

RG10000 – The New Standard In DDOS Protection

- The Fastest, most Powerful DDOS Protection engine in the world today
- The RG10000 series brings 80 high speed CPU cores and 160G RAM to fight DDOS attacks
- 10 GigE with 8 million packets per second (under attack) throughput
- State of the art DDOS algorithm
- The solution for Global 10GigE networks



High Availability Design

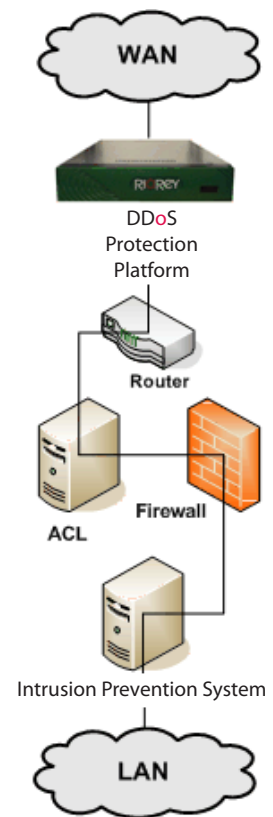
- Eight hot swappable filter blades, load sharing
- Dual Redundant 1:1 hot swappable controller blades
- Quad redundant, hot swappable power supply and fan modules
- Single mode fiber with failover bypass
- 99.999% System availability

Innovative Protection Architecture

- RioRey's platform is placed in front of the router, removing harmful packets before they hit the network
- Protects all network assets against DDOS attacks
- Enables existing network defense elements to function properly even during heavy DDOS attacks

Proven DDOS Detection Algorithms

- Patented algorithms examine packet protocol compliance
- Detection algorithms are independent of human or network behavior related statistics, which are highly unpredictable and unreliable
- Our algorithms examine packet behavior based on IETF and other published application standards. This approach results in very high assurance of passing good traffic



IMMEDIATE • PAINLESS • INTELLIGENT • COST-EFFECTIVE

RG Series Product Specifications (Specifications can change from time to time without notice. Check for the latest update)

	RG10000
Packet Throughput	8 Million Packets per second
Protocol	IP v4, IP v6 Ready
VLAN Support 802.1q	No
Jumbo Frames	No
Types of DDOS Protection and Filtering Capabilities	ICMP, UDP, TCP-SYN, ACK and SYN-ACK, TCP-Session, HTTP, P2P, TCP, UDP & ICMP Random/forged IP address attacks Network scans and port scans Can handle encrypted traffic without need of decoding Combination attacks including: Smurf, Ping floods, Fraggle, Evasive UDP, UDP scans, Pulsing zombie, Tribe Flood Network (TFN), Tribe FloodNet 2K (TFN2K), Stacheldraht, etc.
Typical Latency	< 80µs
Max Simultaneous Victims	1024 (individual victim IP addresses at the same time)
Connections per second	16 million concurrent sessions, no limit on the number of IPs making connection requests
Time to detect DDOS	RG detects and starts to mitigate DDOS attacks in approximately 90 seconds No operator intervention required No network baseline statistics required; the RX is fully functional immediately after installation.
IP Exception Listing	Source and Destination IP white and black lists
Singlemode Fiber Interface	Full duplex, 10GigE-LX, 1310nm, LC connectors, Output power: -10.9dBm min, Input sensitivity: -18.6dBm max. Bypass mode insertion loss: 1.9dB max.
High Availability Mode	Hardware bypass in case of system failures Automatic attempts to restart the system upon failures Ability to fall back to factory defaults
System Availability	99.999%
Attack Records	Retains 10 days of attack records; records can be downloaded for further analysis
SNMP	v1, v2c and v3. Supports Get, Set and Traps
Syslog	Link & configuration status, attack start and stop, victim information
Alarms	Standard Red/Yellow/Green alarm indicators on front panel and on rVIEW Standard dry alarm relay contacts (4 sets of relay outputs) SNMP Traps, SYSLOG and email notification
rVIEW Management Software	Element and cluster of elements manager, allows the manager to configure and monitor the RG Series in real time. Provides detailed statistics and records of network traffic and DDOS attacks.
rVIEW Software Requirement	Windows XP, Vista, Linux and Mac OSX, requires Java 1.5 or later
AC Power Input	Redundant, user replaceable power modules 100V to 240V AC, 50-60Hz, 30 A minimum outlets recommended
Power Consumption	30A at 115V AC, 2.5KW Max
Size	7U, 18.5"W x 29"D x 12.1"H, 470mm x 737mm x 307mm
Weight	85lbs 38 kg
Operating Temperature	0 to 40 °C