ЦИФРОВЫЕ РЕШЕНИЯ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Без ИТ нет ИБ – зеркалирование сетевого трафика

Сергей Плотко

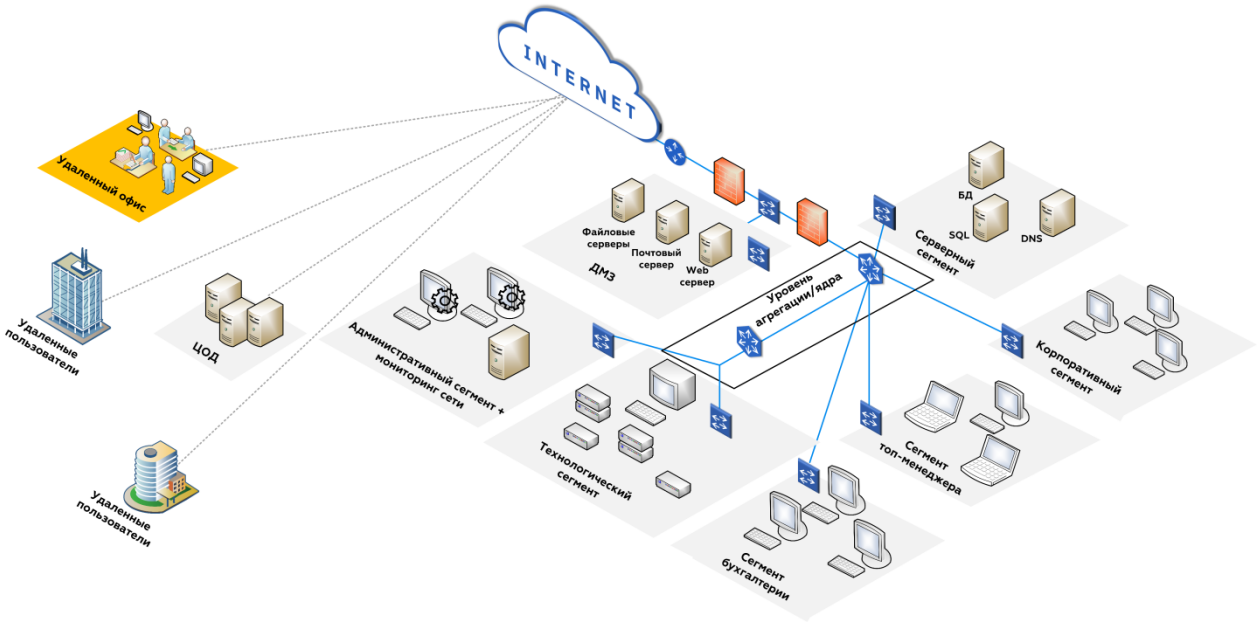
Директор по аналитике и интеграции
АО «НПП «Цифровые решения»

Проблемы современной ИТ-инфраструктуры

ЦИФРОВЫЕ РЕШЕНИЯ

20 лет назад

Сегодня



Усложнение ИТ-инфраструктуры, увеличение скоростей и количества проколов передачи данных требует внедрения инструментов анализа и ИБ различных типов.
В свою очередь, такие инструменты имеют ограничения по подключению и производительности, а также свои требования к исходным данным и критичности работы.

Системы, которым требуется трафик

ЦИФРОВЫЕ РЕШЕНИЯ

ИТ

- NPM
- UC
- APM

ИБ

- NTA
- IPS
- DLP
- Anti-DDoS
- UTM
- NGFW
- IDS
- SIEM

Важность передачи полных и целевых данных

ЦИФРОВЫЕ РЕШЕНИЯ

Попробуйте решить.
Легко?

$$\begin{cases} x^2 + y + 2z = 8 \\ x + 2y^2 + 4z = 11 \\ x + 11y^2 + 8z^2 = 0 \end{cases}$$

А так?

$$\begin{cases} x^2 + y + ?\, z = 8 \\ ? + 2y^? + 4z = 11 \\ x + ?\, y^? + 8z^2 = ? \end{cases}$$

Инструменты обеспечения безопасности эффективны и многофункциональны, но только в том случае, если на них передаются полные и целевые данные.

Связующее звено в ИТ-инфраструктуре

ЦИФРОВЫЕ РЕШЕНИЯ

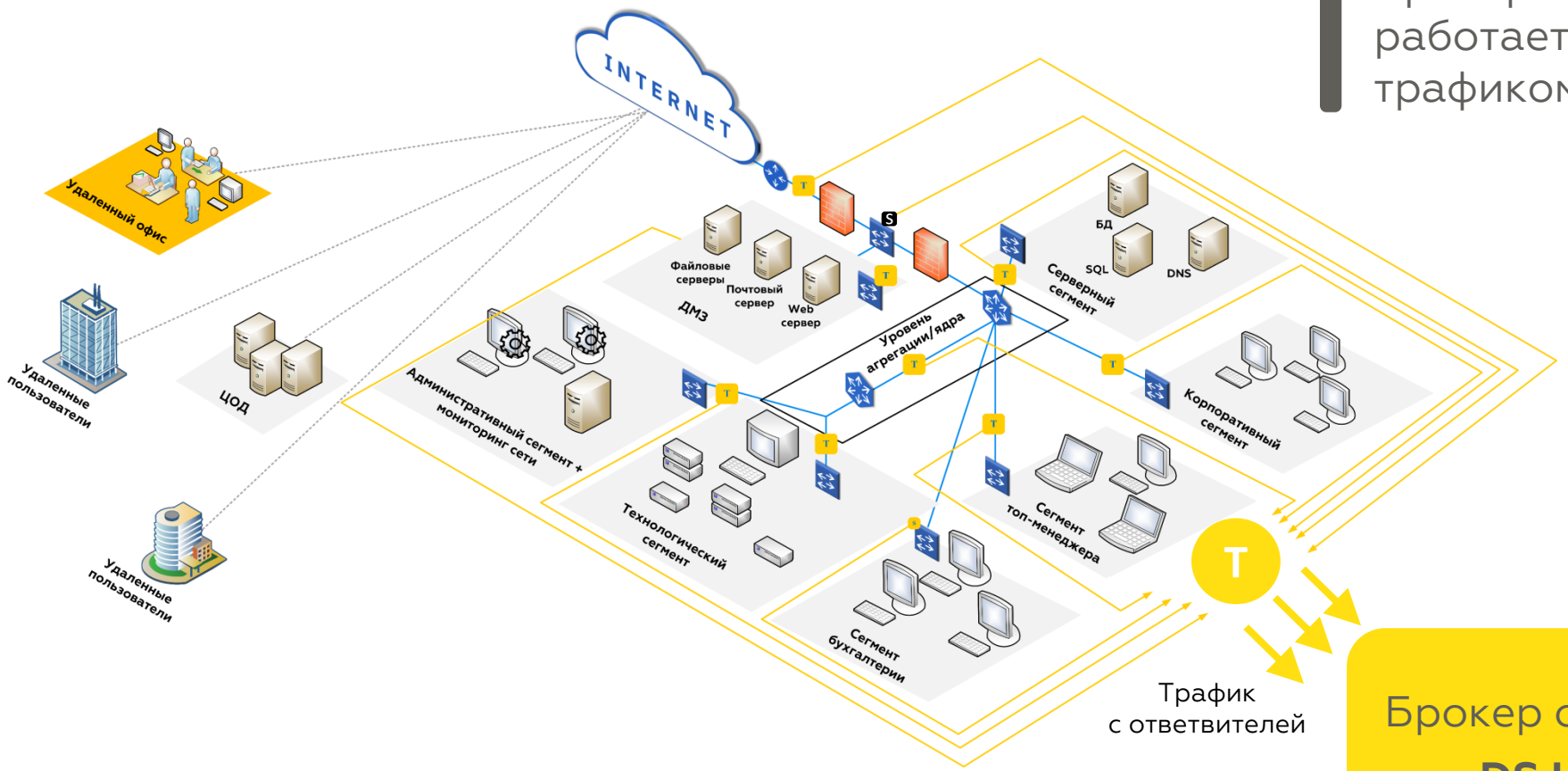
Брокер сетевых пакетов связывает две ключевых области внутри ИТ-инфраструктуры:

- Помогает организовать эффективную схему взаимодействия оборудования
- Оптимизирует весь трафик перед отправкой на системы мониторинга и ИБ

Современный способ подключения

ЦИФРОВЫЕ РЕШЕНИЯ

Брокер сетевых пакетов DS Integrity NG работает как с трафиком от TAP, так и с трафиком со SPAN-портов

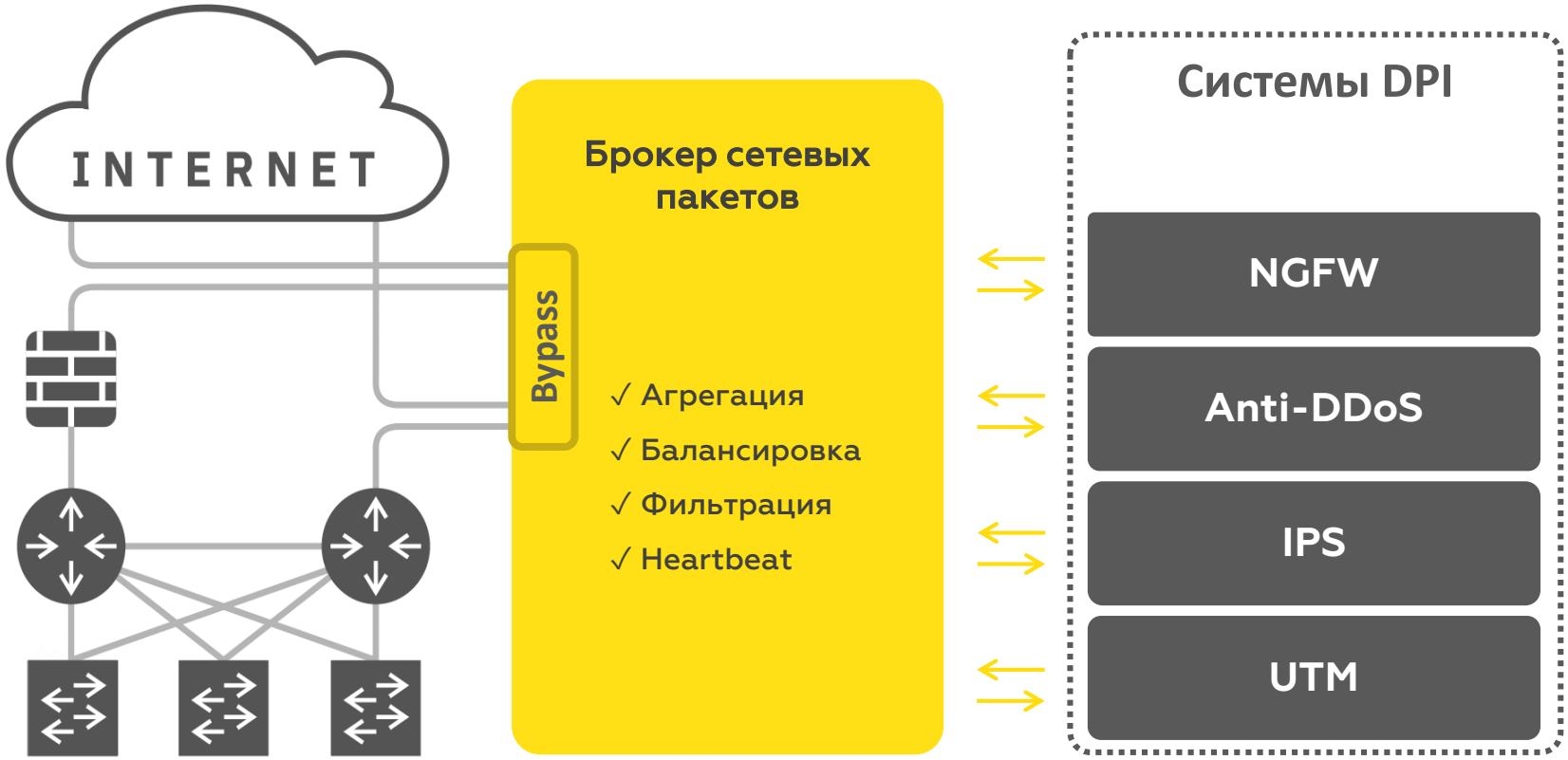


Брокер сетевых пакетов
DS Integrity NG

ИТ

ИБ

Активное подключение средств анализа и ИБ



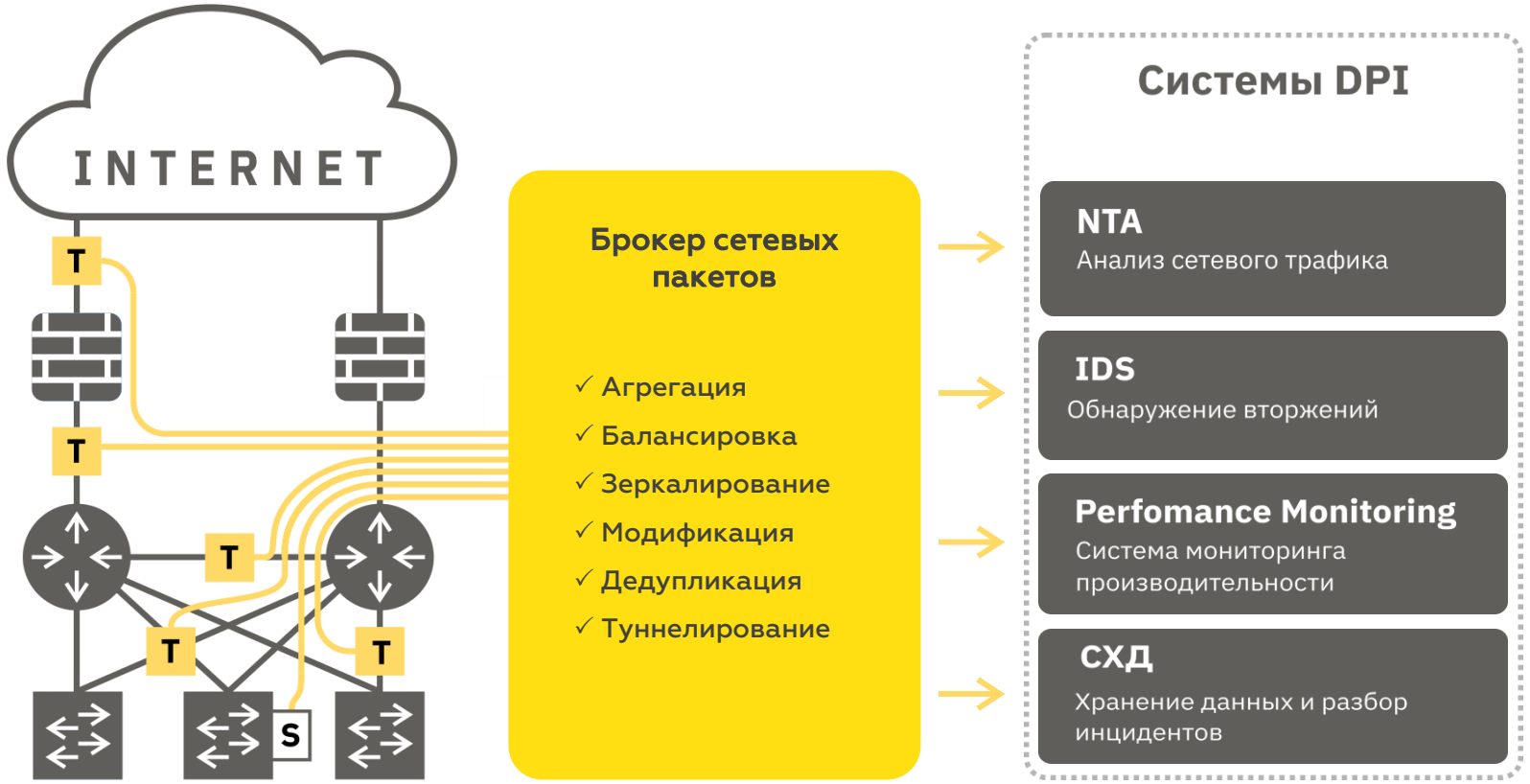
КОД безопасности

UserGate

✓ Технологические партнёры

Активное подключение предполагает установку брокера сетевых пакетов **с функцией Bypass** «в разрыв» канала

Пассивное подключение средств анализа и ИБ



positive technologies

✓ Технологический партнёр

Пассивное подключение брокера сетевых пакетов к ИТ-Инфраструктуре осуществляется через SPAN-порты или ответвители трафика (TAP), например, с помощью ответвителей DS Optic-TAP или DS Copper-TAP

Сравнение пассивного подключения через SPAN и TAP

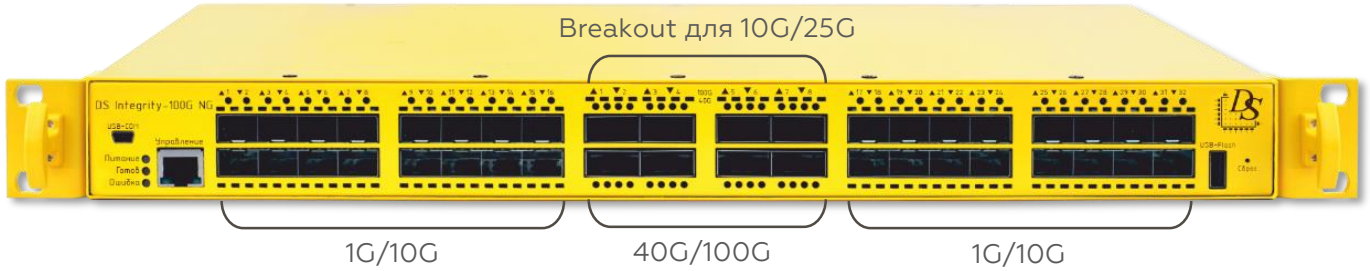
ЦИФРОВЫЕ РЕШЕНИЯ

	ИТ	ИБ
SPAN-порт коммутатора	+ Функция коммутатора обычно уже встроена — Требуется периодическая проверка настроек — Приводит к потере пакетов, к деградации или даже к нарушению функционирования сети	+ Не требует дополнительных расходов — Имеет низкий приоритет, что ведет к потере пакетов — Высокая зависимость от настроек (в т.ч. в случае взлома) — Не все пакеты зеркалируются — Отсутствует возможность оптимизации трафика
TAP ответвители	+ Полная прозрачность для сетевых устройств (нет влияния на передачу трафика) + Не требуют специальной настройки и обновлений + Зеркалируют служебный трафик, полезный для траблшутинга сети — Требуют технологическое окно для установки	+ Снимают 100% копию трафика без искажений + Пассивное решение, которое невозможно вывести из строя внешними атаками + Легко масштабируется — Приобретается как самостоятельное решение

Брокеры сетевых пакетов DS Integrity NG и ответвители трафика DS TAP

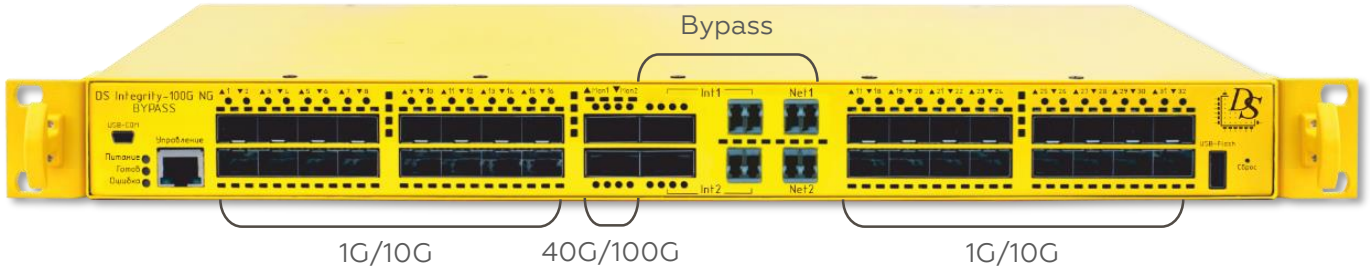
ЦИФРОВЫЕ РЕШЕНИЯ

Включены в реестры
Минпромторга и Минцифры



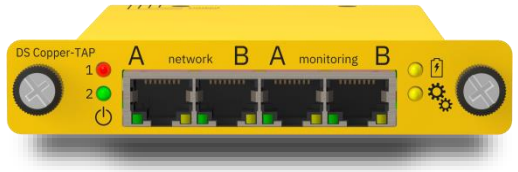
DS INTEGRITY NG

- до 4 интерфейсов 100G Ethernet
- до 8 интерфейсов 40G Ethernet
- до 32 интерфейсов 25G Ethernet
- до 64 интерфейсов 10G Ethernet
- до 32 интерфейсов 1G Ethernet
- Производительность до 720 Гбит/с



DS INTEGRITY NG BYPASS

- до 2 интерфейсов 100G/40G Ethernet
- до 32 интерфейсов 10G/1G Ethernet
- Производительность до 720 Гбит/с
- Контроль состояния средства мониторинга (Heartbeat)

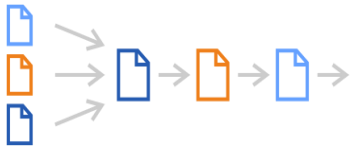


DS COPPER-TAP
Медные ответвители трафика

DS OPTIC-TAP
Оптические ответвители трафика

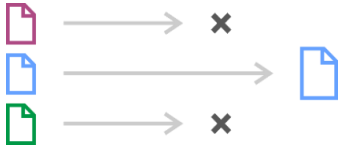
Функционал DS Integrity NG

БАЗОВЫЕ ФУНКЦИИ



АГРЕГАЦИЯ

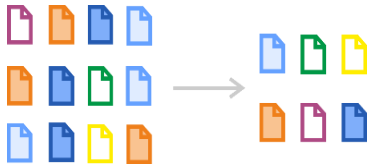
БАЛАНСИРОВКА



ФИЛЬТРАЦИЯ

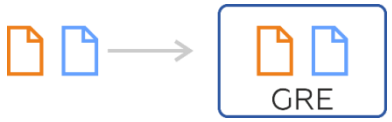
ЗЕРКАЛИРОВАНИЕ

ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ



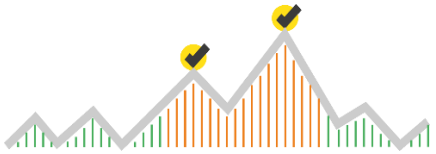
ДЕДУПЛИКАЦИЯ

МОДИФИКАЦИЯ



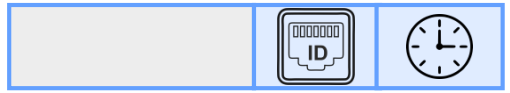
ТУННЕЛИРОВАНИЕ

РАЗБОР ТУННЕЛЕЙ



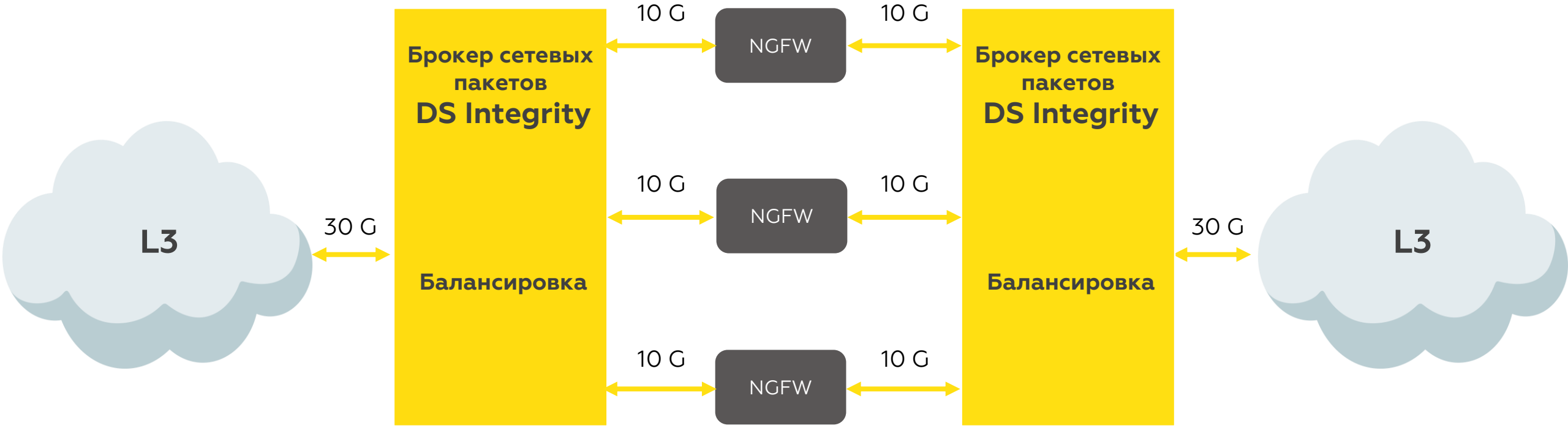
ЗАЩИТА ОТ ВСПЛЕСКОВ

ГЕНЕРАЦИЯ sFlow



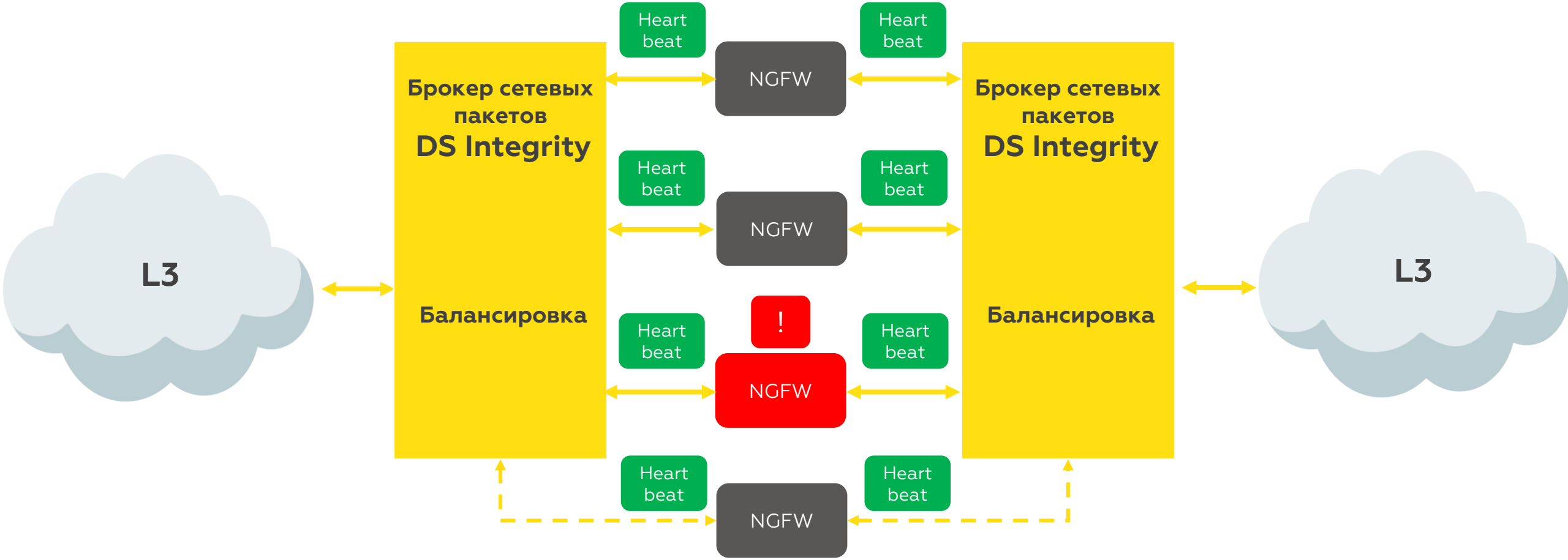
PORT STAMPING, TIME STAMPING

Распределение трафика



Брокер сетевых пакетов DS Integrity балансирует нагрузку на необходимое количество анализаторов, разделяя потоки трафика с сохранением целостности сессий/потоков

Резервирование систем и проверка их работоспособности



Для контроля работоспособности отдельных устройств, брокер сетевых пакетов DS Integrity NG добавляет в трафик специальные пакеты (технология Heartbeat).
Если обнаруживается нерабочее устройство, происходит мгновенная перебалансировка трафика между оставшимися в кластере средствами.

Дополнительные возможности

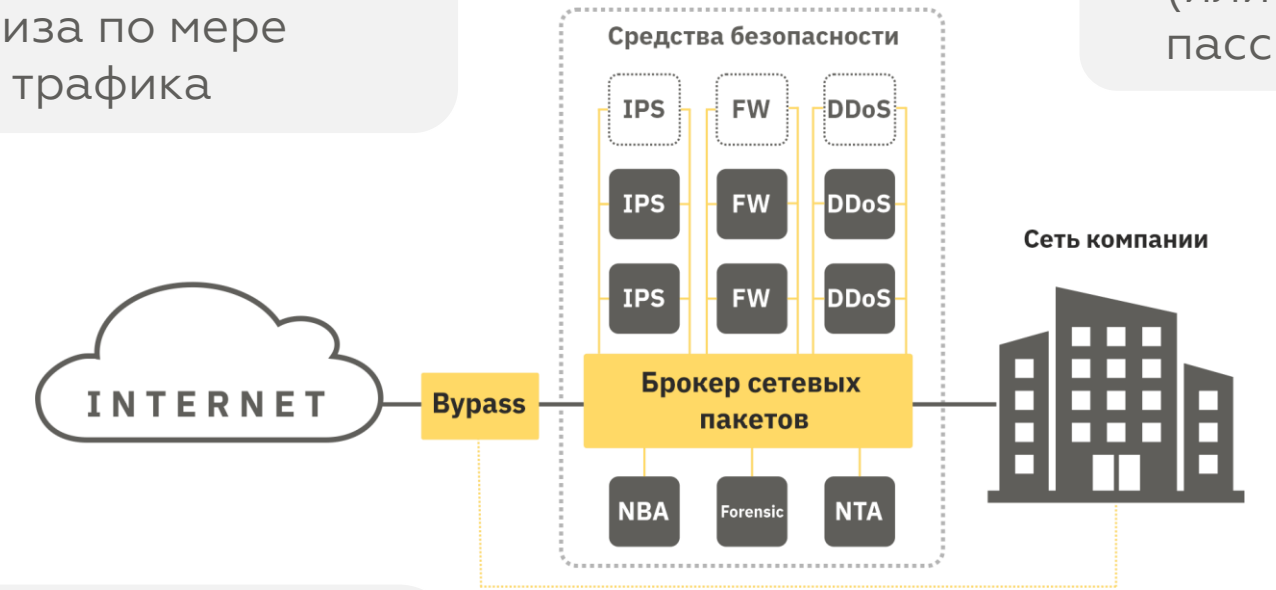
ЦИФРОВЫЕ РЕШЕНИЯ

1

Постепенное добавление дополнительных единиц средства анализа по мере роста потоков трафика

2

Зеркалирование всего (или части) трафика на пассивные средства анализа



3

Подключение активных средств анализа других типов (например, antiDDOS) с независимой балансировкой и резервированием

4

Оптимизация нагрузки за счёт настройки правил фильтрации (отбрасывание или пропуск мимо межсетевого экрана)

От моновендорных решений к комплексной системе

ЦИФРОВЫЕ РЕШЕНИЯ

ЕДИНОЕ РЕШЕНИЕ

+ Простая настройка

– Сложности при масштабировании архитектуры и внедрении новых систем

ЕДИНАЯ СИСТЕМА

+ Дополнительные возможности по конфигурации и предобработке трафика

– Нетипичная первоначальная инициализация

Итоги 2022 года

ЦИФРОВЫЕ РЕШЕНИЯ

6 Министерств и госслужб

8 Российских IT-компаний из ТОП-100

6 Российских банков из ТОП-25

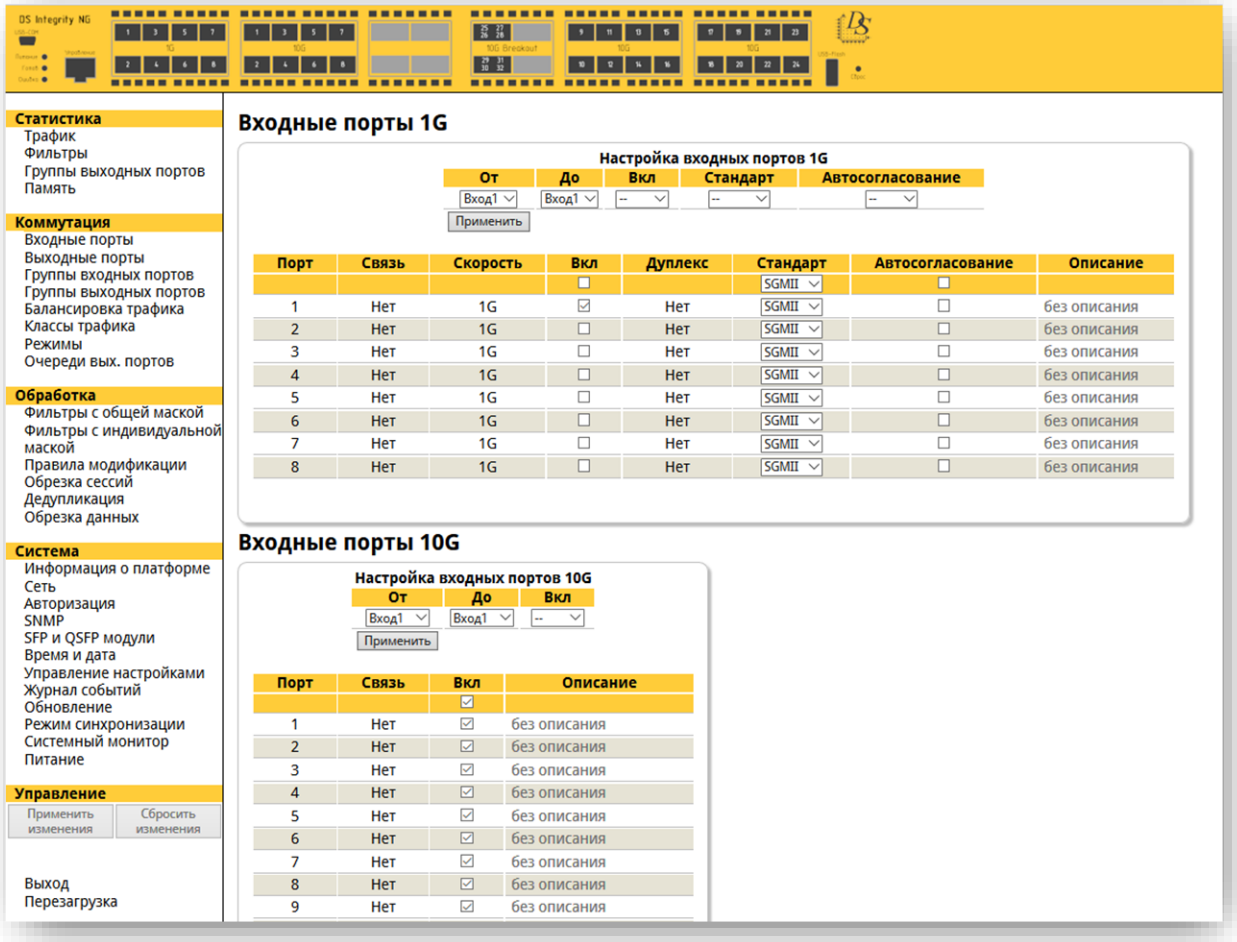
DS Integrity NG в инфраструктуре

5 Логистических и транспортных компаний из ТОП-100

5 Компаний гос. сектора

3 Энергетических компаний

Не упусти возможность «порулить» брокером сетевых пакетов DS Integrity



Пройди QUIZ на стенде нашей компании и **участвуй в розыгрыше**!

ЦИФРОВЫЕ РЕШЕНИЯ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ

г. Москва, проезд Завода Серп и Молот,
д. 10, БЦ Интеграл

8 (495) 978-28-70 (116)

sales@dsol.ru
plotko@dsol.ru

habr