Содержание

SSG DPI Cluster Organization Scheme

The complex is a high-performance, scalable cluster. It is designed for real-time analysis and management of network traffic at L2-L7 levels of the OSI network model and consists of the following elements:

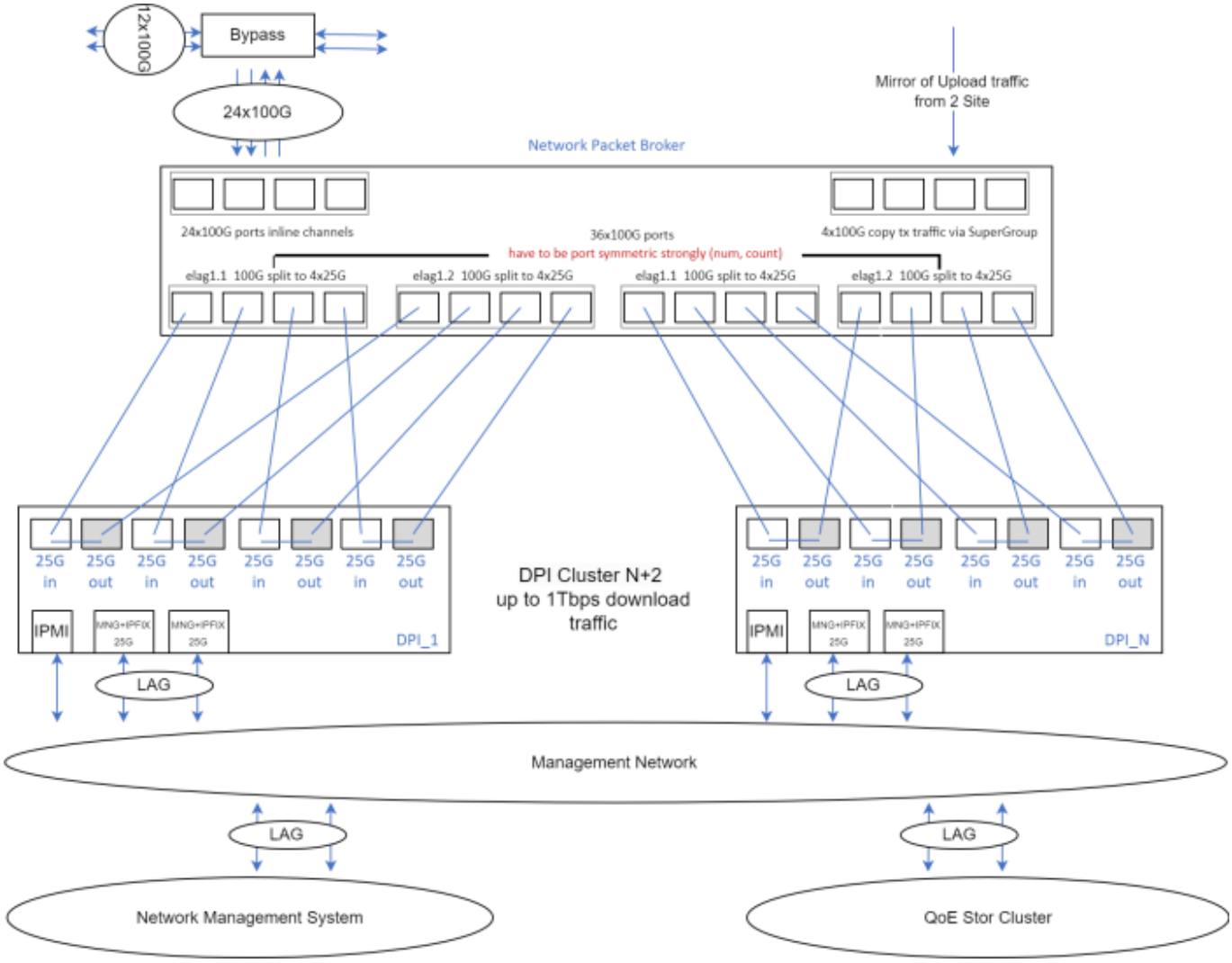
1. External optical bypass (Bypass Switch) with replaceable optical modules providing connection of SM (1310nm) or MM (850nm) lines
2. Traffic aggregator (load balancer) Network Packet Broker (NPB)
3. SSG DPI server cluster
4. Virtualization cluster for deploying the Network Management System (NMS) with a graphical interface (DPIUI2). It also includes FTP and Syslog servers for log collection from system components, an HTTP web server for centralized blacklists loading, and a monitoring system (Zabbix).
5. Data storage complex (QoE Stor) for building statistical and analytical reports, ensuring long-term storage of aggregated information
6. A set of necessary cables for communication and QSFP28/QSFP/SFP28/SFP+ modules
7. Fault-tolerant switches for connecting solution components and management

The complex is designed for inline installation and supports the following Ethernet interface types:

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

Supported encapsulations: MPLS, IPinIP, VLAN, QinQ, GRE.

1xNPB up to 1Tbps:



Traffic Flow

Telecom operator links are connected "inline" to traffic balancing devices via an optical bypass, ensuring network protection in case of hardware failures or software crashes. The traffic balancer distributes flows (sessions) among nodes, ensuring symmetric session-aware load balancing at L3/L4 levels. The entire complex operates as a transparent L2 device and generally does not require additional configurations from the telecom operator or changes in the logical network topology.

Asymmetric Traffic Processing

If asymmetric traffic is present (outgoing traffic passes through one SSG DPI site/cluster while incoming traffic goes through another), a copy of only the OUTGOING traffic from one site must be sent to the other. This ensures that ALL outgoing traffic reaches the SSG DPI clusters at different sites, eliminating traffic asymmetry. The traffic copy is transmitted via direct links between NPBs to minimize latency. The copied traffic is delivered to all DPI devices with load balancing in mind. DPI accounts for this traffic when detecting signatures but does not include it in statistical reporting. After processing, the copied traffic is discarded. This method improves recognition accuracy for asymmetric traffic. Note that outgoing traffic constitutes only 10% of incoming traffic, so mirroring between sites does not require high-bandwidth channels and does not increase the DPI cluster load.

DPI Node

The primary system component is DPI — deep packet inspection equipment. DPI is software running on general-purpose X86_64 servers supporting network cards based on Mellanox/Intel chipsets. In a typical cluster: Servers are equipped with 6x 2-port optical network cards with 10/25GE interfaces, of which 8 ports are used for traffic processing, 2 ports for sending IPFIX to the QoE server, and 2 ports are reserved.

The DPI device is fully transparent at Layer 2. When installed "inline," the client-side ports are called IN (input), and the WAN-side ports are called OUT (output). Port pairs form bridges. Proper port orientation is crucial for correct traffic detection and control functions. Each DPI node can operate independently or be connected to a cluster.

Two types of traffic processing ports are defined:

- IN - ports facing local ISPs or subscribers (LAN)
- OUT - ports facing upstream providers (WAN)

Typical server configuration: AMD EPYC 64-core processor, 512GB RAM, HW RAID controller, 2x SSD disks, 1-2x NVME SSD, 6x NIC 2x25GbE, 2x PSU.

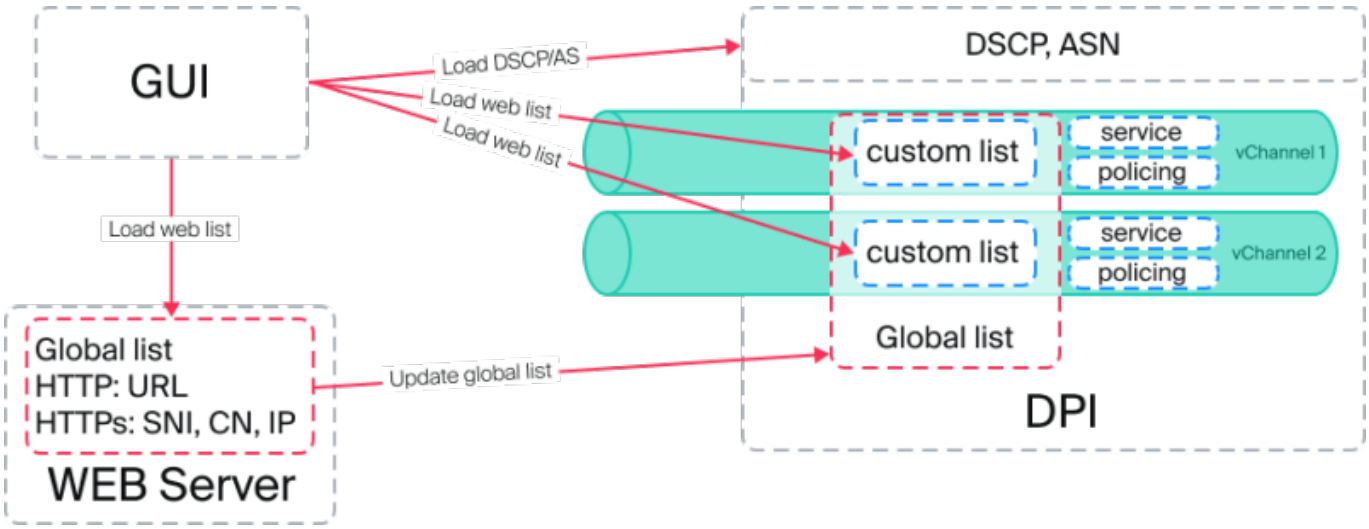
DPI performance also depends on the PPS parameter and the overall traffic profile. Performance parameters are described in detail in this article.

For proper DPI operation, it must receive both forward and reverse subscriber traffic (full bidirectional sessions); otherwise, some functions, including application protocol detection, may not work or function incorrectly. Therefore, it is crucial to ensure that bidirectional subscriber session traffic passes through a single DPI device. Traffic symmetry through DPI is maintained by mirroring outgoing traffic from one site to another and balancing on NPB.

Management

The complex is managed via a web-based management subsystem DPIUI2 — FilterUI. FilterUI manages subscriber profiles and services or downstream ISPs (including BGP signaling), traffic processing policies, including policing, filtering rules — blacklists and whitelists, custom protocols, report generation, etc. Standardized interfaces/APIs are available for integration with third-party systems. SSG DPI implements the 3GPP paradigm, and as an additional option, it supports profile and subscriber service management via an embedded PCRF module with RADIUS, Gx/Gy DIAMETER protocol support.

To switch from DPIUI2 to FilterUI, the appropriate role must be configured.



A dedicated web server is used for centralized Global Lists loading onto DPI. FilterUI exports lists to this server in a prepared format for DPI. Each DPI downloads these lists and applies them according to rules. Additionally, FilterUI exports unique rules for each DPI. If necessary, these lists are merged and applied to a channel or subscriber.

Statistics Storage

The package includes a data storage system and a report builder, allowing the creation of arbitrary (custom) reports. The report builder provides statistics on users, ISPs, IP addresses, subnets, autonomous systems, network protocols, application protocols, and their combinations, ensuring full network transparency for the customer and support for Quality of Experience. The system allows storing both raw IPFIX data and aggregated data.

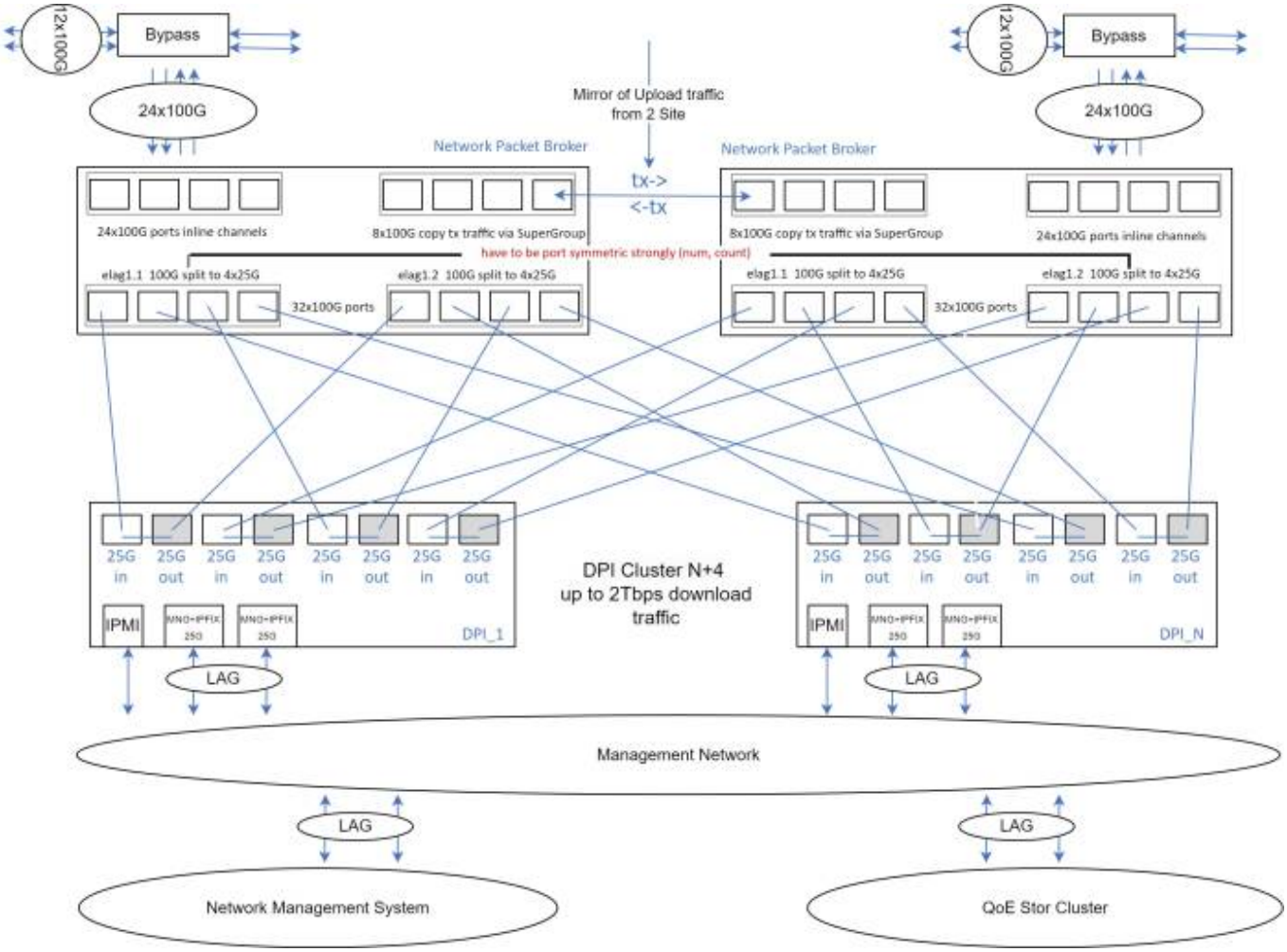
Redundancy

The cluster ensures redundancy based on the N+X principle by adding extra DPI nodes. If one or more DPI nodes fail, traffic is rebalanced based on the configured resilience level. The balancer excludes the faulty node and redirects traffic to the remaining DPI nodes. If multiple devices or the balancer fail, the system switches to bypass mode (configurable behavior). Each DPI node generates heartbeat messages towards balancing devices, which, in turn, control the bypass switches that monitor signal state in the line, power status, and software operability, ensuring the overall functionality of the DPI cluster and balancers.

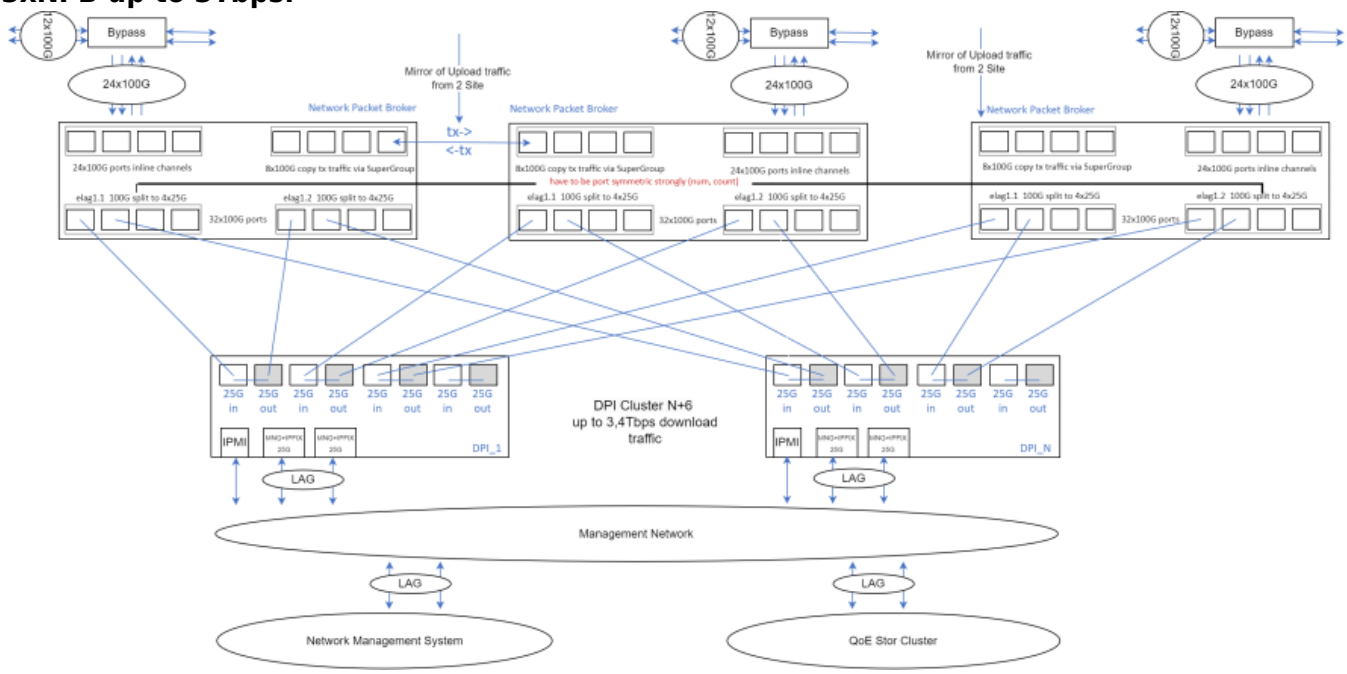
Scalability

A key feature of the system is its simple scalability — throughput increases linearly by adding more DPI devices and balancers.

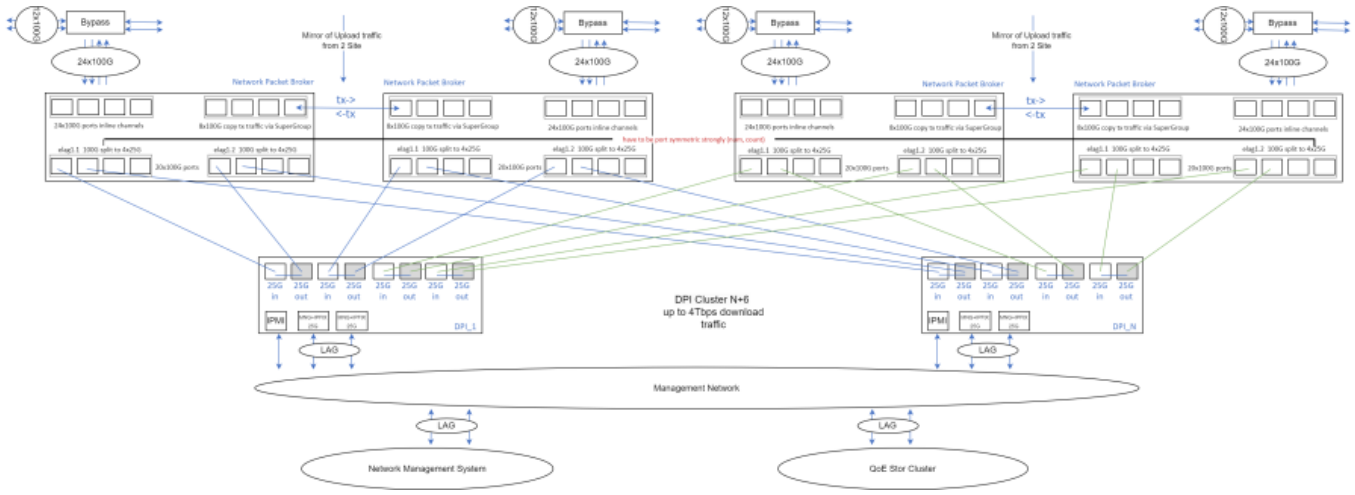
2xNPB up to 2Tbps:



3xNPB up to 3Tbps:



4xNPB up to 4Tbps:


24x100G
Bypass
24x100G
Mirror of Upload traffic from 2 Site
Network Packet Broker
Network Packet Broker
tx->
<-tx
have to be port symmetric strongly (ports_count)
Network Packet Broker
Network Packet Broker
DPI Cluster N+6
up to 4Tbps download traffic
DPI_1
DPI_N
IPMI
LAG
Management Network
Network Management System
QoE Stor Cluster