DDoS Protection: RS40

Enterprise-level DDoS defense built with high-availability design that allows up to four pairs of 10Gbps connections or up to four pairs of 1Gbps connections

Deploy Immediately

Within a few minutes after powering up, RioRey devices begin to filter DDoS attack traffic automatically. Performance is highly reliable and RioRey defense is designed not to drop good traffic even during massive DDoS attacks.

Superior Analytics

Our algorithmic-driven defense focuses on the analytics of network traffic to rapidly identify and mitigate DDoS traffic at line-rate. The RioRey solution means no signatures, no rules, and no waiting.

rWeb Management

rWeb is our best-in-class browser-based management platform that works with all RioRey devices. A single rWeb can manage multiple devices installed in multiple sites. It provides monitoring and reporting of attack traffic with alarms, report summaries, real-time and historic traffic data. Integrate rWeb into security and network operations for data retrieval, automation and configuration by external management and billing systems.

Every year, DDoS attacks are growing in number, severity, complexity, and sophistication. As a result, the fallout from DDoS attacks are even more crippling for businesses, resulting in lost revenue, customers, and credibility. If network or website downtime is not an option, you must have a dedicated DDoS defense strategy.

RioRey is the leader in building the best performing dedicated DDoS defense platforms in the industry for detecting and mitigating DDoS attacks. Our dedicated DDoS defense systems automatically pinpoint and stop attack traffic while allowing legitimate traffic to continue to flow through your network.

The RioRey RS is designed with enterprise-level DDoS defense in mind—flexible deployment configurations addressing needs for multiple 10Gbps links and a filter capacity of up to 40 Gbps and up to 40 million packets per second, and state-of-the-art algorithmic architecture providing fast, automatic protection. Located either at your network's edge for '*always on'* defense, or deployed in a scrubbing center for '*on demand'* protection, the RS40 is the best solution for multiple 10 Gbps protection of your key network assets against even the heaviest of DDoS attacks.

Key Capabilities

High Availability Design. Hardware bypass for all interfaces; No internal moving parts; Redundant hot swap for power supplies; Three redundant hot swap fan modules.

Flexible Deployment Configurations. Up to four pairs of 10G LAN/WAN interfaces, and 10/220V AC and -48V DC power options.

Proven DDoS Detection Algorithms. Protects against all 25 classes of DDoS attacks (including floods and Layer 7 attacks); Detection and mitigation of DDoS is automatic—no "learning period" required or updating signatures; RioRey's algorithmic architecture is designed to avoid false positives while mitigating DDoS attack traffic.

Specification	Specification Detail
Attack Packet Throughput	Up to 40 million packets per second of any mix of DDoS traffic
Attack Blocking Rate	Up to 59.2 million packets per second
Maximum DDoS Blocking Throughput	40Gbps any mix of layer 3-7 attack traffic
Bandwidth Throughput	Field upgradable from 10 Gbps to 40 Gbps via incremental license purchase
VLAN Support 802.1q	Inspects IP payload inside VLAN tags. QinQ supported
GRE Tunnel (Passthrough Tunnel)	Inspects IP payload inside GRE tunnels, tunnel headers are ignored
Jumbo Frames	Supported (RIOS 7.1.5 and forward), up to an MTU of 9216 Bytes
Types of DDoS Protection and Filtering Capabilities	All 25 classes of DDoS attacks (see RioRey Taxonomy). **TCP Based** (*SYN Flood, SYN-ACK Flood, ACK & PUSH ACK Flood, Fragmented ACK, RST or FIN Flood, Synonymous Flood, Fake Session, Half-open Session, Empty Session Attack, Misused Application, Port Scan, Port Sweep)*; **TCP-HTTP Based** *(HTTP Fragmentation, Excessive VERB, Excessive VERB Single Session, Multiple VERB Single Request, Recursive GET, Random Recursive GET, Faulty Application);* **UDP Based** *(UDP Flood, Fragmentation, DNS Flood, VoIP Flood, Media Data Flood, Non-Spoofed UDP Flood);* **ICMP Based** *(ICMP Flood, Fragmentation, Ping Flood)* **Protocol Conformance** *(RFC compliance validation for IP, TCP, UDP, ICMP headers)*
Typical Latency	< 100 µs (micro second)
Maximum Simultaneous Victim IPs	Up to 64,000
Maximum New Connections	12m new connections per second
TCP Connection Limits	16 million concurrent connections per 10G port, up to 64 million total for RS with 4x10GE ports
Detection Time Frame	DDoS detection time is typically 0 - 90 seconds
Mitigation Time Frame	Standard mitigation time is typically 0 - 90 seconds (Force-On Mode may be enabled for even faster mitigation defense against pulsing flood attacks)
IPv4/IPv6 Exception Listing	Global: 250k source white list prefixes, 250k source black and grey list prefixes. Zones support: source white list, source black list, source gray list, 50k destination white list, AS and Country Code blocking
Regular Expression (RegEx)	PCRE regex matching against sample IP packets to enable custom packet matching/blocking
Operating Modes	Each of the 25 classes of DDoS mitigation can be configured to Auto (mitigating), Monitor (reporting only), or Bypass (off)
Interface Types	4 x 10 Gbps single-mode or multi-mode fiber SFP+ interfaces (8 ports total), hardware bypass built in to NIC
SNMP	v1, v2c, and v3. Supports GET and Traps
Alarms	Standard Red/Yellow/Green alarm indicators on rWeb, SNMP traps, SYSLOG and email notification
Management by rWeb	Zone based independent mitigation for up to 5000 zones and 50,000 destination prefixes, network wide management and reporting system, with comprehensive REST API
Power Options	-48VDC or 85 - 240V AC, 50/60 Hz, 350W
Form Factor	2U chassis, fits standard 19″ rack. Dimensions: 3.5″ x 17″ x 17.5"