National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

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

Report Number: CCEVS-VR-VID10380-2012

Dated: December 21, 2012

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers, Senior Validator

Jerome.F.Myers@aero.org

Aerospace Corporation

(410) 312-1404

Dr. Patrick Mallet, Lead Validator

mallett@mitre.org

Mitre Corporation

(703) 983-5615

Common Criteria Testing Laboratory

Prajakta Kulkarni

Swapna Katikaneni

CygnaCom Solutions

McLean, Virginia

Many of the product descriptions in this report were extracted from the RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series), Security Target.

Table of Contents

List of Figures

1 Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product 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.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

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 shunts the WAN and LAN ports, 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.

The TOE performs following security functionality: auditing of security relevant events; TOE user identification and authentication; role based access to management of security functions; DDOS protection and protection of TSF.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in December 2012. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R3 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.1 from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, [CEM].

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document "RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series), Security Target, Version 0.8, October 26, 2012"

2 Identification

Target of Evaluation: 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.

Evaluated Software and Hardware:

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.

Developer:	Riorey, Inc
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr., Suite 5400 McLean, VA 22102-3321
Evaluators:	Prajakta Kulkarni and Swapna Katikaneni
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	**Dr. Jerome Meyers and Dr. Patrick Mallet**
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, July 2009
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R3, July 2009

3 Security Policy

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

The TOE provides the following security features:

3.1 Summary

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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 shunts the WAN and LAN ports, 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.

3.2 Operational Environment Objectives

- The TOE's operating environment must satisfy the following objectives.
- 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
- 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..
- 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.
- 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.
- The IT environment must be configured with an NTP server that is able to provide reliable time to the TOE.
- The IT environment must provide long term storage for audit records and alert data generated by the TOE.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL 4 assurance requirements:

- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- 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

4.2 Assumptions

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.
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.
A.BACKUP	Administrators will back up the audit files, configuration files and monitor disk usage to ensure audit information is not lost.
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.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 4 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The following are not included in the Evaluation Scope:
    a. SNMP browser/Server
    b. SMTP Server
    c. NTP Server
    d. Syslog Server
    e. Web browser
    f. The system hosting the rView application is also part of the IT Environment.
5. The following RioRey Products/Services are not included in the scope of the evaluation:
    a. CLI (status, resetpwd, resetip).
    b. WebUI (deprecated and turned off)

6. The Operational Environment needs to provide the following capabilities:
    a. SNMP browser/Server
    b. SMTP Server
    c. NTP Server
    d. Syslog Server
    e. Web browser
    f. The system hosting the rView application
    g. 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)

5 Architectural Information

The evaluated configuration of the TOE includes the following TOE components:

The TOE consists of two components:

- a RioRey-proprietary hardware device referred to as the Platform. The appliance is running RioRey developed software that provides DDoS protection (RIOS), and
- RioRey developed management software (rView) to manage the device

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 Boundary is depicted in software breakdown figure below.

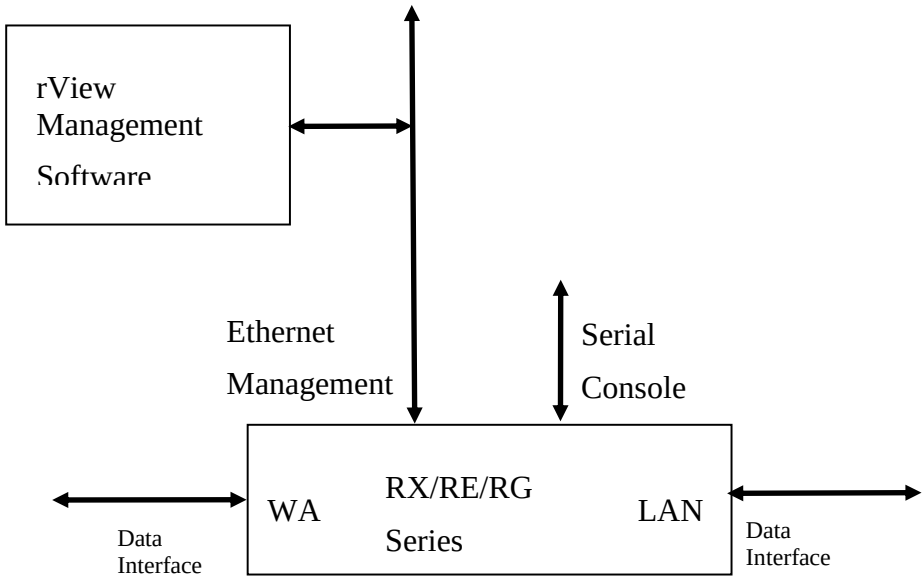

Figure 1: TOE

T

he hardware device has 4 physical connections that are considered external interfaces:

- two data interfaces, nominally labeled WAN and LAN
- an Ethernet management interface (EMI)
- a serial console interface

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. Please see the figure below for an architectural description of the TOE.

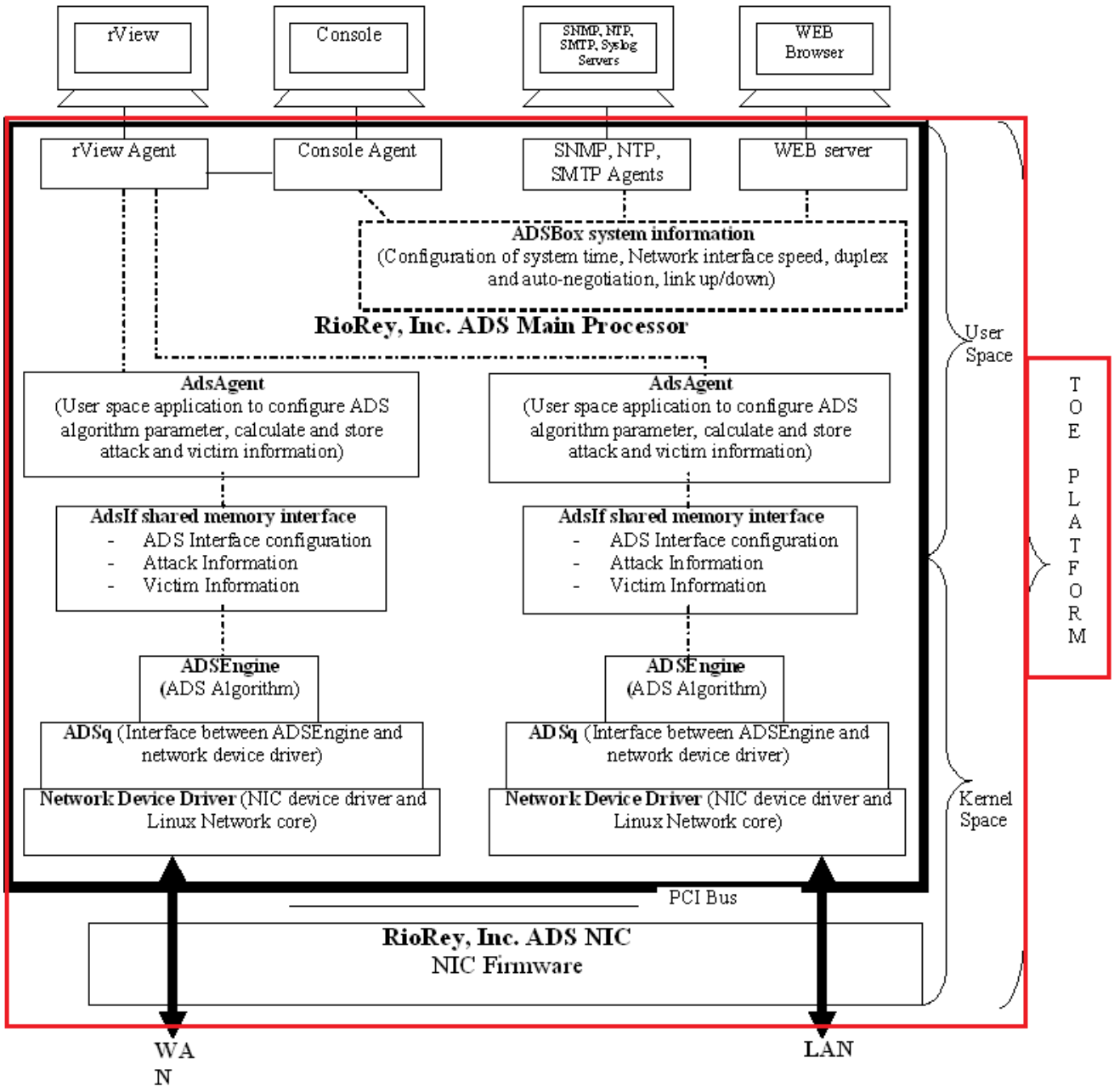

Figure 2: TOE Physical Boundary

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE and methodology for delivery of the evaluated configuration. In these tables, the following conventions are used:

Documentation that is delivered to the customer is shown with **bold** titles.

Documentation that was used as evidence but is not delivered is shown in a normal typeface.

The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered in printed form and as PDFs on the installation media.

6.1 Guidance Documentation

The following documents are developed and maintained by Riorey Inc and delivered to the end user of the TOE:

RE Series Installation and Initial Configuration Guide, Version 5.0, June 2012, V1.3	**[RE-INSTALL]**
RX Series Installation and Initial Configuration Guide, Version 5.0, June 2012, v1.3	**[RX-INSTALL]**
RG Series Installation and Initial Configuration Guide, Version 5.0, June 2012, V1.5	**[RG-INSTALL]**
RE Series DDoS Defense Settings Guide, Version 5.0, June 2012, V1.2	**[RE-ADMIN]**
RX Series DDoS Defense Settings Guide, Version 5.0, June 2012, V1.2	**[RX-ADMIN]**
RG Series DDoS Defense Settings Guide, Version 5.0, June 2012, V1.4	**[RG-ADMIN]**
RioRey Version 5 RG.RX.RE Release Note Supplement, September 2012, V1.2	**[RELEASE]**

6.2 Security Target (ST)

Security Target (ST)

[1] RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800,RX2300, RX4400 and RG Series), Security Target, Version 0.8, October 26, 2012

6.3 Development (ADV) Evidence Documentation

RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800,RX2300, RX4400 and RG Series) Functional Specification V 0.7	[FSP]

6.4 Life-Cycle (ALC) Evidence Documentation

[1] RioRey™ DDOS Protection Platform (RE-Series, RX-Series and RG-Series), RIOS and rView Software Version 5.0 Configuration List Description, Version0.4, September 27, 2012

[2] RioRey™ DDOS Protection Platform (RE-Series, RX-Series and RG-Series), RIOS and rView Software Version 5.0 Configuration Management, Version0.4, October 24, 2012

[3] RioRey™ DDOS Protection Platform (RE-Series, RX-Series and RG-Series), RIOS and rView Software Version 5.0 Delivery Procedures, Version0.1, April 12, 2010

[4] RioRey™ DDOS Protection Platform (RE-Series, RX-Series and RG-Series), RIOS and rView Software Version 5.0 Development Security, Version1.1, May 18, 2012

[5] RioRey™ DDOS Protection Platform (RE-Series, RX-Series and RG-Series), RIOS and rView Software Version 5.0 Basic flaw remediation Version 0.2, May 3, 2010

[6] RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Life-cycle Model Definition Version 0.5, May 15, 2012

[7] RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Development Tools Version 0.4, May 16, 2012

6.5 Testing (ATE) and Vulnerability Analysis (AVA) Documentation

[8] RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Developer Test Plan Version 0.6, April 3, 2012

[1] RioRey™ FUN test procedures and Results Version3, September 26, 2012

[2] RioRey™ DDOS Protection Platform (RE-Series, RX-Series and RG-Series), RIOS and rView Software Version 5.0 Evaluator Test Plan and Report v1.1, October8, 2012.

[3] Riorey Vulnerability Report on Public search.

6.6 Evaluation Technical Report (ETR)

[1] Evaluation Technical Report For a Target of Evaluation, Volume 1: RioReyTM Perimeter Protection Platform (RE500, RE1500, RX1800,RX2300, RX4400 and RG Series), Security Target, Version 3.0, October 26, 2012

[2] Evaluation Technical Report For a Target of Evaluation, Volume 2: Evaluation of the TOE, RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series), Version 2.0, October 26, 2012.

7 IT Product Testing

7.1 Developer Testing

The developer testing effort that is described in detail in the Developer Test Plan involved executing the test sets in the test configurations described in Section 8: Evaluated Configuration.

7.1.1 OVERALL TEST APPROACH AND RESULTS:

The Developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. These test cases were mapped to SFRs, TSFIs, Subsystems and Internal Interfaces listed in the ST, Functional Specification [FSP], TOE Design Document [TDS] and Test Coverage Document [COV]. After the test cases were defined, test procedures were written by the Vendor's development team to exercise each test case.

The tests provided by the developer are manual tests performed via the rView GUI.

7.1.2 DEPTH AND COVERAGE

All developer test cases test the TOE security functions by stimulating an external interface.

All the developer tests are performed using the rView interface. The evaluator determined that the test cases as described in the test documentation adequately exercise the internal interfaces.

TOE testing directly tests external TSF interfaces and indirectly tests (exercised implicitly) internal subsystem interfaces. The behavior of the TSF is realized at its interfaces.

- The Developer's test plan covered all of the security relevant behavior of each Security Function in the ST.
- The Developer executed all of their test procedures and provided a generated report of the actual results.
- Additional tests were provided to the evaluator prior to the onsite visit to address the validator's concern that the DDoS testing coverage appeared lacking for a EAL 4. The supplemental tests were run and the results were provided before the first phase of onsite testing.

Given the Evaluation Assurance level (EAL 4) TOE testing is adequate. All the external TSF interfaces are tested. TOE testing exercises all security functions identified in the Functional Specification [FSP]. It indirectly tests the security functions and subsystem interfaces as presented in the TOE Design [TDS].

The evaluator ensured that the vendor tests provided included the tests such that:

- All Security Functions are tested
- All External interfaces are exercised
- All Security Functional Requirements are tested.
- All relevant security relevant features mentioned in the Administration/User Guides are covered in testing.

7.1.3 RESULTS

The evaluator checked the test procedures and the Test Evidence and found that the expected test results are consistent with the actual test results provided. For each test case examined, the evaluator checked the expected results in the test procedures with the actual results provided in the Test Evidence and found that the actual results were consistent with the expected results. The evaluator checked all of the test procedures.

Given the Evaluation Assurance level (EAL 4), the evaluator determined that Riorey's TOE testing is adequate. All the external TSF interfaces are tested. TOE testing exercises all security functions identified in the Functional Specification.

7.2 Evaluator Independent Testing

The evaluator performed the following activities during independent testing:

- Execution of the Developer's Functional Tests (ATE_IND.2)
- Team-Defined Functional Testing (ATE_IND.2)
- Vulnerability/Penetration Testing (AVA_VAN.2)

7.2.1 EXECUTION THE DEVELOPER'S FUNCTIONAL TESTS

The evaluator selected 100% of the developer's tests:

- As a means of ensuring the coverage of the security features.
- As a means to gain confidence in the developer's test results.
- A quick means of ensuring TOE is in a properly configured state.

The developer's test cases were executed only after the TOE was installed in the evaluated configuration that is consistent with the Security Target (Section 1) and the Common Criteria Supplement Document. The evaluator confirmed that the test configuration was consistent with the evaluated configuration in the Security Target.

The test configurations used by the evaluator were the same as that used by the developer.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the retests being consistent with expected results.

All of the Developer's Functional Tests rerun by the Evaluator received a 'Pass' verdict during phase 2 of testing.

Note: The evaluator found that the actual results observed during testing were inconsistent with the developer test results while rerunning the developer tests.

The evaluator chose to run only a sample of a developer tests on the other two models [RE and RG] based on the equivalency argument provided by the developer in the developer test plan. During the sample testing on RE, the evaluator discovered that the availability of management functions is distinct for each of the platform models.

Additionally the evaluator found that rView management interface was not functioning as expected on RG. Several Menu option on Rview did not function to proceed with any further testing. This was a critical bug found during testing which mandated the customer to address the issue and generate a new release of Rview.

In summary,

1. The TOE behavior was not accurately documented.
2. TheTOE did not behave as expected.

This forced the developer to rerun their entire test set on the new release of the TOE. The evaluator conducted retesting at the developer site

During Phase 2, The evaluator chose to rerun 100% of the developer tests similar to phase 1. The evaluator chose to rerun all the tests on all the three models to ensure that all the models behave as expected and as documented in the evidence documentation.

All the tests were confirmed to pass during phase 2 of testing

7.2.2 TEAM-DEFINED FUNCTIONAL TESTING

The Evaluator selected individual test procedures from the set of Developer Functional Tests, and modified the input parameters to ensure fuller coverage of security functions and correctness of developer reported results (ensuring that the results were not canned).

Additional tests were developed for the purpose of verifying that the product operates in accordance with Vendor claims, i.e. that a bug is fixed or a capability operates as described in the product documentation.

The test results and screenshots for the test cases were recorded during the Evaluator testing. Overall success of the testing was measured by 100% of the tests being consistent with expected results. Anomalies found were addressed by updating the required documents.

All of the Team-Defined Tests received a ‘Pass’ verdict.

7.2.3 VULNERABILITY/PENETRATION TESTING

The Penetration tests for TOE were developed according to the following strategy:

- The Evaluator looked for possible security vulnerabilities by examining the Vulnerability Analysis, Functional Specification, TOE Design Document and TOE Security Target.
- The Evaluator analyzed the different components that comprise the TOE for existing vulnerabilities.
- The Evaluator searched public vulnerability databases for vulnerabilities that corresponded to these components.
- The Evaluator has hypothesized vulnerabilities requiring low attack potential that apply to the TOE.
- The Penetration tests will cover hypothesized vulnerabilities and potential misuse of guidance.
- The tests for potential misuse of guidance will cover installing the TOE from the guidance documentation and sampling the documented administrator procedures.
- The Evaluator will perform a systematic vulnerability analysis of the TOE.

The TOE Penetration testing was performed with the following assumptions and guidelines:

- Penetration testing will be limited to attacks by a malicious entity with limited technical skills and unsophisticated exploits.
- TOE Administrators are trusted personnel; any vulnerabilities resulting from Administrator use constitute a case of misuse, rather than purposeful activity with malicious intent.
- The platforms running all the TOE Components/applications have been configured securely as described in the Guidance documents to include:
    - Minimal OS features installed or enabled
    - Minimal system privileges configured
    - Only user accounts for authorized system administrators
- The organization operating the TOE has defined and is following good backup and recovery procedures that allow the TOE to be recovered to a secure configuration in the event of a loss of the TOE.

The test results and screenshots for the test cases were recorded during the evaluator testing. Overall success of this testing was measured by 100% of the tests being consistent with expected results. Anomalies were documented along with suggested / required solutions.

8 Evaluated Configuration

RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX440 and RG) with RIOS Software version 5.0.12sp8) and rView Software version 5.0.12sp9.

9 Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R3 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 4 augmented with ALC_FLR.1. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

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_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
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
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample

AVA_VAN.3	Focused vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached Pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

10 Validators Comments/Recommendations

The TOE was evaluated for the capability of storing and reviewing audit records locally on the TOE. There are some risks associated with relying solely on that capability. Audit records that are held on the TOE are stored locally in RAM and then moved on an hourly basis to flash memory. Some of the records in flash memory will be overwritten once the flash memory fills. Moreover, if power is lost, the records that are in RAM will always be lost. The number of records that can be stored in flash memory depends upon the product model. The models with the least amount of flash memory can hold appropriately 10 days worth of audit data. Some potential customers will find that capability insufficient to meet their audit retention requirements for Certification and Accreditation. Fortunately, the evaluated TOE permits the use of traditional syslog functionality to export audit records as they are generated. The correctness of the syslog functionality was not part of the scope of the evaluation, but it was established that the functionality does not interfere with the evaluated TOE. By enabling syslog to export the audit records as they are generated the user can implement long term storage of audit records. When deciding whether to use syslog, the protection of the backbone network must be taken into consideration, since the TOE does not implement the more recent variants of the syslog protocols that provide enhanced protection for the syslog payloads.

11 Security Target

RioRey™ Perimeter Protection Platform (RE500, RE1500, RX1800, RX2300, RX4400 and RG Series) Security Target Version 0.8, October 26, 2012

12 Glossary

12.1 Acronyms

The following are product specific and CC 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

12.2 Terminology

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

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.

Term	Definition
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.
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.
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.

Term	Definition
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.
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.

Term	Definition
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

Term	Definition
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.

13 Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com/labs/common-criteria/index.htm).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 3 Final, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-004.