Datasheet

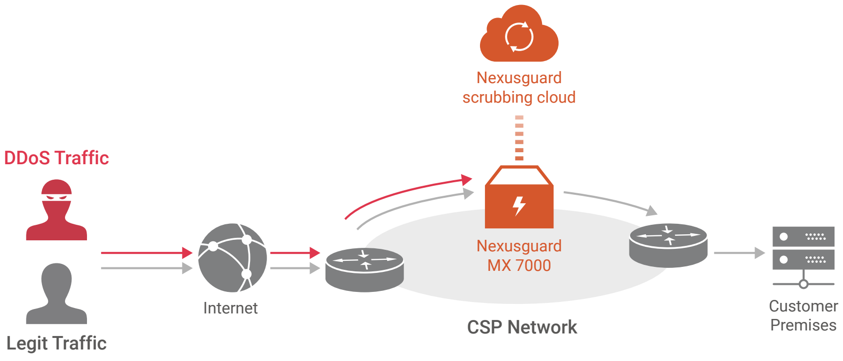
Nexusguard
MX7000 Mitigation Platform

MX7000-100G-CP | MX7000-40G/100G/200G

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

The platform is purpose-built by bringing Nexusguard's proprietary technologies, tools and expertise culminated over 10 years of DDoS fighting experience, into a high-performance modular chassis manufactured by one of the world's largest and leading technological companies.

Nexusguard MX7000 Mitigation Platform 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 threatens to overwhelm local capacities, Nexusguard's globally distributed scrubbing kicks-in, 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.

NEXUSGUARD®

Detection & Mitigation

Nexusguard's all-in-one DDoS detection and mitigation platform defends websites, applications, APIs, infrastructure and DNS servers against DDoS attacks of all types and complexities.

- ### Anomaly detection

  Used to identify the unusual traffic patterns that do not conform to expected behavior. The detection of malicious traffic also prevents against the zero-day attacks.

- ### Blacklisting/Whitelisting

  Blacklisting blocks traffic to prevent flood attacks coming from blacklisted IP resources, while whitelisting lets in legitimate traffic from pre-approved source IPs.

- ### Deep packet inspection

  Used to look within the application payload of a packet or traffic stream and make decisions based on the content of that payload. It enhances the capability to prevent the exploitation of IoT devices to mount DDoS attacks.

- ### Session timeout

  Used to kill idle or semi-open connections that fill up the connection tables in servers. It defends against low and slow attacks that target application or server resources.

- ### Rate limiting

  Used to control the amount of incoming and outgoing traffic to or from a network. This is enforced by setting a traffic threshold for allowing only the desired bandwidth of traffic.

- ### Caching and load balancing

  Used to optimize the network performance and improve latency. This serves as the last line of defence to absorb the final bit of traffic that has slipped the cracks, if any.

Detection

The MX7000 Mitigation Platform continuously monitors and analyzes large pools of IPs and application requests in real time. Using behavioral or threshold based detection mechanisms, CSPs are notified of any occurence of abnormalities and attack events. The detection engine is comprised of flow-based traffic analyzer and collector that supports NetFlow, SFlow, IPFIX and NetStream.

With a low false positive rate, the engine is capable of detecting a large variety of L3/4 attacks such as: TCP based data packets e.g. TCP SYN, TCP ACK, TCP RST, TCP Invalid, TCP Fragment); UDP based data packets e.g. DNS requests and responses, NTP data packets, SNMP data packets, SSDP data packets; ICMP based data packets e.g. ICMP Invalid, ICMP Fragment; IP based data packets e.g. IP Fragment, IP Bogons.

But unlike network-layer attacks, application-based attacks are aimed at Layer 7 of the network stack, which are harder to detect because they look like legitimate HTTP, DNS, SNMP and SYN stateful sessions and typically consume modest bandwidth. The built-in detection engine, including Web Application Firewall (WAF), is also designed to efficiently detect Layer 7 attacks while minimizing operational overhead.

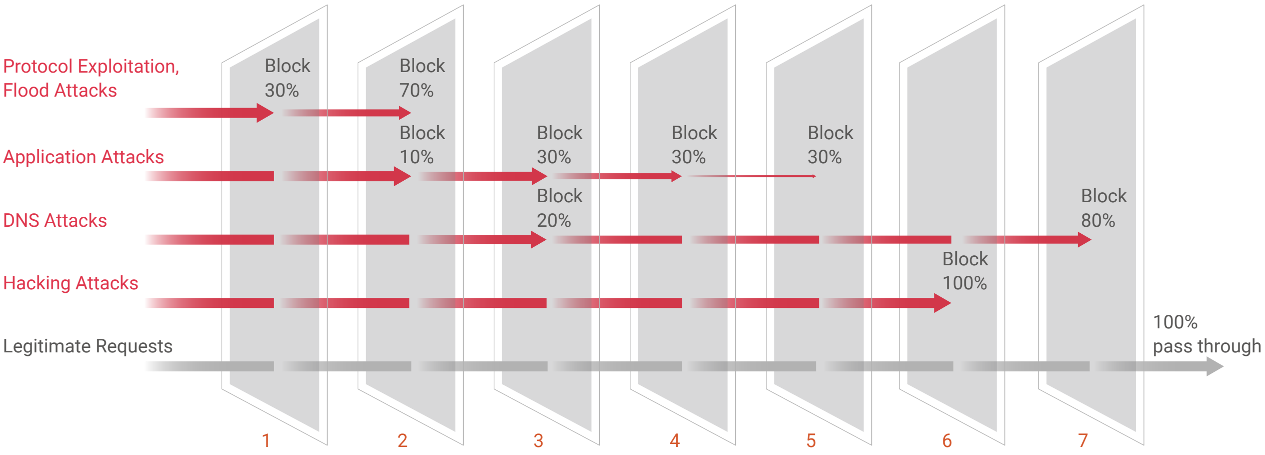
Smart Baselining

Smart Baselining utilizes deep learning to observe and analyze the pattern of traffic to a Site over time, and then recommends upper and lower detection threshold values that adapt to the prevailing traffic pattern. The recommendation provides a reliable reference that helps operators define threshold values for the first time and fine tuning on an ongoing basis.

Mitigation

The mitigation platform has a built-in filtering system to identify and mitigate attacks while keeping the user experience intact. The CSP's local scrubbing facility will work in tandem with Nexusguard's global scrubbing centers to mitigate attacks globally.

Dynamic DDoS attacks require comprehensive, meticulous detection and action in real time. Nexusguard subjects DDoS attack traffic through multiple layers of inspection to deliver fast, clean traffic. Nexusguard's multi-filtering strategy is as follows:



Layer 1 Hi-speed Border Filtering
Layer 2 Protocol Verification Deep Packet Inspection
Layer 3 Adaptive Filtering
Layer 4 Application Level Filtering
Layer 5 Flexible Content Filtering
Layer 6 WAF
Layer 7 Caching & Compression Acceleration & Optimization

Hi-Speed Border Filtering

At Nexusguard's border, traffic is filtered for bandwidth flood using wire speed Access Control Lists. Nexusguard also filters out at this layer bogus IP addresses and infected hosts according to a continually updated database.

Protocol Verification

To mitigate spoofed attacks, Nexusguard utilizes challenge-response algorithms like TCP SYN cookie and TCP SYN authentication to distinguish between spoofed and legitimate traffic.

Adaptive Filtering

Nexusguard's anomaly recognition engine employs machine learning to understand normal baselines. Malicious activities that induce anomalies in networks traffic can then be identified and filtered.

- ### Application-Level Filtering

  To further mitigate application level attacks, HTTP attacks, and Zero-Day attacks, Nexusguard can enforce intelligent HTTP Malformed filtering to ensure the validity of HTTP transactions. Nexusguard can also limit the number of connections or requests to specific objects.

- ### Flexible Content Filtering

  Nexusguard's DDoS mitigation system continuously monitors application traffic for unusual patterns and behaviours. Using its proprietary pattern recognition and analysis system, Nexusguard deters morphing HTTP Flood attacks by adapting flexible content filters to quickly counter even covert attacks.

- ### Web Application Firewall (WAF)

  The Nexusguard WAF engine protects DDoS attack against the OWASP Top 10 common vulnerabilities.

- ### Caching & Compression

  Implement content caching and acceleration to optimize web application performance and user experience.

Web Application Firewall

Taking references from OWASP ModSecurity Core Rule Set, MX7000's WAF module is completely designed from ground-up with service providers in mind. While maintaining multi-tenancy and ease of customer management, it protects service provider's end customer web applications from attacks and exploits including Top 10 threats outlined by the Open Web Application Security Project (OWASP); prevents sensitive information leakage; and controls when and where your applications are accessed by analyzing the content of HTTP and HTTPS traffic targeting applications and making applications for PCI-compliance a breeze.

Centrally managed by Nexusguard SOC team and security experts together with our CSP partners, partners leverage the collective intelligence of a diverse range of customer use cases to constantly update the rule-set to address latest threats and expand its capacity whenever needed.

The hybrid WAF can be deployed in minutes, supports SSL/TLS, requires no additional hardware and software, and incurs very low operational costs for both the CSP and the end customer to maintain. Detailed security event logs and traffic summary information displayed on the Partner/Customer Portal allow the security team to gain visibility and insight into WAF and traffic analytics through continuous monitoring, risk assessments and remediation paths.

Content Caching & Acceleration

As part of the high performance platform's ability to handle the most powerful attacks, the MX7000 mitigation platform employ static and dynamic content caching and acceleration to serve static and event-driven content on behalf of the CSP's customers, both locally as well as via the Nexusguard Cloud. The platform is able to identify frequently accessed content by comparing content from the server to the content that is already cached. If content is requested repeatedly, it will be served from the cache of Nexusguard's scrubbing centers. This reduces the bandwidth required between the CSP's origin server and the scrubbing center while accelerating content delivery to the end-user and reducing the bandwidth cost of the CSP.

This versatility ensures speedy delivery of previously uncacheable dynamic content that is now heavily used by some types of content providers, such as e-commerce/travel, news/sports, local/weather, advertising, and social media.

Features

- **Static content caching, i.e. HTML, images, Javascript, etc.**
- **Event-driven content caching, i.e. API and AJAX requests**
- **Customized HTML-based dynamic content caching**
- **Custom caching rules, i.e. URL specific and extension specific; option to purge cache**
- **Client-side caching**
- **Session reuse optimization**
- **Ability to propagate cache-related HTTP headers from the origin to end-users**

Load Balancing

Traffic and user load-balancing is an integral part of handling not just attack traffic but legitimate peace time traffic as well. The Nexusguard MX7000's load balancing module functions as a on-premise and cloud-based alternative to traditional on-premise, appliance-based load balancers, thereby helping CSPs and their customers cut relevant capital and operating expenses. Our cloud-based load balancers can be integrated with multiple servers within the same data center, or multiple data centers in different locations on a global scale.

Server load balancing

Nexusguard's cloud-based load balancers automatically balance traffic across multiple web servers within a data center based on the load while ignoring non-responsive servers from the pool. Various load balancing methods are supported, including performance, failover and ip-hash. The default load-balancing methods are session persistent and so the requests from the same client will always be directed to the same server unless this server is unavailable.

DNS SmartRoute (DSR)

DNS SmartRoute (DSR) allows for inbound raw traffic to be distributed across Nexusguard's scrubbing centers based on the selected load balancing rules. This is achieved by distributing DNS name resolution requests based on geolocation, ASN/IP prefix, and/or weighted via ratio allocation or other customized rules.

CleanPipe

Internet CleanPipe is an essential DDoS mitigation solution usually delivered both for online businesses and mission critical websites that require real-time protection against volumetric DDoS attacks. It is most commonly delivered as a value-add on top of existing or new connectivity offerings such as IP Transit or Direct Internet Access Services. It can also be offered as VAS in small-office based internet connectivity services such as broadband connections. In order for one to deliver a CleanPipe to its customer, it usually either has in-house capabilities or it could also be delivered via third party MSSPs although this would then incur a delay that is required to perform redirection of the traffic.

MX7000's CleanPipe module is designed for CSPs to immediately expand or complement their existing product offerings by integrating managed enterprise-grade DDoS mitigation services, bringing together best-in-class technology, DDoS experts, and the SLA commitment for the best attack detection, notification and mitigation response times to deliver a truly differentiated cleanpipe service that sets our CSP partners ahead of its competition.

Gain competitive advantage

Ensuring a clean, reliable, pipe for customers is a win-win situation. Optimal network performance adds value to an internet service, and is a powerful competitive differentiator. DDoS protection is a major selling point, and a “no-brainer” for prospective customers. Carriers that capitalize on modern DDoS technology can gain a strong competitive advantage and build loyalty among their customers.

Explore new revenue streams

Customers expect – and are willing to pay for – effective DDoS protection. Therefore, eliminating the DDoS threat at the edge of the network not only protects the CSP and its customers, it provides an opportunity for CSPs to generate incremental revenue. CSPs have a golden opportunity to create valuable new revenue streams by incorporating advanced DDoS mitigation into their service offerings; by doing so they can recoup the cost of their DDoS solution within months.

3-tiered multi-tenant customer management

Designed for multi-tenant environments, Nexusguard Portal is a premier 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” platform for managing DDoS detection and mitigation policies and obtaining actionable intelligence.

There are three tiers of Portals:

- **Customer Portal (e.g. Region A-User 1)**
- **Provider Portal (e.g. CSP Regional A)**
- **Federated Portal (e.g. CSP Global)**

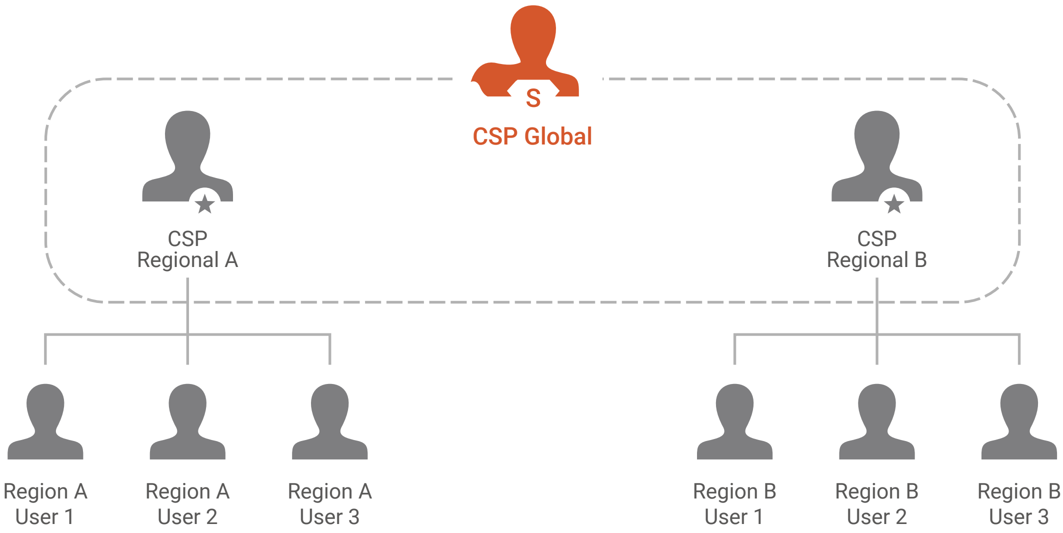


Figure 1. The hierarchical structure of Nexusguard portals

Customer Portal

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

- **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 reports**
- **Configure security policies**
- **Configure load balancer and content caching settings**

Provider Portal

The Provider Portal is designed for the (regional) CSP partner, offering granular visibility into the core network and customer (tenant) networks under protection.

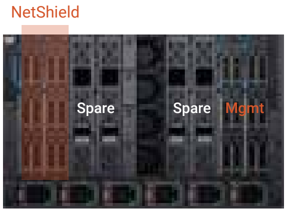
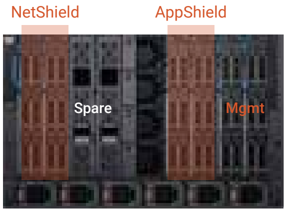
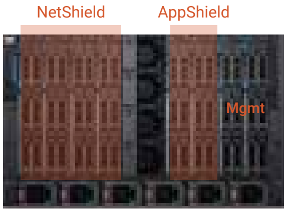
- **Access to all customer accounts under protection**
- **Configure customer policy settings and mitigation templates**
- **Monitor aggregate network traffic, i.e. raw and clean bandwidth, in real time, event/attack details and mitigation results in the integrated dashboard**
- **View Visitor/Threat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

Federated Portal

Equivalent to the “super admin” role, the Federated Portal gives the top-level manager (e.g. the global office of a CSP with multiple regional CSPs operating separately) access to all Provider Portal accounts as well as all Customer Portal accounts down the hierarchy.

Structured like the Provider Portal, the Federated Portal features an integrated dashboard that provides granular network traffic visibility, event summary, etc. The Federated portal provides the ability to implement an over-arching visibility across multiple networks or business systems in environments that requires so.

Specifications

	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
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		
Network Interfaces	**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)		
Bypass (partial failure)	Failover to active server		
Bypass (total failure)	Failover to cloud		
Mitigation			
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.		

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 communication 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