RIOREY

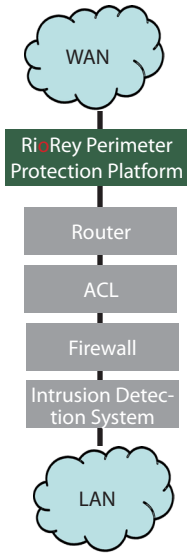
RX TECHNICAL SPECIFICATIONS – JANUARY 2009

Proven DDOS Detection Algorithms

- Patented algorithms examine packet protocol compliance.
- Our algorithms examine packet behavior based on IETF and other published application standards. This approach is independent of human or network behavior, results in very high assurance of passing good traffic.

High Availability Design

- Hardware bypass circuit ensures system protection and 99.999% System availability.
- Two redundant hot swap power supplies.
- Three redundant hot swap fan modules.
- No internal moving parts.



Product Part Number Definition

The RX part number consists of four parts:

RX aa bb c

RX	High availability product series for data center applications	
aa=	12	Low cost platform, suitable for corporate applications
	23	Standard platform, suitable for data centers hosting large number of sites
	44	Special high performance platform, designed for extra high packet rate networks such as interactive games, VoIP and other messaging services.
bb=	10	Copper GigE interface
	11	Multimode SX/LC fiber interface
	12	Singlemode LX/LC fiber interface
c=	U	Filters DDOS attack from the WAN port
	B	Filters DDOS attack from LAN and WAN ports

Example: RX2311U = Standard RX platform with multimode fiber interface and filters DDOS attacks coming in from the WAN port.

FAST • ACCURATE • DEPENDABLE

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

	RX 4400 Series	RX 2300 Series	RX 1200 Series
Packet Throughput	1.4 mpps each direction	425kpps each direction	250kpps each direction
Protocol	IP v4, IP v6(2009)	IP v4	
VLAN Support 802.1q	YES		
Jumbo Frames	No	Yes	
Types of DDOS Protection and Filtering Capabilities	ICMP, UDP, TCP-SYN, ACK, SYN-ACK, FIN/RST, TCP-Session, HTTP, P2P Random/forged IP address attacks Network scans and port scans Can handle encrypted traffic 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	< 70µs		
Max Simultaneous Victims	100 (individual victim IP addresses at the same time)		
Connections per second	No limit on connections or sessions		
Time to detect DDOS	RX 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		
Physical interfaces options	Copper 10/100/1000 CAT5e Multimode fiber gigabit ethernet, 1000Base-SX (850nm), LC/LC connectors Singlemode fiber gigabit ethernet, 1000Base-LX (1310nm), LC/LC connectors		
Copper Interface	10Base-T/100Base-TX/1000Base-T, full and half duplex modes, Auto MDIX selectable		
Multimode Fiber Interface	Full duplex, 1000Base-SX, 850nm, LC connectors, Output power: -10.9dBm min, Input sensitivity: -15.6dBm max. Bypass mode insertion loss: 1.9dB max.		
Singlemode Fiber Interface	Full duplex, 1000Base-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 Compliant with Active-Active HA requirements		
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		
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 and email notification		
rVIEW Management Software	Element and cluster of elements manager, allows the manager to configure and monitor the RX 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		
rCARE Service	An online service from RioRey which allows the administrator to analyze attack trends and to compare their DDOS experience with others in the industry. To use rCARE, the administrator must join the rCARE service and contribute DDOS attack records to our analysis engine. This engine displays the owner's network data, plus anonymous hashed data from all others who contribute.		
rCARE Service Requirement	To join the rCARE service, the network administrator must allow secure access to the RX by the rCARE server, and provide RioRey a <read-only> account on rVIEW. To access data on the RioRey rCARE server, the network administrator needs a web browser, IE6+, Firefox 1.5+, Safari 1.0+.		
AC Power Input	Redundant, user replaceable power modules 100V to 240V AC, 50-60Hz, two 6ft (2m) power cord with standard NEMA 5-15 plug (US) 10 A minimum outlets recommended		
Power Consumption	Max 4A at 115V AC	Max 2.5A at 115V AC	
Size	2U, 19"W x 20"D x 3.5"H, 483mm x 508mm x 89mm		
Weight	32lbs, 15kg	27lbs, 12.5kg	
Operating Temperature	0 to 50 ºC		