Nokia 7750 Defender Mitigation System DMS-1-24D

Release 25.7

The Nokia 7750 Defender Mitigation System (7750 DMS-1-24D) is a compact, purpose-built Distributed Denial of Service (DDoS) mitigation system that performs high-scale, granular removal of malicious IP traffic with unprecedented efficiency.

The 7750 Defender Mitigation System delivers a new benchmark for dedicated DDoS mitigation with its high performance with speed, power efficiency, and flexible capability. It has been designed to address the next-generation requirements for DDoS security and automation capabilities needed for the 5G, IoT and cloud era.

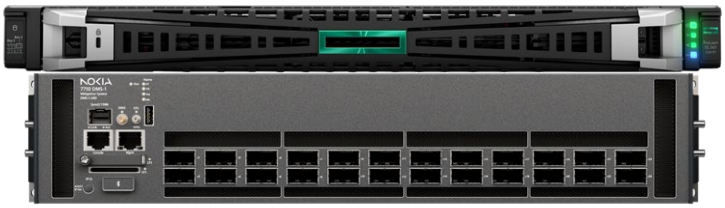
With Nokia's continuous focus on design innovation and sustainability, the 7750 DMS-1-24D is a cornerstone for advanced, network-optimized DDoS mitigation for years to come.

Features

- Dedicated mitigation platform - for deployments where DDoS security enforcement needs to be managed separately
- Advanced processing capability with leading scalability up to 2.8 Tb/s
- Deployment: Co-located with network edge(s) or in scrubbing center(s)
- 3RU form factor
- AC or DC variants
- 24 x 800G QFSP-DD ports
  (20 ports for network connectivity)

Benefits

- Application-layer, stateful and volumetric DDoS attack mitigation
- Highest scrubbing capacity at the best cost point in the industry ($/Gb/s)
- Flexible NetEng/SecOps ownership/management
- Full integration with the network-based mitigation deployments
- Scale-out, high-availability architecture
- Flexible licensing
  (from 100 Gb/s up to 2.8 Tb/s per system)



7750 DMS-1-24D

Functional overview

The 7750 DMS-1-24D is a new addition to the Nokia portfolio – a purpose-built product for DDoS mitigation. As such, the 7750 Defender Mitigation System has an operating system and configuration optimized for next-generation DDoS mitigation. It leverages the full scale and programmability of the Nokia FP5 silicon to mitigate DDoS attacks in the most effective and cost-effective manner. With the addition of the Advanced Countermeasures Engine (ACE), the 7750 Defender Mitigation System can mitigate application-layer and stateful DDoS attacks.

The 7750 Defender Mitigation System is fully controlled and managed by Deepfield Defender.

The primary mode of operation for the 7750 DMS-1-24D is offramp (traffic diversion). After the malicious traffic is detected by Deepfield Defender, it is diverted from the IP network to the 7750 Defender Mitigation System for cleaning (scrubbing). The 7750 DMS-1-24D removes the bad (dirty) traffic and re-injects the good (clean) traffic back into the network.

With the unprecedented growth of DDoS threats and attacks, service providers and operators are challenged to maintain network operations without the downtime of their services or degraded customer experience of their subscribers. The 7750 DMS-1-24D addresses the imperatives of next-generation DDoS security. Its advanced capabilities make it a cornerstone of a secure, self-defending network, enabling operators to build scalable, secure, automated and efficient IP networks with superior return on investment.

Nokia Deepfield DDoS security solution

The Nokia approach to DDoS security is based on combining the power of big data analytics with the advanced processing capabilities of the network (routers and/or DMS) to achieve efficient, scalable and cost-effective DDoS protection directly at the network edge. Nokia Deepfield Defender is a software application that provides fast and accurate DDoS detection and facilitates agile mitigation of all types of DDoS attacks in the network.

Defender is a component of the Deepfield portfolio of IP network intelligence, analytics and security applications, and it leverages Deepfield Secure Genome® to detect and mitigate DDoS threats across the entire network.

Deepfield Secure Genome is a Nokia-proprietary data feed containing up-to-date information about the global security context of the internet. Defender correlates the information obtained from the network with the Secure Genome data feed and acts as the “brain” behind the most comprehensive multi-layer security framework to protect against DDoS attacks of any type, coming from any origin and across any network edge.

DDoS mitigation

The 7750 DMS-1-24D is powered by the FP5 silicon, allowing massive scalability with uncompromised performance. Driven by Nokia Deepfield Defender and Secure Genome, the 7750 DMS mitigates DDoS attacks at scale and with high precision, acting as a next-generation dedicated mitigation system.

Mitigation effectiveness is continuously monitored and tuned using telemetry from the 7750 DMS-1-24D. With quick and accurate DDoS detection and automated mitigation workflows created in Deepfield Defender, the 7750 DMS-1-24D can perform hardware-assisted mitigation of sophisticated, multi-vector, terabit-scale attacks in seconds.

Advanced countermeasures

With the Advanced Countermeasures Engine (ACE), the mitigation capabilities of the 7750 DMS-1-24D extend to support application-layer and stateful countermeasures.

ACE runs on the dedicated Nokia 7750 SR Extended Services Appliance (ESA 400G), optimized for advanced DDoS mitigation.

Advanced DDoS countermeasures enabled by ACE are an integral part of the 7750 Defender Mitigation System's functionality. Deepfield Defender configures and manages all DDoS countermeasures, including advanced DDoS countermeasures.

For more details on ESA 400G hardware specifications, refer to the Nokia 7750 SR Extended Services Appliance (ESA) datasheet.

Typical deployment scenarios

The 7750 DMS-1-24D can be deployed:

- As a next-generation DDoS scrubber, when demands for scalability, advanced countermeasures, higher throughput, better cost efficiency and green factor (power efficiency) disqualify or question further deployment and investment in legacy-based scrubbing systems;
- When the existing IP routers deployed in the network have a limited scale of security-based filtering (or generally, limited scale of ACL filtering);
- When networking teams in charge of DDoS security are concerned about the performance of their IP routers and want to keep the implementation of security policies on a separate platform, or when there is a requirement for a dedicated security enforcement platform;
- When the organizational structure of networking and security teams mandates full ownership and control over security planning and enforcement by the security organization.

The 7750 Defender Mitigation System can find its place in various network environments: from being deployed with advanced IP network elements with strong edge-mitigation capabilities, such as Nokia Service Routers, to being the exclusive point of DDoS mitigation.

Platform overview

The 7750 DMS-1-24D delivers power-efficient, hardware-assisted mitigation performance for the demanding role of the next-generation DDoS mitigation platform.

The compact 7750 Defender Mitigation System is available as 7750 DMS-1-24D, with up to 2.8 Tb/s full duplex capacity and comes with 24 QFSP DD ports capable of 800G on a per-connector basis (20 ports for network connectivity).

At the heart of the 7750 DMS-1-24D is the Nokia FP5 silicon—an essential element for high-performance packet processing. Leveraging a fully programmable network processor (NP) architecture, the 7750 DMS-1-24D delivers a deterministic performance, scalability and power consumption.

Its universal 800G QSFP-DD connectors can adapt to various speeds, enabling high-density 10GE, 25GE, 50GE, 100GE, 200GE, 400GE and 800GE networking environments. All 800G QSFP-DD cages support a variety of compatible optics, including QSFP+ and QSFP28. Various breakout options are available.

Flexible capabilities

The 7750 DMS-1-24D with ACE incorporates a layered approach to mitigating DDoS attacks with agility and precision. Its unique architecture, with network-based processing for volumetric DDoS attacks and CPU-based processing for stateful and application-layer DDoS attacks, provides the best of both worlds: line rate protection from high-volume flood attacks and flexible mitigation techniques for stateful and application-layer attacks.

Network processor-based architecture

Nokia network processors, such as FP5, offer the highest degree of flexibility and programmability in the industry. With a fully programmable data path and zero hard-coded logic, the data path can implement advanced mitigation mechanisms as Nokia Deepfield Defender dynamically compiles them and adapts to new trends in DDoS attacks

without replacing the hardware.

General compute-based architecture

General compute processors are ideal for quickly adapting to the constantly changing landscape of stateful and application DDoS attacks. By leveraging a general-purpose CPU-based architecture for advanced DDoS countermeasures, the 7750 DMS-1-24D with ACE provides easy-to-update protections that don't require changes to silicon as complex attacks morph.

Pay-as-you-grow licensing

The flexible pay-as-you-grow licensing model for additional DDoS processing and mitigation capacity allows in-service growth and scaling according to evolving needs.

Scaling

Nokia's feature-rich 64-bit operating system addresses the most stringent DDoS processing requirements. The 7750 DMS-1-24D supports a massive scale of hardware-assisted mitigation of high bandwidth and/or high packet rate DDoS attacks to achieve wire-speed mitigation performance. The 7750 DMS supports advanced push-based telemetry models to stream flow-level data and insights in near-real time for network assurance and DDoS security.

Hardware overview

The 7750 DMS-1-24D is available in a compact form factor with 800G QSFP-DD connectors, an internal multi-core CPU supporting a simplex control plane, and front-to-back airflow with an optional air filter kit.

The system ships with two redundant power supplies and three redundant fan trays.

High availability

The 7750 DMS-1-24D leverages the strong background of the 7750 family design in the data plane and software stack. It supports link aggregation group (LAG), redundant IP interfaces, equal-cost multipath (ECMP) and graceful restart (GR) (e.g., for BGP).

The platform is designed for a network-based high-availability model, starting with a dual-node deployment, in 1+1 Active/Active or Active/Standby, and allowing for horizontal growth to support the increased mitigation needs of the network, in which case multiple 7750 DMS units can be clustered as a DMS group.

Multiple DMS groups can be deployed in the network for several reasons, such as:

- Geographical distribution
- Scrubbing center redundancy
- Service-based deployment.

Technical specifications

Table 1. Hardware specifications for the 7750 DMS-1-24D system

7750 DMS-1-24D	
System architecture	Centralized, fixed connectors, non-redundant control
System capacity (full duplex)	from 100 Gb/s up to 2.8 Tb/s
Connectors	24 x 800G QSFP-DD (20 ports for network connectivity)
Pre-classification and pre-buffering	10.8 million 64B packet micro-buffer
Buffering	32GB
Hot-swappable modules	2 PSUs, 3 fan trays
Control ports	Front: Optical SyncE/1588, console, management, 1PPS, dual-band GNSS, Bluetooth, SD cards, and USB ports Rear: Alarms, OES and BITs ports
Cooling	Front to back
Dimensions (with air filter kit)	• Height: 8.81 cm (3.47 in), 2RU • Width: 48.26 cm (19 in) • Depth: 59.20cm (23.3 in)
Weight	Loaded: 20.89 kg (46.05 lbs); excludes optics
Power	DC power • DC input: -40 V to -72 V, 80A max per feed • Power feed redundancy • 1+1 PSU redundancy AC power • AC input: 180V AC to 264 V AC, 50 Hz/60 Hz; 20A max per feed • 1+1 PSU redundancy
Port density Interface speed 800G 400G 100G 10G	 Line rate port count (max) 3 7 28 96

Advanced Countermeasures Engine	
System details	• 1RU rackmount server (HPE DL360 Gen 11 based) • Two Intel Xeon Gold 6438N Sapphire Rapids processors (CPU0 and CPU1), 32 cores each (2.0 GHz, 205W) • Dual AC or DC variants are available • 512 GB memory • NIC: Two 100 Gb/s 2-port QSFP56 • One to four ports of up to 100 Gb/s processing throughput each (up to 400 Gb/s total)
Power supply	• AC: 1000 W, redundant (100 to 120 V, 50/60 Hz, 8.8 A max; 200 to 240 V, 50/60 Hz, 4 A max) • DC: 1600 W, redundant (-40 V/-72 V, 22 A max (per PSU))
Cooling	Front to back
Power consumption	• Loads simulated by HPE Power Advisor • 30% load: 400 W • 50% load (single CPU in use): 550 W • 100% load: 890 W
Dimensions and weight	• Height: 4.29 cm (1.69 in) • Width: 43.46 cm (17.11 in) • Rack depth: 75.31 cm (29.65 in) • Weight: 19.1 kg (42.1 lbs)

Table 2. 7750 DMS-1-24 DDoS detection and mitigation specifications

Deployment modes	Diversion/re-injection
Attacks/threats	• **Reflection and amplification flood attacks:** TCP, UDP, ICMP, QOTD, CHARGEN, DNS, TFTP, SunRPC, NTP, SNMP, NetBIOS, cLDAP, SLP, RIPv1, L2TP, SSDP, ARD, WSD, mDNS, CoAP, P2P-Torrent, Memcached and additional emerging misused protocols or malicious port combinations • **Fragmentation attacks:** Fragments as part of amplification attacks as well as standalone • **TCP stack and flood attacks:** SYN, ACK, RST, SYN-ACK, PSH-ACK, other combinations of flags, null flags, Xmas tree • **Spoofed source attacks:** Bogon, random source • **Botnet attacks:** Attack traffic originating from bots, independent from the attack type, including application-layer attacks • **DNS NXDOMAIN attacks:** non-existent domain attacks, also known as DNS water torture attacks • **TCP, HTTP, TLS low-and-slow attacks:** Attacks that send low bandwidth intermittent packets attempting to cause slow state resource exhaustion • **HTTP floods:** Attacks that flood a web or application server with legitimate requests in an attempt to exhaust the server's resources • **Malformed DNS and HTTP attacks:** Attacks that send large numbers of intentionally misconfigured packets to a server attempting to consume its processing resources • **TLS negotiation attacks:** Attacks that attempt to abuse the TLS handshake to exhaust server resources • **VOIP attacks:** Floods or abuse of Session Initiation Protocol (SIP) intended to overwhelm VOIP servers.
DDoS countermeasures	• **Allow and Block Lists:** Bypass traffic filtering for trusted IP addresses and/or defend against traffic from known malicious IP addresses. • **Invalid Packet Defense:** Defend against malformed packets with invalid packet lengths, invalid TCP flag combinations, or IP header options. • **Custom Pre-Filters:** Act on packets with characteristics specified by DFMatch expressions before other filters are applied. • **UDP Amplification Defense:** Defend against any UDP traffic produced by amplification or reflection techniques. • **TCP Reflection Defense:** Defend against SYN-ACK packets produced by reflection techniques. • **Botnet Defense:** Defend against botnet-originated traffic based on continuously updated knowledge of bots and suspicious hosts. • **Spoofing Defense:** Defend against traffic with anomalous patterns and highly improbable headers or payloads. • **UDP Flood Defense:** Defend against UDP traffic with suspicious port combinations or irrelevant QUIC traffic. • **TCP Flood Defense:** Defend against TCP traffic with suspicious port combinations and anomalous packet length or TTL distribution. • **GRE Flood Defense:** Defend against GRE traffic with anomalous packet length distribution while allowing safe traffic from cloud DDoS protection providers. • **IP-in-IP Flood Defense:** Defend against floods of IPv4-in-IPv4 encapsulated traffic. • **ICMP Flood Defense:** Defend against ICMP traffic exhibiting flood attack patterns and implement advanced protections when using a 7750 DMS. • **Topology Misuse Defense:** Defend against packets with suspicious characteristics based on source IP addresses and Deepfield Defender's knowledge of network topology. • **Custom Post-Filters:** Act on traffic with characteristics specified by DFMatch expressions after other filtering and before final rate limiting. • **TCP SYN Baseline:** Rate-limit SYN packets based on source-specific peace-time baselines as a final recourse. • **IP Location Defense:** Defend against traffic based on source geolocation. • **Trusted Nameserver Allow List:**. Allow traffic from trusted upstream DNS nameservers (root, gTLD/sTLD, major ccTLD, and major authoritative nameservers). NETCONF only. • **DNS Server Protection:** Protect authoritative DNS servers with protocol validation and optional rate limiting, domain name filtering, and source authentication. • **HTTP Server Protection:** Protect web servers with protocol validation, optional rate limiting, and optional TCP protections on specified ports.

DDoS countermeasures (cont.)	• **TCP Server Protection:** Protect servers using TCP at Layer 4 with protocol validation, optional rate limiting, and source authentication for specified ports. • **TLS Server Protection:** Protect servers leveraging TLS encryption with protocol validation, optional rate limiting, and source authentication for specified ports. • **SIP Server Protection:** Protect servers using SIP with protocol validation and optional rate limiting for specified ports. • **Protocol Baseline:** Rate limit traffic by protocol based on peacetime baselines as a final recourse.

Deepfield software release 25.7. This is a non-exhaustive list; new vectors and countermeasures are continuously added via Secure Genome.

Feature and protocol support highlights

Feature and protocol support within the 7750 DMS-1-24D includes, but is not limited to, the following:

IP routing features

- IP unicast routing:
  - Multiprotocol Border Gateway Protocol (MBGP)
  - Interior/Exterior Border Gateway Protocol (iBGP/eBGP)
  - Unicast Reverse Path Forwarding (uRPF)
  - Comprehensive control plane protection features for security – IPv4 and IPv6 feature parity
  - IPv4 and IPv6 feature parity
- Control interfaces
  - Supports control interfaces such as CLI and NETCONF

System features

- Extensive fault and performance monitoring.
- Operations, Administration and Maintenance (OAM) Includes:
  - Bidirectional Forwarding Detection (BFD), including Seamless BFD
  - Cflowd
- Timing:
  - Network Time Protocol (NTP)
  - BITS ports (T1, E1, 2M)
  - 1PPS
- High availability:
  - Redundant power supply units and/or power feed redundancy
  - Redundant cooling fan units
  - DMS group clustering based on IP anycast for dirty traffic offramp

Management features

- Managed by Deepfield Defender
- Model-driven management of configuration and state through the MD-CLI, NETCONF and gRPC/gNMI using YANG models; streaming telemetry through gRPC/gNMI subscriptions; operations through NETCONF and gRPC/gNOI
- Read-only SNMP management support, including monitoring and traps
- Comprehensive network and node management

Standards support

Environmental specifications

- Operating temperature: 5°C to 40°C (41°F to 104°F)
- Operating relative humidity: 5% to 95% non-condensing
- Operating altitude: Up to 3,960 m (13,000 ft); operating temperature range de-rated above 1,829 m (6,000 ft)

Refer to the 7750 DMS-1-24D product and release documentation for details on dimensions, weights, hardware, safety standards, compliance agency certifications and protocol support.

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

650654: CID213483 (July)