Методы инспекции пакетов и анализа трафика

Лекция 5
Архитектура расположения DPI в сети оператора связи

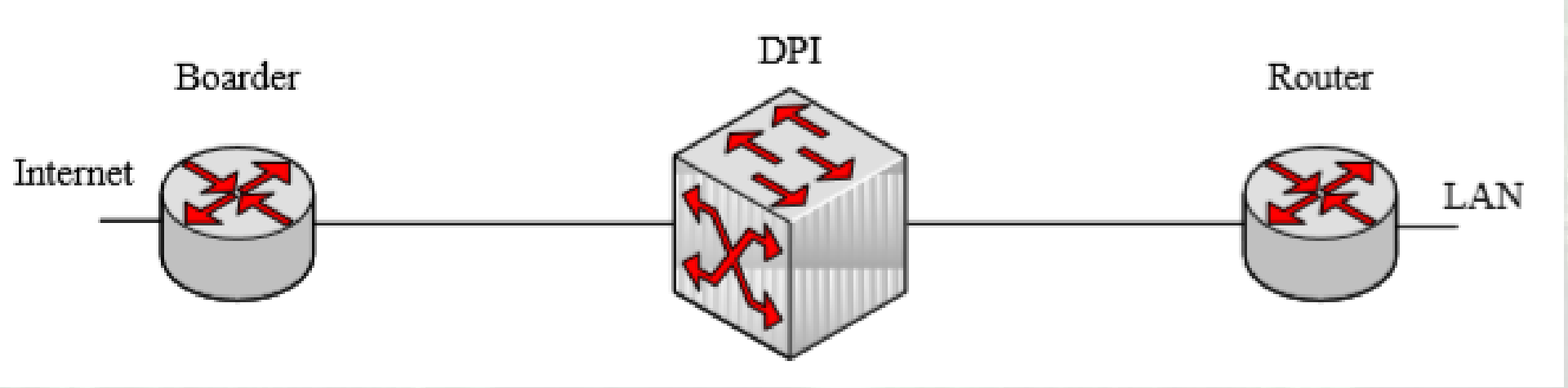
Фицов Вадим Владленович

ст.преп. кафедры ИКС

Содержание лекции:

- Архитектура расположения DPI
- Применение DPI в сети оператора связи
- DPI as Service
- Таргетированная реклама

Арихитектура расположения DPI на сети оператора связи



4

Три типа включения DPI:

- Зеркалирование
- «в разрыв»
- Bypass

Зеркалирование

Зеркалирование (mirroring) дублирует весь сетевой поток канала:
- первая копия идет непосредственно в сеть,
- вторая отправляется на вход системы анализа.

При такой схеме, в отсутствие обратной связи от системы анализа, может выполняться только пассивный анализ,

т. е. система не может влиять на трафик, попадающий в сеть

(например, путем фильтрации или приоретезации).

6

«в Разрыв»

Подключение «в разрыв», когда весь поток направляется на систему, которая становится посредником во всех взаимодействиях WAN и LAN.

Такое подключение вносит дополнительные риски при выходе системы анализа из строя,

- в результате поломки
- целенаправленной сетевой атаки

локальная сеть остается без связи с глобальной.

Bypass

Bypass является гибридным подходом между зеркалированием и подключением «в разрыв»

решает проблему выхода из строя системы анализа.

В нормальных условиях система работает в режиме подключения «в разрыв»,

однако при ее выходе из строя или получении от нее соответствующего сигнала соединение с LAN выполняется напрямую.

8

Bypass

В настоящее время такой вид подключения наиболее распространен

для решений, которым требуется активный анализ, т. е. возможность изменять содержимое передаваемого трафика в соответствии с некоторыми политиками

(блокировать запрашиваемые ресурсы, ограничивать скорость и т. д.).

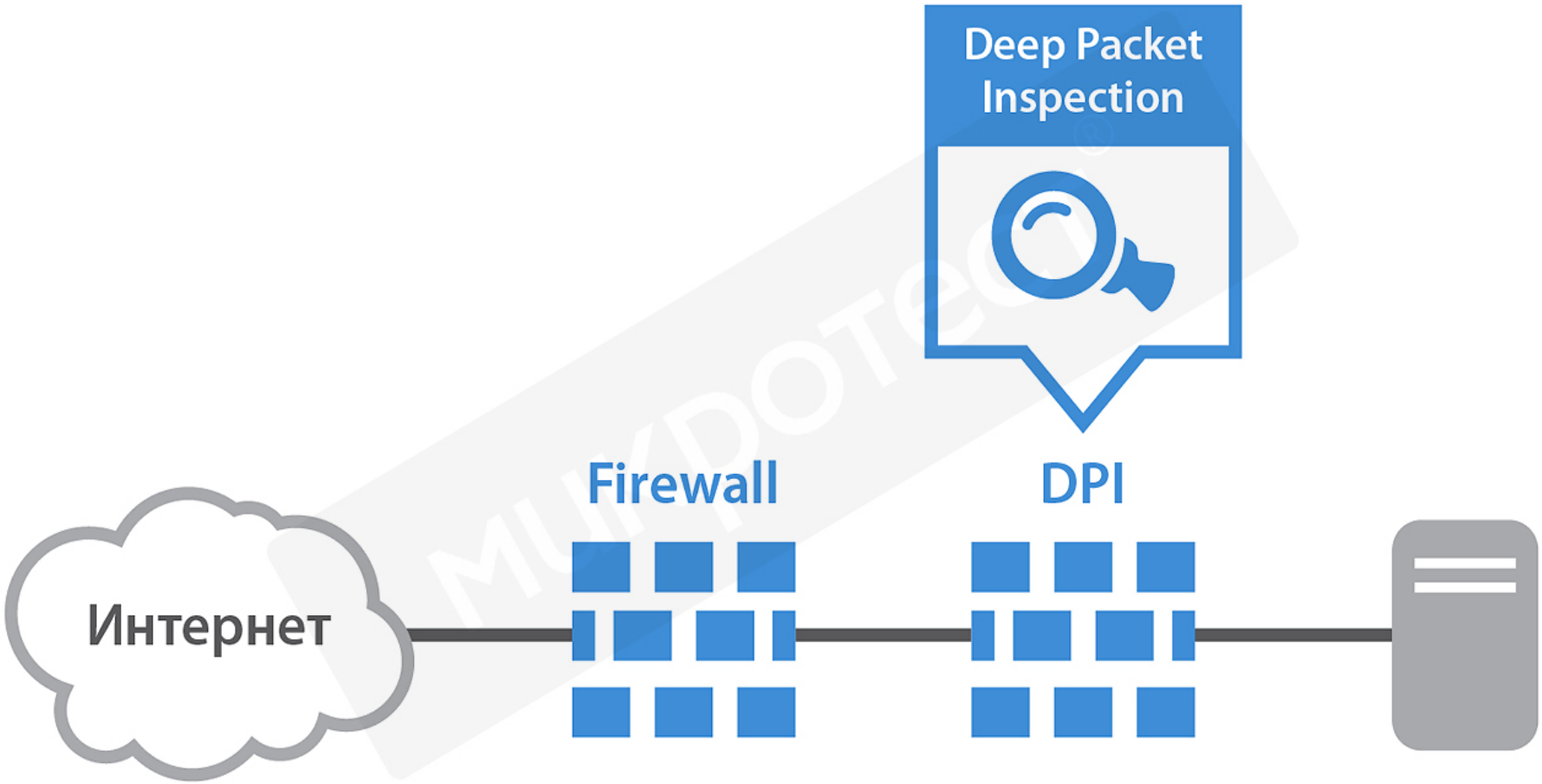
9

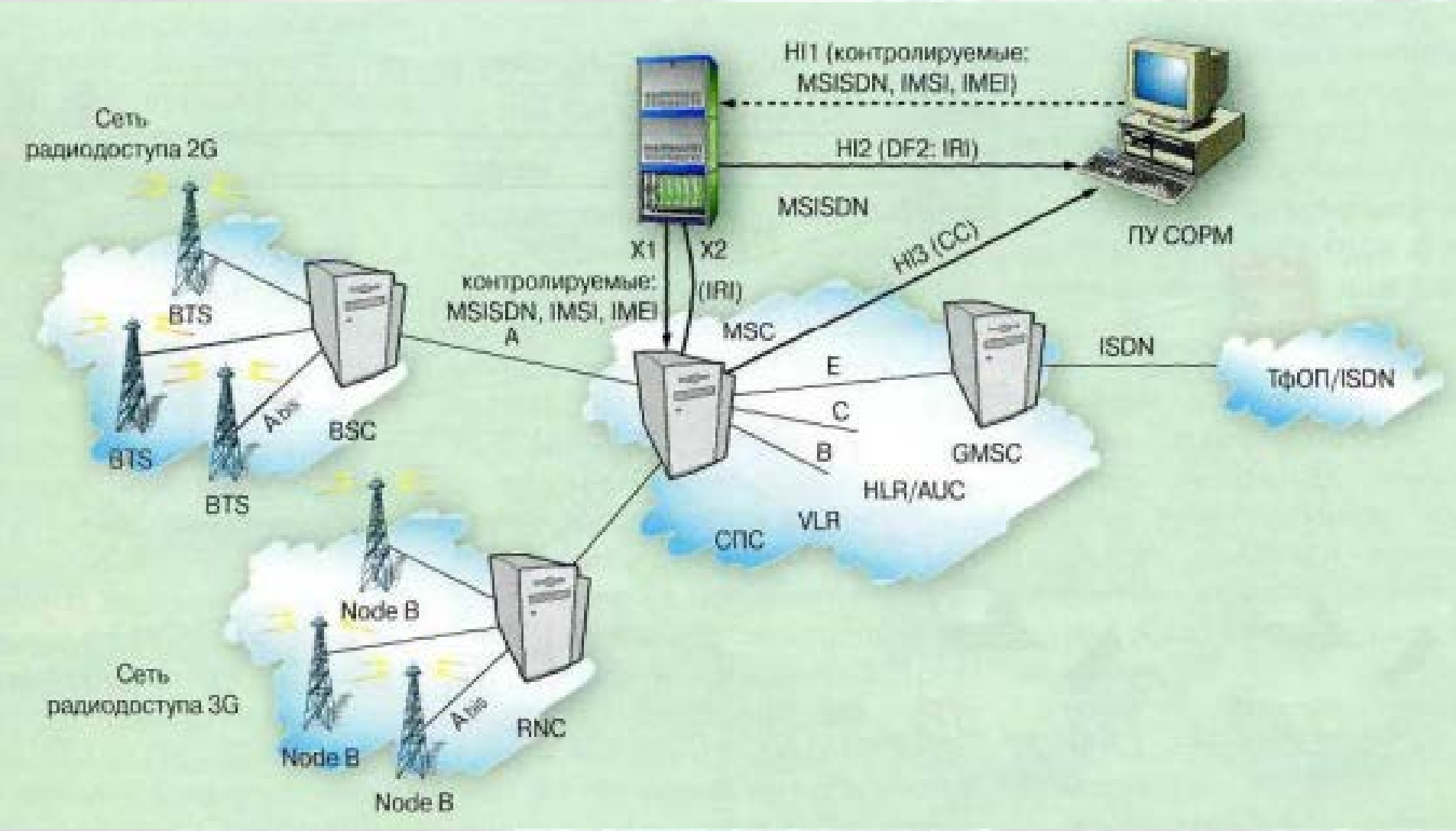
Что вместо Bypass?

Распределенная система
SDN подход

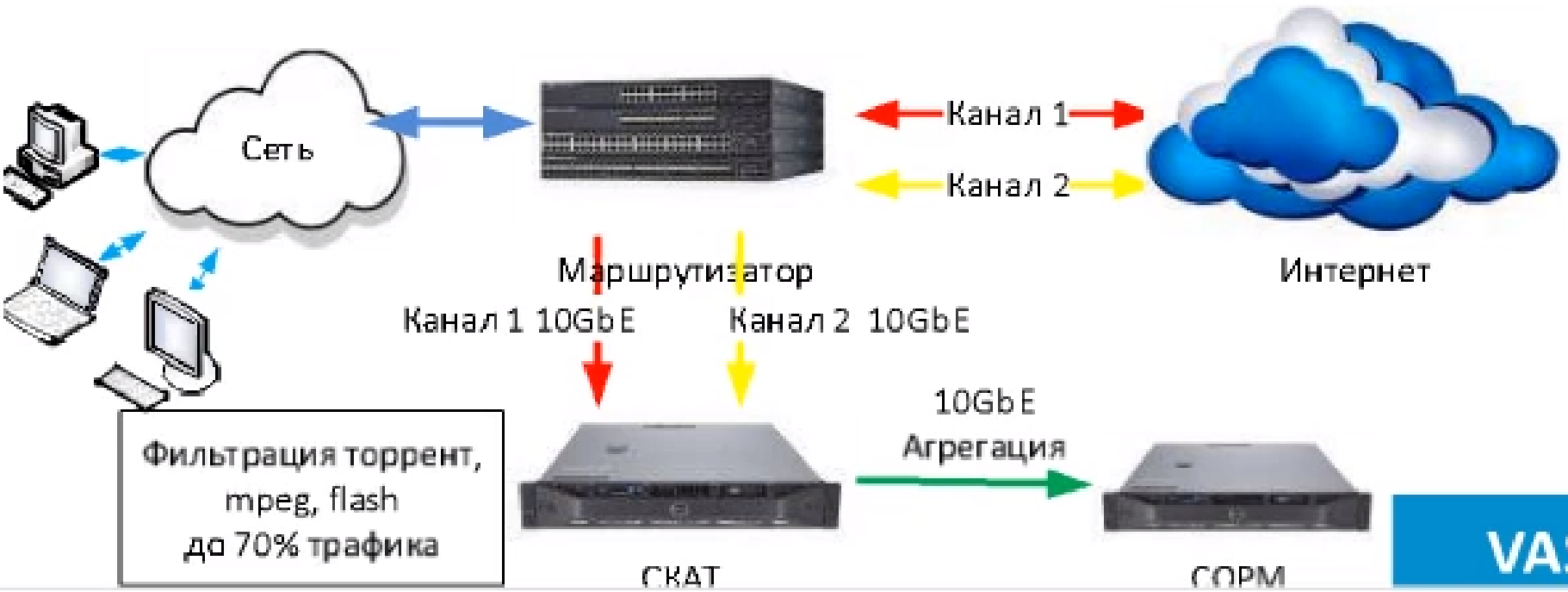
Декомпозиция анализа и
фильтрации

10

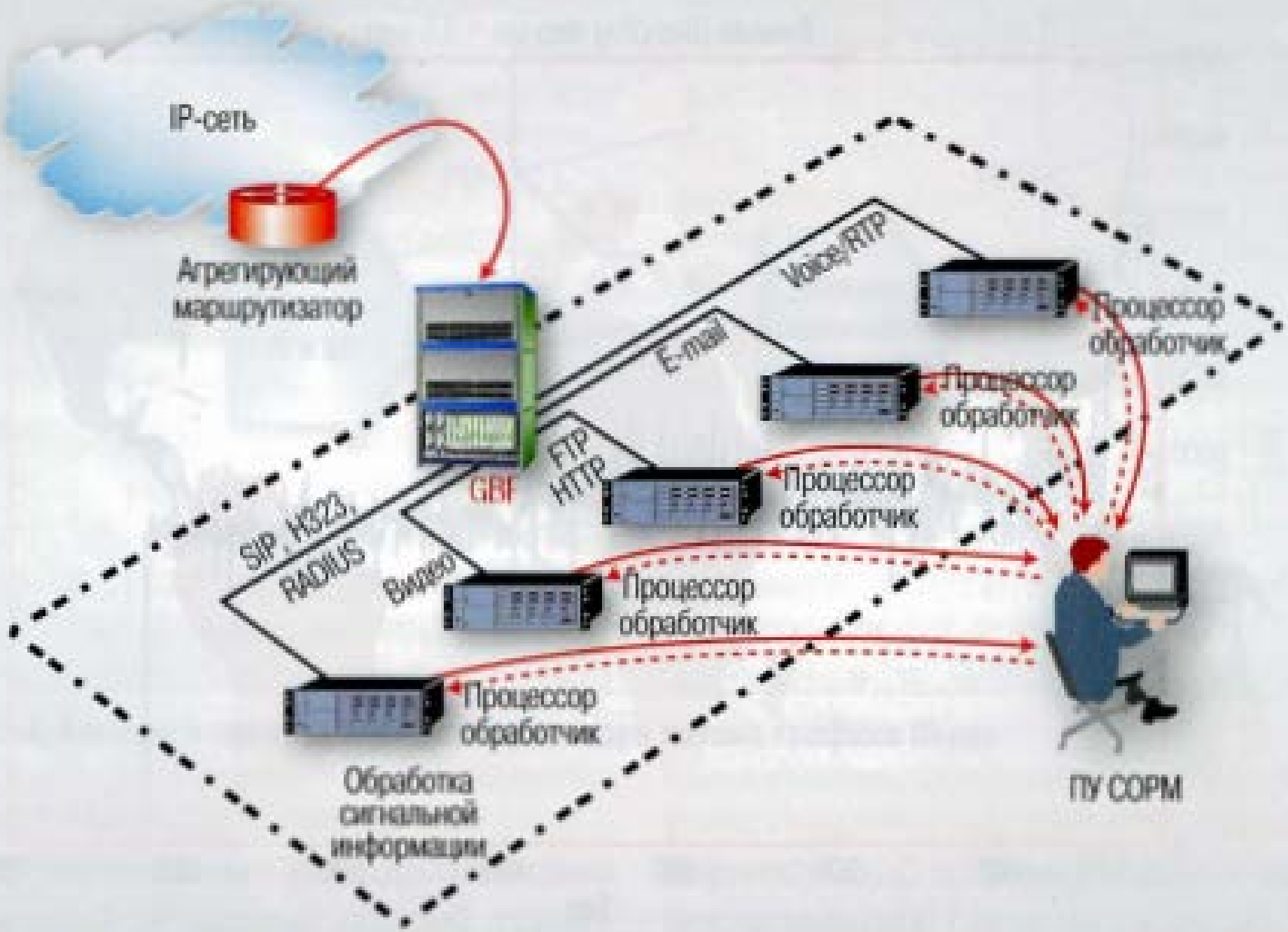

Deep Packet Inspection
Firewall
DPI
Интернет


HI1 (контролируемые:
MSISDN, IMSI, IMEI)
HI2 (DF2: IRI)
MSISDN
ПУ СОРМ
HI3 (CC)
Сеть
радиодоступа 2G
X1
X2
контролируемые:
MSISDN, IMSI, IMEI
A
(IRI)
MSC
ISDN
ТфОП/ISDN
BTS
BTS
BTS
Abis
BSC
E
C
B
GMSC
HLR/AUC
VLR
СПС
Node B
Сеть
радиодоступа 3G
Node B
Node B
Abis
RNC

X.25, V.2A
Центр перехвата
CCC/CDC
Устройство посредника
HI2
HI3
HI1
Probe - точка съема
SIP, H.323
RTP
RTP
RTP
Транспортная сеть
SBC
AS
CSCF
HSS
Ядро IMS
Медиа-шлюз
ТфОП


Сеть
Канал 1
Канал 2
Интернет
Маршрутизатор
Канал 1 10GbE
Канал 2 10GbE
10GbE
Агрегация
Фильтрация торрент,
mpeg, flash
до 70% трафика
СКАТ
СОРМ
VAS

14


IP-сеть
Агрегирующий маршрутизатор
GRE
Voice/RTP
E-mail
FTP
HTTP
SIP, H323, RADIUS
Видео
Процессор обработчик
Процессор обработчик
Процессор обработчик
Процессор обработчик
Процессор обработчик
Обработка сигнальной информации
ПУ СОРМ

15

DPI подсистемы получения данных делятся:

- распределенные
- беспроводные
- локальные.

16

Распределенная система состоит из

• сборщиков данных о сетевом трафике (**probes**)

• и набора его анализаторов (**collectors**), которые получают данные от сборщиков.

В беспроводных системах

отсутствует «канал» типа точка–точка,
что позволяет перехватывать беспроводные коммуникации в достаточно большом радиусе.

Например, Wireless intrusion prevention system (WIPS).

17

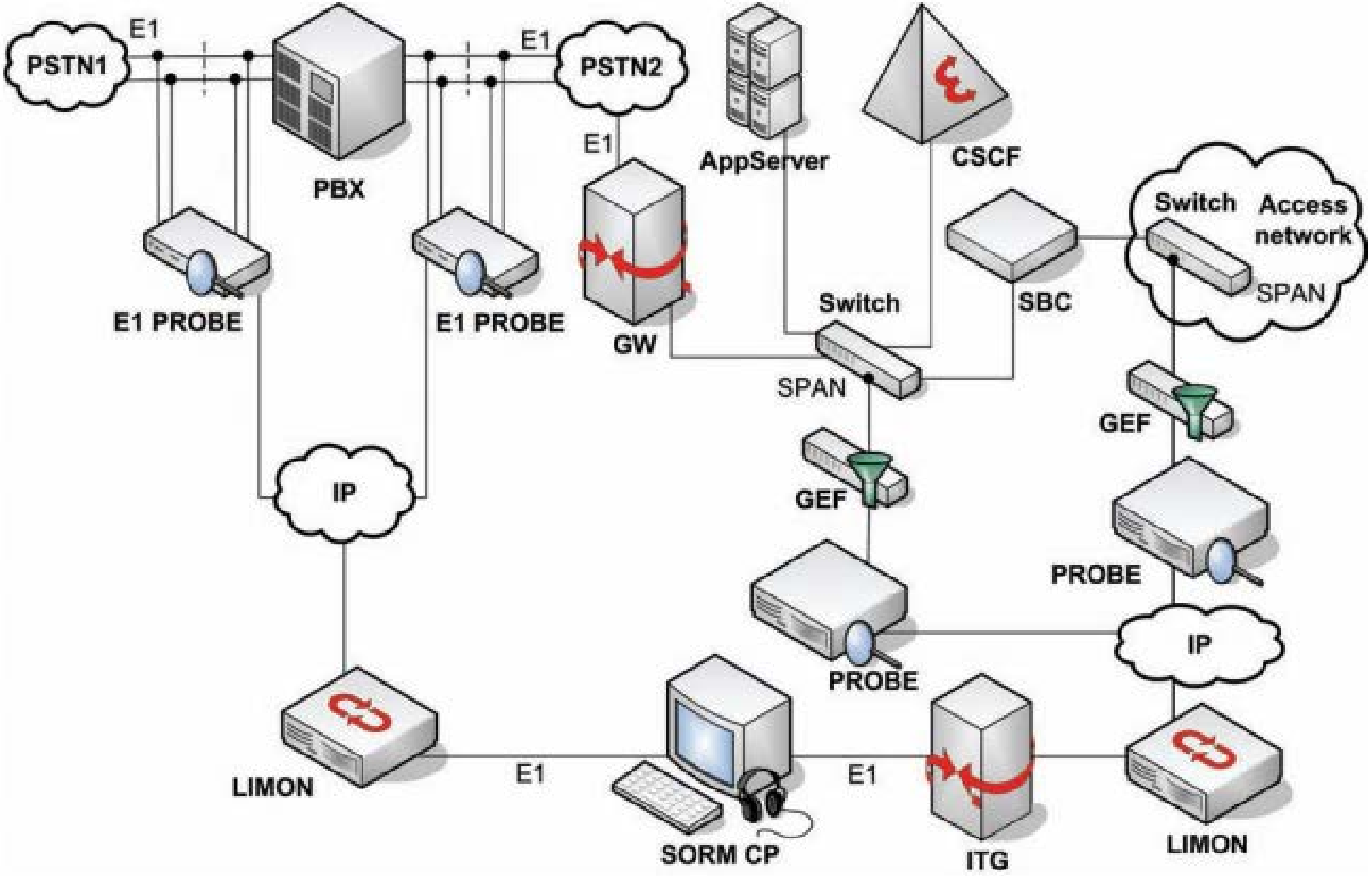
Локальные системы
подключаются к конкретному **каналу** передачи данных (сетевому кабелю).

• на стороне **конечного пользователя** (сетевая карта) (host-based intrusion prevention system (HIPS))

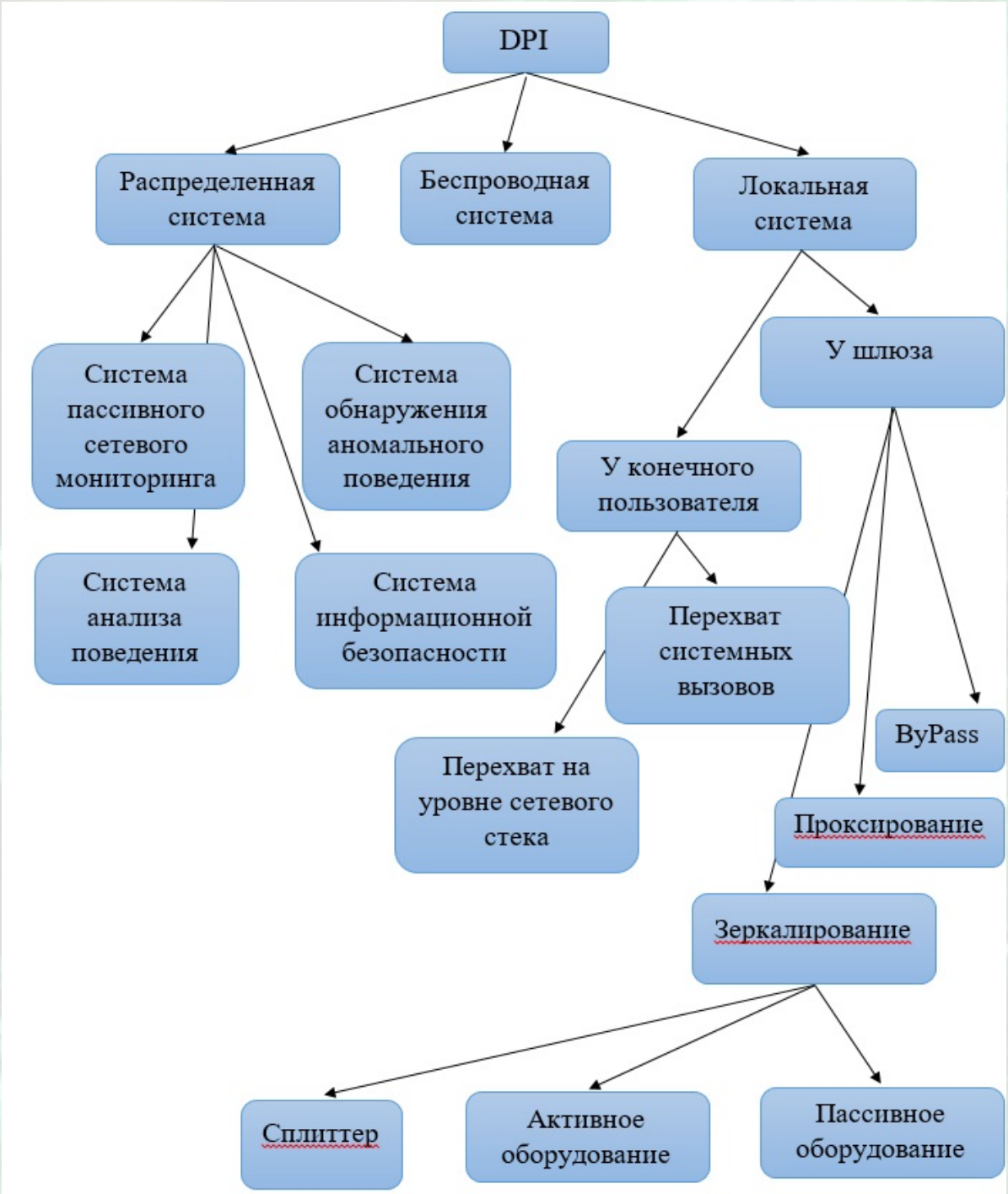
• или у **шлюза (WAN)**.
Если шлюзов НЕСКОЛЬКО:
-может наблюдаться ситуация с «**односторонними потоками**»
(когда, например, исходящий трафик некоторого соединения идет через один шлюз, а входящий – через другой).
(«сетевой асимметрией» (network assymetry).)

- либо созданы условия для «**двусторонних потоков**».

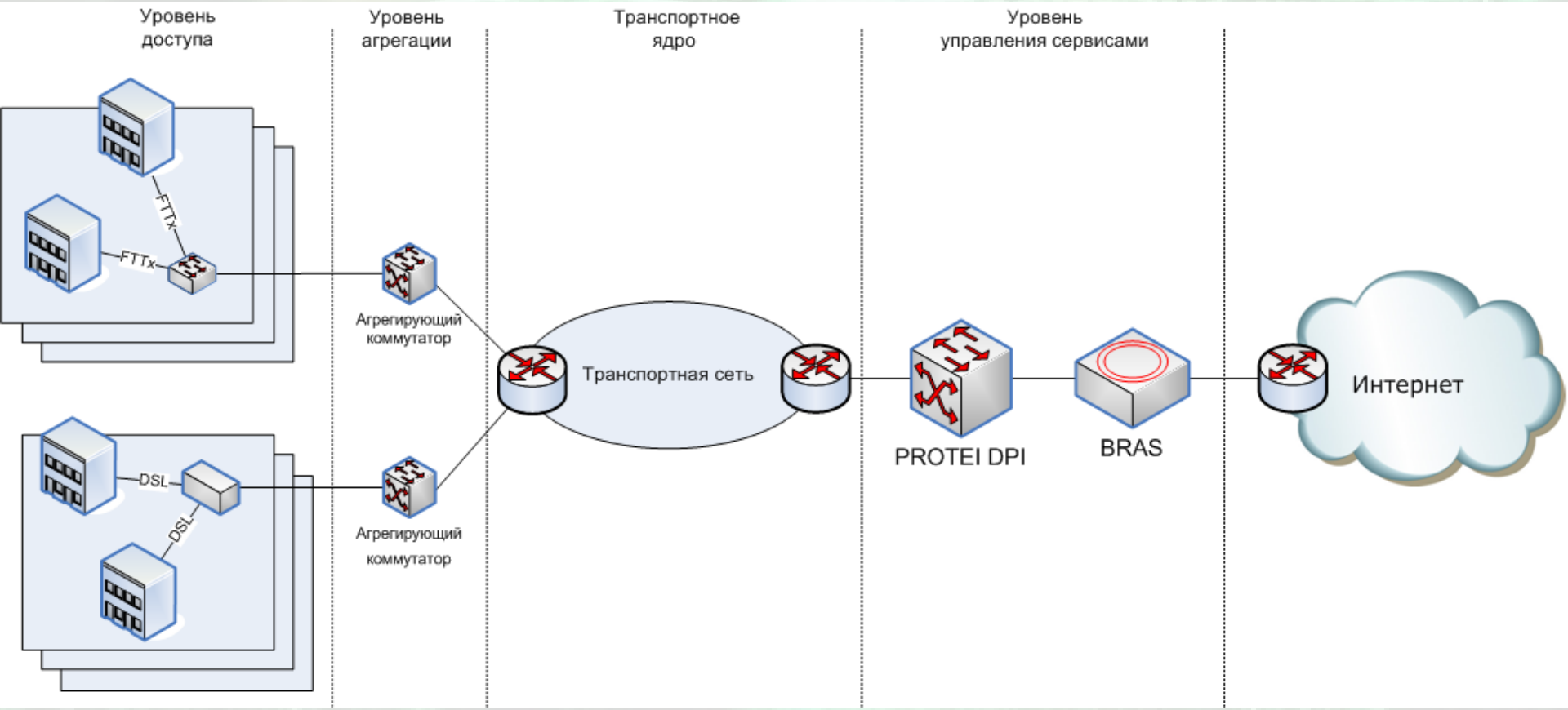
18

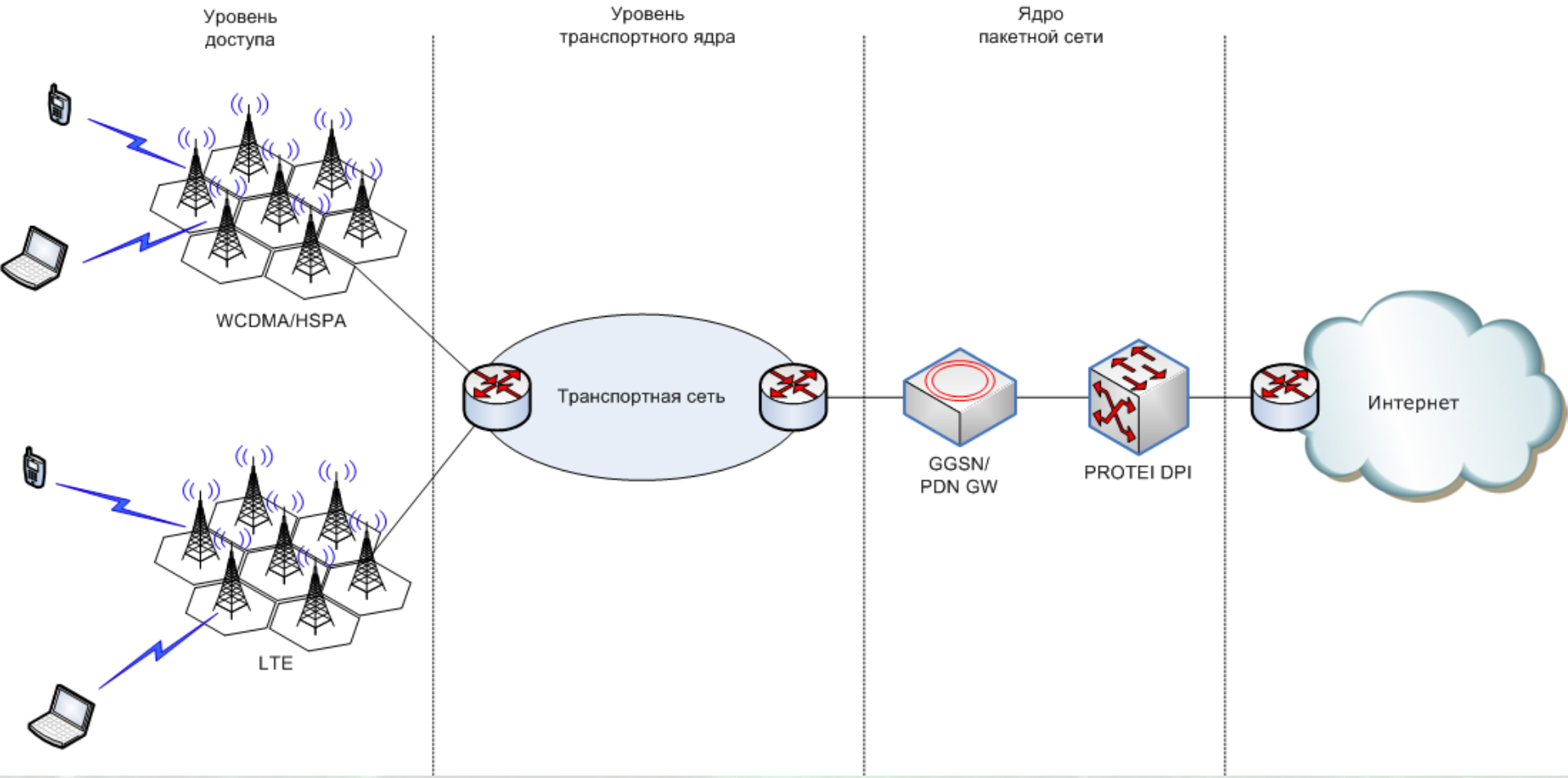

PSTN1
E1
PBX
E1
PSTN2
E1
AppServer
CSCF
Switch
Access network
SPAN
SBC
E1 PROBE
E1 PROBE
GW
Switch
SPAN
GEF
GEF
IP
PROBE
PROBE
IP
LIMON
E1
SORM CP
E1
ITG
LIMON

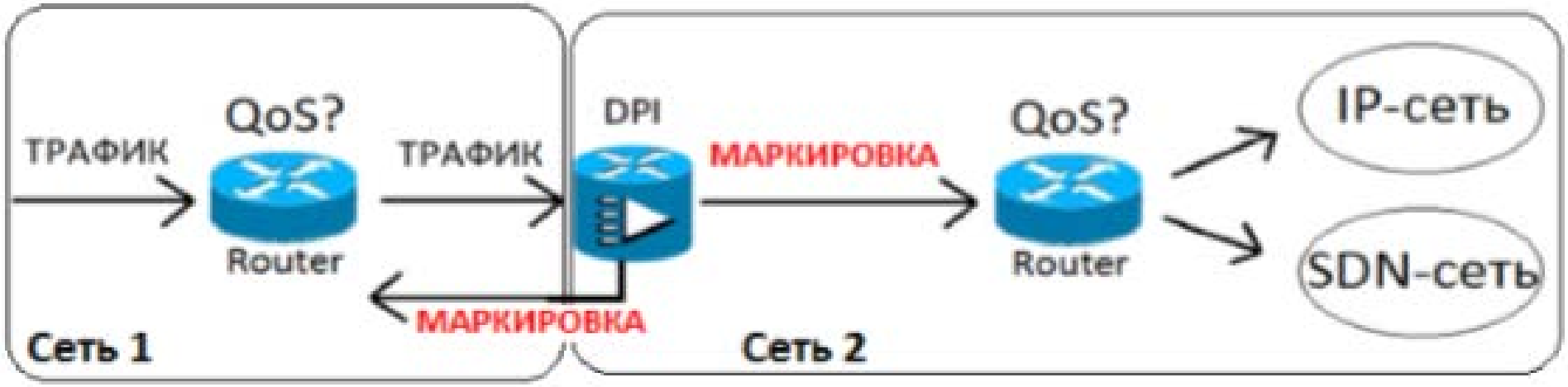
19


DPI
Распределенная система
Беспроводная система
Локальная система
Система пассивного сетевого мониторинга
Система обнаружения аномального поведения
У шлюза
У конечного пользователя
Система анализа поведения
Система информационной безопасности
Перехват системных вызовов
ByPass
Перехват на уровне сетевого стека
Проксирование
Зеркалирование
Сплиттер
Активное оборудование
Пассивное оборудование

20

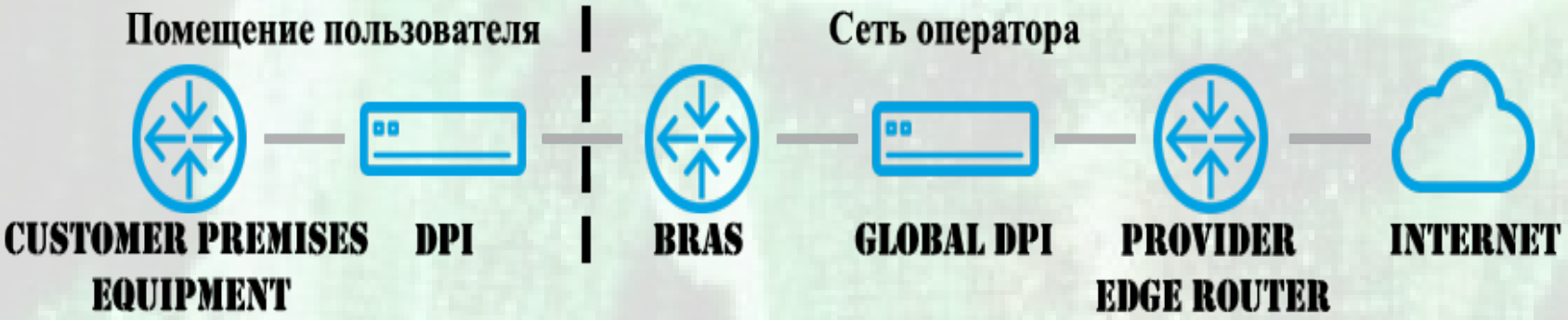

Уровень доступа
Уровень агрегации
Транспортное ядро
Уровень управления сервисами
FTTx
FTTx
Агрегирующий коммутатор
Транспортная сеть
PROTEI DPI
BRAS
Интернет
DSL
DSL
Агрегирующий коммутатор


Уровень доступа
Уровень транспортного ядра
Ядро пакетной сети
WCDMA/HSPA
LTE
Транспортная сеть
GGSN/ PDN GW
PROTEI DPI
Интернет


ТРАФИК
QoS?
Router
ТРАФИК
DPI
МАРКИРОВКА
QoS?
Router
IP-сеть
SDN-сеть
МАРКИРОВКА
Сеть 1
Сеть 2

23

Аппаратное решение



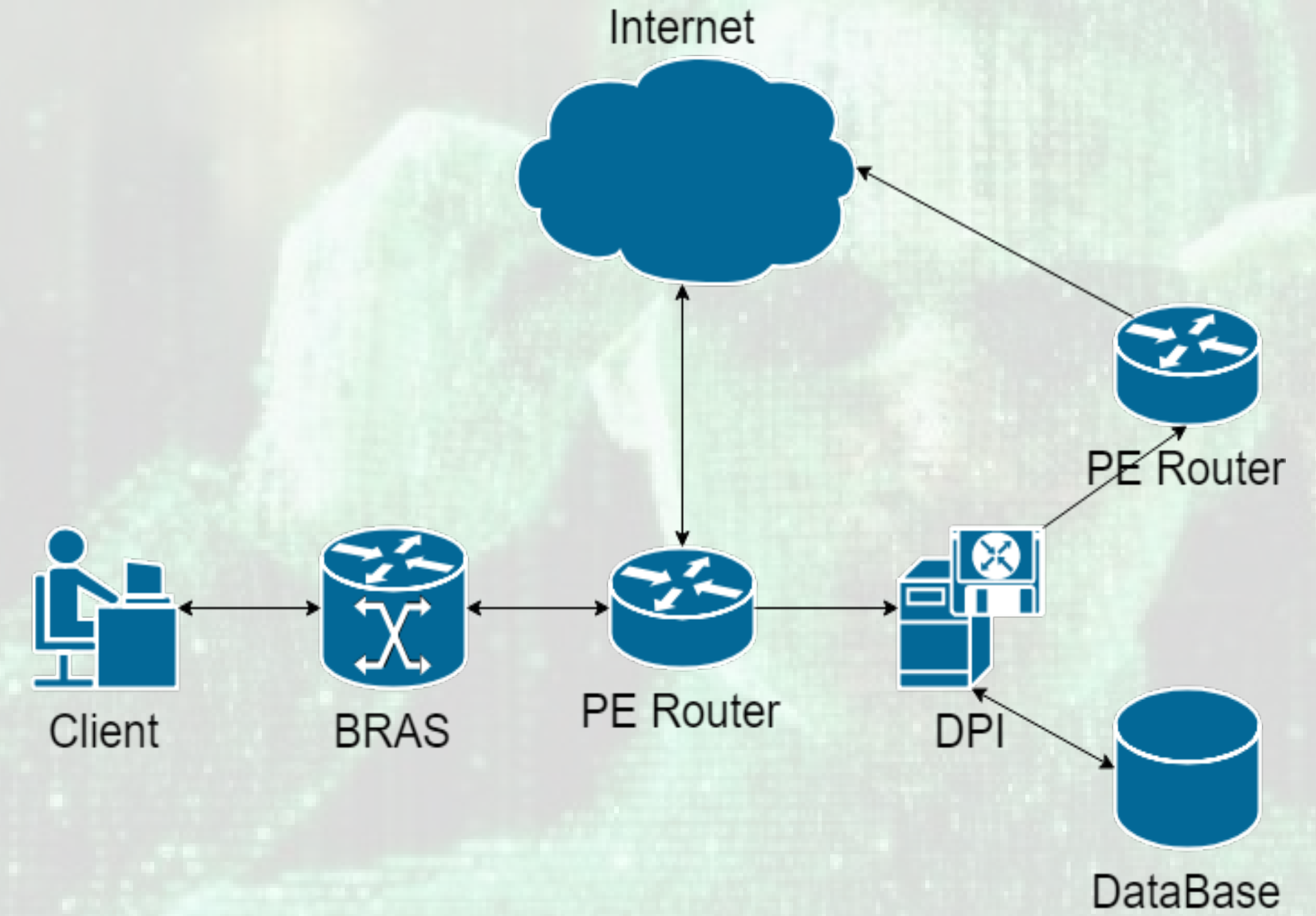
Достоинства:

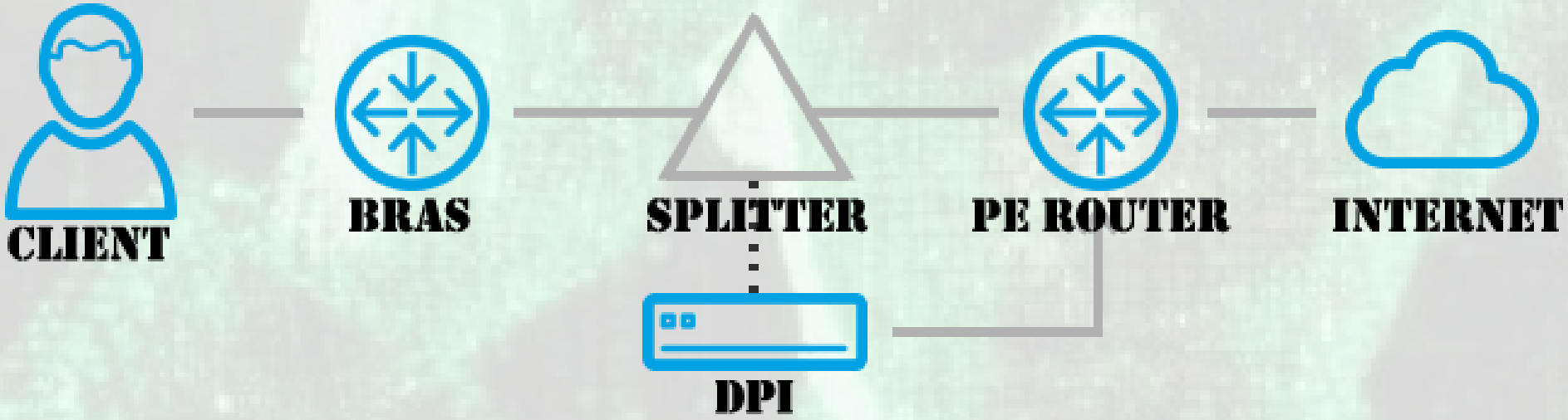
- Сокращение нагрузки на сеть оператора связи
- Более эффективный анализ трафика
- Усиленная защита от нежелательного контента

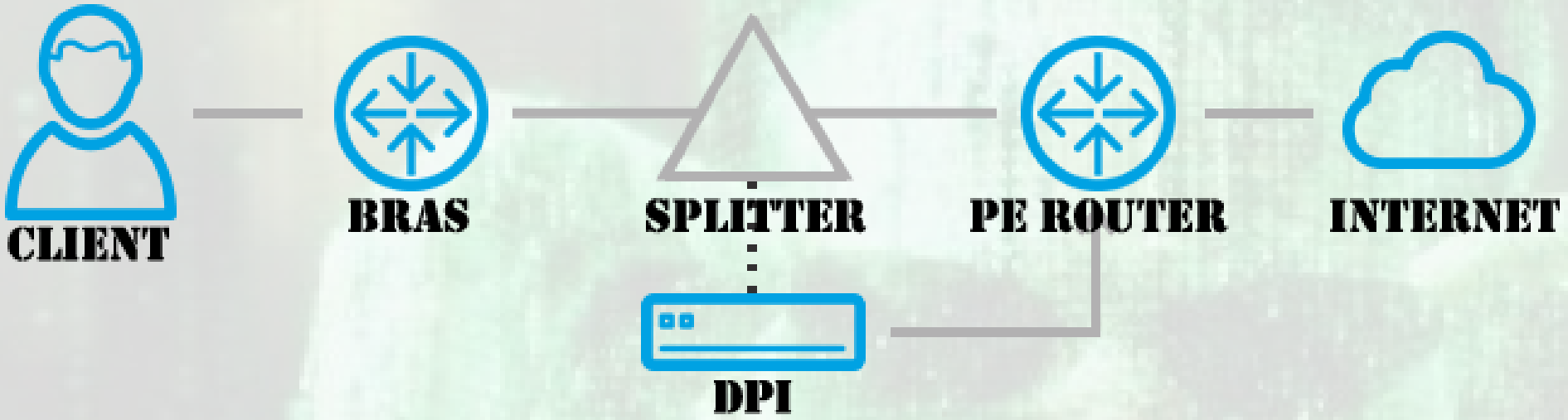
Недостатки:

- Увеличение числа различных устройств в сети
- Увеличение задержки


Помещение пользователя
Сеть оператора
CPE
DPI
BRAS
GLOBAL DPI
PE ROUTER
INTERNET

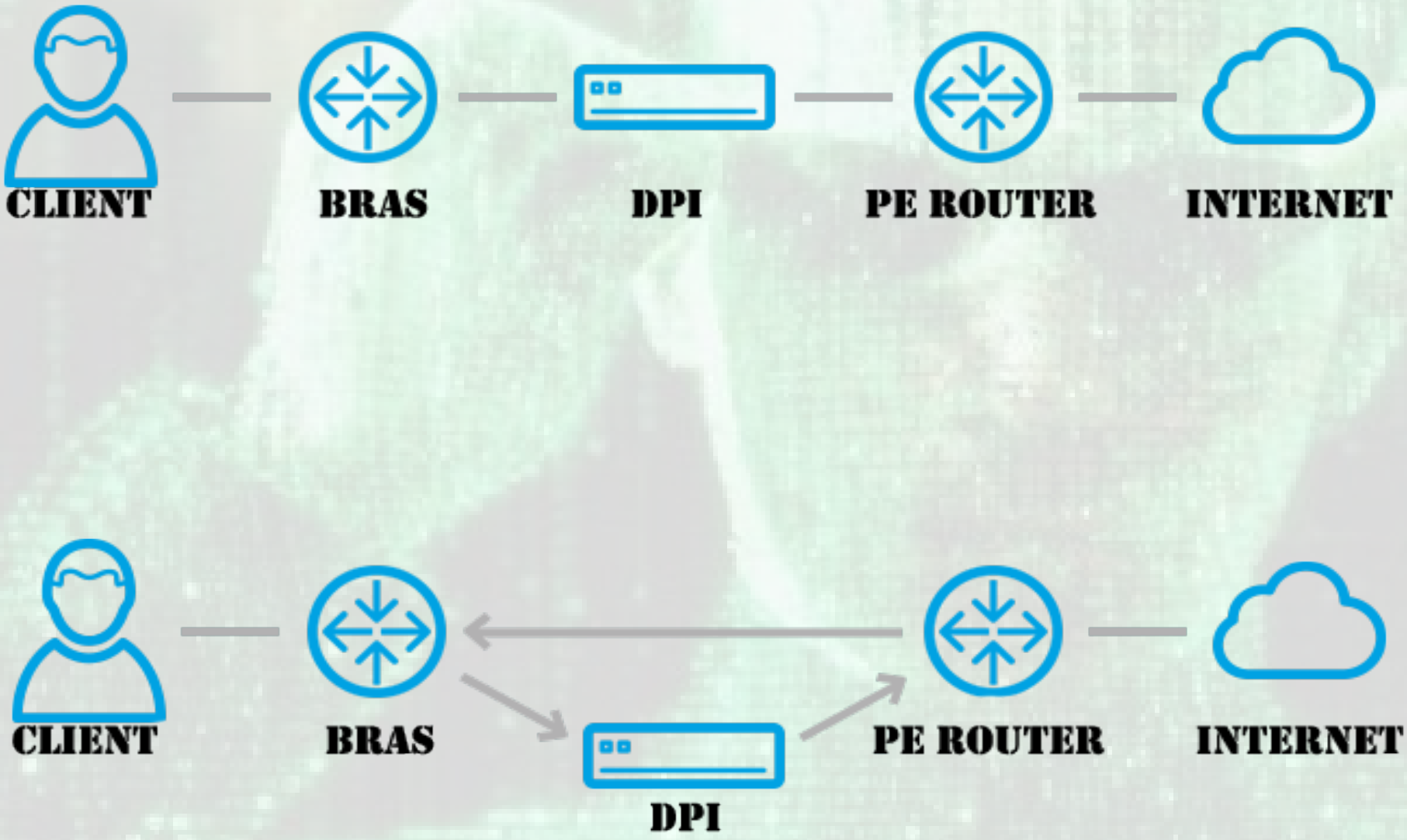

Internet
PE Router
Client
BRAS
PE Router
DPI
DataBase


CLIENT
BRAS
SPLITTER
PE ROUTER
INTERNET
DPI

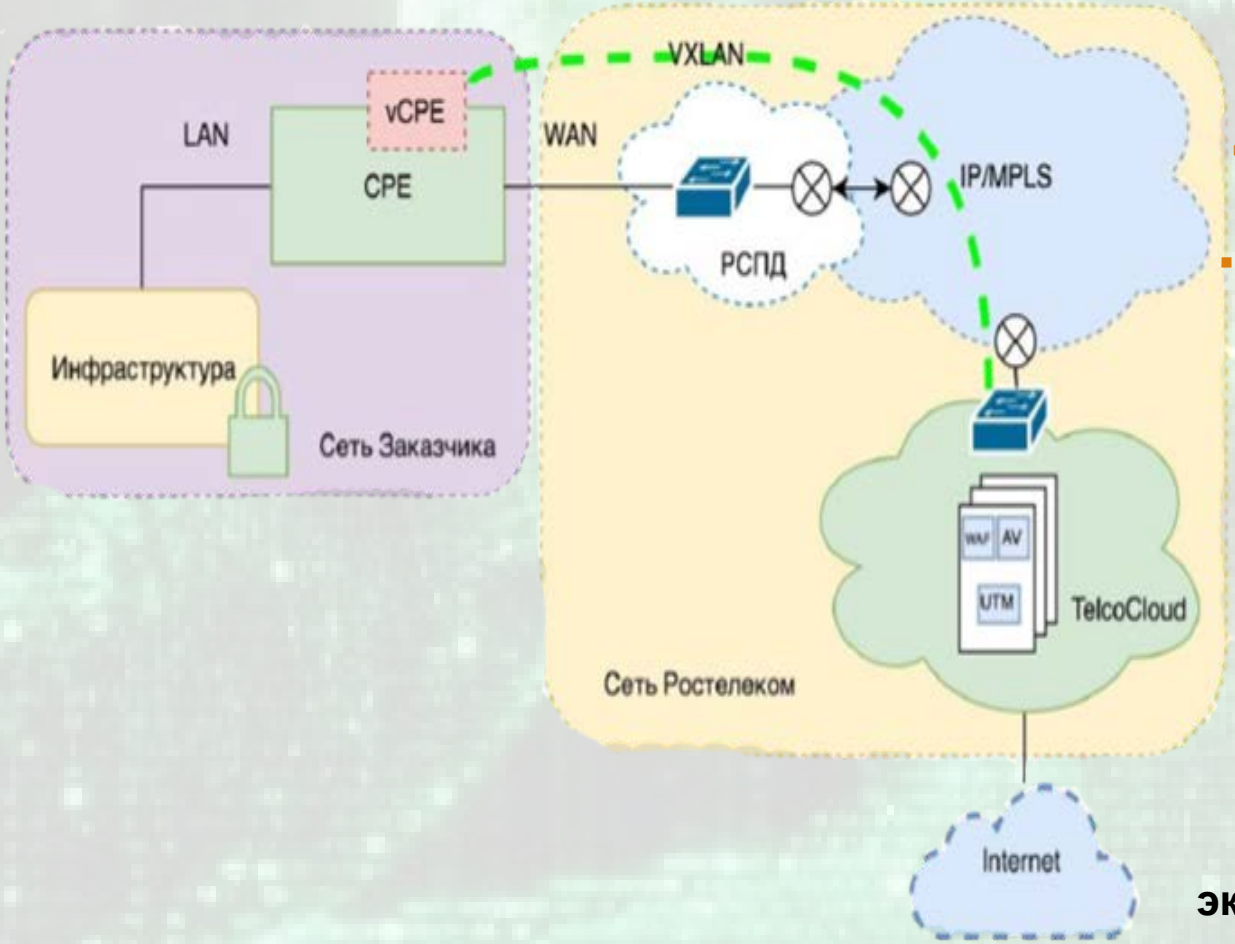


No.	Time	Source	Destination	Protocol	Length	Info
3	0.039411	192.168.5.10	195.82.146.214	TCP	54	51886 → 80 [ACK] Seq=1 Ack=1 Win=29200 Le
4	0.039531	192.168.5.10	195.82.146.214	HTTP	131	GET / HTTP/1.1
5	0.044808	195.82.146.214	192.168.5.10	HTTP	190	HTTP/1.1 302 Found ← Ответ от DPI
6	0.044814	192.168.5.10	195.82.146.214	TCP	54	51886 → 80 [ACK] Seq=78 Ack=137 Win=3001
7	0.079010	195.82.146.214	192.168.5.10	TCP	60	80 → 51886 [ACK] Seq=1 Ack=78 Win=14600 L
8	0.079015	192.168.5.10	195.82.146.214	TCP	54	[TCP Dup ACK 6#1] 51886 → 80 [ACK] Seq=78
9	0.079121	195.82.146.214	192.168.5.10	TCP	436	[TCP Out-Of-Order] 80 → 51886 [PSH, ACK]
10	0.079125	192.168.5.10	195.82.146.214	TCP	54	[TCP ACKed unseen segment] 51886 → 80 [AC
11	3.063369	192.168.5.10	195.82		54	51886 → 80 [FIN, ACK] Seq=78 Ack=383 Win=
12	3.103835	195.82.146.214	192.168	TCP	60	80 → 51886 [FIN, ACK] Seq=383 Ack=79 Win=

Ответ от сайта


CLIENT
BRAS
DPI
PE ROUTER
INTERNET
CLIENT
BRAS
DPI
PE ROUTER
INTERNET

Решение с применением виртуализации

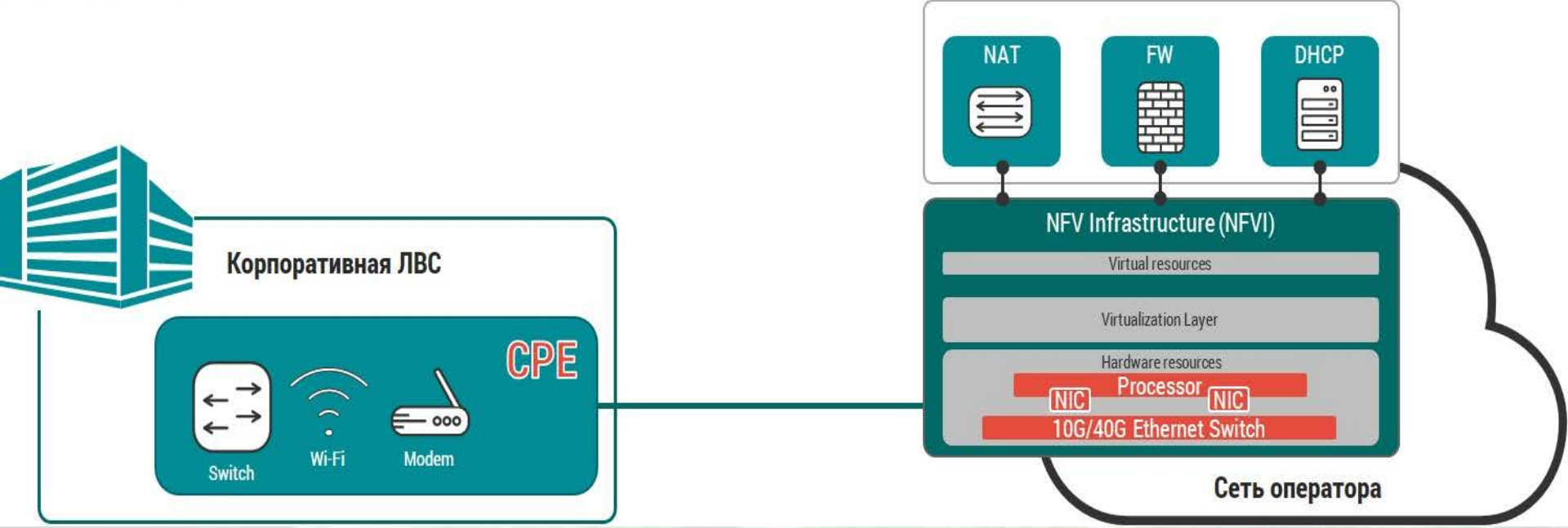


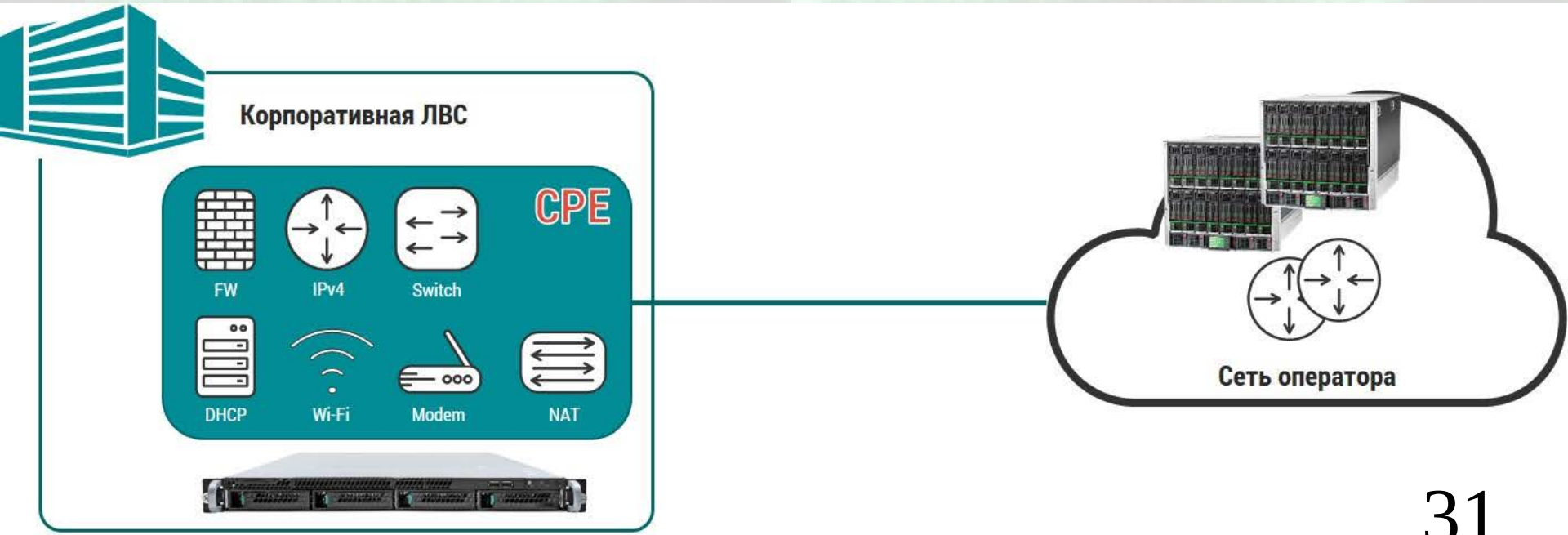
Достоинства:

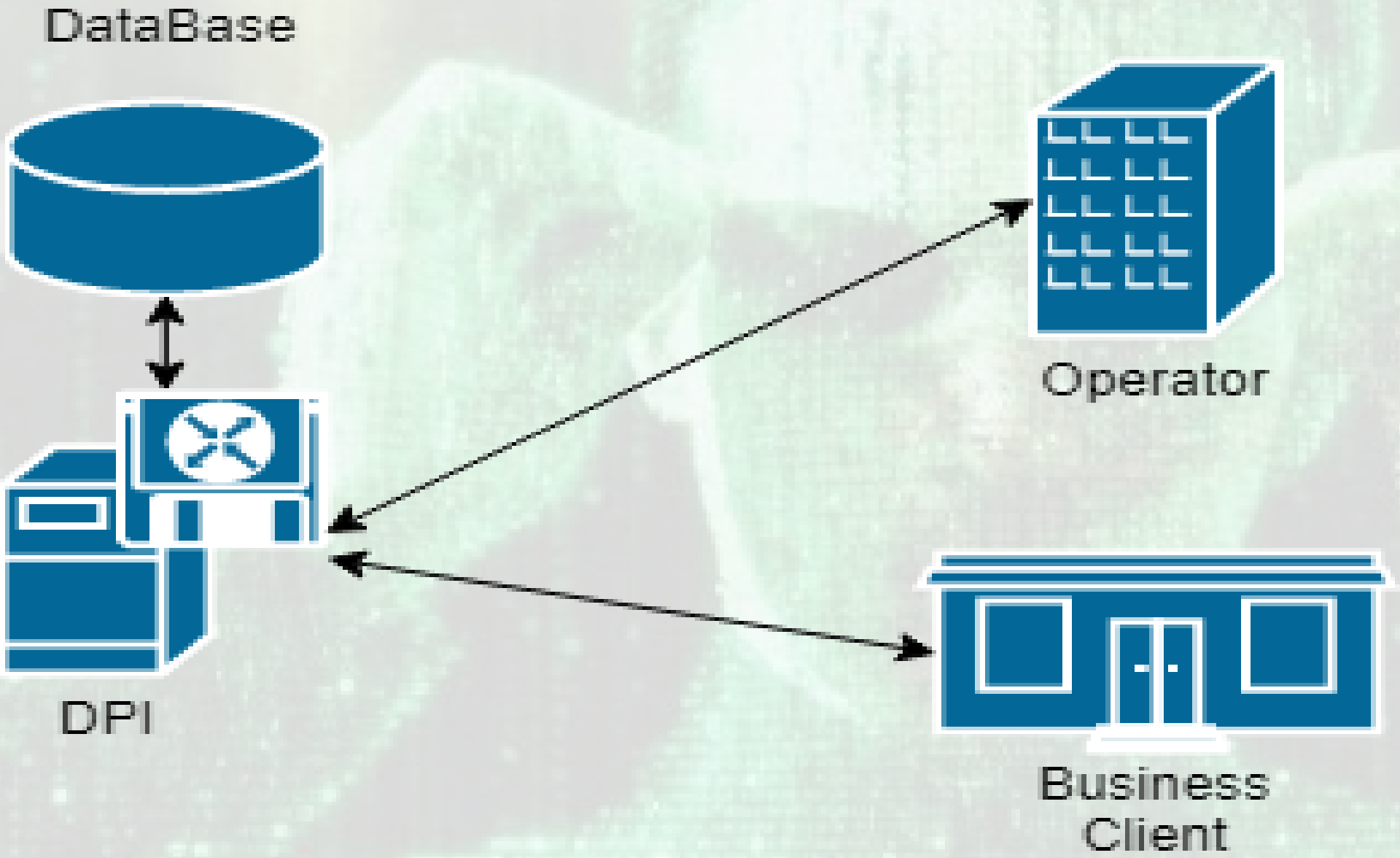
- Унифицированное оборудование
- Гибкость конфигурации
- Упрощенное развертывание и масштабирование системы
- Более быстрое создание VAS

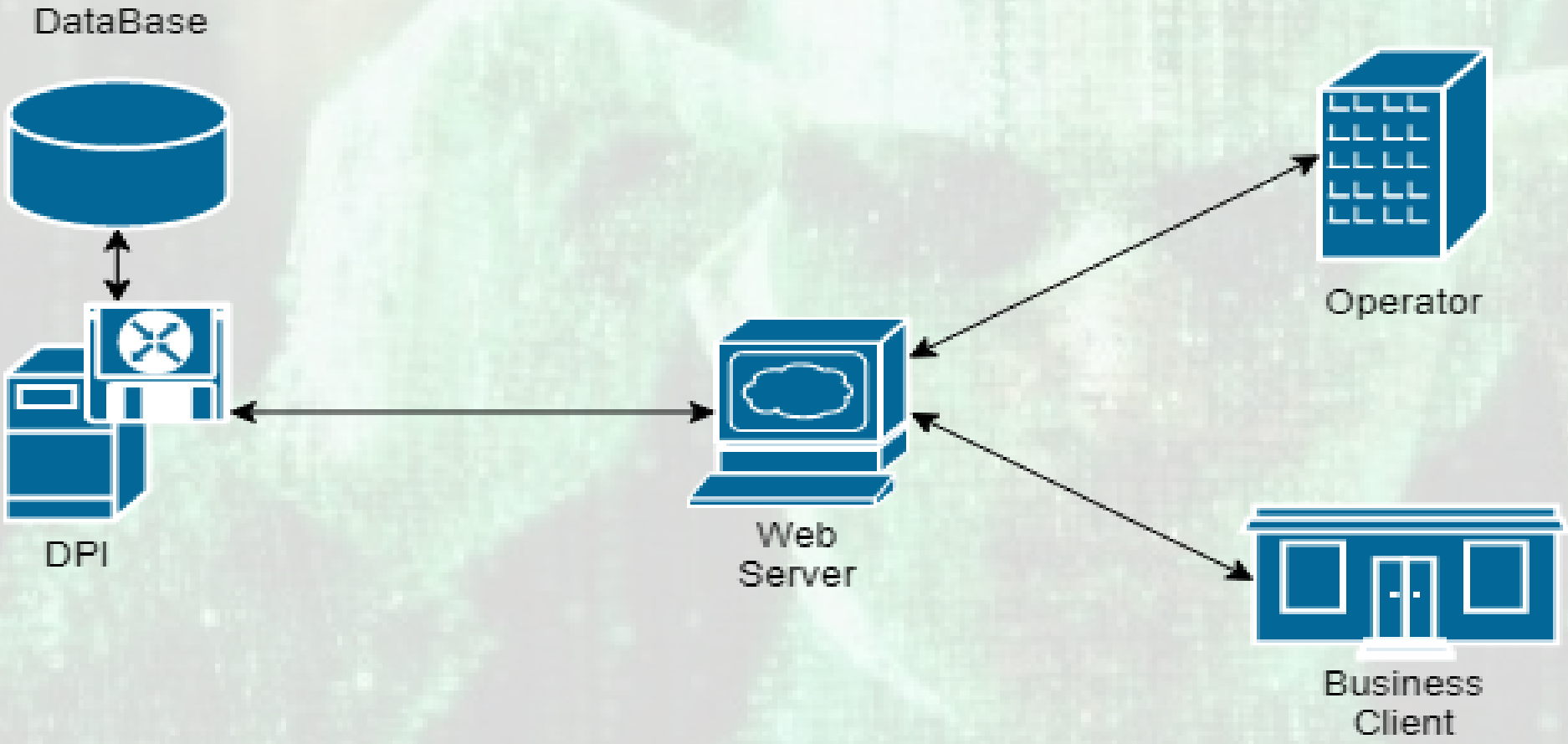
Недостатки:

- Необходимость внедрения дополнительных серверов
- Усложнение систем управления
- Отсутствие четкой экономической эффективности


NAT
FW
DHCP
NFV Infrastructure (NFVI)
Virtual resources
Virtualization Layer
Hardware resources
Processor
NIC
NIC
10G/40G Ethernet Switch
Сеть оператора
Корпоративная ЛВС
CPE
Switch
Wi-Fi
Modem


Корпоративная ЛВС
CPE
FW
IPv4
Switch
DHCP
Wi-Fi
Modem
NAT
Сеть оператора


DataBase
Operator
DPI
Business
Client


DataBase
DPI
Web
Server
Operator
Business
Client

	I группа	II группа	III группа
Число абонентов, человек.	Аб. < 100	100 < Аб. < 500	500 < Аб.
Суммарно скорость трафика, Мбит/с	10	50	100 и более
Число DPI	1	1	1 и более

Применение DPI в сети оператора связи

Внедрение DPI

Для кого?

DPI система, установленная у оператора связи, имеет прямое или косвенное влияние на всех участников единой сети передачи данных, так как оптимизированный/ освобожденный ресурс сети может быть распределён между другими типами абонентов.

Внедрение DPI

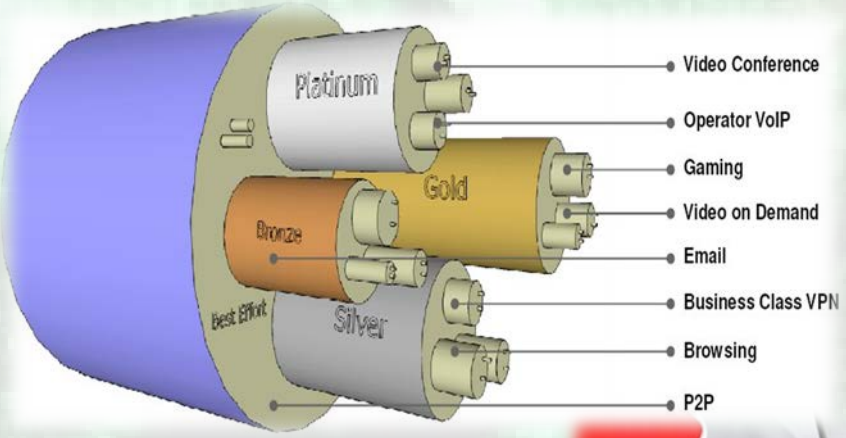
Три основных причины внедрения DPI

Внедрение DPI

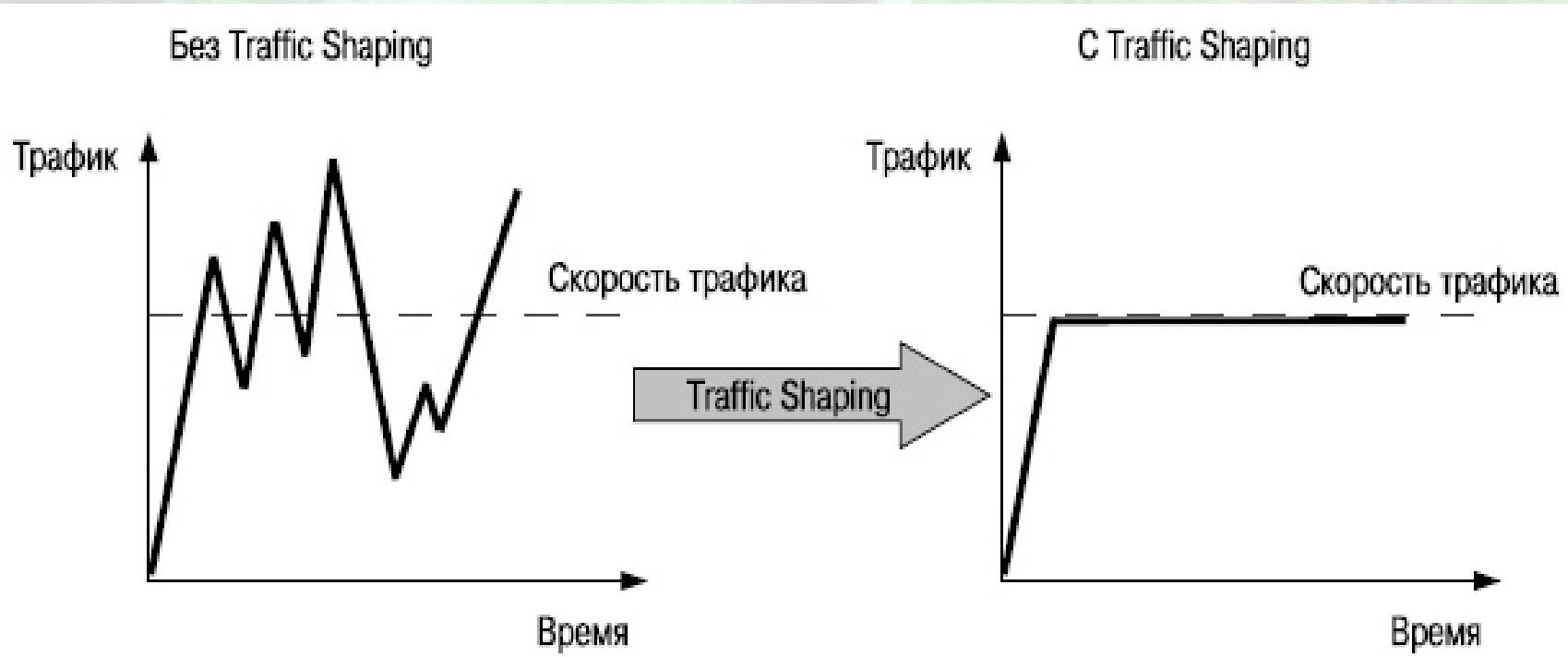
Основные направления применения DPI систем управления трафиком

Чем DPI интересен B2B?

- Фильтрация нежелательных ресурсов
- Защита корпоративной тайны
- QoS
- Управление подписками
- Защита от вирусов и атак




Без Traffic Policing
Трафик
Скорость трафика
Время
Traffic Policing
С Traffic Policing
Трафик
Скорость трафика
Время


Без Traffic Shaping
Трафик
Скорость трафика
Время
Traffic Shaping
С Traffic Shaping
Трафик
Скорость трафика
Время

Сбор статистики:

- по предоставляемым услугам (per-service)
  - (приложениям
  - , протоколам),
- по каждому пользователю (per-subscriber) .

Ограничение передачи:

- к определенным ресурсам (социальные сети, online игры, потоковое видео)

Персонализированные тарифы.

Тарификация по контенту. (доход ~ рост потребления)

Использование аппаратных ресурсов

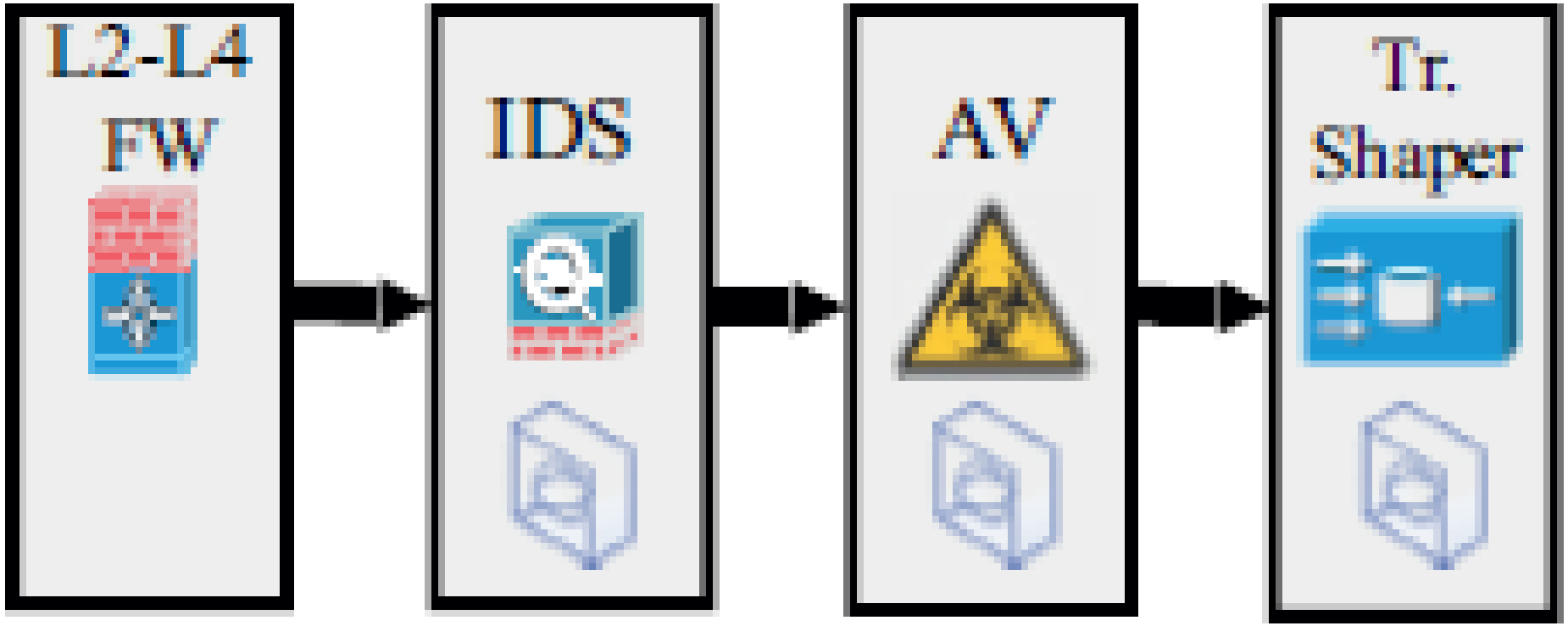
QoS, SLA.

41

Дифференциация услуг:

- **тариф для веб-трафика (HTTP)**
- **~~ограничение~~ тариф для P2P приложений**
- **тариф для соц сетей**
- **тариф для развлечений**
- **…**
- **тарификация:**
  - **time-точки**
  - **geo-точки**
  - **empty-точки**
- **тарификация для телефонии и OTT**

Middlebox – система обнаружения вторжений(IDS), антивирус/антиспам, traffic shaper и др.



43

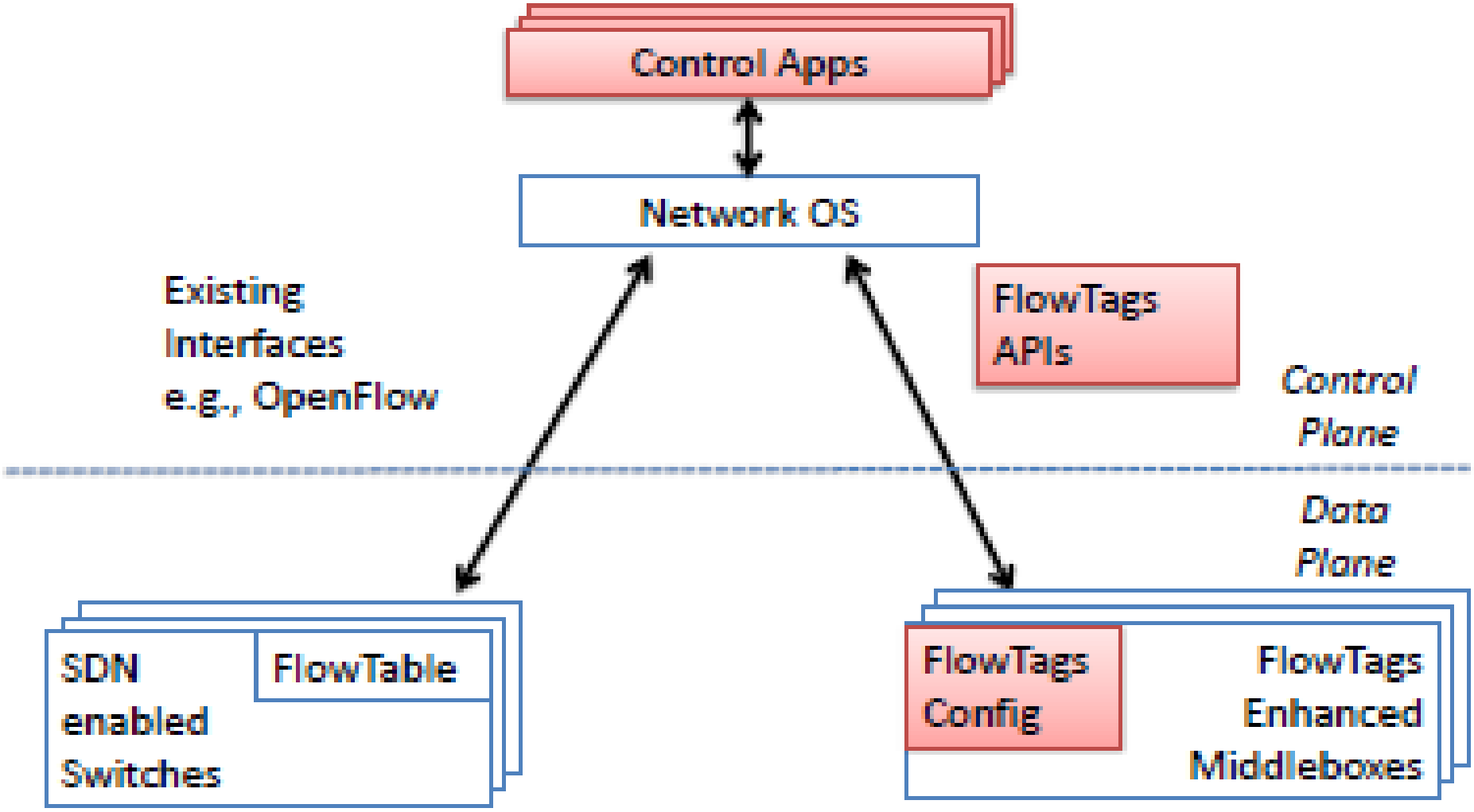
Централизация обеспечения безопасности доступа в Интернет на основе DPI-платформы в сети оператора связи, сокращает издержки клиентов (организаций) на обеспечение безопасности.

Например, это позволит **сократить** использование **антивирусов и фаерволов на каждом оконечном** устройстве, и контроль на прокси-сервере.

Однако это **не спасет от угрозы внутри сети**.

44

Архитектура SDN-сети с расширением FlowTags



45

Внедрение DPI

Сейчас большинство операторов не блокируют конкурирующие сервисы VoIP, IPTV и теряют на этом как минимум сумму равную стоимости утилизации своих каналов связи. Таким образом, пропуская бесплатно ЁМКИЙ риал-тайм трафик внешних сервисов, оператор связи наносит себе экономический ущерб, из-за необходимости практически гарантированно на длительное время выделять необходимую полосу.

Оператор должен зарабатывать на своих сервисах!

DPI системы управления трафика позволяют не только ограничивать подобный трафик, но и управлять им помогая реализовать его как дополнительные сервисы.

DPI-решения управления трафиком в большинстве случаев позволяют снизить нагрузку на сеть от 25 до 50 %.

За счет управления, ограничения и оптимизации трафика P2P приложений, потоковых аудио- и видеосервисов.

Для мобильных операторов системы DPI позволяют контролировать загруженность каждой базовой станции путем распределения ресурсов базовых станций

47

С помощью DPI-систем управления трафиком возможно отслеживание и блокирование источников того или иного контента в сети.

Маркировка цифрового контента позволяет устанавливать источники утечки и распространения нелегальной цифровой продукции.

Технологии цифровой маркировки информации широко используется правообладателями и распространяющими компаниями

48

Системы DPI могут использоваться как инструмент для статистического анализа и проверки маркетинговых проектов, которые осуществляют операторы или их клиенты.

Маркетологам исследование трафика позволяет выстраивать политику продаж, повышать эффективность тарифных планов и, как следствие, планировать доходы и расходы.

Большую популярность набирает вставка персонализированной рекламы на основе выявленных предпочтений пользователя.

49

URL-фильтрация:

Анализируя трафик на уровне приложений DPI позволяет точечно заблокировать запрещенный ресурс по URL-адресу,

без полной блокировки сервера компании хостинга.

Такой подход удовлетворяет требованию по блокировке трафика на основе доменного имени или сочетанию IP-адреса и адреса ведущего к запрещенному контенту.

50

Внедрение системы DPI обеспечивает:

-централизованный **контроль сайтов и нелегального контента** (по адресу ресурса внесенному в черный список в БД категорий **URL**);

-**персонализированный доступ** пользователей (“черный” или “белый” списки общие или частные, - персонализация самого понятия безопасность);

-**уведомление о посещении** потенциально опасных ресурсов, с проверкой трафика на наличие вирусов;

- **контроль трафика файлообменных сетей** на основе политик (ограничение/выделение минимальной гарантированной/блокировка общей скорости передачи, скорости по типу трафика (web, video, P2P, IM и пр.), **указание приоритета** для каждого типа);

Внедрение системы DPI обеспечивает:

-**контроль почтового спама** (по количеству рассылок). При этом зараженный пользователь перенаправляется на страницу с инструкциями по удалению вируса;

-**обнаружение DoS/DDoS атак** (по большой нагрузке на вычислительную систему);

- **обнаружение сканирования** сети;

Внедрение системы DPI обеспечивает:

- **сбор статистики** (используемая полоса пропускания по каждому типу трафика, по каждому интернет серверу или **пользователю**, их процентное соотношение, количество соединений или обьем трафика к интернет серверам);

-**фильтрация** по адресам, портам, доменным именам и протоколам (например, P2P или Skype);

-применение **динамических индивидуальных политик** для фиксированных и мобильных абонентов (APN, телефонный номер, тип доступа (2G, 3G, 4G));

- **блокировка или ограничение** скорости **при** опасности **перегрузки** или высокой загруженности в соте (для сетей подвижной связи).

Применение Оператором

- анализ работы пользователей
- анализ работы приложений
- управление существующим у оператора ресурсом
- контроль разрешенного уровня потребления трафика
- биллинг.

Корпоративное применение

Управление информационной безопасностью:

- Контроль передачи конфиденциальных документов (целиком или любой части текста документа, в том числе и в заархивированном виде)

(ч/з email, site, ftp …)

- Предотвращение утечки конфиденциальной информации
- Выявление нарушителей
- Защита персональных данных

Корпоративное применение

Управление сетью:

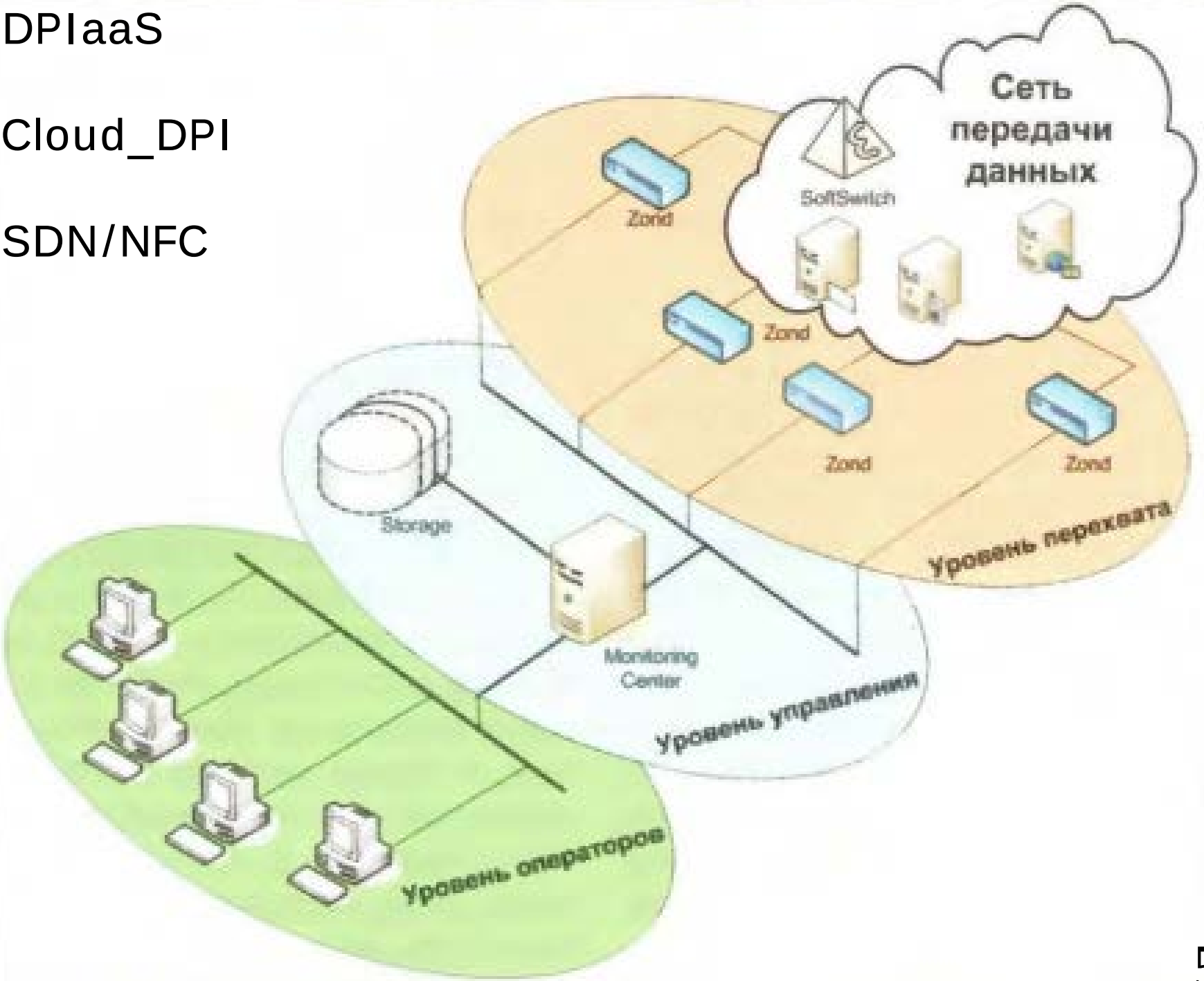
- Контроль интернет активности сотрудников
- Ограничение доступа пользователей корпоративной сети к Интернет ресурсам.
- Мониторинг лояльности сотрудников (сайты о работе и т.д.)

DPI as Service

DPIaaS

Cloud_DPI

SDN/NFC



Таргетированная реклама

59

Конфиденциальность

Технология поведенческого таргетинга

BT (Behavioral Targeting) на основе анализа взаимодействия между сайтами сети Интернет.

Путем применения переменных в ссылках на другие сайты или javascript-указаний, либо посредством запросов данных, хранящихся в веб-браузере (cookies), собирается информация о посещенных страницах.

Все эти данные собираются в профиль интересов пользователя, могут продаваться и использоваться для таргетированной рекламы.

Конфиденциальность

Технология поведенческого таргетинга

BT (Behavioral Targeting)

Средства DPI позволяют сделать поведенческий таргетинг более точным и всеобъемлющим.

Провайдеры, применяющие DPI, могут не только собирать информацию, но и внедрять в проходящий трафик рекламу.

Спасибо за внимание.

Далее: Принцип работы DPI и виды глубокого анализа пакетов.

Вопросы?

Ст. преп. каф. Инфокоммуникационных систем СПбГУТ,

Фицов Вадим Владленович,