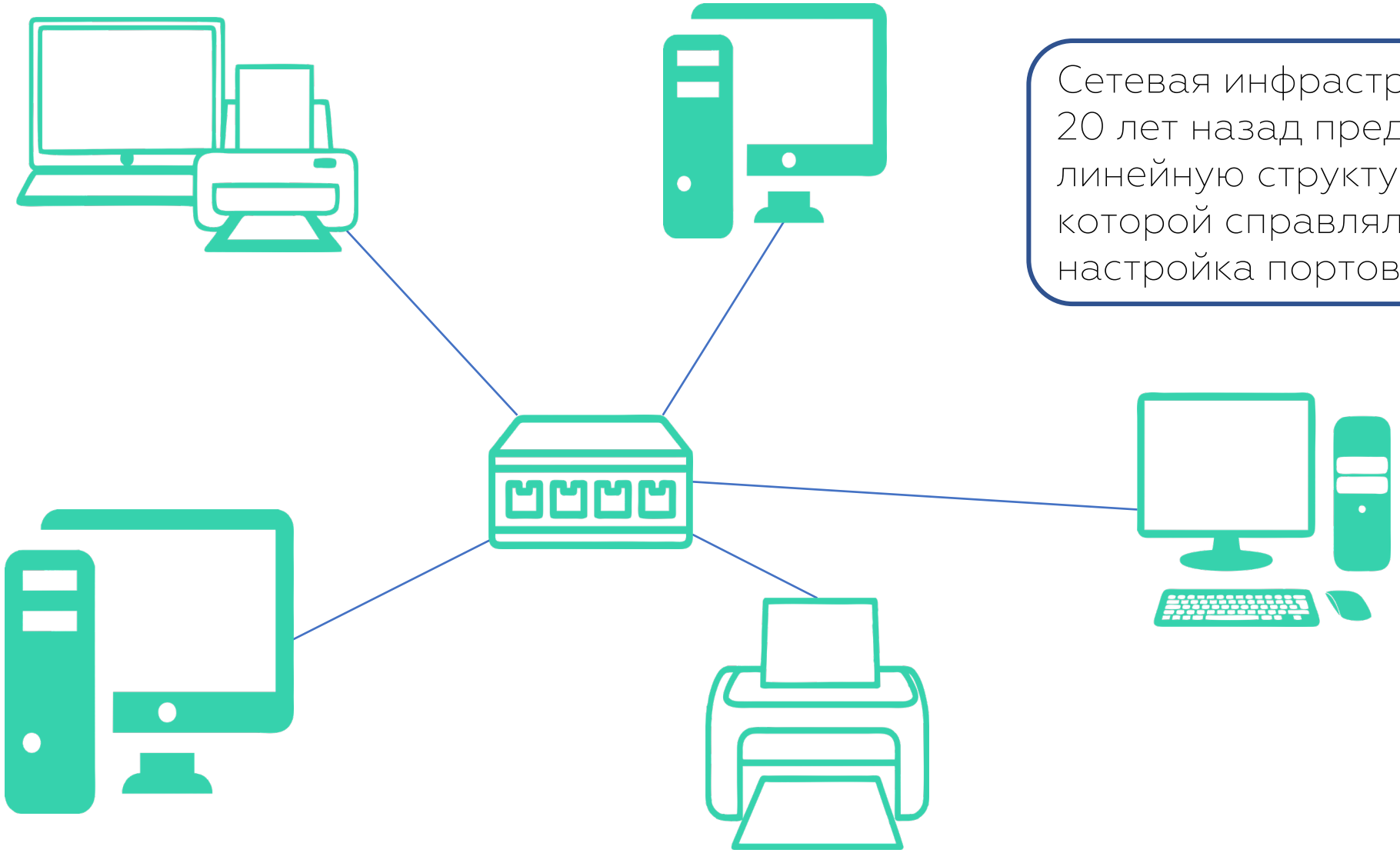
ЦИФРОВЫЕ РЕШЕНИЯ

Импортозамещение как возможность построить технологичную архитектуру ИБ

Сергей Плотко
Директор по аналитике
и интеграции

ЦИФРОВЫЕ РЕШЕНИЯ

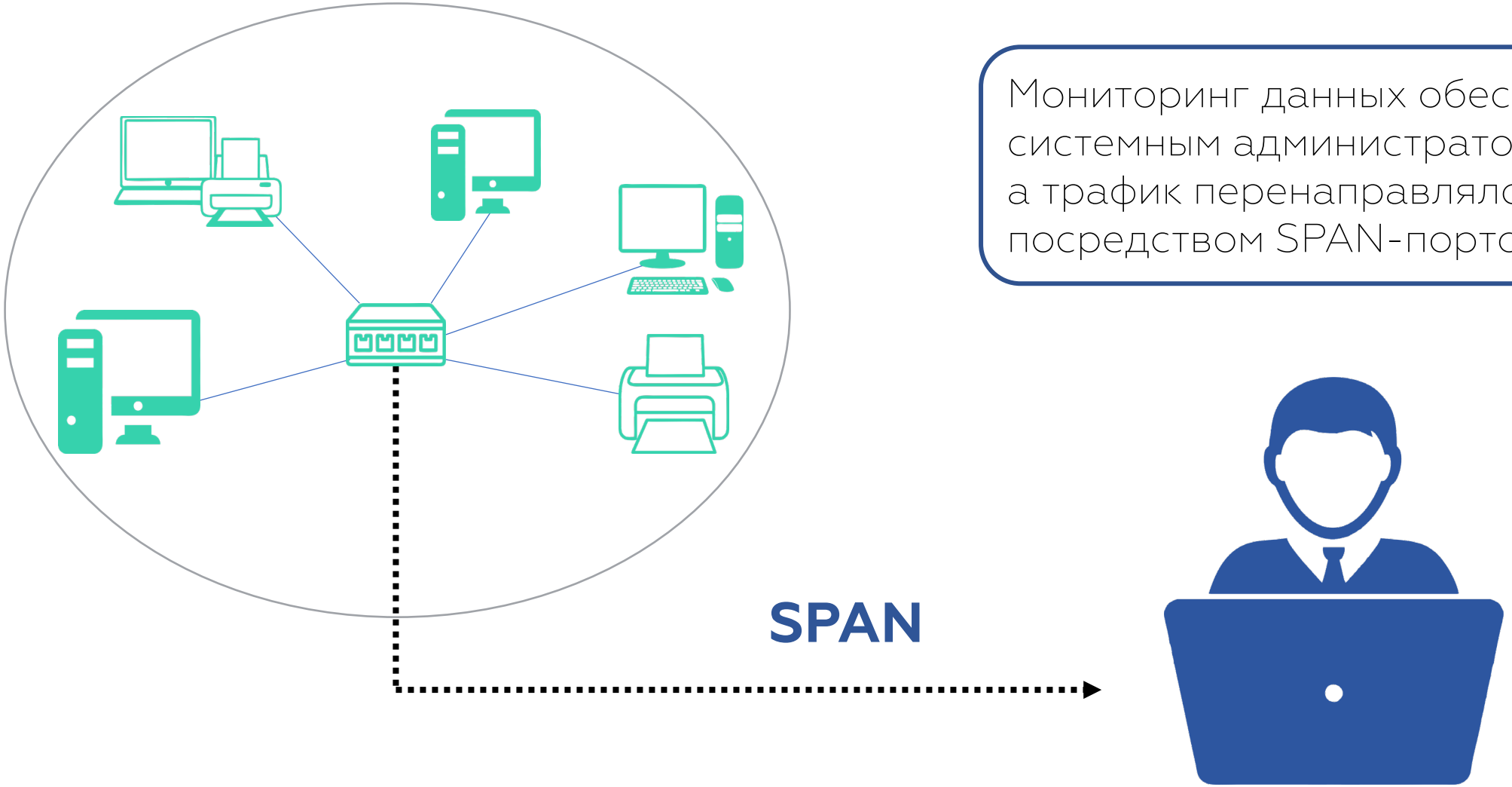
Сетевая инфраструктура 20 лет назад



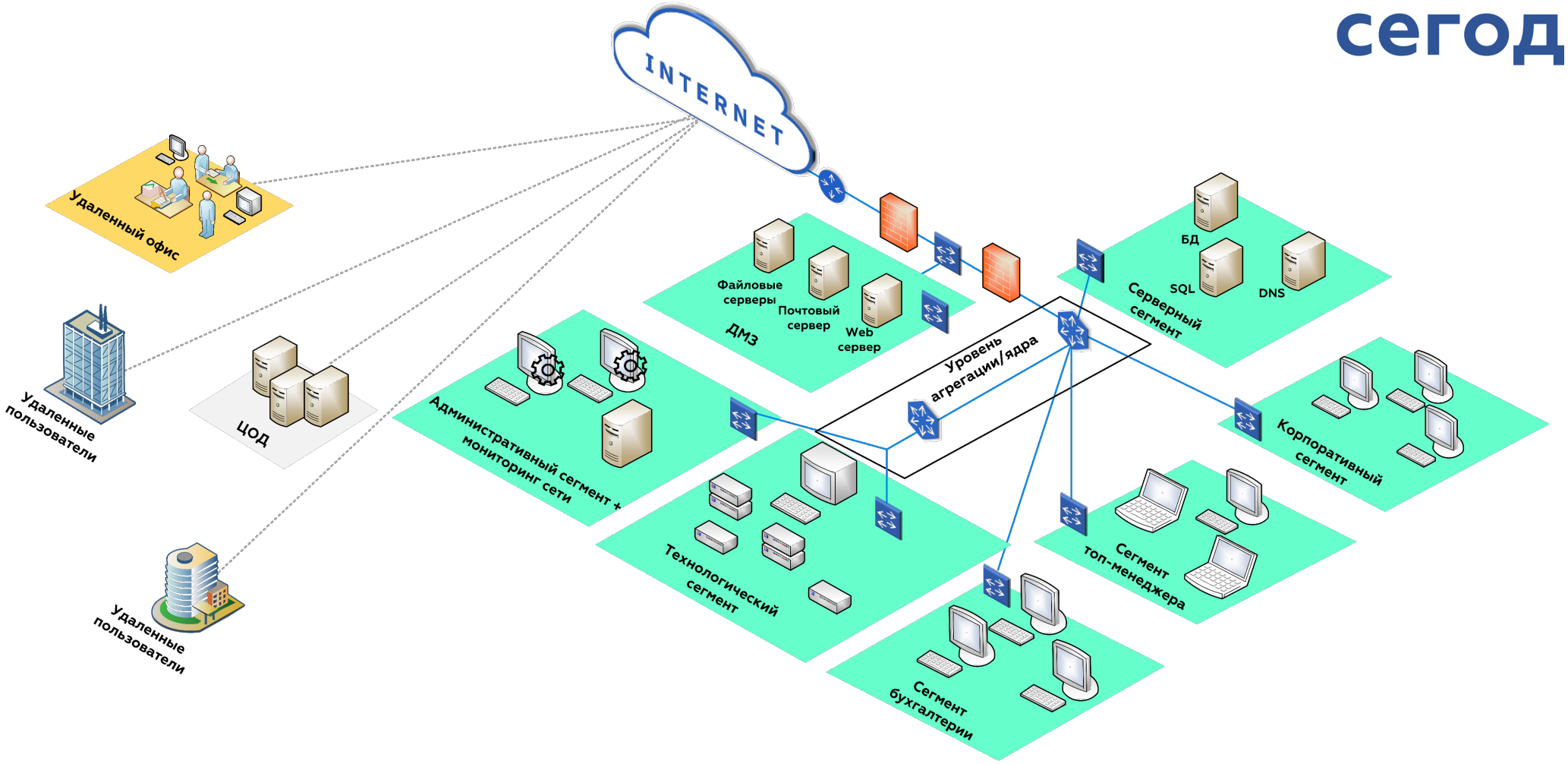
Сетевая инфраструктура организаций 20 лет назад представляла собой линейную структуру, с защитой которой справлялись антивирусы и настройка портов на периметре

Зеркалирование трафика 20 лет назад

Мониторинг данных обеспечивался системным администратором, а трафик перенаправлялся посредством SPAN-портов



Сетевая инфраструктура сегодня

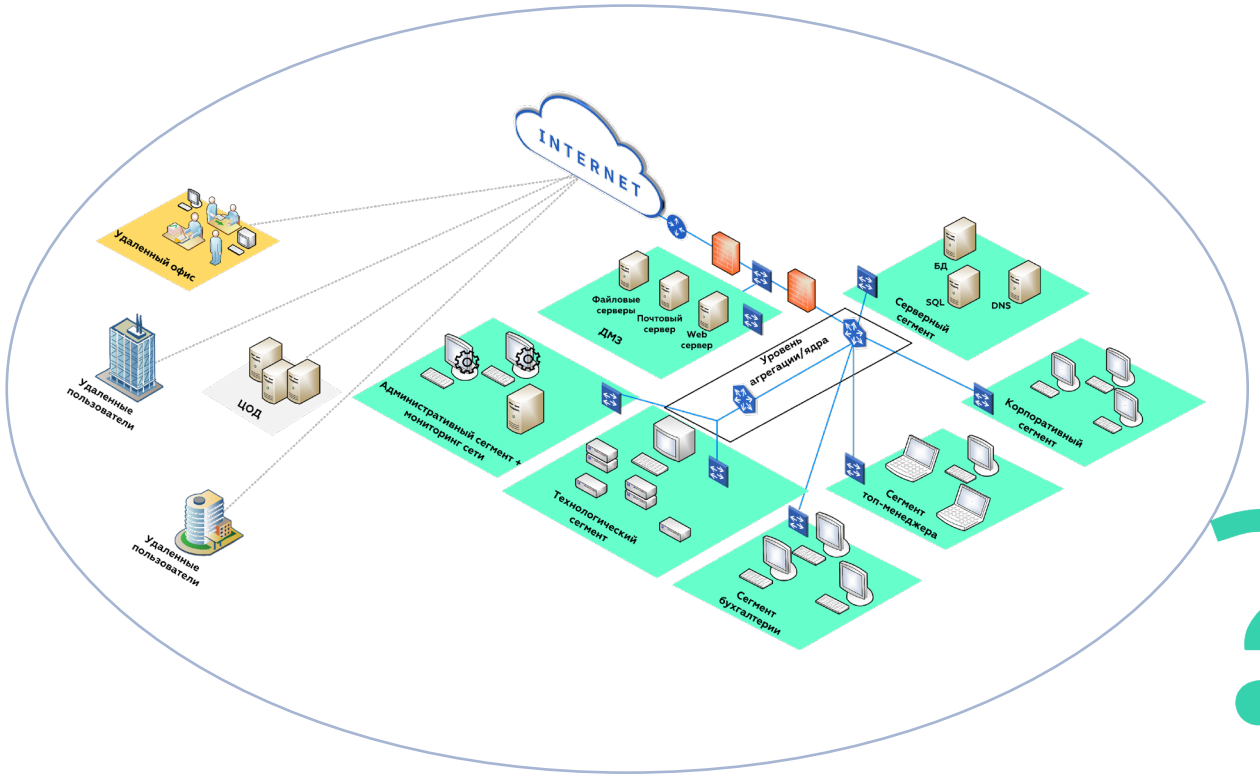


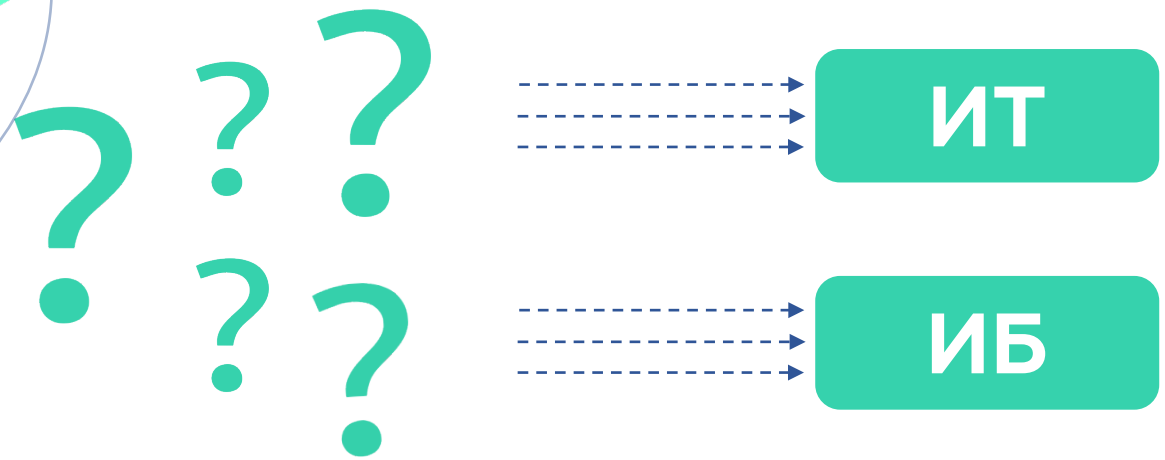
Современная сетевая инфраструктура - сложная сегментированная структура с удаленными офисами, подключением и внешними ресурсами

ЦИФРОВЫЕ РЕШЕНИЯ

Новые требования к зеркалированию трафика

Цифровая трансформация формирует новые требования к мониторингу состояния сети и к информационной безопасности в ней





Системы, требующие трафика

ЦИФРОВЫЕ РЕШЕНИЯ

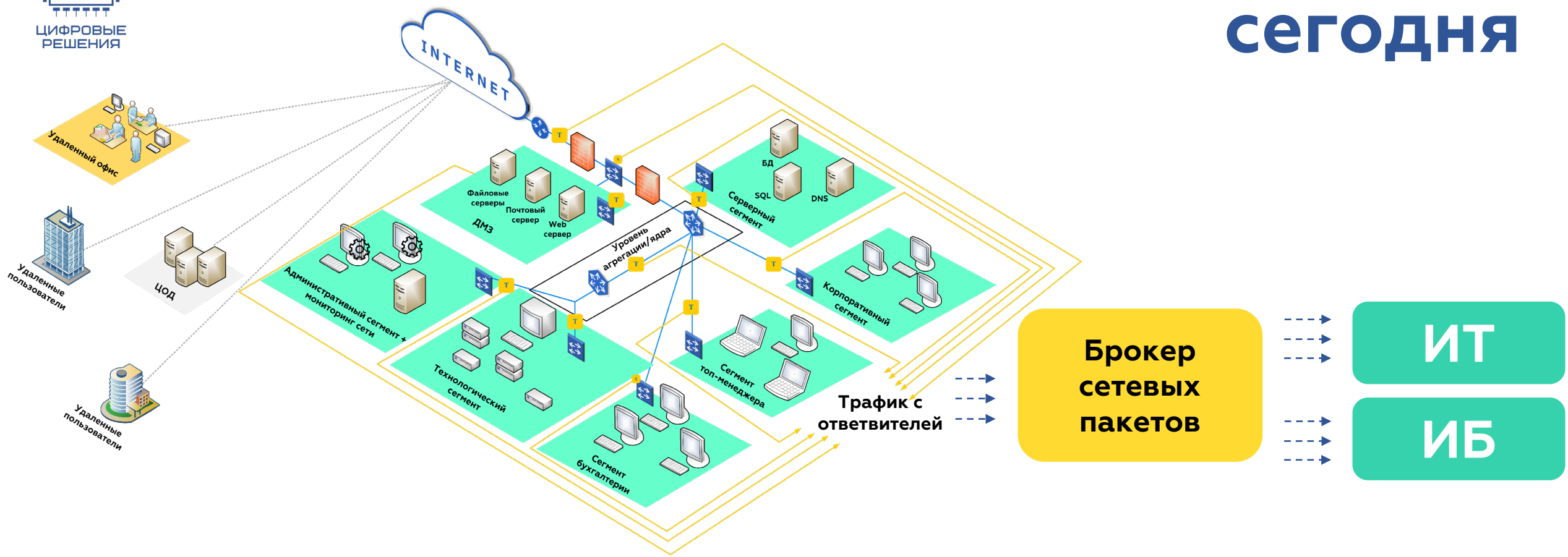
ИТ

- NPM
- UC
- APM

ИБ

- NTA
- IPS
- DLP
- Anti-DDoS
- AMP
- Firewall
- IDS
- SIEM

Зеркалирование трафика сегодня



- Сбор 100% копии трафика из различных точек сети
- Удаление дублирующихся пакетов
- Выделение потоков данных, требующих анализа
- Распределение потоков по системам анализа в необходимом количестве

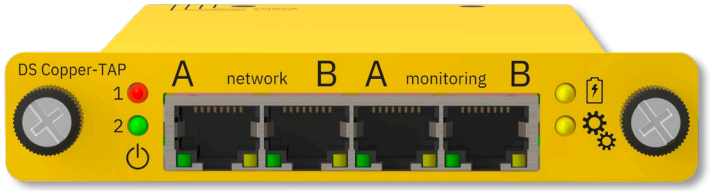
ЦИФРОВЫЕ РЕШЕНИЯ

Ответвители трафика-TAP

DS Optic-TAP
Оптический ответвитель трафика

Включены в реестры Минпромторга

DS Copper-TAP
Медный ответвитель трафика



01 Передача 100% копии трафика без искажений

02 Максимальная надёжность

03 Оптические ответвители не требуют питания

04 Невозможность взлома и вывода из работы путем внешних атак

05 Не влияет на работоспособность сетевой инфраструктуры

06 Модульная архитектура решения позволяет подобрать индивидуальную конфигурацию модулей

ЦИФРОВЫЕ РЕШЕНИЯ

Брокеры сетевых пакетов

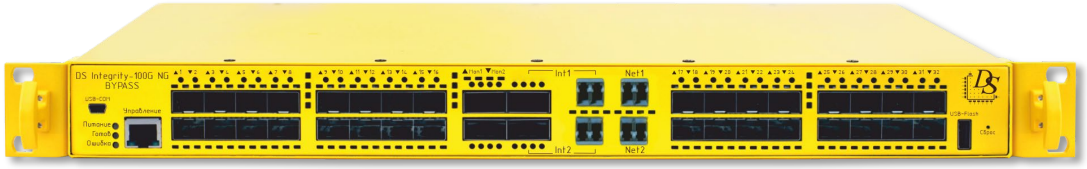
DS INTEGRITY-100G NG

- 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
- Пропускная способность до 2,24 Тбит/с

Включены в реестры Минпромторга и Минцифры

DS INTEGRITY-40G NG

- до 8 интерфейсов 40G Ethernet
- до 64 интерфейсов 10G Ethernet
- до 32 интерфейсов 1G Ethernet
- Пропускная способность до 1,28 Тбит/с



DS INTEGRITY-100G NG BYPASS

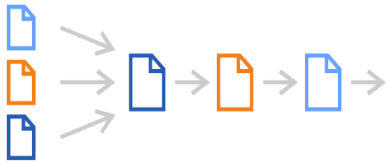
- до 2 интерфейсов 100G Ethernet
- до 32 интерфейсов 10G/1G Ethernet
- Пропускная способность до 1,04 Тбит/с
- Контроль состояния средства мониторинга (Heartbeat)

DS INTEGRITY-40G NG BYPASS

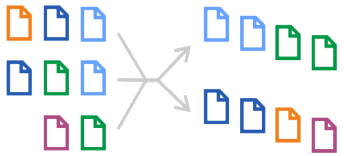
- до 2 интерфейсов 40G Ethernet
- до 32 интерфейсов 10G/1G Ethernet
- Пропускная способность до 0,8 Тбит/с
- Контроль состояния средства мониторинга (Heartbeat)

Функционал DS INTEGRITY

БАЗОВЫЕ ФУНКЦИИ

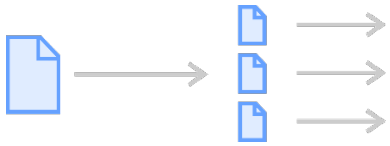


АГРЕГАЦИЯ



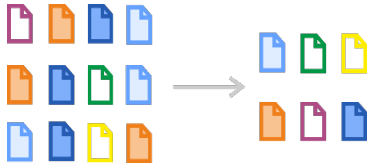
БАЛАНСИРОВКА

ФИЛЬТРАЦИЯ



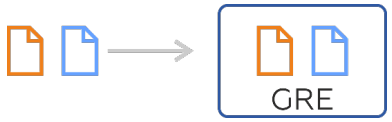
ЗЕРКАЛИРОВАНИЕ

ДОПОЛНИТЕЛЬНЫЕ ФУНКЦИИ

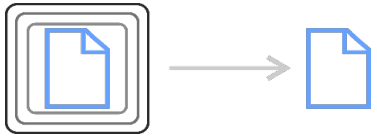


ДЕДУПЛИКАЦИЯ

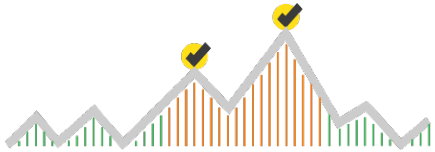
МОДИФИКАЦИЯ



ТУННЕЛИРОВАНИЕ



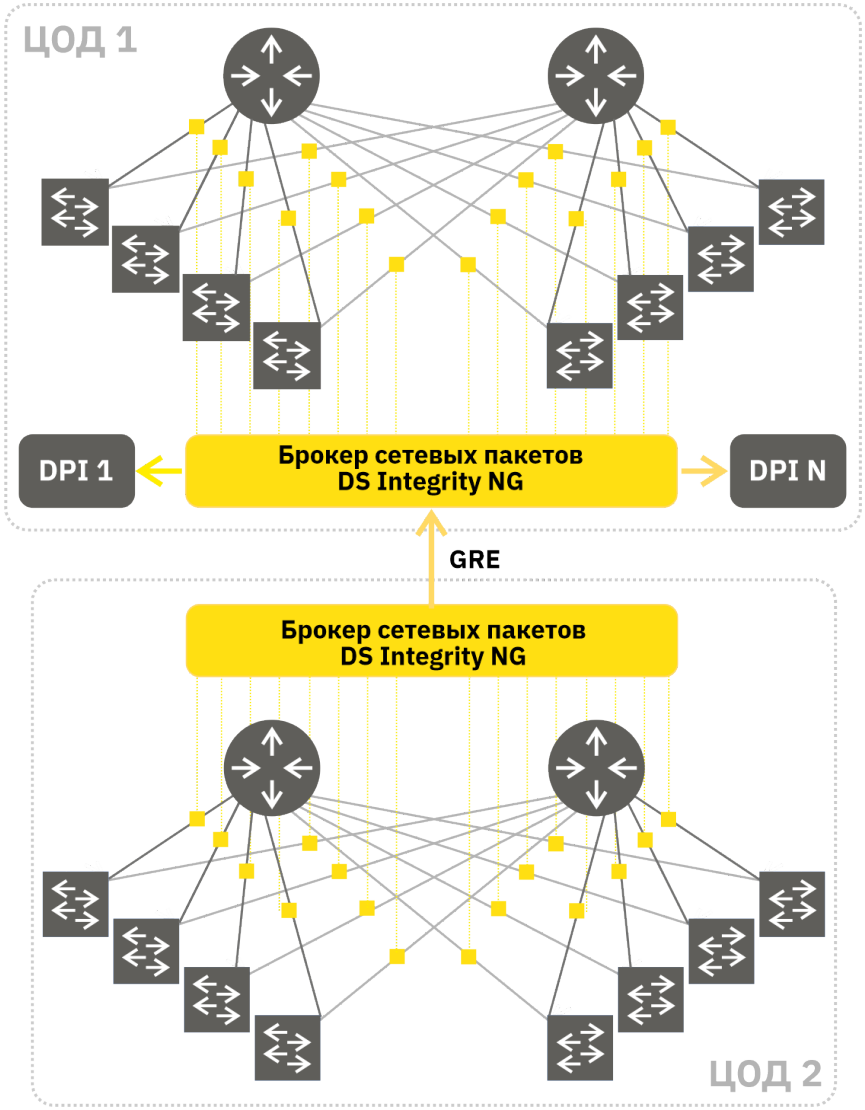
РАЗБОР ТУННЕЛЕЙ



ЗАЩИТА ОТ ВСПЛЕСКОВ

ГЕНЕРАЦИЯ sFlow

Передача трафика для анализа на удаленную площадку



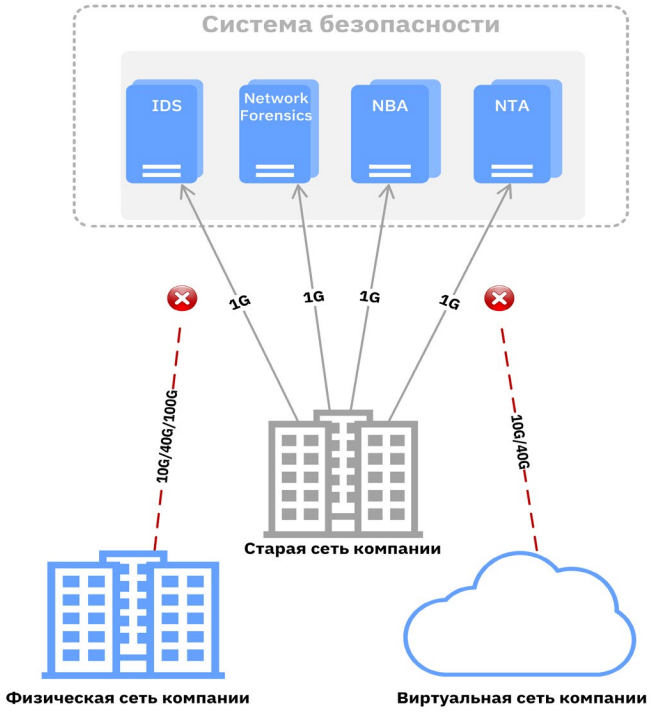
Сбор полной копии трафика и обеспечение одновременной работы нескольких систем анализа и мониторинга, требующих получения идентичного трафика

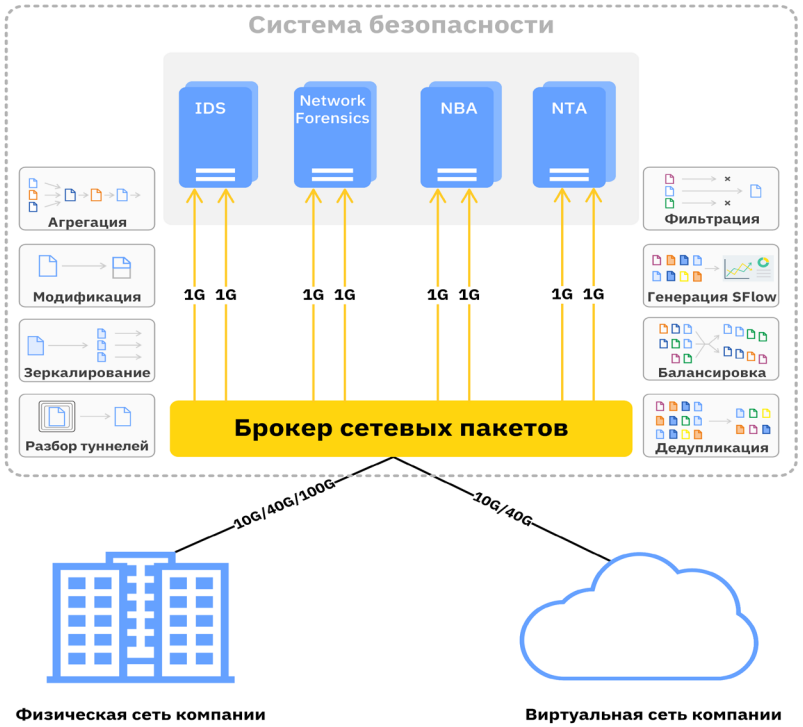
Формирование для каждой из систем анализа и мониторинга потока необходимых для их работы данных

Инкапсуляция трафика в туннель GRE для передачи между несколькими офисами или центрами обработки данных

Группирование портов и фильтрация трафика для сегментации сеть и разделения анализа по географическому или структурному принципу

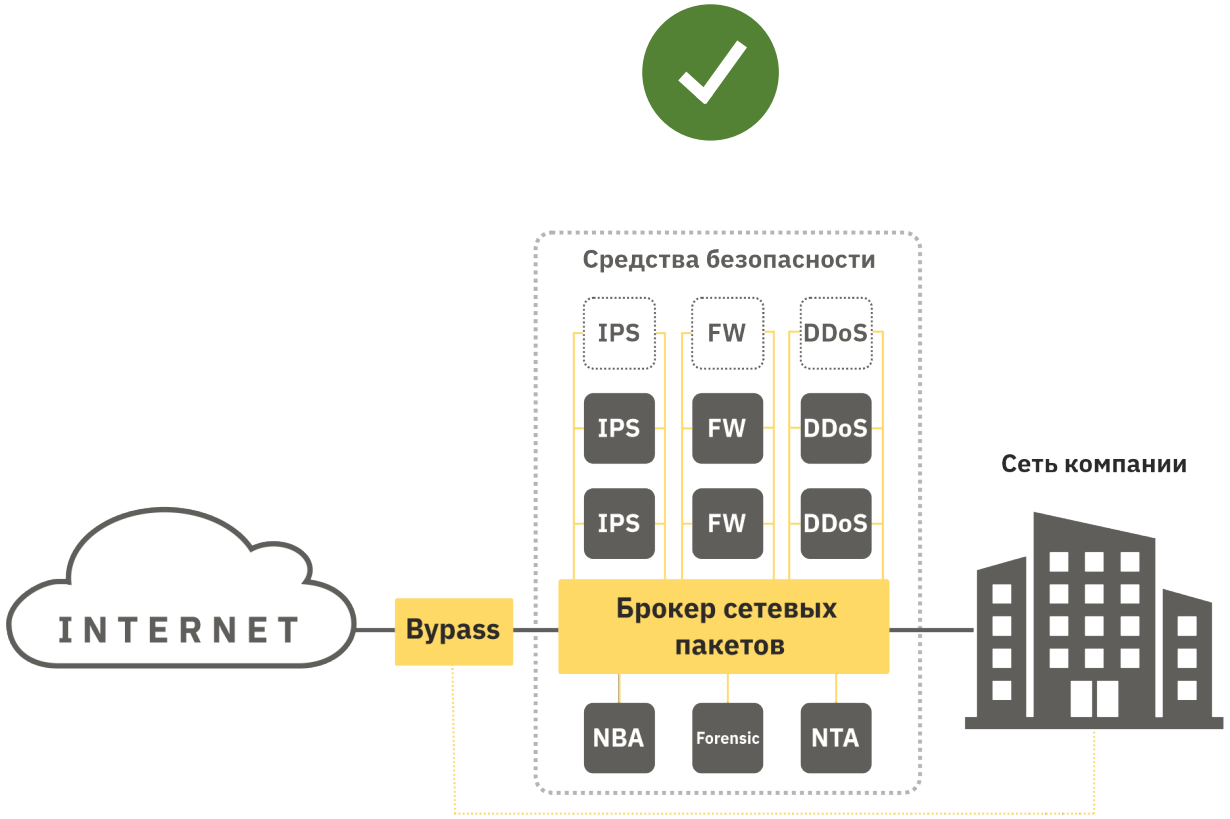
Инструменты безопасности 1G в современных сетях





- Легкое совмещение интерфейсов сети и средств анализа
- Независимая модернизация сети и средств анализа
- Продление срока жизни средств анализа за счёт предобработки трафика

Подключение активных средств безопасности (в разрыв)



- Гарантия целостности инфраструктуры за счёт оптического и логического Bypass
- Возможность логического пропускания части трафика без передачи в средства анализа и мониторинга
- Различные варианты пропускания трафика через активные устройства
- Возможность подключения пассивных средств анализа
- Обеспечение отдельного резервирования для каждого средства анализа и мониторинга
- Возможность балансировки нагрузки между средствами анализа с резервированием по схеме N+1

Оптимизация затрат на системы DPI

Параметр сети	Значение
Среднесуточный совокупный сетевой трафик для каждого набора сетевых инструментов (например, APM, NPM, IDS и т. д.)	100 Гбит/с
Ожидаемый среднегодовой рост трафика за анализируемый период (пять лет)	10%
Средняя производительность отдельного инструмента DPI	20 Гбит/с
Средняя текущая загрузка инструмента	70%
Максимальная загрузка инструментов	80%

Ваша экономия с DS Integrity

СОВОКУПНАЯ ЭКОНОМИЯ ЗАТРАТ ЗА 3 ГОДА

176 млн. руб.

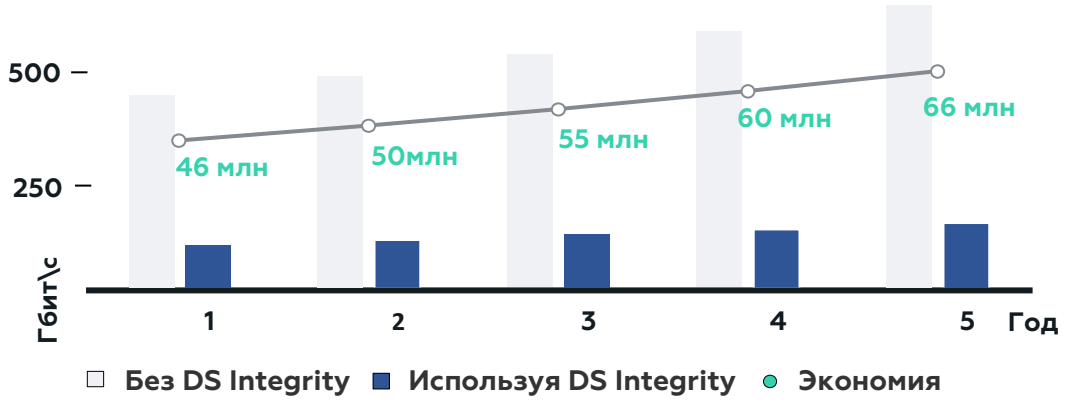
ОКУПАЕМОСТЬ ИНВЕСТИЦИЙ

7 месяцев

Наименование инструмента DPI	Стоимость, руб.*
IDS (Intrusion Detection System)	9 млн.
NPM (Network Performance Monitoring)	6 млн.
COPM (forensics)	34 млн.
DLP (Data Loss Prevention) inline	10 млн.
AMP (Advanced Malware protection)	30 млн.

* Включая обслуживание и обновления на 3 года

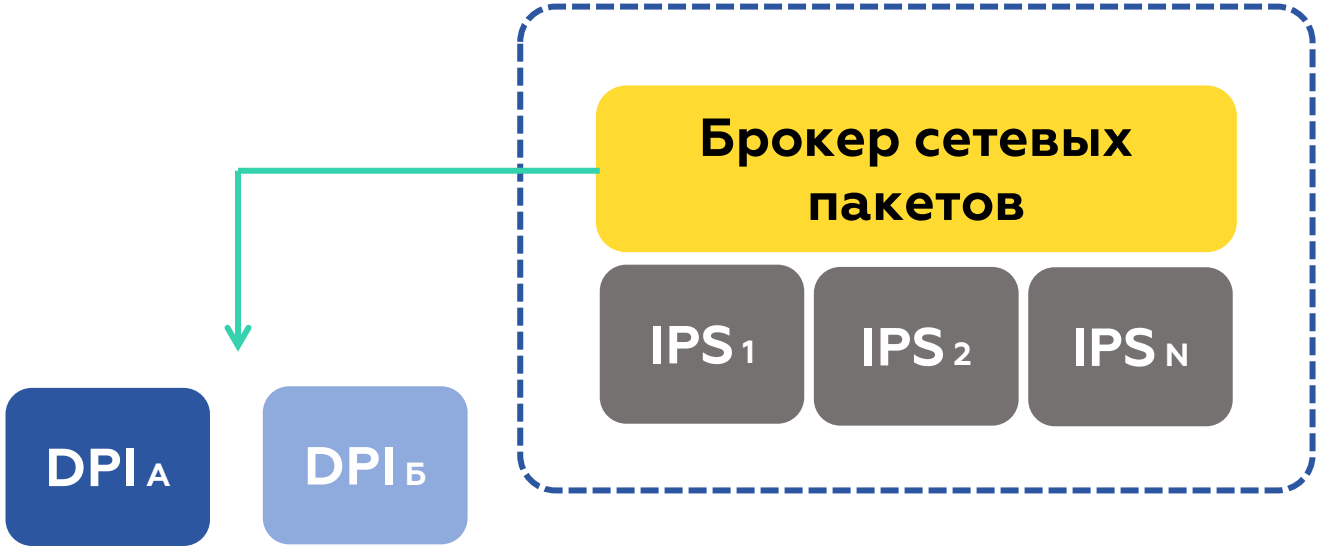
Совокупное снижение трафика с течением времени



От моновендорных решений к комплексной системе

ЕДИНОЕ РЕШЕНИЕ

ЕДИНАЯ СИСТЕМА



+ Простая настройка

– Сложности при масштабировании архитектуры и внедрении новых систем

+ Дополнительные возможности по конфигурации и предобработке трафика

– Нетипичная первоначальная инициализация

Сравнение с зарубежными аналогами

Параметр	НПП «Цифровые решения» DS Integrity-100G NG	Gigamon * GigaVUE-HC1	IXIA * Vision ONE
Количество портов 100G/40G	до 4 / 8	до - / 8	до - / 4
Количество портов 25G	до 32	–	–
Количество портов 10G/1G	до 64 / 32	до 36 / 40	до 48 / 48
Пропускная способность	до 2240 Гбит/с	до 1208 Гбит/с	до 1280 Гбит/с
Производительность на дополнительных функциях	до 1120 Гбит/с	до 100 Гбит/с	до 160 Гбит/с
Дедупликация	✓	✓	✓
Защита от всплесков трафика	✓	–	✓ (только для 1G)
Jumbo Frame	16000 байт	9216 байт	9216 байт
Генерация sFlow/NetFlow/IPFIX	sFlow, NetFlow\IPFIX**	NetFlow/IPFIX	NetFlow/IPFIX
Мониторинг работоспособности подключенных инструментов DPI	✓	✓	✓
Единая система управления / интеграция с сторонним ПО	✓/NETCONF***	✓/REST API	✓/RESTful API
Поддержка протоколов аутентификации	LDAP, TACACS+, RADIUS	LDAP, TACACS+, RADIUS	LDAP, TACACS+, RADIUS
Потребляемая мощность	До 150 Вт	До 212 Вт	До 212 Вт
Срок службы	5 лет	5 лет	5 лет
Стоимость	**70 370 $**	**62 465 $**	**99 800 $**

* Поставки в РФ временно прекращены

**Дорожная карта II квартал 2023

***Дорожная карта II-III квартал 2022

ЦИФРОВЫЕ РЕШЕНИЯ

ЕСЛИ БРОКЕР СЕТЕВЫХ ПАКЕТОВ – ТО DS INTEGRITY

Аппаратная реализация базовых и дополнительных функций
отсутствие снижения производительности и потерь трафика

Обеспечение полного набора функций работы с туннелированным трафиком

Российская разработка и производство

ЦИФРОВЫЕ РЕШЕНИЯ

Используете платформу доставки трафика?

да

Анализируем текущее решение

Пилотируем

Комфортное импортозамещение

Ознакомление с нашей платформой на киберполигоне THE STANDOFF

нет

Проектируем систему

Пилотируем

Интегрируем

Импортонезависимая и технологичная система анализа

ЦИФРОВЫЕ РЕШЕНИЯ

Наши заказчики

Финансовые организации

АСУ ТП Энергетика

Корпорации Крупный бизнес

Гос. ведомства Министерства

ЦИФРОВЫЕ РЕШЕНИЯ

СПАСИБО ЗА ВНИМАНИЕ!

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

sales@dsol.ru
plotko@dsol.ru

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