Содержание

Схема организации кластера CKAT DPI

Комплекс представляет собой высокопроизводительный, масштабируемый кластер. Предназначен для анализа и управления сетевым трафиком в реальном режиме времени на уровнях L2-L7 сетевой модели OSI, состоит из следующих элементов:

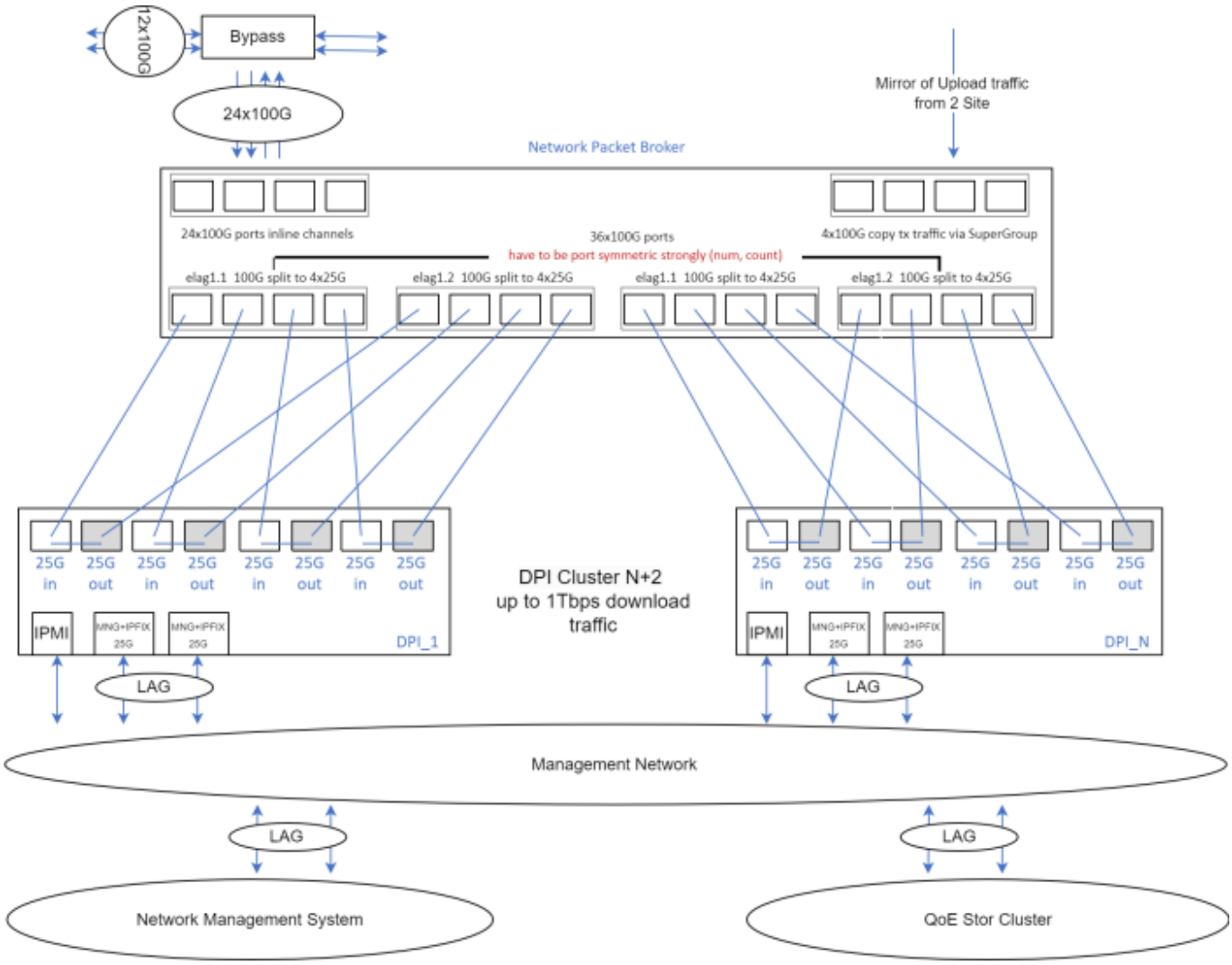
1. Внешний оптический bypass (Bypass Switch) со сменными оптическими модулями, обеспечивающими подключение линий SM (1310нм) или MM (850нм)
2. Агрегатор (балансировщик) трафика Network Packet Broker (NPB)
3. Кластер серверов CKAT DPI
4. Кластер виртуализации для развертывания системы управления (Network Management System) с графическим интерфейсом (DPIUI2). Так же включает серверы FTP, Syslog для сбора логов с компонентов системы, HTTP web-сервер для централизованной загрузки черных списков и систему мониторинга Zabbix.
5. Комплекс хранения данных (QoE Stor) для построения статистических и аналитических отчетов, обеспечивающий длительное хранение агрегированной информации
6. Комплект необходимых кабелей для коммутации и QSFP28/QSFP/SFP28/SFP+ модулей
7. Коммутаторы в отказоустойчивом исполнении для объединения компонентов решения и менеджмента

Комплекс предназначен для установки в разрыв и поддерживает следующие типы интерфейсов Ethernet:

- 10G-BASE SR/LR
- 25G-BASE SR/LR
- 40G-BASE SR4/LR4
- 100G-BASE SR4/L4

Поддерживаются инкапсуляции: MPLS, IPinIP, VLAN, QinQ, GRE.

1xNPB до 1Tbps:



Прохождение трафика

Линки оператора связи подключаются «в разрыв» в устройства балансировки трафика через оптический bypass, что обеспечивает защиту сети при выходе из строя аппаратных компонентов или сбое программного обеспечения. Балансировщик трафика распределяет потоки (flow) между узлами обеспечивая симметричное прохождение трафика на уровне сессии через один и тот же узел DPI (symmetric session aware load balancing L3/L4). Комплекс целиком функционирует как прозрачное L2-устройство и в общем случае не требует от оператора связи дополнительных настроек на своей стороне или изменения логической схемы построения сети.

Обработка ассимметричного трафика

В случае наличия асимметричного трафика (исходящий трафик проходит через одну площадку/кластер СКАТ DPI, а входящий трафик через другую площадку), необходимо осуществлять отправку копии только ИСХОДЯЩЕГО трафика с одной площадки на другую. Тем самым ВЕСЬ исходящий трафик попадает в кластеры СКАТ DPI на разных площадках и устраняется асимметричность трафика. Передача копии трафика осуществляется по прямым линкам между NPB с целью минимизации задержки. Копия трафика подается на все DPI устройства с учетом балансировки. DPI учитывает данный трафик при детектировании

сигнатуры, но не учитывает при выгрузке статистики. После обработки данный трафик отбрасывается. Использование данного метода повышает процент распознавания при асимметричном трафике.Отметим, что исходящий трафик составляет 10% от входящего, поэтому зеркалирование между площадками не требует широких каналов, так же не повышается нагрузка на кластер DPI.

DPI узел

Основным компонентом системы является DPI — оборудование для анализа трафика. DPI — это программное обеспечение, работающее на серверах X86_64 общего назначения с поддержкой сетевых карт на чипсетах Mellanox/Intel. В типовом кластере: Серверы оснащены 6x 2-портовыми оптическими картами с интерфейсами 10/25GE, из которых 8 портов используются для обработки трафика, 2 порта для отправки IPFIX на QoE сервер, 2 порта в резерве.

Устройство DPI полностью прозрачно на уровне Layer 2. Когда DPI установлен "в разрыв", порты на стороне клиента называются IN «входными», а порты на стороне WAN называются OUT «выходными». Пары портов образуют мосты. Правильная ориентация портов важна для правильного обнаружения и работы функции контроля трафика. Каждый узел DPI может работать независимо или быть присоединенным к кластеру.

Определены два типа портов для обработки трафика:

- входные (IN) - это порт в сторону местных интернет-операторов или абонентов (LAN)
- выходные (OUT)- это порт в сторону вышестоящего провайдера (WAN)

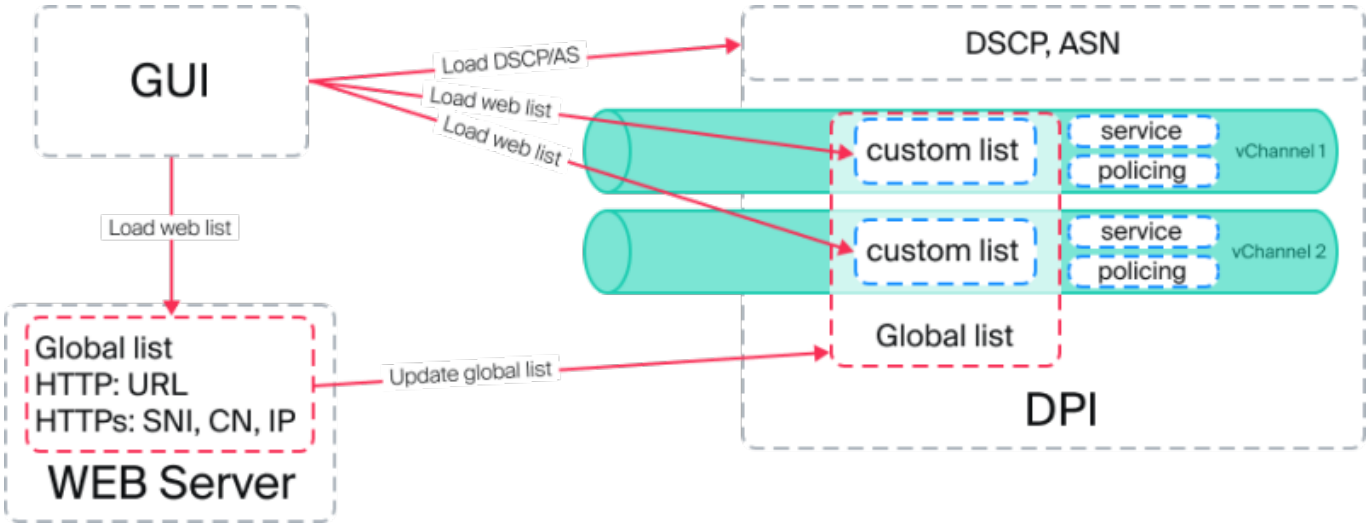
Типовая конфигурация сервера: процессор AMD EPYC 64 cores, 512GB RAM, HW RAID controller, 2xSSD disks, 1-2x NVME SSD, 6x NIC 2x25GbE, 2xPSU. Важно, что производительность DPI также зависит от параметра PPS и общего профиля трафика. Параметры производительности подробнее описаны в статье.

Для правильной работы всех функций DPI он должен получать прямой и обратный абонентский трафик (полные двунаправленные сеансы), в противном случае некоторые функции, в том числе обнаружение протоколов приложений, могут не работать или работать некорректно. Поэтому важно обеспечить, чтобы двунаправленный трафик сеанса абонента проходил через одно устройство DPI. Симметричность трафика, проходящего через DPI, обеспечивается с помощью отправки зеркала исходящего трафика одной площадки на другую и балансировки на NPB.

Управление

Управление комплексом производится через web based подсистему управления DPIUI2 — FilterUI. FilterUI обеспечивает управление профилями и услугами абонентов или нижестоящих операторов (в том числе по сигнализации BGP), политиками обработки трафика, в том числе полисингом, правилами фильтрации — черными и белыми списками, пользовательскими протоколами, построением отчетов и т.д. Для интеграции со сторонними системами имеются стандартизированные интерфейсы/API. CKAT DPI реализует парадигму 3GPP, в качестве дополнительной опции и в рамках отдельного технического решения, возможна интеграция управления профилями и услугами абонентов через встроенный модуль PCRF, с поддержкой протокола RADIUS, Gx/Gy интерфейсов DIAMETER.

Для переключения с DPIUI2 на FilterUI необходимо настроить соответствующую роль.



Для централизованной загрузки Глобальных списков на DPI используется выделенный web сервер. FilterUI выгружает списки на данный сервер в подготовленном формате для DPI. Каждый DPI скачивает данные списки и применяет в соответвии с правилами. Так же FilterUI выгружает уникальные правила на каждый DPI. При необходимости данные списки объединяются и применяются на канал или абонента.

Хранение статистики

Комплект поставки включает систему хранения данных и конструктор отчетов, позволяющий строить произвольные (пользовательские) отчеты. Конструктор отчетов предназначен для получения статистики по пользователям, операторам, IP-адресам, подсетям, автономным системам, сетевым протоколам, прикладным приложениям и их комбинации, что обеспечивает для заказчика полную прозрачность сети, а также поддержку Quality of Experience. Система позволяет хранить как сырые данные IPFIX, так и данные в агрегированном виде.

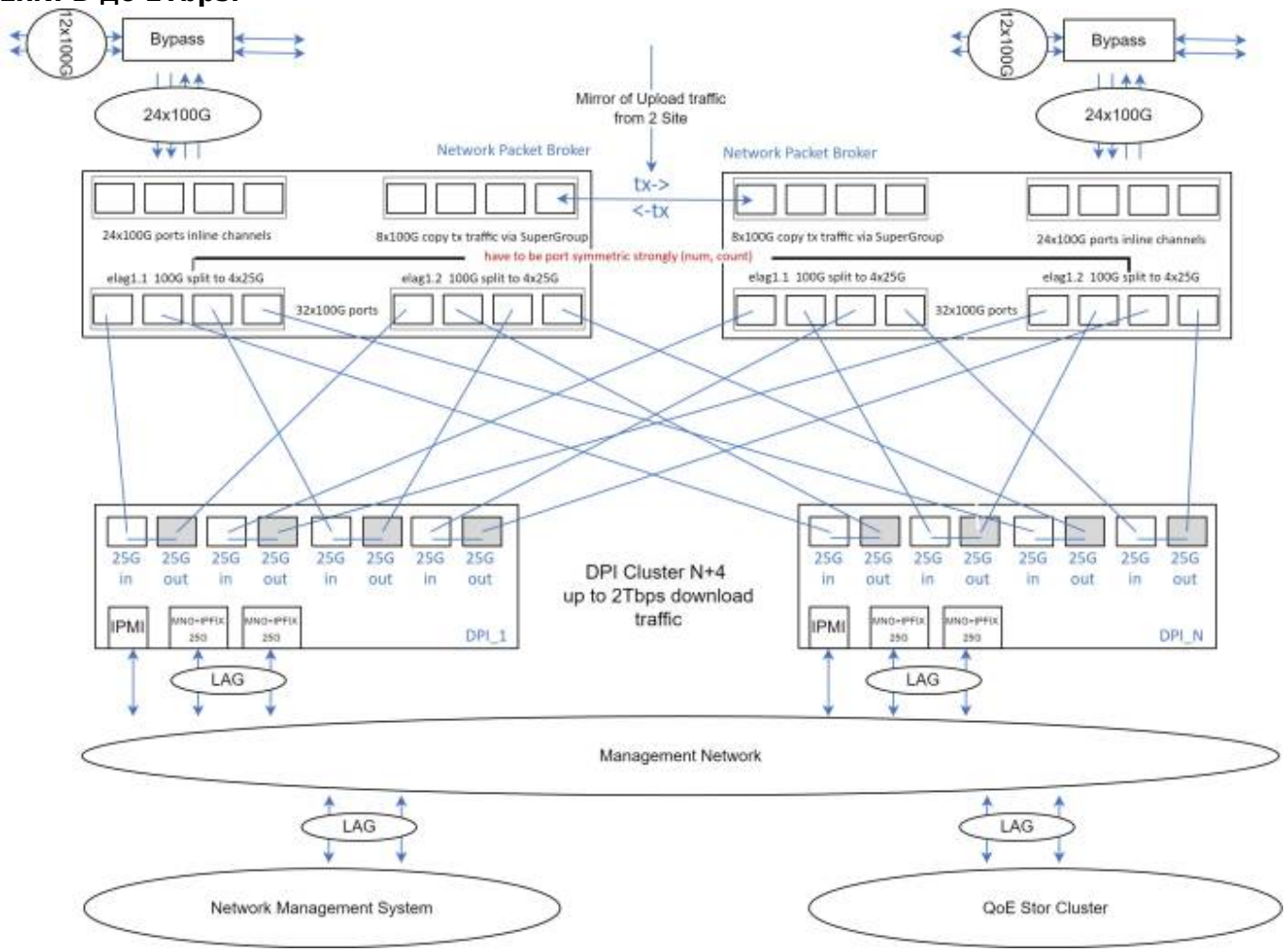
Резервирование

Кластер обеспечивает резервирование по принципу N+X, через добавление избыточных узлов DPI. В случае отказа одного или нескольких узлов DPI, в зависимости от заложенной «прочности» произойдет перебалансировка трафика. Балансировщик выведет из работы сбойный узел и перенаправит трафик на оставшиеся DPI. В случае, если из строя вышло большее количество устройств или балансировщик — система будет выведена в bypass (поведение настраиваемое). Каждый узел DPI генерирует heartbeat сообщения в сторону устройств балансировки, а те в свою очередь управляют непосредственно bypass коммутаторами, которые с одной стороны отслеживают состояние сигнала в линии, а с другой — состояние питания и программного обеспечения, то есть работоспособность кластера DPI и балансировщиков в целом.

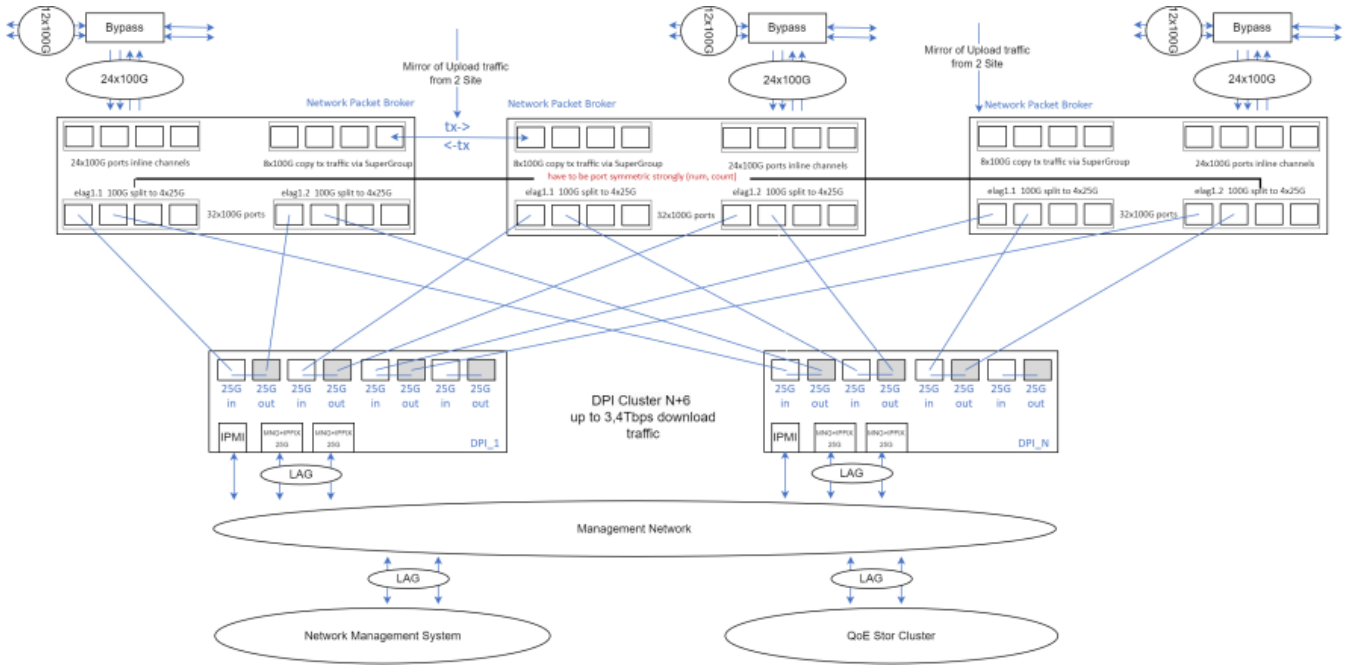
Масштабирование

Принципиальной особенностью системы является ее простое масштабирование — увеличение пропускной способности происходит за счет линейного наращивания количества устройств DPI и балансировщиков в системе.

2xNPB до 2Tbps:



3xNPB до 3Tbps:



4xNPB до 4Tbps: