National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

Marconi Service Edge Routers (BXR-1000 and BXR-5000)

Report Number: **CCEVS-VR-06-0016**
Dated: **March 29, 2006**
Version: **2.0**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE Evaluation was Sponsored by:
Ericsson Incorporated
3000 Marconi Drive
Warrendale, PA 15086 USA

Evaluation Personnel:
Science Applications International Corporation (SAIC)
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046-2554

Terrie Diaz
Jean Petty
Quang Trinh
.

Validation Personnel:
Shaun Gilmore, National Security Agency
Santosh Chokhani, Orion Security Solutions

Table of Contents

1 Executive Summary 1
2 Identification 1
3 TOE Security Services 2
4 Assumptions 3
4.1 Physical Security Assumptions 3
4.2 Personnel Security Assumptions 3
4.3 Personnel Security Assumptions 3
5 Architectural Information 3
6 Documentation 4
7 IT Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 8
8 Evaluated Configuration 9
9 Validator Comments 10
10 Security Target 11
11 List of Acronyms 12
12 Bibliography 13
13 Interpretations 14
13.1 International Interpretations 14
13.2 NIAP Interpretations 14
13.3 Interpretations Validation 14

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Marconi Service Edge Routers (BXR-1000 and BXR-5000). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Marconi Service Edge Routers (BXR-1000 and BXR-5000) was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during March 2006. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 have been met.

The Marconi service edge routers are network appliances that provide network traffic management and control. The Marconi service edge routers are highly scalable and flexible. They support any type of switched or routed data service for virtually any interface; they can manage traffic over essentially any type of network, with the different models providing varying levels of performance speed and scalability of the traffic volume. All packets, frames, and traffic flows on the monitored network are scanned and then compared against a set of rules to determine whether the traffic should be switched or routed, and then it is passed to the appropriate destination.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 3 evaluation. Therefore the validation team concludes that the SAIC Common Criteria Testing Laboratories (CCTL) findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs or candidate CCTLs using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs and candidate CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;

- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	The TOE consists of the following Marconi service edge router models (BXR-1000 and BXR-5000, running ShadeTree Routing Control Software ver 3.1.1)
Security Target	Marconi Service Edge Routers (BXR-1000 and BXR-5000) Security Target Version 1.0, 8 February, 2006
Evaluation Technical Report (Non-Proprietary)	Evaluation Technical Report for Marconi Service Edge Routers (BXR-1000 and BXR-5000), Version 5.0, 29 March 2006
Evaluation Technical Report (Proprietary)	Evaluation Technical Report for Marconi Service Edge Routers (BXR-1000 and BXR-5000), Version 1.0, 15 February 2006
Conformance Result	EAL 3
Sponsor	Ericsson Incorporated. 3000 Marconi Drive Warrendale, PA 15086 USA
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046-2554
CCEVS Validator(s)	Shaun Gilmore National Security Agency Santosh Chokhani Orion Security Solutions 1489 Chain Bridge Road, Suite 300 Mclean, Virginia 22101

3 TOE Security Services

The security services provided by the TOE are summarized below:

Security Audit

The TOE provides an audit feature that provides the ability to audit user actions related to authentication attempts and administrator actions.

Information Flow Control

In general, network devices exchange valuable information among themselves. To mitigate threats of spoofing, replay attacks, unauthorized access and DoS attacks among others, the TOE provides an Information Flow Control mechanism that supports control of the flow of traffic generated by the network devices. The Information Flow Control Policies are configured on each network devices to allow traffic to only flow between the authorized sources and authorized destinations.

Identification and Authentication

The TOE requires administrative users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE provides the ability to define levels of authority for such users via "profiles", providing administrative flexibility by allowing highly granular assignment of management rights down to the level of individual commands or entire "directories" of commands. Only authorized administrators may access the TOE. Note, any user that is defined such that they can directly authenticate to the TOE is considered to be an administrator though the specific authorizations may vary with the profile of the individual TOE user (administrator). End users whose traffic may traverse the TOE via its switching and routing functions do not need to be authenticated to use these services since they have no control over the TOE. Thus the term "user" as applied to the TOE should be understood to refer to administrators unless otherwise specified by terms such as "end users."

Security Management

The TOE is managed through a Command Line Interface (CLI) that can be accessed locally using the terminal console, or remotely using telnet. Additionally, many of the TOE's functions can be monitored remotely via SNMP GET. Through the CLI, authorized administrators can configure and manage all TOE functions, including configuring the TOE and managing administrative user accounts (if authorized by their profile).

Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that administrative users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of administrative user accounts or the configuration of the switching and routing functions. Another protection mechanism is that the TOE is self-contained and therefore maintains its own execution domain. All TOE security functions are confined to the device.

4 Assumptions

4.1 Physical Security Assumptions

- The TOE will be protected from unauthorized physical access.

4.2 Personnel Security Assumptions

- The administrators will be competent and will adhere to the applicable TOE guidance.
- The administrators of the TOE will not be willfully negligent or otherwise hostile.

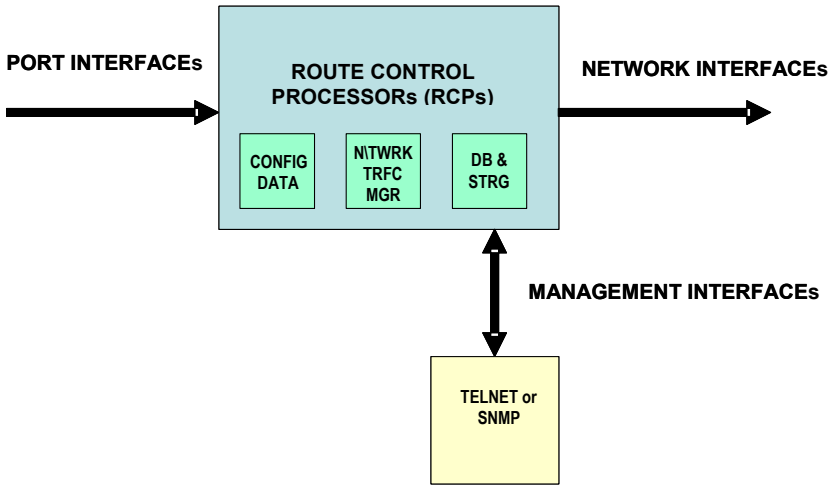
4.3 Connectivity Assumptions

- The TOE will be installed in a network infrastructure such that it can effectively control the flow of the applicable information.

5 Architectural Information

The Marconi service router appliances are designed to provide transport devices for Ethernet, Sonet, Frame Relay, and ATM Layer 2 networks to LAN and WAN environments. The TOE

consists of the hardware appliance that contains the potentially redundant System Input/Output interfaces (SIOs), Route Control Processors (RCPs), Packet Switching Fabrics (PXFs), power supplies, and the device management interface. The TOE is managed by the ShadeTree Routing Control Software (RCS), which controls the TOE's operation. SIOs are the physical network interfaces that allow the TOE to be customized to the intended environment. In the BXR-1000 model of the TOE, the SIO functionality and interfaces are incorporated into the RCPs, while in the BXR-5000 model of the TOE, the SIO functionality and interfaces are contained in a separate card.



The service edge routers are powered by RCPs running the ShadeTree RCS, which are included in the TOE and which manage all network traffic management functions including cell, packet, frame, and IP routing functions. The appliances support numerous routing and switching standards, allowing them to be flexible as well as scalable. The appliances are managed through a locally connected terminal console or remotely via Telnet. Additionally, they may be monitored via SNMP using standard GET commands, although configuration changes may not be made via SNMP. (SNMP operates in Read-Only mode in managing the TOE.).

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Design documentation

Document	Version	Date
BXR-5000/1000 Service Edge Routers - Functional Specification Document, BXR-5k1k_FSP_1.8.doc	1.8	7 February 2006
BXR-5000/1000 Service Edge Routers - High Level Design Document, BXR-5k1k_HLD_v1.2.doc	1.2	12 December 2005
BXR-5000/1000 Service Edge Routers - Common Criteria Certification TSF Representation Correspondence, BBRS-CK-004_BXR-5k&1k_RepCorrespondence_1.2.doc	1.2	21 October 2005

Guidance documentation

Document	Version	Date
BXR-5000 and BXR-1000 User Guide, Volumes 1 to 10, 080-0063-04, 8006304a.pdf	Issue A	September 2005
BXR-5000 and BXR-1000 User Guide, Volume 10: CCC Configuration 080-0074-01 Issue A, November 2005 8007401a1.pdf *NOTE*: The CC Evaluated Configuration Guide was revised after the CC evaluation. The actual filename sent was BXR-5k1k_CCC_Evaluated_Config_1.8.doc	Issue A	February 2006
BXR-5000 and BXR-1000 LScript API Guide, 080-0073-01, 8007301a.pdf	Issue A	September 2005
BXR-5000 and BXR-1000 Service Edge Router Release Notes, ShadeTree System Software Release 3.1.1R2.7, 085-0051-06, 8505106a.pdf	Revision A	September 2005
BXR-5000 Hardware Installation Guide, 081-0023-03, 081002303i1rA_BXR-5000_Hardware_Install.pdf	Issue A	November 2004
BXR-1000 Hardware Installation Guide, 081-0025-02, 081002502i1rA_BXR-1000_Hardware_Install.pdf	Issue A	December 2004

Configuration Management documentation

Document	Version	Date
Control of Unreleased Product (CUP) Procedure 005-0185-01.pdf	Revision E	17 November 2004
Interchangeability Guideline 060-0001-01.pdf	Revision C	8 May 2000
Initial Configuration / New Product Release ECN Requirements Checklist 064-0001-01.htm	Revision B	
Released Product Change ECN Requirements Checklist 064-0002-01.htm	Revision A	
Part Number and Manufacturer Release and Change Procedure CMOP-4430-001.pdf	Revision D	21 November 1997
Engineering Change Notice Procedure CMOP-4490-002.pdf	Revision J	22 November 2004

Document	Version	Date
Lifecycle Document Change, Approval and New Release Procedure LCPD-0011 ApprovalProcessDoc.doc	Revision 2	August 2002
BBRS Process Documentation Procedure LCPD-0012 BBRSProcessDocControl.doc	Revision 2	August 2002
Product Identification Specification MEOP-4800_001.doc	Revision G	Copy Sent 14Apr'05
PAW 4.2.3 BBRS Document Control Process v3.1 PAW_4.2.3-Document_Control_Process_v3.1.doc	Revision 3.1	
PAW 4.2.3.1 BBRS E*Tools Document Management Tool v1.1 PAW_4.2.3.1-ETools_Document_Mgmt_v1.1.doc	Revision 1.1	
PAW 4.2.3.2 BBRS Software Configuration Management v1.2 PAW_4.2.3.2-Software Configuration Management_v1.2.doc	Revision 1.2	
Procedure for Initiating, Controlling, and Revising Controlled Documents QAOP-1017.doc	Revision F	1 November 2004
BBRS-CK-003, Common Criteria Evaluation Submitted Document List for BXR5000/1000	Revision 20	February 2006

Delivery and Operation documentation

Document	Version	Date
Product Outer Packaging Labeling Guidelines MEGL-4154_001	Revision E	1 March 2002
Packaging Specification for Incoming and Outgoing Shipments MEOP-4154_001	Revision B	23 August 2002
Marconi Part Conversion Procedure MEWI-4103-191	Revision E	23 April 2004
Volume Operations Flow Chart PRFC-1030	Revision C	20 March 2003
Distribution Material Flow PRFC-1062	Revision B	31 January 31 2003
Pre-Pack Boxing and Labeling Procedure PROP-4155_001	Revision D	12 February 2003

Document	Version	Date
Handling, Storage, Preservation, and Delivery of Products PRST-4150-001	Revision C	5 September 2002
Packing and Shipping Training Guide and Work Instructions PRWI-1022_RevB	Revision B	1 December 2005
Final Inspection Procedure QAOP-1104	Revision C	24 March 2003

Life Cycle Support documentation

Document	Version	Date
Marconi Information Security Program version 2.1, 07-11-2001 BBRS-PO-001_Marconi Information Security Program ver 2.1.pdf	Version 2.1	11 July 2001
PAW 4.2.3.1 BBRS E*Tools Document Management Tool v1.1 PAW_4.2.3.1-ETools_Document_Mgmt_v1.1.doc		

Test documentation

Document	Version	Date
SWTP-0002 – BXR-5000/1000 Common Criteria Evaluation Test Plan, Procedures, & Results SWTP-0002-BXR5k_CC_Evaluation_Test_Plan_1.7.doc	Version 1.7	7 February 2006
BXR-1000 Audit logs (files named 1Kauthorization, 1Kchange-log, 1Kinteractive, 1Kmessages, 1Kmessages.1, 1Kmessages.2) and Syslog_BXR1k_Tests.txt BXR-1000_logs.zip		October 2005/February 2006
BXR-5000 Audit logs (files named 5Kauthorization, 5Kchange-log, 5Kinteractive, 5Kmessages, 5Kmessages.1, 5Kmessages.2, 5Kmessages.3, and 5Kmessages.4) and Syslog_BXR5k_Tests.txt BXR-1000_logs.zip		October 2005/February 2006

Vulnerability Assessment documentation

Document	Version	Date
PAW-CERT® Security Alert Management	Revision 1.0	

Document	Version	Date
CS-PAW-002 CERT Security Alerts.doc		
BXR-5000 & BXR-1000 Common Criteria Certification Strength of Function Analysis ENDS-0003_BXR-5k1k_SOF_v1.1.doc	Revision 1.1	11 November 2005
BXR-5000 & BXR-1000 Developer Vulnerability Analysis BXR-5k1k_Vulnerability_Analysis_v1.1.doc	Revision 1.1	3 October 2005

Security Target

Document	Version	Date
Marconi Service Edge Routers (BXR-1000 and BXR-5000) Security Target	1.0	08 February 2006

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

Ericsson's approach to security testing for the TOE is interface based. Ericsson developed a set of test cases that correspond to an interface that enforces a security functional requirement. Each test case is subdivided into security functions and each test procedure targets the specific security behavior associated with that security function. The test procedures are designed to be exercised manually using the subsystem interfaces. For each interface identified in the Functional Specification, tests are provided to cover both positive and negative scenarios for identification and authentication of users logging into the TOE, enforcement of the information flow policies that supports control of the flow of traffic generated by the network devices (serial, Ethernet, and Various physical (PHY) network card interfaces), and various administrator management interfaces that are used to manage all TOE functions, including configuring the TOE and managing administrative user accounts (if authorized by their profile) (CLI), and the protection mechanisms are such that administrative users must authenticate before any administrative operations can be performed on the system.

Section 1.6 of the BXR-5000 & BXR-1000 Common Criteria Evaluation Test Plan, Procedures & Results document provides a mapping of test cases to TSFs. The mapping demonstrates that the tests cover all TSFs described in the Security Target document, which the Representation Correspondence document maps to all the interfaces described in the Functional Specification document. Test depth is addressed by analyzing the functionalities described in the high-level design and then associating test cases that cover the described functionalities. The high-level design addressed the general functions of the software and hardware subsystems. Each function maps the appropriate test case and the rationale demonstrates why the test case covers that particular security function. Although the vendor's testing covered all the TSF's there were very few penetration test cases supplied by the vendor.

7.2 Evaluation Team Independent Testing

This section summarizes the team's test coverage analysis approach. The correspondence between security functions and interfaces is clearly defined in the functional specification.

For each interface identified in the Functional Specification, tests are provided to cover both positive and negative scenarios. Interfaces can be categorized in the following areas:

- identification and authentication of users logging into the TOE;
- enforcement of the information flow policies that support control of the traffic flow generated by the network devices (serial, Ethernet, and Various physical (PHY) network card interfaces),
- various administrator management interfaces that are used to manage all TOE functions, including configuring the TOE and managing administrative user accounts (if authorized by their profile) (CLI),
- and audit logging.

In addition, the administrative management actions can only be taken if the user has appropriate roles or privileges. This privilege-based management was tested by the developer and further verified by the evaluation team.

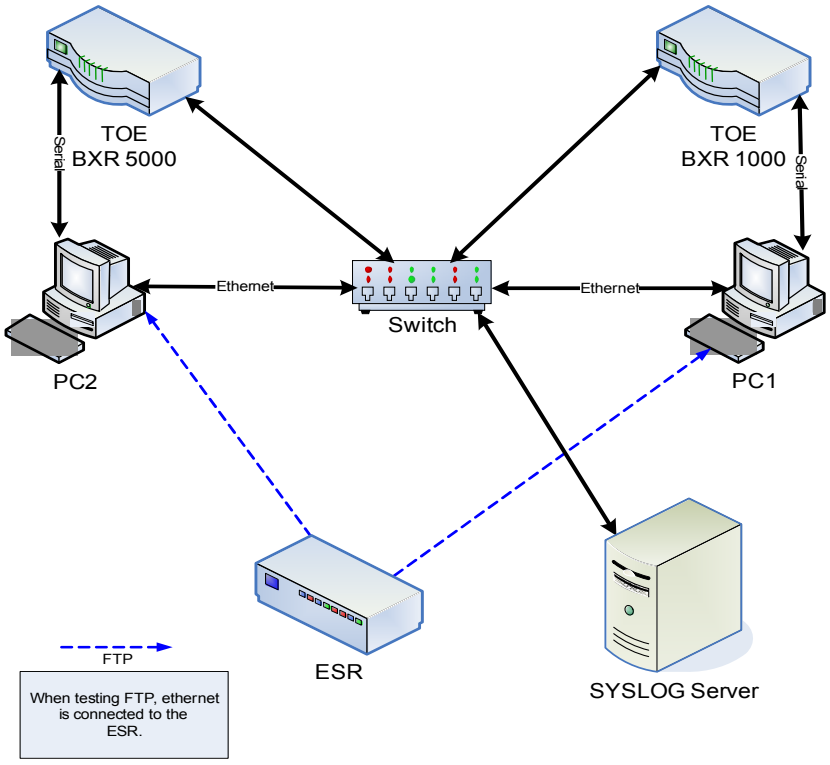
Section 1.6 of the BXR-5000 & BXR-1000 Common Criteria Evaluation Test Plan, Procedures & Results document provides a mapping of test cases to TSFs. The mapping demonstrates that the tests cover all TSFs described in the Security Target document, which the Representation Correspondence document maps to all the interfaces described in the Functional Specification document.

Depth analysis is based on an understanding of the high-level design and is intended to show that the TOE as presented in the high-level design has been adequately tested.

The evaluation team performed the entire developer's test suite and devised an independent set of team tests. The evaluation team determined that the vendor's test suite was comprehensive. Thus the independent set of team tests was limited. The team independent tests covered the following areas: Access Control to CLI, Password Restrictions, Access Control to TOE Resources, and Routing Traffic – IP Filtering. The team's penetration testing was also limited and focused on two primary areas, Password Vulnerability and TOE Availability.

8 Evaluated Configuration

The evaluation team executed the entire suite of vendor tests identified in the BXR-5000 & BXR-1000 Common Criteria Evaluation Test Plan, Procedures & Results document. The test cases were executed following the test procedures as described in the BXR-5000 & BXR-1000 Common Criteria Evaluation Test Plan, Procedures & Results document. The following diagram illustrates the test configuration in which all the tests were executed. The TOE was installed and configured as described in the BXR-5000 and BXR-1000 User Guide, Volume 10: CCC Configuration document.



TOE Hardware

The following hardware is necessary to create the test configurations as depicted in the diagram above:

- 2 Machines for administration (PC1 and PC2)
- 1 Machine to capture the syslog files
- 1 Marconi BXR-1000 (TOE)
- 1 Marconi BXR-5000 (TOE)

In addition to the hardware listed above, there will be a Microsoft Windows machine that will be utilized for remote administration via telnet. (Not depicted in image above)

TOE Software Identification

The following software is required to be installed on the machines used for the test:

- Applicable Microsoft Windows 2000 or Microsoft Windows XP operating system for the Admin and user machines
- ShadeTree Routing Control Software version 3.1.1 (TOE software)

9 Validator Comments

The routing capability of the TOE was not thoroughly covered by the vendor and team testing activities. The team relied almost exclusively on the vendor's test suite, which although adequate, did not comprehensively test all routing capability of the TOE. This was rectified upon validator observation.

The claimed ATM virtual circuit or Ethernet packets within VLANs (Virtual LANs) capabilities of the TOE were not tested in either the vendor's test suite or through team testing and hence can not be verified.

10 Security Target

See Table 1 in this validation report.

11 List of Acronyms

ACL	Access Control Lists
ATM	Asynchronous Transfer Mode
ASIC	Application Specific Integrated Circuits
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CLI	Command Line Interface
CM	Control Management
CPU	Central Processing Unit
DO	Delivery Operation
EAL	Evaluation Assurance Level
HTTP	HyperText Transfer Protocol
I/O	Input/Output
MIB	Management Information Bases
MPLS	MultiProtocol Label Switching
NPB	Network Processor Board
PDF	Portable Document Format
PP	Protection Profile
PXF	Packet Switching Fabric
RCP	Route Control Processor
RCS	Routing Control Software
SF	Security Functions
SFR	Security Functional Requirements
SIO	System Input/Output
SSH	Secure Shell (protocol)
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control
VPN	Virtual Private Network

.

12 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.2, Revision 256, January 2004.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.2, Revision 256, January 2004.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, Version 2.2, Revision 256, January 2004.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.2, Revision 256, January 2004.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.2, Revision 256, January 2004.

[6] Evaluation Technical Report for Marconi Service Edge Routers (BXR-1000 and BXR-5000) Part 2, Proprietary, Version 1.0, 08 February 2006.

[7] Marconi Service Edge Routers (BXR-1000 and BXR-5000) Security Target, Version 1.0, 08 February 2006.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

13 Interpretations

13.1 International Interpretations

The evaluation team performed an analysis of the international interpretations and identified those that are applicable and had impact to the TOE evaluation. The table summarizes the set of interpretations determined to have an impact on the evaluation and identifies the impact.

Impact on Security Target Requirement	Impact on ETR Work Unit	Interpretation Identification (ID)
New element added after ACM_CAP.3.3C		RI-3
ACM_SCP.1.1D and ACM_SCP.1.1C changed		RI-4
	ASE_OBJ.1.2C and ASE_OBJ.1.3C changed (no work unit change indicated)	RI-43
ADO_IGS.1.1C and AVA_VLA.1.1 – 1.3C changed		RI-51
FMT_SMF.1 introduced		RI-65
	ASE_REQ.1-20 work unit changed	RI-84
	ASE_REQ.1.10C (ASE_REQ.1-16 work unit changed)	RI-85
FDP_ACF.1 changed		RI-103
FIA_USB.1 changed		RI-137
	ADO_DEL.1-2 work unit deleted	RI-116
FAU_STG.1 changed		RI-141
FMT_REV.1 changed		RI-201
FAU_GEN.1 changed		RI-202
	All portions of the CC and CEM should be considered "Normative" unless specifically denoted as "Informative.	RI-222

13.2 NIAP Interpretations

Neither the ST nor the vendor's evidence identified any National interpretations. As a result, since National interpretations are optional, the evaluation team did not consider any National interpretations as part of its evaluation.

13.3 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.