

QUANTUM QLS800 LIGHTSPEED FIREWALL



Check Point Quantum Lightspeed Next Generation Firewalls redefine security price performance — enabling enterprises to deploy network security that performs at the speed of business to accelerate large file transfers and provide low latency for high frequency applications.



Secure Hi-speed Data Transfers

800 Gbps line-rate in a single firewall



Protect Hi-frequency Trading Apps

3 μ Sec ultra low latency



Resilient Data Center Security

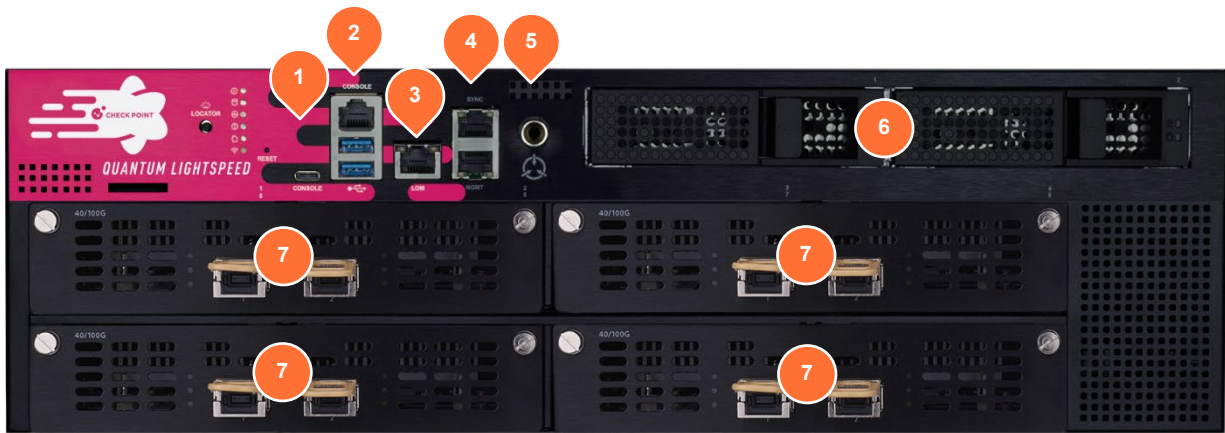
Eliminate failure with a robust clustering technology



QLS800

QUANTUM SECURITY PLATFORM

QLS800 LIGHTSPEED FIREWALL



- | | |
|-------------------------------------------------|---------------------------------------------------|
| 1. RJ45 and USB Type-C console ports | 5. ESD grounding point |
| 2. 2x USB 3.0 ports | 6. 2x 960GB SSD RAID1 |
| 3. Lights-out Management port | 7. 4x double-wide ConnectX NICs |
| 4. Sync and Management 10/100/1000 Base-T ports | 3x redundant power supplies (back view not shown) |

Low Latency, High Throughput Firewall

Quantum QLS800 firewalls are equipped with four NVIDIA ConnectX network interface cards (NIC), each with 2x 100G QSFP28 ports. NVIDIA ConnectX NICs offload network processing from the host CPUs, providing substantial performance gains of up to nearly 800 Gbps for trusted firewall traffic. In addition, firewall latency is significantly reduced to a low 3µSec at nearly line rate ensuring access to data and higher throughput with minimal delay.

All-inclusive Security

Check Point QLS800 firewalls include the Check Point stateful inspection firewall and are also available in all-inclusive security packages such as NGFW (Application Control with IPS), NGTP (NGFW with URL filtering, antivirus, and anti-bot) or SandBlast (NGTP with sandboxing and Threat Extraction, a Content Disarm & Reconstruction technology).

Resilient Security

Modern organizations need robust cyber security to protect their critical systems. High Availability (HA) firewall clusters are designed to minimize downtime for critical systems using redundant systems. If an organization wants to implement a simple HA firewall cluster with up to 5 nodes, this can be accomplished using Check Point's built-in HA and load sharing functionality: ClusterXL.

Check Point ClusterXL is a software-based clustering solution for firewall redundancy and load sharing which uses state synchronization to keep active connections alive and prevent data loss if a cluster member fails. This ensures critical systems are always connected and secure. In addition, each QLS800 has redundancy built-in with two SSD drives in a RAID1 array and hot-swappable redundant power supplies, ensuring continuity when one component fails.

Remote Management and Monitoring

A Lights-Out-Management (LOM) card provides out-of-band remote management to remotely diagnose, start, restart and manage the appliance from a remote location. Also use LOM for remote installs of the GAiA OS.



More is demanded of today's network devices. There are simply more connected devices. Apps and connected applications are more content-heavy. For instance, workloads and data sets move from on-premises data centers to the cloud and back again, encapsulated in VXLAN, GRE and VPN packets. Furthermore, some apps require pure speed. For High Frequency Trading apps, profit or loss is determined by nanosecond differences in network latency. Check Point Quantum Lightspeed firewalls deliver on these demands for high throughput with low latency by securely offloading network processing to NVIDIA ConnectX NICs.

NVIDIA ConnectX

The eight single-width slots in the QLS800 support four NVIDIA ConnectX dual-width network cards, each with 2x 100G QSFP28 ports, supporting an aggregate throughput of close to 200G of firewall throughput through each ConnectX NIC. The dual-width cards maximize the PCIe bandwidth beyond a single slot limit. With the four ConnectX NICs in the QLS800 access to data and higher throughput with minimal delay is ensured for trusted traffic.

How it Works

The first packet of a connection is validated by the firewall to decide if the connection is allowed by policy based upon port and IP address. If allowed, the firewall uses a Data Plane Development Kit (DPDK) API to instruct the ConnectX to allow a bidirectional connection between the client and server. Subsequent packets are processed on the ConnectX NIC. This includes doing stateful inspection checks such as full header validation of TCP state and sequence number validation. In addition, the ConnectX NIC supports Network Address Translation (NAT) and encapsulates and decapsulates packets in VXLAN and GRE tunnels. Furthermore long duration sessions of large data transfers of up to 100G that occur within a single connection, also called elephant flows, are securely offloaded to the ConnectX.

Accelerating connections by offloading connections to a lower OSI layer device is not a new Check Point technology. Check Point SecureXL technology was developed over a decade ago to offload network processing to a lower level device to accelerate packet rates. As a stateful firewall, once a connection is allowed by policy, an entry is created in the firewall's connections table. The firewall then updates lower level devices so that bidirectional connections can be checked and allowed by the device. The device and the firewall update connection tables as the state changes. With NVIDIA, this is done using the industry standard DPDK API. When the connection ends, responsibility for handling the connection teardown is shifted back to the firewall.

Focused, Parallel Processing

For advanced inspection such as IPS that requires pattern matching, connections are distributed to the multiple cores of the QLS800. This is how Check Point delivers a network security architecture that offers true threat prevention, not just threat detection. It does this without delay in one session, scales across multiple sessions, and is agile enough for deployment wherever you need security — on premises and in the cloud.

LIGHTSPEED SECURITY USE CASES

Any Enterprise with a Data Center, Hybrid Cloud or Distributed Data Centers

Secure High Speed Transfers of Large Data Sets: Networks converge at the data center core and in high speed interconnects between data centers and the hybrid cloud. Businesses routinely transfer large data sets across these networks for data analysis, disaster recovery planning and workload migration.

Quantum Lightspeed 100 gigabit network interfaces enables enterprises to accelerate these transfers of large data sets across data center core and data center interconnects — supporting close to 250, 450, 650 and 800 Gbps of single firewall throughput in the QLS250, QLS450, QLS650 and QLS800 respectively. Add redundancy and scale even higher using the unique Maestro Active-Active load sharing solution where multiple Quantum Lightspeed MLS200 and MLS400 firewalls scale throughput nearly linearly with each additional firewall added to the cluster.

Banking and Financial Services

Secure Financial Transactions with Micro-second Latency: In the world of finance where trading and cryptocurrency algorithms generate millions of transactions, a fraction of a second makes a huge difference. In some reports 80% of trading on the stock market is done via algorithmic-based automated programs that execute software programs to buy, sell or hold assets.

High frequency trading firms need network security technology that does not introduce latency and satisfies regulatory and compliance security mandates. The Quantum Lightspeed NGFW series enables banking, insurance and investment firms to securely increase transaction capacity for high frequency applications by deploying network security that performs at the speed of business — with low 3µSec latency.

The 100 gigabit QSFP28 network interfaces in the Quantum Lightspeed firewalls comfortably handle initial transfers of large data sets at the start of the trading day. They also support up to 100G elephant flows. These are characterized by a large, continuous flow that stays open and occupies a disproportionate share of the total bandwidth of a network link for a long duration.

Any Enterprise Requiring Investment Security

Support Hyper-growth with Scalable Security Throughput: Some businesses such as ecommerce see wide and seasonal requirements in online traffic. In 2020 all businesses saw a boost in traffic as workers moved to a work from home model. Other scenarios requiring scalable security are business mergers, data center consolidation and migrations to cloud, hybrid cloud and hybrid data center models.

When used in the unique Maestro Hyperscale Network Security solution with the MLS200 and MLS400, enterprises can scale to up to 3 Tbps of firewall throughput. Each additional firewall added to the Maestro Active-Active load sharing cluster, scales throughput nearly linearly. Furthermore customers can group multiple firewalls into Security Groups and move firewalls manually or dynamically as needed from one group to another as needed to meet changes in traffic demands. Security Groups are logical groups of appliances where each Security Group has dedicated internal and external interfaces and may have a different configuration set and policy. The Maestro Orchestrator MH0175 has a total fabric capacity of 3.2 Tbps with 400 nsec port to port latency and supports up to 32x 100GbE or 128x 10GbE network interfaces.

Telco 5G Networks

Support Hyper-growth with Scalable Security Throughput: The demand for improved speeds, low latency, and connecting a larger number of devices has paved the path to 5G, fifth generation digital cellular networks. Telco mobile operator 5G networks are also expected to be widely used for private networks with applications in industrial IoT, enterprise networking, and critical communications. The network topology will be sliced with logical networks riding on top of the core infrastructure and previously unimaginable services will be created. These use cases require the ability for mobile operators to scale security functions with elasticity using Quantum Maestro in order to guarantee service continuity and availability.

SPECIFICATIONS

QLS800	
Firewall System Performance	
Firewall 1518B UDP (Gbps)	796
Firewall Latency (avg)	3µSec
Connections/sec	546,150
Concurrent Connections	48M
Accelerated 100GbE Ports	8
Additional System Performance	
Firewall (Gbps) ¹	205
IPS (Gbps) ¹	140.9
NGFW (Gbps) ¹	96.1
NGTP (Gbps) ¹	33.3
VPN-AES 128 (Gbps)	45
Virtual Systems (max)	250
Additional Features	
CPU Cores	2x 36 physical, 72 virtual
Storage	2x 960GB SSD RAID1 array
Redundant Power	3x AC (DC option)
Memory (RAM) Default/Max	192 GB
LOM	✓
Console and USB Ports	RJ-45 and 1x USB-C, 2x USB 3.0 ports
Network Connectivity	
Network Ports	2x 10/100/1000Base-T RJ-45 ports, 8x accelerated QSFP28 100G ports
VLAN Maximums	1024 single gateway, 4096 with virtual systems
802.3ad link Aggregation	✓
Deployments	Layer 2 (transparent), Layer 3 (routing)
High Availability	Active-Passive
Unicast and Multicast Routing	OSPFv2 and v3, BGP, RIP, PIM-SM, PIM-SSM, PIM-DM, IGMP v2, and v3
Policy-based Routing	✓
User-based Policy	Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3 rd parties via a Web API
Physical	
Enclosure	3RU
Dimensions (W x D x H)	17.4 x 24 x 5.2 in., (442 x 610 x 132mm)
Weight	46.3 lbs. (21 kg)
Power, Environments	
Dual, Hot-Swappable	✓
Power Input	AC:(100 to 240VAC, 47-63Hz), DC 40--72VDC
Power Supply Rating	AC 850W, DC 1300W
Power Consumption (avg/max)	AC 472W/826W
Thermal Output (max)	2818 BTU/hr.
Operating Environment	Operating (0° to 40°C, humidity 5% to 95%), Storage (-20° to 70°C, humidity 5% to 95% at 60°C)
Certifications	
Safety/Emissions/Environment	UL, CB, CE, TUV GS / FCC, CE, VCCI, RCM/C-Tick / RoHS, WEEE, REACH ¹ , ISO14001

1. Performance measured with enterprise testing conditions with logging enabled. NGFW: FW, App Control and IPS, NGTP: FW, App Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection.

ORDERING QUANTUM QLS800

DEFAULT CONFIGURATION ¹	SKU
QLS800 includes 8x100G QSFP28 ConnectX ports, 192 GB RAM, 2x 960GB SSD, 3x AC PSUs, LOM, telescopic rails and 5 Virtual Systems	CPAP-SG-QLS800

The default package includes 5 virtual system (VS) licenses which are additive when adding additional VS licenses.

¹ NGFW, NGTP and SandBlast (SNBT) packages and renewals are available in the online product catalog.

QLS800 Accessories

QLS800 INTERFACE CARDS AND TRANSCEIVERS	SKU
2 Port 100G QSFP28 ConnectX Transceivers	
QSFP28 transceiver module for 100G fiber ports - short range (100GBase-SR4)	CPAC-TR-100SR
QSFP28 transceiver module for 100G fiber ports - long range (100GBase-LR4)	CPAC-TR-100LR
100G SWDM4, LC connector, 75m/OM3 fiber	CPAC-TR-100SWDM4
100G CWDM4, LC connector, 2Km/ single mode fiber	CPAC-TR-100CWDM4
QSFP+ transceiver module for 40G fiber ports - short range (40GBase-SR)	CPAC-TR-40SR-QSFP-300m
QSFP+ transceiver module for 40G fiber ports - long range (40GBase-LR)	CPAC-TR-40LR-QSFP-10Km
Bi-directional QSFP transceiver for 40G fiber ports - short range (40GBase-SR-BD)	CPAC-TR-40SR-QSFP-BIDI
QSFP28 to SFP28 Adapter - 10G/25G fiber adaptor	CPAC-TR-QSFP28-SFP28
SFP28 transceiver module for 25G fiber ports with QSFP28 adaptor - short range (25GBase-SR)	CPAC-TR-25SR-ADP
SFP28 transceiver module for 25G fiber ports with QSFP28 adaptor - long range (25GBase-LR)	CPAC-TR-25LR-ADP
SFP+ transceiver module for 10G fiber with QSFP28 adaptor - for links up to 40km (10GBASE-ER)	CPAC-TR-10ER-ADP
SFP+ transceiver module for 10G fiber with QSFP28 adaptor - long range up to 10km (10GBase-LR)	CPAC-TR-10LR-ADP
SFP+ transceiver module for 10G fiber with QSFP28 adaptor - short range (10GBase-SR)	CPAC-TR-10SR-ADP
SFP+ transceiver 10GBASE-T RJ45 (Copper) with QSFP28 adaptor - for links up to 30m over CAT6a/CAT7	CPAC-TR-10T-ADP
100G Direct Attach Copper cable (QSFP28), 3 meters	CPAC-DAC-100G-3M
40G Direct Attach Copper cable (QSFP28), 3 meters	CPAC-DAC-40G-3M
25G Direct Attach Copper cable (QSFP28), 3 meters	CPAC-DAC-25G-3M
10G SFP+ Direct Attach Copper (DAC) cable, 3 meters	CPAC-DAC-10G-3M

QLS800 SPARES AND MISCELLANEOUS	SKU
960GB SSD for Lightspeed Security Gateways	CPAC-SSD-960G-C
AC power supply for 16600HS, 26000, 28000, 28600HS Security Gateways	CPAC-PSU-AC-26000/28000
Dual DC power supplies for 16000 and 26000 Security Gateways	CPAC-PSU-DC-Dual-16000/26000/28000
DC power supply for 16000 and 26000 Security Gateways	CPAC-PSU-DC-16000/26000
Replacement Lights-Out Management Module	CPAC-NLOM-C
Replacement Fan	CPAC-FAN-26000/28000
Slide rails for 26000 Security Gateways (22" - 32")	CPAC-RAIL-L
Extended slide rails for 26000 Security Gateways (24" - 36")	CPAC-RAIL-EXT-L

ORDERING QUANTUM QLS800 (Continued)

All-inclusive Security

	FW	NGFW	NGTP	SNBT (SandBlast)
	Firewall	Basic access control plus IPS	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓	✓	✓
VPN (IPsec)	✓	✓	✓	✓
Mobile Access	✓	✓	✓	✓
Identity Awareness	✓	✓	✓	✓
Content Awareness	✓	✓	✓	✓
Application Control		✓	✓	✓
IPS		✓	✓	✓
URL Filtering			✓	✓
Anti-Bot			✓	✓
Anti-Virus			✓	✓
Anti-Spam			✓	✓
DNS Security			✓	✓
SandBlast Threat Emulation				✓
SandBlast Threat Extraction				✓
Zero Phishing				✓

The base includes the firewall. Security subscription NGFW, NGTP and SNBT extensions and renewals for subsequent years are also available.