Datasheet

Nexusguard
Bastions Server R760
R760-400G

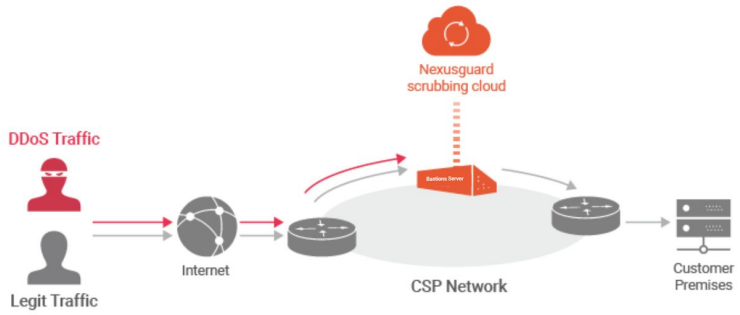
DDoS protection products are vital in a comprehensive and multi-dimensional cybersecurity strategy to secure your digital assets, online services, productivity and reputation in line with your objectives, resources and network infrastructure.

Manufactured by one of the world's leading technology companies, Nexusguard Bastions server R760 is a full-featured enterprise server, designed to optimize workloads performance and data centre density, incorporating Nexusguard's proprietary technologies, tools and over a decade of DDoS fighting experience.

Nexusguard Bastions server R760 integrates seamlessly with CSP network infrastructures, allowing bad DDoS traffic to be identified and blocked automatically in seconds, all the while delivering higher scalability and optimum protection against DDoS attacks.

How Does It Work?

Nexusguard's Bastions server R760 mitigates L3/L4 attacks that attempt to flood the core and downstream networks of the CSP by inspecting traffic, detecting threats and blocking attacks against protected networks, in real-time. When attacks threaten to overwhelm local capacities, Nexusguard's globally distributed scrubbing is activated, stopping global attacks in their tracks, ensuring they never enter the CSP's networks.



Upon detection of traffic anomalies, all traffic is routed to Nexusguard Bastions server R760 for scrubbing. Clean traffic is then routed back to customer premises. Nexusguard scrubbing cloud kicks in if traffic exceeds pre-defined thresholds.

Key Features

- DDoS Protection for all Volumetric and Protocol attacks
- Small footprint 2U engine with 400 Gbps mitigation capability
- 3-tiered multi tenant capabilities, improving user experience and enhancing customer management
- Local and Remote DDoS protection with traffic anomaly monitoring via router telemetries
- Fully managed service including maintenance, monitoring and upgrades
- Flexible deployment architectures
- Integration with Nexusguard Cloud for true-hybrid global mitigation protection
- Fully managed service including monitoring, regular updates and maintenance

Managed Security Service

Nexusguard Bastions server R760 hardware provides comprehensive L3/4 DDoS protection services through its Clean Pipe and Origin Protection, protecting infrastructure networks and downstreams from cyberthreats.

Designed for multi-tenant environments, Nexusguard Portal is a traffic visibility, management and reporting system built to meet the diverse needs of modern networks. Nexusguard Portal combines network visibility, powerful tools and educational resources to create a cost-effective, “single-pane-of-glass” for managing the Bastions server R760 hardware to deliver a comprehensive DDoS detection and mitigation service.

Bastions server R760 can be integrated into the CSP’s on-premise security solutions and dedicated private cloud, augmented by failover to Nexusguard’s global scrubbing cloud network for enhanced protection and mitigation against extensive DDoS attacks.

Customer Portal

Featuring integrated dashboard and tabulated analytics, the Customer Portal allows your customers to view and configure various detection and mitigation settings. Depending on which solution your customer has signed up for, the customer can access any or all of them via the Customer Portal.

- View detection policy
- View policy settings and mitigation templates
- Monitor real-time traffic, i.e. raw and clean bandwidth
- View network performance
- View ongoing and stopped DDoS attacks and potential threats
- View visitor countries/region, source IPs, connection speed, counts, etc.
- View detailed event logs and download raw logs and monthly reports
- View security policies

Partner Portal

The Partner Portal is designed for the CSP partner, offering granular visibility into the core network and customer networks under protection.

- Manage customer accounts and subscriptions
- Define and set detection policy and alerts generation
- Configure customer policy settings and mitigation templates
- Monitor aggregate network traffic, i.e. raw and clean bandwidth, in real time, event/attack details and mitigation results in the integrated dashboard
- View Visitor/Threat Map to track attack source IPs, geolocations, etc.
- Retrieve all logs, including user access and audit logs

Nexusguard Apps

Nexusguard Apps is the extension of the Partner Portal's standard features. These Add-Ons can operate as standalone features or packages, such is the case as our Event Notifier and Logger, for instance, that were developed to enhance the functionality of our Portal's event notification and log management.

Hardware Specification

Hardware	
Network interfaces	R760-400G: 4x 100GbE QSFP28 Optic via transceiver
Rack unit	2U
Dimensions	WxDxH: 482 mm x 758.29 mm x 42.8 mm without bezel WxDxH: 482 mm x 772.13 mm x 42.8 mm with bezel
Weight	36.1 kg
Power Supply	1400W mixed mode (AC: 50/60 Hz, 100~240 Vac/12-8A, 5250 BTU/hr DC: 240 Vdc/6.6 A, 5250 BTU/hr)
Maximum Power Consumption	1100 Watts
Operating temperature	10 (50°F) to 35°C (95°F) with no direct sunlight on the equipment (for altitudes <= 900 m)
Operating humidity	8% RH with -12°C minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point
Operational altitude de-rating	Maximum temperature reduces by 1°C/300 m (33.8°F/984 ft) above 900 m (2953 ft)
Deployment	
Design	Standalone
NetShield engine	1
Network interface options	R760-400G: 4x 100GbE QSFP28 Optic via transceiver
No. of ASN supported	1
BGP	eBGP or iBGP
Flow protocol support	Netflow v5 / 9 IPFIX sflow v2 / 4 / 5 Netstream v5 / 8 / 9
Flow data rate	50 kfps
No flow data alert	Supported via Notifier app
OOB interface & bandwidth requirement	mgt-0 1 Gbps RJ45 | mgt-1 1 Gbps RJ45 | iDRAC 1 Gbps RJ45 Recommended bandwidth - 1 Gbps
SNMP support	v2c
IP support	IPv4 & IPv6
OOB IP	1x /29 default gateway + R760 iDRAC + R760 management x4
Performance	
Maximum L3/4 forwarding rate in bps	400 Gbps
Maximum L3/4 forwarding rate in pps	300 Mpps
Security notes	Management traffic exchanged between commander @ R760 and Nexusguard cloud are transmitted through an encrypted channel. . OOB interface shall be protected by ACL @ border router to restrict unauthorized access.

NEXUSGUARD®

Founded in 2008, Nexusguard is a leading distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communications service providers to deliver DDoS protection solutions as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime. Visit www.nexusguard.com for more information.

contact@nexusguard.com
www.nexusguard.com