Datasheet

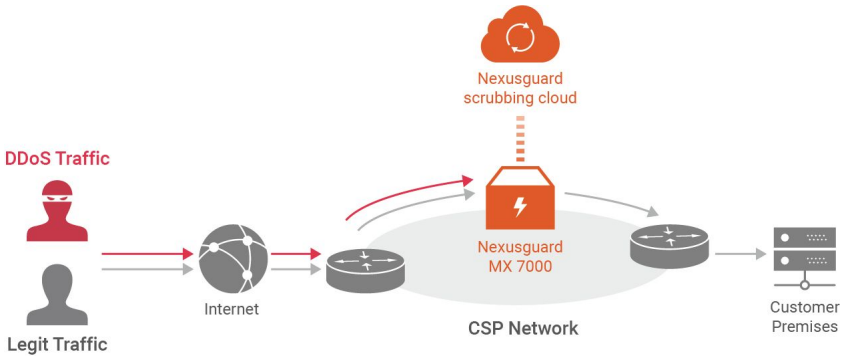
Nexusguard
Bastions Server MX7000

MX7000-100G-CP | MX7000-100G | MX7000-200G

To adequately address the complexities of tomorrow's cyber threat landscape, Communications Service Providers (CSPs) find themselves unnecessarily burdened in the endless cycle of identifying, implementing and refreshing solutions for their business needs. The Nexusguard Bastions server MX7000 provides a powerful, versatile "cloud-in-a-box" DDoS mitigation solution for CSPs dealing with the impacts brought about by cyberattacks, or seeking to add advanced cybersecurity capabilities to their product portfolio.

How Does It Work?

Nexusguard's Bastions server MX7000 mitigates all L3/L4 attacks that attempt to flood the core and downstream networks of the CSP, and mitigates complex L7 attacks that target the computing resources of their customers, by inspecting traffic, detecting threats and blocking attacks against protected networks and application resources, in real-time. And when attacks threaten to overwhelm local capacities, Nexusguard's globally distributed scrubbing is activated, stopping global attacks close to its source and ensuring it never enters the CSP's networks.



Upon detection of traffic anomalies, all traffic is routed to Nexusguard MX7000 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, Protocol and Application Layer attacks
- Reverse web proxy module for superior application security and features
- Origin Protection module for remote networks via GRE Tunnel and BGP traffic diversion
- Web Application Firewall to counteract advanced application attacks
- 3-tiered multi tenant capabilities for enhanced customer management and user experience
- Fully customizable module loadout for different business applications
- Local and Remote DDoS and traffic anomaly monitoring via router telemetries
- Fully managed service including maintenance, monitoring and upgrades

Managed Security Service

Nexusguard Bastions server MX7000 hardware provides comprehensive L3/4 and L7 DDoS protection services through its four pillars: Application Protection, Clean Pipe, DNS Protection 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 MX7000 hardware to deliver a complete DDoS detection and mitigation service.

Bastions server MX7000 can be integrated into the CSP’s on-premise security solutions and dedicated private cloud, augmented by failover to Nexusguard’s global scrubbing cloud for enhanced protection and mitigation against large DDoS attacks.

Bastions Server MX7000 Hardware Features

- Flexible deployment architectures:
  - High Availability (HA) design interconnecting with multiple internet border routers with port channels
  - Standalone design connecting to a single router

- Integration with Nexusguard cloud for true-hybrid global mitigation protection

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, i.e. cached bandwidth and requests
- 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
- View load balancer and content caching settings
- Upload SSL certificate for website protection
- Manage DNS resource records

Partner Portal

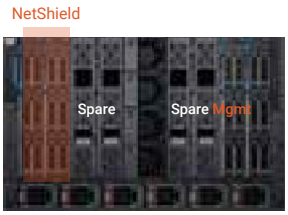
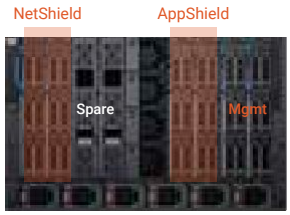
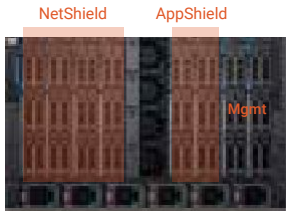
The Partner Portal is designed for the CSP partner, offering granular visibility into the core network and customer networks under protection.

- 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, audit and DNS 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

	MX7000-100G-CP	MX7000-40G/100G	MX7000-200G
			
Hardware			
Power Supply	AC: 3 +1 3000-watt redundant power supplies; 100-240 V AC, 16 AMP. Mx7000 end is IEC C21 connector, PDU end is IEC C20 connector or equivalent.		
Power Requirements	Peak power: 3015 Watts	Peak power: 4195 Watts	Peak power: 5375 Watts
Power Connectors	C22 AC power connector; and one C21/C20 power cable which must be connected to the C22 plug corresponding to each populated PSU.		

Connector	Appliance Inlet	Max Current	Max Pin Temp (°C)
C19 (F)	C20 (M)	16A	70
C21 (F)	C22 (M)	16A	155

Dimensions	Chassis: 7U rack height, Weight: 135 Kg (Min) 183 Kg (Max), Depth: 812 mm, Width: 482 mm, Width: 445 mm (bezel), Height: 307.4 m		
Power Supply	**Uplink:** 2 x 100GbE QSFP28 or 2 x 40GbE QSFP+ or 8 x 10GbE SFP+ or 4 x 10GbE (RJ45) **Management:** 2 x 10Gbe RJ45 (Management)		
Mitigation Engines	2 x NetShield	2 x NetShield 2 x AppShield	4 x NetShield 2 x AppShield
Mitigation Capacity	100Gbps	100Gbps	200Gbps
Environmental	Operating temperature: 10°C (50°F) to 35°C (95°F)		
Reliability	MTBF 33,900 hours	MTBF 22,700 hours	MTBF 17,000 hours
Bypass (partial failure)	Failover to active server		
Bypass (total failure)	Failover to cloud		
Deployment			
Deployment Models	Application Protection: Proxy Mode Origin Protection: Routed Mode DNS Protection: Hosting & Proxy Mode Cleanpipe: Offramp Mode		
Block Actions	Blacklisting/whitelisting; request/IP blocking; rate limiting; challenge/response authentication; HTTP redirection; auto/manual-blackholing		
Types of Attacks Defended	Bogons, CHARGEN, Martian Address, LAND attack, IP Flood, IP Fragmentation, attack, CLDAP amplification attack, DNS amplification attack, DNS attack, HTTP flood, HTTPS flood, ICMP flood, LAND attack, Memcached UDP amplification attack, NTP amplification attack, SIP flood attack, SNMP amplification attack, SSDP amplification attack, SYN flood, TCP flood, TCP Fragmentation, TCP SYN MSS, TCP SYN flood, TCP ACK attack, TCP request and response floods, TCP out-of-state flood, UDP flood, Nuke, multi-vector attacks, zero-day attacks, OWASP Top 10 Threats.		

Performance Specification

	1 x Server	MX7000- 100G-CP	MX7000- 100G	MX7000- 200G
New connection rate - HTTPS*	Clean - 13 kcps Attack - 27 kcps	N/A	Clean - 26 kcps Attack - 54 kcps	Clean - 26 kcps Attack - 54 kcps
New connection rate - HTTP/2*	Clean - 16 kcps Attack - 37 kcps	N/A	Clean - 32 kcps Attack - 74 kcps	Clean - 32 kcps Attack - 74 kcps
New connection rate - HTTP*	Clean - 35 kcps Attack - 92 kcps	N/A	Clean - 70 kcps Attack - 184 kcps	Clean - 70 kcps Attack - 184 kcps
L3 forwarding rate in pps - NetShield	72 Mpps	144 Mpps	144 Mpps	288 Mpps
L3 forwarding rate in bps - NetShield	50 Gbps	100 Gbps	100 Gbps	200 Gbps
DP/L7 forwarding rate in pps*	1 Mpps	N/A	2 Mpps	1 Mpps
DP/L7 forwarding rate in bps*	0.5 Gbps	N/A	1 Gbps	1 Gbps
DNS query per sec*	0.5M	N/A	1M	1M
Concurrent connections*	3M	N/A	6M	3M
AP/L7 forwarding rate in bps - AppShield with cache*	8 Gbps	N/A	16 Gbps	16 Gbps
AP/L7 forwarding rate in bps - AppShield w/o cache*	6 Gbps	N/A	12 Gbps	12 Gbps

* Note: AP AppShield & DP name server share the same server blade on Bastions server MX7000. The forwarding rate on AppShield is tested with no traffic loading on the name server, and the forwarding rate on the name server is tested with no traffic loading on AppShield.

Deployment Specification (per Bastions server MX7000)

	MX7000- 100G-CP	MX7000- 100G	MX7000- 200G
Design	Standalone / HA	Standalone / HA	Standalone / HA
Reference architecture	MX7000-200G	MX7000-100G / MX7000-100G-CP	
AppShield + DNS engine	2	2	2
NetShield engine	4	2	2
Network interface options	100 Gbps (QSFP28) 40 Gbps (QSFP+) 40 Gbps (QSFP+ to 4x SFP+) 10 Gbps (RJ-45) x4		
L3 data rate	200G	100G	100G
L3 packet rate	288Mbps	144Mbps	144Mbps
Uplink routers - must support PBR/VRF & BGP	1 ~ 4		
No. of ASN supported	1		
BGP	eBGP or iBGP		
Max no. of flow data source - soft limit	5		
Flow protocol support	Netflow v5 / 9 IPFIX sflow v2 / 4 / 5 Netstream v5 / 8 / 9		
Flow data rate	90 kfps		
Sampling rate	< 1:1000		
No flow data alert	Supported via Notifier app		
OOB interface & bandwidth requirement	Recommended - 1 Gbps Min - 100 Mbps Note: Congested link or link failure → lost in management control & auto-mitigation functionality		

NEXUSGUARD®

Nexusguard is the only managed security service provider (MSSP) specialized in combating DDoS attacks, leveraging its purpose-built, high-performance scrubbing centers and a growing partner network around the world-collectively equipped with over 2.24Tbps of mitigation capacity. The global scrubbing network is highly scalable and fully redundant, standing ready any time to mitigate DDoS attacks.

We employ remote detection and multi-layered mitigation engines to identify, mitigate and analyze DDoS attacks on websites, applications, networks and DNS servers. This ensures communications service providers (CSPs), large enterprises and organizations can maintain uninterrupted access to networks, websites and applications, even when they are the target of a massive DDoS attack.

contact@nexusguard.com
www.nexusguard.com

Copyright © 2022 Nexusguard Limited. All rights reserved | 20221028-EN-A4