itoro

ANTI-DDOS SERVICES NETWORK SECURITY

Andrisoft Network Security
GOLD PARTNER

WAN GUARD

Anti-DDoS software by Andrisoft.com

- Remotely Triggered Black Hole routing (RTBH)
- Traffic filtering with BGP FlowSpec
- DDoS scrubbing centre traffic redirection

Juniper MX

Advanced security and DDoS mitigation router

- DDoS Filtering Gateway
- Inbound and outbound traffic protection
- Routing Engine security and DDoS filter

Piotr Okupski
CEO ITORO
itoro.com.pl

ABOUT ITORO

WanGuard – anti DDoS Software

- Worldwide dedicated WanGuard integration specialist and Andrisoft GOLD PARTNER
- 95%+ of all deployments use port mirror for fastest detection
- 100% of DPDK deployments (10-400GE) use port mirror

Server provisioning and Linux performance tuning

- WanGuard is the most cost-effective volumetric DDoS protection solution for 10–400 GE environments worldwide
- WanGuard system training and knowledge transfer

Full pre- and post-deployment support

- Expert DDoS security consultancy and network hardening recommendations
- Ongoing WanGuard system support — freeing your team from additional monitoring duties

EXPERIENCED PARTNERS

ITORO

Network Security Integrator

Founded 2017 — built on 25+ years of hands-on ISP and network operations, incl. 20+ years with Juniper platforms.

End-to-end delivery: network design, router & switch configuration, deployment and ongoing support.

WanGuard is our flagship, backed by a growing network-security portfolio.

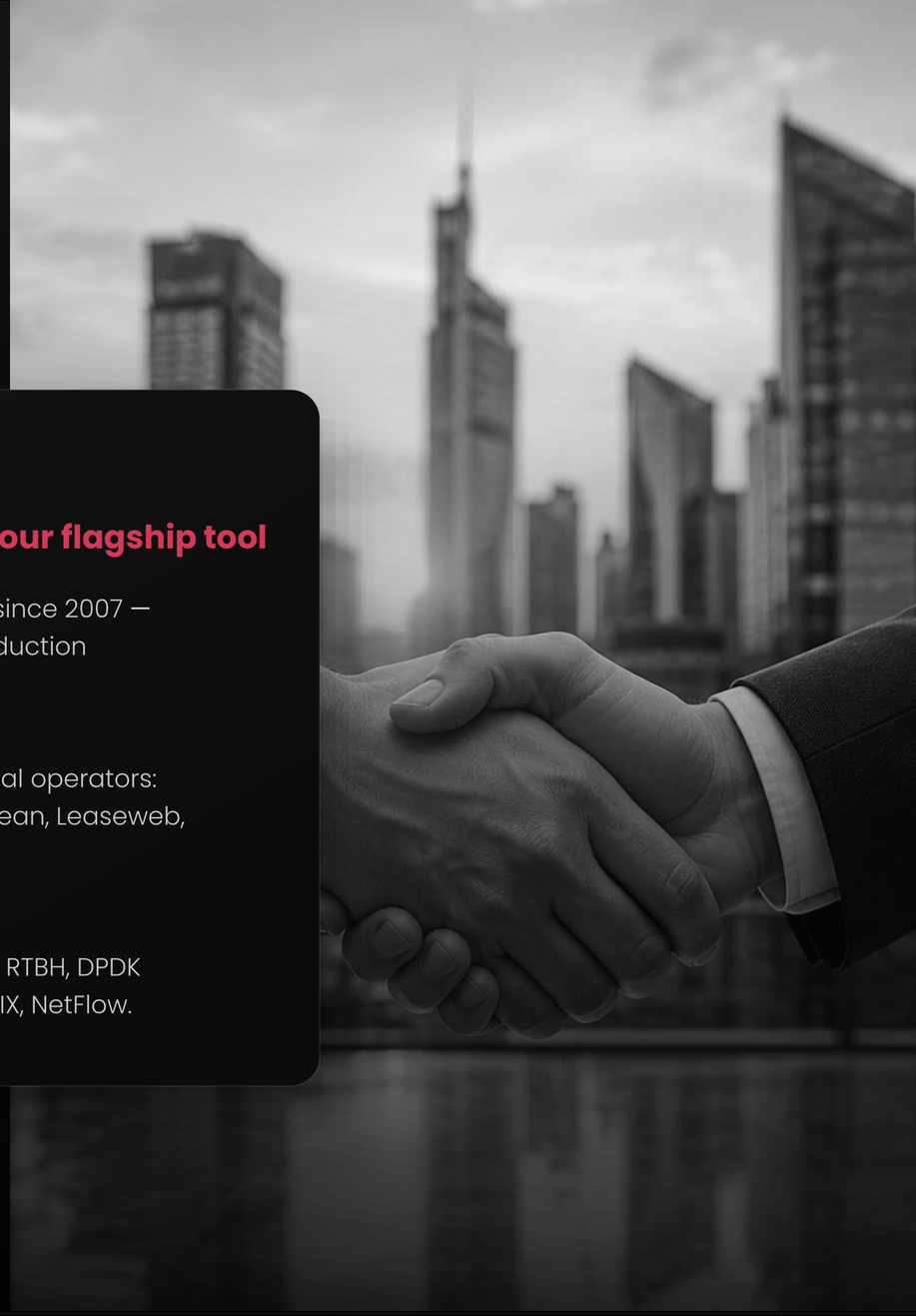
WanGuard

DDoS Platform by Andrisoft — our flagship tool

In continuous development since 2007 — close to two decades of production hardening.

WanGuard is trusted by global operators: Vodafone, Orange, DigitalOcean, Leaseweb, Equinix, Google Fiber.

Full coverage: BGP FlowSpec, RTBH, DPDK line-rate detection, sFlow, IPFIX, NetFlow.



WANGUARD – AN ENTERPRISE-GRADE DDOS PROTECTION PLATFORM WITH PRECISION TRAFFIC FILTERING VIA BGP FLOWSPEC.

Volumetric Attack Protection:

Volumetric attacks exceed the customer's own uplink capacity — making upstream mitigation essential. BGP FlowSpec is the preferred response, allowing granular traffic filtering at the ISP or transit provider level.

RTBH is used as a last resort when attack volume would fully saturate the uplink and FlowSpec alone is insufficient.

Types of DDoS Attacks Blocked by WanGuard:

Network & Amplification

FRAGMENT, SMURF, SNMP

SSDP, MEMCACHED, CHARGEN

SYN-ACK / SYN / ICMP

Application & Protocol

SIP, NETBIOS, LDAP/CLDAP

QUIC, INVALID PACKETS

SYN-ACK / SYN / ICMP

Flood & Volumetric

UDP/TCP Floods

DNS/NTP Flood

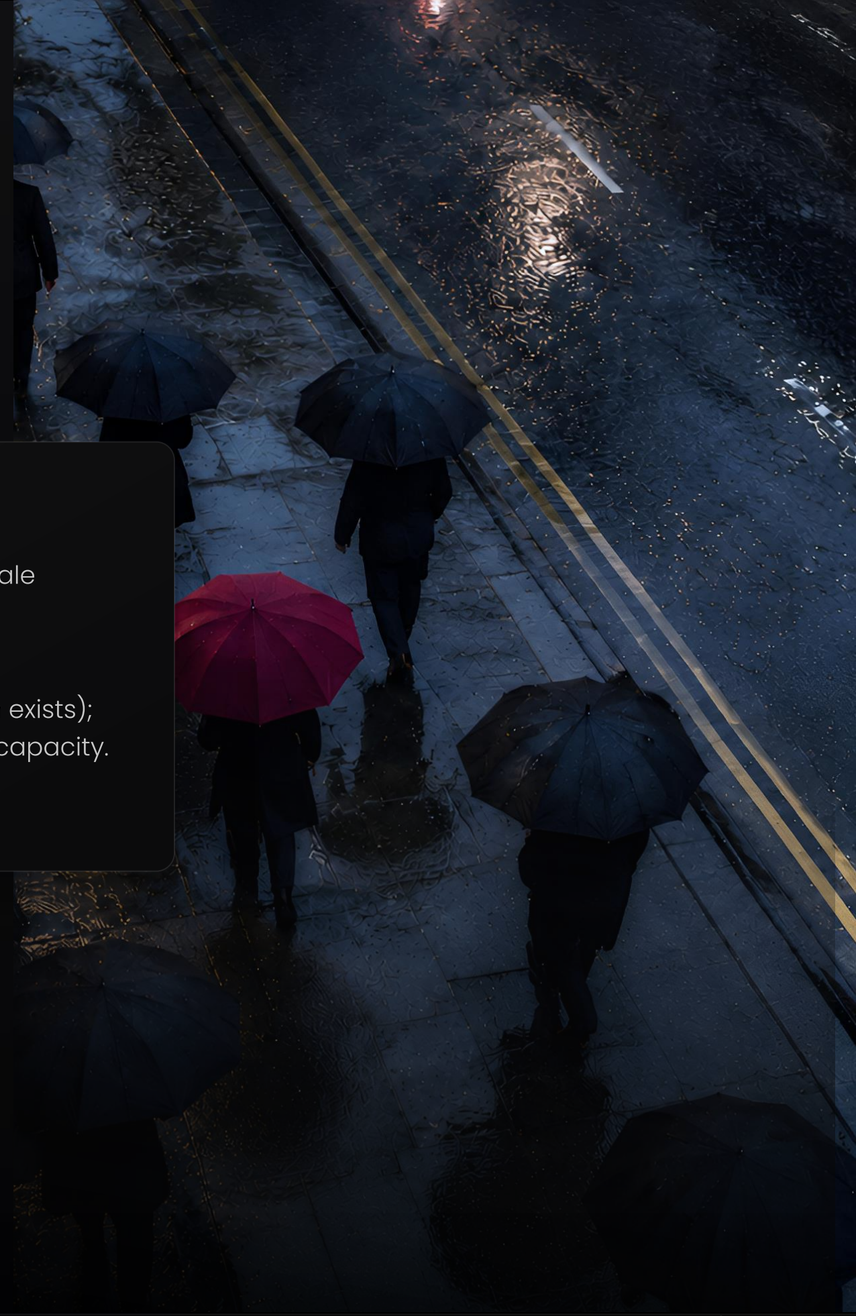
TCP:NULL, RST, ACK, SYN-ACK, XMAS

Carpet Bomb — traffic filtering

How Does WanGuard Protect Networks?

WanGuard automatically generates and deploys BGP FlowSpec filter rules in real time. Where attack volume exceeds filtering capacity, RTBH announcements are sent to upstream providers — dropping malicious traffic before it reaches your network.

WANGUARD
- DDOS PROTECTION SYSTEM



Volumetric DDoS attacks – WanGuard Specialization

These are attacks that involve the use of multiple bots or servers to generate a lot of traffic and packet volumes to block a service or an entire network.

Protection against this type of attack:

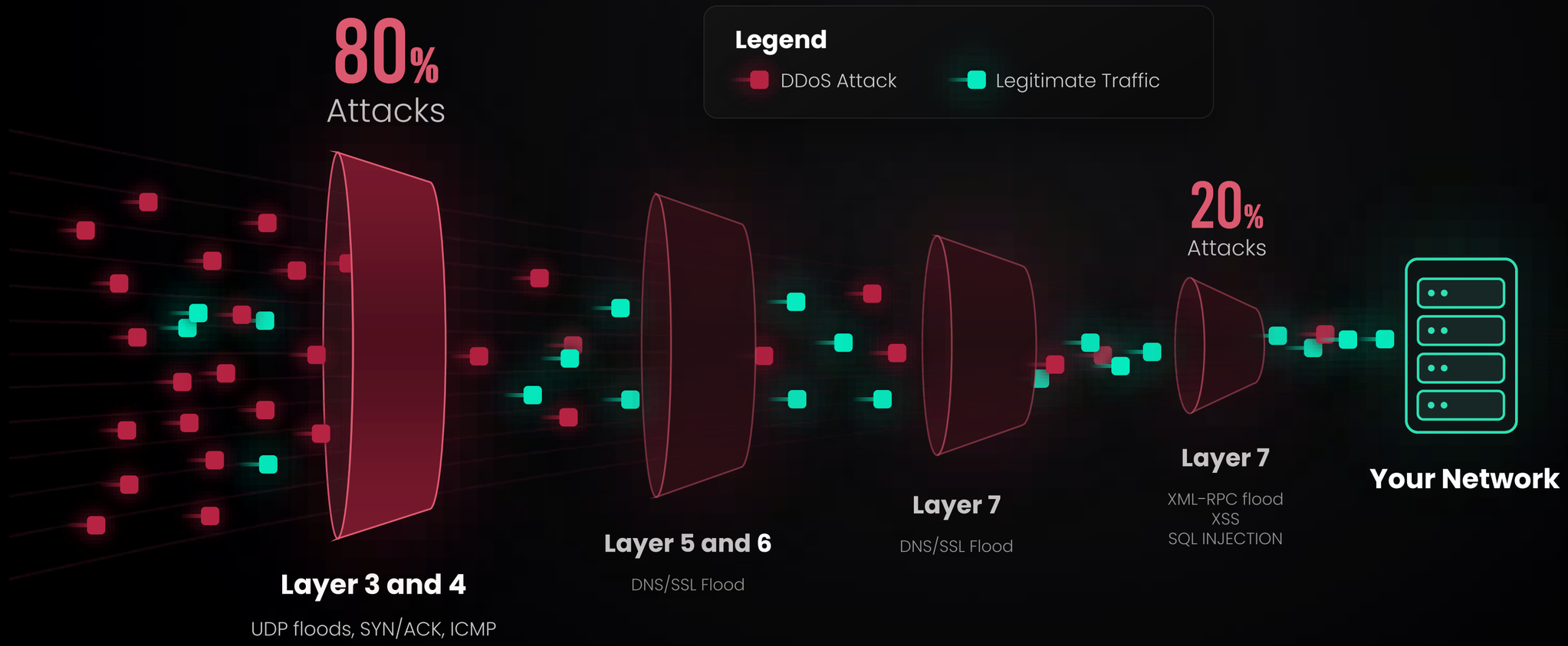
Only the upstream operator or transit provider can absorb large-scale volumetric attacks — they have far greater bandwidth than the end customer.

The first line of defense is traffic filtering (where sufficient bandwidth exists); RTBH blackholing is the fallback when the attack exceeds available capacity.

Other DDoS attacks supported by WanGuard:

- SYN-ACK / SYN / ICMP
- FRAGMENT
- SMURF
- SNMP
- SSDP
- MEMCACHED
- QUIC
- INVALID PACKETS
- NETBIOS
- SIP
- LDAP/CLDAP
- CHARGEN
- UDP/ TCP Floods
- TCP:NULL, RST,ACK
- SYN-ACK,TCP-ALL(XMAS)
- DNS/NTP Flood

WANGUARD DETECTION OPTIONS



Amplification Attacks:

- ARMS
- Chargen
- CLDAP
- COAP
- MS SQL RS
- NTP
- NetBIOS
- RIPv1
- SLP
- SNMP
- SSDP
- STUN
- TCP ACK
- TCP RST
- TCP SYN
- TCP SYN/ACK
- UDP port 0 and 80
- WS-DD
- mDNS
- memcached
- rpcbind

CHOOSE YOUR DETECTION SPEED

TWO WAYS TO SEE AN ATTACK — YOU PICK THE TRADE-OFF

FLOW-BASED

NetFlow / sFlow / IPFIX

35-95SEC

to detect & mitigate

- Lower cost — less work to deploy, no DPDK tuning
- Bandwidth-independent — monitors many routers at once
- Runs for years with little intervention — low support burden
- Slower: by 65 sec uplinks may already be saturated
- Doesn't report FRAGMENTed packets - DDoS Frag Floods
- Best for reporting, Lawful intercept /uniformed sFlow, very high traffic networks

PORT-MIRROR

RECOMMENDED

DPDK packet inspection

<5SEC

RTBH · 15–30 sec filtering

- Fastest detection — reacts before customers notice
- Stops carpet-bomb & volumetric floods at line rate
- Granular FlowSpec rules — legitimate traffic untouched
- Scales with traffic— ITORO tunes it
- The choice for ISPs / DataCenter with transit & DDoS exposure

TRAFFIC COLLECTION — VISIBILITY & COVERAGE

WHAT EACH METHOD ACTUALLY SEES

★ Port-Mirror (DPDK) every packet	sFlow sampled packets	IPFIX (v10) every packet	NetFlow v5 / v9 every packet
EVERY CAPABILITY Detection capabilities	ALL FIELDS — BUT SAMPLED Detection capabilities	COARSE 5-TUPLE ONLY Detection capabilities	COARSE 5-TUPLE ONLY Detection capabilities
FULL COPY OF EVERY PACKET Traffic capture	SAMPLED PACKET COPY (1 IN N) Traffic capture	FLOW RECORDS — COARSE, NO PACKETS Traffic capture	FLOW RECORDS — COARSE, NO PACKETS Traffic capture
100% OF PACKETS Packet coverage	SAMPLED FRACTION ONLY Packet coverage	0% PER-PACKET — COUNTERS ONLY Packet coverage	0% PER-PACKET — COUNTERS ONLY Packet coverage
< 5 S RTBH · 15–30 S FILTERING Detection latency	5–30 S (5 S ON ARISTA) Detection latency	35–95 S — TOO SLOW Detection latency	35–95 S — TOO SLOW Detection latency
VISIBLE — EVERY FRAGMENT Fragmented packets (fragment floods)	ONLY IF THE FRAGMENT IS SAMPLED Fragmented packets (fragment floods)	IN THE IPFIX STANDARD, BUT ROUTERS DON'T EXPORT IT Fragmented packets (fragment floods)	NOT REPORTED AT ALL Fragmented packets (fragment floods)
EXACT FLAGS, PER PACKET TCP-flag attacks (XMAS / NULL / SYN-only)	EXACT — BUT ONLY ON SAMPLED PACKETS TCP-flag attacks (XMAS / NULL / SYN-only)	FLAGS MERGED OVER THE FLOW — COMBOS LOST TCP-flag attacks (XMAS / NULL / SYN-only)	FLAGS MERGED OVER THE FLOW — COMBOS LOST TCP-flag attacks (XMAS / NULL / SYN-only)

Why it matters

Port-mirror sees every field of every packet. Flow aggregation (NetFlow / IPFIX) sees only the coarse 5-tuple — no fragmentation, packet length or exact TCP flags, the signatures of fragment floods and flag-based attacks. sFlow sees those fields too, but only on the sampled fraction.

full · partial / sampled · not available

RTBH black-holing works with all four methods — only the detection detail differs.

WANGUARD DETECTION SPEED ADVANTAGE OVER OTHER ANTI-DDOS SYSTEMS

Mirror based traffic detection with DPDK technology

<5SEC
Detection and mitigation

Black Hole Routing

15-30SEC
Detection and mitigation

Traffic filtering

35-95SEC
Detection and mitigation

Other systems

(sFlow / NetFlow / IPFIX)

By this point, end users have already lost Internet access.

Beyond 65 seconds, uplinks are saturated — ISPs and enterprises experience severe connectivity degradation and high latency.

sFlow export time may vary from network vendor to vendor and can be lower (Arista).

KEY CONCEPTS OF DDOS MITIGATION OPTIONS

Black Hole Routing

Remotely **T**riggered **B**lack **H**ole **R**outing

Blocks all traffic to the targeted destination IP by advertising a null route through BGP

- Drops all traffic matching the attacked destination prefix
- Prevents volumetric floods from saturating transit or edge links
- Fast to deploy, but legitimate traffic is also discarded

FlowSpec

RFC 5575

Instant firewall rules using BGP protocol. Allows for various actions:

- Discard / rate-limit of traffic
- Traffic redirection
- Setting DSCP (differentiated services) bits to provide qos or other filtering options

HONEST SCOPE · WHAT WE CAN & CANNOT BLOCK

MITIGATION HAS LIMITS — AND WE ARE HONEST ABOUT THEM

You pay for expert response and fast mitigation — not a blanket “we block everything” guarantee.

What We Mitigate

- Everything WanGuard + Juniper MX can act on — within your uplink bandwidth.
- Always-on stateless MX filtering: anti-spoofing, anti-amplification, rate-limits, CoPP.
- Dynamic BGP FlowSpec and RTBH activated the moment an attack is detected.
- Granular filtering keeps your customer online — RTBH only as a last resort.

Where We Escalate — Honestly

- Mitigation is bounded by uplink capacity — we cannot filter more than the link carries.
- BGP FlowSpec only blocks what a rule can express — some randomized or adaptive floods cannot be filtered.
- When traffic exceeds your Uplink or cannot be filtered, we escalate to a terabit-scale external scrubbing centre.
- We tell you upfront what we cannot block — that is the brand, not a disclaimer.

WANGUARD AND JUNIPER MX ROUTERS AS A COMPLETE PROTECTION FOR DDOS ATTACKS

ITORO delivers this as a ready-to-deploy, fully managed package. Software, licenses, configuration and ongoing support.

MX204 – 4x100GE Gateway Router

Cost: approx. $10,000 – $20,000

WAN GUARD

Cost: approx. $3000

Always-On Line-Rate Filtering

Juniper MX204 blocks attack traffic at 400 Gbps rate - 24/7, no latency, no manual intervention

Automatic Dynamic Mitigation

WanGuard monitors all traffic via port mirror or sFlow/IPFIX and identifies attack patterns in real time

Intelligent Traffic Detection

WanGuard triggers BGP FlowSpec or RTBH — Juniper executes the rules instantly at line rate

HOW IT WORKS — JUNIPER MX204 + WANGUARD
TWO PRODUCTS. ONE SOLUTION. DELIVERED BY ITORO.

Juniper MX

Static Always-On Gateway

Acts as a permanent line-rate scrubbing engine — filtering known attack traffic before it touches your network.

- 400 Gbps line-rate filtering — ASIC hardware, zero CPU overhead
- Blocks inbound DDoS on uplinks + LAN infected host traffic
- NTP, DNS, ICMP, UDP/TCP amplification, spoofed traffic
- Always-on — no trigger required

WanGuard

Dynamic Detection & Response Engine

Detects what static filters miss, classifies the attack, and automatically instructs Juniper to block it via BGP FlowSpec.

- Sub-second attack detection via DPDK-accelerated engine
- Collects traffic via port mirror or sFlow/IPFIX
- Detects DNS/NTP floods, Carpet Bomb, volumetric anomalies
- Pushes BGP FlowSpec rules to Juniper or triggers RTBH upstream

ITORO packages both as a one-time investment — owned, controlled and managed by You.

Together they form a complete, self-defending network — with no need for an external scrubbing center.

JUNIPER MX — ALWAYS-ON DDOS PROTECTION

Line-rate stateless firewall — active before any attack reaches your network

Input Filter
Inbound DDoS Protection
Blocks spoofed, malformed & amplification attack traffic

lo0 – Routing Engine CoPP
Control Plane Policing and Firewall
Protects access to BGP, OSPF, SSH, SNMP router stays online

Output Filter
Outbound LAN / Customer Protection
Prevents your network from being used as attack source

Internet

uRPF Filtering

Your Network

Layer 1

Transit DDoS Protection (WAN & LAN interfaces)

- Blocks spoofed source addresses
- Eliminates malformed packets
- Blocks 17+ categories of UDP amplification protocols inbound
- Blocks 15+ categories of amplification source ports outbound
- Rate-limits SYN floods, ICMP, DNS, NTP traffic
- ✓ Full IPv4 and IPv6 coverage

Layer 2

Routing Engine Protection (lo0 CoPP)

- Default-deny architecture
- ✓ BGP, OSPF, BFD sessions permitted from configured peers only
- Management access (SSH, SNMP, RADIUS, NTP, DNS)
- All unrecognised traffic is dropped by default

JUNIPER MX FILTER PACKAGE — DEPTH & COMPLEXITY

Delivered by ITORO as a ready-to-deploy configuration

FILTER SCALE

Transit Filters — Hard Blocked Categories:

- Rate-Limited (policed, not dropped):
- SYN floods · IP fragments · ICMP · DNS · NTP

Routing Engine CoPP:

- Default-deny — all unmatched traffic blocked
- Thousands of potential attack vectors eliminated by architecture alone

VISIBILITY & ANTI-SPOOFING

Every filter term has a named counter:

- Real-time visibility via Grafana and Juniper Telemetry
- Counters follow structured naming — protocol, direction, attack type
- Live monitoring available also from JunOS CLI at any time

Anti-Spoofing — uRPF on all interfaces:

- Validates source IP addresses before any filter processing occurs
- Feasible-path mode — supports asymmetric routing in multi-homed environments
- Dedicated fail-counter — RPF violations logged separately from DDoS counters

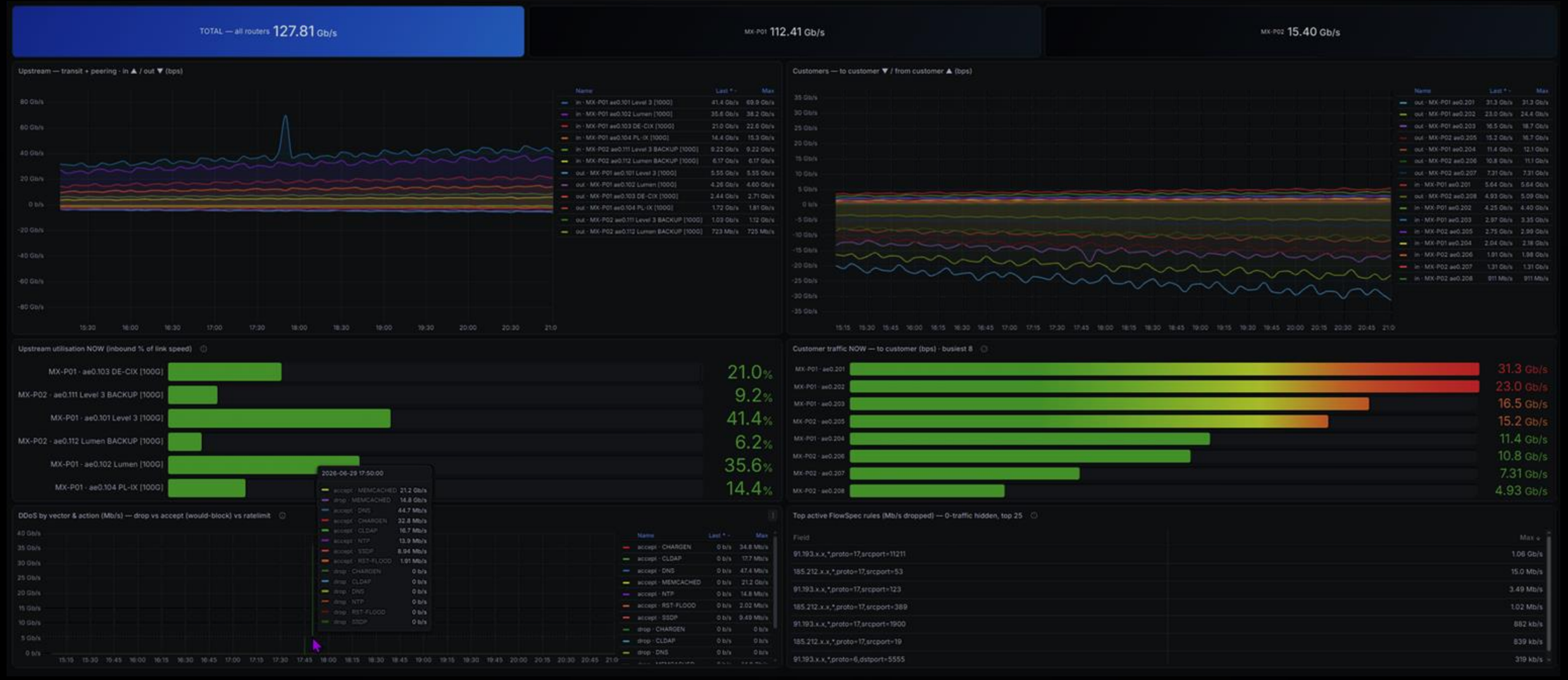
Direction	Malformed	Amplification Protocols
IPv4 / IPv6 Inbound	10 / 9 categories	17 UDP protocol categories
IPv4 / IPv6 Outbound	3 / 3 categories	15 source-port categories

File	Contents	Size
Transit DDoS Filters	4 filters · INPUT/OUTPUT · IPv4 + IPv6 · uRPF · policers	~2,750 lines
Routing Engine CoPP	2 filters · lo0 · IPv4 + IPv6 · dynamic peer resolution	~1,600 lines

REAL-TIME ATTACK TELEMETRY

JUNIPER MX EDGE TELEMETRY

Delivered by ITORO as a ready-to-deploy configuration



WHY ITORO

FROM DESIGN TO PRODUCTION – ONE PARTNER

We guide you end-to-end, and perform all remote WanGuard deployment for you.

Assess

DDoS Attacks, Traffic volume and peaks, number of POPs

Design

Architecture and filters tailored to your network.

Configure

Routers, switches and WanGuard set up correctly.

Deploy

Go live in a single maintenance window.

Support

Ongoing tuning, monitoring and response.

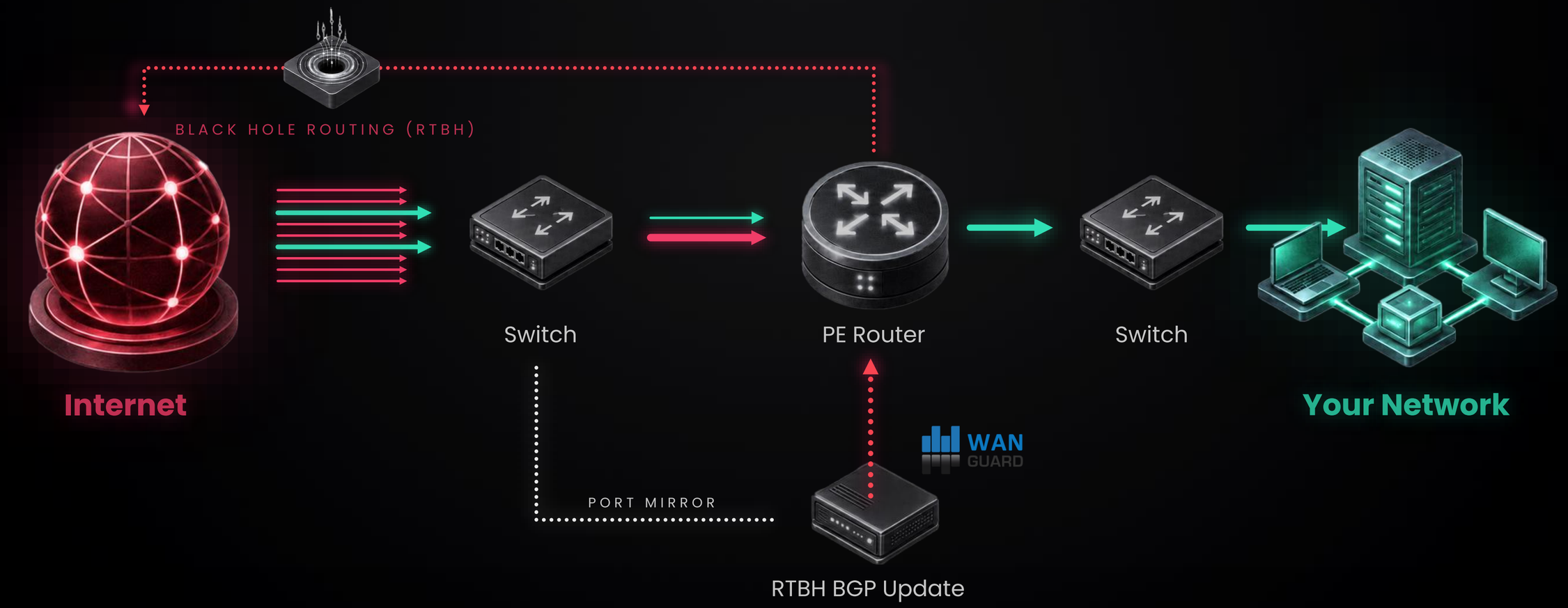
Before choosing a DDoS protection provider, ask:

What are the limits and coverage of DDoS attacks ?

SCOPE OF WANGUARD'S BASIC PROTECTION DEPLOYMENT - RTBH

WANGUARD WITH RTBH (BLACK HOLE ROUTING)

A BGP update with an RTBH community is sent to the upstream service provider (Tier 1/2), causing the attack traffic to be dropped at their network before entering yours.



DDOS TRAFFIC FILTERING

Traffic filtering capabilities:

- BGP FlowSpec filtering on hardware routers
  (Arista /Cisco / Huawei / Juniper / Nokia)
- DPDK-based hardware filtering via
  high-speed network adapters (Intel / Mellanox)
- Software-based filtering using Linux iptables / nftables
  — best suited for targeted or low-volume attacks

ADVANTAGES OF USING BGP FLOWSPEC

Quick response to attacks

BGP FlowSpec pushes filtering rules network-wide in seconds, stopping attacks before they reach their targets.

Integration

Compatible with BGP-capable routers from Cisco, Juniper, and Arista — integrates into your current environment without additional complexity.

Precise traffic filtering

FlowSpec rules target malicious traffic by IP, protocol, port and packet characteristics — legitimate traffic passes through unaffected.

Easy to manage and deploy

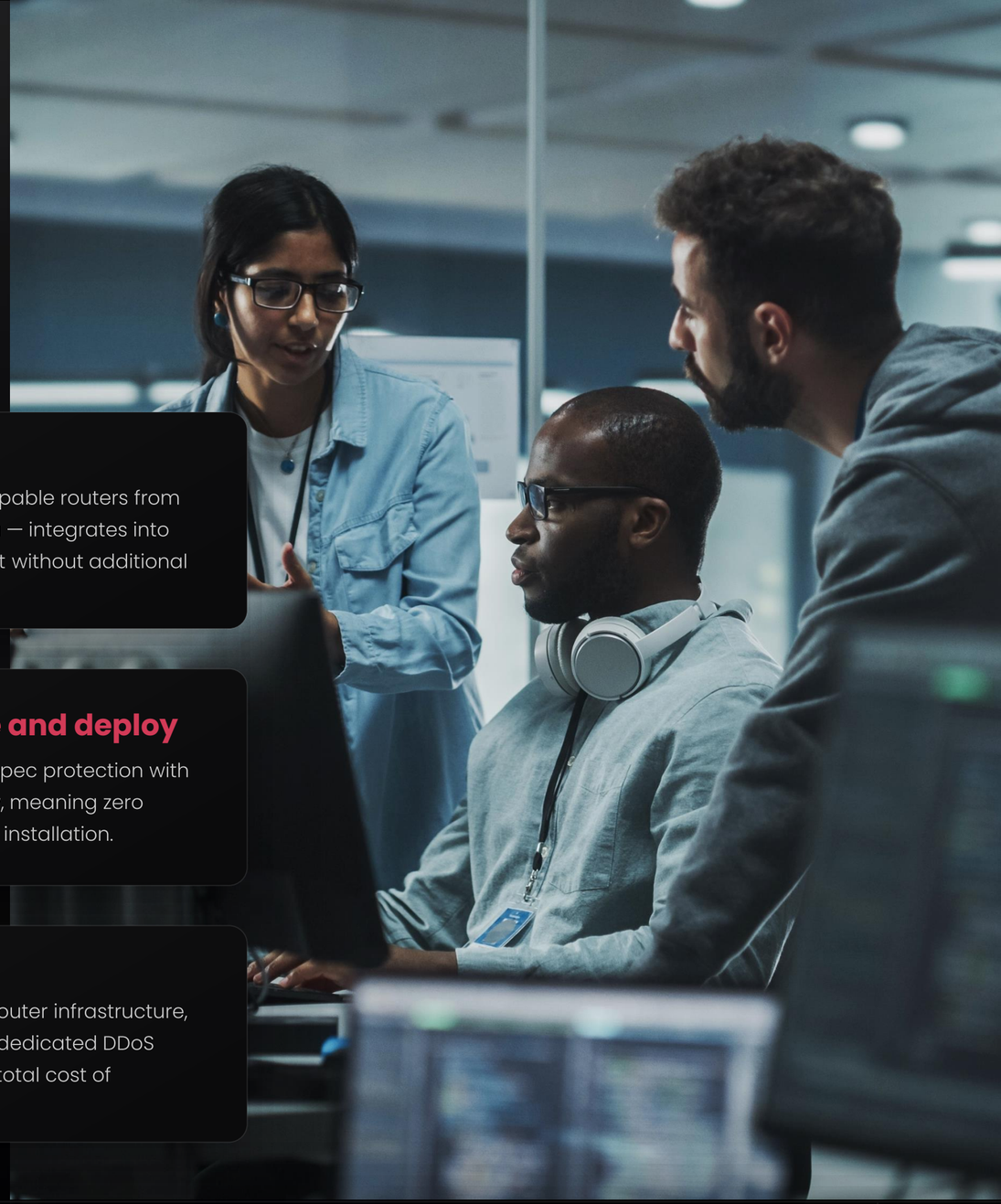
ITORO deploys BGP FlowSpec protection with no maintenance window, meaning zero service disruption during installation.

Scalability

BGP FlowSpec runs on existing BGP infrastructure, without dedicated hardware. Rules can be applied globally or to selected network segments.

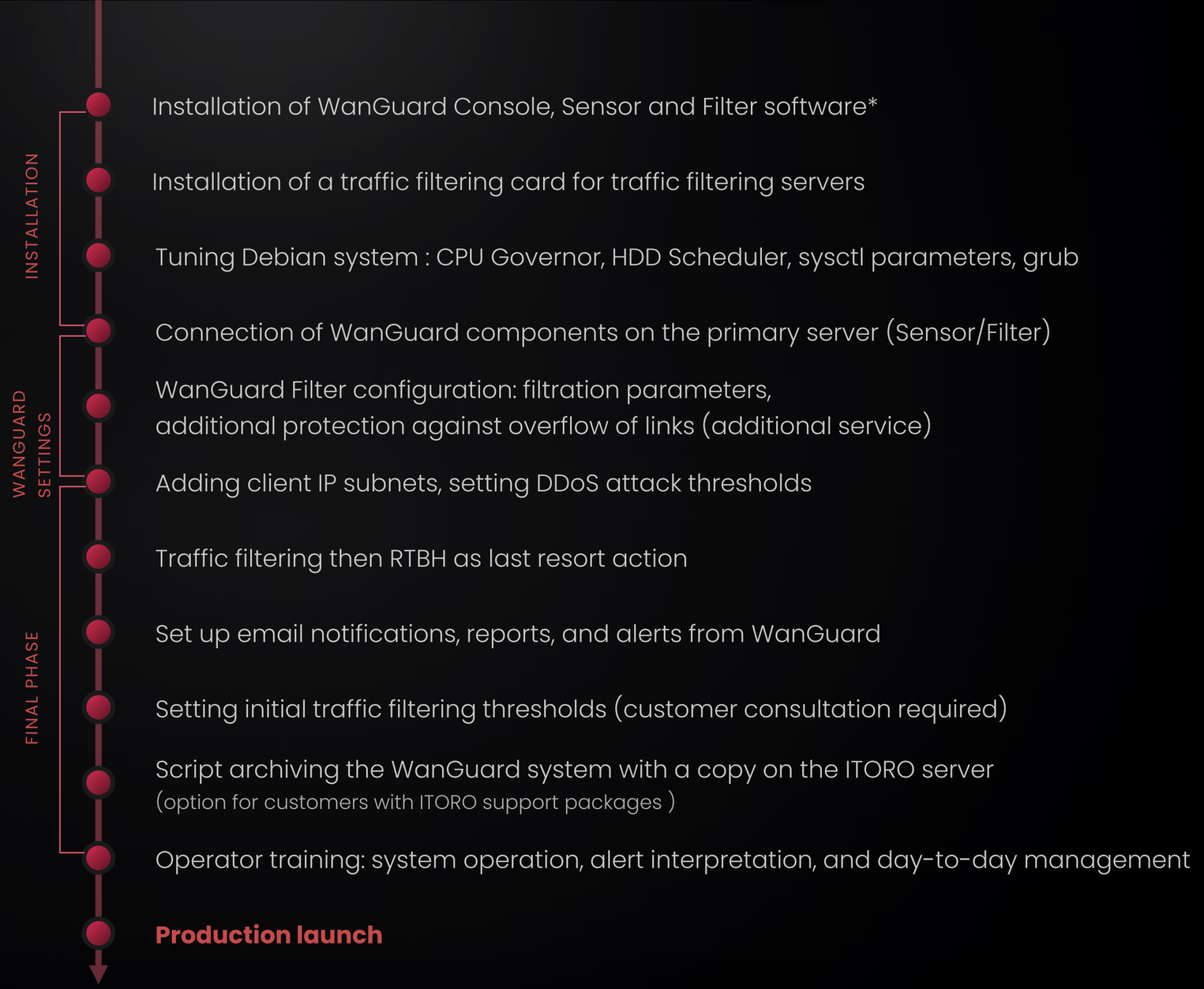
Cost reduction

Leverages your existing router infrastructure, eliminating the need for dedicated DDoS hardware and reducing total cost of ownership.



SCOPE OF WANGUARD'S ADVANCED PROTECTION DEPLOYMENT

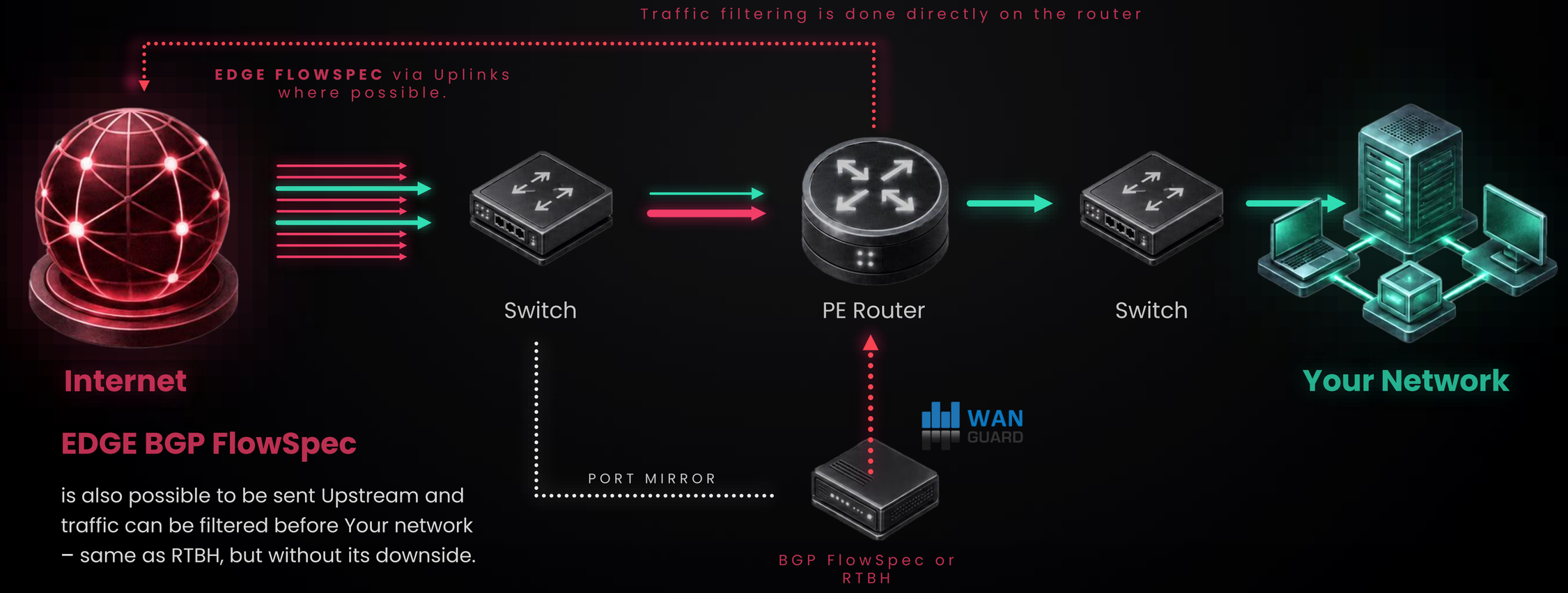
RTBH & BGP FlowSpec Filtering & Traffic Redirection



* WanGuard Filter cannot function alone; it must work together with WanGuard Sensor.

WANGUARD WITH BGP FLOWSPEC

A BGP update with FlowSpec firewall rules is sent to Your routers, causing matched traffic to be dropped at Uplink interfaces, without hitting Your internal network infrastructure.



EDGE BGP FlowSpec

is also possible to be sent Upstream and traffic can be filtered before Your network – same as RTBH, but without its downside.

WANGUARD SYSTEM ARCHITECTURE

The WanGuard DDoS mitigation solution is deployed across dedicated high-performance servers, each serving a specific role:

Management & Control Server

- Hosts the centralized web console for system administration and monitoring
- Runs GoBGP daemon for dynamic filtering rule propagation to upstream routers

High-Speed Filtering Sensors

(Data Plane Development Kit) accelerated processing for ultra-low-latency traffic analysis (Off-Ramp) Dynamically generates and enforces BGP FlowSpec filtering rules against malicious traffic

Deployment Specifications

- Network Interfaces Dual 10-400 Gbps ports (Intel/Mellanox NICs) with DPDK acceleration for full line-rate traffic capture

Protection Methodology

Multi-Stage Mitigation:

- BGP FlowSpec Filtering — granular traffic scrubbing based on real-time attack signatures and adaptive thresholds
- RTBH (Black Hole Routing) — automatically activated within 5 seconds as a last-resort measure to prevent full link saturation during extreme volumetric attacks

False Positive Reduction

- Detection thresholds fine-tuned per industry best practices to minimize disruption to legitimate traffic

WANGUARD EXAMPLE DDOS ATTACK - UDP PORT 80

Description of the Attack:

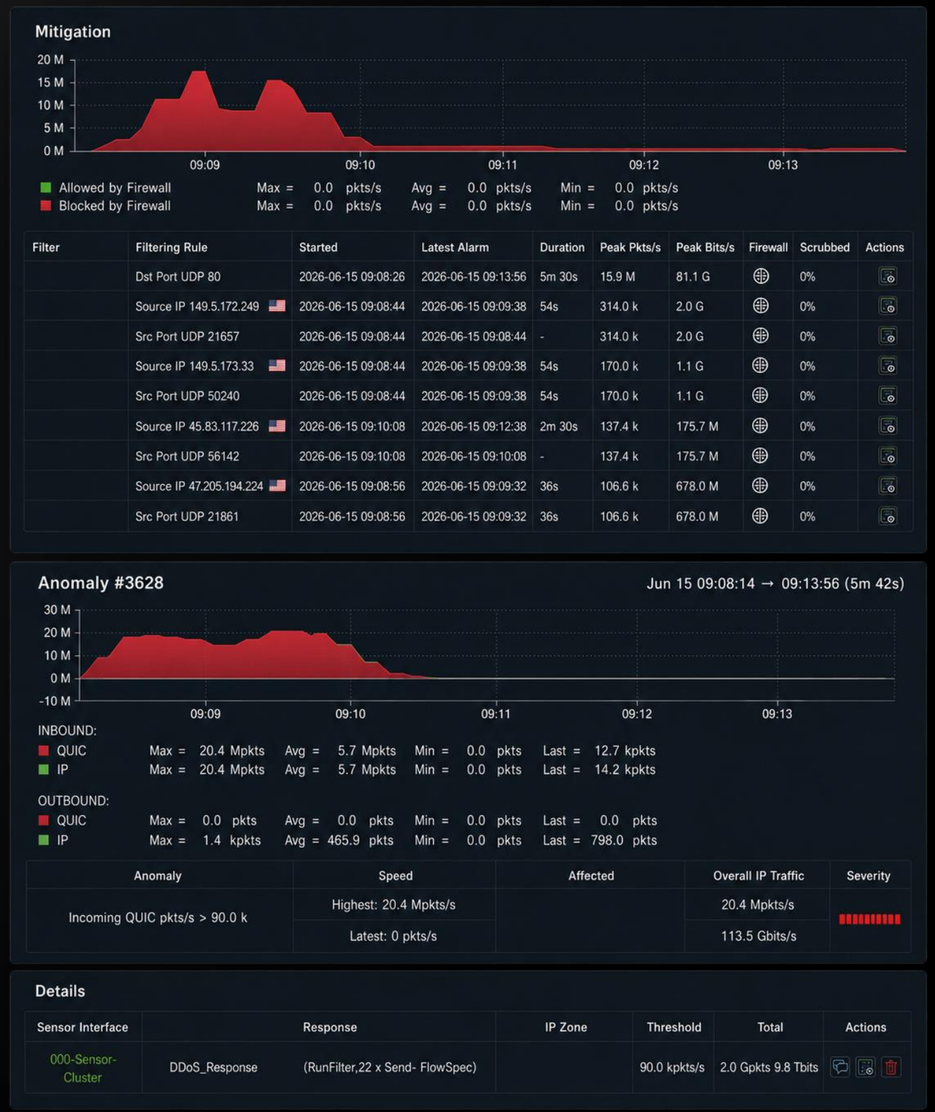
A volumetric DDoS attack targeting UDP port 80, peaking at 113 Gbps with up to 20.4 million packets/second. The attack was identified as a QUIC protocol flood.

WanGuard System Response:

WanGuard automatically classified the attack and deployed 22 BGP FlowSpec filtering rules, which were distributed via the GoBGP daemon to upstream routers.

Effect:

Attack traffic was fully scrubbed before reaching the client's network. The client's service remained stable and uninterrupted throughout the 5-minute 42-second attack window. Zero legitimate traffic was disrupted.



WANGUARD CASE STUDY - ISP OPERATOR, CARPET BOMB ATTACK (50 GBPS)

The Problem

In September 2024, an ISP operator came to ITORO facing daily volumetric DDoS attacks exceeding their 10 Gbps link capacity — with peaks of 50–60 Gbps. Their only defense was RTBH, which meant black-holing entire IP addresses and taking customers offline.

The Attack

A Carpet Bomb DDoS distributes attack traffic across every IP in a target network. A single /22 prefix holds 1,022 IP addresses — at just 50 Mbps per IP, that totals over 51 Gbps of inbound attack traffic, bypassing traditional threshold-based detection.

The solution

ITORO deployed WanGuard with BGP FlowSpec in partnership with ORANGE Poland. Granular filter rules were pushed directly to ORANGE's upstream routers, scrubbing malicious traffic before it reached the operator's network — eliminating the need for black hole routing entirely.

The Result

Over the course of a month, ITORO and the operator continuously adapted filters against evolving attack vectors, blocking amplified protocols at the router level. The attacker eventually abandoned the campaign once it became clear the network was unaffected.

No ↓	Prefix	Anomaly	Speed	Duration	IP pkts/s	IP Bits/s	Severity
12824	.68.2	TCP pkts/s > 110.0 k	660.0 k	5s	660.0 k	7.6 G	
12823	.68.1	FRAGMENT pkts/s > 50.0 k	392.7 k	2s	392.8 k	4.6 G	
12822	.68.1	TCP pkts/s > 110.0 k	392.7 k	2s	392.8 k	4.6 G	
12821	.68.37	TCP pkts/s > 110.0 k	341.8 k	<5sec	341.9 k	3.9 G	
12820	.68.37	FRAGMENT pkts/s > 50.0 k	341.9 k	6s	341.9 k	3.9 G	
12819	.68.36	FRAGMENT pkts/s > 50.0 k	554.6 k	6s	554.7 k	6.4 G	
12818	.68.36	TCP pkts/s > 110.0 k	554.5 k	3s	554.7 k	6.4 G	
12817	.68.35	FRAGMENT pkts/s > 50.0 k	428.9 k	3s	429.0 k	5.0 G	
12816	.68.35	TCP pkts/s > 110.0 k	428.8 k	3s	429.0 k	5.0 G	
12815	.68.34	FRAGMENT pkts/s > 50.0 k	516.4 k	8s	516.4 k	6.0 G	
12814	.68.34	TCP pkts/s > 110.0 k	516.3 k	6s	516.4 k	6.0 G	
12813	.68.33	FRAGMENT pkts/s > 50.0 k	504.0 k	6s	504.5 k	5.8 G	
12812	.68.33	TCP pkts/s > 110.0 k	504.4 k	3s	504.5 k	5.8 G	
12811	.68.32	FRAGMENT pkts/s > 50.0 k	501.0 k	2s	501.0 k	5.8 G	
12810	.68.32	TCP pkts/s > 110.0 k	500.9 k	2s	501.0 k	5.8 G	
12809	.68.29	FRAGMENT pkts/s > 50.0 k	52.2 k	<5sec	52.2 k	607.7 M	
12808	.68.30	FRAGMENT pkts/s > 50.0 k	235.6 k	3s	235.7 k	2.7 G	
12807	.68.30	TCP pkts/s > 110.0 k	235.5 k	<5sec	235.7 k	2.7 G	
12806	.68.31	FRAGMENT pkts/s > 50.0 k	375.7 k	3s	375.7 k	4.3 G	
12805	.68.31	TCP pkts/s > 110.0 k	375.6 k	3s	375.7 k	4.3 G	
12804	.68.18	FRAGMENT bits/s > 300.0 M	571.2 M	<5sec	49.5 k	571.3 M	
12803	.68.19	FRAGMENT bits/s > 300.0 M	574.1 M	<5sec	49.8 k	574.2 M	
12802	.68.20	FRAGMENT pkts/s > 50.0 k	51.0 k	<5sec	51.1 k	589.8 M	
12801	.68.21	FRAGMENT pkts/s > 50.0 k	58.4 k	<5sec	58.5 k	675.5 M	
12800	.68.22	FRAGMENT bits/s > 300.0 M	492.7 M	<5sec	42.7 k	493.0 M	
12799	.68.23	FRAGMENT pkts/s > 50.0 k	52.0 k	<5sec	52.1 k	601.5 M	
12798	.68.24	FRAGMENT pkts/s > 50.0 k	51.7 k	<5sec	51.7 k	596.8 M	
12797	.68.25	FRAGMENT pkts/s > 50.0 k	50.4 k	<5sec	50.4 k	582.4 M	
12796	.68.26	FRAGMENT pkts/s > 50.0 k	50.8 k	<5sec	50.8 k	586.6 M	
12795	.68.27	FRAGMENT pkts/s > 50.0 k	57.7 k	<5sec	57.8 k	666.7 M	
12794	.68.28	FRAGMENT pkts/s > 50.0 k	52.3 k	<5sec	52.4 k	604.5 M	
12793	.68.29	FRAGMENT bits/s > 300.0 M	569.2 M	<5sec	49.3 k	569.3 M	
12792	.68.30	FRAGMENT bits/s > 300.0 M	579.8 M	9s	29.3 k	338.0 M	
12791	.68.10	FRAGMENT pkts/s > 50.0 k	88.2 k	<5sec	88.3 k	1.0 G	

WANGUARD CARPET BOMB ATTACK

Attack Detection

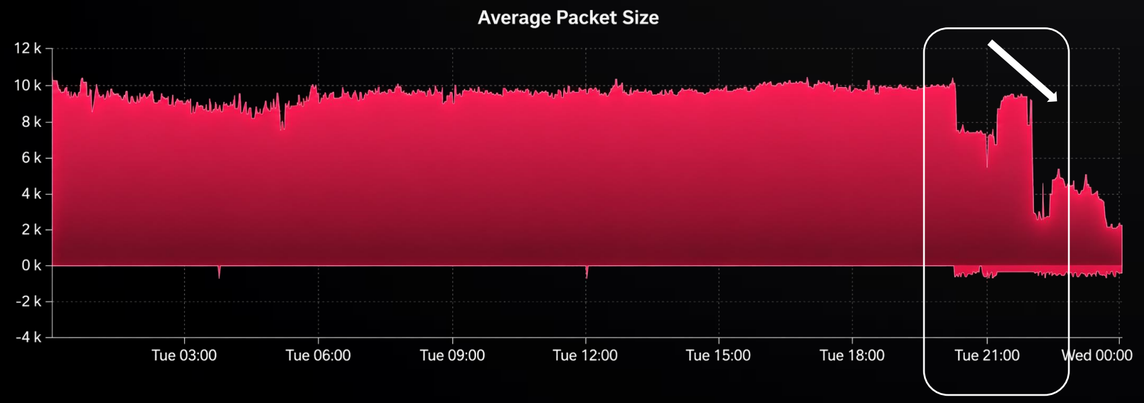
WanGuard detected a volumetric DDoS event saturating the uplink to 7 Gbps, with small packet rate spiking to nearly 1 million packets/second.

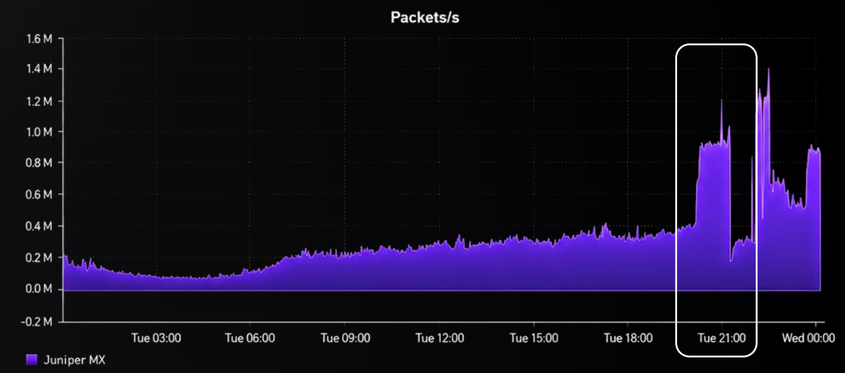
Attack Classification: DNS & NTP Amplification

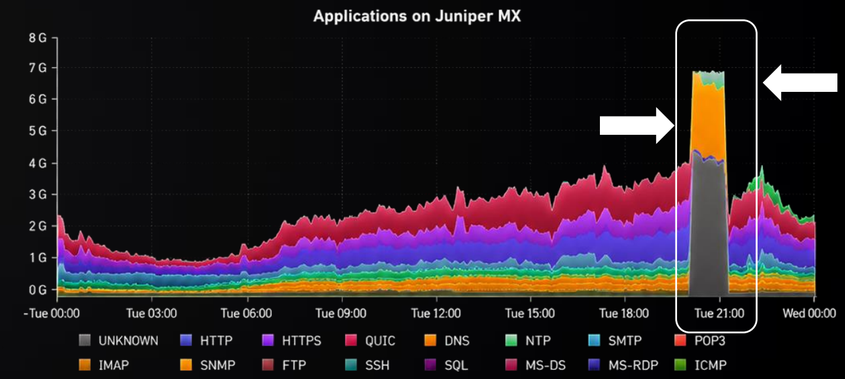
WanGuard identified the attack as a DNS and NTP amplification attack.
Carpet Bomb distribution was confirmed as the number of internal IPs under attack jumped from ~200 to over 1,800 — meaning every IP in the prefix was being targeted simultaneously to evade per-IP threshold detection.

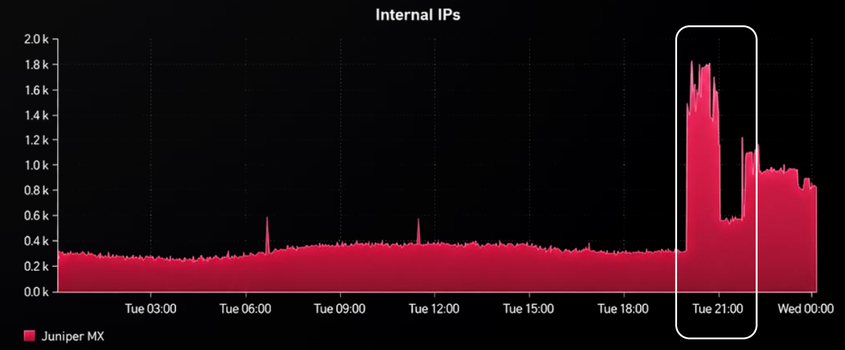
Mitigation

- The attack was mitigated using a combination of:
- BGP FlowSpec — granular filter rules pushed upstream to block amplified UDP traffic (port 53/DNS, port 123/NTP)
- RTBH — black hole routing was applied where needed.









CARPET BOMB SAMPLE REPORT

Anomaly #119704

Jul 03 13:17:07 → 13:39:57 (22m 50s)

INBOUND:

UDP-HTTP	Max	=	28.4	Gbits/s	Avg	=	3.5	Gbits/s	Min	=	0.0 bits/s	Last	=	4.8	Mbits/s
IP	Max	=	28.4	Gbits/s	Avg	=	3.5	Gbits/s	Min	=	0.0 bits/s	Last	=	4.8	Mbits/s

OUTBOUND:

UDP-HTTP	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s	Last	=	0.0	bits/s
IP	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s	Last	=	0.0	bits/s

Anomaly	Speed	Affected	Overall IP Traffic	Severity
Incoming UDP-HTTP bits/s > 1.0 M	Highest: 28.4 Gbits/s		2.6 Mpkt/s	
	Latest: 0 bits/s		28.4 Gbits/s	

Details

Sensor Interface	Response	IP Zone	Threshold	Total	Actions
Sensor-2x100GE	DDoS Response (Uruchom Filtr, RTBH, 911 x Wsylij FlowSpec, 79 x Carpet Bomb, Raport DDoS)		1.0 Mbits/s	445.8 Mpkt/s 4.8 Tbits	

Mitigation

DPDK Filter

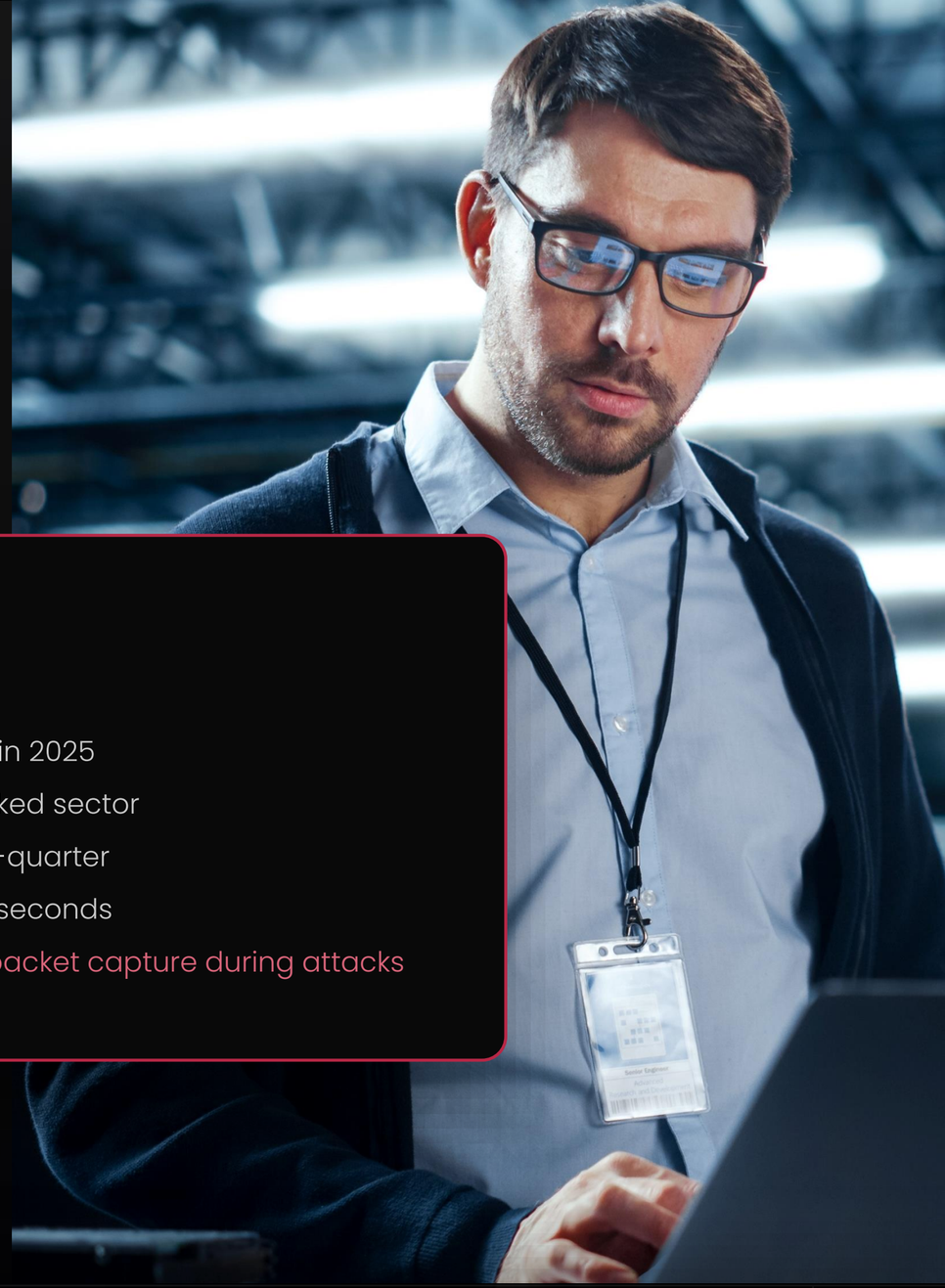
Allowed by Firewall	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s
Blocked by Firewall	Max	=	0.0	bits/s	Avg	=	0.0	bits/s	Min	=	0.0 bits/s

Filter	Filtering Rule	Started	Latest Alarm	Duration	Peak Pkts/s	Peak Bits/s	Firewall	Scrubbed	Actions
DPDK Filter	Packet Length 1428	2026-07-03 13:17:17	2026-07-03 13:31:33	14m 16s	626.0 k	7.2 G	Ⓕ	-	-
DPDK Filter	TimeToLive 57	2026-07-03 13:17:17	2026-07-03 13:29:47	12m 30s	459.2 k	5.0 G	-	-	-
DPDK Filter	TimeToLive 58	2026-07-03 13:17:17	2026-07-03 13:30:58	13m 41s	428.7 k	4.7 G	-	-	-
DPDK Filter	TimeToLive 56	2026-07-03 13:17:17	2026-07-03 13:28:52	11m 35s	346.2 k	3.8 G	-	-	-
DPDK Filter	Packet Length 1468	2026-07-03 13:17:17	2026-07-03 13:29:47	12m 30s	325.1 k	3.8 G	Ⓕ	-	-
DPDK Filter	TimeToLive 55	2026-07-03 13:19:07	2026-07-03 13:29:27	10m 20s	254.7 k	2.8 G	-	-	-
DPDK Filter	Source IP 82.165.183.200	2026-07-03 13:21:57	2026-07-03 13:22:57	1m	84.8 k	928.9 M	Ⓕ	-	-
DPDK Filter	Src Port UDP 14587	2026-07-03 13:21:57	2026-07-03 13:22:52	55s	73.1 k	800.0 M	Ⓕ	-	-

NEW FOR 2026 · INCIDENT RESPONSE

EMERGENCY DDOS RESPONSE

When an attack is live — Friday evening, mid-extortion, thresholds need tuning?
— ITORO acts first. Live monitoring, packet analysis, and threshold / BGP FlowSpec tuning.



ANNUAL

€6000

year

Acting as Your remote SOC.
Ask for more information via
sales@itoro.com.pl

Why it matters now

- DDoS attacks more than doubled to 47.1M in 2025
- Telecom / ISPs are now the #1 most-attacked sector
- Ransom-DDoS threats up 68% quarter-on-quarter
- Largest 2025 attack hit 31.4 Tbps in just 35 seconds
- Most ISPs have no one who can read the packet capture during attacks

Source: Cloudflare 2025 DDoS reports · NETSCOUT 2025

PORT-MIRROR SENSOR CAPACITY

SENSOR & FILTER PRICING SCALES WITH PORT SPEED

More throughput means more dedicated CPU cores and more tuning — the price reflects the real work.
2×100GE is today's default; 1-2×400GE is the premium tier for high-uplink and growing networks.

Sensor (2 ports)	Approx. CPU cores	Detection	One-time deploy	Best fit
2 × 10GE	~12–16	<5s / 15–30s	**€3,000**	Small / edge
2 × 40GE	~16-24	<5s / 15–30s	**€4,500**	Mid-size ISP
2 × 100GE ★ default	~24-32	<5s / 15–30s	**€6,000**	Most ISPs today
1-2 × 400GE premium	~64-128 (1-2 x CPU)	<5s / 15–30s	**€24,000**	400G uplinks / growth
Flow (NetFlow/sFlow)	minimal	35–95s	**€3,400**	Reporting / gov / light

Add-ons:

Extra 2×100GE sensor
(no downtime)
€5,000

BGP FlowSpec config
(Cisco/Juniper)
€1,000

NetFlow archiving
2–40TB
€1,000

WanSight reporting license from
€318

TECHNICAL SUPPORT · 2026

PICK THE LEVEL OF COVER — MOST ISPS CHOOSE GOLD

Emergency DDoS Response, DDoS analysis, on-demand Thresholds Tuning – consider lowering burden on Your NOC/SOC.

SD = Same Day · SBD = Same Business Day · NBD = Next Business Day, 10:00–22:00.

Support task	Silver NBD · Entry	Gold SBD · ★ Most Chosen	Gold + Same-day	Platinum Full Admin
Email support · WanGuard & Linux issues · updates 2×/yr	✓	✓	✓	✓
DDoS threshold recommendations backups · false-positive advice	✓	✓	✓	✓
Active attack monitoring by ITORO	✗	✓	✓	✓
Bi-weekly anomaly & config Monitoring Zoom sessions	✗	✓	✓	✓
ITORO makes changes in WanGuard for you	✗	✓	✓	✓
Remote sensor health monitoring + auto-heal (always-online)	✗	✓	✓	✓
Full administration / outsourcing (no in-house admin needed)	✗	✗	✗	✓
Price (net, EUR)	**€3,000** /yr	**€1,500** /month	**€1,800** /month	**€4,000** /month

PUTTING IT TOGETHER

A TYPICAL DEPLOYMENT — AND WHY IT'S LOW-RISK

Recommended package	EUR
Port-Mirror deployment — 2×100GE Sensor & Filter (DPDK)	€6000
30-day threshold tuning + operator training	**included**
GOLD support — active monitoring + auto-heal (year 1)	€1,500 /month
WanGuard licences — Sensor + Filter (with 30% ITORO discount)	**~€2,500 / yr**
First-year total	**€26,500**
Following years	€20,500

LOW-RISK BY DESIGN

30-day tuning guarantee
we calibrate until false positives are minimized

Acceptance milestone
mitigation proven to spec before sign-off

Your servers and total control
no external scrubbing center, no lock-in

Backed by 20+ years of hands-on ISP
transit experience

Are You under DDoS attack?
We can deploy WanGuard in 2 hours

30
day offer validity

COMPLIANCE · EU NIS2 DIRECTIVE (2022/2555)

DDOS RESILIENCE IS NOW A LEGAL OBLIGATION

NIS2 makes DDoS protection and incident reporting mandatory for ISPs, telecoms and digital infrastructure across the EU.

What NIS2 Requires	How ITORO Covers It
Technical measures to manage cyber risk Including ddos detection and mitigation (art. 21)	Always-on filtering + monitored mitigation deliver the technical risk measures NIS2 expects.
Incident reporting Early warning within 24h, notification within 72h, final report within 1 month (art. 23).)	The Emergency retainer gives you a documented, time-bound incident-response process.
Management accountability Management bodies are accountable for overseeing these measures	Reporting-ready telemetry and packet capture support your 24h / 72h notifications.
Applies to essential & important entities: ISPs, IXPs, DNS, cloud and telecom providers.	Non-compliance risks fines up to €10M or 2% of global annual turnover — we help keep you covered.

itoro

Let’s talk about your network.

Scoped to fit — no overselling.

sales@itoro.com.pl