

Defending the Realm with Deepfield Defender

José Alberto Nistal

BalticNOG – September 25, 2025

The Nokia logo is centered within a large, stylized circular graphic on the right side of the slide. The graphic consists of two concentric circles: an outer white ring and an inner dark blue circle. The word "NOKIA" is written in white, uppercase, sans-serif font within the dark blue inner circle.

NOKIA

DDoS traffic and attack trends - 2024

DNS

#1 vector
36% of attacks

Botnets

1M active bots
60% of attacks
use < 100 bots

New

Residential Proxy abuse

Leveraging Millions
of residential IP's in
“free” VPN services

Carpet bombing

on the rise
13% to 256+ IPs
2.8% to >1K IPs
Largest: 16K IPs

AI & automation

Driving faster
morphing attacks

Duration

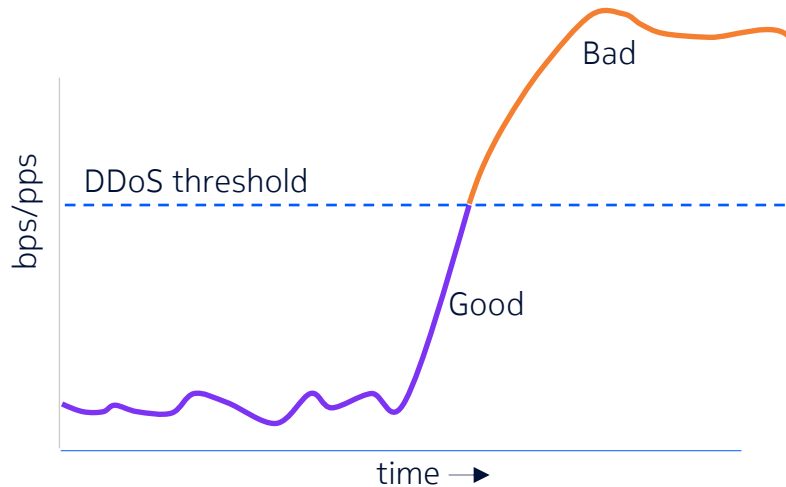
44% lasts
< 5 minutes
But higher
frequency



How do legacy DDoS tools detect DDoS?

Traffic is good... until it isn't

- Other DDoS tools use Flow-based traffic thresholds to trigger DDoS events.
- Traffic is good until it crosses some configured threshold, and then it's suddenly bad.



Ok, so what's the big deal?

1. Flows are only identified as DDoS once an object is configured for detection, thresholds are set, and thresholds are exceeded
2. Operators must maintain thresholds and configuration for every type of DDoS misuse out on the Internet
3. Hard to maintain, very inaccurate

Host Detection	Enabled	Edit Shared Settings
Severity Duration (min for Fast Flood Host alerts)	180 seconds	
Fast Flood Detection	Enabled	
Misuse Type	Trigger Rate	High Severity Rate
chargen Amplification (bps)	250 Mbps	500 Mbps
chargen Amplification (pps)	25 Kpps	50 Kpps
CLDAP Amplification (bps)	250 Mbps	500 Mbps
CLDAP Amplification (pps)	25 Kpps	50 Kpps
DNS	10 Kpps	30 Kpps
DNS Amplification (bps)	250 Mbps	500 Mbps
DNS Amplification (pps)	25 Kpps	50 Kpps
ICMP	5 Kpps	10 Kpps
IP Fragment	25 Kpps	50 Kpps
IP Private	5 Kpps	10 Kpps
IPv4 Protocol 0	5 Kpps	10 Kpps
L2TP (bps)	25 Mbps	50 Mbps
L2TP (pps)	25 Kpps	50 Kpps
mDNS (bps)	25 Mbps	50 Mbps
mDNS (pps)	25 Kpps	50 Kpps
memcached Amplification (bps)	250 Mbps	500 Mbps
memcached Amplification (pps)	25 Kpps	50 Kpps
MS SQL RS Amplification (bps)	250 Mbps	500 Mbps
MS SQL RS Amplification (pps)	25 Kpps	50 Kpps
NetBIOS (bps)	250 Mbps	500 Mbps
NetBIOS (pps)	25 Kpps	50 Kpps
NTP Amplification (bps)	250 Mbps	500 Mbps
NTP Amplification (pps)	25 Kpps	50 Kpps
RIPv1 (bps)	25 Mbps	50 Mbps
RIPv1 (pps)	25 Kpps	50 Kpps
rpcbind (bps)	25 Mbps	50 Mbps
rpcbind (pps)	25 Kpps	50 Kpps
SNMP Amplification (bps)	25 Mbps	50 Mbps
SNMP Amplification (pps)	25 Kpps	50 Kpps
SSDP Amplification (bps)	250 Mbps	500 Mbps
SSDP Amplification (pps)	25 Kpps	50 Kpps
TCP RST	1.5 Kpps	20 Kpps
TCP SYN	1.5 Kpps	20 Kpps
TCP SYN/ACK Amplification (bps)	125 Mbps	150 Mbps
TCP SYN/ACK Amplification (pps)	125 Kpps	150 Kpps
UDP	30 Kpps	400 Kpps

How do you need your DDoS tool to be today?

1

Automated

2

Lightning-fast

3













At scale

1. Automated

The Secure Genome Advantage

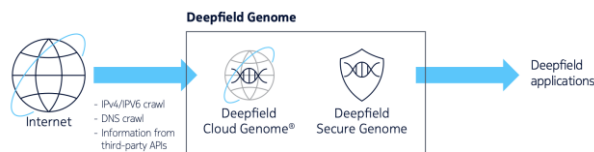
1. Collect & learn every DDoS

From Defender customers, GDTA sharing, public forums, CVE notes etc. Learn attacks' characteristics & develop countermeasures.

GID	Attack	Src IP	Dest IP	Rate	Pps	Filters	False Positive	Status
3	 SYN Flood Specified UDP Flood with most TTL outside of expected range. All traffic with 1 byte protocol and invalid checksum may be mitigated if DMZ supported TTL and/or transport.	43.203.331	1	7.2 Gbps	31.2 Gbps	1	0%	
10	 ACK Flood TCP ACK Flood with most TTL outside of expected range. All TCP and IP distribution equally parse done. All TCP checks are enabled. Mostly used for DoS attacks. We used to be invariant to block in addition to TTL and TCP baselines.	91.705.664	1	9.4 Gbps	28.8 Gbps	1	0%	
102	 ICMP Echo Flood Daily reported ICMP Echo Flood with IP randomized from 0.0.0.0 to 255.255.255. TTL mostly distributed outside normal range 50-255.	33.330.986	1	5.3 Gbps	23.9 Gbps	1	0%	
81	 TCP Reset Daily reported TCP Reset Flood with most TTL outside of any normal range. Not sure what happens this "Reset" TCP Flood. A few ICMP Echo from Botnet checking status. We can block with Syn-flood block.	18.134.655	100 Mbps	313 Mbps	0	0%		
2	 SYN Flood Specified TCP SYN Flood with most TTL outside of any normal range. All TCP baselines are enabled and set to get to 100% mitigation without peer or other anti-spamming measures.	14.407.444	1	3.7 Gbps	9.5 Gbps	3	0%	
75	 SYN Flood UDP Flood with most TTL outside of normal range. IP randomized 0.0.0.0-255.255.255 and port number 1-65535. We can block with TTL and bytes invariant.	13.344.478	57 Mbps	223 Mbps	0	0%		
45	 SYN Flood Yet another UDP Flood with TTL outside of normal range and an IP in 192.168.0.0/24 range. Source port randomized 1-65535.	12.985.611	1	2.9 Gbps	8.3 Gbps	1	0%	

2. Profile the "dark" Internet

Form 'maps' of the Internet -> fingerprint IoT apps, flag DDoS amplifiers & botnets, identify vulnerable hosts & classify DDoS sources.



3. Detect with Big Data & AI

Combine Genome with state-of-the-art AI/ML and DDoS samples to automatically detect real-time attacks with accuracy.



2. Lightning-fast

~~Traditional flow~~ → Packet sampling



- Zero cache → Real-time DDoS detection
- Header + payload telemetry: TCP SEQ & ACK numbers, DNS queries, etc.

2. Lightning-fast

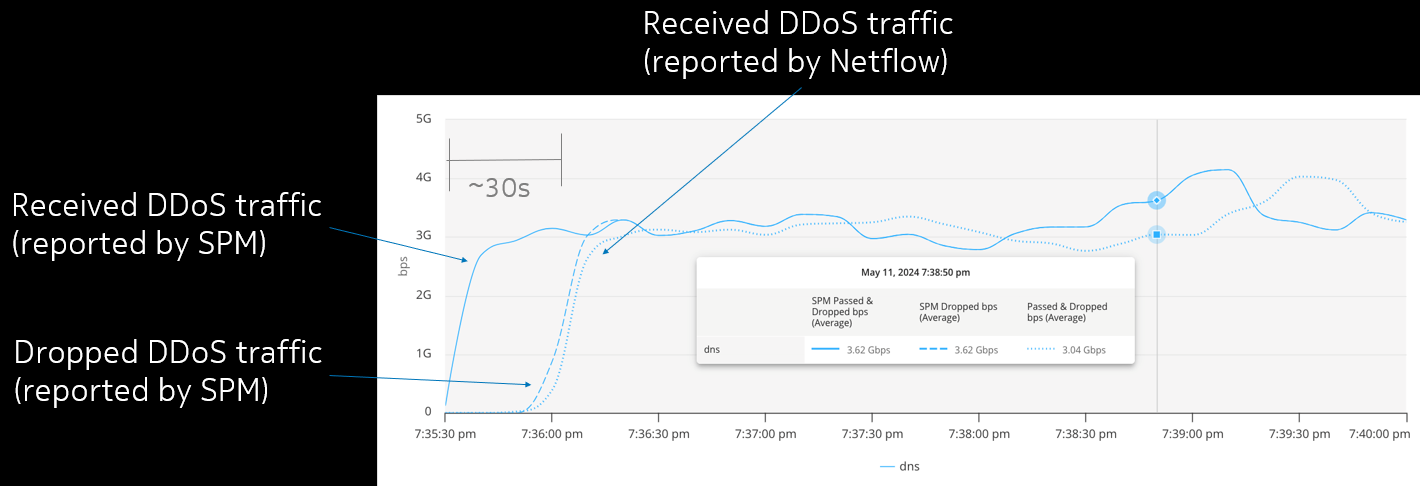
~~Traditional flow~~ → Packet sampling

SPM Sampled Port Mirroring	Nokia, Juniper
IPFIX 315 IPFIX Information Elements 315	Nokia, Juniper (IMON), Cisco
sFlow	Arista

- SPM mirror bandwidth: **1 Tbps = 30 Mbps mirrored** with 1:5k sampling rate, 128B slicing and avg pkt size 1100
- **IPFIX 315** <> **IPFIX** → Do not confuse them!

SPM in action at Bitè

SPM based fast protection



Traffic was dropped before Netflow was able to report it!!!

3. At scale

Nokia Service Routers



FP4/FP5 processor

...or FPcx processor

- **Large filter-scale:** 256K filter-entries
- **Predictable terabit-scale performance:** surgical filtering, without impacting Router-scaling and performance
- **Fast programming** of filters

Deepfield Defender Mitigation System (DMS)

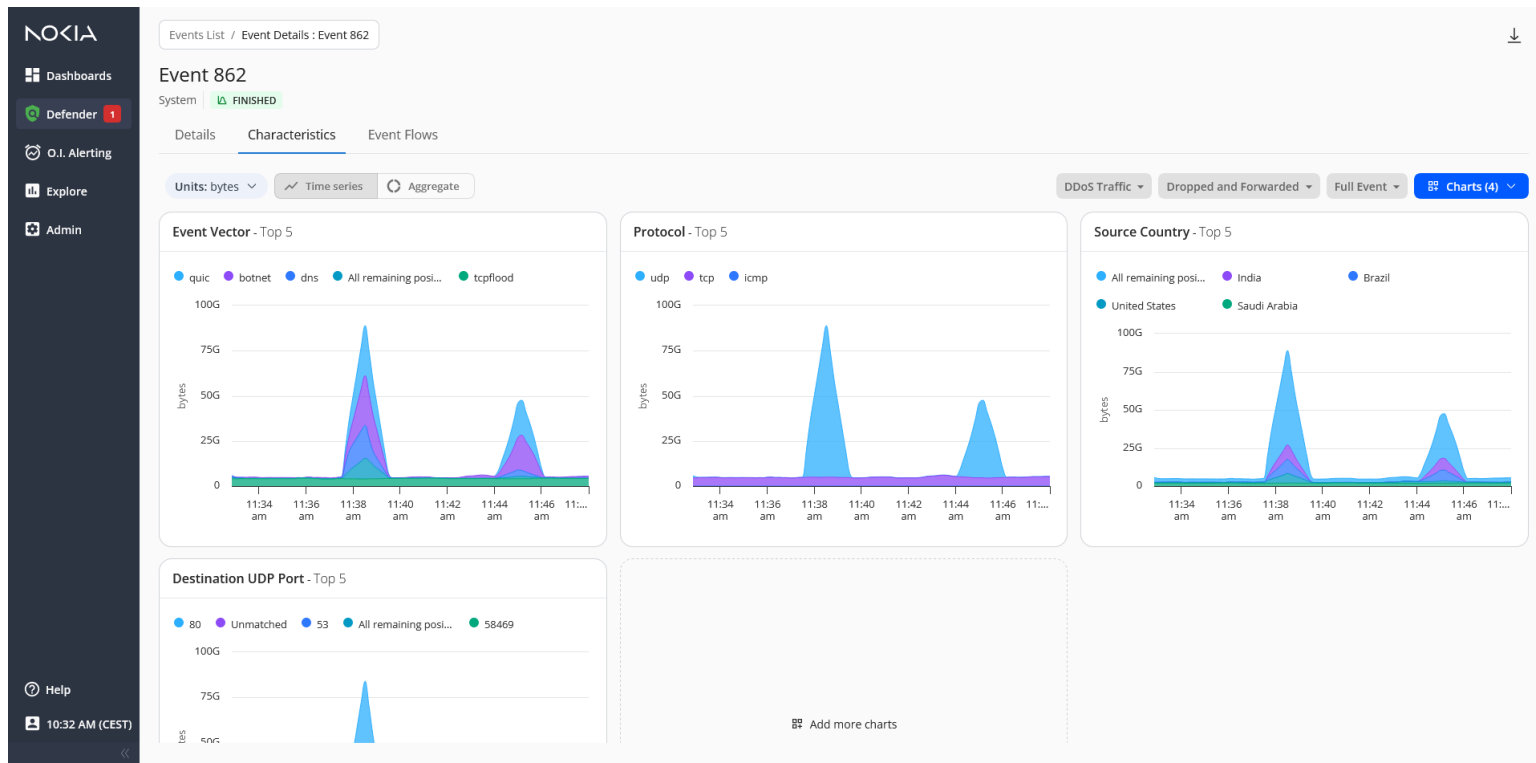


7750 DMS-1-24D

- Purpose-built **DDoS mitigation appliance** for offramp scrubbing
 - FP5-powered with Advanced Countermeasures Engine
 - Optimized SROS software variant for DDoS mitigation (only)
- **2.8 Tbps mitigation capacity**
 - 24 x QFSP-DD supporting 10G/40G/100G/800G per port
 - Pay-as-You-Go licenses
- **Fully Managed and controlled by Deepfield Defender**

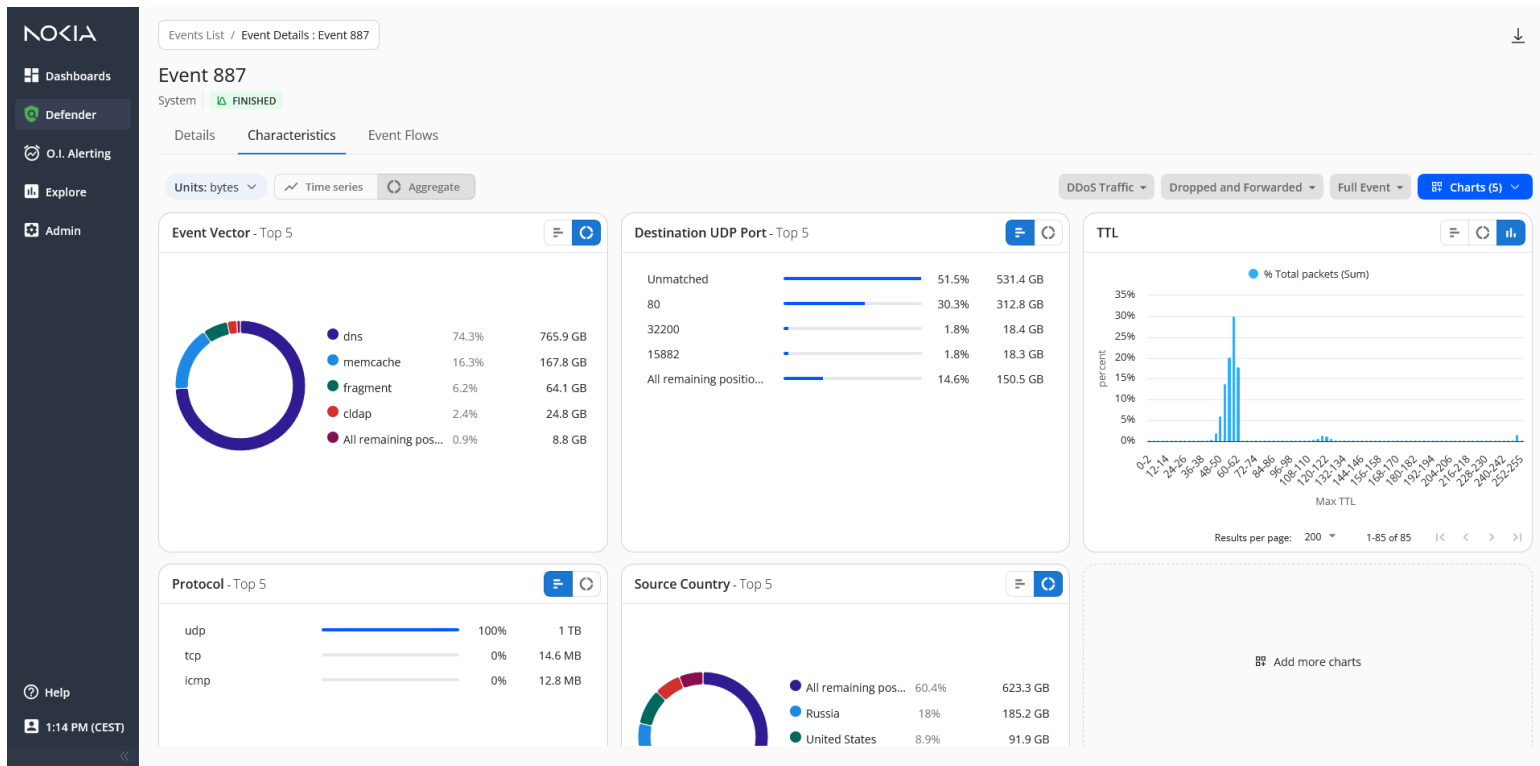
Bonus: DDoS insights

Pre-defined + custom charts, 10-second granularity



Bonus: DDoS insights

Pre-defined + custom charts, 10-second granularity



How do you need your DDoS tool to be today?

Deepfield Defender

1

Automated
Secure Genome

2

Lightning-fast
Packet sampling

3

At scale
FP chipset family

NOKIA

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use by Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular

purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.