RioRey™ Perimeter Protection Platform

(RE500, RE1500, RX1800, RX2300, RX4400 and RG Series)

Security Target

Version 0.9
Jan 16, 2013

Prepared For

RioRey, Incorporated

Prepared By

CYGNACOM SOLUTIONS

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

Table of Tables and Figures

Table / Figure **Page**

1 Security Target Introduction

1.1 Security Target Reference

ST Title: **RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series)**

ST Version: Version 0.9

ST Date: Jan 16, 2013

ST Author: CygnaCom Solutions, Inc.

Please see Table 1-7 for a list of documents used to develop this Security Target.

1.2 TOE Reference

TOE Identification: RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9

TOE Vendor: RioRey™, Incorporated

1.3 TOE Overview

The TOE is RioRey™ Perimeter Protection Platform Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9

The TOE (RioRey™ solution) provides an integrated hardware and software platform to protect Internet Protocol (IP) networks against DDOS attacks by identifying and filtering attacks while forwarding normal traffic through the network without impacting service.

The Platform recognizes an attack, sends an alert for the threat level it poses and ultimately protects the network from harm rapidly and without operator intervention. RioRey's proprietary technology continuously performs Micro Behavioral Analysis (MBA), looking for distinctive characteristics of network communication. Because RioRey's Perimeter Protection Platforms quickly identify traffic that does not follow normal communications protocol, invalid traffic is immediately blocked. Valid traffic flows are unimpeded and normal network communication is maintained. The hardware and software design is dedicated to this single function, the design is also optimized to tackle high throughput, large numbers of sessions and IP address situations.

An enterprise can deploy multiple RioRey appliances. In such scenarios, the same rView software can be used to manage several appliances individually in the same manner. The TOE does not provide hierarchical management of its appliances.

If a hardware failure occurs and the Platform does not repair itself, the Platform goes into a hardware bypass mode. This connects the WAN and LAN ports, physically bypassing the TOE's filtering mechanisms, maintaining all customer traffic flow through the equipment. An administrator can manually configure the TOE into hardware bypass mode as well. Thus, the DDOS filtering function becomes unavailable, but the flow of traffic will not be impeded. In case of a software failure, the multiple watchdogs embedded in the Platform will attempt to restart the Platform and report the incident to the operator. The Platform bypasses customer traffic during the restart phase, maintaining service.

The Platform audits user access events and system processing events (including DDOS attack information) and stores the statistics in RAM for a period of 10 days. The rView Software provides a user friendly way to perform ongoing management of the Platform and obtain Audit information.

This Security Target (ST) defines the Information Technology (IT) security requirements for the TOE. The TOE is being evaluated at assurance level EAL4+.

1.3.1 TOE Type

The TOE is a DDOS mitigation appliance. RioRey's RE/RX/RG Series Perimeter Protection Platform and rView Software package is the network's first line of defense against DDOS attacks.

1.3.2 Hardware/Firmware/Software Required by the TOE

- The RE/RX/RG series models are appliances. All needed Hardware and Software is included in the appliance. No additional Hardware/Firmware or Software is required.
- rView is a Java application that allows an administrator to configure and monitor the Platform in real time. The rView software can run on Windows XP, Vista, Linux and Mac OSX.

  Minimum Requirements for rView running on Windows Machines:

  - Windows XP, Vista, Windows 7 (all editions)
  - 100MB of free hard disk space
  - 1GB of RAM
  - Java JRE 1.6 installed on the windows

  Minimum Requirements for rView running on Linux Machines:

  - Any major LINUX distribution
  - 100MB of free hard disk space
  - 1GB of RAM
  - Java JRE 1.6 installed on the Linux system
  - X-Windows installed on the Linux system

  Minimum Requirements for rView running on MAC Machines:

  - OS X 10.5 or higher
  - 100MB of free hard disk space
  - 1GB of RAM

- Java JRE 1.6 installed on the MAC machines

- A web browser is required for initial Platform configuration
- An application software which controls the serial port, such as HyperTerminal is required to access the Console

1.4 TOE Description

1.4.1 Acronyms

Table 1-1 and Table 1-2 define product specific and CC specific acronyms respectively.

Table 1-1: Product Specific Acronyms

Acronym	Definition
CLI	Command Line Interface
DDOS	Distributed Denial of Service
GUI	Graphical User Interface
JDBC	Java Database Connectivity
HTTPS	Hypertext Transfer Protocol Secure
MBA	Micro Behavioral Analysis
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
XML	Extensible Markup Language

Table 1-2: CC Specific Acronyms

Acronym	Definition
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

1.4.2 Terminology

Table 1-3 defines the product-specific and CC-specific terminology.

Table 1-3: Terminology

Term	Definition
Authorized User	A user who may, in accordance with the TSP, perform an operation.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
Audit Data	The logs generated based on the actions of the TOE itself. This includes the authentication of users accessing the TOE, actions taken directly on the TOE, and actions of the TOE itself. Audit data is a type of TSF data.
User Data	Data created by external IT entities that does not affect the operation of the TSP. User data is separate from the TSF data. The information flows created by Clients and Servers is an example of user Data.
TOE Security Function (TSF) Data	Information used by the TSF in making TOE security policy (TSP) decisions.
External IT Entity	Any IT product or system(s) located in the WAN side of the TOE that interacts with the TOE.
Internal IT Entity	Any IT product or system(s) located in the LAN side of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
Threat Agent	Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.
WAN	Wide Area Network
LAN	Local Area Network
WAN Port	The port that is wired to an external network such as the Internet.
LAN Port	The port that is wired to a Local Area Network.
Filter (Mode)	Filtering will begin as soon as a suspected attack is identified. This is the default setting.
Monitor (Mode)	User will be notified of an attack in progress, but the attack traffic will not be filtered.
Bypass (Mode)	Turns off all detection and filtering operations. This mode is a software level bypass and is not equivalent to the hardware bypass mode under a failure condition.

Term	Definition
TCP SYN Rate Config	Is a set of defined values for the <Per IP SYN Rate Limit>, <Max SYN Rate> and <SYN block minutes>. Based on these values the Platform filters the real time traffic flowing through the Platform. These values should be refined by the operator during an aggressive attack to lower values in order to filter more traffic. * Per IP SYN Rate - source addresses are not permitted to send more than this number of SYNs every minute. If a source address crosses this number, the excess SYNs are dropped. * Max SYN Rate - source addresses sending SYNs at a rate exceeding this number (per minute) will have all of their SYN traffic dropped for a period of time defined by SYN Block Minutes * SYN Block Minutes - source addresses exceeding the Max SYN Rate will be blocked for this amount of time. Under attack, the Max SYN Rate and Per IP SYN Rate can both be stepped down gradually to alleviate excess SYN traffic on a network.
Service Definition	This setting is used to eliminate any traffic that is sent to a generally unused port on a Server. The default entry is: Destination IP = 0.0.0.0, Type = ALL, start port = 0, end port = 65535. This default value allows all traffic through to be passed through the Platform filtering algorithms. If the default line is present, all subsequent lines drop all traffic for the specified IP except for the type and port(s) that are specified in the entry. If the default line is not present, all traffic is blocked except traffic specified in the entries in this table.
Fragmentation Control	This setting is used to manually set fragmentation controls. The amount of fragmented traffic vs. real traffic for TCP, UDP and ICMP can be set. Once the incoming traffic stream exceeds the preset fragmentation percentage, packets will be aggressively examined so that all aspects of the fragment streams are examined, counted and tracked. In addition the product could be configured to enforce RFC 1858.
Per IP SYN Rate Limit	This setting adjusts how many SYNs per minute per source IP are allowed. If the number of SYNs exceeds the number specified, the requests will be dropped by the Platform. If the limit set on the SYNs per IP per minute is set to zero, the function will by disabled, allowing all SYN packets to be passed through.
Max SYN Rate	If a source IP address generates more SYNS at a rate exceeding the max SYN rate specified, the IP address will be temporarily blocked for a specified amount of time.
SYN block minutes	Once an IP address has been placed on the temporary block list established by the max SYN rate, the specified value on the SYN block minutes determines how much time the IP address remains on the blocked list.
Confidence Level	The confidence level reflects the degree of certainty that an attack is being correctly detected. The Confidence Level ranges from 0 (least certain) to 6 (most certain).
Micro Behavioral Analysis (MBA)	RioRey's term for this session examination. The objective of this analysis is to identify invalid traffic, i.e., traffic that does not conform to normal communications protocol behavior. After the first examination, the confidence level will be set to 1. If invalid traffic is detected in a second examination, the confidence level will increase to 2 and so on. A confidence level of 3 triggers the filtering software to start blocking the invalid traffic. If subsequent sessions show the same or higher levels of invalid traffic, the confidence level will increase by one value for each session, up to 6. As the incidence of invalid traffic subsides, the Confidence Level will decrease.

Term	Definition
Pollution Percentage	The entries under “Pollution Percentage” define the amount of pollution for each attack type. The user should be aware that two different sets of parameters are used to calculate the results found in this column, depending on the type of attack listed in column “Type”: − The entries for “ALL” and “TCP” represents aggregate statistics, that is, the sum in bytes of all pollution for all types of traffic divided by the total link capacity in bytes. − For all other attack types, the result is derived by dividing the bytes of invalid traffic by the total bytes of a particular type of traffic on the link.
Whitelists and Blacklist	There are two types of Whitelists and one type of Blacklist contained in the rView software: − destination whitelist (Destination IP Whitelist) − incoming whitelist (Source IP Whitelist) − incoming blacklist (Source IP Blacklist) The Platform only filters incoming traffic, and therefore any information read from packets is from incoming packets. This means that IP addresses read by the Platform to filter packets according to the Whitelists and Blacklists are found only on incoming packets.
Destination IP Whitelist	The Platform will bypass through any traffic that falls into the specifications of the whitelist that are set up in this section, even if the traffic is detected as attack traffic. All packets associated with this destination IP address in this WHITE list is considered good and transmitted. If a white listed IP behaves badly, it will be reported in the attacker list, in either green or gray color on the GUI, but all packets will still be treated as good and transmitted. Each entry in the Whitelist table specifies a pattern of traffic: − Specified destination IP address − Traffic type: ALL, TCP, UDP or ICMP − A range of destination ports, specified by Port Start and Port End
Source IP Whitelist	Defined IP addresses of clients to always send information unfiltered through the Platform. All packets associated with this source IP address in this Whitelist is considered good and transmitted. All information from IP addresses specified in this list will be sent to the host, whether or not the information is valid. It is important to only place clients on this list if they are known to be trustworthy. If a white listed IP behaves badly, it will be reported in the attacker list, in either green or gray color on the GUI, but all packets will still be treated as good and transmitted.
Source IP Blacklist	All packets associated with the IP addresses in this list are assumed to be bad and is blocked by the Platform. Once an IP is put onto the black list, traffic from this IP remains blocked as long as it is left on the list.
Victim History (Log)	Displays the victim history of the last 10 days in a tabular form. This report initially displays the first 1,000 records for the current interface selection. Navigation buttons may then be used to move forward and backward through each set of 1,000 records. When any particular victim is selected by double clicking the row, a window pops up displaying the attacker’s IP address and the port numbers both the attacker and the victim.
Attacker History (Log)	Displays attack history of the last 10 days in a tabular form. This report displays the first 1,000 records for the current interface selection. Users may navigate forward and backward through each set of records. To see information about the number attack packets, filtered packets, total packets, attack bytes, and filtered bytes, hover the cursor over a particular attack.
ADS	Advanced DDOS Scrubber, Automatic DDOS Software protects networks from DDOS attacks while allowing clean traffic to pass through
RIOS	A software bundle that includes all OS files and ADS files that together are required on an RG, RX or RE Hardware device.
System Log	Displays the system log file (/var/log/messages) with Time Stamp, Subsystem that generated the message and Data with information about the auditable event.
BOT/BOTs/BOTNET	They are applications that run automated tasks (in this specific case DDOS attacks) over the Internet.

1.4.3 Description

The TOE is RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9.

The RioRey Platform sits at the perimeter of the network to protect Internet Protocol (IP) networks against DDOS attacks by successfully identifying and filtering DDOS minutes, while forwarding normal traffic through the network. The rView Software manages the Platform and displays detailed statistics and records of network traffic and DDOS attacks.

The Following diagram presents a typical deployment of the RioRey Platform.

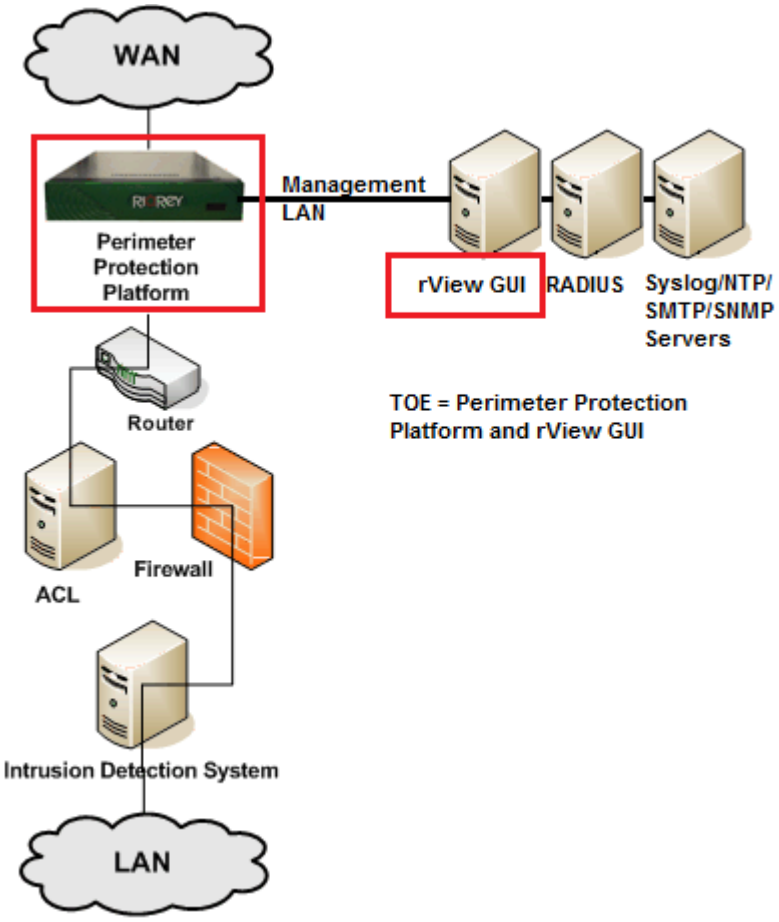

Figure 1: RioRey Deployment

DDOS attacks can be classified as Network Layer or Application Layer attacks. In a Network Layer attack, the attacker floods the victim network with packets of forged random IP addresses. The challenge for the defender with this type of attack is the volume of bad traffic: the defending system must be able to handle millions of incoming IP addresses, sorting out valid packets from attacking packets. Application Layer attacks target specific vulnerabilities in the application layer. The challenge with this type of attack

is that a well-structured attack can so easily look like a legitimate session. An Application Layer attack uses the correct application handshake and establishes proper connections and data request, making the attacker seem like a normal application client. Application Layer attacks are devastating to web services because a small number of attacking BOTS can bring down most small and medium size ecommerce servers.

1.4.3.1 Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series with RIOS Software)

The Platform is a hardware appliance with embedded RIOS software. It is available in RE500, RX1800, RX2300, RX4400 and RG Series. Each series is available with copper Ethernet, single-mode fiber, and multi-mode fiber interfaces.

A hardened Linux kernel is used for the deployed RIOS Software Platform. All Open Source software is in source control of RioRey, Inc. and is compiled by RioRey Inc.

The Platform design is a “smart cable” concept, with the product’s WAN and LAN ports functioning as two ends of an Ethernet cable. The Platform checks for DDOS behaviors in the IP packets traveling through the WAN and LAN ports. The Platform drops the DDOS attack traffic but continues to connect good traffic through the WAN and LAN ports.

The Platform behaves like a cable in that:

- The Platform WAN and LAN ports have no IP addresses.
- DDOS attack traffic is filtered, but good traffic is not modified as it goes through the Platform
- Under failure conditions, such as power loss to the Platform, the Platform maintains all traffic flow with minimal interruption. A brief traffic interruption may be observed as the hardware bypass is activated and the far-side devices re-negotiate or re-connect.

The RE/RX/RG Platform’s key functions are:

- DDOS Protection and Filtering Capabilities
- Auditing of Administrator actions
- Auditing of Attack information
- Provide Operational Management capabilities via rView Software.

The tables below (Table 1-4, Table 1-5 and Table 1-6) present a comprehensive description of the similarities and differences between the Platform types.

Table 1-4: RE Series Product Specifications

	RE 500 Series	RE 1500 Series
Packet Throughput	150 Thousand packets per second each direction	300 Thousand packets per second each direction

Protocol	IP v4
VLAN Support 802.1q	YES
Jumbo Frames	YES
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	< 70µs
Max Simultaneous Victims	1024 (individual victim IP addresses at the same time)
Connections per second	4 million concurrent sessions, No limit on connections or sessions
Time to detect DDOS	Platform detects and starts to mitigate DDOS attacks in approximately 90 seconds No operator intervention required No network baseline statistics required; the Platform 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
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	rView Alarms and email notification, SYSLOG support included
rVIEW Management Software	Element and cluster of elements manager, allows the manager to configure and monitor the Platform 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 ver. 1.6 or later
AC Power Input	Single 100V to 240V AC, 50-60Hz 4 A minimum outlets recommended
Power Consumption	Max 2.5A at 115V AC

Size	1U, 17.2" x 1.7" x 11.3" (437mm x 43mm x 287mm)
Weight	13lbs, 6kg
Operating Temperature	10 to 35°C

Table 1-5: RX Series Product Specifications

	RX 1800 Series	**RX 2300 Series**	**RX 4400 Series**
Packet Throughput	250 Thousand packets per second each direction	425 Thousand packets per second each direction	1.4 Million Packets per second in each direction
Protocol	IPv4		
VLAN Support 802.1q	YES		
Jumbo Frames	YES		NO
Types of DDOS Protection and Filtering Capabilities	ICMP, UPD, TCP-SYN, ACK AND SYN-ACK, 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 FloodNet2K (TFN2K), Stacheldrht, 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.		
Do Not Filter Listing	Provision up to 5000 "do not filter" IP addresses on both WAN and LAN directions for special network requirements		
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		
System Availability	99.995%		

	RX 1800 Series	RX 2300 Series	RX 4400 Series
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		
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 3A at 115V AC		Max 4 A at 115V AC
Size	1U, 19”W x 20”D x 3.5”H, 483mm x 508mm x 89 mm		
Weight	27lbs, 12.5kg		28.5lbs, 13kg
Operating Temperature	0 to 50 °C		

Table 1-6: RG Series Product Specifications

	RG
Packet Throughput	14.5 Million Packets per second
Protocol	IP v4, IP v6(2009)
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	Platform detects and starts to mitigate DDOS attacks in approximately 90 seconds No operator intervention required No network baseline statistics required; the Platform is fully functional immediately after installation.
IP Exception Listing	Source and Destination IP white and black lists

RG	
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
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 1.6 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

1.4.3.2 rView Software

rView is a Java application that provides an interface to monitor attacking traffic, attack alarm notifications, traffic summaries, real-time and historic traffic pollution, and real-time and historic victim lists. It uses the standard secure SSH-2 protocol (included in the TOE) to connect to the RioRey™ platform and can simultaneously manage more than one RioRey™ unit installed on the network. rView is located remotely from the Platform equipment via an encrypted channel (SSH) on the network.

The PC that runs rView must therefore be on a network where TCP Port 8022 access is enabled to the Platform Management Port. Users connect to the Platform series platform by entering the IP address, username and password into the rView login window. At that point a secure connection is established between the PC and the RE/RX/RG Platform. Since each login is independent, multiple users may be signed on to Platforms through the same PC.

The Platform series is self-running and does not require operator intervention to perform DDOS filtering functions. The rView Software displays multiple views of network traffic and DDOS attack statistics.

rView's key functions are:

- Platform configuration
- Monitor audit events (including DDOS attack information)

1.4.4 Data

TSF Data includes information used by the TSF in making decisions. It includes the systems parameters set by administrators to configure the security of the TOE Security attributes, authentication data and traffic control attributes. Examples of TSF Data include administrative roles and audit logging parameters.

User Data includes the Data created by external and internal IT entities that do not affect the operation of the TSP. User data is separate from the TSF data. The information flows created by Clients and Servers are examples of user Data.

1.4.5 Users

Administrators are those privileged users who have access to the TSF Data through the administrative interface component: rView. Access to administrative functions is further restricted by the defined administrative roles (sets of hardcoded privileges):

ADMIN (must access with local authentication only),

NORMAL (can be accessed with local or RADIUS authentication) and

VIEWONLY (local or RADIUS authentication).

1.4.6 Product Guidance

The following product guidance documents are provided with the TOE

Table 1-7: TOE User Guidance Documents

Reference Title	***ID***
Common Criteria for Information Technology Security Evaluation, CCMB-2009-07-002, Version 3.1, Revision 3	***[***CC***]***
RX Series Installation and Initial Configuration Guide	***[***RE-INSTALL***]***
RE Series Installation and Initial Configuration Guide	***[***RX-INSTALL***]***
RG Series Installation and Initial Configuration Guide	***[***RG-INSTALL***]***
RX Series DDoS Defense Settings Guide	***[***RE-ADMIN***]***
RE Series DDoS Defense Settings Guide	***[***RX-ADMIN***]***
RG Series DDoS Defense Settings Guide	***[***RG-ADMIN***]***
rView RELEASE NOTES	***[***RELEASE***]***
RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800,RX2300, RX4400 and RG Series)	***[***ST***]***
Command Line Interface (CLI) for RioRey PPP System	***[***ADMIN***]***

1.4.7 Physical Scope of the TOE

The physical boundary of the TOE is the RE, RX or RG Platform loaded with the RIOS software version 5.0.12sp8 The TOE also includes the rView Software Version 5.0.12sp9 The TOE consists of the RioRey components described in Section 1.4.3. Please see the figure below for an architectural description of the TOE.

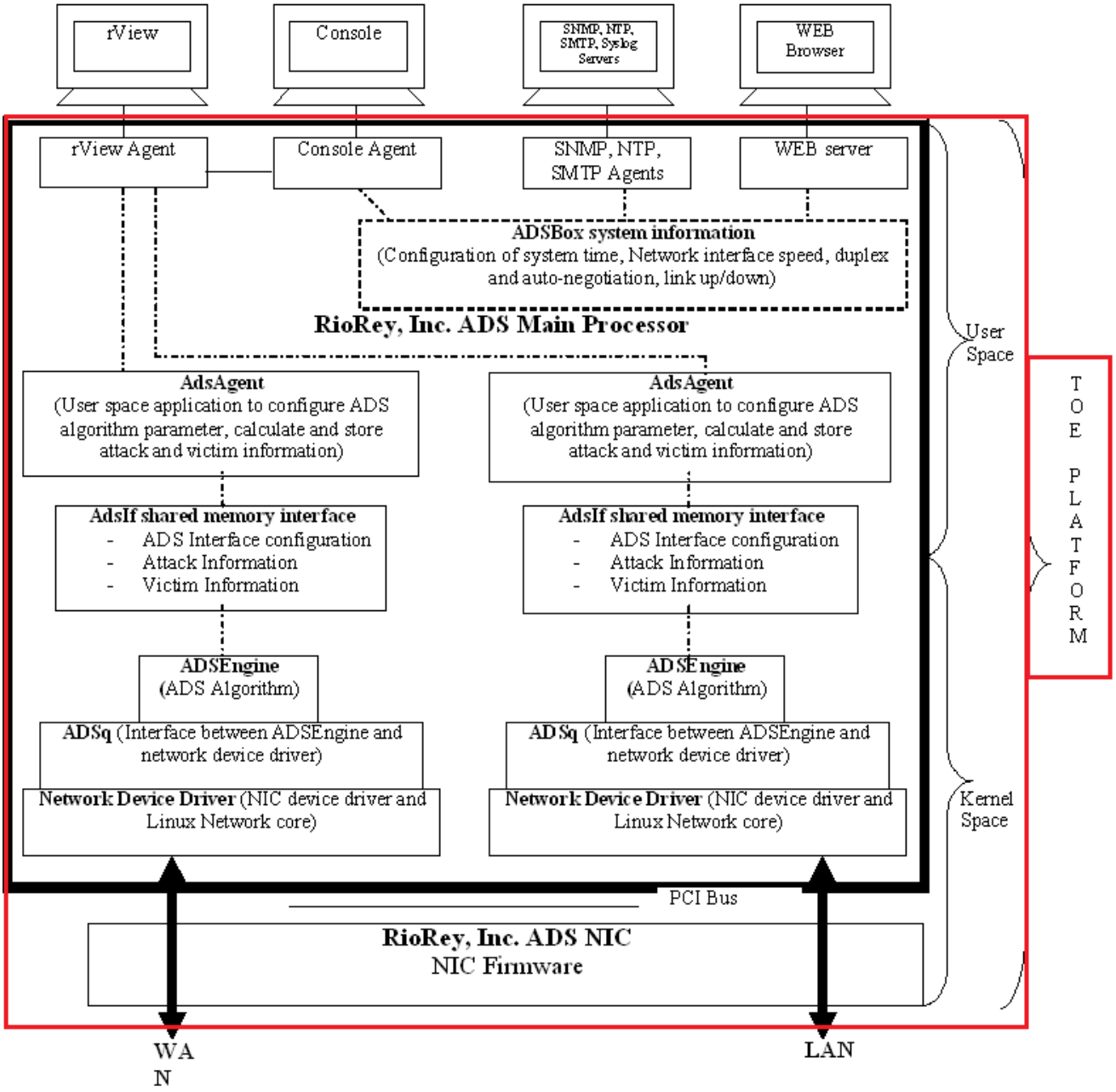

Figure 2: TOE Physical Boundary

The RIOS software is designed to isolate execution code space from incoming packets space. Packets from LAN and WAN are examined by ADS Engine in "near real-time" kernel space and by ADS Agent in the user space. LAN/WAN data packets are treated as "bit and byte patterns" in designated memory spaces and not as data packets. Therefore, these packets are never processed or interpreted by any TCP, UDP or ICMP protocol stacks.

1.4.7.1 Included in the TOE:

The scope of the evaluation includes the following product components and/or functionality:

- RE500, RE1500, RX1800, RX2300, RX4400 and RG Series appliances running RIOS software version 5.0.12sp8.
- rView Software Version 5.0.12sp9

TOE configuration conditions for evaluation:

- Must ensure that the Firewall is enabled and configured on the RioRey™ Perimeter Protection Platform.
- Must ensure that the Firewall IT environment has a NTP server available for the RioRey™ Perimeter Protection Platform to connect and obtain reliable time.
- Must ensure that the IT environment has a NTP server available for the RioRey™ Perimeter Protection Platform to connect and obtain reliable time.
- Separate Ethernet Management LAN is established and restricted to management personnel and security supporting IT infrastructure (external authentication server, syslog server, NTP Server, SMTP server, SNMP server, and rView Host. Monitored traffic does not enter or exit this network interface)

1.4.7.2 Excluded from the TOE:

The following are included in the IT Environment and are not part of the TOE:

- SNMP browser/Server, SMTP Server, NTP Server, Syslog Server and Web browser are not included in the TOE boundary.
- The system hosting the rView application is also part of the IT Environment.

The following RioRey Products/Services are not included in the scope of the evaluation:

- CLI (status, resetpwd, resetip).
- WebUI (deprecated and turned off)

1.4.8 Physical Interfaces

1.4.8.1 Network Interfaces

The RioRey platform is available in Copper and Fiber physical interface configurations. The figures below (Figure 3 and Figure 4) show the typical arrangement on the RX Platform. RE and RG Platforms have similar interface configurations.

- Copper Face Plate Configuration

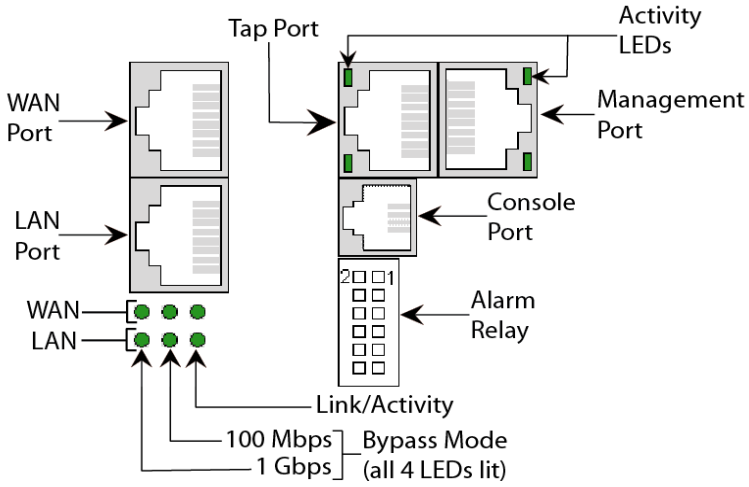

Figure 3: Copper Faceplate Configuration Interfaces

- Fiber Face Plate Configuration

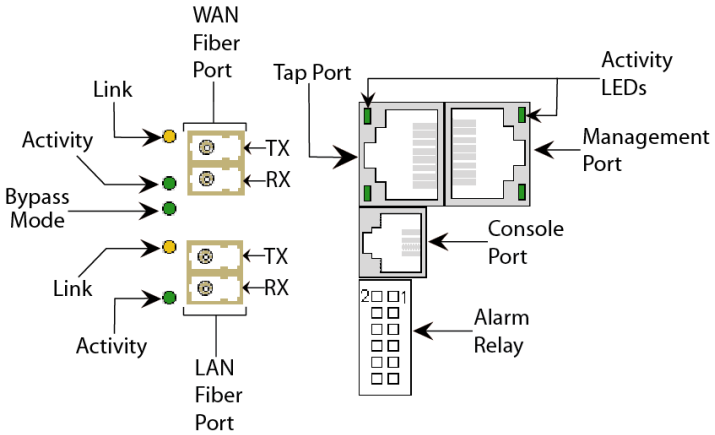

Figure 4: Fiber Faceplate Configuration Interfaces

1.4.8.2 Alarm Relay Interface

The RX family of products has 4 dry-contact relays available on the front panel to indicate the following events:

- Power failure – relay 1
- Critical alarm – relay 2
- Minor alarm – relay 3
- Attack detected – relay 4

By default, the relays are mapped as above, the relay mapping can be changed through the alarm relay configuration screen. Additionally, the maintenance mode can be set on a device, this causes the front panel LEDs to blink, allowing the device to be identified in a data center.

1.4.8.3 LED Interface

The LED interface consists of three different colored LEDs, red, green and orange that can be found on the front of the RX/RE unit and are also reflected in rView. RG models do not have this LED interface. These LEDs indicate current system status including hardware failure, data interface connectivity, system initialization and operation status.

- Flashing Red indicates Internal monitoring system fault
- Solid Red indicates hardware failure such as power supply and number one, two and three fan failure or software not functioning.
- Blinking Orange indicates management interface or/and data interface are disconnected.
- Solid Orange indicates a DDoS attack is happening.
- Flashing Green indicates system is initializing.
- Solid Green indicate system operate normally.

1.4.9 Management Interfaces

The TOE supports a number of management interfaces:

Serial Console- The Platform supports an operator accessible console connection which allows the operator to check the status of the platform, reset the admin password back to the default password, and reset the IP address of the platform back to the default (192.168.1.1). In order to access the console, application software which controls the serial port, such as HyperTerminal, must be used. This interface is out of scope as it should only be used for setup or recovery of the TOE.

WebUI Access using HTTPS- This is a deprecated administrative interface that is now unsupported by RioRey. It is still compiled into the code however it is not started by default.

rView - The rView Software connects to the Platform using the standard SSH protocol via the Ethernet Management Interface (EMI). The EMI is a separate network interface for the establishment of IT supporting environment such as external authentication mechanisms, NTP server, syslog servers, and the PC the runs rView (i.e no monitored network traffic enters or exits this port). This network should be restricted to management personnel only. The PC that runs rView must have TCP Port 8022 access enabled to the Platform Management Port. After successful user login, the default rView screen is displayed. The rView allows an administrator to manage and monitor the Platform, and view other network traffic analysis and attack data collected.

1.4.10 Logical Scope of the TOE

RioRey provides the following security functionality:

- **Security Audit**

  The TOE's auditing capabilities include recording information about system processing and users' access to the TOE. Subject identity (user login name) and outcome are recorded for each event audited. The audit records generated by the TOE are protected by the TOE.

  See the corresponding section in the TSS for more detailed information.

- **Identification and Authentication**

  Each user must be successfully identified and authenticated with a username and password by the TSF or the external authentication mechanism invoked by the TOE before access is allowed to the TSF. The TOE provides a password based authentication mechanism to administrators.

  Access to security functions and data is prohibited until a user is identified and authenticated.

  See the corresponding section in the TSS for more detailed information.

- **Security Management**

  The TOE maintains administrative users with "ADMIN" and "NORMAL" management roles. The TOE also maintains a "VIEWONLY" role for read-only administrative (executive) oversight.

  The TOE allows only authorized users with appropriate privileges to administer and manage the TOE. Only authorized administrators with appropriate privileges may modify the TSF data related to the TSF, security attributes, and authentication data.

  See the corresponding section in the TSS for more detailed information.

- **Resource Utilization (DDOS Protection)**

  The TOE sits at the perimeter of the network to protect Internet Protocol (IP) networks against DDOS attacks by successfully identifying and filtering DDOS attacks, while forwarding normal traffic through the network without impacting service. The TOE can function in FILTER, MONITOR or BYPASS modes. The TOE provides capabilities to filter traffic based on Whitelist, Blacklist, Service Definition, Fragmentation Control and TCP SYN Rate Config specifications.

  See the corresponding section in the TSS for more detailed information.

- **Protection of TSF**

  The TOE transfers all packets passing through the TOE only after processing the traffic based on traffic attributes. If a hardware failure occurs and the Platform does not repair itself, the Platform goes into a hardware bypass mode. This connects the WAN and LAN ports, physically bypassing the TOE's filtering mechanisms, maintaining all traffic flow through the equipment. Thus, the DDOS filtering function may be unavailable, but the flow of traffic will not be impeded. The communication between rView and Platform are protected from disclosure and modification. The TOE provides reliable timestamps with the support of an NTP Server in the IT environment.

  The TSF is protected because the hardware, the OS and the application are part of the TOE and there in a protected physical environment. The logical access to the TOE is controlled by the identification and authentication functionality provided by the TOE.

  See the corresponding section in the TSS for more detailed information.

2 Conformance Claims

2.1 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 4+ from the Common Criteria Version 3.1 R3.

This document conforms to the Common Criteria (CC) for Information Technology (IT) Security Evaluation, Version 3.1, Revision 3, dated July 2009.

2.2 Protection Profile Claim

This ST does not claim conformance to any existing Protection Profile.

2.3 Package Claim

This ST claims conformance to the assurance requirements package: Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.1.

3 Security Problem Definition

3.1 Threats

The TOE must counter the threats to security listed in Table 3-1. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

Table 3-1: TOE Threats

Item	Threat ID	Threat Description
1	T.DDOSATTACK	An External IT Entity or group of External IT Entities may exhaust service resources of the TOE or Internal IT Entities by passing information flows thorough the TOE by DDOS attacks thus making the resources unavailable to its intended users.
2	T.MANAGE	An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE
3	T.PROCOM	An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
4	T.AUDIT	Unauthorized attempts by users and external IT entities to access network resources through the TOE, TOE data or TOE security functions may go undetected because the actions they conduct are not audited or audit records are not reviewed, thus allowing an attacker to escape detection.
5	T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
6	T.FAILURE	A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for the TOE.

3.3 Assumptions

The assumptions regarding the security environment and the intended usage of the TOE are listed in Table 3-2.

Table 3-2: Assumptions

Item	Assumption ID	Assumption Description
1	A.CONNECT	The TOE will separate the network on which it is installed and operates into external and internal networks. Information cannot flow between the external and internal networks without passing through the TOE.
2	A.PHYSICAL	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
3	A.BACKUP	Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.
4	A.NOEVIL	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are listed in Table 4-1.

Table 4-1: TOE Security Objectives

Item	TOE Objective	Description
1	O.DDOSMITIGATE	The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDoS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDoS attacks, and authorized users who may overuse resources.
2	O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
3	O.PROCOM	The TOE will provide a secure session for communication between the User Management GUI on the Management Station and the TOE.
4	O.AUDIT	The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.
5	O.DDOSALERT	The TOE will provide the capability to alert administrators when DDOS attacks are detected.
6	O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.
7	O.FAILSAFE	The failure of the TOE must not interrupt the flow of traffic through the TOE between networks.

4.2 Security Objectives for the Operational Environment

The security objectives for the Operational Environment are listed in Table 4-2.

Table 4-2: Security Objectives for the Operational Environment

Item	Environment Objective	Description
8	OE.CONNECT	Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE.
9	OE.BACKUP	Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost.
10	OE.NOEVIL	Those responsible for the TOE must ensure that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Item	Environment Objective	Description
11	OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
12	OE.TIME	The IT environment must be configured with an NTP server that is able to provide reliable time to the TOE.
13	OE.AUDIT	The IT environment must provide long term storage for audit records and alert data generated by the TOE.

4.3 Security Objectives Rationale

Table 4-3: Mapping of TOE Security Objectives to Threats/Policies

Item	TOE Objective	Threat
1	O.DDOSMITIGATE	T.DDOSATTACK
2	O.MANAGE	T.MANAGE
3	O.PROCOM	T.PROCOM
4	O.AUDIT	T.AUDIT
5	O.DDOSALERT	
6	O.IDAUTH	T.NOAUTH
7	O.FAILSAFE	T.FAILURE

Table 4-4: Mapping of Security Objectives for the Operational Environment to Threats/Policies/Assumptions

Item	Environment Objective	Threat/Policy/Assumption
8	OE.CONNECT	A.CONNECT
9	OE.BACKUP	A.BACKUP
10	OE.NOEVIL	A.NOEVIL
11	OE.PHYSICAL	A.PHYSICAL
12	OE.TIME	T.AUDIT
13	OE.AUDIT	

Table 4-5 shows that all the identified Threats to security are countered by Security Objectives. Rationale is provided for each Threat in the table.

Table 4-5: All Threats to Security Countered

Item	Threat ID	Objective	Rationale
1	T.DDOSATTACK An External IT Entity or group of External IT Entities may exhaust service resources of the TOE or Internal IT Entities by passing information flows thorough the TOE by DDOS attacks thus making the resources unavailable to its intended users.	O.DDOSMITIGATE The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDOS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDOS attacks, and authorized users who may overuse resources.	This threat is mitigated by O.DDOSMITIGATE, which requires that the TOE must limit resource usage to an acceptable level (stop legitimate clients from overusing resources and stop DDOS attacks). The TOE must also be able to serve as a rate based controller and police both malicious users who attempt to flood your network with DOS and DDOS attacks, and authorized users who may overuse resources.
2	T.MANAGE An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete TSF data on the TOE	O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	This threat is mitigated by O.MANAGE, which requires that The TOE must protect stored TSF data from unauthorized disclosure, modification, or deletion.
3	T.PROCOM An unauthorized person or unauthorized IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.	O.PROCOM The TOE will provide a secure session for communication between the User Management GUI on the Management Station and the TOE.	This threat is mitigated by O.PROCOM which requires that the TSF must provide a secure session for communication between the User Management GUI on the Management Station and the TOE, thus protecting the communication between the GUI and the TSF.
4	T.AUDIT Unauthorized attempts by users and external IT entities to access network resources through the TOE, TOE data or TOE security functions may go undetected because the actions they conduct are not audited or audit records are	O.AUDIT The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.	O.AUDIT which requires that the TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding security.
		O.DDOSALERT The TOE will provide the capability to alert administrators when DDOS attacks are detected.	O.DDOSALERT provides the alerting required warning administrators.

Item	Threat ID	Objective	Rationale
	not reviewed, thus allowing an attacker to escape detection.	OE.TIME The IT environment must be configured with an NTP server that is able to provide reliable time to the TOE.	OE.TIME ensure that Reliable time stamps are applied to audit records and allow the reconstruction of a sequence of events at a later date.
		OE.AUDIT The IT environment must provide long term storage for audit records and alert data generated by the TOE.	OE.AUDIT requires that IT environment must provide for the long term audit and alert data generated by the TOE.
5	T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.	This threat is mitigated by O.IDAUTH, which provides for unique identification and authentication of administrative users.
6	T.FAILURE A Hardware, Software and/or Power failure of the TOE may interrupt the flow of traffic between networks thus making them unavailable.	O.FAILSAFE The failure of the TOE must not interrupt the flow of traffic through the TOE between networks.	This threat is mitigated by O.FAILSAFE which ensures that the flow of traffic through the TOE is not interrupted during TOE failure.

Table 4-6 shows that the security objectives for the operational environment uphold all assumptions. Rationale is provided for each Assumption in the table.

Table 4-6: All Assumptions Upheld

Item	Assumption ID	Objective	Rationale
1	A.CONNECT The TOE will separate the network on which it is installed and operates into external and internal networks. Information cannot flow between the external and internal networks without passing through the TOE.	OE.CONNECT Those responsible for the TOE must ensure that the TOE is installed and operated on a network and separates the network into external, internal and management networks. Information cannot flow between the networks without passing through the TOE.	This objective provides for placing the TOE at the network perimeter and ensuring that information flow can not flow between internal and external networks without TOE inspection.

Item	Assumption ID	Objective	Rationale
2	A.PHYSICAL The TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	OE.PHYSICAL Those responsible for the TOE must ensure that the TOE hardware and software critical to security policy enforcement will be protected from unauthorized modification and the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	This objective provides for the protection of the TOE from untrusted software and users. This objective provides for the physical protection of the TOE software.
3	A.BACKUP Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.	OE.BACKUP Those responsible for the TOE must ensure that the audit files, configuration files are backed up and disk usage is monitored to ensure audit information is not lost.	This objective provides for the backup of the TOE audit and configuration files by administrators to ensure data loss minimization due to hardware or software errors.
4	A.NOEVIL There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	OE.NOEVIL Those responsible for the TOE must ensure that there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains and the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	This objective provides for competent and non hostile personnel to administer the TOE. This objective ensures the TOE is delivered, installed, managed, and operated by competent individuals.

5 Extended Components Definition

All of the components defined below have been modeled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding "_EXT" in the component name.

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	FIA_UAU_EXT.2	User authentication before any action
2	FRU_DDOS_EXT.1	DDOS Defense

5.1 FIA_UAU_EXT.2 User authentication before any action

5.1.1 Class FIA: Identification and authentication

See Section 12 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.1.2 Family: User authentication (FIA_UAU)

5.1.3 Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.1.4 Management

The following actions could be considered for the management functions in FMT:

- Management of the authentication data by an administrator
- Management of the authentication data by the user associated with this data

5.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism
- Basic: All use of the authentication mechanism

5.1.6 Definition

FIA_UAU_EXT.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 The TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

5.1.7 Rationale

FIA_UAU_EXT.2 is modeled closely on the standard component FIA_UAU.2: User authentication before any action. FIA_UAU_EXT.2 needed to be defined as an extended component because the standard component was broadened by adding the text *"either by the TSF or by an authentication service in the Operational Environment invoked by the TSF".*

Note: The definition and use of the wording in FIA_UAU_EXT.2.1 was approved by the validation team for FAU_UAU_EXT.2 in a previous CygnaCom evaluation.

5.2 FRU_DDOS_EXT.1 DDOS Defense

5.2.1 Extended Component Definition

5.2.1.1 Class: FRU: Resource Utilization

See Section 16 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3.

5.2.1.2 Family: DDOS Defense (FRU_DDOS)

5.2.1.3 Family Behaviour

This family provides requirements for the availability of network resources in the case of DDOS attacks. The requirements of this family ensure that the TOE will protect networks against DDOS attacks.

5.2.1.4 Management

The following actions could be considered for the management functions in FMT:

- Management of TSF data.

5.2.1.5 Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Detection and Actions taken due to detected potential attacks

.

5.2.1.6 Definition

FRU_DDOS_EXT.1 DDOS Defense

Hierarchical to: No other components.

Dependencies: No other components

FRU_DDOS_EXT.1.1 The TSF shall be able to detect the following type of DDOS attacks

[

Assignment: Types of DDOS Attacks.

]

FRU_DDOS_EXT.1.2 The TSF shall be able to mitigate the detected DDOS attacks.

FRU_DDOS_EXT.1.3 The TSF shall provide the following additional information flow control capabilities

[

Assignment: Additional Traffic Control Capabilities.

]

5.2.2 Rationale

FRU_DDOS_EXT.1 had to be explicitly stated because the CC Part 2 does not have any DDOS mitigation related SFRs that can describe the functions of the TOE. FRU_DDOS (DDOS) is modeled as a Family of the standard class FRU (Resource Utilization) as it is the only class that deals with availability and prioritization of resources.

6 Security Requirements

This section provides the security functional and assurance requirements for the TOE.

6.1 Security Functional Requirements for the TOE

Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 3.1 of the Common Criteria for Information Technology Security Evaluation.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined as:

iteration: allows a component to be used more than once with varying operations;

assignment: allows the specification of parameters;

selection: allows the specification of one or more items from a list; and

refinement: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in ***[italicized bold text]****.*
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *Extended components* defined in Section 5 have been denoted with the suffix "_EXT" following the family name.

The functional security requirements for the TOE consist of the following components taken directly from Part 2 of the CC and the extended components defined in Section 5, and summarized in Table 6-1 below.

Table 6-1: Functional Components

Item	SFR ID	SFR Title
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association
3	FAU_STG.1	Protected audit trail storage
4	FAU_SAR.1	Audit review
5	FAU_SAR.3	Selectable audit review
6	FRU_DDOS_EXT.1	DDOS Defense
7	FPT_FLS.1	Failure with Preservation of Secure State
8	FIA_ATD.1	User attribute definition

Item	SFR ID	SFR Title
9	FIA_UAU_EXT.2	User authentication before any action
10	FIA_UID.2	User identification before any action
11	FMT_SMR.1	Security roles
12	FMT_MTD.1	Management of TSF data
13	FMT_SMF.1	Specification of management functions
14	FPT_ITT.1	Basic internal TSF data transfer protection
15	FIA_UAU.5	Multiple authentication mechanism

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[not specified]*** level of audit; and

c) ***[the following auditable events: events listed in column 3 of Table 6-2]***

Table 6-2: Functional Components

Item	SFR ID	Auditable Event
1	FAU_GEN.1	None
2	FAU_GEN.2	None
3	FAU_STG.1	None
4	FAU_SAR.1	None
5	FAU_SAR.3	None
6	FRU_DDOS_EXT.1	Detection and Blocking of DDOS Attack Traffic
7	FPT_FLS.1	None
8	FPT_ITT.1	None
9	FIA_ATD.1	None
10	FIA_UAU_EXT.2	User login and logout
11	FIA_UID.2	User login and logout
12	FMT_SMR.1	None
13	FMT_MTD.1	Changes to Whitelist Service definition changes Fragmentation Control changes Changes to Blacklist Interface mode changes between filter, monitor and bypass modes. Alarm Relay configuration Changes
14	FMT_SMF.1	All Actions defined in FMT_MTD.1
15	FIA_UAU.5	None

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST: ***[the additional information identified in Table 6-3]***.

Table 6-3: Audit Record Information

Audit Source	Field	Description
System Log	Timestamp	The date and time that the event occurred.
	Subsystem	Name of the internal subsystem that generated the event (e.g. Auth for Authentication subsystem)
	Data	Data with details about the event. (e.g. User admin logged from IP address 192.168.1.1)
Traffic Alarm Summary	Source	Source IP address
	Type	Type of attack detected (e.g. TCP, UDP)
	Severity	Perceived Severity of the attack (Critical (C), major (M), and minor (m))
	Confidence	The confidence level reflects the degree of certainty that an attack is being correctly detected. The Confidence Level ranges from 0 (least certain) to 6 (most certain).
	Pollution %	Amount of pollution for each attack type.
	Timestamp	The date and time that the event occurred.
System Alarm Events	Digit Code	Operational events with the corresponding code.
	Message	These alarms are seen in real time using the alarm relays configured by the user. (e.g. Alarm Relay 3 was set to the ON state)
	Timestamp	The date and time that the event occurred.
Victim Information	Victim IP address	Presumed IP address of Victim
	Attack type	Type of Attack
	Start time	Starting time of Attack
	Duration	Duration of Attack
	Total Packets	Total Packets
	Attack Packets Percentage	Percentage of Attack Packets
	Total Bytes	Total Packets
	Attack Bytes Percentage	Percentage of Bytes of Attack Packets
	Top Attacker (IP/Port)	IP address and Port of Top Attacker
	Dropped Packets	Number of Dropped Packets
	Projected Dropped	Projected Number of Packets Dropped
Attacker History	Attacker IP	Presumed IP address of Attacker
	Attacker Port	Source Port Attacker
	Victim IP	Presumed IP address of Victim
	Victim Port	Port of the Victim
	Attack Type	Type of Attack
	Start Time	Start time of Attack
	Expiring Time	The time duration an attacker IP is kept on the internal filter list
	Packet Length	Length of Packet
	Fragment Offset	For fragmented packets, the Fragment Offset byte in the packet
	Protocol	The protocol used
	TCP Flags	Reports the TCP Flag byte in the attacking packet
	Packet Status	Reports the status byte in the attacking packet
	Extra Info	

Application Note: The "…outcome (success or failure) of the event" will only be included if applicable.

The audit startup and shutdown equate to the system startup and shutdown.

The "type of event" maps to the TOE's "Attack Type" value.

6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***[prevent]*** unauthorized modifications to the audit records in the audit trail.

Application Note: Audit data resides on the TOE Platform and can only be accessed using the management GUI (rView). The TOE does not allow unauthorized modifications to the audit data residing on it through any of its management GUIs. The management GUI does not provide an option for administrators and monitors to delete System Logs, but allows administrators with Admin and Normal roles to delete Victim History Data audit data. The TOE automatically deletes old audit data when audit storage is exhausted. The TOE user is recommended to read the TOE guidance documents to understand the limitations of relying on the storage mechanism on the RE/RX/RG and it is strongly suggested that the user periodically download pertinent attack information to an external memory device.

6.1.1.4 FAU_SAR.1 Audit review

Hierarchical to: No other component

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[successfully authenticated users]*** with the capability to read ***[all audit data]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: Only the Audit data that resides on the TOE can be reviewed by users. Audit data collected by Syslog servers and SNMP servers cannot be reviewed using the local audit review GUI.

6.1.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply ***[searching and sorting]*** of audit data based on

[

All possible combinations of the following fields:

- ***IP Address (Attacker/Victim)***
- ***TimeStamp***
- ***Attack Type***

]

6.1.2 Class FRU: Resource Utilization

6.1.2.1 FRU_DDOS_EXT.1 DDOS Defense

Hierarchical to: No other components.

Dependencies: None

FRU_DDOS_EXT.1.1 The TSF shall be able to detect the following types of DDOS attacks

[

- ***Spoofed IP Attacks***

  Attacks involving

  - ***Forged source IP/port flood attacks using TCP syn, syn-ack, ack, fin, rst, fragmented packets***
  - ***Forged source IP/port flood attacks using UDP, fragmented packets, small, large and random size packets***
  - ***Forged source IP flood attacks using ICMP, fragmented packets, small, large and random size packets***
  - ***Flood with malformed packets***
  - ***Flood packets with private IP per RFC 1918***

- ***Violation of RFC 1858 for fragmented traffic of all types***
- ***Advanced variations of the above floods, making them appear non-spoofed***

- ***Non-Spoofed IP Attacks***

  Attacks involving

  - ***HTTP attacks and variations such as excessive Queries***
  - ***Port 80 based attacks using P2P and other compromised services***
  - ***non-spoofed UDP floods***
  - ***non-spoofed ICMP floods***

]

Application Note: Historically, when DDOS attacks were infrequent events, every new major DDOS attack was studied, characterized and named. The result was an interesting array of DDOS attack names such as Smurf, Teardrop, Fraggle, Stacheldraht and the like. Given the current proliferation of DDOS attacks, however, the labeling of individual attacks is no longer considered informative or productive.

A more effective way to classify DDOS attack is to look at the nature of the packets as they arrive at the victim server. This view is especially useful when there is more than one tool available to generate the same attack. This approach, however, also produces an unwieldy number of attack types than a short list of attack names can capture.

Therefore, RioRey uses a more generic approach to label DDOS attacks in order to capture "classes" of attacks rather than individual types. RioRey uses the Spoofed IP and Non-Spoofed IP classification techniques to sort all DDOS attacks observed on the Internet today. Using these classifications, a Smurf attack, for example, would be grouped into the forged source IP flood attacks using ICMP small size packet. A Teardrop attack would be classified as a TCP fragmented attack.

FRU_DDOS_EXT.1.2 The TSF shall be able to mitigate the detected DDOS attacks.

FRU_DDOS_EXT.1.3 The TSF shall provide the following additional information flow control capabilities

[

Capability to:

- ***function in FILTER, MONITOR or BYPASS modes***
- ***bypass through any traffic that falls into the specifications of the White List***
- ***block traffic that falls into the specifications of the Black List***
- ***filter traffic based on Service Definition specifications***
- ***implement Fragmentation Control over the traffic***
- ***rate limit the traffic based on TCP SYN Rate Config***

]

Application Note: See section 1.4.2 Terminology, for details on FILTER, MONITOR, BYPASS, Whitelist, Blacklist, Service Definitions, Fragmentation Control and TCP SYN Rate Config.

For additional details on description of DDOS attack types and mitigation mechanisms, see Section 7.1.2.

6.1.3 Class FPT: Protection of TSF

6.1.3.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: None

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

[

- ***Power Failure***
- ***Hardware Failure***
- ***Software Failure***

]

6.1.3.2 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from ***[disclosure, modification]*** when it is transmitted between separate parts of the TOE.

6.1.4 Class FIA: Identification and authentication

6.1.4.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

- ***Username***
- ***Password***
- ***Role assignment***

]

6.1.4.2 FIA_UAU_EXT.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU_EXT.2.1 TSF shall require each user to be successfully authenticated either by the TSF or by an authentication service in the Operational Environment invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.5.1 The TSF shall provide ***[Local Password Authentication]*** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the ***[***

Following rules:

- ***Use Local Password Mechanism when enabled (default) AND no external authentication server is configured***

  else

- ***Invoke authentication request to the optionally configured external authentication mechanism***
- ***If external authentication mechanism is offline then all authentication attempts fail***

].

Application Note: The external authentication servers are NOT part of the TOE. The TOE only claims compatibility with RADIUS servers).

6.1.4.4 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles ***[ADMIN, NORMAL, VIEWONLY]*.**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: ADMIN, NORMAL, VIEWONLY roles apply when local authentication is used. NORMAL and VIEWONLY role apply when RADIUS authentication is configured.

6.1.5.2 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to ***[query, modify, delete, and [other operations as specified in Table 6-4]*** the ***[TSF Data as specified in Table 6-4]*** to ***[the role as specified in Table 6-4].***

Table 6-4: Management of TSF Data

Local			**RADIUS***		**Platform Availability**			**TSF DATA**
Admin	**Normal**	**ViewOnly**	**Normal**	**ViewOnly**	**RX**	**RE**	**RG**	
View	View	View	View	View	yes	yes	yes	Interface Status and Statistical Data
Login to another RIOS	Login to another RIOS	Login to another RIOS	Login to another RIOS	Login to another RIOS	yes	yes	yes	none

Logout of another RIOS	Logout of another RIOS	Logout of another RIOS	Logout of another RIOS	Logout of another RIOS	yes	yes	yes	none
Quit Session	Quit Session	Quit Session	Quit Session	Quit Session	yes	yes	yes	none
View all users	View own account only	View own account only			yes	yes	yes	user account attributes
Add, delete, modify, Apply	Modify own password only. Apply	Modify own password only, Apply			yes	yes	yes	user account attributes
Create, Modify, Delete, Apply	Create, Modify, Delete, Apply		Create, Modify, Delete, Apply		yes	yes	yes	Custom Filter Sensitivity parameters
Modify, Apply	Modify, Apply		Modify, Apply		yes	yes	yes	Filter Sensitivity parameters
Create, Modify, Delete, Apply	Create, Modify, Delete, Apply		Create, Modify, Delete, Apply		yes	yes	yes	Custom TCP Syn Rate parameters
Modify, Apply	Modify, Apply		Modify, Apply		yes	yes	yes	TCP SYN Rate Config parameters
Create, Modify, Delete, Apply	Create, Modify, Delete, Apply		Create, Modify, Delete, Apply		yes	yes	yes	Source IP BlackList parameters
Create, Modify, Delete, Apply	Create, Modify, Delete, Apply		Create, Modify, Delete, Apply		yes	yes	yes	Source IP Whitelist parameters
Create, Modify, Delete, Apply	Create, Modify, Delete, Apply		Create, Modify, Delete, Apply		yes	yes	yes	Destination IP Whitelist parameters
Modify, Apply	Modify, Apply		Modify, Apply		yes	yes	yes	Fragmentation Control parameters
Modify, Apply	Modify, Apply		Modify, Apply		yes	yes	yes	Interface Config parameters
Create, Modify, Delete, Apply	Create, Modify, Delete, Apply		Create, Modify, Delete, Apply		yes	yes	yes	Service Definition parameters
Modify, Apply	none		Modify, Apply		yes	yes	yes	Syslog Server parameters
Modify, Apply	none		Modify, Apply		yes	no	no	WAN/LAN Hardware Bypass parameters
Create, Delete, Modify, Apply	none		Create, Delete, Modify, Apply		yes	yes	yes	Configure Firewall parameters
Modify, Apply	none		Modify, Apply		yes	yes	no	Configure SNMP parameters

Modify, Apply	none		Modify, Apply		yes	yes	yes	Email Notification parameters
Modify, Apply	none		Modify, Apply		yes	yes	yes	Configure Interface parameters
Modify, Apply	none		Modify, Apply		yes	yes	NTP ONLY	Date/Time (NTP) parameters
Modify, Apply	none		Modify, Apply		yes	yes	no	Configure Radius parameters
Modify, Apply	none		Modify, Apply		yes	yes	yes	WAN/LAN Link Mode parameters
Modify, Apply	Modify, Apply		Modify, Apply		yes	no	no	Alarm Relays Configuration
Execute Import / Export					yes	yes	yes	System Configuration Parameters and logs
Execute Save Configuration	Execute Save Configuration		Execute Save Configuration		yes	yes	yes	System Configuration Parameters and logs
Install License					yes	yes	yes	none
Execute Update / downgrade RIOS					yes	yes	yes	RIOS - shouldn't be used.
Reboot					yes	yes	yes	none
View	View	View	View	View	yes	yes	yes	Pollution data
View, Clear	View, Clear	View, Clear	View, Clear	View, Clear	yes	yes	yes	Victim History data
View	View	View	View	View	yes	yes	yes	Attacker History data
View Sort	View Sort	View Sort	View Sort	View Sort	yes	yes	yes	rView Log
View, Sort	View, Sort		View, Sort		yes	no	no	System Alarm Events History
Execute Support Upload	Execute Support Upload		Execute Support Upload		yes	yes	yes	none
Execute Traffic Capture	Execute Traffic Capture		Execute Traffic Capture		yes	yes	no	none
View	View	View	View	View	yes	yes	yes	Displays version number
Execute Change Locale	Execute Change Locale	Execute Change Locale	Execute Change Locale	Execute Change Locale	yes	yes	yes	none

* Radius logins are only supported on RX and RE platforms

6.1.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

[

- ***operations as specified in Table 6-4 on the TSF Data as specified in Table 6-4 (See FMT_MTD.1)***

]

6.2 Security Assurance Requirements for the TOE

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 4 augmented (EAL4+) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 6-5.

Table 6-5: EAL4+ Assurance Components

Class	Component	Component Title
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic Flaw Remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample

Class	Component	Component Title
AVA: Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6.3 Security Requirements Rationale

6.3.1 Dependencies Satisfied

Table 6-6 shows the dependencies between the functional requirements including the extended components defined in Section 5. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 6-6: TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	IT Environment*
2	FAU_GEN.2	User identity association	FAU_GEN.1	1
			FIA_UID.1	10 (H)
3	FAU_STG.1	Protected audit trail storage	FAU_GEN.1	1
4	FAU_SAR.1	Audit review	FAU_GEN.1	1
5	FAU_SAR.3	Selectable audit review	FAU_SAR.1	4
6	FRU_DDOS_EXT.1	DDOS Defense	None	None
7	FPT_FLS.1	Failure with preservation of secure state	None	None
8	FIA_ATD.1	User attribute definition	None	None
9	FIA_UAU_EXT.2	User authentication before any action	FIA_UID.1	10(H)
10	FIA_UID.2	User identification before any action	None	None
11	FMT_SMR.1	Security roles	FIA_UID.1	10 (H)
12	FMT_MTD.1	Management of TSF data	FMT_SMF.1	13
			FMT_SMR.1	11
13	FMT_SMF.1	Specification of management functions	None	None
14	FPT_ITT.1	Basic internal TSF data transfer protection	None	None
15	FIA_UAU.5	Multiple authentication mechanism	None	None

* Reliable timestamps for use by the audit functions are provided by the support of an NTP Server in the IT environment (OE.TIME).

6.3.2 Functional Requirements

Table 6-7 traces each SFR back to the security objectives for the TOE.

Table 6-7: Mapping of TOE SFRs to TOE Security Objectives

Item	SFR ID	SFR Title	TOE Security Objective
1	FAU_GEN.1	Audit data generation	O.AUDIT O.DDOSALERT
2	FAU_GEN.2	User identity association	O.AUDIT
3	FAU_STG.1	Protected audit trail storage	O.AUDIT
4	FAU_SAR.1	Audit review	O.AUDIT O.DDOSALERT
5	FAU_SAR.3	Selectable audit review	O.AUDIT
6	FRU_DDOS_EXT.1	DDOS defense	O.DDOSMITIGATE O.DDOSALERT
7	FPT_FLS.1	Failure with preservation of secure state	O.FAILSAFE
8	FPT_ITT.1	Basic internal TSF data transfer protection	O.PROCOM
9	FIA_ATD.1	User attribute definition	O.IDAUTH
10	FIA_UAU_EXT.2	User authentication before any action	O.IDAUTH
11	FIA_UID.2	User identification before any action	O.IDAUTH
12	FMT_SMR.1	Security roles	O.MANAGE
13	FMT_MTD.1	Management of TSF data	O.MANAGE
14	FMT_SMF.1	Specification of management functions	O.MANAGE
15	FIA_UAU.5	Multiple authentication mechanism	O.IDAUTH

Table 6-8 demonstrates that the SFRs meet all security objectives for the TOE. Rationale for each objective is included in the table.

Table 6-8: All TOE Objectives Met by Security Functional Requirements

Item	Objective ID	SFR ID/Title	Rationale
1	O.DDOSMITIGATE The TOE must limit resource usage to an acceptable level (stop legitimate/illegitimate clients from overusing resources and stop DDOS attacks). The TOE must be able to serve as a rate based controller and police both malicious users who attempt to flood the network with DDOS attacks, and authorized users who may overuse resources.	FRU_DDOS_EXT.1	The TOE protect Internet Protocol (IP) networks against DDOS attacks by successfully identifying and filtering attacks, while forwarding normal traffic through the network without impacting service. The TOE could function in FILTER, MONITOR or BYPASS modes. The TOE provides a way to filter traffic based on the specifications of Whitelists and Blacklists. The TOE rate limits the traffic through the TOE based on TCP SYN Rate Config.

Item	Objective ID	SFR ID/Title	Rationale
2	O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrative users, before granting an administrative user access to TOE functions.	FIA_UID.2	All users are successfully identified before allowing any other TSF-mediated actions on behalf of that user
		FIA_UAU_EXT.2	All authorized users are successfully authenticated before allowing any management actions on behalf of that user.
		FIA_ATD.1	User attributes required for authentication are stored by the TOE.
		FIA_UAU.5	Provides for local authentication and the invocation of an external authentication mechanism (RADIUS server)
3	O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_SMR.1 FMT_SMF.1	This objective is met by supporting multiple management roles (FMT_SMR.1) (Admin and Normal) , and ensuring that the TOE security Function data may only be modified by an appropriate administrator (FMT_SMF.1).
		FMT_MTD.1	The TOE allows for the appropriate management TSF data within each Security function (FMT_MTD.1).
4	O.PROCOM The TOE will provide a secure session for communication between the User Management GUI on the Management Station and the TOE.	FPT_ITT.1	The System must protect the collected data from modification and ensure its integrity when the data is transmitted between separate parts of the TOE rView to Platform
5	O.AUDIT The TOE must provide a means to record, store and review security relevant events in audit records to trace the responsibility of all actions regarding	FAU_GEN.1 FAU_GEN.2	An audit record can be generated for security-relevant events and a user/source is associated with the audit events (FAU_GEN.1 and FAU_GEN.2).
		FAU_STG.1	The TOE is able to protect audit records stored internally.
		FAU_SAR.1	The TOE provides the ability to review and manage the audit trail of the system .

Item	Objective ID	SFR ID/Title	Rationale
	security.	FAU_SAR.3	The TOE is capable of providing searching and sorting capabilities of the audit records. The TOE is capable of providing selection capabilities for auditing to include or exclude auditable events from the set of audited events
6	O.DDOSALERT The TOE will provide the capability to alert administrators when DDOS attacks are detected.	FAU_GEN.1 FRU_DDOS_EXT.1 FAU_SAR.1	The TOE is capable of generating audit records based on combination of DDOS detection algorithms. The TOE is capable of providing the capability to review the generated audit records in a suitable manner.
7	O.FAILSAFE The failure of the TOE must not interrupt the flow of traffic through the TOE between networks.	FPT_FLS.1	FPT_FLS.1 ensures that the TOE preserves a secure state when there is a hardware, software or power failure.

6.3.3 Assurance Rationale

Evaluation Assurance Level 4 (EAL) 4+ was chosen because it provides appropriate assurance measures for the expected application of the product. EAL4+ ensures a product is methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It also requires a moderate to high level of independently assured security. The security assurance requirement AVA_VAN.3 includes an independent vulnerability analysis demonstrating resistance to penetration attackers with an attack potential of Enhanced-Basic.

As appropriate for selection of EAL4+ for the expected uses of the TOE, some confidence in correct operation is required, but the threats to security are not viewed as serious. Independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

Augmentation with ALC_FLR.1 adds some assurance about the vendor's ability to perform flaw remediation over the life of the product. This will be important to many customers.

7 TOE Summary Specification

Section 7 describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 1.4.10 Logical Scope of the TOE.

The following sub-sections describe how the TOE meets each SFR listed in Section 6.

Table 7-1: Security Functional Requirements Mapped to Security Functions

Security Class	SFRs	Security Functions
Security audit	FAU_GEN.1	SA-1
	FAU_GEN.2	
	FAU_STG.1	SA-2
	FAU_SAR.1	SA-3
	FAU_SAR.3	SA-4
Resource Utilization (DDOS Protection)	FRU_DDOS_EXT.1	DDOS-1 DDOS-2
Protection of TSF	FPT_FLS.1	FPT-1
	FPT_ITT.1	FPT-2
Identification and authentication	FIA_ATD.1	IA-1
	FIA_UAU_EXT.2	IA-2
	FIA_UID	
	FIA_UAU.5	
Security Management	FMT_SMR.1	SM-1
	FMT_MTD.1	SM-2
	FMT_SMF.1	SM-3

7.1.1 Security Audit

7.1.1.1 SA-1: Audit Generation

(FAU_GEN.1 and FAU_GEN.2)

Audit records are generated within the TOE by the TSF for the events listed in FAU_GEN.1. Audit records contain a timestamp, the information of the entity triggering the event (e.g. username, IP address of subject (Attacker/Victim)), and a summary of the event as well as the additional information listed in Table 6-2 and Table listed in Section Table 6-3.

The System Log, Traffic Alarm Summary, System Alarm Events, Victim Information and Attacker History are all stored in the Platform's RAM for a period of 10 days. The TOE loses these logs when power is turned off or the TOE's software is rebooted. The TOE allows an administrator to download these logs to the system running rView software for persistent storage.

There is no separate startup/shutdown of audit as it is all part of the TOE's startup and shutdown procedures. The startup and shutdown of the system is audited.

7.1.1.2 SA-2: Audit Protection

(FAU_STG.1)

The TSF protects the stored audit records on the TOE from unauthorized deletion and modifications via the TSFI. The TSF retains log files on the local system (System Information and Attack Information).

The RX/RE/RG Platform is designed to keep up to 10 days of records. The TOE uses RAM storage space to record auditable events as they are happening. Once every hour the audit records are copied down from the RAM onto the flash memory for storage for up to 10 days storage. Therefore, worst case scenario could be 1 hour of data lost in the event of a power failure. If the syslog server has been set up then the only records loss would be those be transferred to the syslog server at the time of power loss (at most 1 to 2 records).

Both System Log and Attack Information can be viewed using the rView GUI. The management GUI does not provide an option for administrators to delete System Logs, but allows administrators with Admin and Normal roles to delete Victim History Data audit data. The TOE automatically deletes old audit data when audit storage is exhausted.

When the maximum allowed size of a log file is reached, the log file is rotated and the next log file is created by overwriting a previous log file.

The TOE provides options for administrators to configure SNMP and/or Syslog servers for long term storage of log messages. Once syslog/SNMP has been configured the TOE will automatically send syslog/SNMP trap messages to the respective servers to inform them of internal status changes and various events, for instance DDoS events like the beginning or the end of a DDoS attack, etc. It is highly recommended to use the syslog/SNMP option to minimize loss of audit data as the records are sent as they are created.

At a minimum, the RioRey administrator should manually download these logs at least once a week using the rView software for persistent storage to ensure no loss of audit.

7.1.1.3 SA-3: Audit Review

(FAU_SAR.1)

From the administrative interface available through the rView, an authorized user can read all the audit data generated. All audit records are displayed in a manner suitable for the user. Only Audit data that resides on the TOE can be reviewed by successfully authenticated users. Audit data collected by Syslog servers and SNMP servers cannot be reviewed using the local (rView) audit review.

7.1.1.4 SA-4: Selectable Audit Review

(FAU_SAR.3)

The TSF is able to perform searches and sorting of stored audit data based on various criteria and logical relations specified by an authorized administrator. At a minimum searching and sorting of audit data can be based on the presumed IP address of the Subject (Attacker/Victim), Attack Type and Timestamp (Date and Time).

7.1.2 Resource Utilization (DDOS Protection)

The TOE uses three general notions of *lists*:

1. A *Black List* for manually designating a certain IP as bad. This is a persistent classification and the RioRey detection and filter algorithms will consider all IP addresses on this list as permanently bad. The black list is created manually by the user either by entering addresses by hand into the "Source IP Blacklist" tab under the "Interface Configuration" menu (Select WAN under Sensor Network > Management dropdown > Interface Configuration) or by clicking the "Permanently Block Selected IPs" button with a line selected in the 'Attacker List'. The user can view these blacklisted addresses in the "Source IP Blacklist".

2. A *White List* for manually designating a certain IP to be always trusted. This is a persistent classification and the RioRey detection and filter algorithms will consider all IP addresses on this as permanently good. The white list is created manually by the user either by entering addresses by hand into the "Source IP Whitelist" tab under the "Interface Configuration" menu(Select WAN under Sensor Network > Management dropdown > Interface Configuration) or by selecting the "Unblock Selected IP address" button with a line selected in the 'Attacker List'. The user can view these whitelisted addresses in the "Source IP Whitelist".

3. A *Filter list* for algorithmically generated list (not manually generated) where one or more of RioRey's algorithms determine if an IP or FLOW is currently bad. Depending on the nature of the attack (that is, the magnitude of threat it poses), some attacks are designated as all bad traffic and therefore all traffic from the offending IP is filtered. For other attacks, where an attacking FLOW can be identified confidently, the TOE will designate a FLOW in this filter list to be filtered. All entries in the Filter list have an expiration time associated with it. By default, most expiration times are in the range of 2 to 10 minutes depending on the nature of the attack. However, there are certain attacks where the operator can control a specific expiration time which can be set anywhere between 3 minutes to a year. The filter list is internal to the unit and is exposed to the customer by way of the attacker list.

All packets entering the Platform are first screened and marked for invalid IP, malformed packets, bad checksums and private IP spaces before any other logical tests are applied. This ensures offloading of illegitimate packets without further burdening computing resources in the system.

Next the TOE's DDOS algorithms proceed to examine the packets and decide if the entries need to be added into the Filter List. When a packet is ready to exit the Platform, they are now checked against the Black, Filter and White lists, and the following actions are taken:

a) Any packets not matching any Black or Filter lists are allowed through, and

b) any packets matching a White list are allowed through.

7.1.2.1 DDOS-1: DDOS Protection Mechanisms

(FRU_DDOS_EXT.1.1 and FRU_DDOS_EXT.1.2)

DDOS Protection Algorithms Description

Spoofed IP Test:

An IP distribution test algorithm is applied to all packets. This algorithm maps the source/destination IP and ports to observe changes in client distribution. This IP distribution analysis is the *core algorithm* used to detect spoofed IP attacks. By observing the entropy in the source/destination IP and ports, the following can be trapped

a) Spoofed IP attacks that uses fully random IP source range, and

b) a Spoofed IP attack that only use a limited range of source IP address.

This IP distribution algorithm is equally effective for all modes of attack including TCP and its variations--ICMP and UDP attacks. Any IP that failed a spoofed IP detection algorithm are entered into the Filter List.

Responsiveness Test:

For TCP traffic, packets are further screened for responsiveness. This allows further tuning of spoofed IP TCP packets to calibrate the filter scope down to a particular flow. This additional filter, allows further narrowing down to a per flow filtering, which means an “innocent” computer that has been compromised as a Bot, can also be a source of legitimate traffic that will be allowed to enter the network.

Fragmentation Test:

All fragmented packets are counted and traced to assure that they are valid fragments. These are checked against RFC1858 as well as packet payload randomness checks and a number of tests for reasonable fragmented packet characteristics.

Payload Randomness Test:

All UDP, ICMP and fragmented packets are subjected to a reasonable payload randomness tests. These checks are designed to identify if packets are generated by random generator or by sending a segment of memory in the Bot's RAM or disk. This test is targeted at large payload attacks as well as fixed payload size attacks.

TCP Session Checker Test:

For TCP attacks, a special state analysis is performed on the incoming packets. This analysis detects excessive open sessions that are used for TCP session based attacks.

TCP Regex Checker Test:

This test checks HTTP and other TCP session for proper syntax. This analysis detects specific TCP application layer attacks.

TCP Port Usage Conformance Test:

This test allows users to limit some TCP based protocols to its specified usage, therefore detecting attacks that use compromised P2P servers, mail servers etc., for application layer TCP attacks.

TCP Application Layer Analysis Test:

This set of algorithms detects attacks such as HTTP. For example, HTTP page usages are taken into consideration. Also the Platform restricts session set up to a reasonable level according to the server characteristics.

Other Tests:

The RioRey platform has other additional algorithms that monitor such behavior as packet arrival rates, port sequencing and the like to capture other minor but important features that can help distinguish good *vs*. bad traffic. All these computations contribute to identifying offending Bots and placing their IP into the Filter List.

7.1.2.2 DDOS-2: DDOS Information Flow Control Capabilities

(FRU_DDOS_EXT.1.3)

FILTER, MONITOR or BYPASS modes

When the Platform is in filter mode, it checks each packet and blocks attack traffic while allowing good traffic to pass through with minimal time delay. The device filters all main types of DDOS attacks, including ICMP, UDP, TCP, TCP-SYN, ACK and SYN-ACK, TCP-Session, HTTP, and P2P. Random IP address attacks, forged IP address attacks, network scans and port scans are blocked by the Platform. Combination attacks including smurf, ping floods, fraggle, evasive UDP, pulsing zombie, and others are also blocked. Encrypted traffic is scanned by the Platform without being decoded. All data pertaining to attacks is logged for ten days.

When in monitor mode, the device monitors data but does not block attack traffic. All data concerning attacker and victim are logged. The pollution percentage, severity of attack, and confidence that an attack is being made upon the network are all monitored in this operating mode. Data is logged for ten days.

In bypass mode, the Platform counts packets and bytes, but does not perform any other action. Data is not logged when the device is in bypass mode.

In hardware bypass mode, whether through hardware failure or administratively configured, data passes through the Platform without the Platform collecting any information from the data.

Traffic control based on Whitelist Specifications

All packets associated with the Whitelist are considered good and transmitted. The Whitelist overrides all Blacklist and block list settings. If a Whitelisted IP behaves badly, it will be reported in the attacker list, in either green or gray color, but all packets will still be treated as good and transmitted. The green/gray report is used to inform the customer how the traffic behaves. It is a useful tool to help customers understand network behavior. All information coming through from clients on this list will come in without being filtered.

Traffic control based on Blacklist Specifications

All packets associated with this IP are bad and is blocked. This list is “set” and does not time out. So once an IP is put onto the Blacklist, traffic from this IP remains blocked as long as it is left on the list. Any attack packet from a Blacklisted IP will be displayed in RED in the attacker list. All packets, regardless of port or application, originating from an IP address on the Blacklist will be blocked. The only exception to this rule is if the IP address on the Blacklist is also placed on the source IP Whitelist.

Service Definitions

The Platform provides a firewall-like feature to assist common firewalls during a DDOS attack. Any traffic that is sent to a generally unused port on a server can be eliminated. Up to 20,000 entries can be placed in the table with a limitation of 5,000 discrete IP addresses.
The list is in XML format and the list can be both uploaded and downloaded easily in this format. The default entry is: Destination IP = 0.0.0.0, Type = ALL, start port = 0, end port = 65535. This default value allows all traffic through to be passed through the Platform filtering algorithms. If the default line is present, all subsequent lines drop all traffic for the specified IP except for the type and port(s) that are specified in the entry. If the default line is not present, all traffic is blocked except traffic specified in the entries in this table. Any entry with the specified IP 0.0.0.0 can open all IPs or all ports to particular types of traffic except for IPs that have a separate entry on this list.

For the CC evaluation configuration the administrator:

- must ensure that the Firewall is enabled and configured on the RioReyTM Perimeter Protection Platform and

- must ensure that the Firewall IT environment has a NTP server available for the RioReyTM Perimeter Protection Platform to connect and obtain reliable time.

Fragmentation Control

The Platform allows an administrator to manually set fragmentation controls. The amount of fragmented traffic vs. real traffic for TCP, UDP and ICMP can be set. Once the incoming traffic stream exceeds the set fragmentation percentage, packets will be aggressively examined so that all aspects of the fragment streams are examined, counted and tracked. The aggressive

examination mode is less tolerant with errors and therefore may generate a higher rate of false positives, but will find and remove all fragmented DDOS packets. The amount of partial headers allowed can also be set. Be default, proper headers for TCP packets are required for the Platform to allow traffic through.

The administrator can loosen the header requirements in two ways:

Allow Partial Headers: All TCP packets with partial headers in the first fragment are allowed and all TCP, UDP and ICMP packets with partial headers in middle fragments are allowed.

Enforce RFC 1858: All TCP/UDP middle fragments with a fragment offset of --1 are blocked. This option is only available when the operator has already chosen to allow partial headers.

Filtering algorithms will continue to check for other signs of DDOS traffic regardless of whether the operator has loosened the restriction on proper heading requirements.

TCP SYN Rate Config

The Platform controls how many SYNs per minute per source IP are allowed based on per IP SYN rate limit setting. If the number of SYNs exceeds the number specified, the requests will be dropped by the Platform. If the limit set on the SYNs per IP per minute is set to zero, the function will be disabled, allowing all SYN packets to be passed through.

The Platform controls source IP addresses that generate more SYNS at a rate exceeding the **max SYN rate** specified. These IP address will be temporarily blocked. All TCP traffic from these IP addresses will be blocked for the amount of time specified by the setting.

Once an IP address has been placed on the temporary block list established by the max SYN rate, the specified value on the **SYN block minutes** determines how much time the IP address remains on the blocked list.

7.1.3 Protection of TSF

7.1.3.1 FPT-1: Failure with preservation of secure state

(FPT_FLS.1)

Secure State for this product is defined as the state when the TOE Platform provides uninterrupted access to resources on the Internal Network to intended users. The failure of the TOE must not make the resources unavailable. The 3 types of failures are described below:

Hardware Failure:

1a. A partial hardware failure, such as a single power supply in a RX or RG with redundant power supplies, has no traffic impact.

1b. A complete hardware failure, will trigger the hardware bypass, if enabled. The hardware bypass occurs within Nano-seconds, the impact to the traffic is caused by the re-negotiation performed by the copper or optical ports on the router/switches that the device was connected to. The duration of re-negotiation is independent of the amount of traffic. Typically, this renegotiation occurs in milli-seconds, sometime a couple of hundred milli-seconds. - this in most cases is not enough to cause a TCP conversation to reset and therefore the link can still be said to be functional. Typical TCP timeouts are much longer duration (often in 10s of seconds) so that they are unaffected by the hardware switchover.

Power failure:

2. Power failure is handled the same as 1b above.

When the device powers back on after power loss (the device reboots automatically when power is restored), the boot is reported through syslog. Reviewing syslog for these reboot messages will reveal any unexpected power losses. Additionally, the system indicators under sensor network in rView will turn gray.

Software Failure:

3a. A software failure in any subsystem other than the bypass software is detected within 3 seconds, which triggers the hardware bypass. This is followed by the external devices renegotiating as described in 1b above.

3b. A software failure in the bypass software is detected by the bypass hardware due to loss of heartbeat within 3 seconds. This triggers the hardware bypass and is followed by the external devices renegotiating as described in 1b above.

If a reboot was generated through rView, there will be a message displayed indicating that the rView will log out of the device. If the user initiated the reboot themselves (for instance, by cycling power), then the device will turn gray under sensor network. The syslog messages are generated on device bootup.

The LED indicators in rView (not the physical LEDs) show the last known state so the failure/reboot can be visually seen until refresh happens.

7.1.3.2 FPT-2: Basic internal TSF data transfer protection

(FPT_ITT.1)

The rView Software connects to the Platform using the standard SSH-2 protocol through OpenSSH version 5.1p1 which provides confidentiality and integrity of data over an insecure network. The PC that runs rView must therefore be on a network where TCP Port 8022 access is enabled to the Platform Management Port.

The rView GUI (which is the client here) attempts to authenticate itself to the Platform (which is the server here) using Password Authentication. A session key produced by the Platform is established between the rView GUI and the Platform. The traffic is encrypted using the session key and 128bit AES

symmetric algorithm in the CTR mode (*meaning symmetric 128-bit key is generated for this at the beginning of each session*). The integrity of the session between the rView and Platform is provided through HMAC-MD5 used as a message authentication code algorithm.

Optional restrictions that can also be implemented are as follows:

- a firewall mechanism that restricts open ports and closes all unused ports (open port is TCP 8022)
- ACL that restricts login using a defined valid IP address or network (i.e connections from an invalid IP addresses will be rejected).

Note: There is a known vulnerability in OpenSSH version 5.1p1 (Vulnerability CVE-2008-5161). The impact of this vulnerability is that an attacker can potentially recover data from an ongoing connection provided the encryption mode used is CBC. The TOE uses CTR/AES mode instead of CBC, and as such is not affected by this vulnerability.

Note: VU#836068 relates to the MD5 hashing algorithm. This OpenSSH configuration is using HMAC-MD5 as a message authentication code (MAC) algorithm. HMAC-MD5 is not affected by this vulnerability as described here: https://tools.ietf.org/html/rfc6151. To summarize, the attacks on HMAC-MD5 do not seem to indicate a practical vulnerability when used as a message authentication code.

7.1.3.3 IA-1: User Attributes

(FIA_ATD.1)

The TSF maintains the following security attributes for each individual TOE user for use with local password authentication only:

- Username
- Password
- Role assignment

7.1.3.4 IA-2: User I&A

(FIA_UAU_EXT.2, FIA_UAU.5, and FIA_UID.2)

The TSF requires each user to self-identify before being allowed to perform any other actions. The TSF requires an administrator to be successfully authenticated with a password before being allowed any other management actions. Authentication is handled via local password protection or the TOE invokes an external authentication mechanism (RADIUS) for the authentication decision. The TOE must be administratively configured to talk with the RADIUS server via the rView interface after installation.

Local passwords have no software enforced password policy. It is recommended within the user manual that the user should use a minimum 8 character password with at least one numeral, one symbol, and at least on capital letter.

If the RADIUS server is unavailable all users configured with RADIUS authentication fails and no access is granted. However, those users configured for local password authentication can still be authenticated. Another words there is no automatic try that goes from RADIUS authentication to Local authentication or vice versa.

7.1.4 Security Management

7.1.4.1 SM-1: Management of TSF Data

(FMT_MTD.1)

The allowed operations on TSF Data and the administrative roles required to execute them are defined in Table 6-4: Management of TSF Data (See Section 6.1.5.2 FMT_MTD.1 Management of TSF data).

7.1.4.2 SM-2: Specification of Management Functions

(FMT_SMF.1)

The TOE is capable of performing the security management functions as defined in 6.1.5.3 and Table 6-4: Management of TSF Data (See Section 6.1.5.2 FMT_MTD.1 Management of TSF data).

All management functions are limited to the administrative roles as defined in Section 7.1.4.3 SM-3: Security Roles below.

7.1.4.3 SM-3: Security Roles

(FMT_SMR.1)

The TOE supports the 3 roles listed below:

- **ADMIN (available via local authentication only)**
- **NORMAL (available via local or remote RADIUS authentication *[*RADIUS Privilege Level 8*]*)**
- **VIEWONLY (only available via remote RADIUS authentication *[*RADIUS Privilege Level 1*]*)**

The *ADMIN*, *NORMAL, and VIEWONLY* roles are assigned when creating a user for local authentication.

When RADIUS authentication is used *NORMAL* and *VIEWONLY* roles are assigned during the authentication decision response based on the privilege level returned (8:Normal, 1: VIEWONLY). These particular security attributes assignments are saved on the RADIUS server not in the TOE.

See Section 6.1.5.2 FMT_MTD.1 Management of TSF data table for details on the specific function available to each role.

7.2 TOE Protection against Interference and Logical Tampering

The TOE consists of both hardware (RE/RX/RG Platform with RIOS) and software (rView and Management GUI).

The TSF is protected because the hardware, the OS and the application are part of the TOE and there in a protected physical environment. The logical access to the TOE is controlled by the identification and authentication functionality provided by the TOE.

The rView and Management GUI components on the Management Station are software only TOE components. They rely upon the protection mechanisms of the underlying operating system platform to protect against untrusted subjects tampering with TSF code or data through OS interfaces. The GUI is designed to ensure that TSF policies are enforced when accessed through its own interfaces. The TSF creates a management session whenever a successfully authenticated user connects to the Platform. The session continues until the user ends the session. The TSF ensures that TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE's Scope of Control is allowed to proceed. All user operations are conducted in the context of an associated user session. This user session is allocated only after successful identification and authentication by the TSF. The user session is destroyed when the corresponding user logs out of that session.
The Data Interfaces are separated from the Management Interfaces. The device has two data interfaces which connect the inside network to the outside network. Data packets are scanned as they enter and as they leave the network through either 1 gigabit or 10 gigabit Ethernet cable. Copper or fiber optic interfaces are used to transfer data. Single-mode and multimode fiber interfaces are available on all models and copper interfaces are available on RE and RX models.

On these data interfaces, the device may be viewed as a layer 1 device in the ISO model – as a hub or a repeater. It has no layer 2 or layer 3 addresses on the data interfaces, does not participate in any protocols (layer 2 routing or layer 3 routing) and does not originate any traffic from within. Good traffic passes through the platform with a time delay of 70- 120μs.

7.3 TOE Protection against Bypass of Security Functions

The TOE resides as a network perimeter device thus physically separating the external networks from the protected networks. All network traffic flows from and to the internal networks flows through the TOE only after inspection by various DDOS algorithms and filters. The Platform hardware and RIOS software ensure that all packets are forwarded to, and processed through the filtering functions of the filtering functions and are not by passable. However, the TOE by design is developed to provide availability of resources to its intended users. In the case of hardware errors, it enters into a fail-safe mode bypassing all the traffic consistent with the TSP. In case of a software failure, multiple watchdogs embedded in the Platform will attempt to restart the platform and report the incident to the operator. The platform bypasses traffic during the restart phase, maintaining service.

The TSF requires that all users successfully authenticate before any TSF functions (other than entering identification and authentication data and accessing help files available through the rView software) can be performed. Once a user is identified and authenticated, they are associated with a role that determines which function interfaces the TOE will offer to the user. The TSF does not offer general programming capabilities that might offer the opportunity to attempt to bypass the TSP.

Access to management functions are allowed only for users who have been assigned the required administrative role. Authorized administrators can only view the security attributes and TSF data through the administrative interfaces and only after successfully identifying and authenticating themselves.

Additionally, the TSF does not accept any commands from or offer any functions to the networks that are monitored by the TOE. This ensures that network entities cannot cause the TOE not to apply its TSPs to applicable network traffic.

A firewall mechanism can be configured to restrict open ports and close all unused ports on management interface (TCP 8022 port is required and cannot be shut off)

The TOE can be configured to restrict login access to those using a defined valid IP address or network (i.e connections from an invalid IP addresses will be rejected).