ЦИФРОВЫЕ РЕШЕНИЯ

НА ГРАНИЦЕ ИТ И ИБ:
зеркалирование трафика
и эффективное подключение
NTA/NDR

Плотко Сергей
Коммерческий директор
«Цифровые решения»

Зачем нужна копия трафика?

ЦИФРОВЫЕ РЕШЕНИЯ

- Выборочный мониторинг портов для помощи в поиске неисправностей
- Обеспечение информационной безопасности на портах, выходящих за границы периметра
- **Вспомогательная функция коммутаторов/маршрутизаторов**

- Выборочный мониторинг портов для помощи в поиске неисправностей
- Поиск угроз безопасности по трафику в сети
- Одновременное подключение систем мониторинга и ИБ
- **Базовая необходимость для работы систем мониторинга**

Кому нужна копия трафика?

ЦИФРОВЫЕ РЕШЕНИЯ

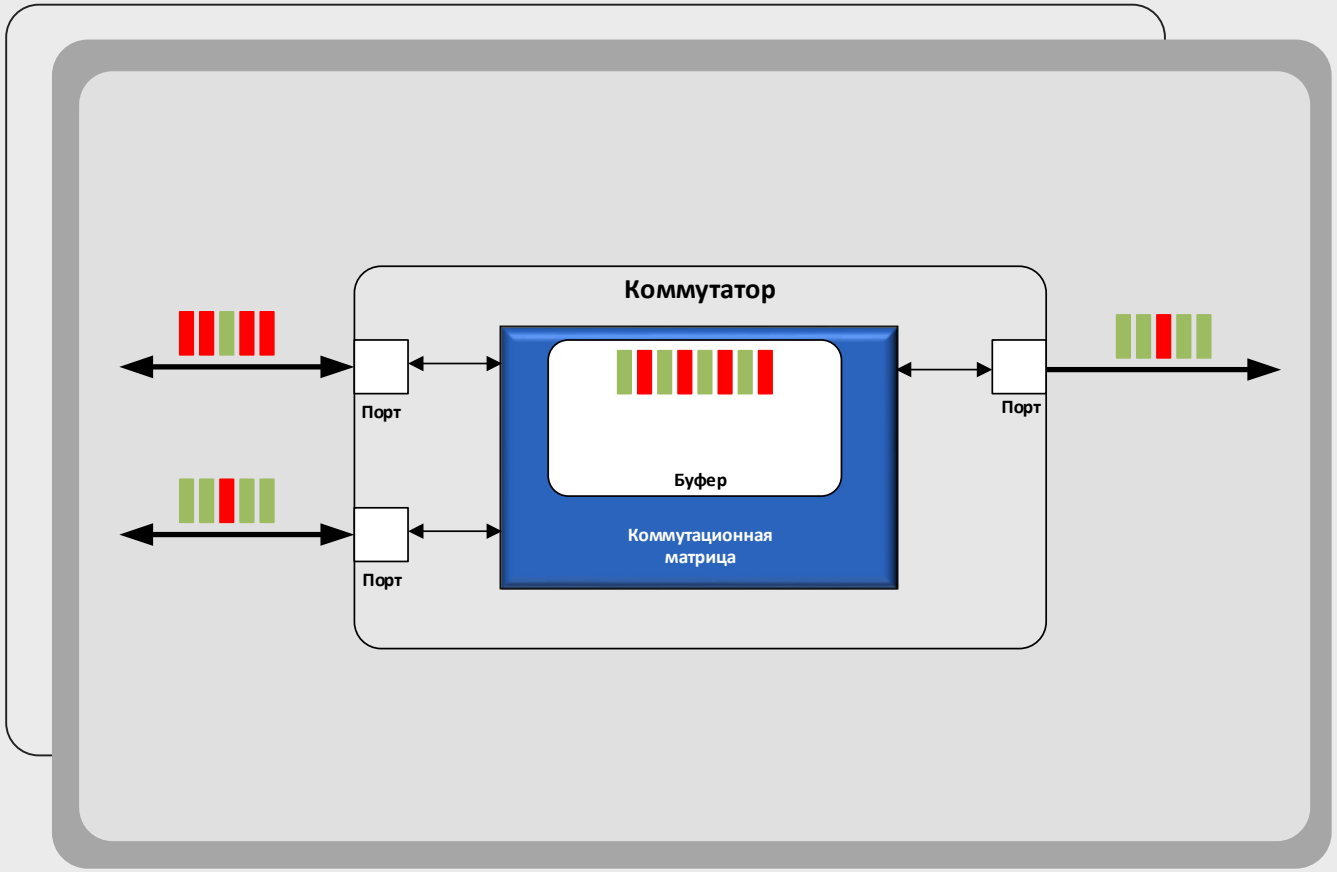
Атаки могут быть инициированы даже с внутренних узлов.

Если цель атаки находится в доверенной сети, трафик не выйдет за границы сетевого периметра и **межсетевой экран в этом случае будет бесполезен**.

Как работает коммутатор без SPAN

ЦИФРОВЫЕ РЕШЕНИЯ

1. Получили пакет – записали в буфер
2. Определили выходной порт
3. Дождались пока он освободится
4. Передали на выход
5. Удалили из буфера

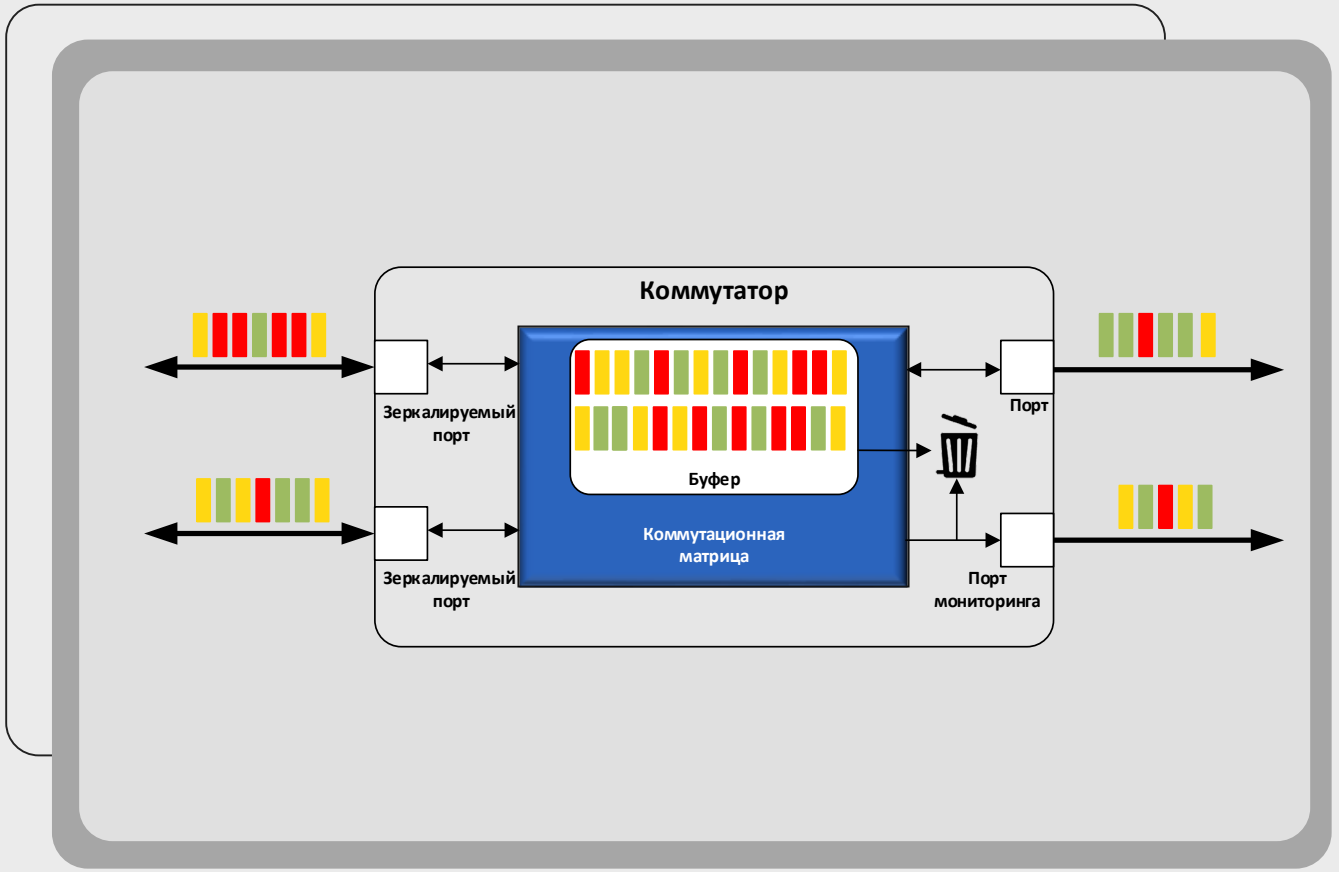


Проблемы, которые создает SPAN

ЦИФРОВЫЕ РЕШЕНИЯ

Пропускная способность даже одного обычного порта в 2 раза выше пропускной способности SPAN

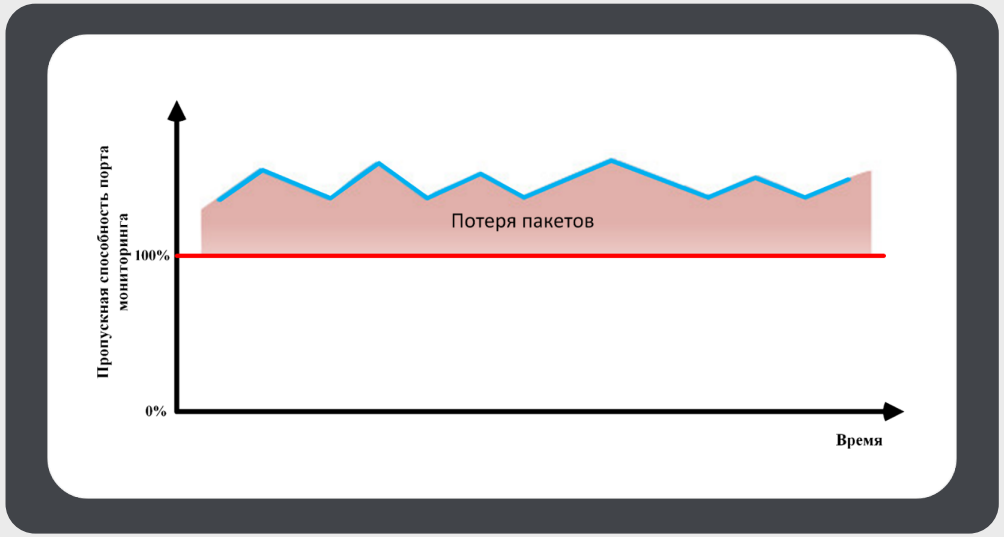
1. Пакеты накапливаются в буфере, переполняя его
2. Зеркалируемые пакеты отбрасываются и анализатор не может собрать сессию
3. Пакеты основного обмена перестают помещаться в буфер и отбрасываются
4. UDP пропадают навсегда, а переповторы TCP **снижают** производительность сети



Очень хорошо, если очень плохо

ЦИФРОВЫЕ РЕШЕНИЯ

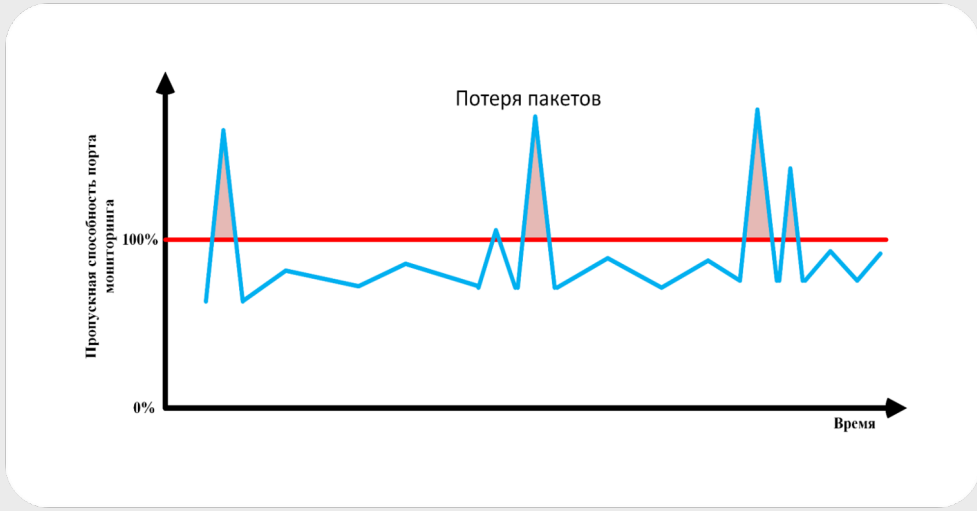
Не работает



Зеркалируемый трафик в разы больше пропускной способности порта мониторинга и потери видны сразу

!

Почти работает

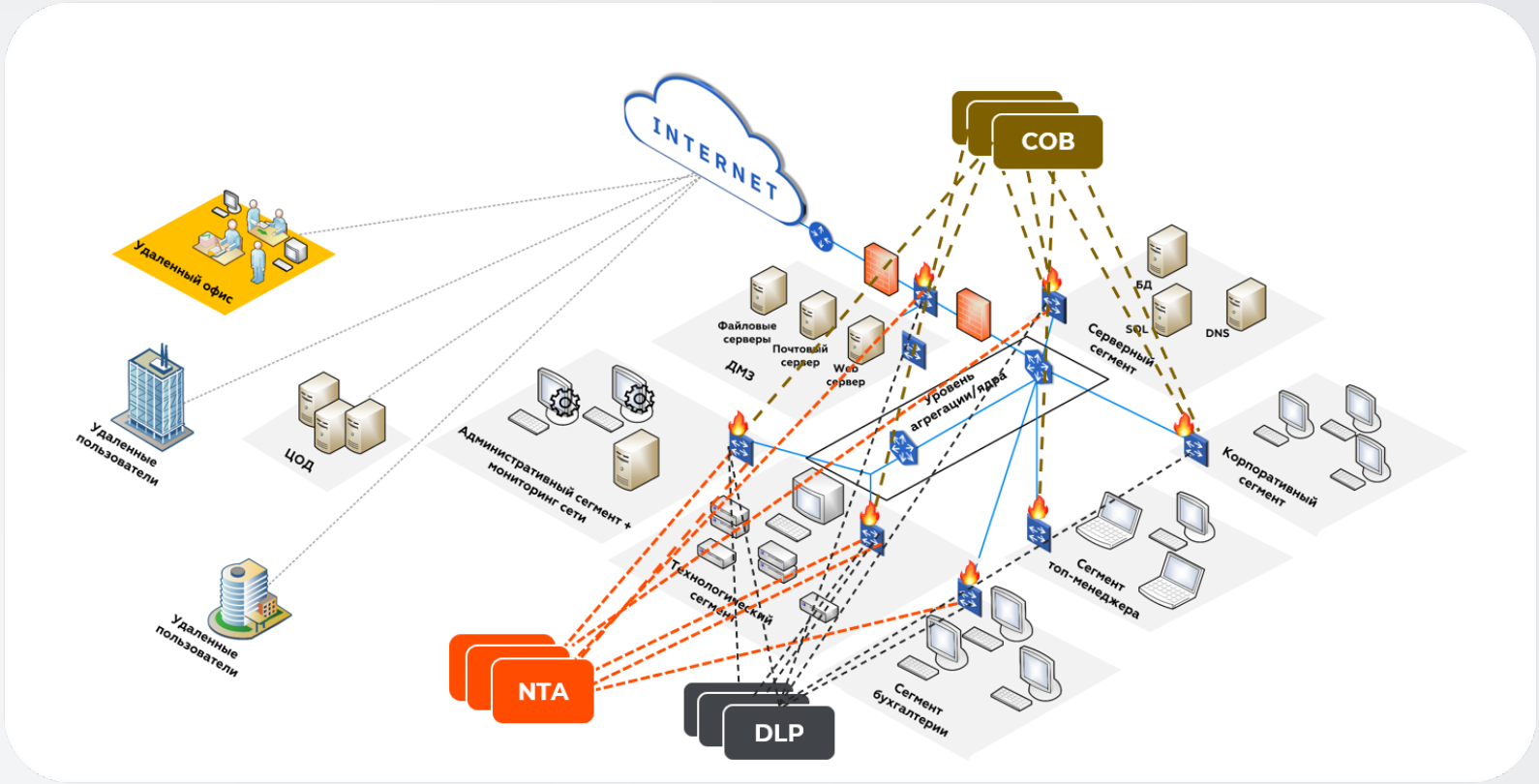


100 Мбит/с на порту 1 Гбит/с = 90% времени трафика нет

Совпадение передачи по нескольким портам приводят к потерям

Сложно понять
Невозможно эксплуатировать

ЦИФРОВЫЕ РЕШЕНИЯ

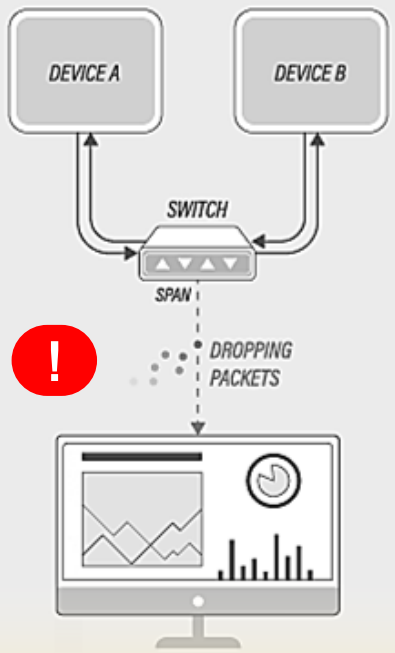


- ✓ Много точек управления
- ✓ Непредсказуемые потери пакетов
- ✓ Ограничения по источникам копий
- ✓ Конкуренция за копию трафика
- ✓ Необходимость расхода ресурсов анализатора на фильтрацию

Снятие сетевого трафика с ИТ-инфраструктуры

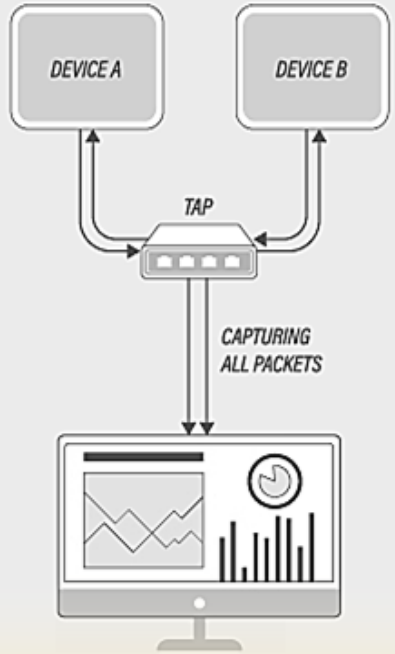
ЦИФРОВЫЕ РЕШЕНИЯ

SPAN



VS

TAP

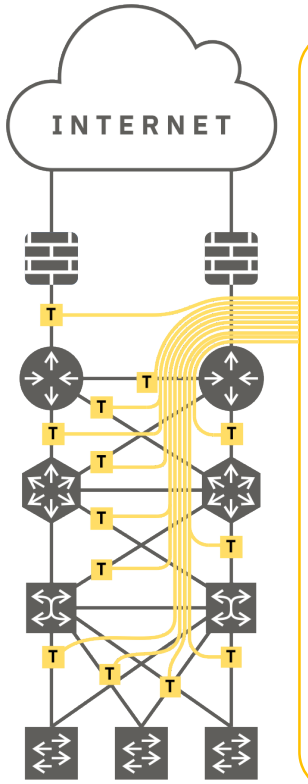


Сняли трафик

что дальше?

ЦИФРОВЫЕ РЕШЕНИЯ

?



- Что делать с нехваткой входов в анализаторе
- Как убрать лишние пакеты и сессии
- Как подать один и тот же трафик на несколько систем
- Как поделить большой поток на несколько анализаторов

NTA/NDR

DLP

Анализ БД

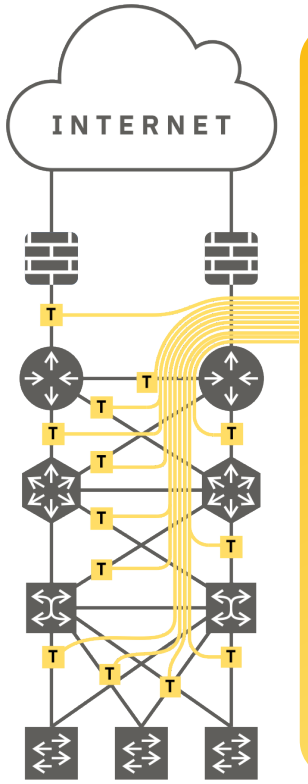
Troubleshooting

Performance Monitoring

Распределение трафика

ЦИФРОВЫЕ РЕШЕНИЯ

подача на анализаторы только необходимого трафика



Брокер сетевых пакетов

DS Integrity

Агрегация

Фильтрация

Дедупликация

Репликация

Балансировка

- NTA/NDR
- DLP
- Анализ БД
- Troubleshooting
- Performance Monitoring

Брокер сетевых пакетов получает трафик, подготавливает и передает копии на несколько систем

SPAN в АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

загрузка коммутатора

до *5%*

низкая вероятность потерь

- Дополнительное устройство - потенциальная точка отказа
- За SPAN не нужно платить
- Не занимает места

Только не SPAN в АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

потеря пакетов в технологической сети наиболее критична

- Зависимость зеркалирования от целостности настроек
- Дублирование пакетов при зеркалировании через SPAN
- Непредсказуемая реакция на рост нагрузки
- SPAN не везде есть
- Риск попадания трафика из сети мониторинга в сеть АСУ ТП

3 эшелона защиты сети в АСУ ТП

ЦИФРОВЫЕ РЕШЕНИЯ

- Оптический однонаправленный сигнал
- Физический разрыв на печатной плате
- Отсутствие логической связи в коммутационной матрице на ПЛИС

Сертификат ФСТЭК

Сертифицирован по 4 уровню доверия

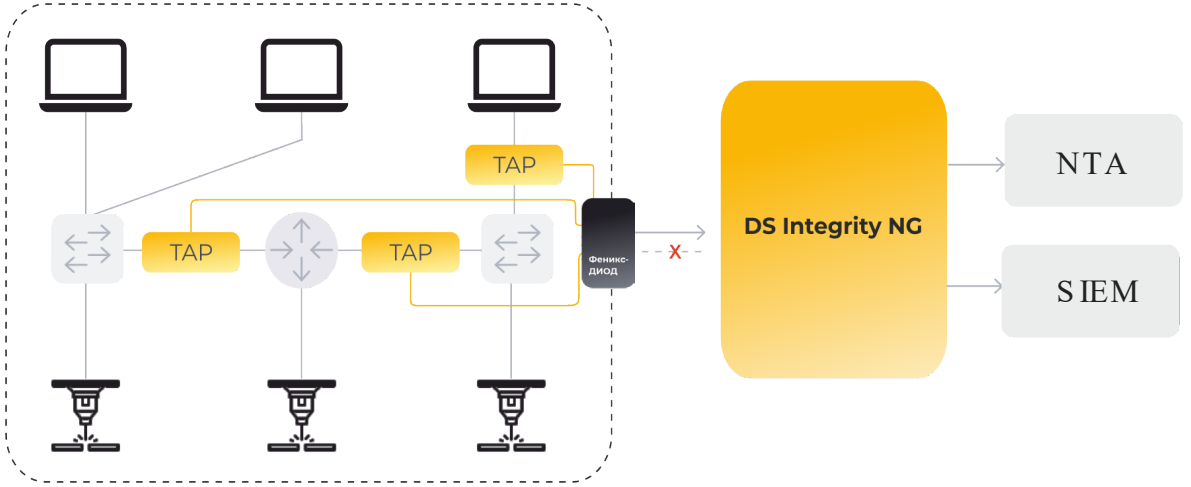
История из энергетической компании

ЦИФРОВЫЕ РЕШЕНИЯ

зеркалирование трафика на промышленную NTA и SIEM

Задача

Копирование трафика из АСУ ТП для передачи на промышленную NTA с однонаправленной передачей трафика



Решение

- Установка ответвителей сетевого трафика (TAP), однонаправленного агрегирующего шлюза и брокера сетевых пакетов с функцией дедупликации

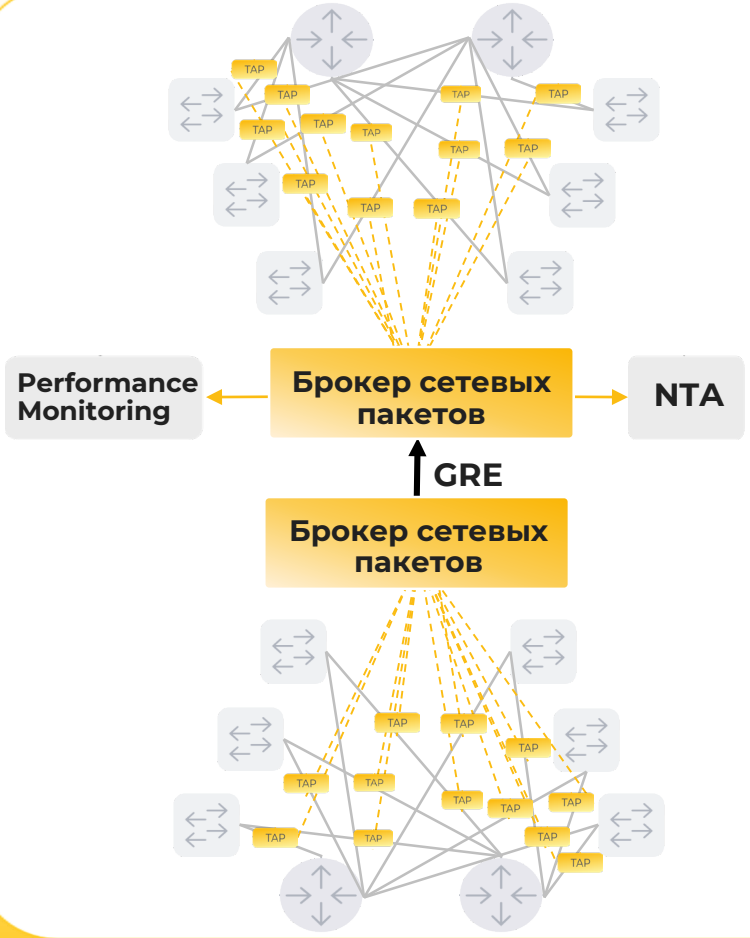
Результат

- **0%** Вероятность влияния внешних систем на АСУ ТП
- **50%** Снижение нагрузки на NTA за счёт дедупликации
- **100%** Мониторинг сети АСУ ТП

История из банка ТОП-10

внедрение NTA и Performance Monitoring

ЦИФРОВЫЕ РЕШЕНИЯ



Задача

Копирование трафика основного и резервного ЦОД для передачи на NTA и систему мониторинга производительности

Решение

- Установка ответвителей сетевого трафика (TAP) и брокеров сетевых пакетов с функциями дедупликации и туннелирования в обоих ЦОД
- Передача оптимизированного трафика из резервного ЦОД на брокер основного ЦОД

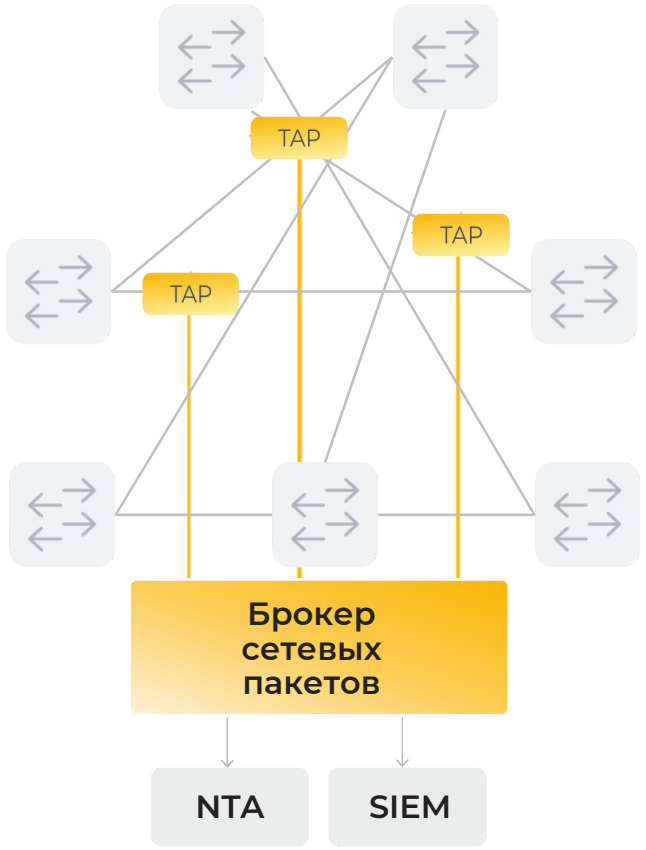
Результат

- **45%** Снижение нагрузки на NTA за счёт дедупликации
- Ликвидация всплесков трафика при Backup’е
- Централизация средств анализа

История из крупной корпорации

внедрение NTA и SIEM

ЦИФРОВЫЕ РЕШЕНИЯ



Задача

Копирование трафика с границ сегментов сети для NTA и передача статистики на SIEM

Решение

- Установка ответвителей сетевого трафика (TAP) и брокера сетевых пакетов
- Оптимизация трафика за счет дедупликации и фильтрации
- Передача sFlow и Syslog на SIEM

Результат

- **40%** Снижение нагрузки на NTA за счёт дедупликации
- **20%** Снижение нагрузки на NTA за счёт фильтрации
- **100%** Исключение перегрузки NTA во время backup’ов

Строим независимую ИБ учитывая потребности бизнеса

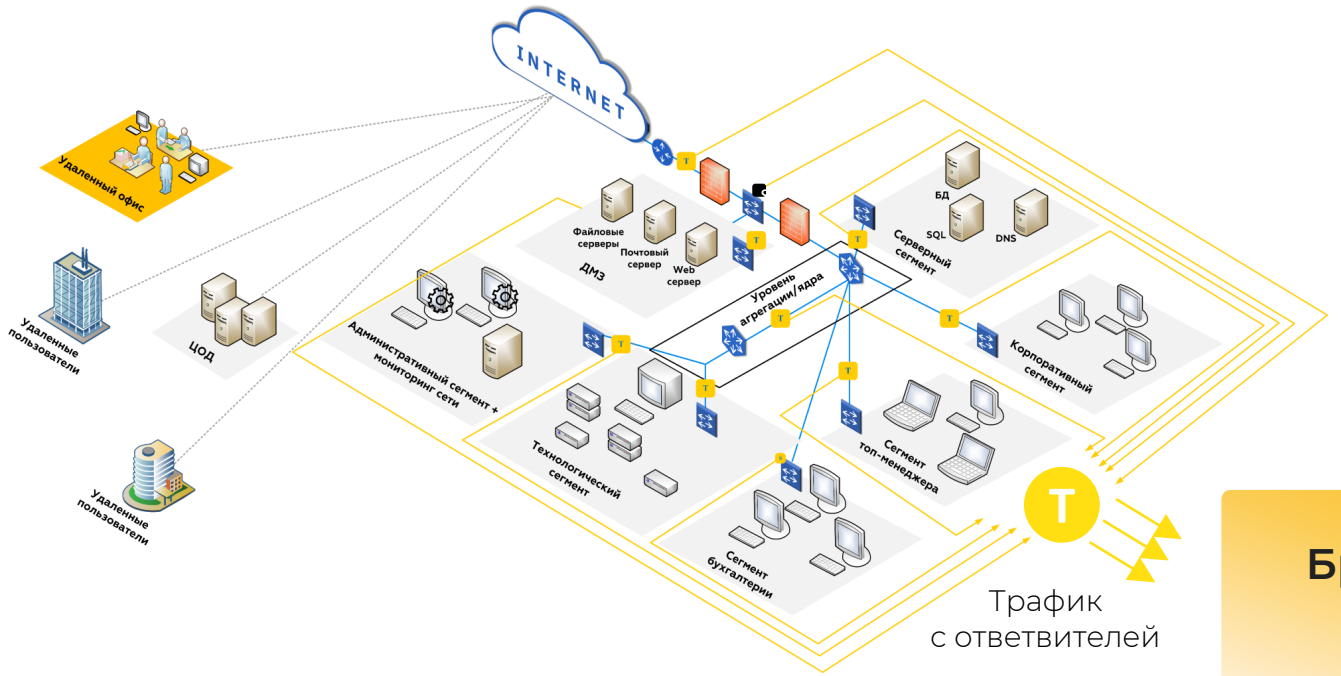
ЦИФРОВЫЕ РЕШЕНИЯ

ПОТРЕБНОСТИ БИЗНЕСА

- Надежная работа сетевой инфраструктуры
- Разделение зон ответственности между ИТ и ИБ
- Снижение требований к квалификации персонала
- Эффективное использование средств на ИБ
- Скорость интеграции ИБ-систем

Красота спасёт мир

ЦИФРОВЫЕ РЕШЕНИЯ



- Простая, легко масштабируемая архитектура
- Снижение нагрузки на сеть. Минимизация точек отказа
- Нет слепых зон и конкуренции за трафик
- Каждый получает нужный трафик в удобном формате

Брокер сетевых пакетов

- NTA/NDR
- DLP
- СОВ

ДАВАЙТЕ СТРОИТЬ РОССИЙСКИЙ ИНФОБЕЗ ВМЕСТЕ

sales@dsol.ru | partners@dsol.ru