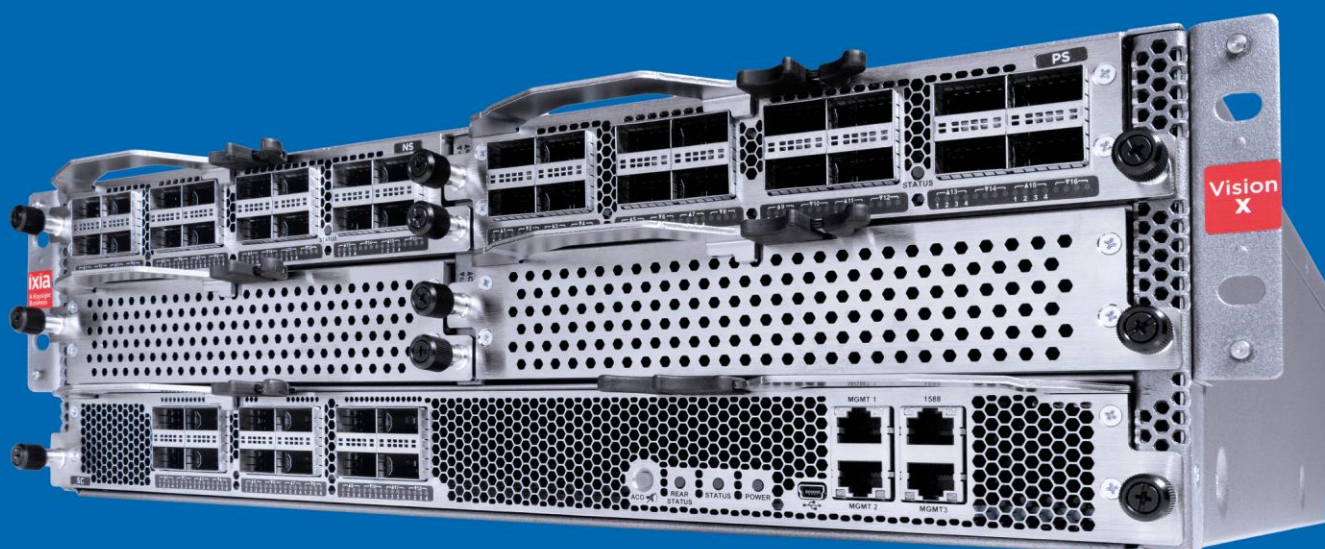


АКМЕТРОН

KEYSIGHT · NETWORK VISIBILITY



БРОКЕРЫ СЕТЕВЫХ ПАКЕТОВ

NETWORK PACKET BROKERS

Практическое руководство по проектированию, выбору, испытаниям и эксплуатации

Актуализация 2026

НАЗНАЧЕНИЕ ДОКУМЕНТА

Руководство для инженеров и лиц, принимающих решения

Как спроектировать фабрику сетевой видимости, выбрать NPВ по измеримым критериям, доказать его производительность в PoC и безопасно эксплуатировать в физической, виртуальной и облачной среде.

КЛЮЧЕВОЙ ПРИНЦИП

NPВ не создает видимость сам по себе. Он сохраняет, нормализует и доставляет наблюдаемые данные. Полнота результата ограничена качеством исходной точки доступа, производительностью конвейера и возможностями подключенного инструмента.

Для кого предназначено руководство

Роль	Какие решения помогает принять документ
Сетевой инженер / архитектор	Где снимать трафик, как рассчитать емкость, выбрать интерфейсы, туннели, фильтры и схему отказоустойчивости.
SecOps / SOC	Как доставлять достоверные пакеты и метаданные в NDR, IDS/IPS, DLP и forensic-системы без скрытых потерь.
NetOps / NOC / APM	Как разделять сетевую и прикладную проблематику, организовать timestamping и ускорить локализацию неисправностей.
CloudOps / Platform Engineering	Как объединить VPC/VNet mirroring, виртуальные узлы, Kubernetes/eBPF и on-premises-инструменты.
ЛПР / закупки / финансы	Как сравнивать предложения, считать TCO/ROI, формировать RFP и принимать решение на основании PoC.

Как использовать документ

- Начать с резюме и дерева решения, чтобы определить целевой эффект и границы проекта.
- Провести обследование по чек-листу и выполнить расчет трафика до запроса коммерческих предложений.
- Перенести требования в матрицу RFP и исключить формулировки, которые нельзя проверить.
- Провести PoC на одинаковом профиле трафика и зафиксировать потери, latency, переключение и ресурсные ограничения.
- Использовать приложения как основу протокола приемки и эксплуатационного runbook.

ГРАНИЦА ОТВЕТСТВЕННОСТИ

Документ не заменяет datasheet, release notes, руководство конкретной версии ПО и проектную документацию. Все численные характеристики оборудования должны подтверждаться для выбранной модели, лицензии и версии программного обеспечения.

Содержание

Структура построена от бизнес-задачи к архитектуре, проверке и эксплуатации.

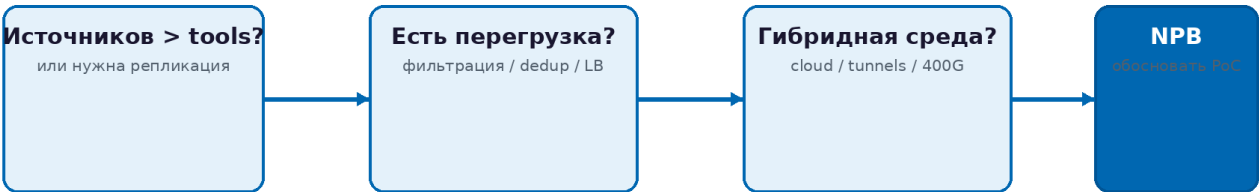
Раздел	Содержание
01	Резюме для принятия решения
02	Основы: роль NPB, TAP/SPAN, out-of-band и inline
03	Функции обработки пакетов и метаданных
04	Производительность, sizing и 100/400G
05	Архитектуры: ЦОД, cloud, Kubernetes и 4G/5G
06	Шифрование, Zero Trust и безопасность самого NPB
07	Отказоустойчивость, управление и автоматизация
08	Выбор решения, RFP и продуктовые классы Keysight
09	PoC, bake-off и приемочные испытания
10	Внедрение, эксплуатация и диагностика
11	TCO, ROI и бизнес-кейс
A-E	Шаблоны требований, протокол PoC, чек-листы, глоссарий и источники

01

РЕЗЮМЕ ДЛЯ ПРИНЯТИЯ РЕШЕНИЯ

Что NPВ дает организации, когда он нужен и какие результаты должны быть измеримыми

НУЖЕН ЛИ NPВ?



Если везде «нет»: прямое подключение может быть проще и дешевле.

Рисунок 1. Упрощенное дерево решения. Итоговый выбор подтверждается расчетом и PoC.

Что такое NPВ

Брокер сетевых пакетов (Network Packet Broker, NPВ) — это специализированный слой между источниками копий сетевого трафика и средствами анализа или предотвращения. Он агрегирует, фильтрует, реплицирует, преобразует и доставляет пакеты так, чтобы каждый инструмент получал необходимые данные в допустимом объеме и формате.

РЕШЕНИЕ ДЛЯ ЛПР

NPВ следует приобретать не ради «100% видимости», а ради конкретного измеримого результата: устранить перегрузку инструментов, консолидировать точки наблюдения, обеспечить контролируемую доставку трафика, снизить риск скрытых потерь либо поддержать новую скорость/среду.

Пять эффектов, которые можно защищать цифрами

Эффект	Измеряемый показатель	Как подтвердить
Полнота данных	Потери на ingress/processing/egress, packet ordering	Трафик-генератор и анализатор, сверка счетчиков
Разгрузка tools	Гбит/с, Mpps, доля дубликатов, объем payload	До/после фильтрации, dedup и slicing
Масштабирование	Число источников, портов, правил, туннелей и инструментов	Расчет на 3–5 лет плюс проверка лимитов
Отказоустойчивость	Время переключения и число потерянных пакетов	Иньекция отказов в PoC
Экономика	TCO, высвобожденные tool-порты, storage/egress	Базовый и консервативный сценарии ROI

Когда NPВ особенно оправдан

- точек наблюдения больше, чем доступных портов аналитических инструментов;

- один и тот же трафик нужен нескольким командам или инструментам;
 - 100/200/400G-трафик должен анализироваться пулом менее быстрых tools;
 - дубликаты, туннели или payload создают лишнюю нагрузку;
 - нужна централизованная политика для нескольких ЦОД и облаков;
 - inline-инструменты требуют bypass, балансировки и контролируемого поведения при отказе;
 - необходимы точные временные метки, flow affinity или корреляция мобильных сессий.
- Когда NPВ не решит проблему**
- исходный SPAN уже теряет или усекает пакеты — NPВ не восстановит отсутствующие данные;
 - полезная информация доступна только на конечной точке, в логах приложения или trace-контексте;
 - один источник напрямую подключен к одному инструменту и запас производительности достаточен;
 - причина инцидента находится вне наблюдаемого сегмента;
 - инструмент не способен обработать даже оптимизированный поток;
 - организация не готова управлять политиками, доступом, сертификатами и изменениями конфигурации.

Карточка решения до начала закупки

Поле	Формулировка для проекта
Проблема	Какой конкретный feed, инструмент или процесс сейчас теряет данные, перегружен или не масштабируется?
Baseline	Какими счетчиками, PCAP и измерениями подтверждено текущее состояние?
Целевой KPI	Допустимые loss, load, coverage, switch time, capacity reserve и срок достижения.
Альтернативы	Прямое подключение, дополнительный TAP/SPAN, upgrade tools, cloud-native сбор или NPВ.
Владелец результата	Кто принимает архитектуру, кто эксплуатирует и кто подтверждает качество feed?

СТОП-КРИТЕРИЙ

Если проблему, baseline и критерий успеха нельзя сформулировать до RFP, проект преждевременен: количество функций в коммерческом предложении не заменит измеримую цель.

02

ОСНОВЫ И МЕСТО NPB В ИНФРАСТРУКТУРЕ

Точки доступа, потоки данных, внеполосное наблюдение и inline-предотвращение

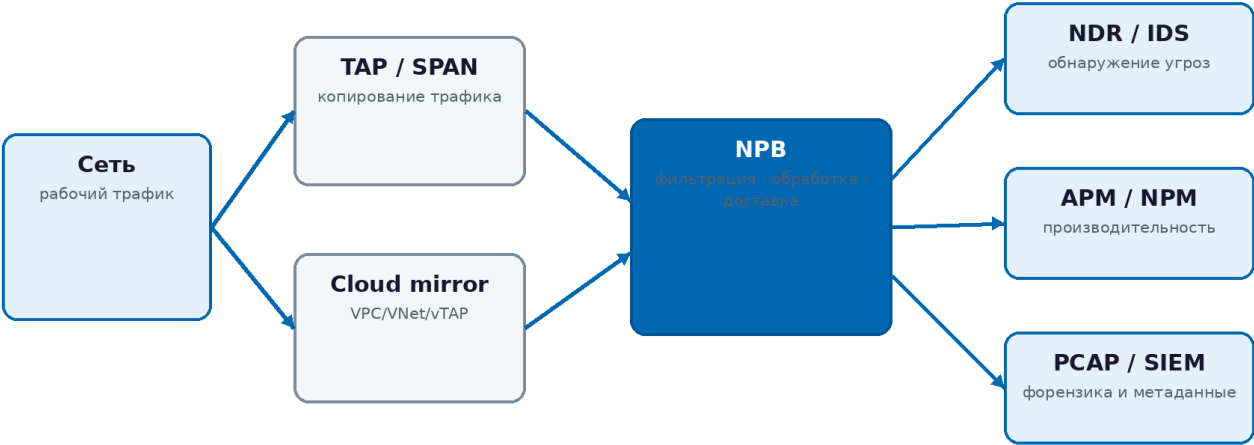


Рисунок 2. NPB связывает физические и виртуальные источники копий трафика с несколькими классами инструментов.

Две плоскости, которые нельзя смешивать

Плоскость	Содержание	Риск
Data plane	Копии пакетов, inline-потоки, туннели, фильтрация, репликация, балансировка.	Потеря, изменение порядка, неверная маршрутизация или обход inspection.
Management plane	GUI/API/CLI, учетные записи, политики, лицензии, сертификаты, журналирование.	Несанкционированное изменение фильтра или получение доступа к расшифрованным данным.

TAP, SPAN, ERSPAN и облачное зеркалирование

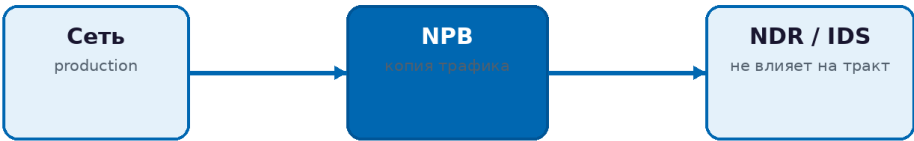
Источник	Сильные стороны	Ограничения / проверки
Физический TAP	Пассивная или контролируемая точка доступа; независимость от конфигурации SPAN; удобен для forensic.	Тип TAP, split/aggregation, optical budget, link negotiation, питание и bypass.
SPAN / mirror port	Быстрое включение без разрыва линии; подходит для локальной диагностики.	Oversubscription, приоритет производственного трафика, пропуск ошибок L1/L2, направление RX/TX.
ERSPAN / GRE mirror	Доставка удаленной копии через IP-сеть.	MTU, encapsulation overhead, reorder/loss в транспортной сети, outer/inner filtering.
VPC/VNet mirroring	Облачный способ копировать трафик ENI/vNIC к виртуальным средствам анализа.	Поддерживаемые источники, стоимость, MTU, квоты, availability zones, egress.
vTAP / агент / eBPF	Видимость VM, контейнеров и east-west traffic ближе к workload.	CPU overhead, coverage, kernel/CNI compatibility, lifecycle и доверие к агенту.

ПРАКТИЧЕСКАЯ ПРОВЕРКА

До проектирования NPB снимите контрольный PCAP непосредственно у источника и сравните число пакетов, длины, VLAN/tunnel headers и timestamps с копией после всей цепочки. Иначе потери источника ошибочно будут отнесены к NPB.

Out-of-band и inline

ВНЕПОЛОСНЫЙ МОНИТОРИНГ



INLINE-СХЕМА



Рисунок 3. Внеполосная копия не влияет на forwarding; inline-компонент становится частью критического тракта.

Критерий	Out-of-band	Inline
Типичные tools	NDR, IDS, APM/NPM, packet recorder, forensic	IPS, NGFW, WAF, DLP prevention
Влияние отказа	Обычно теряется наблюдаемость, рабочий трафик продолжает идти	Возможен простой или обход защиты
Обязательные функции	Счетчики drops, резервирование feeds, health tools	Bypass, heartbeat, fail-open/fail-close, symmetric steering
Ключевой KPI	Достоверность копии	Доступность production и эффективность предотвращения

Fail-open и fail-close

- **Fail-open** — при отказе inspection трафик пропускается; сохраняет доступность, но временно снижает контроль безопасности.
- **Fail-close** — при отказе трафик блокируется; сохраняет контроль, но повышает риск простоя.
- **Решение** — должно приниматься для каждого сегмента владельцами сервиса и ИБ, а не оставляться настройкой по умолчанию.

03

ФУНКЦИИ ОБРАБОТКИ ПАКЕТОВ

Что происходит с пакетом, какие ограничения проверять и какие данные доставлять инструментам

КОНВЕЙЕР ОБРАБОТКИ ПАКЕТОВ

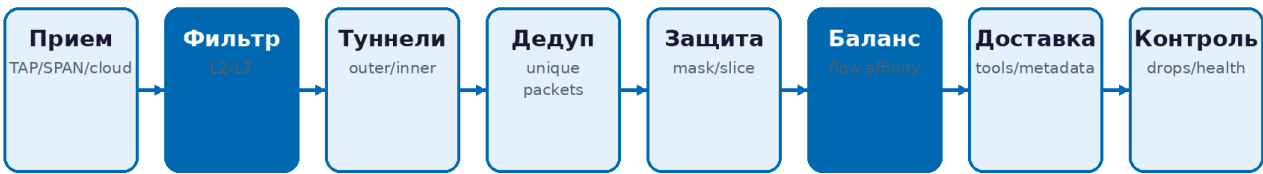


Рисунок 4. Логический pipeline. Реальный порядок и доступные комбинации функций зависят от платформы.

Карта функций

Функция	Назначение	Что обязательно проверить
Агрегация	Объединяет несколько источников	Oversubscription и корректность маркировки источника
Репликация	Передаёт один поток нескольким tools	Рост egress и коэффициент репликации
Фильтрация L2–L4	MAC/VLAN/IP/protocol/port	Размер таблиц, overlapping rules, IPv6 и fragments
Фильтрация L7	Приложения, категории, контекст	Точность классификации, encrypted traffic, first packets
Дедупликация	Удаляет повторные копии пакетов	Window, поля сравнения, NAT/tunnels, buffer exhaustion
Packet slicing	Оставляет заголовки и заданную часть payload	Минимальная длина для конкретного tool
Masking	Затирает чувствительные поля	Offsets после decapsulation, контроль необратимости
Header stripping	Удаляет внешнюю инкапсуляцию	Outer/inner context и последовательность операций
Load balancing	Распределяет потоки по пулу tools	Flow affinity, asymmetry, rebalance при отказе
Timestamping	Добавляет время приема/передачи	Ingress/egress point, PTP/NTP/1PPS, точность
Tunneling	Переносит копии между площадками	MTU, overhead, security и congestion
Flow metadata	Экспортирует NetFlow/IPFIX/application metadata	Sampling, template lifecycle, timestamps

Дедупликация без упрощений

Дубликаты возникают, когда один поток наблюдается на нескольких участках пути, копируются оба направления или зеркалирование выполняется до и после виртуального switching. Dedup должен снижать нагрузку, не удаляя законные повторные передачи TCP и не искажая forensic-картину.

Параметр	Вопрос для RFP/PoC
Окно сравнения	Каков диапазон и точность deduplication window? Что происходит с пакетами вне окна?

Параметр	Вопрос для RFP/РoC
Сигнатура	Какие байты/поля сравниваются? Можно ли игнорировать VLAN, ToS/Traffic Class, TCP Sequence?
Туннели	Сравнение выполняется до или после decapsulation? Поддерживается inner packet?
NAT	Как исключаются ложные совпадения при изменении адресов, портов и checksums?
Переполнение	Пакеты отбрасываются, пропускаются с дубликатами или функция деградирует и подает alarm?
Метрики	Доступны ли count/drop, occupancy, overflow и эффективность dedup?

Балансировка: поток, а не «снижение скорости»

NPB обычно распределяет совокупность потоков между несколькими инструментами. Он не превращает один 100G-поток в десять независимых 10G-потоков, если весь flow должен оставаться целым. При малом числе крупных elephant flows возможна неравномерная загрузка даже при большом количестве tools.

Алгоритм	Когда применять	Риск
5-tuple / session-aware	Большинство stateful tools	Изменение состава пула может перераспределить активные сессии
Asymmetric-aware	Маршруты RX/TX приходят из разных точек	Нужна нормализация и корректный ключ потока
Weighted	Инструменты разной производительности	Вес должен соответствовать реальной Mpps/Gbps емкости
Outer header	Туннель анализируется как единый поток	Все inner sessions могут попасть на один tool
Inner header	Нужно распределить сессии внутри VXLAN/GTP	Требуется поддержка decapsulation/parser
Random / packet-based	Только stateless-задачи	Разрушает порядок и session context

Инкапсуляции и контекст

Протокол / контекст	Что требуется от NPB
802.1Q / QinQ	Фильтрация по одному или нескольким VLAN; сохранение или удаление tags.
MPLS / L3VPN	Распознавание label stack и доставка внутреннего IP-пакета инструменту.
VXLAN / GENEVE	Фильтрация outer VTEP и inner tenant traffic; VNI/option context.
GRE / ERSPAN / L2GRE	Tunnel termination, извлечение mirrored packet, контроль sequence/metadata.
GTP-U	Inner subscriber flow, TEID, direction, user-session balancing и корреляция.
Проприетарный header	Programmable parser/strip с проверкой на всех скоростях и размерах пакета.

Четыре формы данных для tools

Форма	Содержание	Компромисс
Полный пакет	Заголовки и payload	Максимум контекста, максимум bandwidth/storage и требований к доступу
Packet slice	Заголовки + первые N байт	Снижает объем; может удалить нужное поле приложения
Flow record	5-tuple, counters, time, flags	Хорош для масштаба; нет полного payload/forensic
Application metadata	App/user/location/transaction attributes	Высокая ценность; зависит от классификации и шифрования

Как выбрать форму данных

Задача	Предпочтительная форма	Почему
Forensic и восстановление последовательности	Полный пакет	Нужны payload, flags и исходные длины
NDR/IDS при высокой нагрузке	Packet slice или полный пакет по фильтру	Баланс контекста и tool capacity
Долгосрочный capacity planning	IPFIX/flow metadata	Меньше storage при большом горизонте
APM и service dependency	Application metadata + traces	Нужен прикладной и сервисный контекст
Compliance-minimized monitoring	Filters + slicing + masking	Сокращается объем чувствительных данных

Антипаттерны pipeline

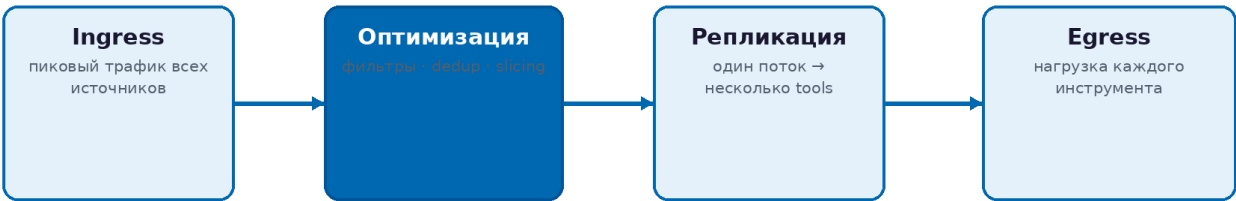
- удалить tunnel header до того, как его поля использованы для tenant/source attribution;
- дедуплицировать после изменения пакета, не проверив влияние masking/trimming на сигнатуру;
- балансировать по outer IP и ожидать равномерного распределения тысяч inner sessions;
- создать несколько независимых filters с перекрытиями без проверки результирующей политики;
- считать generated metadata эквивалентом исходного PCAP для forensic-задач.

04

ПРОИЗВОДИТЕЛЬНОСТЬ И SIZING

От Гбит/с к Mpps, микровсплескам, ресурсам обработки и реальной нагрузке инструментов

РАСЧЕТ ЕМКОСТИ



Egress = Σ(Ingress × доля после фильтрации × коэффициент репликации)

Рисунок 5. Расчет ведется от пикового ingress до каждого egress с учетом оптимизации и репликации.

Какие показатели нужны вместо одного числа «throughput»

Показатель	Почему важен
Switching/backplane capacity	Показывает базовую возможность пересылки, но не обязательно емкость расширенной обработки.
Advanced processing capacity	Отдельно для dedup, TLS, DPI, trimming, metadata и их комбинаций.
Mpps при 64/128 байтах и IMIX	Малые пакеты ограничивают packet-processing раньше, чем канал достигает номинальных Гбит/с.
Rule/filter scale	Влияет на возможность реализовать политику без конфликтов и ручной оптимизации.
Buffers / burst absorption	Определяют устойчивость к микровсплескам и кратковременной oversubscription.
Replication capacity	Один входной пакет может несколько раз пройти через egress fabric.
Tunnels / sessions / metadata rate	Отдельные таблицы состояния и CPU/FPGA-ресурсы могут стать узким местом.

Оценка packet rate

Для минимального Ethernet-кадра грубая оценка wire rate учитывает 64 байта кадра, 8 байт preamble/SFD и 12 байт inter-frame gap: 84 байта на пакет. Значения ниже не включают особенности кодирования, FEC и конкретной физической реализации.

Скорость	Максимальная оценка при 64-байтных кадрах
10 GbE	≈ 14,88 Mpps
25 GbE	≈ 37,20 Mpps
100 GbE	≈ 148,81 Mpps
200 GbE	≈ 297,62 Mpps
400 GbE	≈ 595,24 Mpps

ФОРМУЛА

Packet rate $\approx$ line rate, bit/s $\div$ (84 $\times$ 8). Для PoC используйте одновременно 64/128/256/512/1024/1518 байт и профиль IMIX.

Рабочий пример sizing

Исходные данные: четыре 100G TAP-порта с пиком 70% каждый; после фильтрации остается 45% трафика; dedup удаляет 20% от оставшегося; два инструмента получают весь оптимизированный поток, третий — 25%.

Шаг	Расчет	Результат
Пиковый ingress	4 $\times$ 100 $\times$ 0,70	280 Гбит/с
После фильтрации	280 $\times$ 0,45	126 Гбит/с
После dedup	126 $\times$ 0,80	100,8 Гбит/с
Egress tools A+B	100,8 $\times$ 2	201,6 Гбит/с
Egress tool C	100,8 $\times$ 0,25	25,2 Гбит/с
Суммарный egress	201,6 + 25,2	226,8 Гбит/с
Проектный запас 30%	226,8 $\times$ 1,30	$\approx$ 295 Гбит/с

НЕОБХОДИМАЯ ОГОВОРКА

Проценты фильтрации и dedup должны быть измерены на репрезентативном трафике. Для sizing нельзя переносить показатели из демонстрации производителя без проверки на собственной топологии.

Микровсплески и очереди

- снимайте peak не только в 1- или 5-минутных интервалах, а на субсекундной шкале;
- проверяйте burst при нескольких одновременно активных ingress-портах;
- фиксируйте queue occupancy, watermark, tail drops и head-of-line blocking;
- проверяйте, различает ли система congestion, processing overload и недоступность tool;
- требуйте alarm до потери данных, а не только постфактум счетчик drops.

100/200/400G: вопросы к физическому уровню

Область	Проверить
Порты и breakout	Допустимые комбинации QSFP/QSFP-DD, fan-out, ограничение соседних портов и port groups.
Оптика и DAC/AOC	Vendor qualification, wavelength, reach, DOM, polarity, loss budget.
FEC	Поддерживаемые режимы и согласованность на обоих концах; counters corrected/uncorrectable.
Скорости tools	Переход 400→100/25/10G, aggregate capacity и алгоритм распределения.
Модернизация	Лицензии, сменные модули, запас слотов/портов, support lifecycle и энергопотребление.

05

АРХИТЕКТУРЫ РАЗВЕРТЫВАНИЯ

Физический ЦОД, виртуализация, облака, Kubernetes, мобильное ядро и синхронизация времени

ЕДИНАЯ ФАБРИКА ВИДИМОСТИ

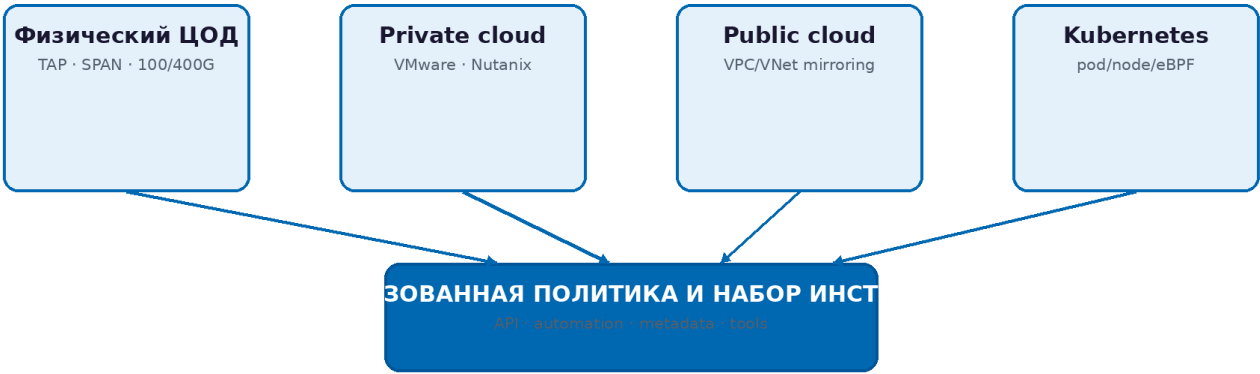


Рисунок 6. Единая политика видимости должна учитывать разные методы получения трафика и стоимость его транспорта.

Пять типовых архитектур

Архитектура	Схема	Ключевой риск
Rack / небольшой ЦОД	Локальные TAP/SPAN → один NPB → локальные tools	Единая точка отказа и недостаток портов при росте
Распределенный ЦОД	Edge NPB → центральный tool farm	Транспорт копий, MTU и межплощадочная oversubscription
Inline active-active	Bypass/NPB → пул IPS/NGFW	Flow affinity, fail-open/fail-close, state при переключении
Hybrid / multi-cloud	Cloud mirrors/vTAP → virtual nodes → cloud/on-prem tools	Egress cost, autoscaling, AZ/region failure
4G/5G mobile core	CP+UP feeds → correlation NPB → probes	Миллионы сессий, GTP/PFCP correlation, user privacy

Облачное зеркалирование

Облачный NPB должен рассматриваться как распределенная система: источник зеркалирования, filters, tunnel/target, virtual processing nodes, tool tier и orchestrator. В расчет включаются compute, лицензии, межзонный и межрегиональный перенос данных и egress к on-premises.

AWS MTU

AWS указывает дополнительный overhead Traffic Mirroring и возможность усечения зеркального пакета при несовместимом MTU. Для IPv4 документация рекомендует разницу 54 байта между source и target MTU, для IPv6 — 74 байта [6].

Проверка cloud-архитектуры	Критерий приемки
Coverage	Все требуемые ENI/vNIC/workloads включаются автоматически по тегам/политике.

Проверка cloud-архитектуры	Критерий приемки
Scale-out	Новые processing nodes создаются без потери flows и без ручной перенастройки feeds.
Failure domain	Отказ instance/AZ не лишает видимости критический сегмент сверх допустимого RTO.
Data transfer	Известны GRE/VXLAN/IPsec overhead, MTU, latency и egress/inter-AZ стоимость.
Security	Управляющий доступ, secrets, images, IAM roles и tunnels соответствуют cloud policy.

Kubernetes и east-west traffic

Наблюдаемость Kubernetes требует комбинации источников: node/vSwitch mirroring, CNI/eBPF telemetry, service-mesh data и application traces. NPВ полезен для пакетной доставки и нормализации, но не заменяет метрики, логи и distributed tracing OpenTelemetry [7].

Уровень	Что видно	Что может отсутствовать
Физическая сеть	Node-to-node, north-south, underlay	Pod identity и трафик внутри node
vSwitch / node	Pod-to-pod на узле, overlay	Application context и encrypted payload
eBPF / CNI	Process/pod/identity context, flows	Полный PCAP или трафик вне host
Service mesh	L7, service identity, retries	Нешифрованный контекст вне проху и non-mesh traffic
OpenTelemetry	Metrics/logs/traces и baggage	Точная packet-level последовательность

Мобильное ядро 4G/5G

МОБИЛЬНОЕ ЯДРО 4G/5G

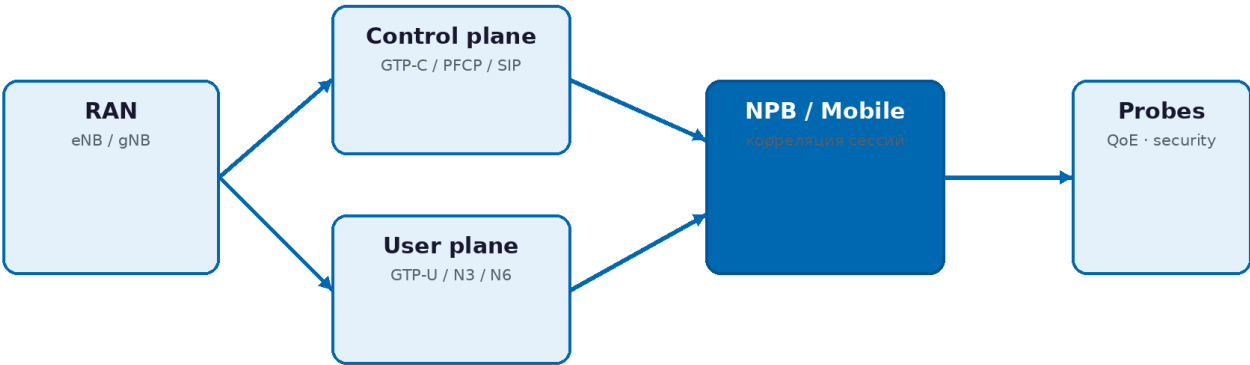


Рисунок 7. Для subscriber-aware visibility необходима корреляция управляющей и пользовательской плоскостей.

- фильтрация по TEID, inner IP, APN/DNN, направлению и, при разрешенной архитектуре, идентификаторам абонентской сессии;
- корреляция GTP-C/PFCP/SIP с GTP-U для сохранения контекста при изменении туннелей;
- балансировка всей сессии на один probe и контролируемое sampling;
- учет N3/N6, roaming, network slices и распределенных UPF;
- минимизация и защита персональных данных, отдельный доступ и аудит.

Временная синхронизация

Вопрос	Требование
Источник времени	NTP, IEEE 1588 PTP и/или 1PPS; резервирование и holdover.
Точка timestamp	Ingress предпочтителен для времени наблюдения; egress — для измерения обработки.
Точность	Определить требуемую погрешность и подтвердить ее на всех скоростях.
Формат	Native trailer/header, совместимость с packet recorder/analyzer.
Мониторинг	Offset, sync state, clock class, alarms и потеря grandmaster.

Архитектурная карточка площадки

Поле	Что зафиксировать
Traffic sources	Физические/виртуальные точки, owner, speed, peak, Mpps, encapsulation.
Processing location	Edge, central DC, cloud VPC/VNet; причина размещения и failure domain.
Tool destinations	Локальные/удаленные tools, capacity, stateful behavior, security zone.
Transport	L2GRE/VXLAN/IPsec, MTU, path bandwidth, latency, packet-loss monitoring.
HA	Node/port/tool redundancy, fail policy, RTO и тест переключения.
Data governance	Allowed traffic classes, masking/slicing, retention и administrators.

РЕЗУЛЬТАТ РАЗДЕЛА

Для каждой площадки должна существовать одна согласованная схема с направлениями потоков, портами, filters, tunnels, owners и capacity. Словесного описания недостаточно для приемки и последующей диагностики.

06

ШИФРОВАНИЕ И БЕЗОПАСНОСТЬ

TLS 1.3, QUIC, минимизация данных, Zero Trust и защита управляющей плоскости

TLS: корректные границы возможностей

В современном документе следует использовать термин «дешифрование TLS», а SSL оставлять как устаревшее историческое обозначение. TLS 1.3 определен RFC 8446 [3]. Возможность дешифрования зависит от места терминатии, владения ключами, режима проху, политики организации и поведения приложения.

Сценарий	Что требуется	Ограничения
Inbound reverse proxy	Сертификат/ключ сервиса либо контролируемая TLS-терминация	PFS, key lifecycle, HSM, HA и privacy
Outbound forward proxy	Enterprise CA и доверие endpoint	Pinning, unmanaged devices, mTLS, исключения
Passive key-log/session keys	Поддержка endpoint/app и безопасная доставка secrets	Не универсально; высокий риск утечки ключей
Metadata without decryption	Flow/TLS fingerprints, IP, timing, certificate context	Нет application payload; ECH/QUIC сокращают доступный контекст
Endpoint/EDR telemetry	Агент на host	Coverage, performance и доверие к endpoint

QUIC и HTTP/3

ОГРАНИЧЕНИЕ ПАССИВНОГО НАБЛЮДЕНИЯ

RFC 9312 отмечает, что большая часть transport-control информации QUIC зашифрована и на сети видно меньше, чем в TCP. Полноценная инспекция может потребовать управляемой конечной точки или проху; пассивный NPB сам по себе не снимает это ограничение [4].

- в RFP отдельно требовать обнаружение QUIC, балансировку QUIC-потокoв, trimming и собственно дешифрование;
- не считать распознавание UDP/443 доказательством L7-видимости;
- проверять connection migration, Connection ID, long/short headers и разные версии QUIC;
- для DoH/DoT учитывать влияние зашифрованного DNS на доменный контекст и политику исключений.

Минимизация данных

Механизм	Цель	Контроль
Фильтрация	Не получать нерелевантные сегменты	Default deny/allow, owner, change approval
Packet slicing	Не передавать полный payload	Длина по типу tool и протоколу
Masking	Скрывать определенные поля	Offsets/parser, тестовые шаблоны, необратимость
Tokenization outside NPB	Сохранять аналитику без исходного значения	Key/token vault и scope
RBAC и аудит	Ограничить доступ к feeds и decrypted data	Least privilege, MFA, immutable logs
Retention	Ограничить срок PCAP/metadata	Политика удаления и legal hold

NPB в Zero Trust

NPB не является Policy Decision Point и не заменяет контроль идентичности. Его роль — предоставлять достоверную сетевую телеметрию для аналитики, непрерывной проверки и обнаружения бокового перемещения. NIST SP 800-207 переносит фокус с сетевого периметра на защищаемые ресурсы; практические архитектуры NIST включают агрегацию и анализ сетевой телеметрии on-premises и в cloud [1][2].

Модель угроз для самого NPB

Угроза	Мера
Изменение фильтра и появление blind spot	RBAC, four-eyes approval, audit log, configuration diff и регулярная светка intent/actual.
Кража TLS-ключей	HSM/secure storage, минимальные права, rotation, запрет export и отдельные администраторы.
Доступ к расшифрованному feed	Физическая/логическая изоляция tool ports, allow-list и мониторинг подключений.
Компрометация management plane	Выделенная сеть, MFA, bastion, IP allow-list, patched firmware, signed images.
Supply-chain/обновление	Проверка происхождения, hash/signature, staged rollout, rollback и поддерживаемая версия.
DoS через traffic pattern	PoC с малыми пакетами, fragments, tunnels, bursts и parser edge cases.

Governance дешифрования

Решение	Кто утверждает	Обязательное evidence
Какие сегменты расшифровываются	Security Architecture + владельцы данных	Scope, data classes, исключения
Где хранится ключевой материал	PKI/HSM owner	Key flow, permissions, rotation, backup
Кто получает decrypted feed	Data owner + SOC	Tool ports, RBAC, network isolation
Какие данные маскируются	Privacy/Compliance	Test cases и образцы до/после
Сколько хранятся PCAP/metadata	Legal/Compliance + service owner	Retention/deletion policy
Как расследуются изменения	SOC / Internal Control	Immutable audit export и timestamps

Security-приемка NPB

- все default/admin credentials заменены, неиспользуемые сервисы отключены;
- management доступен только через выделенный доверенный контур;
- роли разделяют configuration, security feeds, key management и audit;
- обновление, rollback и проверка подписи пакета протестированы;
- критические события и изменения filters поступают в SIEM;
- сканирование и hardening не нарушают data-plane performance.

07

НАДЕЖНОСТЬ И УПРАВЛЕНИЕ

HA, измеримые показатели переключения, централизованная политика, API и эксплуатационная ответственность

ОТКАЗОУСТОЙЧИВОСТЬ: ПРОВЕРЯЕТСЯ, А НЕ ДЕКЛАРИРУЕТСЯ

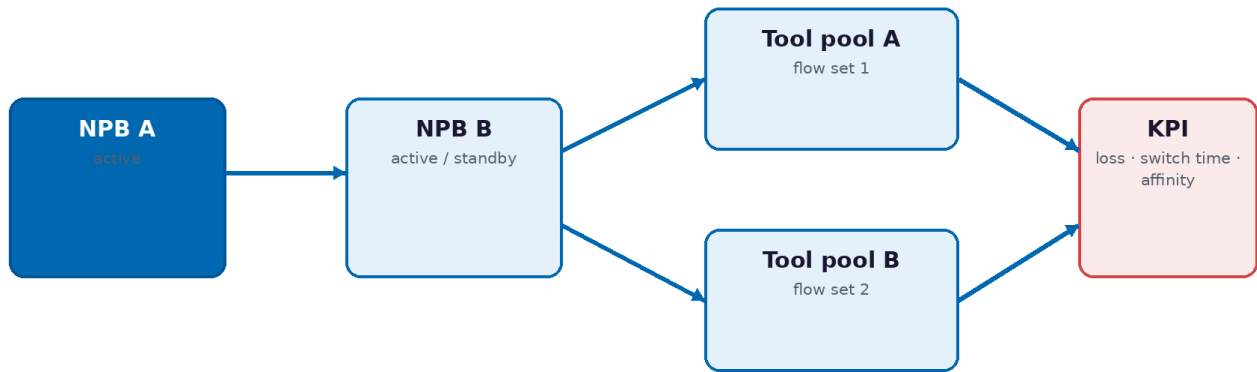


Рисунок 8. «Мгновенное восстановление» заменяется измеримыми KPI и тестами отказа.

Матрица отказов

Отказ	Ожидаемое поведение	Измерить
Tool port / tool instance	Flow перенаправлен в здоровый пул либо feed отключен по политике	Detection time, lost packets, affinity
Data port	Резервный feed/port активируется	Link/LOS detection, packet gap
Processing module	Функция сохраняется или явно деградирует с alarm	Feature state, drops, duplicates
NPB node	Peer принимает трафик без split-brain	Switch time, session distribution
Management system	Data plane продолжает работать по last known policy	Autonomy time, config access
Clock source	Переход на резерв/holdover	Offset, alarm, timestamp validity
Software upgrade	ISSU/rolling upgrade или согласованное окно	Packet loss, rollback time

KPI отказоустойчивости

- MTTD отказа компонента;
- время переключения data plane;
- точное число потерянных, дублированных и reorder-пакетов;
- сохранение симметрии и flow affinity;
- доля активных сессий, которые инструмент должен переобнаружить;
- доступность management plane и возможность rollback;
- поведение при одновременном отказе двух зависимостей.

Управление и автоматизация

Возможность	Минимальное требование
API / CLI	Документированный, versioned API; idempotent operations; понятные error codes.
Identity	LDAP/AD, RADIUS/TACACS+, RBAC, MFA или интеграция с контролируемым access path.

Возможность	Минимальное требование
Configuration lifecycle	Export/backup, diff, review, scheduled activation, rollback и golden config.
Telemetry	SNMP/syslog/API/streaming counters для ports, queues, filters, processing и HA.
Orchestration	Intent/policy, automatic node discovery, шаблоны сервисов и устранение configuration drift.
Automation tools	Проверенная интеграция с Ansible/Terraform/ITSM либо возможность безопасно ее реализовать.
Audit	Кто, когда и что изменил; экспорт в SIEM; синхронизированное время.

Keysight Vision Orchestrator позиционируется как централизованная точка управления физическими, облачными и edge-узлами, с intent-based policies, dashboards и cluster management [12]. Эти функции следует оценивать по фактическому охвату выбранных моделей и версий.

Распределение ответственности

Процесс	Владелец	Согласование
Точки доступа и capacity	NetOps / Network Architecture	Application owners, SecOps
Security feeds и TLS policy	SecOps / Security Architecture	Legal/Privacy, PKI
Cloud mirror и compute	CloudOps	FinOps, SecOps
Изменение фильтров	Visibility platform owner	Потребитель данных + change management
HA и аварийные тесты	Service owner / Operations	ИБ и владельцы production-сервисов
Обновление ПО	Platform owner	Change board, vendor support

Минимальный SLO-dashboard

Сигнал	Порог / представление	Действие
Ingress/egress utilization	Текущее, 95th, peak и forecast	Capacity review до исчерпания резерва
Drops	По port/queue/function/tunnel	Incident при любом необъясненном росте
Processing resources	Dedup/TLS/DPI utilization и buffer occupancy	Scale/filter до деградации
Tool health	Heartbeat, link, feed rate	Rebalance или controlled bypass
Time sync	Offset/state/GM	Пометить timestamps недостоверными
Policy drift	Intent vs actual, last change	Rollback или внеплановая сверка

Контролируемое изменение filter/policy

- 6. Зафиксировать owner, цель, затронутые sources/tools и план rollback.
- 7. Скомпилировать результирующую политику и проверить overlaps вне production.
- 8. Применить в согласованное окно с сохранением pre-change counters/config.
- 9. Передать маркированный test flow и подтвердить нужные/запрещенные направления.
- 10. Сравнить drops, load и tool visibility; закрыть изменение только с evidence.

08 ВИБОР РЕШЕНИЯ И RFP

Оценочная матрица, продуктовые классы, лицензирование и проверяемые требования

Оценочная модель

Группа	Рекомендуемый вес	Примеры критериев
Производительность	25%	Line rate, Mpps, advanced functions, bursts, no hidden drops
Функциональность	20%	Filters, dedup, LB, tunnels, masking, timestamp, metadata
Архитектура и HA	15%	Failure domains, bypass, clustering, switch behavior
Управление и безопасность	15%	API, RBAC, audit, automation, secure update
Совместимость и масштаб	10%	Ports, optics, tools, cloud, rules, sessions
Эксплуатация и поддержка	5%	Documentation, training, TAC, lifecycle, sparing
TCO	10%	Hardware, licenses, optics, support, power, cloud and staffing

ПРАВИЛО ОЦЕНКИ

Критерий без метода проверки — маркетинговое пожелание. Для каждого обязательного требования укажите evidence: datasheet, configuration screenshot, API response, test case или измеренный результат PoC.

Ключевые вопросы RFP

Область	Вопрос поставщику
Performance	Каковы forwarding и advanced-processing capacity при одновременном dedup + timestamp + tunnel termination?
Packets	Какова производительность для 64-byte, IMIX, IPv6 fragments и bursts?
Loss	Где и как учитываются drops? Есть ли queue watermarks и alarms до потери?
Rules	Каковы лимиты filters/rules на port, group, module и chassis? Как разрешаются overlaps?
Load balance	Как сохраняется flow affinity при асимметрии и изменении пула?
Dedup	Window, signature, NAT/tunnel behavior и действие при исчерпании buffer?
Cloud	Поддерживаемые mirrors, autoscaling, tunnels, regions и модель лицензирования?
Security	RBAC/MFA/audit, key storage, signed updates, vulnerability response?
HA	Какие failures покрыты и каковы измеренные loss/switchover values?
Lifecycle	EoS/EoL policy, upgrade path, spare parts, compatibility matrix?

Продуктовые классы Keysight

Ниже приведена ориентировочная карта классов, а не замена актуального конфигуратора. Состав функций определяется аппаратной платформой, лицензиями и версией ПО.

Класс	Типовой сценарий	Что подтвердить
Edge / rack NPB	Локальная агрегация и сервис для одной стойки/площадки	Плотность, speeds, local processing, tunnels
High-density modular	Крупный ЦОД и общий tool farm	Backplane, modules, HA, rule scale, processing slots
400G compact	Leaf/spine и AI/HPC edge на 100/200/400G	Breakout permutations, FEC, Mpps, burst protection
Mobile visibility	4G/5G core и subscriber-aware feeds	Session scale, GTP/PFCP correlation, sampling
Virtual/cloud	VPC/VNet/VM workloads	Marketplace images, autoscale, licensing, egress
Central management	Единая политика для нескольких NPB	Model/version coverage, APIs, HA and audit

Актуальные ориентиры для 400G

В актуальном datasheet Vision 400/400XT заявлены 10/25/40/50/100/200/400G, 9,2 Тбит/с full-duplex non-blocking L2 forwarding, поддержка NTP/PTP/1PPS, L2GRE/VXLAN, inline и out-of-band, а также отдельная FPGA-обработка для deduplication, trimming, timestamping и burst protection [8]. Эти параметры требуют проверки для конкретной конфигурации и одновременно включенных функций.

Vision X позиционируется как модульное высокоплотное шасси с портами до 100G в базовом datasheet и отдельной емкостью advanced packet processing; для 400G следует использовать актуальный вариант платформы и соответствующий datasheet [9].

Лицензии и скрытая стоимость

- лицензия по устройству, порту, bandwidth, feature stack, node или подписке;
- ограничение advanced processing лицензией или аппаратным модулем;
- отдельная лицензия централизованного управления, cloud nodes и metadata;
- стоимость оптики, fan-out, TAP/bypass, серверов управления и резервных блоков;
- обязательная поддержка для обновлений, signature/app identification и безопасности;
- рост стоимости при scale-out в cloud и межзонной передаче данных.

Иерархия доказательств поставщика

Уровень	Evidence	Вес при решении
1	Измерение в вашем PoC с внешним analyzer	Максимальный
2	Публичный test report с topology, versions и raw methodology	Высокий
3	Актуальный datasheet и release-specific documentation	Средний
4	Письменное обязательство в спецификации/договоре	Зависит от условий приемки
5	Демо, презентация или устное заявление	Только основание для проверки

Готовность shortlist

- обязательные функции подтверждены для одной и той же модели и версии ПО;
- получена полная BOM с лицензиями, оптикой, поддержкой и резервированием;
- поставщик принял единую методику PoC и критерии FAIL;
- известны product lifecycle, upgrade path и ограничения совместимости;
- TCO рассчитан на одинаковый срок и одинаковый прогноз роста;
- отклонения внесены в risk register до выбора победителя.

09

РОС, ВАКЕ-OFF И ПРИЕМКА

Одинаковая методика для всех поставщиков, положительные и отрицательные сценарии, фиксируемые результаты

Принципы честного сравнения

- 11. Одинаковые порты, оптика, topology, traffic profile, duration и инструменты измерения.
- 12. Зафиксированные версии hardware, firmware, licenses и configuration export.
- 13. Нагрузка 64/128/256/512/1024/1518 bytes, IMIX, IPv4/IPv6, tunnels и fragments.
- 14. Проверка функций одновременно, а не по одной в независимых демонстрациях.
- 15. Измерение с внешнего analyzer, а не только по счетчикам тестируемого NPB.
- 16. Публикация всех drops, duplicates, reorder, latency и resource alarms.
- 17. Отдельная фиксация заявлений производителя и измеренных результатов.

Базовая топология РоС

Компонент	Назначение
Traffic generator/analyzer	Формирует воспроизводимые потоки и измеряет loss, reorder, latency, sequence.
TAP/SPAN emulator	Воспроизводит несколько источников и дубликаты на разных задержках.
NPB under test	Фиксированная конфигурация и включенные функции.
Tool pool	Разная емкость, stateful/stateless behavior, health failure.
Management/telemetry collector	Сохраняет counters, logs, SNMP/API и события HA.
Time source	PTP/NTP/1PPS для проверки timestamping, если требуется.

Набор обязательных тестов

ID	Тест	Нагрузка / действие	Критерий
P01	Baseline forwarding	Line rate без advanced functions	0 unexplained loss; counters agree
P02	Small packets	64/128 bytes на всех ingress	Заявленная Mpps; alarm до overload
P03	IMIX + burst	Sustained + microbursts	Drops/queues измерены и объяснены
P04	Filters	Overlaps, include/exclude, IPv6	Нет blind spots/extra traffic
P05	Dedup	Разные windows, NAT, VLAN, tunnels	Нет false dedup; overflow documented
P06	Load balance	Elephant/mice, asymmetric, weighted	Affinity и допустимый imbalance
P07	Tunnels	VXLAN/GRE/ERSPAN/GTP inner/outer	Корректная decap/filter/re-encap
P08	Mask/slice	Offsets и разные packet lengths	Чувствительные поля отсутствуют
P09	Timestamp	All speeds + load	Погрешность в пределах требования
P10	HA	Port/tool/module/node/clock failures	Loss и switch time в пределах SLA
P11	Management	RBAC, audit, backup/restore, API	Все изменения трассируются
P12	Soak	24–72 h mixed load	Нет утечек ресурсов и скрытой деградации

Отрицательные сценарии

- переполнение dedup buffer и filter table;

- egress tool медленнее входного потока или полностью недоступен;
- неправильный MTU и фрагментация зеркального tunnel;
- конфликтующие include/exclude rules;
- потеря management connectivity при работающем data plane;
- истечение TLS-сертификата или недоступность HSM/PKI;
- потеря PTP grandmaster и переход на holdover;
- rollback после неуспешного обновления;
- одновременный отказ tool и одного NPB-node.

Форма результата

Поле	Заполняемое значение
Test ID / дата / исполнитель	_____
Модель / serial / версия ПО	_____
Лицензии и модули	_____
Конфигурация / hash export	_____
Traffic profile / duration	_____
Ожидаемый результат	_____
Фактический результат	_____
Loss / reorder / latency	_____
Логи / counters / evidence	_____
Статус и отклонение	PASS / FAIL / CONDITIONAL

10

ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ

Обследование, ввод в эксплуатацию, регулярные проверки и таблица диагностики

Предпроектное обследование

Категория	Собрать
Точки наблюдения	Site/rack/device/port, TAP/SPAN/cloud mirror, RX/TX, owner
Трафик	Average/95th/peak/burst, Gbps/Mpps, packet sizes, multicast, elephant flows
Encapsulation	VLAN/QinQ/MPLS/VXLAN/GENEVE/GRE/ERSPAN/GTP
Tools	Ports, max Gbps/Mpps, stateful, symmetric flow, packet format
Processing	Filters, dedup, slicing, masking, TLS, timestamp, metadata
Availability	OOB/inline, fail mode, RTO/RPO, maintenance windows
Management	IP plan, AAA, NTP/PTP, syslog/SIEM, API, backup
Growth	3–5 years, new sites/clouds, 100/400G, extra tools
Compliance	Data classes, retention, decryption authority, audit

Чек-лист ввода в эксплуатацию

- ☐ Сверить BOM, serial numbers, licenses, firmware и support entitlement.
- ☐ Проверить питание A/B, airflow, grounding, кабели, optics, DOM и FEC counters.
- ☐ Разнести data и management plane; настроить AAA/RBAC/MFA/allow-list.
- ☐ Настроить NTP/PTP/1PPS и проверить offset/alarm.
- ☐ Импортировать policy по утвержденной change-заявке; сохранить golden config.
- ☐ Провести port-by-port тест с маркированными потоками и сверкой ingress/egress.
- ☐ Проверить фильтры, tunnels, dedup, masking, slicing и каждый tool feed.
- ☐ Выполнить failure tests и подтвердить loss/switchover.
- ☐ Подключить telemetry, syslog, traps и dashboards; проверить тестовые alarms.
- ☐ Зафиксировать baseline counters, utilization, queue watermarks и capacity reserve.
- ☐ Передать схемы, конфигурацию, runbook, контакты поддержки и матрицу ответственности.

Эксплуатационный runbook

Периодичность	Проверки
Ежесменно / ежедневно	Critical alarms, port state, drops, queues, tool health, HA, clock sync.
Еженедельно	Peak/95th, processing utilization, dedup efficiency, tunnel loss, config changes.
Ежемесячно	Capacity trend, licenses/certificates, backup restore sample, user/RBAC review.
Ежеквартально	Failure drill, firmware/security review, inventory, spare parts, growth forecast.
После изменения	Targeted regression: affected feeds, counters, masking, affinity, rollback evidence.

Диагностика: симптом → проверка

Симптом	Что проверить	Действие
Tool видит меньше трафика	Source drops, filter hit counters, queues, egress congestion, tunnel loss	Сравнить sequence на каждом этапе
Tool перегружен	Replication, dedup ratio, packet size, elephant flows	Уточнить filters/slicing/LB weights
Неверные показатели приложения	Duplicates, truncation, timestamp, asymmetric flows	Проверить dedup и session affinity
Пропал tenant/VLAN	Outer/inner rules, tag stripping, overlap compiler	Тестовый маркированный flow
Пакеты усечены	Source/target MTU, cloud mirror, slicing	Сверить original_len/captured_len
LB неравномерен	Flow cardinality, hash key, elephant flows, weights	Распределение по flows и bytes
Timestamp скачет	PTP state, offset, GM failover, ingress/egress mode	Сравнить с эталонным time source
НА вызвал большой gap	Failure detection, rebalance, tool state, link timers	Воспроизвести с sequence traffic

Процедура после инцидента

- 18. Зафиксировать время, affected feeds/tools, текущую конфигурацию и все counters до перезапуска.
- 19. Локализовать первую точку расхождения sequence/packet count по цепочке source → NPB → tool.
- 20. Отделить source loss, transport loss, processing overload и tool congestion.
- 21. Воспроизвести минимальным синтетическим потоком без изменения production-policy.
- 22. После исправления выполнить regression, обновить runbook и capacity/risk assumptions.

Ежеквартальный capacity forecast

Метрика	Текущее	Прогноз 12 мес.	Порог действия
Peak ingress, Gbps	_____	_____	_____
Peak ingress, Mpps	_____	_____	_____
Advanced processing	_____	_____	_____
Peak egress/tool	_____	_____	_____
Filter/rule utilization	_____	_____	_____
Tunnel/session scale	_____	_____	_____

11

ЭКОНОМИКА И БИЗНЕС-КЕЙС

Полный TCO, сценарный ROI и решение на основании рисков и измерений

ТСО: что включить

Категория	Статьи затрат
CAPEX	NPB chassis/modules, TAP/bypass, optics, fan-out, management servers, spare units.
Лицензии	Feature stacks, bandwidth/ports, orchestrator, virtual/cloud nodes, subscriptions.
Инфраструктура	Rack units, power, cooling, cross-connects, transport links.
Cloud	Compute, storage, inter-AZ/region transfer, egress to on-prem, marketplace fees.
Внедрение	Design, lab/PoC, installation, migration, professional services, training.
Эксплуатация	Support, upgrades, certificates, monitoring, staffing, incident work.
Риск	Downtime during change, EoL migration, vendor lock-in, missing capability.

Формула ROI

СЦЕНАРНАЯ МОДЕЛЬ

ROI = (экономия tool-capacity + продление срока эксплуатации + снижение storage/egress + снижение трудозатрат + ожидаемое снижение потерь от инцидентов – TCO NPB) ÷ TCO NPB.

Параметр	Консервативный	Базовый	Оптимистичный
Сокращение входного потока tools	_____ %	_____ %	_____ %
Отложенная закупка tool-портов	_____	_____	_____
Экономия storage/cloud egress	_____	_____	_____
Снижение часов диагностики	_____	_____	_____
Годовой TCO NPB	_____	_____	_____
Срок окупаемости	_____	_____	_____

Решение инвестиционного комитета

Вопрос	Evidence
Какой риск или узкое место устраняется?	Baseline: drops, overload, blind spots, tool utilization, incident data.
Почему нельзя решить дешевле?	Сравнение direct/SPAN/TAP/upgrade tool/cloud-native alternatives.
Как рассчитана емкость?	Ingress/egress model, Mpps, bursts, replication и growth reserve.
Как доказана функция?	PoC results с внешним analyzer и сохраненными logs/config.
Что произойдет при отказе?	HA test results, fail policy, runbook и ownership.
Каков полный срок и TCO?	3–5-year model, licenses, support, cloud, power и migration.

ФИНАЛЬНАЯ РЕКОМЕНДАЦИЯ

Решение о закупке следует принимать только после согласования целевой архитектуры, расчета capacity, матрицы обязательных требований и успешного PoC. Сравнивать нужно не количество функций, а гарантированный результат в вашей комбинации скоростей, пакетов, туннелей и инструментов.

Рабочая таблица TCO на 3–5 лет

Статья	Год 0	Год 1	Год 2	Год 3–5
NPB/TAP/bypass/optics	_____	_____	_____	_____
Лицензии и подписки	_____	_____	_____	_____
Support и spare units	_____	_____	_____	_____
Power/rack/transport	_____	_____	_____	_____
Cloud compute/transfer	_____	_____	_____	_____
Внедрение/обучение/FTE	_____	_____	_____	_____
Миграции и upgrades	_____	_____	_____	_____
ИТОГО	_____	_____	_____	_____

Протокол инвестиционного решения

Решение	Обоснование / условие
☐ Одобрить	_____
☐ Одобрить условно	_____
☐ Вернуть на доработку	_____
☐ Отклонить	_____
Ответственный / срок	_____



ШАБЛОН ТРЕБОВАНИЙ RFP

Фрагмент заполняемой матрицы для переноса в закупочную документацию

ID	Приоритет	Требование	Проверка	Ответ
R-01	Обязательное	0 необъясненных потерь при заявленной нагрузке и профиле пакетов	PoC P01–P03	
R-02	Обязательное	Отдельные counters ingress/egress/drop/queue	GUI/API evidence	
R-03	Обязательное	Фильтрация outer и inner headers для требуемых tunnels	PoC P07	
R-04	Обязательное	Session-aware LB с сохранением affinity	PoC P06	
R-05	Обязательное	Dedup window и overflow behavior документированы	Datasheet + P05	
R-06	Обязательное	RBAC, central AAA, audit export	Demo + config	
R-07	Обязательное	Backup/restore и rollback	PoC P11	
R-08	Обязательное	HA loss/switch time ≤ согласованного порога	PoC P10	
R-09	Желательное	Intent-based centralized policy	Demo/API	
R-10	Желательное	Cloud autoscale и tag-based onboarding	Cloud PoC	
R-11	Желательное	PTP/1PPS timestamping	PoC P09	
R-12	Информационно е	EoS/EoL и upgrade roadmap 5 лет	Письмо производителя	

В ПРОТОКОЛ РОС

Минимальный набор полей и критериев фиксации результата

Параметр	Значение
Заказчик / площадка	
Поставщик / решение	
Модель / аппаратная ревизия	
Версия ПО / build	
Лицензии / feature stacks	
Дата / исполнители	
Схема / номера портов	
Traffic generator/analyzer	
Ограничения / исключения	

Итоговая ведомость

Test ID	PASS	FAIL	Отклонение / evidence
P01	☐	☐	
P02	☐	☐	
P03	☐	☐	
P04	☐	☐	
P05	☐	☐	
P06	☐	☐	
P07	☐	☐	
P08	☐	☐	
P09	☐	☐	
P10	☐	☐	
P11	☐	☐	
P12	☐	☐	



ЧЕК-ЛИСТ ПРИЕМКИ

Подписи выдаются после проверки данных, управления, НА и документации

- ☐ Фактическая аппаратная и программная конфигурация соответствует BOM.
- ☐ Все обязательные тесты PoC/приемки имеют PASS либо согласованное отклонение.
- ☐ Счетчики NPB согласованы с внешним analyzer в пределах допуска.
- ☐ Фильтры и tool feeds проверены владельцами данных.
- ☐ Masking/slicing исключают согласованные категории чувствительных данных.
- ☐ Inline fail policy и НА подтверждены владельцами сервисов и ИБ.
- ☐ AAA/RBAC/audit/syslog/NTP/PTP настроены и протестированы.
- ☐ Golden config и backup сохранены; restore/rollback проверен.
- ☐ Capacity reserve соответствует прогнозу роста.
- ☐ Схемы, runbook, support contacts и ответственность переданы эксплуатации.

Роль	ФИО	Решение / подпись / дата
Архитектор сети		
Информационная безопасность		
Эксплуатация		
Владелец сервиса		
Руководитель проекта		



ГЛОССАРИЙ

Основные термины сетевой видимости

Термин	Определение
NPB	Network Packet Broker — брокер сетевых пакетов.
TAP	Test Access Point — специализированная точка получения копии трафика.
SPAN	Switched Port Analyzer — зеркальный порт/сессия коммутатора.
ERSPAN	Удаленное зеркалирование пакетов с инкапсуляцией через IP/GRE.
OOB	Out-of-band — внеполосная обработка копии трафика.
Inline	Режим, в котором устройство находится в рабочем тракте forwarding.
Bypass	Механизм обхода inline-инструмента при отказе или обслуживании.
Fail-open	При отказе трафик пропускается в обход inspection.
Fail-close	При отказе трафик блокируется.
Line rate	Обработка на полной скорости интерфейса при оговоренном профиле.
Mpps	Миллионы пакетов в секунду.
IMIX	Смесь размеров пакетов, приближенная к реальному трафику.
Deduplication	Обнаружение и удаление повторных копий пакета в заданном окне.
Packet slicing	Обрезка пакета до заданной длины с сохранением нужных заголовков.
Flow affinity	Доставка всех пакетов одной сессии на один и тот же инструмент.
DPI	Deep Packet Inspection — классификация по содержимому/контексту пакета.
IPFIX	Стандартизованный протокол экспорта информации о потоках [5].
PTP	Precision Time Protocol IEEE 1588 — точная синхронизация времени.
VXLAN	Overlay-инкапсуляция L2 поверх UDP/IP с идентификатором VNI.
GTP-U	Туннелирование пользовательского трафика мобильной сети.
PFS	Perfect Forward Secrecy — свойство, ограничивающее расшифрование прошлых сессий при компрометации долговременного ключа.
RTO	Целевое время восстановления сервиса.



ИСТОЧНИКИ

Стандарты, официальная документация и материалы производителя

[1] NIST SP 800-207 — Zero Trust Architecture

<https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf>

[2] NIST NCCoE — Implementing a Zero Trust Architecture, Architecture and Builds

<https://pages.nist.gov/zero-trust-architecture/VolumeB/architecture.html>

[3] RFC 8446 — The Transport Layer Security (TLS) Protocol Version 1.3

<https://www.rfc-editor.org/info/rfc8446>

[4] RFC 9312 — Manageability of the QUIC Transport Protocol

<https://www.rfc-editor.org/info/rfc9312>

[5] RFC 7011 — Specification of the IP Flow Information Export (IPFIX) Protocol

<https://www.rfc-editor.org/info/rfc7011>

[6] AWS — Traffic Mirroring limitations

<https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-network-limitations.html>

[7] Kubernetes — Boosting container runtime observability with OpenTelemetry

<https://kubernetes.io/blog/2022/12/01/runtime-observability-opentelemetry/>

[8] Keysight — Vision 400 and Vision 400XT NextGen Network Packet Broker

<https://www.keysight.com/us/en/assets/3122-1991/data-sheets/Vision-400-and-Vision-400XT-NextGen-Network-Packet-Broker.pdf>

[9] Keysight — Vision X Network Packet Broker

<https://www.keysight.com/us/en/assets/3120-1029/data-sheets/Vision-X-Network-Packet-Broker.pdf>

[10] Keysight — MobileStack

<https://www.keysight.com/us/en/assets/3121-1141/data-sheets/MobileStack.pdf>

[11] Keysight / Tolly — Vision X Performance and Features

<https://www.keysight.com/us/en/assets/7121-1050/reports/Tolly-Test-Report-Keysight-Vision-X-Network-Packet-Broker-Performance-and-Features.pdf>

[12] Keysight — Vision Orchestrator

<https://www.keysight.com/us/en/assets/3122-2256/data-sheets/Keysight-Vision-Orchestrator.pdf>

[13] Keysight — Best Practices for Network Monitoring

<https://www.keysight.com/us/en/assets/3120-1092/white-papers/Best-Practices-for-Network-Monitoring.pdf>

[14] CISA — Encrypted DNS Implementation Guidance

https://www.cisa.gov/sites/default/files/2024-05/Encrypted%20DNS%20Implementation%20Guidance_508c.pdf

[15] RFC 9065 — Considerations around Transport Header Confidentiality

<https://www.rfc-editor.org/rfc/rfc9065.html>

[16] AWS — What is Traffic Mirroring?

<https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html>

[17] NIST SP 800-207A — Zero Trust Architecture Model for Cloud-Native Applications

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf>

[18] Keysight — Vision Edge 400P

<https://www.keysight.com/us/en/assets/3124-1511/data-sheets/Vision-Edge-400P.pdf>

ПРИМЕЧАНИЕ ОБ ИСТОЧНИКАХ

Характеристики продуктов приведены по доступным официальным материалам на дату подготовки руководства. Перед закупкой необходимо использовать актуальные datasheet, release notes, compatibility matrix и коммерческую спецификацию поставщика.