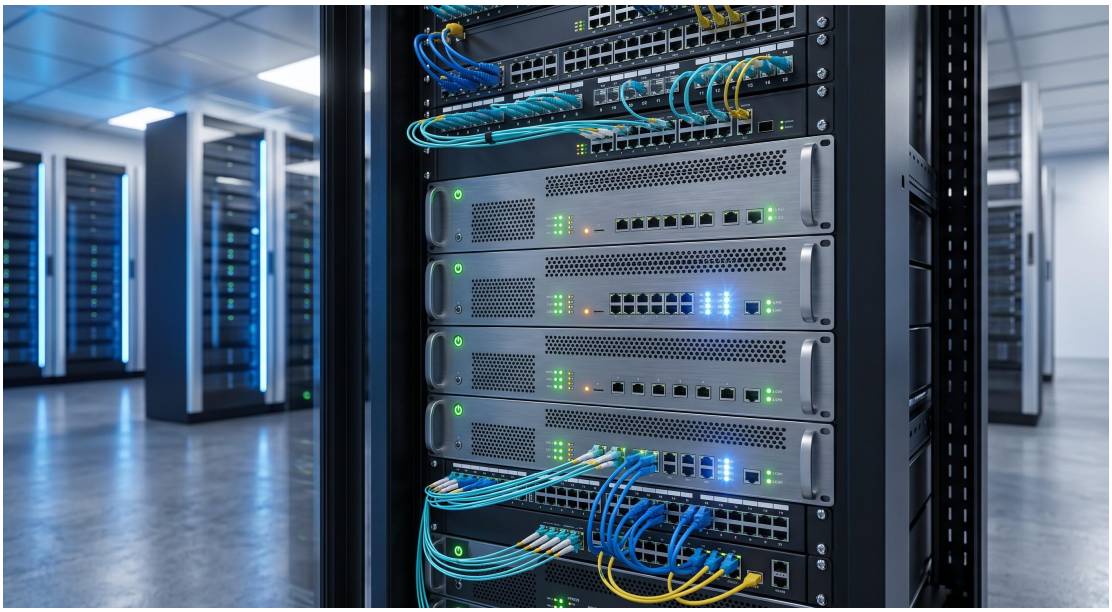
Carrier-Grade Routing Solution Brief: Deploying Hardware Firewall Inspection Engine Optimization for High-Concurrence TCP Traffic

TARGET NETWORK POSITIONING

The Hardware Firewall Inspection Engine Optimization for High-Concurrence TCP Traffic is a carrier-grade security and routing platform purpose-built for service provider edge, mobile backhaul, and large enterprise core deployments. It addresses the critical performance bottleneck that occurs when stateful firewall inspection is applied to massively concurrent TCP sessions, where per-session state tracking, deep packet inspection, and flow table lookups can degrade forwarding throughput and increase latency. This solution integrates a dedicated hardware inspection engine that offloads session state management, TCP proxy operations, and security policy enforcement from the main forwarding ASIC, enabling line-rate firewall inspection even under extreme session concurrency.



HARDWARE-LEVEL FAILOVER REDUNDANCY

The platform is engineered for uninterrupted operation in carrier environments. Dual hot-swappable power supplies, redundant fan trays, and a 1+1 control plane redundancy architecture ensure that no single component failure interrupts traffic inspection. The hardware inspection engine itself supports stateful session synchronization across redundant nodes, allowing TCP sessions to survive failover events without re-establishment. This is achieved through dedicated inter-chassis synchronization links that replicate session state tables in real time, with sub-second convergence.

PROTOCOL SUPPORT MATRIX

The inspection engine supports a comprehensive suite of protocols required for

high-concurrence TCP environments, including TCP, UDP, ICMP, SCTP, and application-layer gateways for HTTP, HTTPS, SIP, and DNS. It includes full IPv4 and IPv6 dual-stack inspection, NAT44, NAT64, and DS-Lite capabilities. Advanced TCP proxy features such as SYN flood protection, session aging, and per-session QoS marking are handled directly in hardware.

CORE PARAMETERS

- Concurrent TCP Sessions: 120 million
- New Sessions per Second: 2.5 million
- Firewall Inspection Throughput: 400 Gbps
- Latency (Inspection Enabled): < 12 microseconds
- Session Table Memory: 128 GB DDR5 dedicated
- Redundancy: 1+1 control plane, N+1 power

Parameter	**Specification**
Form Factor	2RU Modular Chassis
Switching Capacity	800 Gbps
Firewall Inspection Throughput	400 Gbps
Concurrent TCP Sessions	120 Million
New Sessions per Second	2.5 Million
Inspection Latency	< 12 µs

Session Table Memory	128 GB DDR5
Power Supply	Dual Hot-Swappable Redundant AC/DC
Redundancy	1+1 Control Plane, N+1 Fan/Power
MTBF	> 500,000 Hours
Protocol Support	TCP, UDP, ICMP, SCTP, HTTP, HTTPS, SIP, DNS, IPv4/IPv6, NAT44, NAT64, DS-Lite
Routing Protocols	BGP, OSPF, IS-IS, MPLS L3VPN

LIFECYCLE ASSURANCE (MTBF)

The platform is designed for a mean time between failures (MTBF) exceeding 500,000 hours, validated through accelerated life testing and field reliability data from carrier deployments. Comprehensive lifecycle management includes predictive failure analysis, hot-swappable components, and a 10-year hardware support commitment with guaranteed spares availability.

TARGET BACKBONE TOPOLOGIES

Typical deployments include service provider security gateways at the peering

edge, mobile core Gi/SGi firewall clusters, and datacenter perimeter inspection nodes. The platform supports BGP, OSPF, IS-IS, and MPLS L3VPN, enabling integration into existing carrier routing domains. It can be deployed in active/active clusters with session synchronization, or in active/standby configurations for simplified management.

