BLUE RIDGE
VIRTUAL PRIVATE NETWORKS

Security Target

For

Blue Ridge Networks BorderGuard

Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2

Revision 1.10

December 17, 2003

Document Number: E2-ST-001-10

BLUE RIDGE
VIRTUAL PRIVATE NETWORKS

Security Target Title:

Blue Ridge Networks Security Target for Blue Ridge Networks BorderGuard Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2.

Criteria Version:

This Security Target (ST) was developed using Version 2.1 of the *Common Criteria for Information Technology Security Evaluation* (CC).

Authors:

Blue Ridge Networks

Table of Content

1 Security Target (ST) Introduction

1.1 Security Target (ST), TOE, and CC Identification

1 **Title:** Security Target for Blue Ridge Networks BorderGuard Centrally Managed Embedded PKI Virtual Private Network (VPN) Firmware Release 6.2 and VPN Manager Application Software Release 2.2.

2 **ST Version:** Revision 1.10

3 **ST Date:** December 17, 2003

4 **ST Document Number:** E2-ST-001-10

5 **TOE Identification:** The BorderGuard 3140/4000 VPN Firmware Release 6.2 and the VPN Manager Application Software Release 2.2

6 **Assurance Level:** Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.1*.

7 **Authors:** Blue Ridge Networks

8 **CC Version:** Common Criteria (CC) for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

9 **Keywords:** Virtual Private Network, VPN, Security Target, BorderGuard, encryption, decryption

1.2 Security Target (ST) Overview

10 The *Blue Ridge Networks* Centrally Managed PKI Embedded Virtual Private Network (VPN) enables multiple sites (enclaves) to communicate securely over an untrusted communication infrastructure (i.e. the internet). It provides secure communications combining the best security practices with simplicity of use. *Blue Ridge Networks* VPN allows access to corporate information from anywhere, at any time, with uncompromised security.

11 The TOE consists of the BorderGuard 3140/4000 Firmware (release 6.2) and the VPN Manager Application Software (release 2.2). The functionality offered by the TOE provides the capability for BorderGuard enclaves to communicate sensitive unclassified information securely with other BorderGuard enclaves. The TOE only provides protection of data in transit over a network. It does not provide security for data stored on enclave systems.

12 The TOE has the capability of encrypting network traffic between peer BorderGuard Cryptoservers running the BorderGuard 3140/4000 Firmware, authenticating an Authorized Administrator via a trusted path, and auditing security-relevant events that occur in the TOE. The TOE is intended for use in environments that are restricted to the processing of, up to and including, sensitive unclassified information.

13 This security target is closely based upon the NIAP developed *Basic VPN Protection Profile* (preliminary draft as of July, 2002). The principal difference is the TOE definition. Whereas, the Basic VPN PP defines a distributed managed architecture, the Blue Ridge security target defines a centrally managed VPN.

14 Blue Ridge Networks believes that the expanded TOE better reflects the way customers actually deploy and use VPNs, especially within the U.S. Government. In our experience, the skill and expertise required to reliably operate a VPN is not available at each site that hosts a VPN appliance. Therefore, these devices are commonly managed remotely over untrusted networks. In our opinion, the Basic VPN PP addresses a remote management model that will not scale.

15 The proper handling of public-keys used for authentication is a core requirement for all other VPN security. The *Blue Ridge Networks* VPN TOE includes trusted channels among Cryptoservers and the central management station. This expanded TOE scope encompasses all of the elements required for the exchange of public-key certificates used for node authentication.

1.3 Common Criteria (CC) Conformance Claim

16 The TOE has been developed to include components as defined in the Common Criteria (CC) Part 2. The TOE has been developed to conform to the (CC) Part 3 EAL2 assurance level.

1.4 Conventions, Terminology, Acronyms

17 The following section describes the conventions, terminology, and acronyms used in this document.

1.4.1 Conventions

18 The following section describes the conventions used in this document.

19 All requirements in this Security Target follow the requirements defined in CC v2.1.

20 Part 2 of the Common Criteria (CC) for Information Technology Security Evaluation defines a set of operations which are applied to Security Functional Requirements (SFR). The operations (iteration, assignment, selection, and refinement) are described below:

21 Iteration is the repetitive use of the same component. Iterations are indicated by a letter surrounded by parenthesis placed at the end of the component. An example of iteration is FMT_MSA.1(1) and FMT_MSA.1(2). This example shows two iterations of the FMT_MSA.1 requirement.

22 Assignment allows the author to specify a policy or a set of values. Assignments are indicated using bold and are surrounded by brackets ([**assignment**]).

23 Selection allows the author to pick an element from a list. Selections are indicated using underlined text and are surrounded by brackets ([selection]).

24 Refinement allows the author to add or remove details in order to meet a security objective. Refinements are indicated by using bold italics (***additions***).

1.4.2 Terminology and Acronyms

25 The following is a list of terminology and acronyms used in this Security Target (ST).

AES	Advanced Encryption Standard
BRE	Basic Robustness Environment
CC	Common Criteria for Information Technology Security Evaluation
CM	Configuration Management
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standard Publication
IATF	Information Assurance Technical Framework
IT	Information Technology
NOC	Network Operation Center
PKI	Public Key Infrastructure
PP	Protection Profile
SOC	Secure Operation Center
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSP	TOE Security Policy
VPN	Virtual Private Network

2 Target of Evaluation (TOE) Description

2.1 TOE Description

26 The TOE consists of two distinct components:

- the BorderGuard 3140/4000 Firmware, release 6.2; and,
- the VPN Manager Application Software, release 2.2.

27 The BorderGuard 3140/4000 Firmware resides on the *Blue Ridge Networks* VPN device. This device, also called a Cryptoserver, is either the BorderGuard 3140 or BorderGuard 4000. The VPN Manager Application Software resides and executes on a dedicated Windows based PC. The relationship between the two TOE components and the IT environment can be seen in Figure 1 – TOE and IT environment architecture.

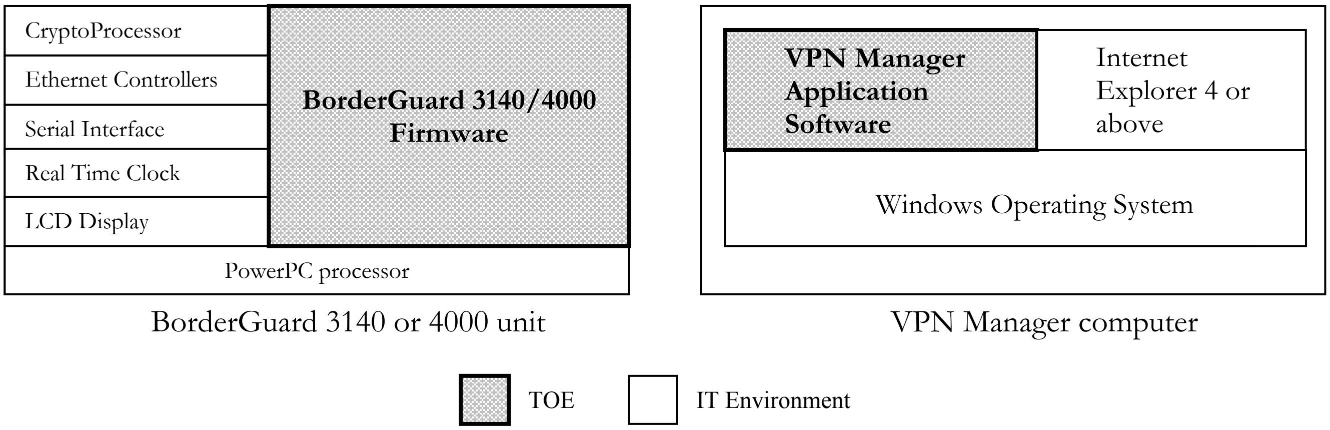

Figure 1 – TOE and IT environment architecture[1,2]

28 The TOE provides the functionality for the *Blue Ridge Networks* Virtual Private Network (VPN). The fundamental concept of operation for a *Blue Ridge Networks* VPN is a network of Cryptoservers centrally managed by a VPN Manager (see Figure 2 - VPN Architecture). Each Cryptoserver runs the BorderGuard 3140/4000 Firmware. The VPN Manager computer is directly connected via an ethernet crossover cable to a Cryptoserver, which is called the Secure Administrator Device, both the VPN Manager computer and the Secure Administrator Device are located in physically secure areas. The Secure Administrator Device provides secure connections to each Cryptoserver in the VPN for management traffic flowing to and from the VPN Manager Application Software.

[1] The Crypto Processor only exists on the BorderGuard 4000 unit.

[2] The VPN Manager computer requires Internet Explorer 4 or above for functionality reasons. Internet Explorer does not provide or support any security functions.

29 The TOE's security functionality protects the information transmitted via the VPN by:

- positively identifying each remote site using Public Key Infrastructure (PKI) technology
- protecting against man-in-the-middle intrusion by authenticating each packet of information that is transferred
- protecting against eavesdropping by encrypting each packet of information
- monitoring the entire system operation for unauthorized usage attempts.

30 The *Blue Ridge Networks* VPN is used to interconnect sites within a public or private internetwork. Even within a single organization, the Cryptoservers are generally used as gatekeepers that regulate the types of traffic that enter and exit the groups of computers and computer users. The BorderGuard 3140/4000 Firmware uses packet filtering to control information flow. With packet filtering it is possible to select all traffic that is legitimately going from one Cryptoserver to a specific remote Cryptoserver and protect it by sending it through a *sleeve,* which is a logical connection between the BorderGuard 3140/4000 Firmware running on each Cryptoserver. This sleeve armors the traffic moving between the Cryptoservers and sites according to the policy the authorized administrator sets for the connection. The policy defines the specific combination of encryption and tamper prevention for the data.

31 There are two parts to using a sleeve:

- When the first message is to be sent between two Cryptoservers, the Firmware on the respective BorderGuard units go through an authentication procedure. This procedure ensures that each BorderGuard unit knows that it is talking to the correct BorderGuard unit at the other end and that it is a trusted peer and not a potentially malicious third party attempting to receive the traffic.

- Once the message and source are authenticated, the two instances of Firmware can forward traffic between themselves over the sleeve. An operating sleeve is a "tunnel" between two points on an intermediate network that transports packet data without regard to its contents. If the sleeve is configured to do so, cryptographic protection of the data sent over the sleeve will ensure that anyone on the path between the two sites will find it impossible to effectively examine, or alter without detection, the data flowing between the sites.

32 As shown in Figure 2 - VPN Architecture, a system in enclave "A" is able to communicate with a system in enclave "C" via a secure channel while simultaneously communicating with a system in enclave "B" without encryption or authentication of the communication stream. As a result, enclave "A" is capable of creating VPN connections (sleeve) as well as non-VPN connections. This mechanism is known as a "VPN bypass capability."

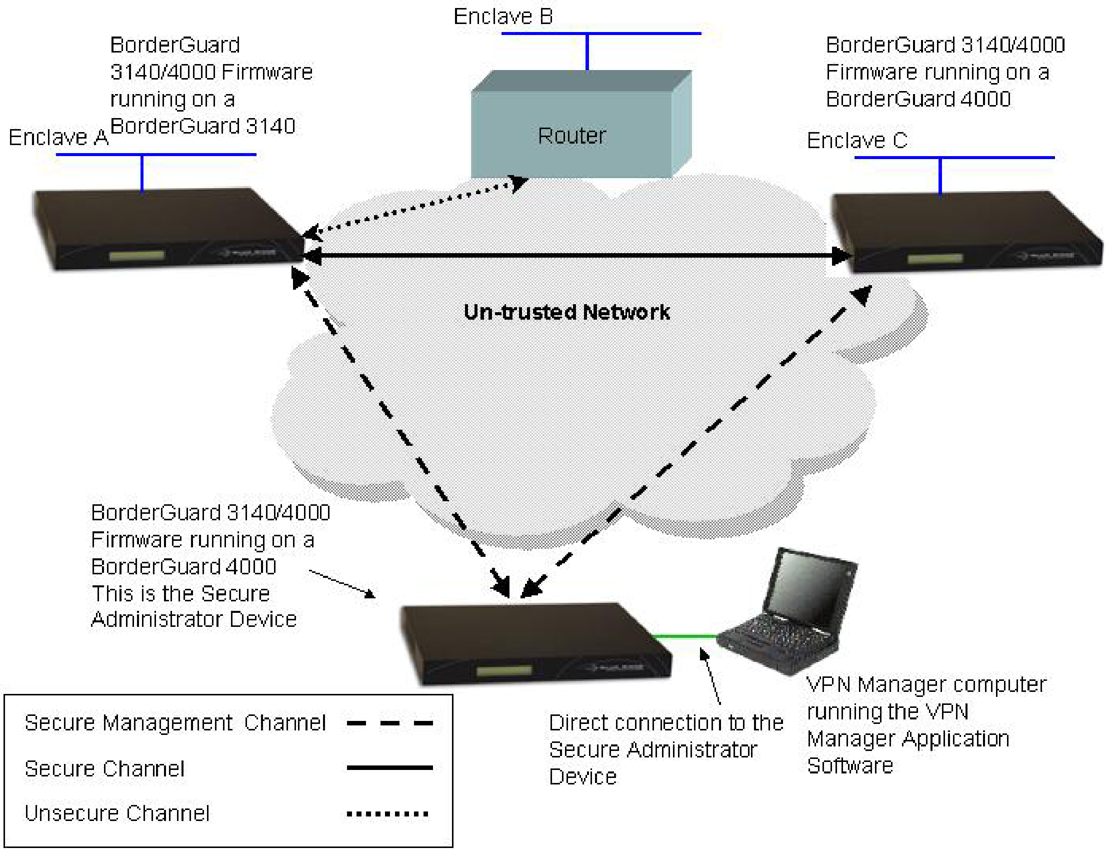
Enclave B
BorderGuard 3140/4000 Firmware running on a BorderGuard 3140
BorderGuard 3140/4000 Firmware running on a BorderGuard 4000
Enclave A
Router
Enclave C
Un-trusted Network
BorderGuard 3140/4000 Firmware running on a BorderGuard 4000 This is the Secure Administrator Device
VPN Manager computer running the VPN Manager Application Software
Direct connection to the Secure Administrator Device
Secure Management Channel - - -
Secure Channel ——
Unsecure Channel ....

Figure 2 - VPN Architecture

33 The VPN Manager Application Software is the primary management tool for managing the *Blue Ridge Networks* VPN. Communication to the managed Cryptoservers is secured by the Secure Administrator Device. The VPN Manager Application Software is used to define networks and associated Cryptoservers, provide a real time status display of the Cryptoservers, and it is the collection point of audit and alarm information from the entire VPN. The VPN Manager logs all user activity and monitors for intrusion attempts. Every connection, disconnection and failed authentication is logged to the VPN Manager by the Firmware. Audit records identify users and are time stamped. Any attempts to access a Cryptoserver using non-authenticated protocols are also recorded. Audit review is supported by the NT Event Viewer, which is part of the IT security environment.

34 The BorderGuard 3140/4000 Firmware (on a Cryptoserver) is located at each enclave boundary. Each instance of the Firmware authenticates itself to each of its peers. The Firmware, based upon VPN Manager Policy, agree upon cryptographic keys and algorithms. The Firmware generates cryptographic keys and encrypts network traffic in

accordance with the TOE security policy. The VPN Manager acts as the certificate authority for the Blue Ridge VPN, exchanging public keys.

35 Two types of information flow polices are implemented by the BorderGuard 3140/4000 Firmware, the Management Filter Policy allows management data to flow from the VPN Manager to each individual Cryptoserver, and, the User Security Policy allows communication between peer Cryptoservers.

36 The BorderGuard 4000/3140 Firmware implements cryptography (data encryption), key management, access control, authentication, data compression, replay prevention, and data integrity. The Firmware implements Triple DES and AES and the data integrity mechanisms conform to HMAC SHA-1. Key management and key exchange is implemented using Public Key Infrastructure (PKI).

2.2 Evaluated Configuration

37 ***Hardware:*** The BorderGuard 3140/4000 Firmware is evaluated on both BorderGuard 3140 and BorderGuard 4000 Cryptoservers. Both Cryptoservers contain the Firmware running on a PowerQuicc II processor which contains a PowerPC 603e core. A BorderGuard Cryptoserver contains 16 Mbytes of flash memory and 64 Mbytes of SDRAM. The 3140 and 4000 models differ only in that the 4000 series includes an additional 10/100 base-T Ethernet port, removable media (USB smartcard token, which is cryptographically mated with the chassis), and hardware cryptographic acceleration. Removing the USB smartcard token disables the boot firmware. This feature allows for "safeing" the BorderGuard, adding another level of security for an unattended, or an "in transit" BorderGuard.

38 The VPN Manager Application Software is run on a dedicated computer which conforms to the following specifications:

- Pentium series IBM PC-compatible computer with network interface card, HyperTerminal installed on a serial interface, CD-ROM reader, and a 3½" floppy drive
- 128 MB RAM
- 20 MB free disk space (varies due to database size)
- WinNT Server version 4.0 with NT Service Pack 4 or above and Microsoft Internet Server installed for the FTP Server capability, **OR**

  WinNT Workstation version 4.0 with NT Service Pack 4 or above and the Peer Web services installed for the FTP services, **OR**

  Windows 2000 Pro with Service Pack 1 or above and Internet Services Manager installed for the FTP services
- Microsoft TCP/IP installed on the network interface card
- Internet Explorer version 4 or above (including required Internet dlls)

39 ***VPN Configuration:*** The evaluated configuration consists of three instances of the BorderGuard 3140/4000 Firmware, running on two BorderGuard 3140 Cryptoservers and one BorderGuard 4000 Cryptoserver, and one instance of the VPN Manager Application Software. The VPN configuration can be seen in Figure 3 – Evaluated Configuration Architecture. The Firmware is configured so that a secure communications channel exists between LAN A and LAN B, and between each LAN A and LAN B and the Cryptoserver (Secure Administrator Device) protecting the VPN Manager PC at the bottom.

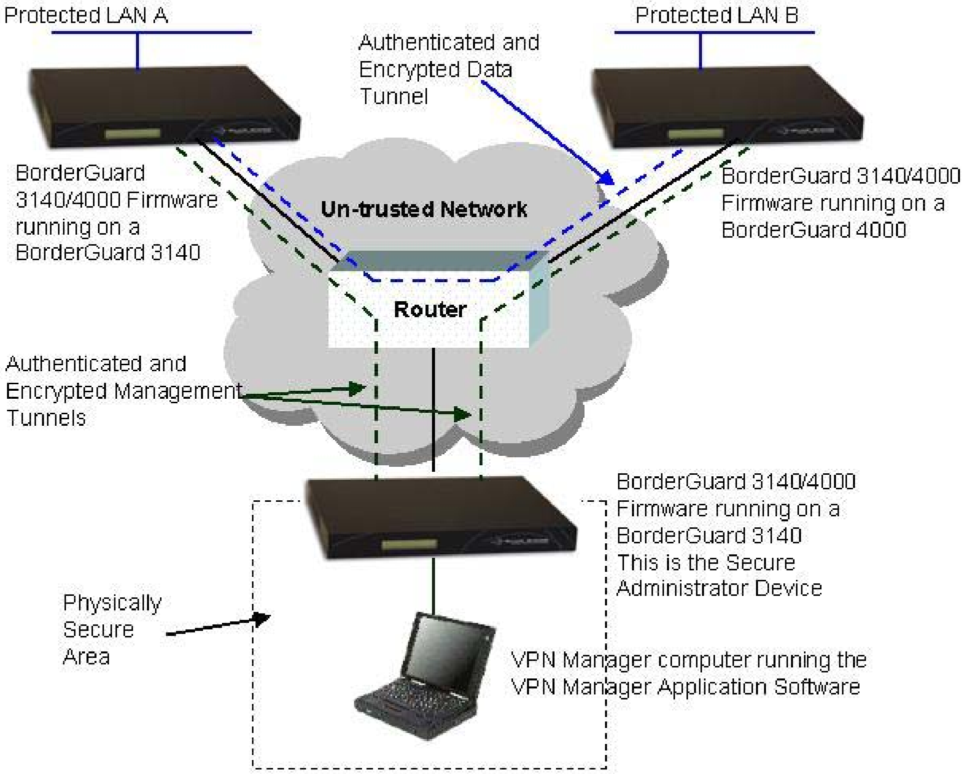
Protected LAN A
Protected LAN B
Authenticated and Encrypted Data Tunnel
BorderGuard 3140/4000 Firmware running on a BorderGuard 3140
Un-trusted Network
BorderGuard 3140/4000 Firmware running on a BorderGuard 4000
Router
Authenticated and Encrypted Management Tunnels
BorderGuard 3140/4000 Firmware running on a BorderGuard 3140 This is the Secure Administrator Device
Physically Secure Area
VPN Manager computer running the VPN Manager Application Software

Figure 3 – Evaluated Configuration Architecture

40 ***BorderGuard 3140/4000 Firmware Configuration:*** The Firmware of the LAN A Cryptoserver has been configured as a "bump in the wire" meaning that it is acting as a bridge between the inside and outside Ethernets it attaches. All packets pass freely except for those addressed to LAN B. These are encrypted, re-encapsulated and forwarded to the LAN B Cryptoserver. Encrypted packets arriving from LAN B are decrypted and forwarded to the appropriate station on LAN A.

41 The Firmware of the LAN B Cryptoserver has been configured as a "perfect firewall" separating the trusted and un-trusted Ethernet subnets. Only packets arriving through an

authenticated tunnel from LAN A are forwarded into the trusted subnet. The only data packets permitted to flow from the trusted to the un-trusted side of the BorderGuard are ones that have been encrypted for delivery to LAN A.

42 The third instance of the Firmware has been configured as a “Secure Administrator Device”, which protects the VPN Manager PC and provides an authenticated and encrypted management channel to the Firmware of the LAN A Cryptoserver and to the LAN B Cryptoserver.

2.3 Physical Boundaries

43 The physical boundary of the TOE is defined by the two distinct components that comprise the TOE: the BorderGuard 3140/4000 Firmware, version 6.2 and, the VPN Manager Application Software, version 2.2. Figure 1 – TOE and IT environment architecture illustrates these two components and how they are related to other system components.

2.4 Logical Boundaries

44 The logical boundary of the TOE is defined by the functionality provided by the BorderGuard 3140/4000 Firmware, version 6.2 and, the VPN Manager Application Software, version 2.2, as described in the preceding sections.

3 TOE Security Environment

This section describes the assumptions about the security aspects of the TOE environment, threats to TOE assets or to the TOE environment that must be countered and organizational security policies that the TOEs must enforce.

3.1 Security Usage Assumptions

45 The following is a list of security assumptions made of the TOE environment. The Authorized Administrator manages the BorderGuard 3140/4000 Firmware on the Cryptoservers from a separate secured enclave (see Figure 2 - VPN Architecture) using the VPN Manager Application Software. The only user of the TOE is the Authorized Administrator.

A.HARDENED

46 The underlying operating system of the VPN Manager computer will be installed and configured so that all mechanisms and services that are not required by the TOE are disabled. The Cryptoserver units will not run any other software or firmware other than the BorderGuard 3140/4000 Firmware.

A.NO_ENCLAVE_PROTECTION

47 The Firmware component of the TOE will not protect the confidentiality or integrity of data from threat agents inside an enclave. However, the Firmware component of the TOE will protect the confidentiality and integrity of data in transit between peer Cryptoservers.

A.NO_EVIL

48 Authorized Administrators are non-hostile, appropriately trained and follow all administrator guidance. However, they are capable of error.

A.NO_GENERAL_PURPOSE

49 There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the hardware on which the TOE components reside (the Cryptoservers and the VPN Manager computer).

A.PHYSICAL_SECURITY

50 The hardware on which the TOE components reside (the Cryptoservers and the VPN Manager computer) will reside in a physically secure environment.

A.VPNMNGR_ACCESS

51 Only Authorized Administrators have access rights to the VPN Manager computer.

A.SECURITY_POLICY

52 The Firmware on peer Cryptoservers will be administered to enforce compatible[3] security policies.

A.TOE_ENTRY_POINT

53 Information cannot flow between external IT entities located in different enclaves without passing through the Firmware.

A.PROTECTION

54 The IT environment will protect the TOE from inadvertent bypass or disablement.

A.TIMESTAMPS

55 The IT environment will provide the TOE with reliable timestamps.

3.2 Threats To Security

56 This section lists the threats to the TOE and to the operating environment. Threats to the TOE are based on the Basic Robustness Environment (BRE). Threats associated with TEMPEST, covert channels, and coding errors have been excluded from consideration. Attacks by improper use of the TOE bypass capability are also not considered.

3.2.1 Threats Addressed by the TOE

57 The threats discussed below are addressed by the TOE. The threat agents are unauthorized persons or external IT entities not authorized to access the TOE (i.e., administer the TOE).

T.ADMIN_ACCESS

58 A threat agent may circumvent the TOE's security policy (TSP) by gaining access to the administrative functions of the TOE.

[3] Compatible is defined to mean that a core set of policy rules are identical and any differences are more restrictive.

T.ATTACK_CONFIGURATION_DATA

59 A threat agent may attempt to read, modify, or destroy security-critical TOE configuration data.

T.ATTACK_POTENTIAL

60 A threat agent, using obvious vulnerabilities, may attempt to circumvent TOE security functions (TSF) to gain access to the TOE or the assets it protects.

T.AUDIT_UNDETECTED

61 A threat agent may undertake some action which causes auditable events to go undetected.

T.BRUTE_FORCE

62 A threat agent may repeatedly try to guess the Authorized Administrator's authentication data in order to launch an attack against the TOE.

T.CRYPTOGRAPHIC_ATTACK

63 A threat agent, using a cryptographic attack, may obtain information for which they are not authorized.

T.KEY_COMPROMISE

64 A threat agent, through the use of stolen or compromised cryptographic keys, may decrypt sensitive data and gain unauthorized access to sensitive data.

T.INTEGRITY

65 A threat agent may modify sensitive information while it is in transit between protected enclaves.

T.MASQUERADE

66 A threat agent, through the use of stolen or compromised cryptographic keys, may masquerade as an element of the TOE, thereby gaining unauthorized access to sensitive data. A threat agent, through the use of captured identification and authentication data, may masquerade as an Authorized Administrator of the TOE. A threat agent may masquerade as an element of the TOE thereby capturing valid identification and

authentication data.

3.2.2 Threats addressed by the Non-IT Environment

67 Threats to the non-IT environment are associated with improperly configuring of the TOE. These threats will be countered by procedural measures or administrative methods.

T.CONFIGURATION

68 The TOE may be inadvertently configured, administered or used in an insecure manner by an Authorized Administrator.

T.POOR_MAINTENANCE

69 Authorized Administrators may not have installed software or hardware patches correcting known problems that may result in a compromise of confidentiality or integrity of TOE data.

3.2.3 Threats addressed by the IT Environment

T.PROTECTION

70 The TOE security functionality could be bypassed or compromised by a threat agent.

T.NONAUTH_ACCESS

71 A threat agent may circumvent the TOE's security policy (TSP) by gaining access to the VPN Manager computer and hence the TOE.

3.3 Organizational Security Policies

72 The organizational security policies described below are addressed by the TOE.

P.ACCOUNTABILITY

73 Authorized Administrators shall be held accountable for all security-relevant actions.

P.AUDIT_REVIEW

74 Audit data shall be reviewed, analyzed, and acted upon, when necessary.

P.BYPASS

75 All network traffic not sent to a peer Cryptoserver shall be allowed to bypass the Firmware device security mechanisms. Specifically, for outbound traffic not associated with a peer Cryptoserver, the local Firmware will not invoke the security mechanisms and a secure channel will not be established. Likewise, for inbound network traffic not associated with a peer Cryptoserver, the local Firmware will not invoke the security mechanisms and a secure channel will not be established.

P.CONFIDENTIALITY

76 All network traffic sent to or received from addresses associated with a peer Cryptoserver shall be encrypted or decrypted by the Firmware where specified by the security policy. Specifically, for outbound traffic associated with a peer Cryptoserver the local Firmware will create or use an existing secure channel between the peer Cryptoservers. Likewise, for inbound traffic associated with a peer Cryptoserver, the local Firmware will use an existing secure channel between the peer Cryptoservers.

4 Security Objectives

77 This chapter describes the security objectives for the Target of Evaluation (TOE) and the operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 TOE Security Objectives

78 This section defines the security objectives that are to be addressed by the TOE. The mapping and rationale for the security objectives are described in Section 8.

O.ACCOUNTABILITY

79 The TOE must provide accountability of Firmware and of Authorized Administrator use of security functions before granting access to a TOE functions.

O.ADMINISTRATION

80 The TOE must provide administrative tools to enable the Authorized Administrator to effectively manage and maintain the Firmware component of the TOE. The administrative tools provide the only means to administer the TOE and are only accessible by an Authorized Administrator.

O.AUDIT

81 The TOE must provide a means to accurately detect and record security-relevant events in audit records.

O.CONFIDENTIALITY

82 The TOE must protect the confidentiality of data between Cryptoservers via the use of encryption. Additionally, the TOE must protect the confidentiality of the Firmware's dialogue with the Authorized Administrator through encryption.

O.INTEGRITY

83 The TOE must be capable of protecting the integrity of data transmitted to Cryptoservers via encryption. Upon receipt of data from a peer Cryptoserver, the Firmware on the Cryptoserver must verify that the received data accurately represents the data that was originally transmitted

O.CYRPTO

84 The TOE must utilize cryptographic modules that are compliant with FIPS PUB 140-2.

O.MEDIATE

85 The TOE must mediate the flow of information between Cryptoservers in accordance with its security policy.

O.SECURITY_INFRASTRUCTURE

86 The TOE must protect the confidentiality and integrity of key management data and must ensure the proper exchange of keys.

O.SELF_PROTECT

87 From its initial startup, the TOE must protect itself against attempts to modify, deactivate, or circumvent the TOE security functions (TSF).

4.2 Security Objectives for the Environment

88 This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The mapping and rationale for the security objectives are described in Section 8.

OE.HARDENED

89 The underlying operating system of the VPN Manager computer will be installed and configured so that all mechanisms and services that are not required by the TOE are disabled. The Cryptoserver units will be installed and configured with only the BorderGuard 3140/4000 Firmware.

OE.NO_ENCLAVE_PROTECTION

90 The Firmware component of the TOE will not protect the confidentiality or integrity of data from threat agents inside an enclave. However, the Firmware component of the TOE will protect the confidentiality and integrity of data in transit between peer Cryptoservers.

OE.NO_EVIL

91 Authorized Administrators are non-hostile, appropriately trained and follow all administrator guidance. However, they are capable of error.

OE.NO_GENERAL_PURPOSE

92 There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the hardware on which the TOE components reside (the Cryptoservers and the VPN Manager computer).

OE.PHYSICAL_SECURITY

93 The hardware on which the TOE components reside (the Cryptoservers and the VPN Manager computer) will reside in a physically secure environment.

OE.VPNMNGR_ACCESS

94 Only Authorized Administrators have access rights to the VPN Manager computer.

OE.SECURITY_POLICY

95 The Firmware on peer Cryptoservers will be administered to enforce compatible[4] security policies.

OE.TOE_ENTRY_POINT

96 Information cannot flow between external IT entities located in different enclaves without passing through the Firmware.

OE.CONFIGURATION

97 The TOE, and any underlying operating system and hardware, must be installed, administered, and maintained (i.e., security-related hardware and software fixes) in a manner that preserves the integrity and confidentiality of TOE data (e.g., configuration data, administrative data, etc.) and data traversing the TOE.

OE.TIMESTAMPS

98 The IT environment shall provide the TOE with reliable timestamps.

OE.PROTECTION

99 The IT environment will protect the TOE from inadvertent bypass or disablement.

[4] Compatible is defined to mean that a core set of policy rules are identical and any differences are more restrictive.

OE.AUDIT_REVIEW

100 The IT environment will provide the Authorized Administrator a means of reviewing the audit records generated by the TOE.

OE.ACCESS

101 The IT environment will ensure only the Authorized Administrator has access to the VPN Manager Application Software by providing the identification and authentication mechanism.

5 IT Security Requirements

102 This section provides functional and assurance requirements that are satisfied by the TOE and the IT environment. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 TOE Security Functional Requirements

103 The security functional requirements for the TOE consist of the following components derived from Part 2 of the CC, summarized in Table 1 below. The functional components are presented in alphabetical order by component name as in the CC.

Functional Components	
FAU_ARP.1	Security Alarms
FAU_GEN.1(1)	Audit Data Generation
FAU_SAA.1	Potential Violation Analysis
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Distribution
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1(1,2&3)	Cryptographic Operation
FDP_IFC.1(1&2)	Subset Information Flow Control
FDP_IFF.1(1&2)	Simple Security Attributes
FDP_ITT.1	Basic Internal Transfer Protection
FDP_ITT.3	Integrity Monitoring
FIA_AFL.1(1)	Authentication Failure Handling
FIA_UAU.2(1)	User Authentication Before Any Action
FIA_UID.2(1)	User Identification Before Any Action
FMT_MOF.1	Management of Security Functions Behavior
FMT_MSA.1(1&2)	Management of Security Attributes
FMT_MSA.3(1&2)	Static Attribute Initialization
FMT_MTD.1	Management of TSF Data
FMT_MTD.3	Secure TSF Data

Functional Components	
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_ITT.2	TSF Data Transfer Separation
FPT_ITT.3	TSF Data Integrity Monitoring
FPT_RPL.1	Replay Detection

Table 1 – TOE Security Functional Requirements

5.1.1 Security audit (FAU)

FAU_ARP.1 Security alarms

104 FAU_ARP.1.1 - The TSF shall take [**action to generate an audit record and alert the Authorized Administrator**] upon detection of a potential security violation.

FAU_GEN.1(1) Audit data generation

105 FAU_GEN.1.1(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 events:**

- **User identification (success/failure)**
- **User authentication (success/failure)**
- **Firmware authentication (on a request to establish a sleeve) (success/failure)**
- **Sleeve establishment (success/failure)**
- **Key generation (success/failure)**
- **Key destruction (success/failure)**
- **Cryptographic Operation (encryption/decryption, data integrity hash) (success/failure)**

- **Potential security violations**
- **Replay occurred**
- **The VPN Manager Application Software generates the following audit data:**
- **Key distribution (success/failure)**
- **Firmware upload (success/failure)**
- **Cryptoserver status**
- **Firmware initialization (success/failure)**
- **Password change (success/failure)**].

106 FAU_GEN.1.2(1) - 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, 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 specified for each event in the document *Blue Ridge VPN Manager User Guide (part no. BRN-EN-VUG-112502-002-002)]***.

FAU_SAA.1 Potential violation analysis

107 FAU_SAA.1.1 – The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

108 FAU_SAA.1.2 – The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [**unsuccessful use of authentication mechanisms and cryptographic operation failure**] known to indicate a potential security violation;

b) [no additional rules].

5.1.2 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

109 FCS_CKM.1.1 – The TSF shall generate cryptographic keys in accordance with a

specified cryptographic key generation algorithm [**Diffie-Hellman**] and specified cryptographic key sizes [**512 and 1024 binary digits in length**] that meet the following: [**none**].

FCS_CKM.2 Cryptographic key distribution

110 FCS_CKM.2.1 – The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**Public Key Infrastructure (PKI)**] that meets the following: [**FIPS PUB 140-2, Security Level 1**]

FCS_CKM.4 Cryptographic key destruction

111 FCS_CKM.4.1 - The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**which zeroizes all plaintext cryptographic keys and other unprotected security parameters within the device**] that meets the following: [**FIPS PUB 140-2, Security Level 1**].

FCS_COP.1(1) Cryptographic operation

112 FCS_COP.1.1 (1) - The TSF shall perform [**encryption and decryption as defined in the TOE security policy**] in accordance with a specified cryptographic algorithm [**Triple Data Encryption Standard (3DES)**] and cryptographic key sizes [**that are 112 bits in length (2 Des key EDE cipher)**] that meet the following: [**FIPS PUB 140-2, Security Level 1**].

FCS_COP.1(2) Cryptographic operation

113 FCS_COP.1.1 (2) - The TSF shall perform [**encryption and decryption as defined in the TOE security policy**] in accordance with a specified cryptographic algorithm [**Advanced Encryption Standard (AES)**] and cryptographic key sizes [**that are 256 binary digits in length**] that meet the following: [**FIPS PUB 140-2, Security Level 1**].

FCS_COP.1(3) Cryptographic operation

114 FCS_COP.1.1 (3) - The TSF shall perform [**a secure hash of network traffic as defined in the TOE security policy**] in accordance with a specified cryptographic algorithm [**Secure Hash Standard 1 (SHA-1)**] and cryptographic key sizes [**160 bits in length**] that meet the following: [**FIPS PUB 140-2, Security Level 1**].

5.1.3 User data protection (FDP)

FDP_IFC.1(1) Subset information flow control

115 FDP_IFC.1.1 (1) - The TSF shall enforce the [**management filter policy**] on

[a) **subjects: VPN Manager or managed VPN devices that send and receive management traffic through the TOE to one another;**

b) **information: management traffic sent to or from the TOE; and**

c) **operation: pass encrypted information based on destination IP address**].

FDP_IFC.1(2) Subset information flow control

116 FDP_IFC.1.1 (2) - The TSF shall enforce the [**user filter policy**] on

[a) **subjects: external IT entities or peer VPN devices that send and receive information through the TOE to one another;**

b) **information: traffic sent through the TOE; and**

c) **operation: pass encrypted information based on destination IP address and pass unencrypted (i.e., plain text) information based on destination IP address**].

FDP_IFF.1(1)Simple security attributes

117 FDP_IFF.1.1 (1) - The TSF shall enforce the [**management filter policy**] based on the following types of subject and information security attributes:

[a) **subject security attributes:**

- **management filter policy settings for presumed address; and**

b) **information security attributes:**

- **presumed address of source subject (IP); and**
- **presumed address of destination subject (IP)**].

118 FDP_IFF.1.2 (1) – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **[for any traffic destined to a managed VPN device from the VPN Manager, the SA device will create or use an existing secure**

channel to the managed VPN devices; and

- **for any traffic destined to the VPN Manager from a managed VPN device, the managed device will create or use an existing secure channel to the VPN Manager SA device**.].

119 FDP_IFF.1.3 (1) - The TSF shall enforce the [**no additional information control SFP rules**].

120 FDP_IFF.1.4 (1) -The TSF shall provide the following [**no additional SFP capabilities**].

121 FDP_IFF.1.5 (1) - The TSF shall explicitly authorise an information flow based on the following rules: [**source address and destination address**].

122 FDP_IFF.1.6 (1) - The TSF shall explicitly deny an information flow based on the following rules: [**if management traffic is sent to a destination address (IP) for a device that has not been defined to the VPN Manager**].

FDP_IFF.1(2) Simple security attributes

123 FDP_IFF.1.1 (2) - The TSF shall enforce the [**user filter policy**] based on the following types of subject and information security attributes:

[**a) subject security attributes:**

- **presumed address**

b) information security attributes:

- **presumed address of source subject (IP);**
- **presumed address of destination subject (IP);**
- **transport layer protocol; and**
- **Security Labeling**].

124 FDP_IFF.1.2 (2) - The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[**a) Subjects on an internal network can cause information to be encrypted over a secure channel if:**

- **for outbound traffic associated with a peer VPN device, the local VPN device will create or use an existing secure channel between the peer VPN devices; and**

- **for inbound traffic associated with a peer VPN device, the local VPN device will use an existing secure channel between the peer VPN devices.**

b) **Subjects on a network can cause information to be sent unencrypted over an open channel if:**

- **for outbound traffic not associated with a peer VPN device, the local VPN device will not invoke the security mechanisms and a secure channel will not be established; and**
- **for inbound network traffic not associated with a peer VPN device, the local VPN device will not invoke the security mechanisms and a secure channel will not be established**].

125 FDP_IFF.1.3 (2) - The TSF shall enforce the [**no additional informational control SFP rules**].

126 FDP_IFF.1.4 (2) - The TSF shall provide the following [**no additional SFP capabilities**].

127 FDP_IFF.1.5 (2) - The TSF shall explicitly authorize an information flow based on the following rules: [**source address and destination address**].

128 FDP_IFF.1.6 (2) - The TSF shall explicitly deny an information flow based on the following rules: [**if management traffic is sent to a destination address (IP) for a device that has not been defined to the VPN Manager**].

FDP_ITT.1 Basic Internal Transfer Protection

129 FDP_ITT.1.1 The TSF shall enforce the [**user filter policy**] to prevent the [disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.3 Integrity Monitoring

130 FDP_ITT.3.1 The TSF shall enforce the [**user filter policy**] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [modification of data, substitution of data, re-ordering of data, deletion of data].

131 FDP_ITT.3.2 Upon detection of a data integrity error, the TSF shall [**drop the packet and generate an alarm**].

5.1.4 Identification and Authentication (FIA)

FIA_AFL.1(1) Authentication failure handling

132 FIA_AFL.1.1 (1) - The TSF shall detect when [**one**] unsuccessful authentication attempts occurs related to [**an Authorized Administrators' attempt to authenticate on the BorderGuard 3140/4000 Firmware**].

133 FIA_AFL.1.2 (2)- When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**log the event and alert the Authorized Administrator**].

FIA_UAU.2(1) User authentication before any action

134 FIA_UAU.2.1 (1) - The ***BorderGuard 3140/4000 Firmware*** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2(2)User identification before any action

135 FIA_UID.2.1 (2) - The ***BorderGuard 3140/4000 Firmware*** shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

5.1.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behavior

136 FMT_MOF.1.1 - The TSF shall restrict the ability to [determine the behavior of, enable, disable, modify the behavior of] the functions [

- **VPN membership;**
- **Public Key exchange between Cryptoservers in a VPN;**
- **Security attributes for information flow control policies on each Cryptoserver;**
- **Cryptographic key attributes;**
- **Cryptographic parameters of a VPN connection (VPN cryptographic policy); and,**
- **User network access policy for each enclave**]

to [**an Authorized Administrator**].

FMT_MSA.1(1) Management of security attributes

137 FMT_MSA.1.1 (1) - The TSF shall enforce the [**management filter policy**] to restrict the ability to [modify**,** delete, **or [create]**] the security attributes [**information flow rules in FDP_IFF.1(1)**] to [**an Authorized Administrator**].

FMT_MSA.1(2) Management of security attributes

138 FMT_MSA.1.1 (2) - The TSF shall enforce the [**user filter policy**] to restrict the ability to [modify, delete, **or [create]**] the security attributes [**information flow rules in FDP_IFF.1(2)**] to [**an Authorized Administrator**].

FMT_MSA.2 Secure security attributes

139 FMT_MSA.2.1 - The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3(1) Static attribute initialisation

140 FMT_MSA.3.1 (1) - The TSF shall enforce the [**management filter policy**] to provide [restrictive] values for security attributes that are used to enforce the SFP.

141 FMT_MSA.3.2 (1) - The TSF shall allow the [**Authorized Administrator**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3 Static attribute initialization (2)

142 FMT_MSA.3.1 (2) - The TSF shall enforce the [**user filter policy**] to provide [restrictive] values for security attributes that are used to enforce the SFP.

143 FMT_MSA.3.2 (2) - The TSF shall allow the [**Authorized Administrator**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

144 FMT_MTD.1.1 - The TSF shall restrict the ability to [query, delete, **or [generate]**] the [**cryptographic key attributes in FCS_CKM.1**] to [**the Authorized Administrator**].

FMT_MTD.3 Secure TSF data

145 FMT_MTD.3.1 - The TSF shall ensure that only secure values are accepted for TSF data.

FMT_SMF.1 Specification of Management Functions

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

- **Initialize Firmware;**
- **Manage information flow control policies;**
- **Regenerate session keys;**
- **Create, modify and delete VPNs;**
- **Public key exchange;**
- **Manage cryptographic key elements;**
- **Manage Firmware authentication data; and,**
- **Monitor VPN status**].

FMT_SMR.1 Security roles

147 FMT_SMR.1.1 - The TSF shall maintain the roles [**Authorized Administrator**].

148 FMT_SMR.1.2 - The TSF shall be able to associate users with role.

5.1.6 Protection of the TOE Security Functions (FPT)

FPT_AMT.1 Abstract machine testing

149 FPT_AMT.1.1 – The TSF shall run a suite of tests [during initial start-up] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_ITT.2 TSF Data Transfer Separation

150 FPT_ITT.2.1 - The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

151 FPT_ITT.2.2 The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

FPT_ITT.3 TSF Data Integrity Monitoring

152 FPT_ITT.3.1 The TSF shall be able to detect [modification of data, substitution of data, re-ordering of data, deletion of data] for TSF data transmitted between separate parts of the TOE.

153 FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: [**drop the packet and raise an alarm**].

FPT_RPL.1 Replay detection

154 FPT_RPL.1.1 - The TSF shall detect replay for the following entities: [**peer VPN device authentication**].

155 FPT_RPL.1.2 - The TSF shall perform [**ignore the attempted replay operation and generate an audit record**] when replay is detected.

5.2 Security Functional Requirements for the IT Environment

The security functional requirements for the IT Environment consist of the following components derived from Part 2 of the CC, summarized in Table 2 – IT Environment Security Functional Requirements below. The functional components are presented in alphabetical order by component name as in the CC.

Functional Components	
FAU_GEN.1(2)	Audit Data Generation
FAU_SAR.1	Audit Review
FIA_AFL.1(2)	Authentication Failure Handling
FIA_UAU.2(2)	User authentication before any action
FIA_UID.2(2)	User identification before an action
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps

Table 2 – IT Environment Security Functional Requirements

5.2.1 Security audit (FAU)

FAU_GEN.1(2) Audit data generation

156 FAU_GEN.1.1(2) - The ***IT environment*** 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 events:**

- **User identification (success/failure)**
- **User authentication (success/failure)].**

157 FAU_GEN.1.2(2) - The ***IT environment*** shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, 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, [**none**].

FAU_SAR.1 Audit review

158 FAU_SAR.1.1 - The ***IT Environment*** shall provide [**Authorised Administrator**] with the capability to read [**all audit trail data**] from the audit records.

159 FAU_SAR.1.2 - The ***IT Environment*** shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.2 Identification and Authentication (FIA)

FIA_AFL.1(2) Authentication failure handling

160 FIA_AFL.1.1 (2) - The ***IT environment*** shall detect when [**one**] unsuccessful authentication attempts occurs related to [**an Authorized Administrator's attempt to authenticate on the VPN Manager**].

161 FIA_AFL.1.2 (2)- When the defined number of unsuccessful authentication attempts has been met or surpassed, the ***IT environment*** shall [**log the event**].

FIA_UAU.2(2) User authentication before any action

162 FIA_UAU.2.1 (2) - The ***IT environment*** shall require each user to be successfully authenticated before ***the TOE allows*** any TSF-mediated actions on behalf of that user.

FIA_UID.2(2)User identification before any action

163 FIA_UID.2.1 (2) - The ***IT environment*** shall require each user to identify itself before ***the TOE allows*** any TSF mediated actions on behalf of that user.

5.2.3 Protection of the TOE Security Functions (FPT)

FPT_RVM.1 Non-bypassability of the TSP

164 FPT_RVM.1.1 - The ***IT environment*** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

165 FPT_SEP.1.1 - The ***IT environment*** shall maintain a security domain for ***the TOEs*** execution that protects ***the TOE*** from interference and tampering by untrusted subjects.

166 FPT_SEP.1.2 - The ***IT environment*** shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

167 FPT_STM.1.1 - The ***IT environment*** shall be able to provide reliable time stamps for ***the TOEs*** use.

5.3 TOE Security Assurance Requirements

168 The assurance security requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL2 level of assurance. These assurance components are summarized in Table 3.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 3 - Assurance Requirements: EAL2

5.4 TOE Strength of Function Claim

169 The probabilistic or permutational mechanisms in the Blue Ridge VPN TOE are the security functional requirements that provide cryptographic support (FCS family) and the authentication of the Authorized Administrator (FIA_UAU.2). The claimed minimum strength of function is SOF-basic.

6 TOE Summary Specification

170 The TOE summary specification describes the security functions and assurance measures, and traces them to the TOE Functional and Assurance requirements.

6.1 Security Function Description

6.1.1 Audit

171 The Audit function is performed by both components of the TOE. The VPN Manager is the central component for all audit data for the VPN. The BorderGuard 3140/4000 Firmware sends audit events to the VPN Manager. These event messages are transmitted to the VPN Manager over the encrypted secure management channel that exists between each Cryptoserver and the Secure Administrator Device. The connection between the Secure Administrator Device and the VPN Manager computer is secured physically by connecting the Secure Administrator Device directly to the VPN Manager, using an Ethernet cross-over cable, with no other network appliances in between.

172 The BorderGuard 3140/4000 Firmware generates the following audit data:

- User identification (success/failure)
- User authentication (success/failure)
- Firmware authentication (on a request to establish a sleeve) (success/failure)
- Sleeve establishment (success/failure)
- Key generation (success/failure)
- Key destruction (success/failure)
- Cryptographic Operation (encryption/decryption, data integrity hash) (success/failure)
- Potential security violations
- Replay occurred

173 The VPN Manager Application Software generates the following audit data:

- Key distribution (success/failure)
- Firmware upload (success/failure)
- Cryptoserver status
- Firmware initialization (success/failure)
- Password change (success/failure)

The audit messages include the following information:

- Date and time of event
- Type of event
- Subject identity
- Success or Failure of the event
- And the additional information specified for each event in the document *Blue Ridge VPN Manager User Guide (part no. BRN-EN-VUG-112502-002-002).*

174 The VPN Manager formats event messages that it generates, and those received from the Firmware, and reports them to the local Windows Application Event log using Windows APIs embedded in the VPN Manager program. The Windows NT Event log provides the storage for the audit trail and allows audit review by the authorized administrator.

175 When an event is sent to the Event Log, the Alarm Button on the VPN Manager Graphical User Interface (GUI) will change color to indicate the highest severity of the alarms that were logged. The Windows Event Viewer can be accessed directly from the Window's control panel or it can be invoked from the VPN Manager by clicking on the Alarm Button on the VPN Manager GUI. Once the Alarm Button on the VPN Manager is clicked the color will revert back to cyan indicating that no alarms have been recorded since the last inspection.

176 The Audit function maps to the following TOE SFRs:

- FAU_ARP.1
- FAU_GEN.1
- FAU_SAA.1
- FIA_AFL.1(1)

6.1.2 Cryptographic

177 The Cryptographic function is performed by the DPF Cryptographic subsystem of the BorderGuard 3140/4000 Firmware. The DPF Cryptographic subsystem's core function is to establish and maintain the cryptographic tunnels (sleeves). To provide this functionality, the BorderGuard 3140/4000 Firmware performs key generation, key distribution, key destruction, encryption, decryption, replay protection, integrity checking and authentication. The DPF Cryptographic subsystem consists of several components:

- An "authentication task" charged with establishing and maintaining sleeves. This consists of originating the RSA public key and Diffie-Hellmann key exchange challenges to a remote DPF entity, receiving and processing such traffic from remote sites, and sending background traffic to ensure the sleeve is still active. The authentication task also provides facilities to negotiate cryptographic Type Of Service with the remote end, and a set of timeout facilities to terminate a sleeve, or establish a sleeve to an alternate destination, if the current one proves unresponsive.

- A "codec" that is responsible for the cryptographic transformation of data packets, given an already negotiated Type Of Service and secret session keys.
- Forwarding logic that receives packets to be cryptographically encoded from the Filtering function, or receives incoming cryptographically encoded packets from remote DPF entities and arranges for their successful decryption.

The DPF Cryptographic subsystem maps to the following TOE SFRs:

- FCS_CKM.1: The DPF Cryptographic subsystem creates keys using Diffie-Hellmann Key Exchange. Two different key sizes are generated, 512 bits for short keys and 1024 bits for long keys.
- FCS_CKM.2: The Cryptographic function manages key distribution using Public Key Infrastructure (PKI). Each instance of Firmware generates its own public/private key pair (using the DPF Cryptographic subsystem) and sends its public key to the VPN Manager Application Software. The VPN Manager Application Software acts as the certificate authority for the Blue Ridge VPN, exchanging public keys. A database containing all of the public keys for the VPN are distributed to each instance of Firmware by the VPN Manager.
- FCS_CKM.4: The DPF Cryptographic subsystem is responsible for key destruction, which is carried out using zeroisation, a technique which writes zero bits over all plaintext cryptographic keys and other associated security parameters. Each instance of Firmware is responsible for destruction of the keys it holds.
- FCS_COP.1 (1,2&3): The DPF Cryptographic subsystem supports two encryption/ decryption algorithms: 3DES and AES.

  For the purposes of integrity checking, the DPF Cryptographic subsystem will compute an HMAC by computing the cryptographic residue of the packet contents, any possible replay header, and a portion of the secret cryptographic key material computed at session initialization. The residue is appended to the end of the packet during transmission. Upon receipt by the receiving DPF Cryptographic subsystem, the residue is recomputed and compared with the value supplied with the delivered packet; the packet is considered to be unaltered if the two match. One data integrity algorithm is supported: SHA-1.
- FDP_ITT.3: The DPF Cryptographic subsystem provides integrity checking on all data that is transmitted between peer Cryptoservers. Integrity checking is performed by using a HMAC as described above. If any alteration to the data is detected

(modification, substitution, re-ordering, deletion) by the receiving DPF Cryptographic subsystem it drops the packet and generates an event message. This event message is sent to the VPN Manager via the Audit function. The Audit function then generates an alarm when the event is sent to the Event Log via the Alarm Button on the VPN Manager Graphical User Interface (GUI) which will change color to indicate the severity of the alarms that was logged.

- FPT_ITT.3: The DPF Cryptographic subsystem provides integrity checking on all data that is transmitted between the Secure Administrator Device and each Cryptoserver. Integrity checking is performed by using a HMAC as described above. If any alteration to the data is detected (modification, substitution, re-ordering, deletion) by the receiving DPF Cryptographic subsystem it drops the packet and generates an event message. This event message is sent to the VPN Manager via the Audit function. The Audit function then generates an alarm when the event is sent to the Event Log via the Alarm Button on the VPN Manager Graphical User Interface (GUI) which will change color to indicate the severity of the alarms that was logged.
- FPT_RPL.1: The DPF Cryptographic subsystem provides Replay Prevention, or the ability to reject packets that are re-presented to a DPF Cryptographic subsystem receiver some time after they were originally transmitted by the sender. The DPF Cryptographic subsystem performs this action by stamping a header on the packet consisting of a packet sequence number and the time of sleeve establishment. Upon receipt, the receiving DPF Cryptographic subsystem will determine whether the packet has been received before, and generate an audit message and ignore the packet if so.

6.1.3 Filtering

178 The Filtering function resides in the BorderGuard 3140/4000 Firmware. It uses packet filter policies to monitor and control the flow of packets through the Cryptoserver based on policy rules. The TOE has two distinct information flows, management data and user data. The two information flows use sleeves to secure the data. Management data is data that terminates at BorderGuard 3140/4000 Firmware or at the VPN Manager. User data is data that is destined for a subnet protected by a Cryptoserver in the VPN, which is running BorderGuard 3140/4000 Firmware. Both information flows use the rules set in the packet filter policy definitions to determine the appropriate action for a given packet.

179 The Authorized Administrator sets the packet filtering policy definitions via the VPN Manager Application software. When a policy is created or modified, the affected Cryptosevers are uploaded with the new definitions. Upon initial installation, The VPN Manager enables each instance of the BorderGuard 3140/4000 Firmware with a default set of secure packet filtering policies.

180 The Firmware uses the packet filtering policies and the packet's source and destination

address to determine if a given packet needs to be directed down a sleeve to its destination or if it can be transmitted in the clear (VPN Bypass). The function enforces a security policy as follows:

- for outbound traffic associated with a peer Cryptoserver, the local Cryptoserver will create or use an existing secure channel between the peer Cryptoserver;
- for outbound traffic not associated with a peer Cryptoserver, the local Cryptoserver will not invoke the security mechanisms and a secure channel will not be established;
- for inbound traffic associated with a peer Cryptoserver, the local Cryptoserver will use an existing secure channel between the peer Cryptoserver; and
- for inbound network traffic not associated with a peer Cryptoserver, the local Cryptoserver will not invoke the security mechanisms and a secure channel will not be established.

181 The process of establishing the sleeves is the responsibility of the Cryptographic function, however the responsibility for determining which packets are sent through which sleeves (or bypass a sleeve) is the responsibility of the Filtering function.

182 All communication between the Cryptoservers and the VPN Manager occurs over a secure encrypted channel. This includes configuration data being sent from the VPN Manager to the Cryptoservers as well as the audit records sent from the Cryptoservers to the VPN Manager. This is accomplished by having the VPN Manager behind a Cryptoservers called a security administrator device. The VPN Manager and all of the managed Cryptoservers are configured to only communicate to each other over this secure channel. The filter policies and cryptographic support allows the channel to be encrypted, authenticated, and allows the filtering out of any packets not allowed by any of the VPN devices.

183 The Filtering function maps to the following TOE SFRs:

- FDP_IFC.1 (1&2): The Filtering function enforces the Management Filter Policy and the User Filter Policy on all packets passing through the Cryptoserver.
- FDP_IFF.1 (1&2): The Filtering function determines if a packet falls under the Management Filter Policy or the User Filter Policy. Once the correct policy is determined (based on source and destination address) the Filtering function determines if the packet should be sent over a secure channel, and if so which secure channel) or if it can be sent in the clear(open channel).
- FDP_ITT.1: The Filtering function enforces the User Filter Policy on data that needs to be sent over a sleeve between peer Cryptoservers. The enforcement of the rules in this

policy ensure that the data is protected (by encryption) from disclosure and modification while it is being transmitted between the peers.

- FDP_ITT.3: The Filtering function enforces the User Filter Policy on data that needs to be sent over a sleeve between peer Cryptoservers. This ensures the data is monitored (via an attached HMAC) for integrity errors when it is being transmitted between the peers.

- FPT_ITT.1: The Filtering function enforces the Management Filter Policy on all TSF (Management) data which is transmitted between the Secure Administrator Device and each Cryptoserver by using a secure encrypted channel. This ensures that the data is protected (by encryption) from disclosure and modification while it is being transmitted and ensures that management data is transmitted through its own sleeve that does not transmit any user data, thus keeping management and user data separate.

6.1.4 Identification & authentication

184 The BorderGuard 3140/4000 Firmware and the VPN Manager require the Authorized Administrator to be identified and authenticated prior to allowing any security function actions to be taken. The TOE has one role, the Authorized Administrator. The Authorized Administrator logs onto the VPN Manager computer using their valid Windows NT user id and password. Once successfully authenticated by Windows the Authorized Administrator has access to the VPN Manager Application Software. To access the individual Cryptoservers, the Authorized Administrator must then log in to the Firmware running on each. This process is managed by the VPN Manager Application Software, which communicates (via a secure channel) to the Firmware.

185 The Identification and Authentication function maps to the following TOE SFRs:

- FIA_UID.2(1): The user must be successfully identified before the TOE allows any security function actions to be taken by the user.

- FIA_UAU.2(1): The user must be successfully authenticated before the TOE allows any security function actions to be taken by the user.

6.1.5 Security management

186 The VPN Manager Application Software provides the interface to management functions for the TOE. The Firmware on the Cryptoservers is centrally managed by the VPN Manager. One security role is maintained, that of the Authorized Administrator. The Security Management function allows the Authorized Administrator to:

- Initialize Firmware with default secure policies with secure security attributes for the management filter policy and user filter policy
- Change the initial values for the information flow control policies when the Firmware is initialized

- Add or remove Cryptoservers from the VPN; a VPN consists of two or more Cryptoservers that can be configured into three types of VPNs:
    - Fully Meshed: All VPN segments are virtually connected to each other. The Cryptoservers located at each site enable communications to every other site in the VPN.
    - Central Office: Only a single Cryptoserver (at the Central Office) is enabled to communicate to all other Cryptoservers in the VPN. Every other Cryptoserver in the VPN enables communications only to and from the Central Office Site.
    - Partial Mesh: Sleeves defined in a fully meshed VPN can be "Undefined" to create a partial mesh VPN.
- Monitor the status of Cryptoservers on the VPN
- Define the VPN cryptographic policy (all sleeves defined for the VPN will be defined the same, in other words they will all use the same key length, encryption, integrity checking, and replay prevention settings). The VPN policy will consist of a set devices that can participate in the VPN. The policy will be specified by IP Addresses. Devices participate fully in the VPN, in other words the policy will not specify that a device can communicate with one device and not be able to communicate with another device.
- Change the password for each instance of Firmware
- Access the audit trail (provides a means to access the NT Event Viewer)
- Generate, delete and query the status of cryptographic key attributes
- Modify, delete or assign the authentication data associated with the Authorized Administrator role

187 All security attribute settings and changes to TSF data are made via the VPN Manager GUI. The packet filter policies generated by the during initialization are by default restrictive and secure. However there is a mechanism to change to the default filter policy by editing the policy on the VPN device of interest. The VPN Manager is designed to ensure that any of the configurable attributes present to the administrator only allow secure values.

188 The security management function maps to the following TOE SFRs:

- FMT_MOF.1
- FMT_MSA.1(1&2)
- FMT_MSA.2
- FMT_MSA.3(1&2)

- FMT_MTD.1
- FMT_MTD.3
- FMT_SMF.1
- FMT_SMR.1

6.1.6 Self Test

189 The Self Test function of the TOE performs abstract machine testing. During start up the BorderGuard 3140/4000 Firmware performs a series of tests on the underlying hardware of the Cryptoserver. If any test fails, the Cryptoserver is considered defective and the boot process halts. The reason for the test failure is provided to the Authorized Administrator in the Cryptoserver LCD display.

190 The Self Test function maps to the following TOE SFR: FPT_AMT.1

6.1.7 TSF to SFR Mapping

191 The following table provides a visual mapping between the TSF identified above and the TOE security functional requirements.

	AUDIT	CRYPTOGRAPHIC	FILTERING	IDENTIFICATION & AUTHENTICATION	SECURITY MANAGEMENT	SELF TEST
FAU_ARP.1	X					
FAU_GEN.1(1)	X					
FAU_SAA.1	X					
FCS_CKM.1		X				
FCS_CKM.2		X				
FCS_CKM.4		X				
FCS_COP.1(1)		X				
FCS_COP.1(2)		X				
FCS_COP.1(3)		X				
FDP_IFC.1(1)			X			
FDP_IFC.1(2)			X			
FDP_IFF.1(1)			X			

	AUDIT	CRYPTOGRAPHIC	FILTERING	IDENTIFICATION & AUTHENTICATION	SECURITY MANAGEMENT	SELF TEST
FDP_IFF.1(2)			X			
FDP_ITT.1			X			
FDP_ITT.3		X	X			
FIA_AFL.1		X				
FIA_UAU.2(1)				X		
FIA_UID.2(1)				X		
FMT_MOF.1					X	
FMT_MSA.1(1)					X	
FMT_MSA.1(2)					X	
FMT_MSA.2					X	
FMT_MSA.3(1)					X	
FMT_MSA.3(2)					X	
FMT_MTD.1					X	
FMT_MTD.3					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_AMT.1						X
FPT_ITT.2			X			
FPT_ITT.3		X				
FPT_RPL.1		X				

Table 4 – TOE Security Functions to SFR mapping

6.2 Assurance Measures

6.2.1 Configuration Management

192 The configuration and control of the VPN Manager Application Software and the BorderGuard 3140/4000 Firmware consists of uniquely identifying each release, each release has an associated unique label, configuration list describing the items that comprise the release, uniquely identifying the individual items, and documentation on how the items are uniquely identified.

193 These procedures are document in:

- "*Engineering Practices and Procedures*"
- "*Configuration Management Plan*".

194 The configuration management assurance measures satisfy the following assurance requirements:

ACM_CAP.2

6.2.2 Delivery and Operation

195 The delivery documentation describes the procedures to ensure that the TOE is received in a secure unmodified state. The installation and quick start operation guide describe the steps necessary for secure installation and start-up of the TOE.

196 These procedures are document in:

- "*Delivery Procedures*"
- "*VPN Manager Installation & Quick Start Guide*".

197 The delivery and operation assurance measures satisfy the following assurance requirements:

ADO_DEL.1

ADO_IGS.1

6.2.3 Development

198 The design documentation package contains functional specifications that completely describe the TOE security function (TSF) and its external interfaces. The external interfaces purpose and method of use is described including details of effects, exceptions, and error messages.

199 The high level design document describes the subsystems of the TOE with regards to the TSF. Each subsystem describes its, security functionality, interfaces to the subsystems, and if it is externally visible.

200 The high document flow from security target (ST) to functional specification (FS) to high level design (HLD) resolves detail of the security functionality respectively.

201 These development documents are listed below:

- "*BorderGuard Functional Specification*"
- "*VPN Manager Functional Specification*"
- "*BorderGuard High Level Design*"

- “*VPN Manager High Level Design*”

202 The development assurance measures satisfy the following assurance requirements:

ADV_FSP.1

ADV_HLD.1

ADV_RCR.1

6.2.4 Guidance Documents

203 Blue Ridge Networks provides administrator (user)[5] manuals for both the BorderGuard (Cryptoserver running BorderGuard 3140/4000 Firmware) and the VPN Manager (Application Software). These documents explain in great detail how the devices are to be utilized and give guidance on how to maintain a secure environment. The manuals describe the administrative functions, security functions, security parameter under the administrator control, and interfaces.

204 The guidance documentation is listed below:

- “*VPN Manager User Manual*”
- “*BorderGuard Manual*”

205 The guidance document assurance measures satisfy the following assurance requirements:

AGD_ADM.1

AGD_USR.1

6.2.5 Tests

206 The test documentation includes evidence of coverage, functional testing, and independent testing samples. The evidence of coverage describes the correspondence between the test and the security functions outline in the functional specification. The functional testing documentation consists of test plans, test procedures, and expected/actual test results. The test plans focus is on identifying the security functions that need to be tested and describe the goal of the tests. The test procedure describes how the tests are performed. The expected test results and test results from the developer should demonstrate that each tested security function behaves as specified.

207 The test documentation is listed below:

- “*Security Claims to Functional Tests Cross Matrix*”
- “*Test Plan*”

[5] The only role is that of administrator.

208 The test assurance measures satisfy the following assurance requirements:

ATE_COV.1

ATE_FUN.1

ATE_IND.2

6.2.6 Vulnerability Assessment

209 The Strength of Function (SOF) claims and the vulnerability assessment documentation detail the compliance of the BorderGuard to the SOF claims, in this SOF-basic security target (ST), and the relevant vulnerabilities of the TOE.

210 The SOF and vulnerability documentation is listed below:

- "*SPOCK*"
- "*Strength of Function (SOF) Compliance of the BorderGuard 6.2 firmware*"

211 The vulnerability assessment assurance measures satisfy the following assurance requirements:

AVA_SOF.1

AVA_VLA.1

7 Protection Profile (PP) Claims

212 There is no claimed PP conformance.

7.1 Protection Profile (PP) Reference

213 N/A

7.2 Protection Profile (PP) Refinements

214 N/A

7.3 Protection Profile (PP) Additions

215 N/A

8 Rationale

216 This section describes the rationale for the Security Objectives defined in Section 4 and the Security Requirements in Section 5. Additionally, this section describes the rationale for not satisfying all of the dependencies. Table 5 - Security Objectives to Threats/Policies Mapping illustrates the mapping from TOE Security Objectives to Threats and Policies. Table 6 – Environment Security Objectives to Threats Mapping illustrates the mapping from IT environment Security Objectives to Threats addressed by the IT environment.

8.1 Rationale for TOE Security Objectives

O.ACCOUNTABILITY

217 This security objective ensures that the Authorized Administrator is identified and authenticated before access to the TSF is granted and is accountable for all security-relevant actions; and ensures peer instances of Firmware are properly identified and authenticated prior to a secure connection being established. This objective counters the threats: T.ADMIN_ACCESS, T.BRUTE_FORCE, T.MASQUERADE, and supports P.ACCOUNTABILITY.

O.ADMINISTRATION

218 This security objective ensures that at all times only the Authorized Administrator can access the administrative functions and ensures that the Authorized Administrator can administer the TOE effectively and securely. This objective is necessary to counter the threats: T.ADMIN_ACCESS, T.BRUTE_FORCE and T.MASQUERADE.

O.AUDIT

219 This security objective ensures that security-relevant events are always completely and accurately recorded. This objective is necessary to counter the threats: T.AUDIT_UNDETECTED and T.BRUTE_FORCE.

O.CONFIDENTIALITY

220 This security objective ensures that the TOE utilizes encryption to protect data traveling between peer Cryptoservers and all administrative data between the Authorised Administrator (via the Secure Administrative Device) and the peer Cryptoservers . This objective is necessary to counter the threats: T.ATTACK_CONFIGURATION_DATA, T.CRYPTOGRAPHIC_ATTACK and T.KEY_COMPROMISE; the objective also supports the policy P.CONFIDENTIALITY.

O.INTEGRITY

221 This security objective ensures that all data transmitted between peer Cryptoservers is checked for integrity upon receipt to detect any changes made during transmit. This objective is necessary to counter the threats: T.ATTACK_CONFIGURATION_DATA, T.KEY_COMPROMISE, and T.INTEGRITY.

O.CRYPTO

222 This security objective ensures the TOE employs cryptography of adequate strength to protect data traveling between peer Cryptoservers (including the Secure Administrative Device). This objective is necessary to counter the threats: T.ATTACK_CONFIGURATION_DATA, T.CRYPTOGRAPHIC_ATTACK, T.KEY_COMPROMISE and T.MASQUERADE.

O.MEDIATE

223 This security objective ensures that all information flowing between peer TOEs will be mediated in accordance with the TOE security policy. This objective is necessary to counter the threats: T.ADMIN_ACCESS and T.ATTACK_POTENTIAL. The object also addresses the policies: P.BYPASS and P.CONFIDENTIALITY.

O.SECURITY_INFRASTRUCTURE

224 This security objective ensures that the TOE protects the confidentiality and integrity of key management data and ensures the proper exchange of keys. This objective is necessary to counter the threats: T.ATTACK_CONFIGURATION_DATA, T.CRYPTOGRAPHIC_ATTACK, T.KEY_COMPROMISE, T.MASQUERADE and T.INTEGRITY. The objective also addresses the policy P.CONFIDENTIALITY.

O.SELF_PROTECT

225 This security objective ensures that the TOE is always invoked, tamperproof and not capable of being circumnavigated. This objective is necessary to counter the threats: T.ATTACK_CONFIGURATION_DATA and T.ATTACK_POTENTIAL.

8.1.1 Mapping of Threats to TOE Security Objectives

T.ADMIN_ACCESS

226 This threat is mitigated by ensuring that the Authorized Administrator is identified and authorized prior being allowed access to the TOE (O.ACCOUNTABILITY) and by ensuring that only the Authorized Administrator has access to the management tools of

the TOE(O.ADMINISTRATION).

T.ATTACK_CONFIGURATION_DATA

227 This threat is mitigated by ensuring that the TOE encrypts all administrative data traveling between the Authorised Administrator (via the Secure Administrative Device) and the peer Cryptoservers (O.CONFIDENTIALITY); that the integrity of the data is verified upon receipt (O.INTEGRITY); and that strong cryptographic algorithms are used for both the encryption and integrity checking of the data (O.CRYPTO).

T.ATTACK_POTENTIAL

228 This threat is mitigated by reducing the attack potential of the TOE: by ensuring that the TOE always transmits data according to its security policy (O.MEDIATE) and ensuring the TOE protects itself against attempts to modify, deactivate or circumvent the TSF (O.SELF_PROTECT).

T.AUDIT_UNDETECTED

229 This threat is mitigated by ensuring that all relevant events are always detected by the TOE which then creates an audit record of the event (O.AUDIT).

T.BRUTE_FORCE

230 This threat is mitigated by reducing the chance of success of a brute force attack and providing an audit trail of such attempts. The TOE only has one user, the Authorized administrator, who must identify and authenticate themselves before gaining access to any TOE functions (O.ACCOUNTABILITY); the Authorized Administrator has the only access to administrative tools (O.ADMINISTRATION); and all failed authentication attempts will be audited to allow the Authorized Administrator to respond as appropriate (O.AUDIT).

T.CRYPTOGRAPHIC_ATTACK

231 This threat is mitigated by ensuring all data between TOE components is encrypted (O.CONFIDENTIALITY); that the encryption used is strong enough to protect the data (O.CRYPTO); and that the cryptographic keys are protected from unauthorized use (O.SECURITY_INFRASTRUCTURE).

T.KEY_COMPROMISE

232 This threat is mitigated by ensuring the cryptographic keys are managed in a way that

reduces the opportunity for a threat agent to steal or compromise them, by ensuring all administrative data is encrypted (O.CONFIDENTIALITY) and integrity checked (O.INTEGRITY), by using strong cryptographic algorithms are used ensuring strength of the keys (O.CRYPTO), and by ensuring that the cryptographic keys are protected from unauthorized use (O.SECURITY_INFRASTRUCTURE).

T.INTEGRITY

233 This threat is mitigated by ensuring that all data transferred is integrity checked upon receipt (O.INTEGRITY) and by ensuring that a threat agent does not have access to the cryptographic keys (O.SECURITY_INFRASTRUCTURE).

T.MASQUERADE

234 This threat is mitigated by reducing the opportunity for the threat. This is done by ensuring that the Authorized Administrator and peer Cryptoservers must identify and authenticate themselves before access to TOE security functions are permitted (O.ACCOUNTABILITY), ensuring that the Authorized Administrator has the only access rights to the administrative tools (O.ADMINISTRATION), ensuring all data is encrypted for transfer (O.CONFIDENTIALITY) and not sent in the clear where a third party could read identification and authentication data, ensuring the cryptographic algorithms in use are strong enough to protect the data (O.CRYPTO), and that the cryptographic keys are protected from unauthorized use (O.SECURITY_MANAGEMENT).

	T.ADMIN_ACCESS	T.ATTACK_ CONFIGURATION_DATA	T.ATTACK_POTENTIAL	T.AUDIT_UNDETECTED	T.BRUTE_FORCE	T.CRYPTOGRAPHIC_ ATTACK	T.KEY_COMPROMISE	T.INTEGRITY	T.MASQUERADE	P.ACCOUNTABILITY	P.BYPASS	P.CONFIDENTIALITY
O.ACCOUNTABILITY	X				X				X	X		
O.ADMINISTRATION	X				X				X			
O.AUDIT				X	X							
O.CONFIDENTIALITY		X				X	X		X			X
O.INTEGRITY		X					X	X				
O.CRYPTO		X				X	X		X			
O.MEDIATE	X		X								X	X
O.SECURITY_INFRASTRUCTURE		X				X	X	X	X			X
O.SELF_PROTECT		X	X									

Table 5 - Security Objectives to Threats/Policies Mapping

8.2 Rationale for Security Objectives for the Environment

235 All but four of the security objectives for the environment, OE.CONFIGURATION, OE.PROTECTION and OE.AUDIT_REVIEW, is a restatement of an assumption found in Section 3. Therefore, those security objectives for the environment trace to the assumptions trivially.

236 The non-IT security objective OE.CONFIGURATION is necessitated by the threats T.CONFIGURATION and T.POOR_MAINTENANCE. This additional non-IT security objective ensures that the TOE is properly administered.

237 The IT security objective OE.PROTECTION is necessitated by the threat T.PROTECTION. This additional IT security objective ensures that the TOE security functions are protected from bypass and compromise by the IT security environment.

238 The IT security objective OE.AUDIT_REVIEW is necessitated to assist meeting the policy P.AUDIT. This additional IT security objective ensures that the IT environment provides the Authorized Administrator will the means to review the TOE audit trail.

239 The non-IT security objective OE.ACCESS is necessitated by the threats T.NONAUTH_ACCESS. This additional IT security objective ensures that only the Authorized Administrator has access to the VPN Manager Application Software.

	T.CONFIGURATION	T.POOR_MAINTENANCE	T.PROTECTION	T.NONAUTH_ACCESS
OE.CONFIGURATION	X	X		
OE.PROTECTION			X	
OE.ACCESS				X

Table 6 – Environment Security Objectives to Threats Mapping

8.3 Rationale for Security Requirements

240 The functional and assurance requirements presented in this ST are mutually supportive and their combination meets the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. Table 5 - Security Objectives to Threats/Policies Mapping demonstrates the relationship between the threat, policies and the TOE security objectives. Table 6 – Environment Security Objectives to Threats Mapping demonstrates the relationship between the environmental security objectives and the threats addressed by the environment. Table 7 - Functional Requirements to Security Objectives Mapping demonstrates the mapping between the security requirements and the security objectives. Together these tables demonstrate the completeness and sufficiency of the security requirements.

8.3.1 Rationale for TOE Security Functional Requirements[6]

FAU_ARP.1 Audit Alarms

241 This component aids in the detection of intrusions and provides a function to alert the Authorized Administrator. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.AUDIT.

FAU_GEN.1(1) Audit Data Generation

242 This component outlines the data that must be included in audit records and the events that must be audited. It relies on FPT_STM.1 in the environment to provide reliable time stamps. This component traces back to and aids in meeting the following objective: O.AUDIT.

FAU_SAA.1 Potential Violation Analysis

243 This component ensures that repeated failed attempts to authenticate or to encrypt data are monitored and alarmed if the threshold of one unsuccessful attempt is reached. This component traces back to and aids in meeting the following objectives: O.AUDIT and O.SELF_PROTECT.

FCS_CKM.1 Cryptographic Key Generation

244 This component ensures that the keys and key management data generated are of adequate strength to protect the confidentiality and integrity of data transmitted between peer Firmware. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY, O.CRYPTO and O.SECURITY_INFRASTRUCTURE.

[6] For more detail on how the TOE meets the SFRs, refer to section 6.1.

FCS_CKM.2 Cryptographic Key Distribution

245 This component ensures that the keys and key management data are distributed securely to provide confidentiality and integrity of data transmitted between peer Firmware. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY, and O.SECURITY_INFRASTRUCTURE.

FCS_CKM.4 Cryptographic Key Destruction

246 This component ensures that the keys and key management data are correctly destroyed to protect the confidentiality and integrity of data transmitted between peer Firmware. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY, and O.SECURITY_INFRASTRUCTURE.

FCS_COP.1 (1) Cryptographic Operation

247 This component ensures that all data sent between peer Firmware components of the TOE, including Authorized Administrator communications, are encrypted using Triple Data Encryption Standard (3DES). This component identifies one of two encryption algorithms used by the TOE. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY and O.CRYPTO.

FCS_COP.1 (2) Cryptographic Operation

248 This component ensures that all data sent between peer Firmware components of the TOE, including Authorized Administrator communications, are encrypted using Advanced Encryption Standard (AES). This component identifies one of two encryption algorithms used by the TOE. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY, O.INTEGRITY and O.CRYPTO.

FCS_COP.1 (3) Cryptographic Operation

249 This component ensures that a secure hash of all data sent between peer Firmware components of the TOE, including Authorized Administrator communications, is created used Secure Hash Algorithm 1 (SHA-1). This component traces back to and aids in meeting the following objectives: O.INTEGRITY and O.CRYPTO.

FDP_IFC.1 (1) Subset Information Flow Control

250 This component identifies the entities involved in the Management Filter Policy information flow control SFP. This component traces back to and aids in meeting the following objective: O.MEDIATE.

FDP_IFC.1 (2) Subset Information Flow Control

251 This component identifies the entities involved in the User Filter Policy information flow control SFP. This component traces back to and aids in meeting the following objective: O.MEDIATE.

FDP_IFF.1 (1) Simple Security Attributes

252 This component identifies the attributes of the subjects sending and receiving the information in the Management Filter Policy SFP, as well as the attributes for the information itself. Then the operations identify under what conditions information is permitted to flow through the TOE. This component traces back to and aids in meeting the following objectives: O.MEDIATE.

FDP_IFF.1 (2) Simple Security Attributes

253 This component identifies the attributes of the subjects sending and receiving the information in the User Filter Policy SFP, as well as the attributes for the information itself. Then the operations identify under what conditions information is permitted to flow through the TOE. This component traces back to and aids in meeting the following objectives: O.MEDIATE.

FDP_ITT.1 Basic Internal Transfer Protection

254 This component ensures that user data is protected from disclosure and modification when it is transmitted between separate parts of the TOE (between separate instances of the Firmware) by enforcing the User Filter Policy on transmitted user data. This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY.

FDP_ITT.3 Integrity Monitoring

255 This component ensures that user data is protected from integrity errors when it is transmitted between separate parts of the TOE (between separate instances of the Firmware) by enforcing the User Filter Policy on transmitted user data. If an integrity error is detected the operation then drops the packet in questions and raises an alarm. This component traces back to and aids in meeting the following objectives: O.INTEGRITY.

FIA_AFL.1 (1) Authentication Failure Handling

256 This component ensures that human users who are not Authorized Administrators cannot endlessly attempt to authenticate without being detected. An audit log is created for each unsuccessful authentication attempt and the Authorized Administrator is alerted. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION, O.AUDIT and O.SELF_PROTECT.

FIA_UAU.2(1) User Authentication Before Any Action

257 This component ensures that the Authorized Administrator is authenticated before any action is allowed by the TSF. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FIA_UID.2(2) User Identification Before Any Action

258 This component ensures that the Authorized Administrator identity is identified to the TOE before anything occurs on behalf of the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FMT_MOF.1 Management of Security Functions Behavior

259 This component ensures that the TSF restricts the ability to modify the behavior of the specified functions to an Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MSA.1(1) Management of Security Attributes

260 This component ensures that the TSF restricts the ability to add, delete, and modify the security attributes that affect the Management Filter Policy SFP to only the Authorized Administrator. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.MEDIATE.

FMT_MSA.1(2) Management of Security Attributes

261 This component ensures that the TSF restricts the ability to add, delete, and modify the security attributes that affect the User Filter Policy SFP to only the Authorized Administrator. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.MEDIATE.

FMT_MSA.2 Secure Security Attributes

262 This component ensures that appropriate values are assigned to the security attributes used in the Management Filter Policy and User Filter Policy SFPs. This component traces back to and aids in meeting the following objectives: O.SELF_PROTECT.

FMT_MSA.3 (1) Static Attribute Initialization

263 This component ensures that there are restrictive default values implemented in the Management Filter Policy SFP which the Authorized Administrator can change. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.MEDIATE.

FMT_MSA.3 (2) Static Attribute Initialization

264 This component ensures that there are restrictive default values implemented in the User Filter Policy SFP which the Authorized Administrator can change. This component traces back to and aids in meeting the following objectives: O.ADMINISTRATION and O.MEDIATE.

FMT_MTD.1 Management of TSF Data

265 This component ensures that the TSF restricts the ability to modify the cryptographic key attributes (as defined in FCS_CKM.1) to only the Authorized Administrator. This

component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_MTD.3 Secure TSF Data

266 This component was chosen to ensure that appropriate values are assigned to TSF data. This component traces back to and aids in meeting the following objectives: O.SELF_PROTECT.

FMT_SMF.1 Security Roles

267 This component defines the security management functions of the TOE. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FMT_SMR.1 Security Roles

268 This component was chosen because each of the FMT components depends on the assignment of a user to the Authorized Administrator role. This component traces back to and aids in meeting the following objective: O.ADMINISTRATION.

FPT_AMT.1 Abstract Machine Testing

269 This component ensures that the security assumptions provided by the underlying abstract machine are tested during start-up. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FPT_ITT.2 TSF Data Separation

270 This component ensures that TSF (management) data is protected from disclosure and modification when it is transmitted between separate parts of the TOE (between separate instances of the Firmware). The operation also ensures the TSF data is separated from user data during transmission This component traces back to and aids in meeting the following objectives: O.CONFIDENTIALITY.

FDP_ITT.3 Integrity Monitoring

271 This component ensures that TSF (management) data is protected from integrity errors when it is transmitted between separate parts of the TOE (between separate instances of the Firmware). If an integrity error is detected the operation then drops the packet in questions and raises an alarm. This component traces back to and aids in meeting the following objectives: O.INTEGRITY.

FPT_RPL.1 Replay Detection

272 This component ensures that replay of authentication attempts are detected and audited. This component traces back to and aids in meeting the following objectives: O.AUDIT and O.ACCOUNTABILITY.

273 A summary of the security requirements to security objectives mapping is contained in the Table 7 - Functional Requirements to Security Objectives Mapping below.

8.3.2 Rationale for Security Functional Requirements for the Environment

FAU_GEN.1(2) Audit Data Generation

274 This component outlines the data that must be included in audit records and the events that must be audited. This component traces back to and aids in meeting the following objective: OE.AUDIT_REVIEW

FAU_SAR.1 Audit Review

275 This component ensures that the audit is understandable by an Authorized Administrator. This component traces back to and aids in meeting the following objective: OE.AUDIT_REVIEW.

276 The IT environment includes the Windows NT Event Viewer which runs on the VPN Manager computer. The NT Event Viewer provides the Authorized Administrator the ability to review and sort the TOE audit trail (the VPN Manager passes all generated event logs to the NT Event Application Log). The Authorized Administrator has the only access to the VPN Manager computer and therefore the only access to the NT Event logs.

FIA_AFL.1(2) Authentication failure handling

277 This component ensures that human users who are not Authorized Administrators cannot endlessly attempt to authenticate without being detected. An audit log is created for each unsuccessful authentication attempt. This component traces back to and aids in meeting the following objectives: OE.ACCESS.

278 The Windows operating system will log a failed authentication attempt on the VPN Manager computer after each failed attempt. The audit record is accessible by the administrator via the NT event viewer.

FIA_UAU.2(2) User Authentication Before Any Action

279 This component ensures that the Authorized Administrator is authenticated by the Windows operating system on the VPN Manager computer before any action is allowed by the TSF. This component traces back to and aids in meeting the following objective: OE.ACCESS.

280 The BorderGuard 3140/4000 Firmware and the VPN Manager require the Authorized Administrator to be identified and authenticated prior to allowing any security function actions to be taken. The TOE has one role, the Authorized Administrator. The Authorized Administrator logs onto the VPN Manager computer using their valid Windows NT user id and password. Once successfully authenticated by Windows the Authorized Administrator has access to the VPN Manager Application Software.

FIA_UID.2(2) User Identification Before Any Action

281 This component ensures that the Authorized Administrator identity is identified by the Windows operating system on the VPN Manager computer before anything occurs on behalf of the Authorized Administrator. This component traces back to and aids in meeting the following objective: OE.ACCESS.

282 The BorderGuard 3140/4000 Firmware and the VPN Manager require the Authorized Administrator to be identified and authenticated prior to allowing any security function actions to be taken. The TOE has one role, the Authorized Administrator. The Authorized Administrator logs onto the VPN Manager computer using their valid Windows NT user id and password. Once successfully authenticated by Windows the Authorized Administrator has access to the VPN Manager Application Software.

FPT_RVM.1 Non-bypassability of the TSP

283 This component ensures that the TSF enforcement functions are always invoked from initial start-up. This component traces back to and aids in meeting the following objective: OE.PROTECTION.

284 The BorderGuard 3140 and 4000 units run the Firmware on start up. Until the Firmware is properly initialized and running, no data can pass through the unit. The Windows operating system on the dedicated VPN Manager computer ensure non-bypassability of the VPN Manager Application Software.

FPT_SEP.1 TSF Domain Separation

285 This component ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: OE.PROTECTION.

286 The BorderGuard 3140 and 4000 units provide the Firmware with a dedicated secure domain. No other firmware or software runs in this environment, this providing the Firmware with a separate domain of execution. The by virtue of the operation of the Windows operating system, the VPN Manager Application Software is provided a separate domain of execution on the VPN Manager computer.

FPT_STM.1 Reliable Time Stamps

287 This component was included because FAU_GEN.1 depends on having the date and time accurately recorded in the audit records. This component traces back to and aids in meeting the following objective: OE.TIMESTAMPS.

288 The BorderGuard 3140 and 4000 units have a hardware clock. This clock is kept synchronized with the clock running on the VPN Manager computer. The combination of the hardware clock and the Windows operating system provide the reliable time stamp required for the audit records.

	O.ACCOUNTABILITY	O.ADMINISTRATION	O.AUDIT	O.CONFIDENTIALITY	O.INTEGRITY	O.CRYPTO	O.MEDIATE	O.SECURITY_ INFRASTRUCTURE	O.SELF_PROTECT		OE.AUDIT_REVIEW	OE.PROTECTION	OE.TIMESTAMPS	OE.ACCESS
FAU_ARP.1		X	X											
FAU_GEN.1(1)			X											
FAU_SAA.1			X						X					
FCS_CKM.1				X	X	X		X						
FCS_CKM.2				X	X			X						
FCS_CKM.4				X	X			X						
FCS_COP.1(1)				X	X	X								
FCS_COP.1(2)				X	X	X								
FCS_COP.1(3)					X	X								
FDP_IFC.1(1)							X							
FDP_IFC.1(2)							X							
FDP_IFF.1(1)							X							
FDP_IFF.1(2)							X							
FDP_ITT.1				X										
FDP_ITT.3					X									
FIA_AFL.1(1)		X	X						X					
FIA_UAU.2(1)	X													
FIA_UID.2(1)	X													
FMT_MOF.1		X												
FMT_MSA.1(1)		X					X							
FMT_MSA.1(2)		X					X							
FMT_MSA.2									X					
FMT_MSA.3(1)		X					X							
FMT_MSA.3(2)		X					X							
FMT_MTD.1		X												
FMT_MTD.3									X					
FMT_SMF.1		X												
FMT_SMR.1		X												

	O.ACCOUNTABILITY	O.ADMINISTRATION	O.AUDIT	O.CONFIDENTIALITY	O.INTEGRITY	O.CRYPTO	O.MEDIATE	O.SECURITY_ INFRASTRUCTURE	O.SELF_PROTECT		OE.AUDIT_REVIEW	OE.PROTECTION	OE.TIMESTAMPS	OE.ACCESS
FPT_AMT.1									X					
FPT_ITT.2				X										
FPT_ITT.3					X									
FPT_RPL.1	X		X											
FAU_GEN.1(2)											X			
FAU_SAR.1											X			
FIA_AFL.1(2)														X
FIA_UAU.2(2)														X
FIA_UID.2(2)														X
FPT_RVM.1												X		
FPT_SEP.1												X		
FPT_STM.1													X	

Table 7 - Functional Requirements to Security Objectives Mapping

8.4 Rationale for Assurance Requirements

289 The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

290 The general level of assurance for the TOE is:

- Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
- Appropriate for the threat environment specified in Section 3.

8.5 Rationale for Not Satisfying All Dependencies

291 Table 8 – Security Functional Requirement Dependencies Mapping shows the required dependencies for the security functional requirements defined in sections 5.1 and 5.2 and details if there are dependencies met within this Security Target.

SFR	Dependencies	Met By
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1
FAU_GEN.1(1)	FPT_STM.1	FPT_STM.1
FAU_SAA.1	FAU_GEN.1(1)	FAU_GEN.1(1)
FCS_CKM.1	[FCS_CKM.2 OR FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.2, FCS_COP.1(1,2&3), FCS_CKM.4, FMT_MSA.2
FCS_CKM.2	[FDP_ITC.1 OR FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	[FDP_ITC.1 OR FCS_CKM.1], FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1(1)	[FDP_ITC.1 OR FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1(2)	[FDP_ITC.1 OR FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_COP.1(3)	[FDP_ITC.1 OR FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1(1), FMT_MSA.3(1)
FDP_IFF.1(2)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1(2), FMT_MSA.3(2)
FDP_ITT.1	[FDP_ACC.1 OR FDP_IFC.1]	FDP_IFC.1(2)

SFR	Dependencies	Met By
FDP_ITT.3	[FDP_ACC.1 OR FDP_IFC.1], FDP_ITT.1	FDP_IFC.1(2), FDP_ITT.1
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2(1)
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1)
FIA_UID.2(1)	-	-
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1(1)	[FDP_ACC.1 OR FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_IFC.1(1), FMT_SMF.1, FMT_SMR.1
FMT_MSA.1(2)	[FDP_ACC.1 OR FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_IFC.1(2), FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 OR FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_IFC.1, FMT_MSA.1 (1&2), FMT_SMR.1
FMT_MSA.3(1)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1(1&2), FMT_SMR.1
FMT_MSA.3(2)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1(1&2), FMT_SMR.1
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3	ADV_SPM.1, FMT_MTD.1	ADV_SPM.1, FMT_MTD.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_AMT.1	-	-
FPT_ITT.2	-	-
FPT_ITT.3	FPT_ITT.1	FPT_ITT.2
FPT_RPL.1	-	-
▨	▨	▨
FAU_GEN.1(2)	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1(1)	FAU_GEN.1(1)
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2(2)
FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2)
FIA_UID.2(2)	-	-
FPT_RVM.1	-	-
FPT_SEP.1	-	-
FPT_STM.1	-	-

Table 8 – Security Functional Requirement Dependencies Mapping

292 With the exception of FMT_MSA.2 and FMT_MTD.3, all dependencies are contained in this Security Target. Both of these components have the assurance component

ADV_SPM.1, Informal TOE Security Policy Model, as a dependency. The removal of ADV_SPM.1 is justified because it was felt that the testing requirement specified in this ST would provide adequate assurance for a Basic Robustness Environment. ADV_SPM.1 is an EAL4 requirement and therefore is not aligned with the rationale provided for the chosen EAL.

8.6 Rationale for Strength of Function Claim

293 Part 1 of the CC defines "Strength of Function (SOF)" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three Strength of Function levels defined in Part 1, SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this security target (ST). SOF-basic states, "*a level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential*". The rationale for choosing SOF-basic was based on the TOE security objectives documented in Section 4 of this ST. SOF-basic level is necessary and sufficient to address the TOE security objectives that counter the threat T.ATTACK_POTENTIAL. Consequently, the metrics (i.e., passwords and keys) chosen for inclusion in this ST were determined to be acceptable for SOF-basic and would adequately protect information in a Basic Robustness Environment.

294 This security target includes a number of probabilistic or permutational functions. The list of relevant security functions and security functional requirements includes:

- Cryptographic support
  - FCS_COP.1(1,2&3) - Data Encryption, Hashing, Key Exchange
  - FCS_CKM.1 - Cryptographic Key Generation
  - FCS_CKM.2 - Cryptographic Key Distribution
  - FCS_CKM.4 - Cryptographic Key Destruction
- Identification and Authentication
  - FIA_UAU.2 – Authentication of administrators

9 References

[1] *Common Criteria for Information Technology Security Evaluation,* CCIB-98-031 Version 2.1, August 1999.

[2] *U.S. Department of Defense Virtual Private Network (VPN) Boundary Gateway Protection Profile for Basic Robustness Environments (BRE),* Version .6, September 2001.

[3] Federal Information Processing Standard Publication (FIPS-PUB) 197, *Advanced Encryption Standard (AES),* November 2001.