Plumla-NGN

Plumla-NGN is an FPGA based packet processor compatible with SDN OpenFlow architecture with full speed packet processing up to 160 Gbps with extremely low latency < 8μs.

Ready to support high throughput network interconnections in core and access networks, 5G networks and industrial control systems infrastructure (ICS/OT).

Key features

Compliant with SDN OpenFlow 1.3 specification and ready to be integrated with SDN controllers

Network interfaces:

- ✓ 4 x 40 Gbps (QSFP+)
- ✓ 4 x 10 Gbps (SFP+)

Best in class network performance

- ✓ packet processing 160 Gbps, 240M pps
- ✓ low latency - only <8μs
- ✓ 0 packet loss proved by RFC 2544 tests

Take advantage of unique functionalities of new Plumla-NGN appliance.

Optimize implementation cost of network services IPSec, IDS/IPS, packet analysis, SSL decryption, MPLS processing.

Apply Plumla-NGN in your core and access networks or ICS infrastructure.

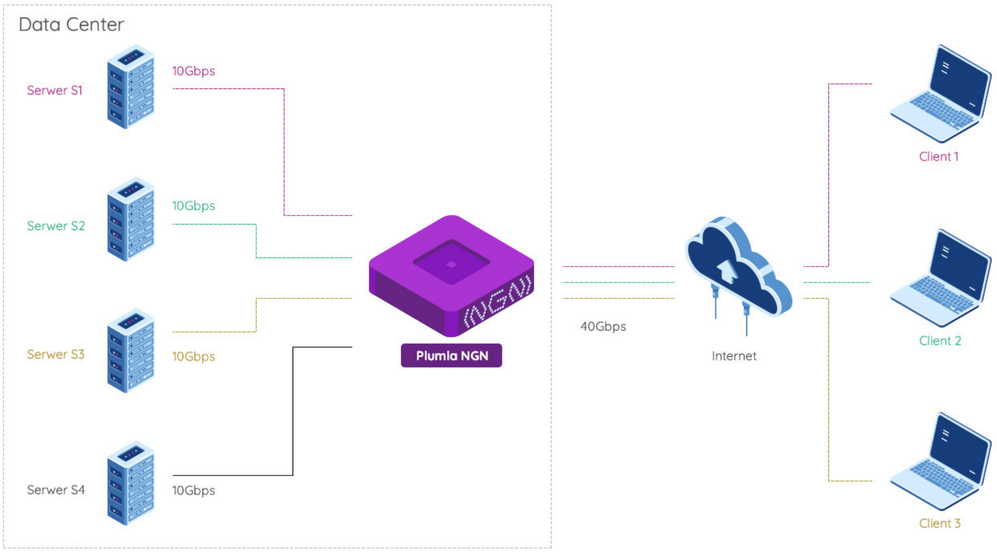
Use Plumla-NGN to enhance your Security Operation Center (SOC) and Network Operation Center (NOC) capabilities.

PLUMLA

Network use cases

The diagrams below present various network architecture use cases in which Plumla-NGN can be most effective to use.

Load Balancing



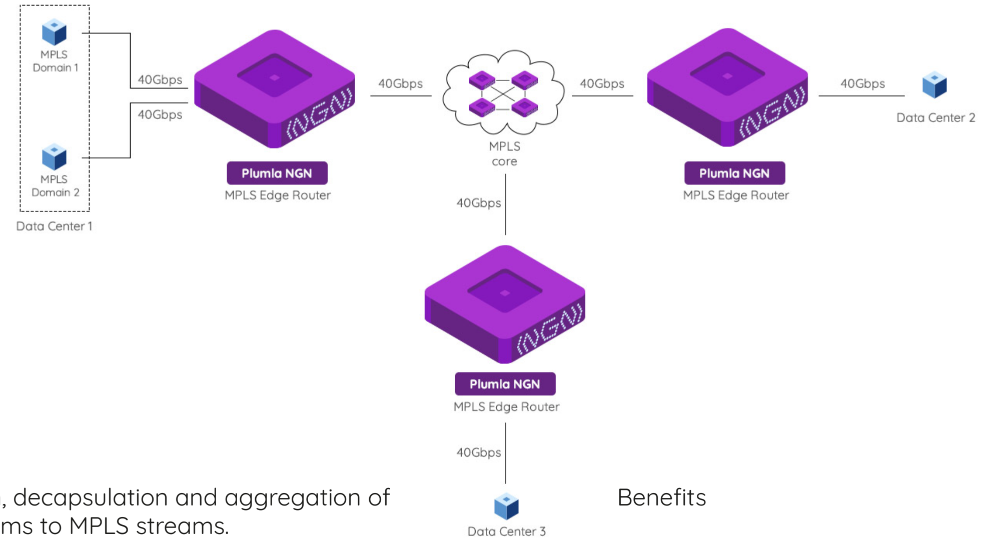
Split 40 Gbps network streams/flows into 4 x 10 Gbps interfaces – load balancing based on:

- ✓ TCP sessions
- ✓ service availability on selected servers/nodes

Benefits

- ✓ Increased services availability
- ✓ Flexible session splits
- ✓ Services uptime monitoring

MPLS VPN



Encapsulation, decapsulation and aggregation of network streams to MPLS streams.

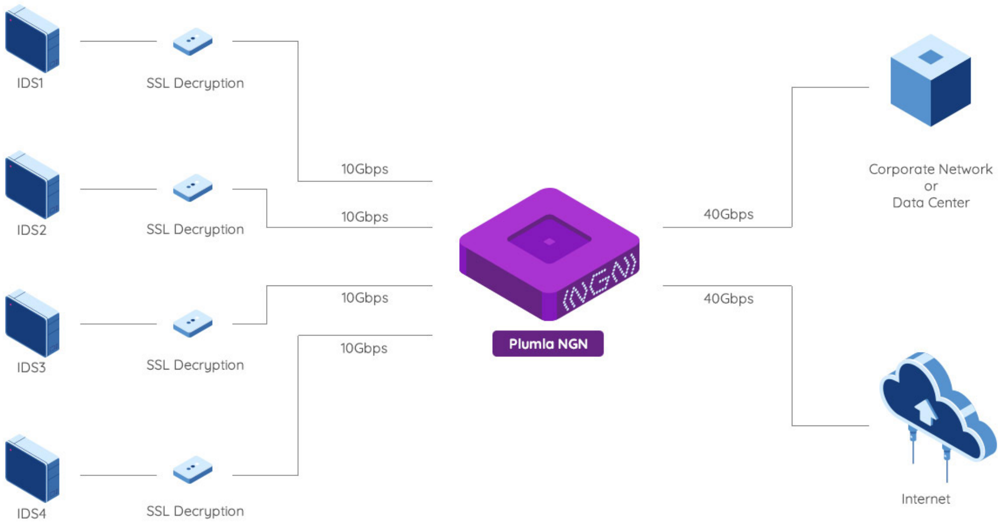
Works as an MPLS edge router as well as MPLS core router.

Benefits

- ✓ MPLS configuration flexibility
- ✓ Ingress and core MPLS traffic processing
- ✓ Access and core networks
- ✓ High speed MPLS processing (160 Gbps) with low latency

PLUMLA

SSL Decryption & IDS Monitoring



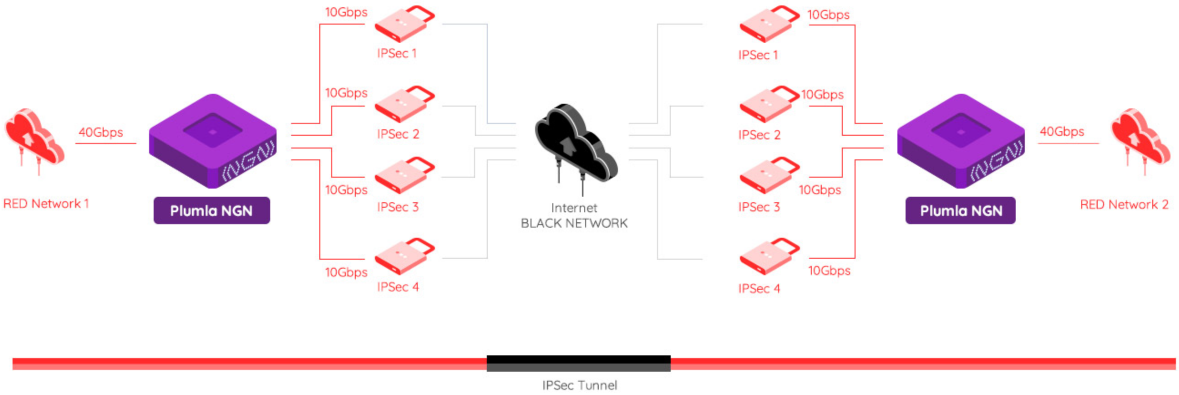
Selected network traffic can be transferred to IDS appliances or SSL decryption devices. Flexible open flow rules can be used to select traffic based on all ISO/OSI layers.

Ability to process network traffic transparently inline as well as traffic mirroring (tap).

Benefits

- ✓ Reduced cost of IDS licenses
- ✓ Wider selection of IDS appliances and SSL decryption devices
- ✓ Increased decryption and packet analysis performance
- ✓ Inline processing and traffic mirroring (tap)
- ✓ Flexible network traffic selection and filtering rules

IPSec Traffic Aggregation



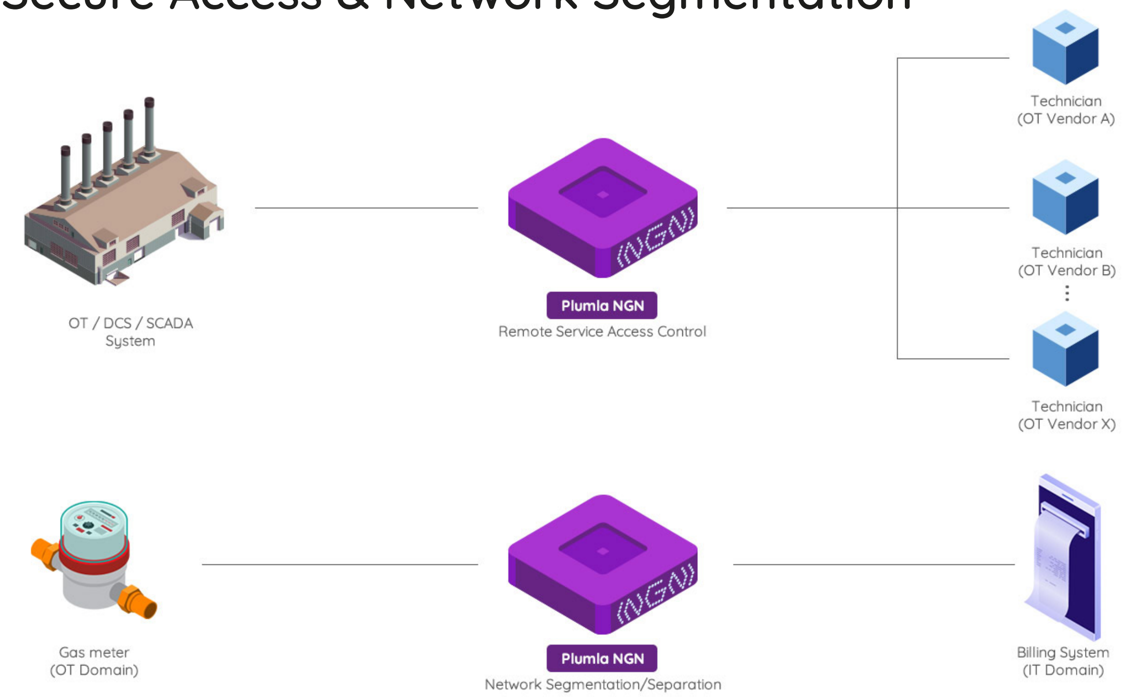
Aggregation and split of network traffic into multiple IPSec devices up to their throughput limit.

Enables to increase the total IPSec throughput using existing or more cost-effective IPSec devices

Benefits

- ✓ Increased total IPSec throughput
- ✓ Removed IPSec bandwidth limit
- ✓ Flexible traffic division rules into multiple IPSec devices

OT Secure Access & Network Segmentation



Provide secure remote service access to industry control systems (SCADA) for technicians. Improve control over the remote sessions by applying firewall rules, service window definitions and network traffic monitoring for accountability.

Implement proper network segmentation according to Purdue model for ICS systems and utilize unidirectional connections for critical components, take advantage of fully flexible traffic flow control.

Benefits

✓ Remote service access control in ICS systems (DCS/SCADA)
✓ Data exchange control in ICS systems
✓ Network segmentation
✓ Traffic separation

Contact

Sales: sales@plumla.com
Support: support@plumla.com

Tel: +48 22 822 0673

PLUMLA Sp. z o.o.
Mołdawska 9 Street
02-127 Warsaw, Poland