

SOC
FORUM
2023

DPI в NGFW: Никакой магии

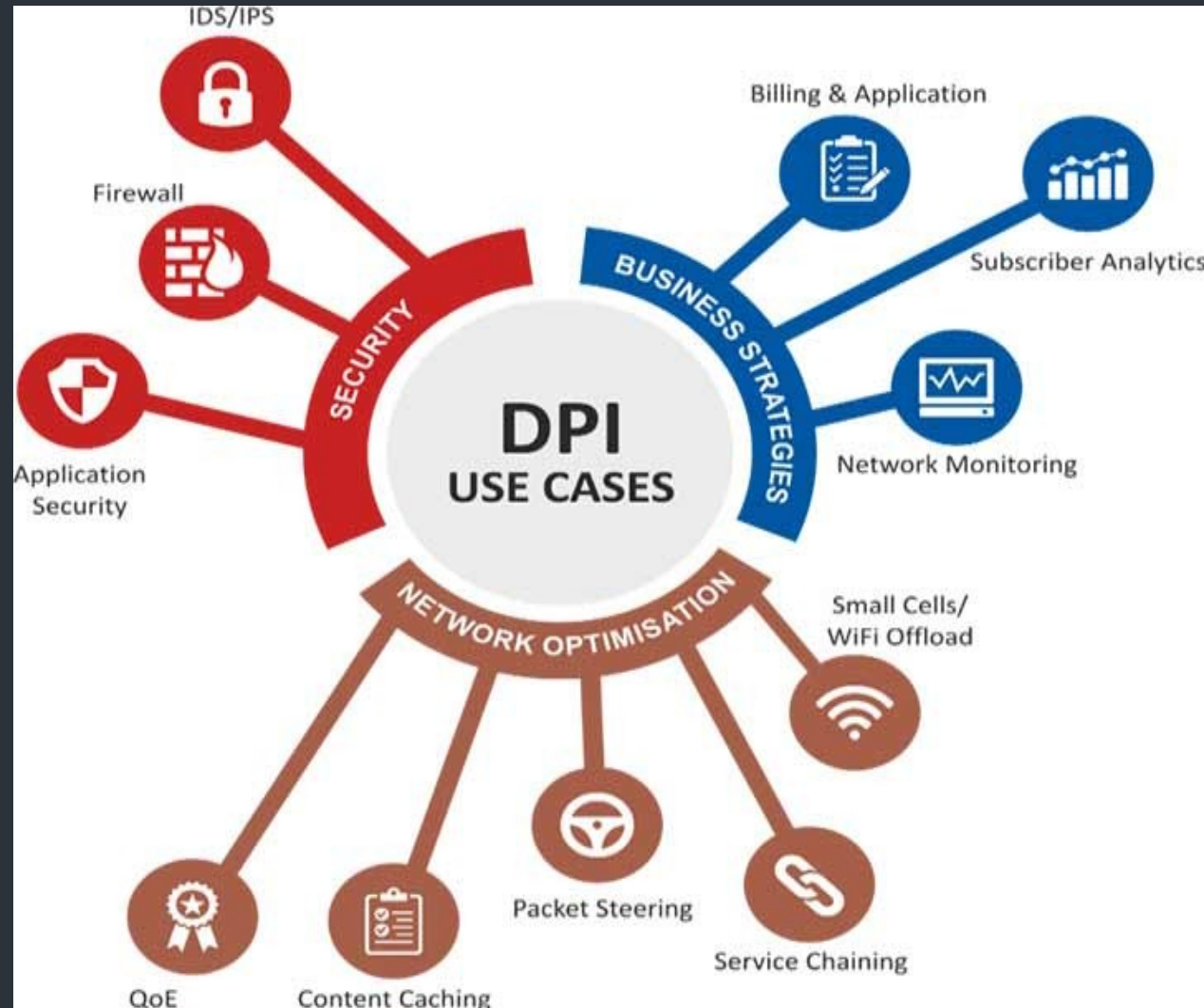
SOC
FORUM
2023



Сергей Кормушин

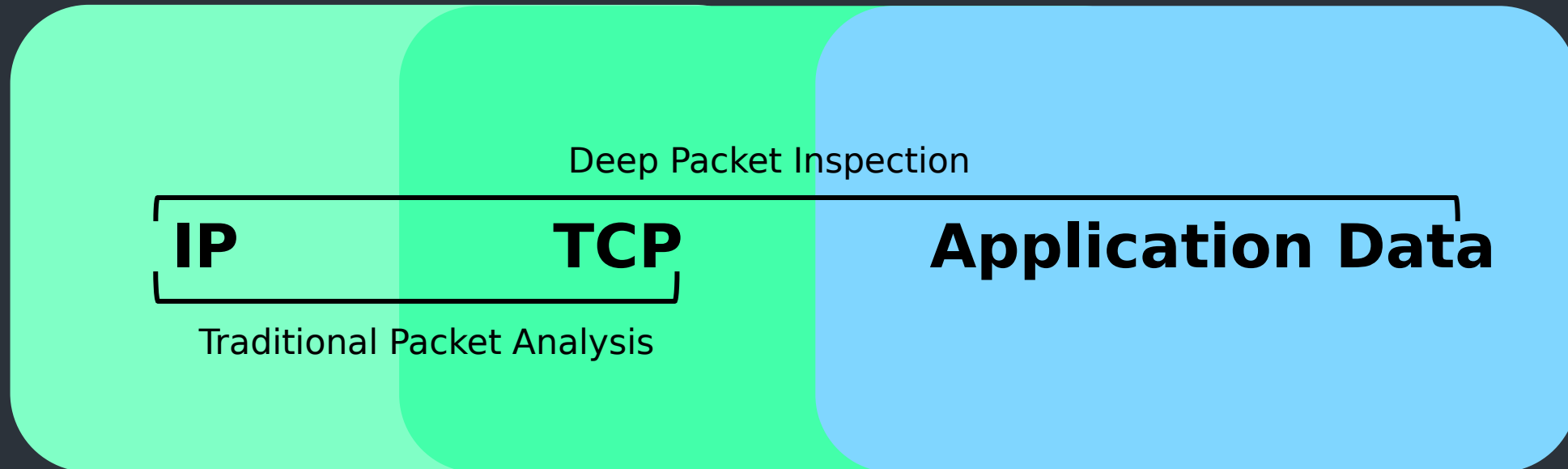
Код Безопасности

Сценарии работы DPI



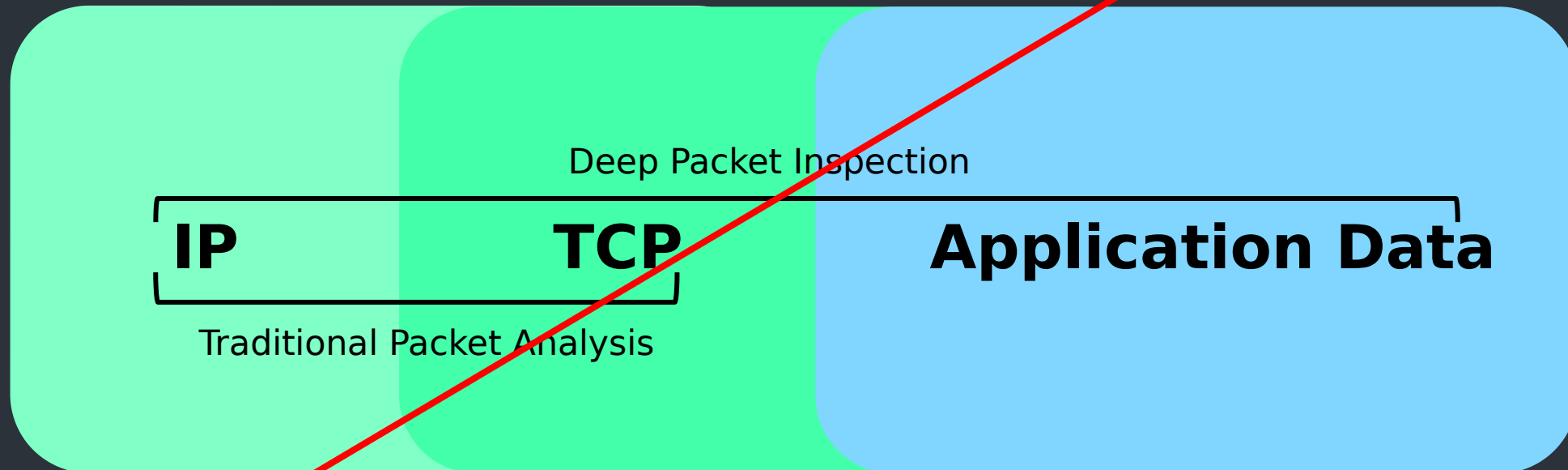
Что такое DPI?

Deep Packet Inspection

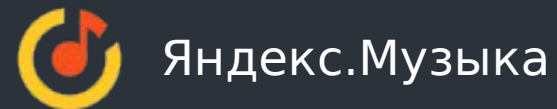
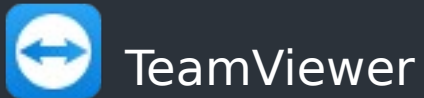
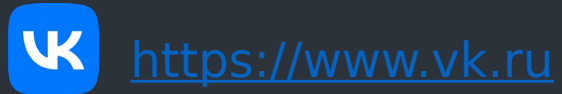


Что такое DPI?









Deep Packet Inspection



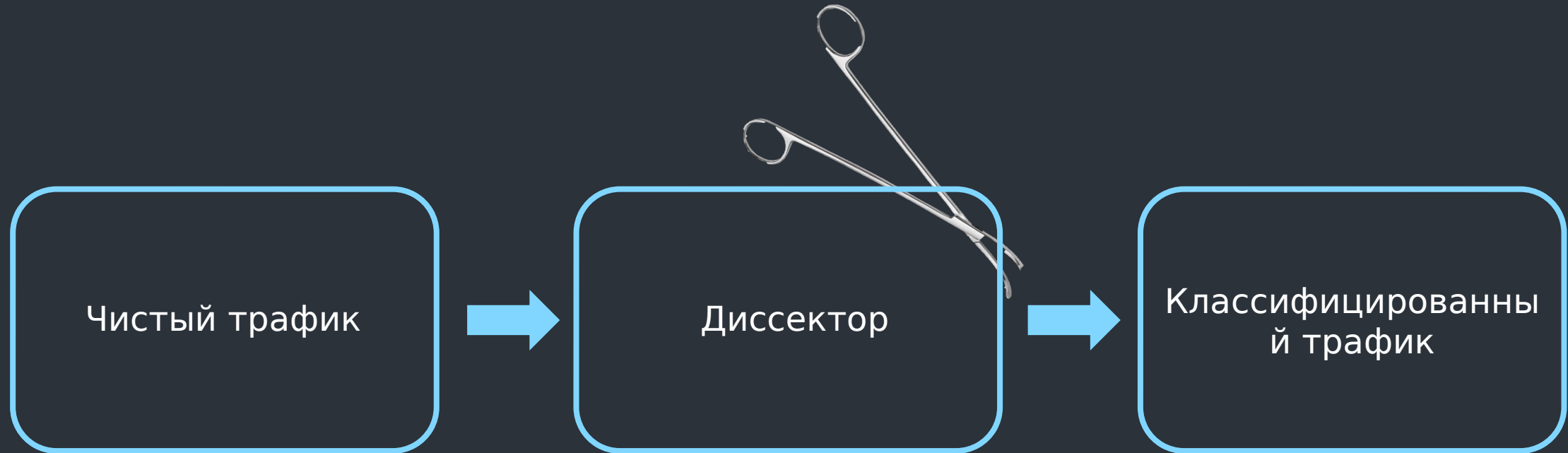
Такие разные приложения



Такие разные приложения

- | | | | | | |
|-------------------------------------------------------------------------------------|---------------------------------------------------|-------------------|---------------------------------------------------------------------------------------|---------------|----------------------------------|
|  | https://www.vk.ru | → Веб-страница |  | Apache | → HTTP-сервер |
|  | TeamViewer | → Другой протокол |  | Яндекс.Музыка | → Аудио-стриминг |
|  | Facebook.Video | → Видео-стриминг |  | Skype | → Первый активный сменщик портов |
|  | Telegram | → Telegram |  | SSH | → Протокол управления |

Как работает DPI?



Что происходит в диссекторе?

- ◆ Подготовка пакета:
 - ◆ Объединение кадров
 - ◆ Извлечение из туннеля
 - ◆ Дефрагментация IP- пакета
- ◆ Буферизация
- ◆ Классификация
- ◆ Декодирование:
 - ◆ Извлечение метаданных

На однозначное
определение трафика
нужно 3-8 пакетов

**Важен не
пакет, важна
сессия!**

DRP движок – это много диссекторов

Диссектор 1

Диссектор 4

Диссектор 7

Диссектор 2

Диссектор 5

Диссектор 8

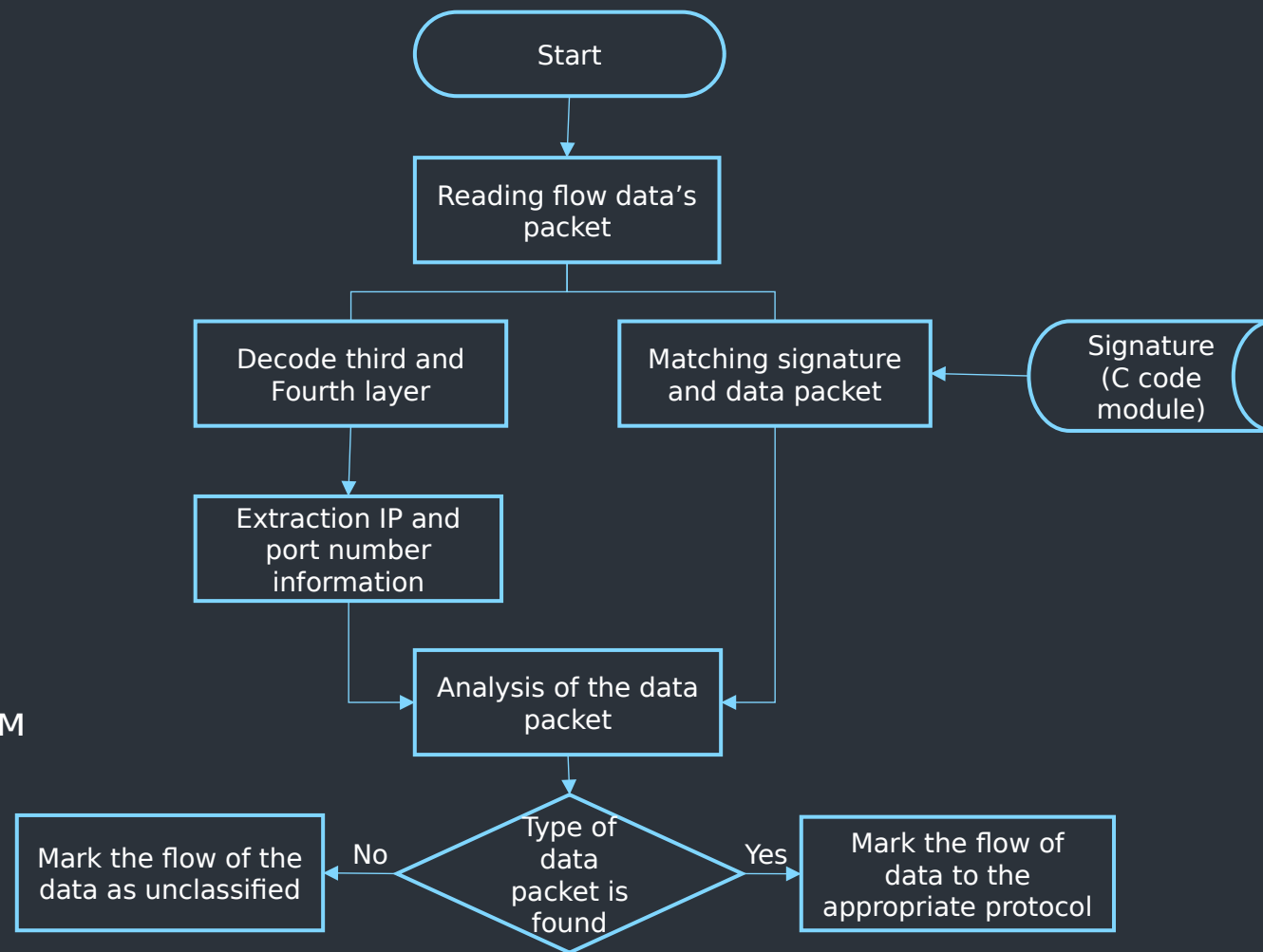
Диссектор 3

Диссектор 6

Диссектор 9

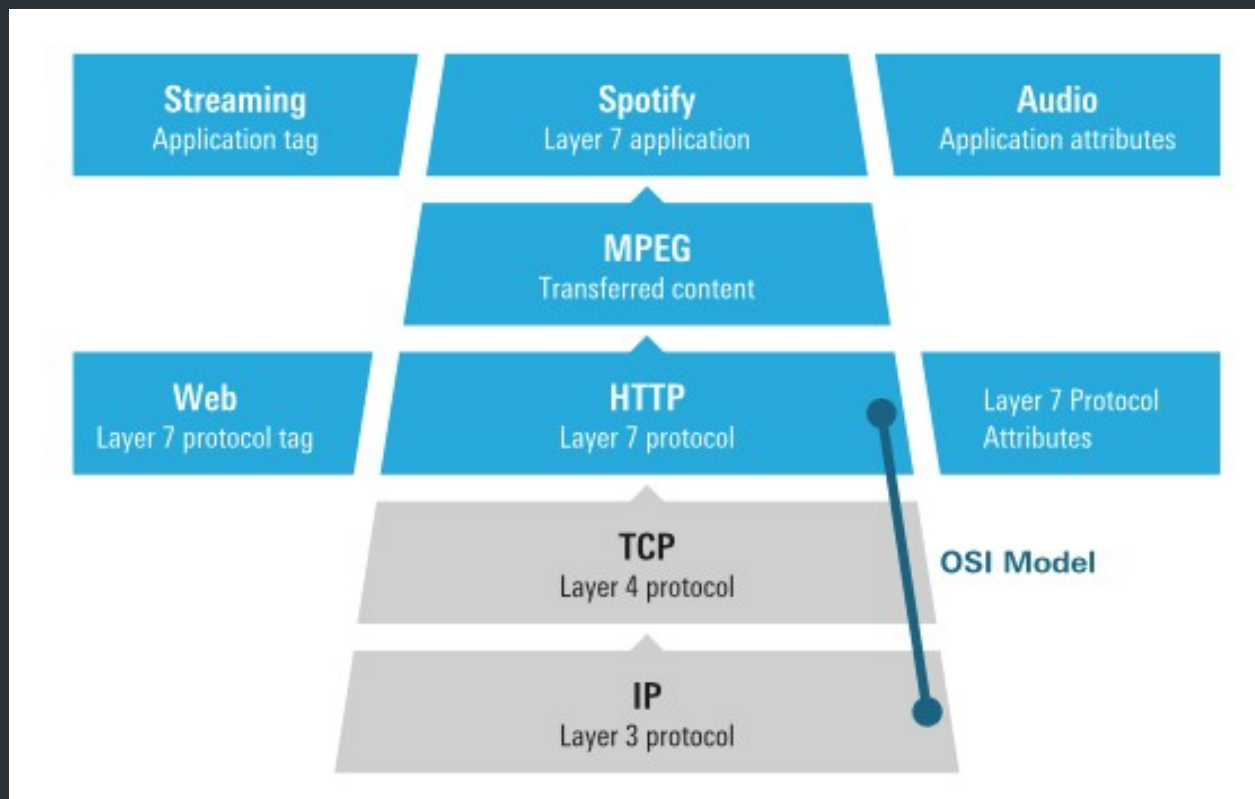
Как работает DPI?

- ◆ Анализируем порт
- ◆ Пытаемся угадать нужный диссектор
- ◆ Если угадываем – разбираем пакет/сессию
- ◆ Если несколько раз не угадываем – помечаем



Что получаем на выходе?

Это все метаданные



На чем можно реализовать?

Бесплатные

- ◆ nDPI
- ◆ L7Filter
- ◆ Suricata

Коммерчески е ПО

- ◆ P&S Pace2
- ◆ Qosmos
- ◆ Allot
- ◆ VAS Experts
- ◆ MicroOLAP

Коммерческо е железо

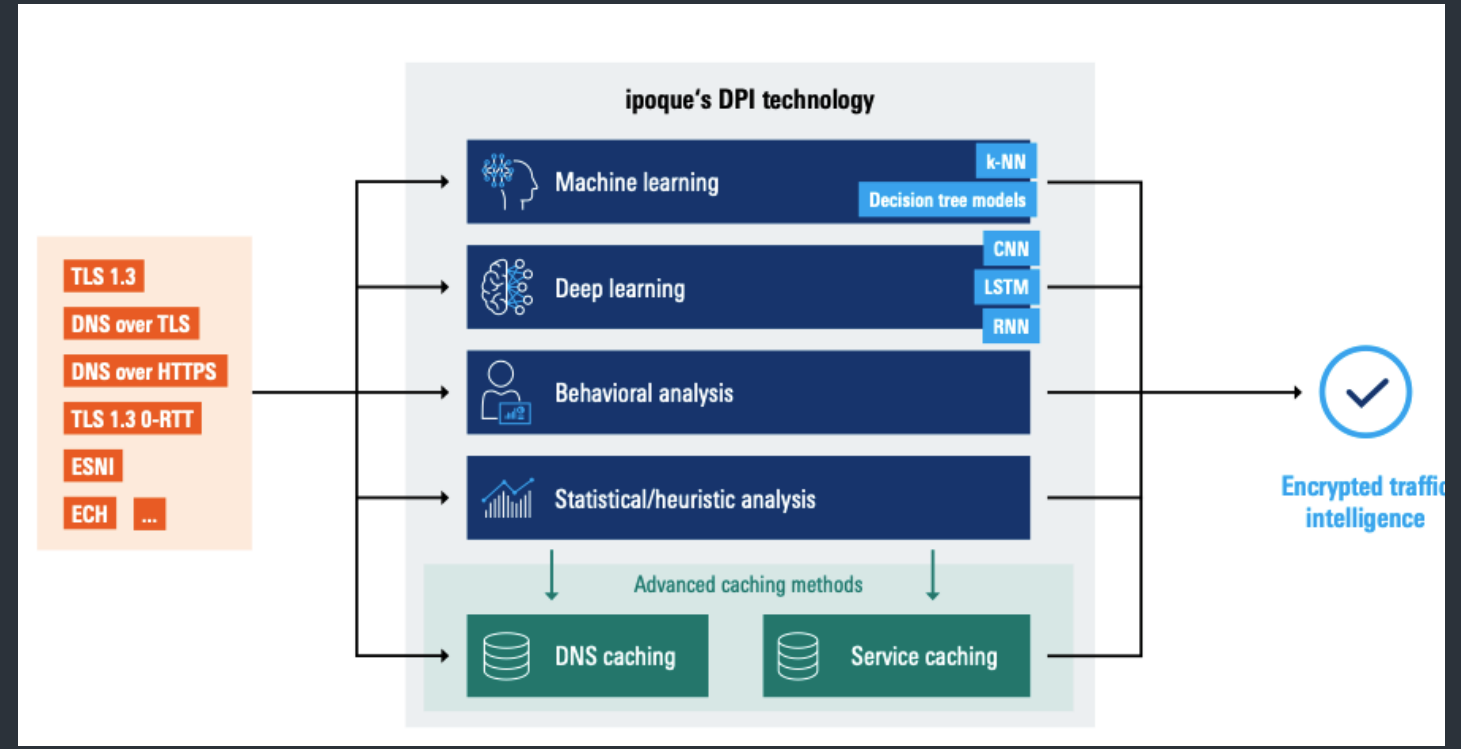
- ◆ Mellanox
- ◆ Napatech

Что делать с зашифрованным трафиком?

Страдать...

НО есть немного вариантов:

- ◆ SNI для веб-сайтов
- ◆ ИИ
- ◆ Анализ энтропии



Ограничения в контексте Security- сценария

Анализируются первые 10 пакетов сессии. А остальные?

2 Way Auth все еще боль

Чем больше эвристики, тем выше вероятность FP

Много анализа – много ресурсов – низкая
производительность

MitM дорог по ресурсам

GoodByeDPI и прочие средства обхода

**DPI в NGFW не спасет от целенаправленного обхода.
Нужен эшелонированный подход
(NTA, контроль эндпоинтов, общая аналитика)**

SOC FORUM 2023



+7 (495) 982-30-20
info@securitycode.ru

115230, Россия, Москва,
1-й Нагатинский проезд, д.
10, стр. 1.