itoro

Andrisoft GOLD PARTNER

WAN GUARD

Anti-DDoS Services

Piotr Okupski
CEO
ITORO
itoro.com.pl

- **WanGuard** – 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

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 (10/40/100GE) use port mirror.

- Server provisioning and Linux performance tuning
- WanGuard is the most cost-effective volumetric DDoS protection solution for 10–100 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

itoro

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.

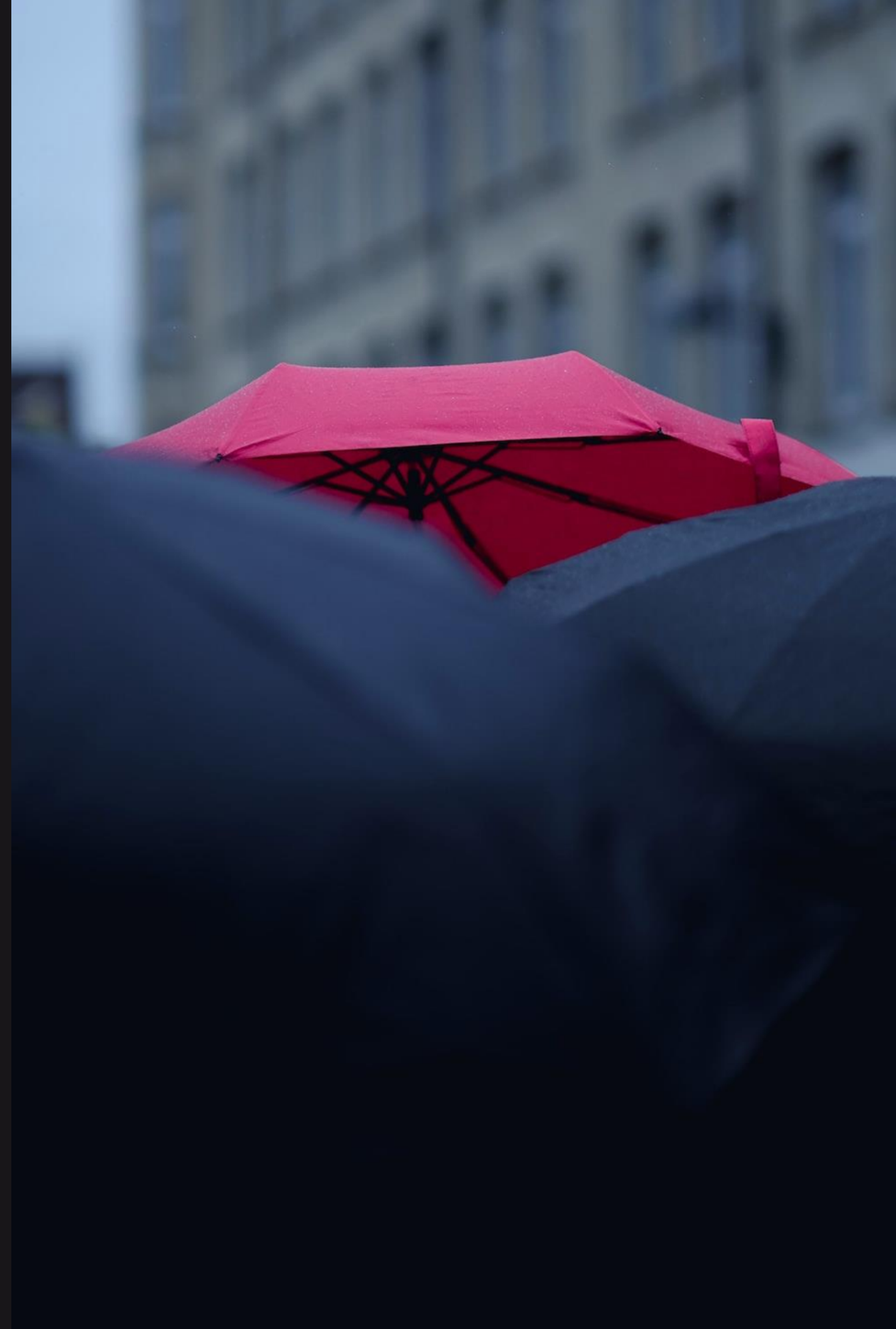
Types of DDoS Attacks Blocked by WanGuard :

Network & Amplification	Application & Protocol	Flood & Volumetric
FRAGMENT, SMURF, SNMP	SIP, NETBIOS, LDAP/CLDAP	UDP/TCP Floods
SSDP, MEMCACHED, CHARGEN	QUIC, INVALID PACKETS	DNS/NTP Flood
SYN-ACK / SYN / ICMP		TCP:NULL, RST, ACK, SYN-ACK, XMAS
		Carpet Bomb — traffic filtering

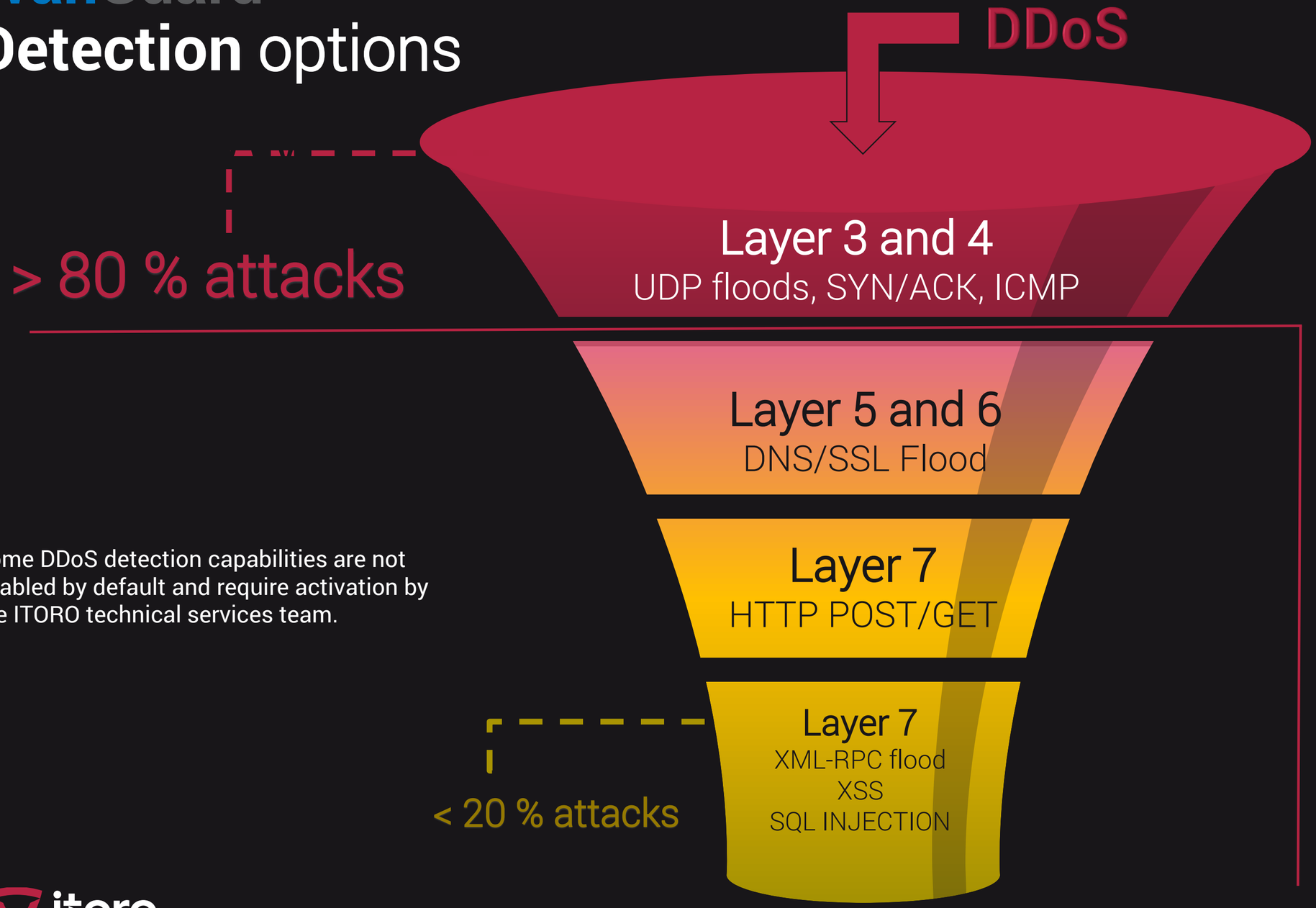
How WanGuard Protects Networks?

- 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.

itoro



WanGuard
Detection options



Some DDoS detection capabilities are not enabled by default and require activation by the ITORO technical services team.

Recognized attacks

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

itoro

WanGuard Detection Speed Advantage over other anti-DDoS systems

Mirror based traffic detection with DPDK technology

- Detection and mitigation: < 5 seconds (Black Hole Routing)
- Detection and mitigation: 15–30 seconds (Traffic filtering)

Other systems (sFlow / NetFlow / IPFIX)

- Detection and mitigation: 35–95 seconds *

* 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).

itoro

WanGuard and Juniper MX routers as a complete protection for DDoS attacks

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 — 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

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

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*

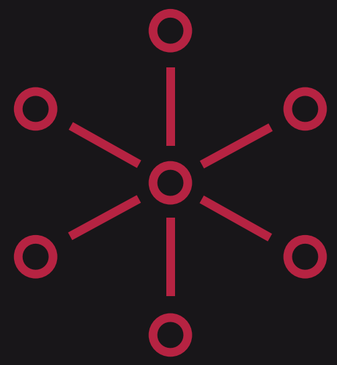
Detects what static filters miss, classifies the attack, and automatically instructs Juniper to block it via BGP FlowSpec.

- 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

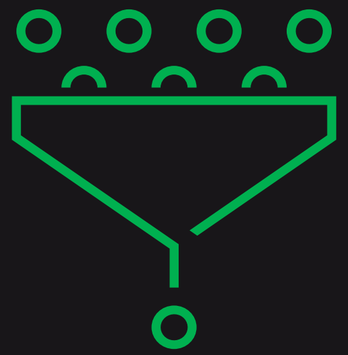
ITORO packages both as a one-time investment — owned, controlled and managed by You.
Together they form a complete, self-defending network — with no need for an external scrubbing center.

itoro

Key Concepts of DDoS mitigation options



Black Hole Routing (**R**emotely **T**riggered **B**lack **H**ole **R**outing)
Block all incoming traffic to the destination IP address.



FlowSpec (RFC 5575)
Instant firewall rules using BGP protocol.
Allows for various actions :

- discard / rate-limit of trrafic
- traffic redirection
- setting DSCP (Differentiated Services) bits to provide QoS or other filtering options

itoro

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.
  It has a much higher bandwidth than the bandwidth available to the end customer.
- The first line of defence 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

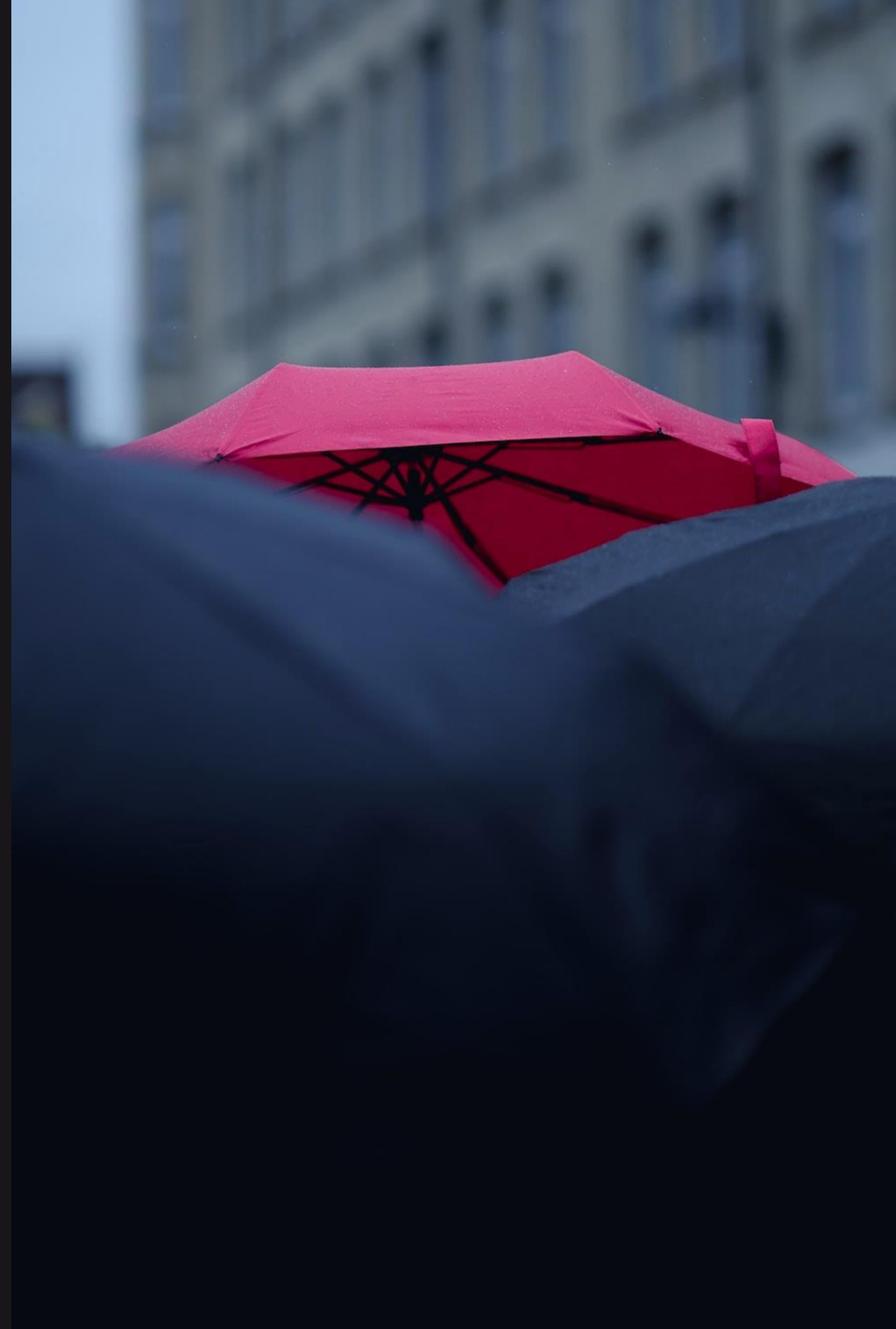
QUIC
INVALID PACKETS
NETBIOS
SIP
LDAP/CLDAP
CHARGEN

UDP/ TCP Floods
TCP:NULL, RST,ACK,
SYN-ACK,TCP-ALL(XMAS)
DNS/NTP Flood

Protection against this type of attack :

- WanGuard generates the appropriate filter rules.

itoro



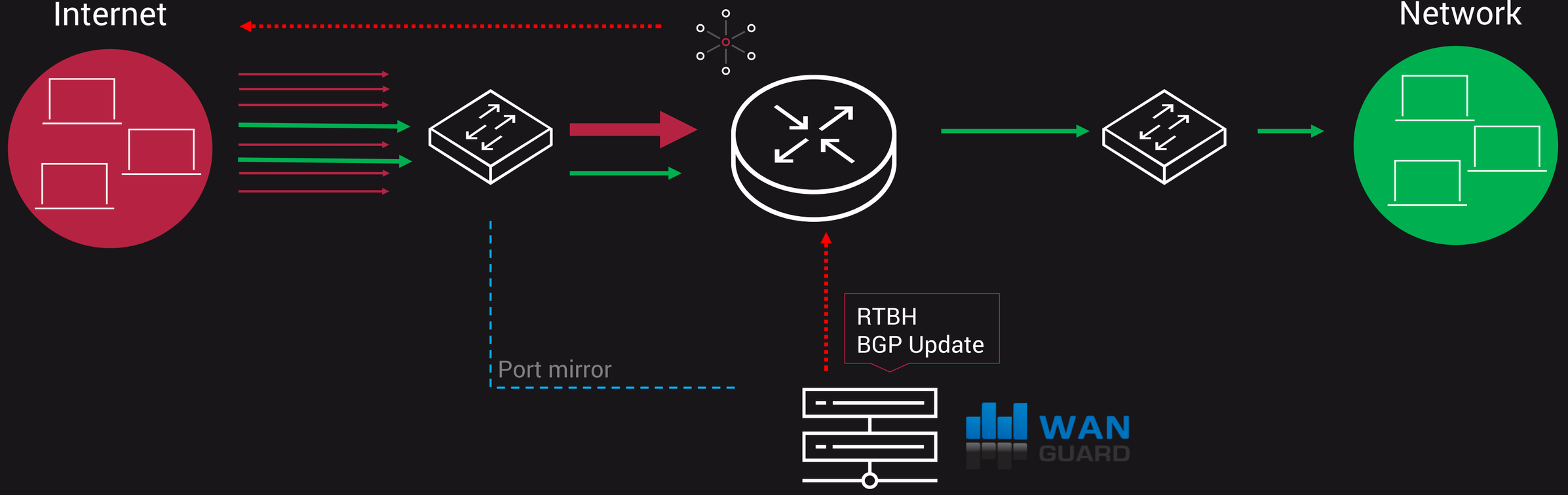
Scope of WanGuard's Basic Protection Deployment - RTBH

1. WanGuard Console and Sensor software installation
2. Installation of Intel/Mellanox network adapter drivers and appropriate netmap/PF_RING/DPDK modules.
3. Tuning of Debian system : CPU Governor, HDD Scheduler, sysctl parameters, GRUB.
4. Installation and configuration of the BGP GoBGP server.
5. WanGuard Sensor configuration and CPU optimization for current traffic levels.
6. Adding Ips advertised by Your AS and transit prefixes, setting DDoS thresholds.
7. Configure email notifications, reports, and alerts from WanGuard.
8. Setting the data retention of data collected by WanGuard.
9. Setting pre-thresholds for blocking traffic with RTBH.
10. Backup of WanGuard system with a copy on the ITORO server (option for all customers with ITORO support packages)
11. Training in system operation and learning attack analysis.
12. Production launch.

itoro

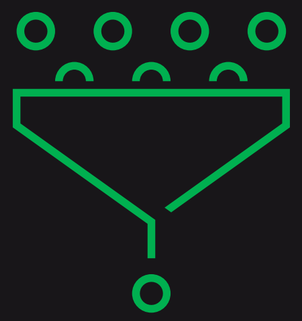
WanGuard with RTBH (Black Hole Routing)

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.



PE Router | Switch | Firewall | FlowSpec | Black Hole Routing (RTBH)

itoro



DDoS traffic filtering

Traffic filtering capabilities :

- BGP FlowSpec filtering on hardware routers (Cisco / Juniper / Arista)
- 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

itoro

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.

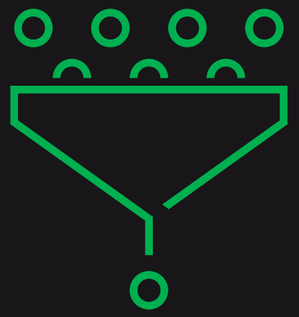
Precise traffic filtering
FlowSpec rules target malicious traffic by IP, protocol, port, and packet characteristics — legitimate traffic passes through unaffected.

Scalability
BGP FlowSpec runs on your existing BGP infrastructure — no dedicated hardware or maintenance windows required for deployment.
Rules can be applied globally or on selected network segments.

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

Easy to manage and deploy
ITORO deploys BGP FlowSpec protection with no maintenance window, meaning zero service disruption during installation.

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

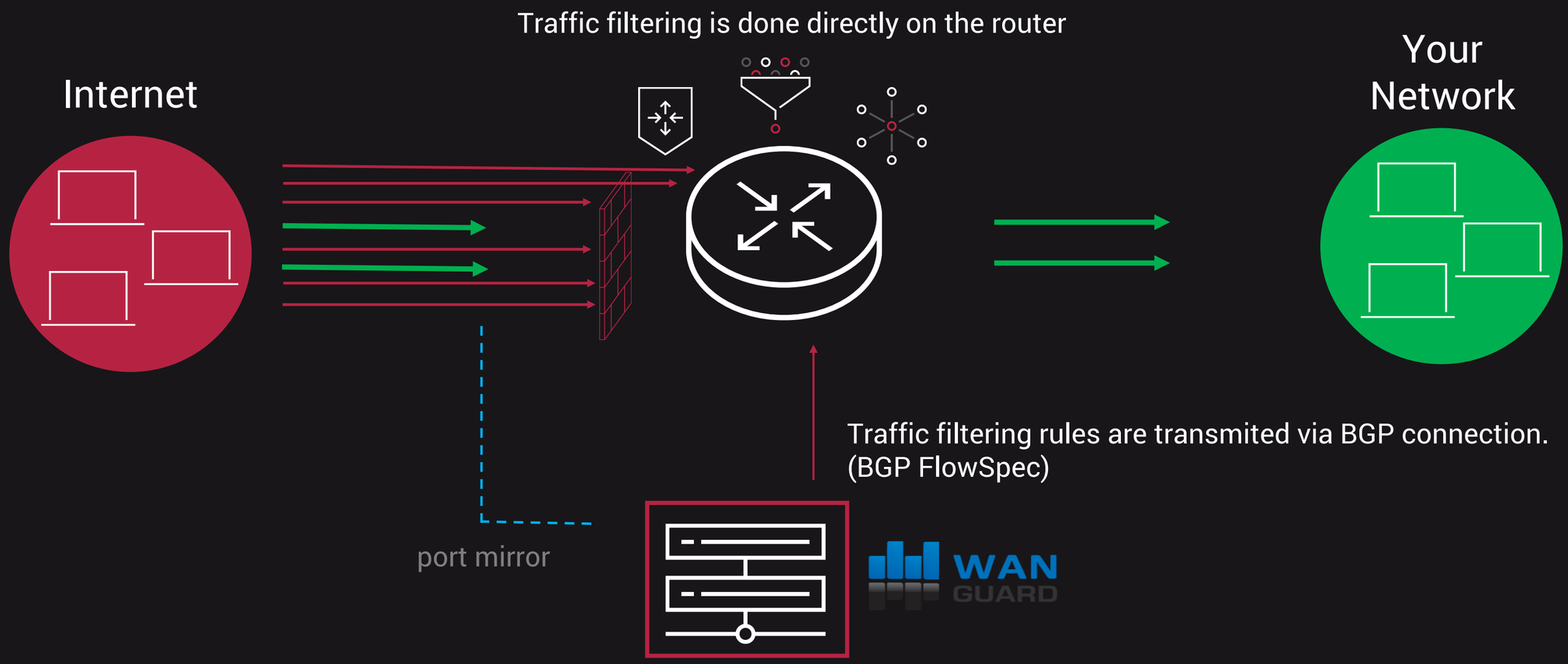
RTBH & BGP FlowSpec Filtering & Traffic Redirection

1. Installation of WanGuard Console, Sensor and Filter software. *
2. Installation of a traffic filtering card for traffic filtering servers.
3. Tuning Debian system : CPU Governor, HDD Scheduler, sysctl parameters, grub.
4. Connection of WanGuard components on the primary server (Sensor/Filter).
5. WanGuard Filter configuration: filtration parameters, additional protection against overflow of links (additional service).
6. Adding client IP classes, setting DDoS attack thresholds.
7. Configuration of the sequence and sequence of events (protection).
8. Set up email notifications, reports, and alerts from WanGuard.
9. Setting initial traffic filtering thresholds (customer consultation required).
10. Script archiving the WanGuard system with a copy on the ITORO server (option for customers with ITORO support packages)
11. Operator training: system operation, alert interpretation, and day-to-day management.
12. Production launch.

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

itoro

WanGuard – Complete DDoS traffic filtering with BGP FlowSpec



Types of DDoS Protection

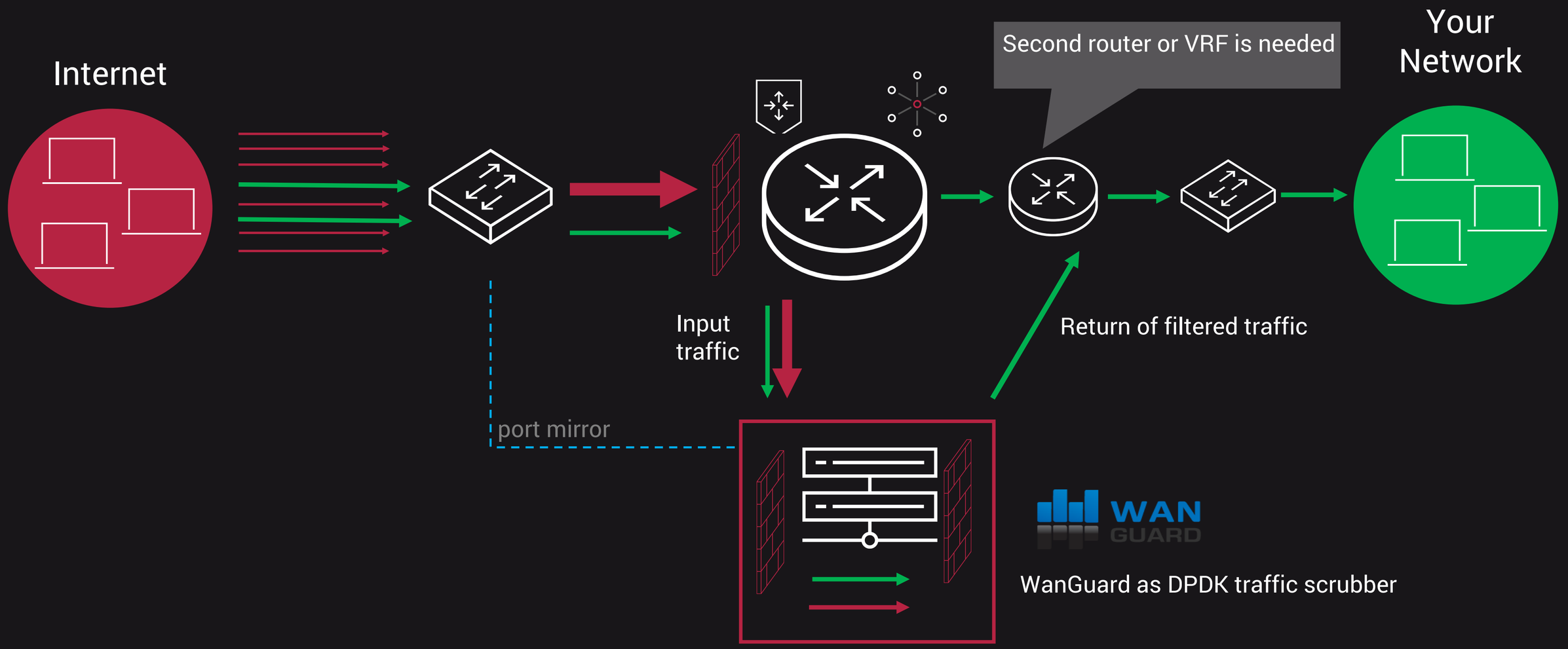
FlowSpec | Firewall | Black Hole Routing (RTBH)

JUNIPER NETWORKS

Router

itoro

Traffic filtering via WanGuard server – 2 stages without FlowSpec



itoro

WanGuard - Example DDoS attack - UDP port 80

Description of the Attack:

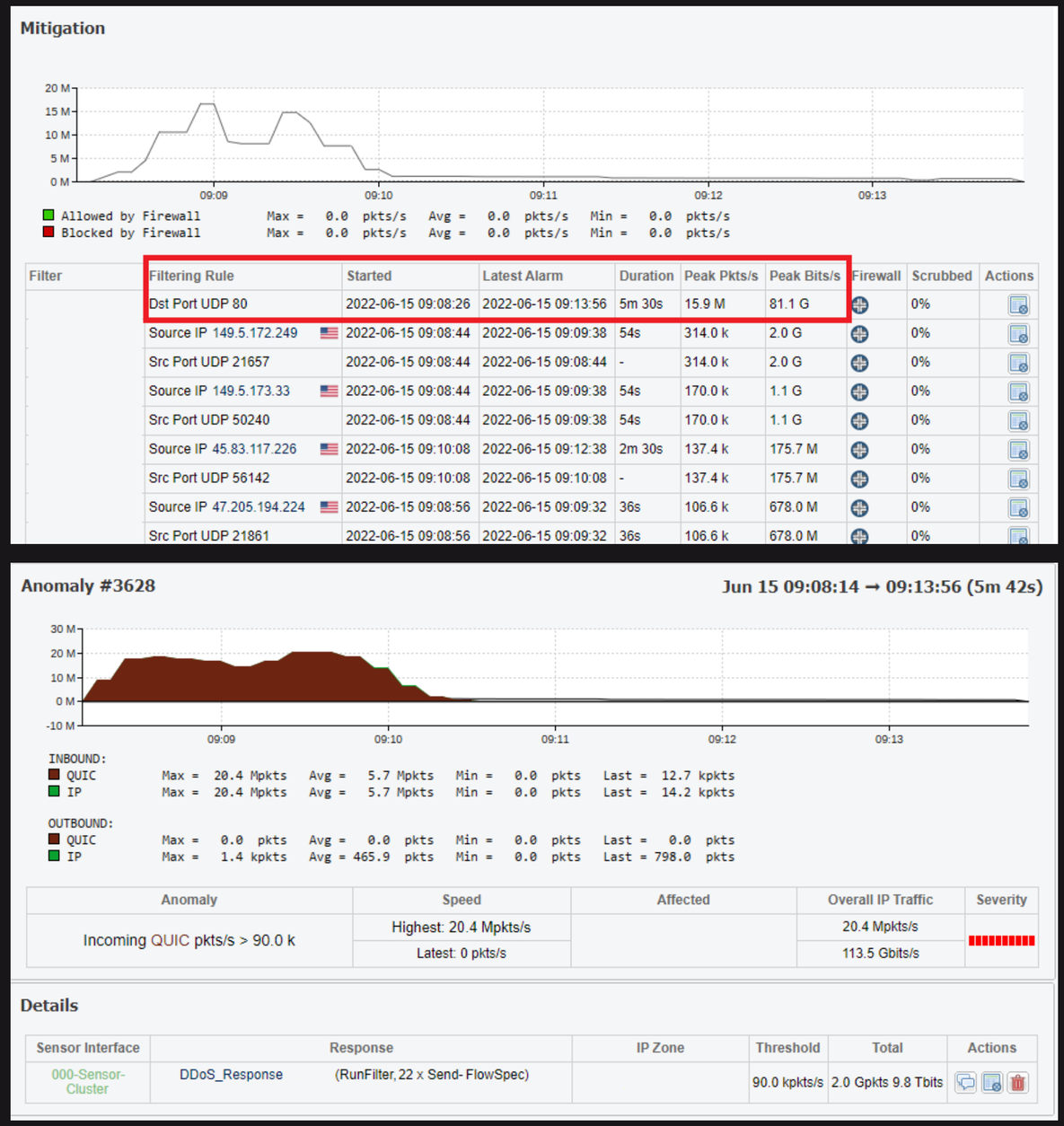
A volumetric DDoS attack targeting UDP port 80, peaking at 113 Gbps with up to 20.4 million packets/second.
The attack was identified as a QUIC protocol flood — a technique increasingly used to bypass traditional UDP filtering due to its resemblance to legitimate HTTPS traffic.

WanGuard System Response:

WanGuard automatically classified the attack and deployed 22 BGP FlowSpec filtering rules within seconds — targeting malicious source IPs and source ports across multiple attack vectors simultaneously.
Rules were distributed via the GoBGP daemon to upstream filtering points.

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

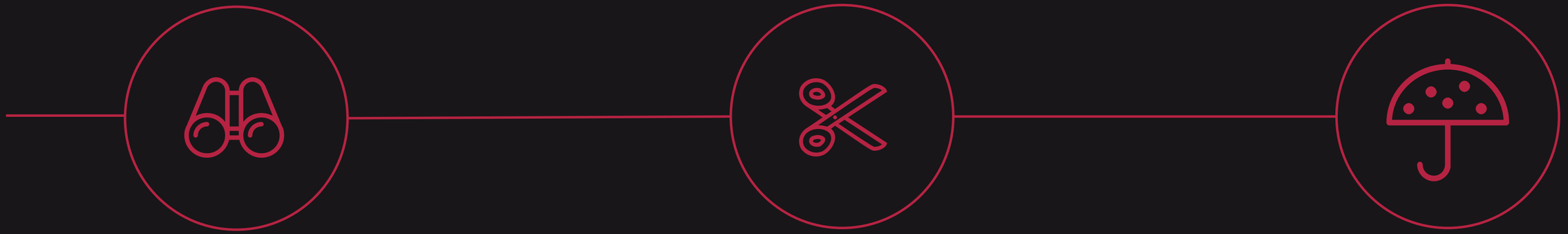
ITORO deployed **WanGuard** with BGP FlowSpec in partnership with ORANGE Poland. Granular filter rules were pushed directly to ORANGE 's upstream routers, scrubbing malicious traffic before it reached the operator's network — eliminating the need for black hole routing entirely.

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.

№ ↓	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	601.3 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	
12790	.68.11	FRAGMENT pkts/s > 50.0 k	76.8 k	<5sec	77.1 k	886.7 M	
12789	.68.12	FRAGMENT pkts/s > 50.0 k	88.2 k	<5sec	88.2 k	1.0 G	
12788	.68.13	FRAGMENT pkts/s > 50.0 k	87.1 k	<5sec	87.1 k	1.0 G	
12787	.68.14	FRAGMENT pkts/s > 50.0 k	81.6 k	<5sec	81.6 k	942.0 M	
12786	.68.15	FRAGMENT pkts/s > 50.0 k	90.8 k	<5sec	91.0 k	1.1 G	

Advantages of DDoS network protection with WanGuard



Visibility

- Full visibility into your network security posture
- Complete control over DDoS protection settings
- Optional customer portal — allows business clients to monitor their own protection status, building service confidence
- Detailed attack history and per-client traffic analytics

Traffic Filtering

- Automatic DDoS detection and filter rule deployment via WanGuard
- BGP FlowSpec support for granular, upstream traffic filtering
- Effective protection for networks of all sizes, including small prefixes
- Industry-leading detection and mitigation response times

Protection

- 24/7 network traffic monitoring
- Detailed DDoS attack reports after each incident
- Dedicated support from the ITORO technical team
- Full remote administration of WanGuard infrastructure by ITORO
- Continuous health monitoring of sensors and servers

itoro

ITORO's offer for Your Network

WanGuard

- 2 x DPDK Sensor and Filter with 2x100GE ports
- RTBH protection
- BGP FlowSpec protection (traffic filtering)
- Traffic redirection to Scrubbing Center (50 Gbps+)

Licenses per server	Wan Sight	Wan Sensor	Wan Filter	DPDK
Interfaces	x	40/100GE	40/100 GE	40/100 GE
Required licenses	x	1	1	1
Sum EUR	€			
Summary	**~ € per year with the ITORO discount**			

Prices are indicative and may vary slightly with EUR/USD exchange rates.
Current prices for the day are available at manufacturer's website.

ITORO optional and additional services	Price
Ready to use BGP FlowSpec configuration	€
NetFlow Archiving Configuration (2-40TB)	**€**

100GE Port Mirror option

- Responsiveness and protection :
  - ✓ RTBH – 5 seconds
  - ✓ Filtering - 15-30 seconds

ITORO Services – Sensor & Filter 2x100GE	Price
ITORO implementation of Sensor & DPDK Filter	€
- Additional 2x100GE Sensor and Filter	€
Training	Included
Technical suport:	
- SILVER support 1 year	€
- GOLD 1 support 1 year	€/month
- PLATINUM support 1 year	€/month
Summary (with SILVER support)	**€**

Offer Summary	Price
ITORO implementation + technical support	€
Licenses (annually)	€
Summary	**€**

Offer is valid for 30 days.

itoro

WanGuard System Architecture

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

1. Management & Control Server

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

2. High-Speed Filtering Sensors *(2 ports × 1-100 Gbps each)*

- DPDK (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

3. Flexible Expansion

- Additional sensors can be integrated at any time without service downtime

4. Optional WanSight License

- sFlow/NetFlow traffic visualisation for reporting, compliance and forensic analysis
- Cost-effective addition for organisations requiring auxiliary monitoring capabilities

5. Training & Optimisation

- Knowledge transfer and onboarding for IT staff
- 30-day calibration period — threshold tuning to refine anomaly detection and eliminate false alarms

Deployment Specifications

- Network Interfaces — Dual 100 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 minimise disruption to legitimate traffic

itoro Support Options

Support tasks / response time	Silver / NBD	Gold / SBD	Platinum / SBD
Email support	✅	✅	✅
Problems and questions related to WanGuard	✅	✅	✅
WanGuard servers and underlying linux problems	✅	✅	✅
WanGuard and System Updates including CVEs	✅	✅	✅
DDoS attack threshold setting recommendations	✅	✅	✅
Backup of WanGuard systems	✅	✅	✅
Analysis and advice on DDoS attacks (minimizing false positives)	✅	✅	✅
Active monitoring of attacks by ITORO		✅	✅
Monitoring of anomalies and system settings every 2 weeks		✅	✅
Customer support and Zoom sessions for technical staff		✅	✅
Direct changes to WanGuard systems by ITORO		✅	✅
Remote monitoring of WanGuard Sensors (always online)*		✅	✅
Full administration of WanGuard systems (outsourcing)*			✅

Still not convinced ?
Let’s meet and talk about it.
Contct us at sales@itoro.com.pl

itoro

Technical attachments

List of attacks which BGP FlowSpec cannot effectively mitigate (block)

TLS / HTTP - Attacks using encrypted traffic — HTTPS Floods & SSL/TLS Exhaustion

- Encrypted DDoS — high-volume HTTPS flood using valid encrypted requests
- SSL/TLS Exhaustion — overloading servers with costly encryption handshakes

⚠ *BGP FlowSpec operates at the packet header level and cannot inspect encrypted payload content — it is unable to distinguish malicious from legitimate traffic inside TLS/SSL tunnels.*

GEO - Geographically Distributed Botnets

- Attack traffic originates from thousands of global sources with no common pattern, IP range or port signature

⚠ *Without common identifiable parameters, FlowSpec cannot generate blocking rules without a significant risk of false positives affecting legitimate traffic.*

Clean DDoS - Distributed attacks with no identifiable header signature

- Botnets using randomised source IPs and ports across thousands of unrelated hosts
- Multi-vector attacks mixing random TCP/UDP/ICMP packets with no consistent pattern

⚠ *BGP FlowSpec requires traceable characteristics — specific ports, protocols or IP ranges — to build effective filter rules. Attacks without a clear signature cannot be reliably blocked.*

Inside / L2 - Attacks exploiting internal infrastructure

- Internal attacks originating from compromised devices within the network
- Layer 2 attacks — ARP spoofing, MAC flooding

⚠ *BGP FlowSpec operates at the inter-autonomous system (BGP/Layer 3) level and has no visibility into Layer 2 traffic or attacks originating inside the local network.*

List of attacks which BGP FlowSpec cannot effectively mitigate (block)

Layer 7 - Advanced Application Layer Attacks

- HTTP/HTTPS floods using legitimate-looking requests
- SQL Injection and XSS — require deep packet inspection of payload content
- Slowloris — slow connection exhaustion using dispersed, low-rate sources

⚠ BGP FlowSpec operates at Layers 3–4 (packet headers only) and cannot analyse traffic content or application behaviour. Attacks that exploit Layer 7 logic will not be detected or blocked.

HTTP – Low-and-Slow Attack Types

- Slow HTTP POST — keeps connections open by uploading data at minimal speed
- RUDY (R-U-Dead-Yet) — exhausts server connection pools using deliberately slow HTTP requests

⚠ *These attacks generate minimal traffic volume and leave no clear header signature. BGP FlowSpec is designed for high-volume traffic blocking – it cannot detect subtle, time-based connection anomalies.*

Clean DDoS - Distributed attacks with no identifiable header signature

- Botnets using randomised source IPs and ports across thousands of unrelated hosts
- Multi-vector attacks mixing random TCP/UDP/ICMP packets with no consistent pattern

⚠ *BGP FlowSpec requires traceable characteristics – specific ports, protocols or IP ranges – to build effective filter rules. Attacks without a clear signature cannot be reliably blocked.*

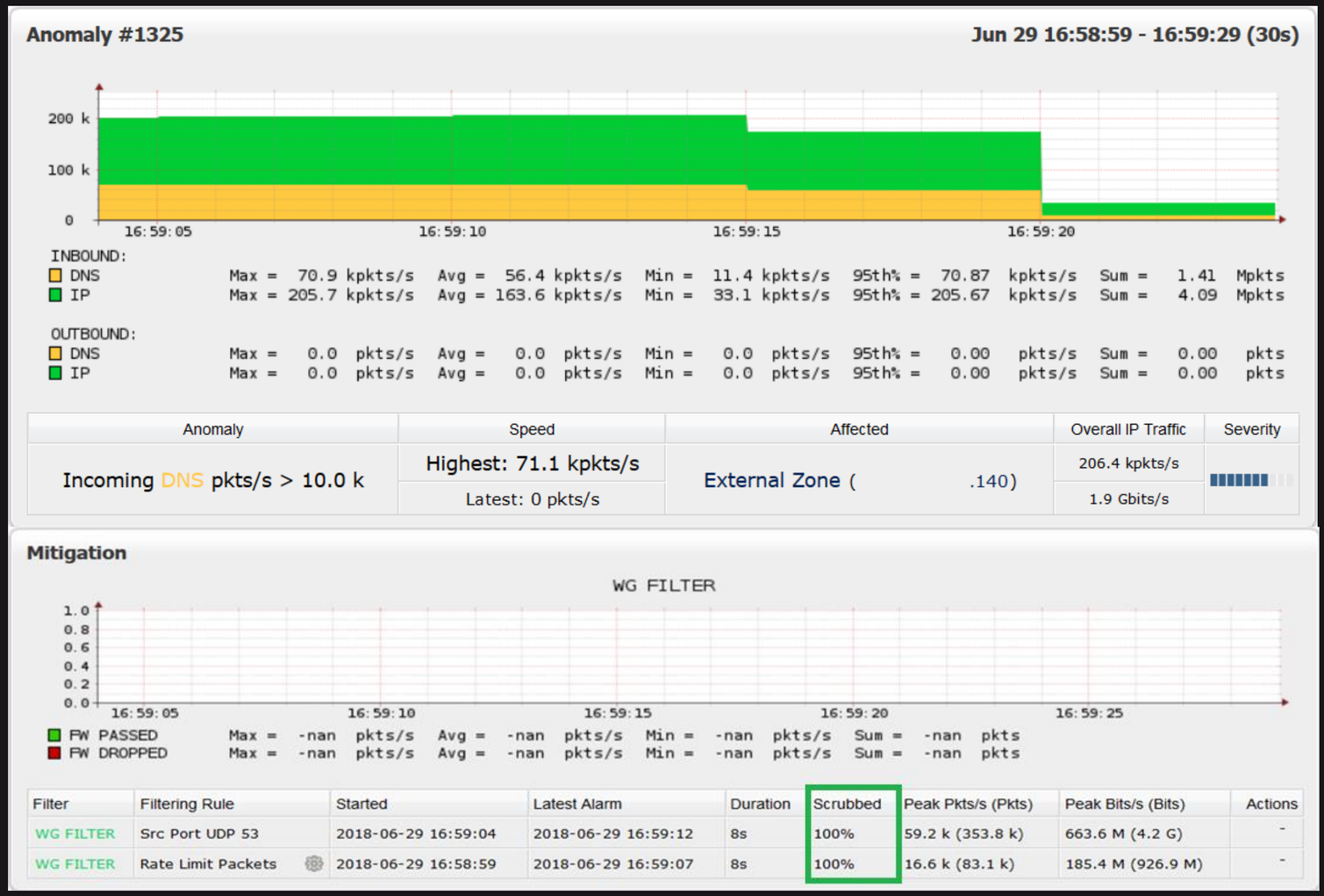
0-Day - Exploit-Based Attacks and Software Vulnerabilities

- Zero-Day Exploits — targeting unknown vulnerabilities in servers or applications
- Buffer Overflow — crashing or hijacking services via malformed crafted packets

⚠ *BGP FlowSpec does not inspect packet payloads or monitor application behaviour. Exploit-based attacks will not be detected or mitigated.*

itoro

WanGuard – Software traffic filtering with DPDK



Information:

In this case, traffic with attack signatures does not reach the WanGuard sensor.
It is blocked on the router with a FlowSpec, so the graph is empty.
In the case of a filtering server, the attack graph is visible, but its performance is much lower.

itoro

FlowSpec filtering on a Juniper router

```
mx80.lab> show firewall filter __flowspec_default_inet__

Filter: __flowspec_default_inet__
Counters:
Name                                            Bytes              Packets
*,*,proto=17,srcport=123                        841816             5234116
```

```
mx80.lab> show route protocol bgp table inetflow.0 extensive

inetflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
*,*,proto=17,srcport=123/term:2 (1 entry, 1 announced)
TSI:
KRT in dfwd;
Action(s): routing-instance DIRTY-VRF,count
        *BGP    Preference: 170/-101
                Next hop type: Fictitious, Next hop index: 0
Next-hop reference count: 1
                State: <Active Int Ext>
                Local AS: 65000 Peer AS: 65000
                Age: 37
Task: BGP_65000.10.0.9.66
                Announcement bits (1): 0-Flow
                AS path: I
                Communities: traffic-rate:0:1875
                Accepted
                Localpref: 100
                Router ID: 10.0.9.66
```

itoro

WanGuard Carpet Bomb Attack

Attack Detection

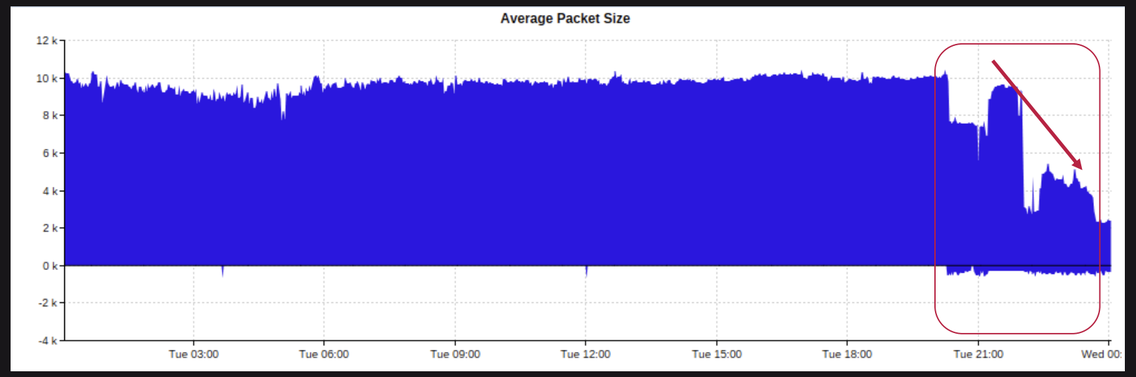
WanGuard detected a volumetric DDoS event saturating the uplink to 7 Gbps, with small packet rate spiking to nearly 1 million packets/second — consistent with a large-scale amplification campaign.

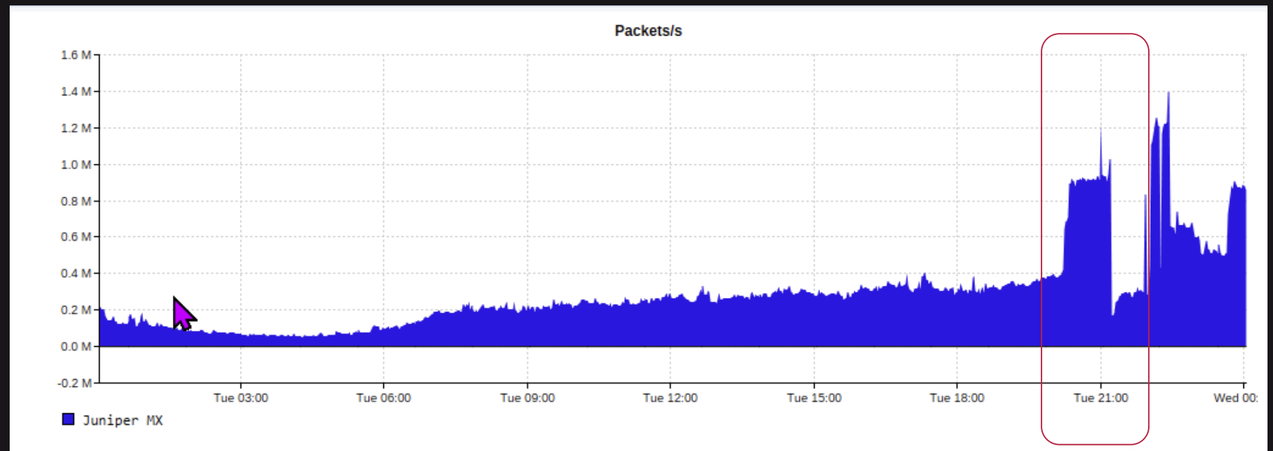
Attack Classification: DNS & NTP Amplification

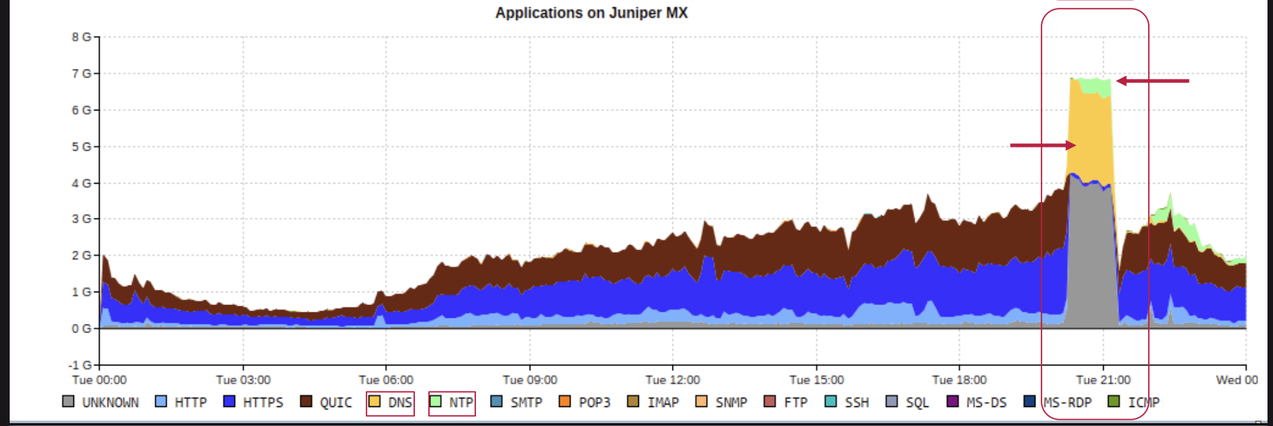
WanGuard identified the attack as a DNS and NTP amplification attack — a reflection-based technique where attackers spoof the victim's IP and send small requests to open resolvers and NTP servers, which respond with traffic up to 50× larger, directed at the target.
The Carpet Bomb distribution was confirmed 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.

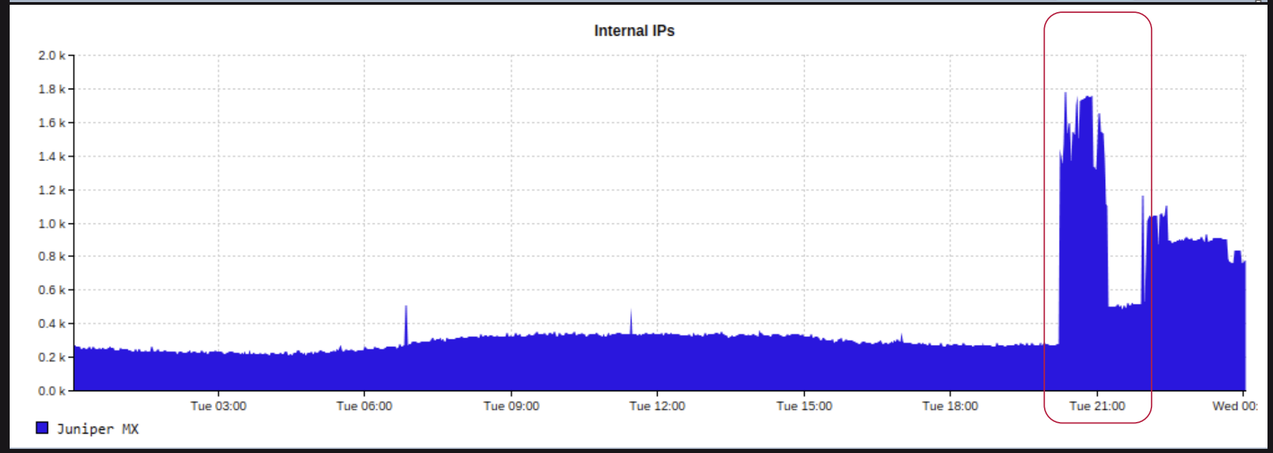
Mitigation

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.
As visible in the graphs, traffic was cut off abruptly once mitigation rules took effect, restoring normal network operation.









itoro