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

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