, поэтому каждый новый socket «отговаривал» search engine посылать больше данных.

вопрос на 6 миллионов: а зачем столько данных в запросе?!!!



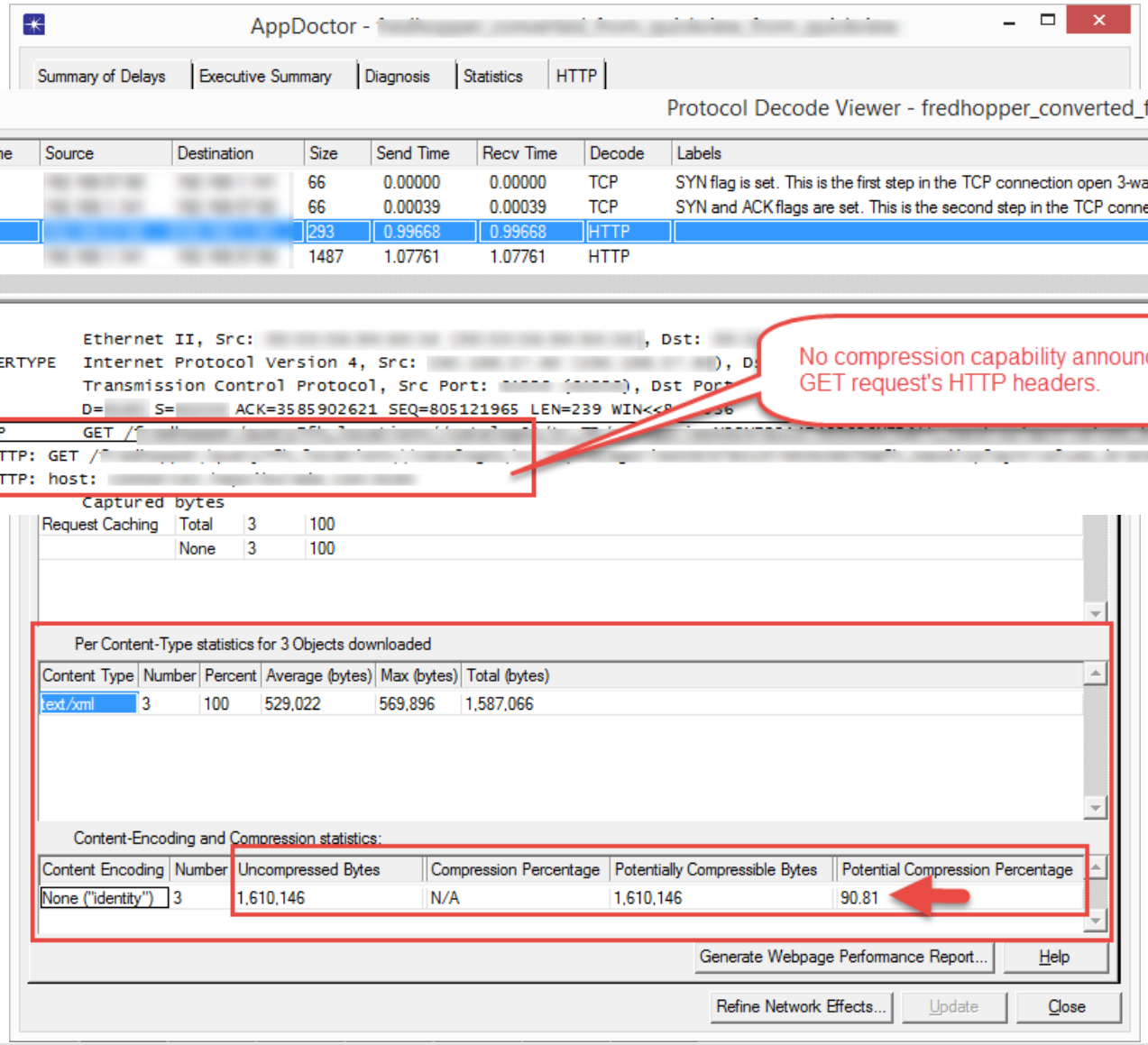
В нашей компании работает ни один Сисадмин и ни один не встречал проблему с размером данных в TCP. То что вы говорите чушь !!! Наш алгоритм не будет работать без всех этих данных, которые мы запрашиваем.

Mr. Knows Everything

Outsourcer Companies Military Grade Architect

но Transaction Analyzer знает даже больше...

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA



Ладно Бог с Вами и с Вашими данными, но в спецификации сказано что вы поддерживаете компрессию данных...?

Средства NPM

из чего состоит любой мониторинг

Net Flow

Мониторинг каналов с точки зрения прохождения трафика

SNMP

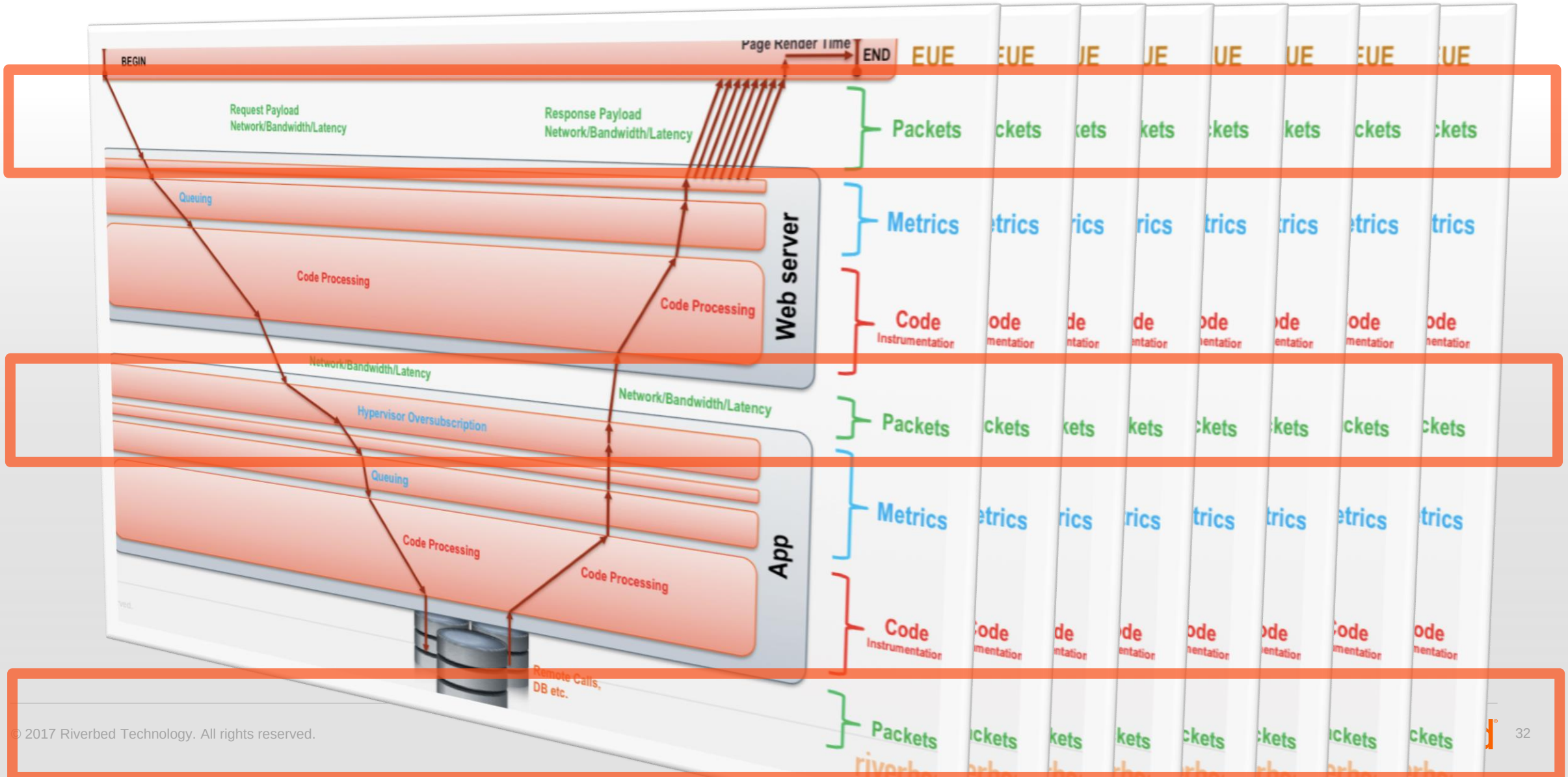
Взаимодействие с компонентами инфраструктуры

Пакеты

Детальный анализ сетевого трафика

NPM в реальной жизни

riverbed FORCE
FORCE FOR BUSINESS | RUSSIA

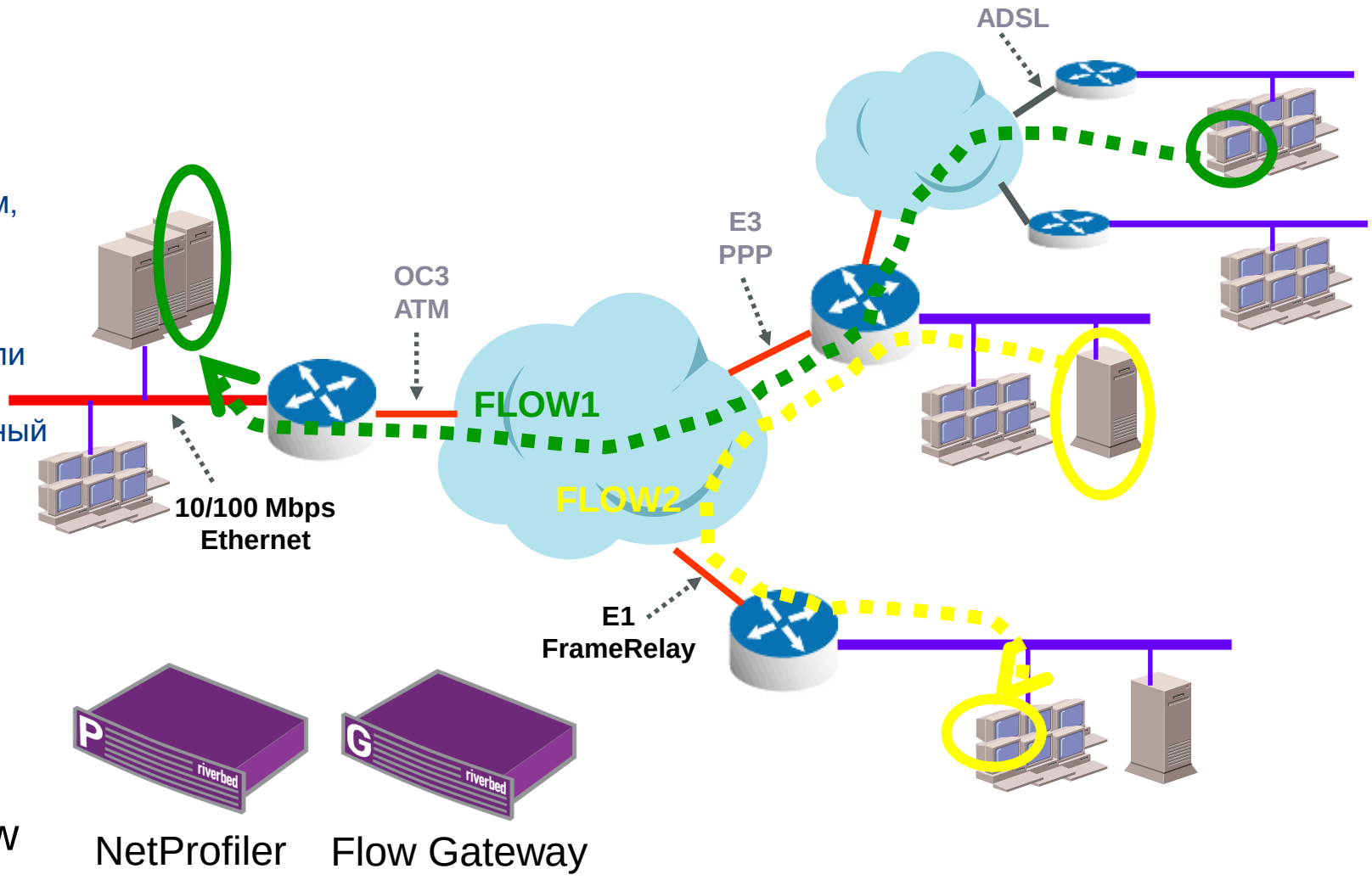


NetFlow only

Плюсы:
- Очень просто и доступно
- Недорого
- Информация об использовании сети (кем, чем, когда)

Минусы:
- Нет ответа на вопрос как быстро работали пользователи
- Интеллектуальные устройства + служебный трафик.
- Внесение изменений в конфигурацию устройств + доп. нагрузка на железо.
- Степень детализации обратно пропорциональна стоимости
- Количественный, но не качественный анализ трафика.

Riverbed NetProfiler –
Продукт для анализа NetFlow

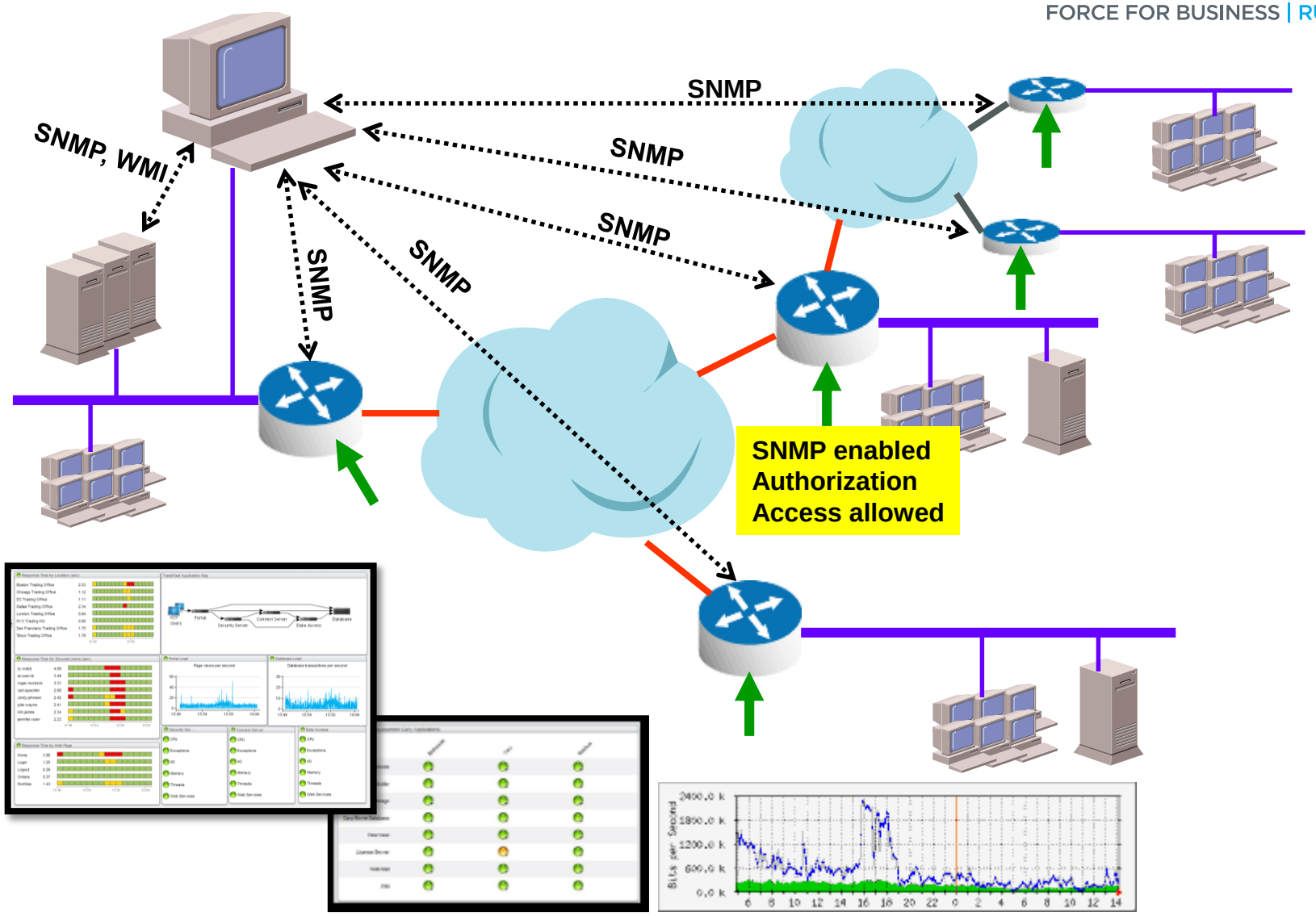


SNMP only

Плюсы:
- Очень просто дёшево и доступно
- Информация о поведении ключевых устройств
- Варьируемая степень детализации

Минусы:
- Служебный трафик + Служебный Доступ
- **Отсутствие понимания того, кто и что вызвало то или иное событие**
- **Усреднение показателей…**

Riverbed NetIM
Продукт для работы с компонентами инфраструктуры с использованием SNMP



Packets

Плюсы:
- Абсолютная полная видимость кто, что, куда, зачем
- Реальное время

Минусы:
- как и где перехватывать?
- ТОННЫ данных в которых надо уметь разбираться и где-то хранить?

Riverbed NetShark
Riverbed AppResponce eXperrt

Wireshark
PacketAnalyzer-
TransactionAnalyzer

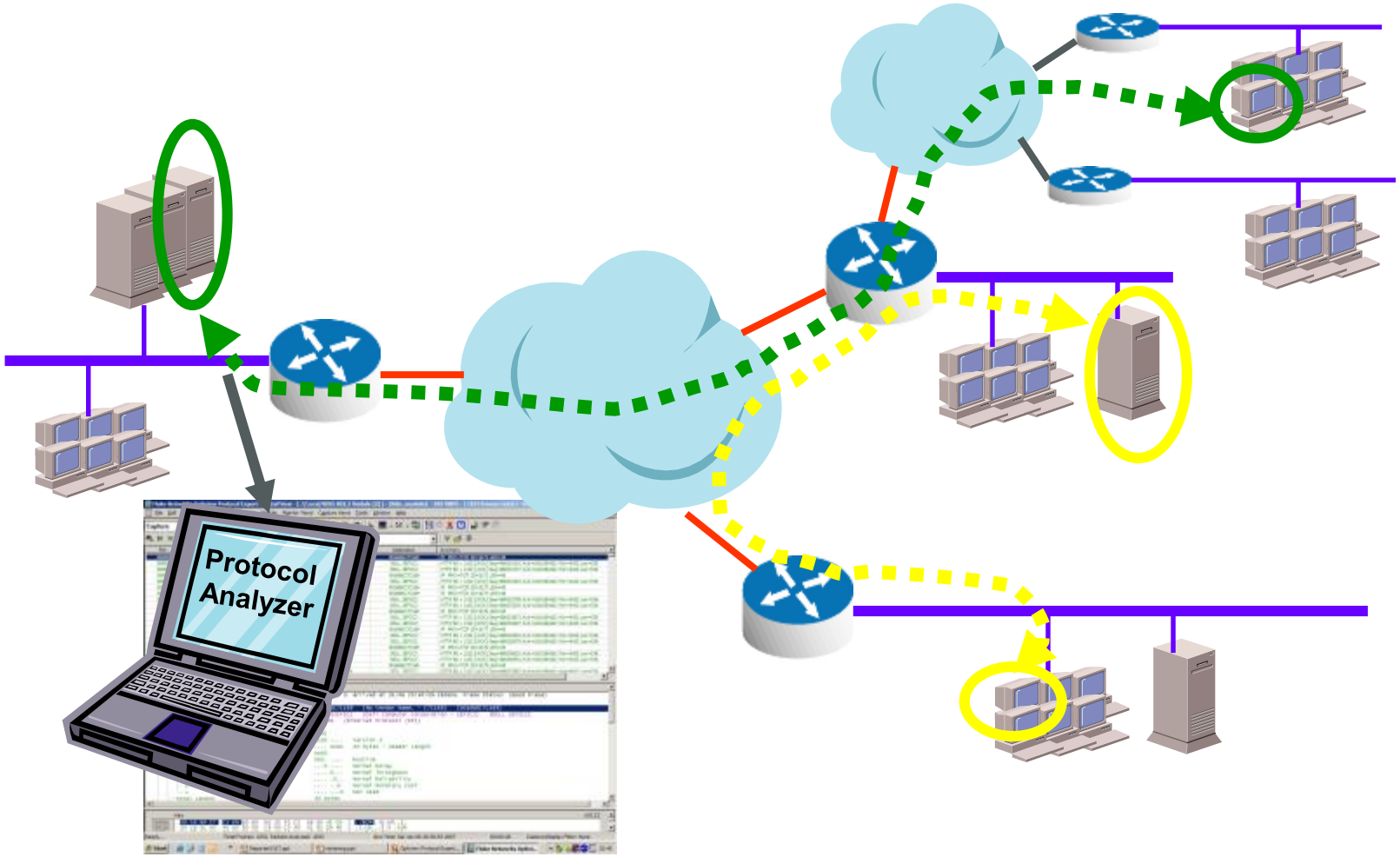
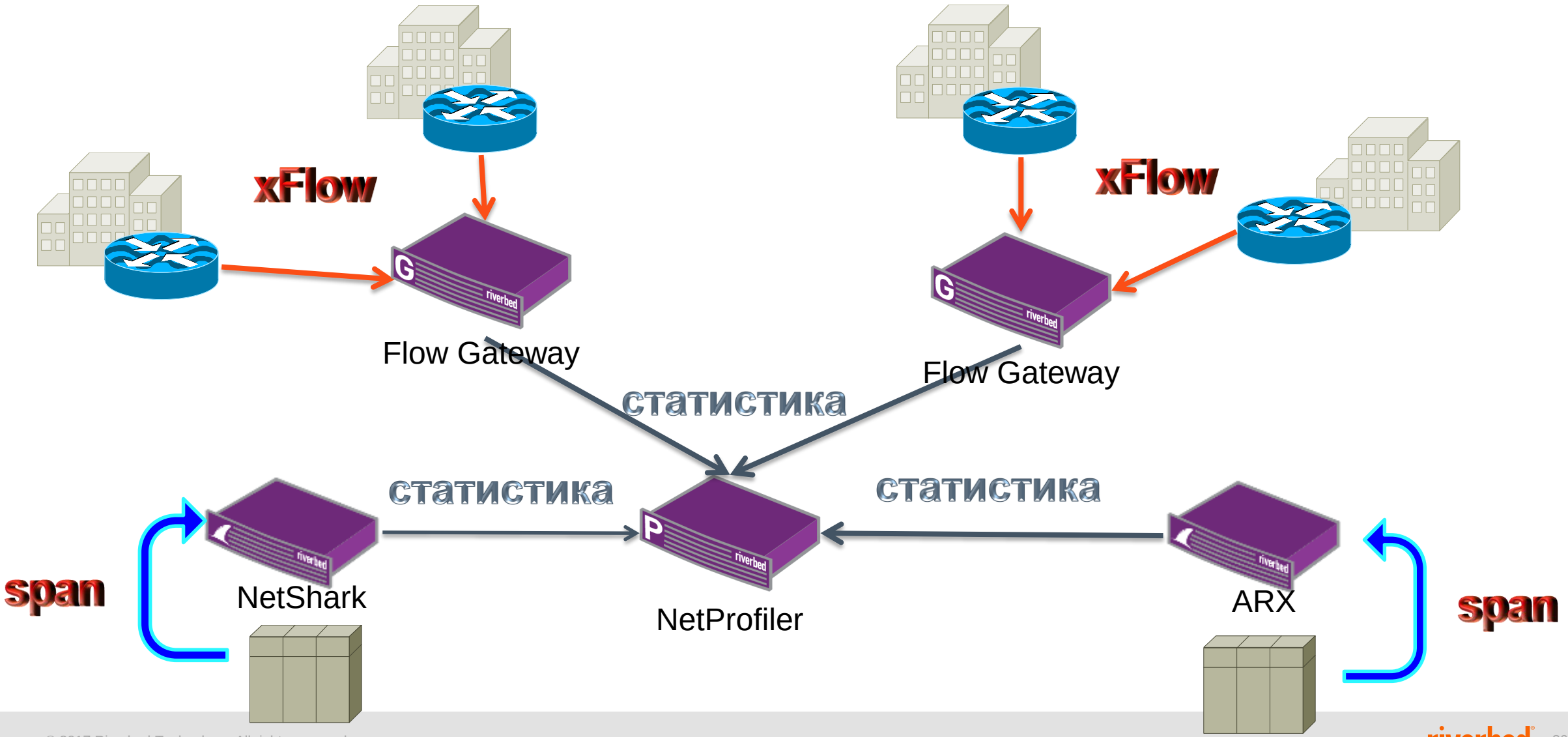


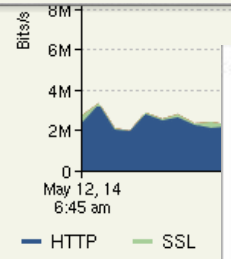
Схема Внедрения

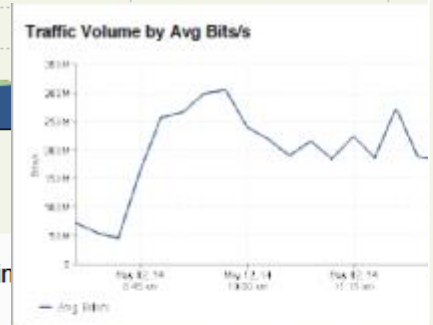


Service Health

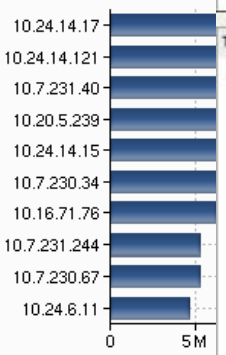
Service Tree

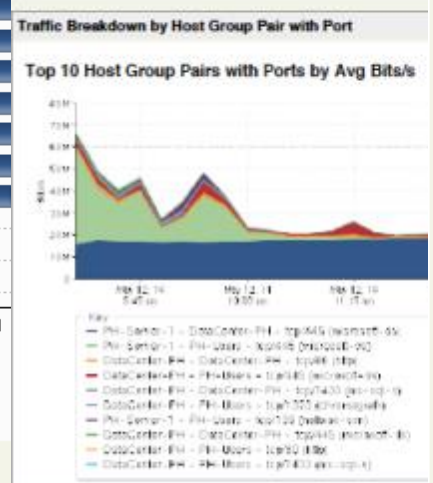
- PH-CIFS
  - Other-CIFS
  - CIFS-over-
  - RDP-over-
  - LDAP-over
    - Connec
    - User Ex
    - Efficien
  - Inner-CIFS





Hosts Starting 1 min





Ports Starting 1 min

tcp/445 (microsoft-ds)
tcp/1433 (ms-sql-s)
tcp/25 (smtp)
udp/4500 (ipsec-nat-t)
tcp/8080 (webcache)
tcp/80 (http)
tcp/3389 (ms-wbt-server)
tcp/1373 (chromagrafx)
tcp/6001 (x11)
tcp/389 (ldap)

Host Group Pair with Port 1 - 200 of 711

Server Group	Client Group	Port	
PH-Server-1	DataCenter-PH	tcp/445 (microsoft-ds)	17,456
PH-Server-1	PH-Users	tcp/445 (microsoft-ds)	5,411
DataCenter-PH	DataCenter-PH	tcp/80 (http)	1,156
DataCenter-PH	PH-Users	tcp/445 (microsoft-ds)	809
DataCenter-PH	DataCenter-PH	tcp/1433 (ms-sql-s)	512
DataCenter-PH	PH-Users	tcp/1373 (chromagrafx)	419
PH-Server-1	PH-Users	tcp/139 (netbios-ssn)	215
DataCenter-PH	DataCenter-PH	tcp/445 (microsoft-ds)	202
DataCenter-PH	PH-Users	tcp/80 (http)	64
DataCenter-PH	PH-Users	tcp/1433 (ms-sql-s)	53
DataCenter-PH	DataCenter-PH	tcp/389 (ldap)	42
DataCenter-PH	DataCenter-PH	tcp/5989 (wbem-https)	28
DataCenter-PH	DataCenter-PH	tcp/1352 (lotusnote)	23
DataCenter-PH	DataCenter-PH	tcp/443 (https)	18
DataCenter-PH	DataCenter-PH	tcp/3268 (msft-gc)	18
DataCenter-PH	PH-Users	tcp/1352 (lotusnote)	16
DataCenter-PH	PH-Users	tcp/25 (smtp)	15
DataCenter-PH	PH-Users	tcp/1025 (blackjack)	6

Service Maps

Other-CIFS

Other-CIFS-Clie

RDP-over-

span

EndUs

Service Even

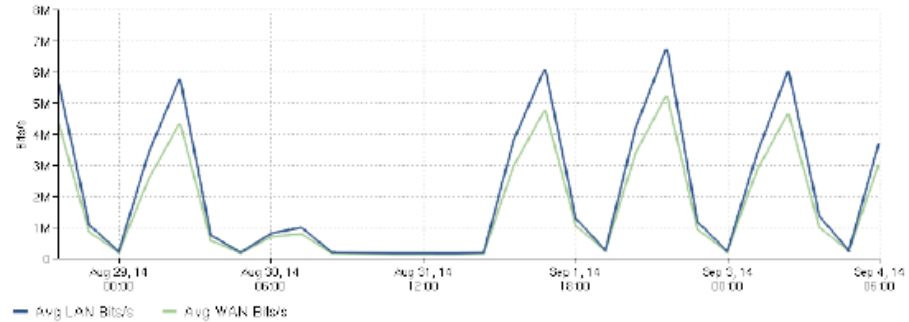
Event ID	Alert L

40 High 88 Service PH-CIFS > LDAP-over-L

riverbed Traffic on interface-group /WAN/Optimized.

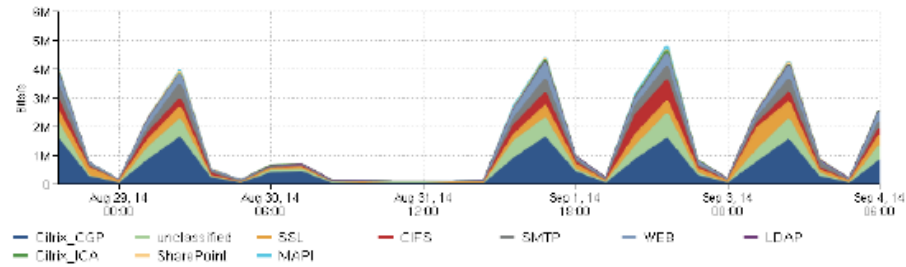
Overall Traffic

Traffic Volume by Avg LAN Bits/s, Avg WAN Bits/s



Inbound Traffic Breakdown by Application

Top 10 Inbound Applications by Avg WAN Bits/s



Inbound Traffic by Application 1 - 200 of 360

Application	Avg LAN Bits/s		Avg WAN Bits/s		% Reduct - Avg Bits	% Reduct - Total Packets	Reduct - Total Bits		Avg Net. RTT (ms)
WEB	297,146	(15%)	149,743	(9%)	49.61%	0%	89,149,374,464	(34%)	24
SMTP	271,941	(13%)	152,973	(10%)	43.75%	0%	71,951,974,400	(27%)	18
Citrix_CGP	589,757	(29%)	501,332	(31%)	14.99%	0%	53,479,432,192	(20%)	34
SharePoint	42,813	(2%)	16,260	(1%)	62.02%	40%	16,059,179,008	(6%)	27
CIFS	175,472	(9%)	153,436	(10%)	12.56%	0%	13,327,785,984	(5%)	16
IPP	8,231	(< 1%)	362.22	(< 1%)	95.60%	82%	4,759,166,456	(2%)	26
WebDav-HTTP	9,986	(< 1%)	3,282	(< 1%)	67.14%	49%	4,054,670,752	(2%)	29
Citrix_ICA	21,948	(1%)	16,809	(1%)	23.42%	0%	3,108,397,056	(1%)	26
NetBIOS_Session_service-CIFS	5,814	(< 1%)	1,256	(< 1%)	78.40%	0%	2,756,748,632	(1%)	29
unclassified	244,708	(12%)	240,742	(15%)	1.62%	0%	2,398,355,456	(< 1%)	19
Google_Analytics-HTTP	5,009	(< 1%)	2,224	(< 1%)	55.60%	4%	1,684,487,736	(< 1%)	31
web_proxy	6,868	(< 1%)	4,090	(< 1%)	40.46%	0%	1,680,457,392	(< 1%)	38
Google-HTTP	7,543	(< 1%)	4,866	(< 1%)	35.49%	0%	1,618,932,224	(< 1%)	26
Rambler.ru-HTTP	3,469	(< 1%)	1,463	(< 1%)	57.82%	2%	1,213,171,216	(< 1%)	30
Doubleclick-HTTP	4,130	(< 1%)	2,204	(< 1%)	46.64%	0%	1,164,957,432	(< 1%)	32

Не верите… Попробуйте сами!

» NetExpress – 30 дней

Всё-в-одном NPM (версия для VMware)

» Packet Analyzer – 30 дней

+ захват пакетов NetShark (версия для VMware)

для тестирования с использованием аппаратных платформ обратитесь к нашим партнёрам

riverbed®

FORCE™

FORCE FOR BUSINESS | RUSSIA