RE-Series DDoS Protection

RioRey's most cost-effective DDoS defense solution for 1Gbps connections

Deploys 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.

RIOREY

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 RE series are cost-effective options for enterprises with up to 1Gbps connections looking for an entry-level solution. Located at your network's edge for '*always on'* defense, the RE series provides the best in-line DDoS protection of your key network assets.

Key Capabilities

- Filters up to 1.4 million packets per second of any combination of DDoS attack traffic (RE4200)
- Efficient and easy-to-install 1U full length form factor
- Redundant power supplies and fans assure high system availability for reliable DDoS protection (RE4200)
- State-of-the-art algorithmic architecture provides fast, automatic protection 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

Specification	Specification Detail
Packet Throughput	RE2000 - 800kpps, RE4200 - 1.4mpps
Bandwidth Throughput	1 Gbps with two 1Gbps link, configured as WAN - LAN inline filter configuration
VLAN Support 802.1q	Inspects IP payload inside VLAN tags. QinQ supported
GRE Tunnel (Pass through Tunnel)	Inspects IP payload inside GRE tunnels, tunnel headers are ignored
Jumbo Frames	Supported (RIOS 7.1.5 and forward), MTU up to 9018 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)
Max. Simultaneous Victim IPs	Up to 1,000
Maximum New Connections	RE2000 - 800k new connections per second, RE4000 - 1.4m new connections per second
TCP Connection Limits	4 million concurrent connections per 1G port
Detection Time Frame	DDoS detection time is typically 0 - 90 seconds
Mitigation Time Frame	Mitigation time is typically 0 - 90 seconds
IP Exception Listing	Source and Destination IP White and Black lists, AS and Country Code White/Black list support 5,000 source white list prefixes, 5,000 destination white list prefixes, 50,000 source black list prefixes
Regular Expression (RegEx)	PCRE regex matching against sample IP packets to enable custom packet matching/blocking
Operating Modes	Each of 25 classes of DDoS mitigation can be configured to Auto (mitigating), Monitor (reporting only), or Software Bypass (off)
Interface	Copper, single-mode and multi-mode 1Gbps fiber, with built in copper or fiber bypass
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 500 zones and 5,000 destination prefixes, network wide management and reporting system, with comprehensive REST API
Power Options	85 - 240V AC, 50/60 Hz, 200W
Size	1U, 17.2" x 1.7" x 11.3" (437mm x 43mm x 287mm)
Weight	13lbs, 6kg
Operating Temperature	10 to 35°C, 50 to 95°F

Contact **sales@riorey.com** for more information or learn more at **www.riorey.com**.

+1.877.497.0331 United States **+1.240.497.0330** International