DDoS Protection: RE100

RioRey's proven DDoS mitigation technology optimized for 100Gbps and 40Gbps networks.

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.

RIOReY

As ISP costs for 40 and 100Gbps links diminish, so should the cost of protecting networks that run those interfaces. RioRey launched the RE100 to reduce the cost of deploying industry leading DDoS protection on these networks and allow network and hosting providers to offer cost effective, multi-tenant DDoS protection services to their clients.

RioRey is the leader in designing dedicated DDoS defense platforms to automatically detect and mitigate DDoS attacks, relieving businesses of the setup, training and staffing burdens normally associated with solutions in this space.

The RioRey RE100 is designed with provider-level DDoS defense in mind. Flexible QSFP28 configurations allow interfacing with 40Gbps or 100Gbps links and a filter capacity up to 40 or 80 million packets per second (depending on License level) of any mix of DDoS, 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.

Flexible Off-Ramp Options. To enable maximum off-ramp flexibility the RE100 is designed to work our Director netflow detection and redirection engine to effectively mitigate DDoS whenever suspicious traffic is diverted through the RE100, or take escalating actions to route extremely large attack through a cloud scrubbing center.

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.

Specifications

License Version	RE100/40	RE100
Attack Packet Throughput RIOS 8.4 forward	Up to **40** million packets per second Layer 3, UDP and ICMP attacks	Up to **80** million packets per second Layer 3, UDP and ICMP attacks (RIOS 8.4 onwards)
Maximum DDoS Blocking Throughput	40Gbps any mix of layer 3-7 attack traffic	100Gbps any mix of layer 3-7 attack traffic
Bandwidth Throughput	40Gbps	100Gbps (or 40Gbps if using 40Gbps QSFP28)
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 up to an MTU of 9000 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	
New Sessions/Second (TCP)	16 million new connections per second	24 million new connections per second
Concurrent Sessions (TCP)	64 million concurrent connections per 100G port	100 million concurrent connections per 100G port
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: 100k source white list prefixes, 200k source black and grey list prefixes. Zones support: 100k source white list, 200k source black list, source gray list, 200k 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	Off-ramp or in-line. Each of the 25 classes of DDoS mitigation can be configured to Auto (mitigating), Monitor (reporting only), or Bypass (off)	
Interface Types	1 x 100/40 Gbps QSFP28 interface (2 ports). External 1U hardware bypass is optional.	
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 10,000 zones and 100,000 destination prefixes, Network wide management and reporting system, with comprehensive REST API	
Power Options	Dual hot swap power supplies. 85 - 240V AC, 50/60 Hz, 350W or -44VDC to -65VDC / 18A – 10A	
Form Factor	1U chassis, fits standard 19” rack. Dimensions: 1.70" x 17.20" x 19.80". (external bypass is 1U, also fits standard 19” rack)	