Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00 (NDPP11E3/VPNGEP11) Security Target

Version 0.8
8/24/16

Prepared for:

Brocade Communication Systems, Inc.

130 Holger Way
San Jose, CA 95134

Prepared By:

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00 provided by Brocade Communication Systems, Inc. The TOE is being evaluated as a VPN Gateway.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- The NDPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00 (NDPP11E3/VPNGEP11) Security Target

ST Version – Version 0.8

ST Date – 8/24/16

1.2 TOE Reference

TOE Identification – Brocade Communication Systems, Inc Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00, including the following series and models

- Brocade NetIron MLXe Series Hardware Platforms with the BR-MLX-10GX4-IPSEC-M Card
  - BR-MLXe-4-MR2-M-AC, BR-MLXe-4-MR2-M-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
  - BR-MLXe-4-MR2-X-AC, BR-MLXe-4-MR2-X-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
  - BR-MLXe-8-MR2-M-AC, BR-MLXe-8-MR2-M-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
  - BR-MLXe-8-MR2-X-AC, BR-MLXe-8-MR2-X-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
  - BR-MLXe-16-MR2-M-AC, BR-MLXe-16-MR2-M-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
  - BR-MLXe-16-MR2-X-AC, BR-MLXe-16-MR2-X-DC
    - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
  - BR-MLXE-32-MR2-M-AC, BR-MLXE-32-MR2-M-DC
    - With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X
  - BR-MLXE-32-MR2-X-AC, BR-MLXE-32-MR2-X-DC
    - With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X

TOE Developer – Brocade Communication Systems, Inc

Evaluation Sponsor – Brocade Communication Systems, Inc

1.3 TOE Overview

The Target of Evaluation (TOE) is Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00 family of products.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Brocades' proprietary Multi-Service IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances. The TOE includes a card (BR-MLX-10GX4-IPSEC-M) that supports IPsec processing on the appliances.

All TOE appliances are configured at the factory with default parameters to allow immediate use of the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration (using the Multi-Service IronWare Federal Information Processing Standards and Common Criteria Guide) prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using IPsec. Once configured following the Common Criteria specific guidance, the TOE also offers an encrypted Web Management Interface using IPsec. All of the remote management interfaces are protected using encryption as explained later in this ST.

The hardware platforms that support the TOE have a number of common hardware characteristics:

- Central processor that supports all system operations, i.e. PowerPC etc.
- Dynamic memory, used by the central processor for all system operations

- Non-volatile flash memory, used to store the operating system image, startup configuration and other relevant files.
- Multiple physical network interfaces either fixed in configuration or removable as in a chassis based product.

1.4 TOE Description

The Target of Evaluation (TOE) is Brocade Communications Systems, Inc. Brocade MLXe® Family Devices with Multi-Service IronWare R06.0.00, including the following series and models.

- Brocade NetIron MLXe Series Hardware Platforms with the BR-MLX-10GX4-IPSEC-M Card
    - BR-MLXe-4-MR2-M-AC, BR-MLXe-4-MR2-M-DC
        - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
    - BR-MLXe-4-MR2-X-AC, BR-MLXe-4-MR2-X-DC
        - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
    - BR-MLXe-8-MR2-M-AC, BR-MLXe-8-MR2-M-DC
        - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
    - BR-MLXe-8-MR2-X-AC, BR-MLXe-8-MR2-X-DC
        - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
    - BR-MLXe-16-MR2-M-AC, BR-MLXe-16-MR2-M-DC
        - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
    - BR-MLXe-16-MR2-X-AC, BR-MLXe-16-MR2-X-DC
        - With management cards BR-MLX-MR2-M, BR-MLX-MR2-X
    - BR-MLXE-32-MR2-M-AC, BR-MLXE-32-MR2-M-DC
        - With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X
    - BR-MLXE-32-MR2-X-AC, BR-MLXE-32-MR2-X-DC
        - With management cards BR-MLX-MR2-32-M, BR-MLX-MR2-32-X

The following links offer additional information about the MLX series of the TOE:

- **Brocade MLX Series**

  http://www.brocade.com/products/all/routers/product-details/netiron-mlx-series/index.page

  http://www.brocade.com/content/brocade/en/backend-content/pdf-page.html?/content/dam/common/documents/content-types/datasheet/brocade-mlx-series-ds.pdf

While there are different models in the TOE, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. The MLX Series uses a Freescale MPC 7448, 1700 MHz CPU for the MR2 models. There are some performance differences among the models, but they each provide the same security characteristics as claimed in this security target.

The BR-MLX-10GX4-IPSEC-M Card is common across all platforms and provides the IPsec functionality. This card includes the P2010 processor (specifically P2010e) as well as the AESU 3.0.1, Brocade IPSEC FPGA and BRCD-LP-CRYPTO-VER-1.0 firmware.

1.4.1 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance, the Brocade IronWare OS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing functions). IronWare OS enforces applicable security policies on network information flowing through the hardware appliance.

The basic start-up operation of the TOE is as follows:

1. At system startup the operating system is transferred from flash memory to dynamic memory using a built-in hardware bootstrap.
2. The operating system reads the configuration parameters from the configuration file in non-volatile memory and then builds the necessary data structures in dynamic memory and begins operation.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface. The TOE will process other packets destined for itself (control path packets) based on the requirements of the given protocol (IPsec).

1.4.1.1 Physical Boundaries

Each TOE appliance runs a version of the Brocades software and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an external NTP server in the operational environment.

The TOE can be configured to use external RADIUS and TACACS+ authentication servers.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00: The TOE logical boundary consists of the security functionality of the products summarized in the following subsections

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

Note that use of the following features is limited in the evaluated TOE:

1. The use of SNMP has **not** been subject to evaluation. Note that SNMP can be used only to monitor as SNMP cannot access any security related parameters.
2. The *Strict Password Enforcement* setting is assumed to be **enabled** in the evaluated configuration.
3. The TOE will be operated in Common Criteria mode (a more restricted mode than FIPS mode).

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

The TOE includes the ability to communicate with a SYSLOG server in its environment to access its services. The TOE is designed to interact with each of those servers in accordance with their respective protocols, including security capabilities where applicable

1.4.1.2.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using IPsec to protect the logs while in transit on the network

1.4.1.2.2 Cryptographic support

The TOE contains a cryptographic module with algorithms that have been Cryptographic Algorithm Validation Program (CAVP)-certified that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including IPsec.

1.4.1.2.3 User data protection

The TOE performs a wide variety of network switching and routing functions, passing network traffic among its various network connections. While implementing applicable network protocols associated with network traffic routing, the TOE is carefully designed to ensure that it does not inadvertently reuse data found in network traffic. This is accomplished primarily by controlling the size of all buffers, fully overwriting buffer contents, and zero-padding of memory structures and buffers when necessary

1.4.1.2.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes.

1.4.1.2.5 Security management

The TOE provides Command Line Interface (CLI) commands and an HTTPS over IPsec Graphical User Interface (Web GUI) to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system

1.4.1.2.6 Packet Filtering

The TOE provides extensive packet filtering capabilities for IPv4, IPv6, TCP, and UDP. The authorized administrator can define packet filtering rules that apply to most every field within the identified packet types. The authorized administrator can define each rule to permit, deny, and log each decision.

1.4.1.2.7 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

Note that the TOE is a single appliance, and as such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

1.4.1.2.8 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

1.4.1.2.9 Trusted path/channels

The TOE protects interactive communication with administrators using IPsec for CLI access or for Web graphical user interface access (HTTPS over IPsec). In each case, the both integrity and disclosure protection is ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, the attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using IPsec connections to prevent unintended disclosure or modification of logs

1.4.2 TOE Documentation

Brocade offers a series of documents that describe the installation of the product as well as guidance for subsequent use and administration of the applicable security features. The following list of documents was examined as part of the evaluation:

- Brocade NetIron FIPS and Common Criteria Configuration Guide, Supporting Multi-Service Ironware R05.9.00aa, 53-1003826-01, 18 May 2016.

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant
- *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014 with the Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (NDPP11E3/VPNGEP11)
- Package Claims:
    - Assurance Level: EAL 1 conformant

2.1 Conformance Rationale

The ST conforms to the NDPP11E3/VPNGEP11. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDPP11E3/VPNGEP11 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDPP11E3/VPNGEP11 offers additional information about the identified security objectives, but that has not been reproduced here and the NDPP11E3/VPNGEP11 should be consulted if there is interest in that material.

In general, the NDPP11E3/VPNGEP11 has defined Security Objectives appropriate for network infrastructure device and as such are applicable to the Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00 TOE.

3.1 Security Objectives for the Operational Environment

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

OE.CONNECTIONS TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDPP11E3/VPNGEP11. The NDPP11E3/VPNGEP11 defines the following extended requirements and since they are not redefined in this ST the NDPP11E3/VPNGEP11 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_IPSEC_EXT.1: Extended: Internet Protocol Security (IPsec) Communications
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FIA_PMG_EXT.1: Password Management
- FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FIA_X509_EXT.1: Extended: X.509 Certificates
- FPF_RUL_EXT.1: Packet Filtering
- FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDPP11E3/VPNGEP11. The refinements and operations already performed in the NDPP11E3/VPNGEP11 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDPP11E3/VPNGEP11 and any residual operations have been completed herein. Of particular note, the NDPP11E3/VPNGEP11 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDPP11E3/VPNGEP11 which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDPP11E3/VPNGEP11 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The NDPP11E3/VPNGEP11 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Brocade MLXe Family Devices with Multi-Service IronWare R06.0.00 TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1: Extended: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_PMG_EXT.1: Password Management
	FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_X509_EXT.1: Extended: X.509 Certificates
FMT: Security management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1: Management of TSF Data (for general TSF data)

	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPF: Packet Filtering	FPF_RUL_EXT.1: Packet Filtering
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_FLS.1: Fail Secure
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions;
d) Specifically defined auditable events listed in **Table 2 Auditable Events.**

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, 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, information specified in column three **Table 2 Auditable Events**.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_RBG_EXT.1	None.	
FCS_IPSEC_EXT.1	Session Establishment with peer.	Entire packet contents of packets transmitted/received during session establishment

Requirement	Auditable Events	Additional Audit Record Contents
FDP_RIP.2	None.	
FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_X509_EXT.1	Establishing session with CA	Entire packet contents of packets transmitted/received during session establishment
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets
FPT_SKP_EXT.1	None.	
FPT_APW_EXT.1	None.	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 2 Auditable Events

5.1.1.2 User Identity Association (FAU_GEN.2)

FAU_GEN.2.1

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

5.1.1.3 External Audit Trail Storage (FAU_STG_EXT.1)

FAU_STG_EXT.1.1

The TSF shall be able to [***transmit the generated audit data to an external IT entity***] using a trusted channel implementing the [***IPsec***] protocol.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1)

FCS_CKM.1.1

Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with
- NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' for elliptic curve-based key establishment schemes and implementing 'NIST curves' P-256, P-384 and [***no other curves***] (as defined in FIPS PUB 186-3, 'Digital Signature Standard';
- NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' for finite field-based key establishment schemes;

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

FCS_CKM.1.2

Refinement: The TSF shall generate asymmetric cryptographic keys used for IKE peer authentication in accordance with a: [***FIPS PUB 186-3, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes*** and ***Appendix B.4 for ECDSA schemes and implementing NIST curves P-256, P-384 and [no other curves]]*** and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

5.1.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.1.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1(1).1

Refinement: The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in GCM, CBC, [***no other modes***] and cryptographic key sizes 128-bits, 256-bits, and [***no other key sizes***] that meets the following:
- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- NIST SP 800-38D, NIST SP 800-38A, [***no other standards***].

5.1.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1(2).1

Refinement: The TSF shall perform cryptographic signature services in accordance with a [***RSA Digital Signature Algorithm (RSA) with a key size (modulus) of 2048 bits or greater that meets FIPS PUB 186-2 or FIPS PUB 186-3, 'Digital Signature Standard', Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater] that meets FIPS PUB 186-3, 'Digital Signature Standard' with 'NIST curves' P-256, P-384 and [no other curves] (as defined in FIPS PUB 186-3, 'Digital Signature Standard')***].

5.1.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1(3).1

Refinement: The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-256, SHA-384***] and message digest sizes [***256, 384***] bits that meet the following: FIPS Pub 180-3, 'Secure Hash Standard.'

5.1.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4))

FCS_COP.1(4).1

Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-256, SHA-384***], key size [**equal to the input block size**], and message digest sizes [***256]*** bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

5.1.2.7 Extended: Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1)

FCS_IPSEC_EXT.1.1

The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2

The TSF shall implement [***tunnel mode***].

FCS_IPSEC_EXT.1.3

The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-GCM-128, AES-GCM-256 as specified in RFC 4106, [***no other algoritms***].

FCS_IPSEC_EXT.1.5

The TSF shall implement the protocol: [***IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23***) and [***no other RFCs for hash functions***]

FCS_IPSEC_EXT.1.6

The TSF shall ensure the encrypted payload in the [***IKEv2***] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and [***no other algorithm***].

FCS_IPSEC_EXT.1.7

The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8

The TSF shall ensure that [***IKEv2 SA lifetimes can be configured by an Administrator based on length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs***].

FCS_IPSEC_EXT.1.9

The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ('x' in gx mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [***224, 256, and 384***] bits.

FCS_IPSEC_EXT.1.10

The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^ [***256***].

FCS_IPSEC_EXT.1.11

The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), and [***20 (384-bit Random ECP***].

FCS_IPSEC_EXT.1.12

The TSF shall ensure that all IKE protocols perform peer authentication using a [***ECDSA***] that use X.509v3 certificates that conform to RFC 4945 and [***Pre-shared Keys***].

FCS_IPSEC_EXT.1.13

The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 IKE_SA***] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 CHILD_SA***] connection

5.1.2.8 Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90 using [Hash_DRBG (SHA-256)]***] seeded by an entropy source that accumulated entropy from [***a software-based noise source and a TSF-hardware-based noise source***].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

5.1.3 User data protection (FDP)

5.1.3.1 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.1.4 Identification and authentication (FIA)

5.1.4.1 Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1

Refinement: The TSF shall detect when an Administrator configurable positive integer of successive unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending remote administrator from successfully authenticating until an unlock action is taken by a local Administrator***].

5.1.4.2 Password Management (FIA_PMG_EXT.1)

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [***!, @, #, $, %, ^, &, *, (,),***];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

5.1.4.3 Extended: Pre-Shared Key Composition (FIA_PSK_EXT.1)

FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for IPsec and [***no other protocols]***].

FIA_PSK_EXT.1.2

The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [***up to and including 100 characters***];

-composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3

The TSF shall condition the text-based pre-shared keys by using [***no conditioning on the text string]***].

FIA_PSK_EXT.1.4

The TSF shall be able to [***accept***] bit-based pre-shared keys.

5.1.4.4 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.4.5 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, [***and access to external RADIUS and TACACS+***] to perform administrative user authentication.

5.1.4.6 User Identification and Authentication (FIA_UIA_EXT.1)

FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:
- Display the warning banner in accordance with FTA_TAB.1;
- [***network routing services]***].

FIA_UIA_EXT.1.2

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

5.1.4.7 Extended: X.509 Certificates (FIA_X509_EXT.1)

FIA_X509_EXT.1.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [***no other protocols***] connections.

FIA_X509_EXT.1.2

The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.1.3

The TSF shall provide the capability for authenticated Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

FIA_X509_EXT.1.4

The TSF shall generate a Certificate Request Message as specified in RFC 2986 and be able to provide the following information in the request: public key, Common Name, Organization, Organizational Unit, and Country.

FIA_X509_EXT.1.5

The TSF shall validate the certificate using [***a Certificate Revocation List (CRL) as specified in RFC 5759***].

FIA_X509_EXT.1.6

The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates.

FIA_X509_EXT.1.7

The TSF shall not treat a certificate as a CA certificate if the basicConstraints extension is not present or the cA flag is not set to TRUE.

FIA_X509_EXT.1.8

The TSF shall not establish an SA if a certificate or certificate path is deemed invalid.

~~**FIA_X509_EXT.1.9**~~

~~The TSF shall support peer identifiers of the following types: [**Distinguished Name (DN)**] and [no other reference identifier type].~~

FIA_X509_EXT.1.9A

The TSF shall not establish an SA if the presented identifier does not match the configured reference identifier of the peer

FIA_X509_EXT.1.10

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.5 Security management (FMT)

5.1.5.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1

Refinement: The TSF shall restrict the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this EP to an authenticated Administrator.

5.1.5.2 Management of TSF Data (for general TSF data) (FMT_MTD.1)

FMT_MTD.1.1

The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

5.1.5.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using digital signature and [***no other mechanism***] capability prior to installing those updates;
- Ability to configure the cryptographic functionality;
- Ability to configure the IPsec functionality;
- Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE identified in this EP to the Administrator;
- Ability to configure all security management functions identified in other sections of this EP;
- [***No other capabilities***].

5.1.5.4 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1

The TSF shall maintain the roles: Authorized Administrator.

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions
- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied

5.1.6 Packet Filtering (FPF)

5.1.6.1 Packet Filtering (FPF_RUL_EXT.1)

FPF_RUL_EXT.1.1

The TSF shall perform Packet Filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2

The TSF shall process the following network traffic protocols:
- Internet Protocol (IPv4)
- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR
- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

FPF_RUL_EXT.1.3

The TSF shall allow the definition of Packet Filtering rules using the following network protocol fields:
- IPv4
o Source address
o Destination Address
o Protocol
- IPv6
o Source address
o Destination Address
o Next Header (Protocol)
- TCP
o Source Port
o Destination Port
- UDP
o Source Port
o Destination Port
and distinct interface.

FPF_RUL_EXT.1.4

The TSF shall allow the following operations to be associated with Packet Traffic Filtering rules: permit, deny, and log.

FPF_RUL_EXT.1.5

The TSF shall allow the Packet Traffic Filtering rules to be assigned to each distinct network interface.

FPF_RUL_EXT.1.6

The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF_RUL_EXT.1.5) in the following order: Administrator-defined.

FPF_RUL_EXT.1.7

The TSF shall deny packet flow if a matching rule is not identified.

5.1.7 Protection of the TSF (FPT)

5.1.7.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1)

FPT_APW_EXT.1.1

The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext passwords.

5.1.7.2 Fail Secure (FPT_FLS.1)

FPT_FLS.1.1

Refinement: The TSF shall shutdown when the following types of failures occur: failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.

5.1.7.3 Extended: Protection of TSF Data (for reading of all symmetric keys) (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1

The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.7.4 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.1.7.5 TSF Testing (FPT_TST_EXT.1)

FPT_TST_EXT.1.1

The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2

The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1(2).

5.1.7.6 Extended: Trusted Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1

The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2

The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3

The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [***no other functions***] prior to installing those updates.

5.1.8 TOE access (FTA)

5.1.8.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1

Refinement: The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.8.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.8.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.8.4 Default TOE Access Banners (FTA_TAB.1)

FTA_TAB.1.1

Refinement: Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.9 Trusted path/channels (FTP)

5.1.9.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1

Refinement: The TSF shall use [***IPsec***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication server***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2

The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server *and external authentication functions***].

5.1.9.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1

Refinement: The TSF shall use [***IPsec***] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2

Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 1 components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM coverage
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 3 EAL 1 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic functional specification (ADV_FSP.1)

ADV_FSP.1.1d
The developer shall provide a functional specification.

ADV_FSP.1.2d
The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c
The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c
The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c
The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4c
The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e
The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d
The developer shall provide operational user guidance.

AGD_OPE.1.1c
The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c
The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c
The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c
The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c
The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c
The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c
The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d
The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c
The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c
The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e
The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d
The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c
The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM coverage (ALC_CMS.1)

ALC_CMS.1.1d
The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c
The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c
The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is designed to produce syslog conformant messages in a number of circumstances including warnings about the device itself (such as temperature, power failures, etc.) as well as security relevant events (the success and failure login of the user, regardless of the authentication mechanism; changing a user's password; and adding and deleting user accounts). In each case the audit record includes the time and date, identification of the responsible subject (e.g., by network address or user ID), the type of event, the outcome of the event, and other information depending on the event type.

The audit records are stored in a log (internal to the TOE appliance) that is protected so that only an authorized TOE User can read (for which tools accessible via the CLI and Web Management Interface are provided). The protection results from the fact that the logs can be accessed only after a user logs in (see section 6.4 below).

The local log audit entries until it fills after which the audit entries will be overwritten, oldest first. The administrator (with Super User privilege) can (and should) choose to configure one or more external syslog servers where the TOE will simultaneously send a copy of the audit records. The TOE can be configured to use IPSec to protect audit logs exported to an external server.

The TOE includes a hardware clock that is used to provide reliable time information for the audit records it generates. The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in **Table 2**. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 2**.
- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with the use of IPsec.

6.2 Cryptographic support

The evaluated configuration requires that the TOE be configured in Common Criteria mode to ensure the proper encryption functions are used. The following functions have been CAVP tested in accordance with the identified standards.

Functions	Standards	Cert[1] MLXe MR2
Encryption/Decryption		
• AES CBC, GCM (128 and 256 bits)	FIPS Pub 197 NIST SP 800-38A	3478 (GCM) 1648 (CBC)
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048) • Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater	FIPS Pub 186-2 FIPS Pub 186-3	1413 (RSA) 593/761 (ECDSA)
Cryptographic hashing		
• SHA-256, SHA-384 (digest sizes 256, 384)	FIPS Pub 180-3	2282
Keyed-hash message authentication		
• HMAC-SHA-256(digest size 256)	FIPS Pub 198-1 FIPS Pub 180-3	1696
Random bit generation		
• CTR_DRBG with sw based noise sources with a minimum of 256 bits of non-determinism	NIST SP 800-90	454

Table 4 Cryptographic Functions

The TOE supports NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, and P-384 (as defined in FIPS PUB 186-3, "Digital Signature Standard", Appendix B.4), specifically B.4.2 "Key Pair Generation by Testing Candidates". For elliptic curve and finite-field based key establishment, the TOE implements the following sections of SP 800-56A: 5.6 and all subsections. The TOE does not implement any Brocade-specific extensions.

The TOE uses a software-based random bit generator that complies with Special Publication 800-90 using CTR_DRBG when operating in the FIPS mode. AES-256 is used in conjunction with a minimum of 256 bits of entropy accumulated from the processing stack, hardware serial numbers, and the low-order bits from the current time of day.

The TOE implements the IPsec architecture as specified in RFC 4301. SPD rules can be configured using the firewall rules. Firewall rules are defined using access control List (ACL) entries. Firewall rules are used to distinguish between DROP actions and permit (PROTECT) actions. BYPASS rules are defined using firewall rules as well. The authorized administrator defines a final discard rule so that any packet not matching another rule will be discarded. The TOE supports IKEv2 in tunnel mode. The TOE implements RFC 4106 conformant AES-GCM-128 and AES-GCM-256as encryption algorithms. The TOE also implements HMAC-SHA-256 and HMAC-SHA-384 as integrity/authentication algorithms as well as Diffie-Hellman Groups 14, 19, and 20. The authorized administrator assigns the default Diffie-Hellman Group. The encrypted payload for IKEv2 uses AES-CBC-128, AES-CBC-256[2] as specified in RFC 6379. The authorized administrator can configure the TOE to support lifetimes based on timelimits. It is the responsibility of the authorized administrator to never define stronger ESP algorithms than IKE algorithms.

The TOE generates the secret value x used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using the CAVP tested RBG specified in FCS_RBG_EXT.1 and having possible lengths of 224, 256, or 384 bits. When a

[1] The BR-MLX-10GX4-IPSEC-M Card is common across all platforms and provides the IPsec functionality. This card includes the P2010 processor (specifically P2010e) as well as the AESU 3.0.1, Brocade IPSEC FPGA and BRCD-LP-CRYPTO-VER-1.0 firmware.

[2] The TOE uses Freescale Security Engine for AES-CBC encryption with 128 and 256 bit keys.

random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^{112}, 2^{128}, or 2^{192}

The IPsec implementation supports both ECDSA certificates and pre-shared keys. Pre-shared keys can include any letter from a-z, A-Z, the numbers 0 – 9, and any special character located above the numbers on the keyboard. The specific length of 22 characters required by the NDPP11E3/VPNGEP11 is supported by the TOE as well as pre-shared keys up to 100 characters. The TOE does not perform any processing on pre-shared keys. The TOE simply uses the pre-shared key that was entered by the administrator (either text-based or bit-based).

The TOE supports the following secret keys, private keys and CSPs:

Key or CSP:	Zeroized upon:	Stored in:	Zeroized by:
VPN IKE_SA Keys (Auth initiator and responder, Encryption initiator and responder)	Expiration	Memory	Overwriting with 0xAB
VPN CHILD/IPSEC_SA Keys (initiator and responder)	Expiration	Memory	Overwriting with 0xCD
User IPsec X.509v3 Certs (ECDSA) (public)		N/A – Public information	N/A – Public information
User IPsec X.509v3 Certs (ECDSA) (private)	Command	Memory	Fips zeroize command or 'crypto key zeroize ec'
Appliance IPsec X.509v3 Certs (ECDSA) (public)		N/A – Public information	N/A – Public information
Appliance IPsec X.509v3 Certs (ECDSA) (private)	Flash		Fips zeroize command or 'crypto key zeroize ec'
VPN PSK	Command	Memory	Overwriting with zeros
Administrator Password	Command	Flash	Overwriting once with zeros

Table 5 Keys and CSPs

Zeroization occurs as follows: 1) when deleted from FLASH, the previous value is overwritten once with zeroes; 2) when added or changed in FLASH, any old value is overwritten completely with the new value; and, 3) the zeroization of values in RAM is achieved by overwriting once with a pattern.

The TOE supports the following different zeroization methods for its secret keys, private keys and CSPs (note that no public keys appear in this list; they are public and thus need not be zeroizeable). For any given CSP in the table above, there may be multiple zeroization methods available.

- command: *fips zeroize all* - The device zeros out the shared secrets use by various networking protocols including host access passwords, IPsec session keys.
- command: *no fips enable* or *no fips enable common-criteria* - Zeroizes shared secrets, and the IPsec certificate based on the configured FIPS policy. Either of these commands will take the TOE out of its evaluated configuration and zeroize the secrets assuming a default FIPS policy. An administrator can use the prior command, fips zeroize all, to conclusively zeroize all CSPs, secret, and private keys, irrespective of the configured FIPS policy.
- Command - *crypto key zeroize ec* – Zerozies specific certificates
- The DRBG seed is recomputed periodically on 100 millisecond intervals.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE implements NIST SP800-56A.
- FCS_CKM_EXT.4: Keys are zeroized when they are no longer needed by the TOE.
- FCS_COP.1(1): See Table 4 Cryptographic Functions above.
- FCS_COP.1(2): See Table 4 Cryptographic Functions above.

- FCS_COP.1(3): See Table 4 Cryptographic Functions above.
- FCS_COP.1(4): See Table 4 Cryptographic Functions above.
- FCS_IPSEC_EXT.1: The TOE implements the IPsec architecture as specified in RFC 4301. See above for more information.
- FCS_RBG_EXT.1: See Table 4 Cryptographic Functions above.

6.3 User data protection

The TOE is designed to ensure its own internal integrity as well as to protect user data from potential, unintended reuse by clearing resources (e.g., memory) as they are allocated to create objects used in the implementation of the TOE operations. Note that volatile memory is the primary resource involved in normal TOE execution while its persistent storage is based on non-volatile flash memory.

When the TOE sends a network packet, it must request a buffer from the buffer pool. After using a buffer, the TOE releases the buffer back to the buffer pool. In response to a request, the buffer pool will return a buffer and its length, where the length is greater than or equal to that requested. The TOE will compare the length of the returned buffer to that which it requested (the size of the packet), overwrite the returned buffer with packet data (destroying any residual data present in the buffer), and, if the provided buffer exceeds the requested size of the packet, overwrite any extra space with zeros (thus ensuring that no residual data can leak from the TOE).

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.2: The TOE always overwrites resources when allocated for use in objects

6.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except to display a message of the day banner and to permit network traffic to flow through the TOE without identification or authentication. The network routing services that the TOE allows includes network traffic being routed through the TOE as well as network routing protocol traffic destined to the TOE (including DNS, ARP, ICMP, BootP, DHCP, RIP, OSPF, BGP, VRRP, VRRP-E, Multi-VRF) but does not include any management configuration of the TOE's network routing services. The TOE authenticates TOE Users against their user name, password and privilege level.

The Authorized Administrator with Super User privilege represents the "administrator" referred to in the security requirements of the protection profile. Other accounts with privileges other than Super User were not tested during evaluation. The Authorized Administrator with Super User privilege defines local user (or TOE User) accounts and to assign passwords and privilege levels to the accounts. Each user account has a user name, password, and a privilege level associated with it. There is a default privilege level account associated with each privilege level and each has its own password. It is up to the Authorized Administrator with Super User privilege to decide whether or how to use these legacy accounts. Note however, that each has an identity, password, and privilege level.

The user roles offered by the TOE are categorized differently when described in FIPS documentation. Specifically, the Authorized Administrator with Super User privilege equates to the FIPS Crypto Officer Role, the Port Configuration User equates to the FIPS Port Configuration Administrator Role (and has write access to the interface configuration mode only), and a user with read-only privileges and no configuration mode access equates to the FIPS User Role.

While the Authorized Administrator with Super User privilege can create or otherwise modify accounts freely, other users cannot change their own (or any other) security attributes. Note that the TOE supports a password enforcement configuration where the minimum password length can be set by an administrator up to 48 characters. Passwords can be created using any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1).

Additional authentication mechanisms can also be configured by an Authorized Administrator using an Authentication Method List. This allows some flexibility in setting up authentication mechanisms when desired. The available mechanisms include the Local Password for the Super User Privilege level and TACACS+ or RADIUS authentication, An administrator can create users, associate passwords with user accounts, and can also set the privilege level associated with a user. When authentication succeeds, the TOE looks up the user's defined privilege level, assigns that to the user's session, and presents the user with a command prompt (the "#" character, e.g., "`Brocade(config)#`"). If the administrator's authentication fails for an administrator-defined number of times, the account is locked and an authorized administrator must unlock it before it can be used again.

The TOE supports the use of X.509v3 certificates for VPN authentication. Certificates are stored in plaintext files on the TOE and are loaded by the authorized administrator using SCP. The authorized administrator configures the VPN peers, and specifies the DN associated with an IP. When an incoming request is received, the TOE validates the certificate path (including intermediate CAs) of the CA certificate specified by the user in the VPN configuration. If the validation is successful, the TOE checks the validity of the certificate and its certificate chain including basic constraints field and expiration status. The TOE will reject any certificate for which it cannot determine the validity and reject the connection attempt

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: The authorized administrator can define a value for the failed login attempts for administrators. If that value is reached, the associated account is locked and an authorized administrator must unlock it before it can be used again.
- FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above
- FIA_PSK_EXT.1: The TOE supports a pre-shared key length of 100 characters. The TOE does not condition text-based pre-shared keys (see the IPsec discussion in Section 6.2)
- FIA_UAU.7: The TOE does not echo passwords as they are entered; rather '*' characters are echoed when entering passwords
- FIA_UAU_EXT.2: The TOE can be configured to utilize local password-based authentication mechanism or external RADIUS and TACACS+ authentication servers.
- FIA_UIA_EXT.1: The TOE doesn't offer any services or access to its functions, except for the switching/routing of network traffic and displaying a message of the day banner, without requiring a user to be identified and authenticated.
- FIA_X509_EXT.1: The TOE is able to use X.509v3 certificates. The TOE uses X.509v3 certificates in support of its VPN functionality and performs all required validity checks on the certificates.

6.5 Security management

The TOE associates each defined user account with a privilege level. The most privileged level is Super User (with regards to the requirements in this Security Target users with lesser privilege levels are referred to collectively simply as TOE users since such users do not have complete read-and-write access to the system). Again, as stated in section 6.4 other accounts with privileges other than Super User were not tested during the evaluation. The TOE implements an internal access control mechanism that bases decisions about the use of functions and access to TOE data on those privilege levels. In this manner, the TOE is able to ensure that only the Authorized Administrator with Super User privilege can access audit configuration data, information flow policy ACLs, user and administrator security attributes (including passwords and privilege levels), authentication method lists, the logon failure threshold, the remote access user list; and cryptographic support settings.

Other than the Super User level, the TOE implements a Read Only level where only basic commands can be issued and no changes can be made and a Port Configuration level where non-security device parameters can be managed. Collectively, this ST refers to all users of the TOE as "TOE Users" where the "Authorized Administrator with Super User privilege" is a subset of that broader role.

The TOE offers command line functions which are accessible via the CLI. The CLI is a text based interface which can be accessed from a directly connected terminal or via a remote terminal using IPsec. These command line functions can be used to effectively manage every security policy, as well as the non-security relevant aspects of the TOE.

Similarly, the TOE's offers a Web Management Interface that offers access to the same functions as the CLI. While the Web Management Interface could be configured to be accessible via HTTP or HTTPS, the evaluated configuration only includes the use of HTTPS over IPsec to ensure that the administrative session is not subject to modification or disclosure.

The following table provides the list of security-related commands used to configure or examine the TOE security settings. The services listed here reflect the minimal set needed to properly configure the TOE to comply with the requires of the *Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) with Errata #3, 3 November 2014 with the Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013*.

Command	Tested Command Variantts	Description
write	write memory	Write to persistent storage
crypto	crypto key generate	Invoke cryptographic functions
openssl	openssl s_server	Configure secure connections (e.g., with syslog)
logging	logging host <ip-address> ssl-port <port>	Configure the audit logging host
reload	reload	Reload the current flash image
console	console timeout <time>	Manage console properties
banner	banner motd +	Manage the login banner
exit	exit	Logout or exit current session
ntp	ntp	Switch to ntp configuration mode
config	config t	Switch to configuration mode
username	username <user> password	Manage user accounts
clock	clock set <time>	Manage the internal clock
server	server <ntp server ip> minpoll <time>	Configure external services
crypto-ssl	crypto-ssl certificate generate	Manage web server properties
web-management	web-management session-timeout <time>	Manage web interface
fips	fips enable common-criteria fips show fips zeroize all	Manage FIPS and Common Criteria configuration
aaa	aaa authentication aaa authentication enable default tacacs+ local aaa authentication login default tacacs+ local aaa authentication web-server default local	Configure the aaa authentication functions
tacacs-server	tacacs-server host <ipaddr> ssl-auth-port <port> default tacacs-server retransmit <retransmit period> tacacs-server timeout <timeout period> tacacs-server key <key>	Configure TACACAS+ server
ike	ikev2 proposal ikev2 profile	Configures ike properties
ipsec	ipsec proposal ipsec profile	Configures ipsec properties
tunnel	tunnel protection ipsec ipv4 <ipsec profile name>	Enables ipsec on an interface
ip	access-list	Used to configure acls
enable	enable aaa enable password-min-length 15 enable user password-masking	Enable console login features
show	show flash	Show identified configuration information

Command	Tested Command Variantts	Description
	show ver show clock show ip client-pub-key show ip ssl show logging show run | <options>	

Table 6 Security Related Configuration Commands

The TOE also provides a comprehensive set of network routing configuration commands. These commands were not exercised as the above services in Table 6 represent the minimum set of commands needed to for proper configuration.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: Only the TOE's authorized administrator can enable, disable, determine and modify the behavior of all of the security functions of the TOE
- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Authorized Administrator with Super User privilege (aka Security Administrator).
- FMT_SMF.1: The TOE includes the functions necessary to enable/disable available network services, to manage the cryptomodule and associated functions, to configure IPsec parameters, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes roles associated with privileges. 'Authorized Administrator with Super User privilege' corresponds to the required 'Authorized Administrator' also referred to as 'Security Administrator' in some requirements

6.6 Packet Filtering

The TOE has a rich packet filtering interface implemented through the use of access control lists (ACLs). ACLS can be applied to both inbound and outbound interfaces. The TOE only supports one inbound ACL but that ACL may have multiple entries. ACLs can be applied to any interface for either 'inbound' traffic or 'outbound traffic'. The ACL interface has options for filtering on IPv4, IPv6, TCP, and UDP as well as source and destination address. The TOE processes traffic that ACLs filter in hardware. The TOE creates an entry for each ACL in the Content Addressable Memory (CAM) at startup or when the ACL is created. The TOE uses these CAM entries to permit or deny packets in the hardware, without sending the packets to the CPU for processing. Each rule can be set for permit, deny, and log. Rules are applied in order and the first matching rule is applied to the traffic.

To prevent the flat layer 2 network from being flooded with excessive amount of broadcast, unknown-unicast, and multicast (a.k.a BUM) traffic, the BUM traffic received on a port can be restricted using BUM rate-limiter. With BUM rate-limit configured on the port, when a high rate of BUM traffic is received on the port, BUM traffic will be throttled to the configured data rate associated with the BUM rate-limit before being replicated across the Layer 2 network. When the received BUM traffic exceeds the pre-defined rate limit, the physical port can be configured to be automatically shutdown or disable using the shutdown option of the rate-limit command. The port shutdown occurs within 2.5 seconds after the BUM traffic exceeds the defined limit. The port can be enabled again through the use of the clear command. The disabling and re-enabling are both audited.

The default action when no ACL is applied on a TOE interface is to permit all traffic. The CC Guide states a final deny ACL needs to be set on each interface since the requirement is to deny all traffic not matching a rule.

During initial boot, before the network interface becomes fully functional, the network interface drops all packets until the TOE is fully functional.

The Packet Filtering function is designed to satisfy the following security functional requirements:

- FPF_RUL_EXT.1: The TOE supports all of the required protocols, ipv4 (RFC 791), ipv6 (RFC 2460), tcp (RFC 793), and udp (RFC 768) as well as source and destination address. The firewall rules implement permit and deny possibilities. Each rule can be configured to log status of packets pertaining to the rule.

6.7 Protection of the TSF

The TOE is an appliance and as such is designed to work independent of other components to a large extent. Secure communication with third-party peers as addressed in section 6.2 and secure communication among multiple instances of the TOE is limited to a direct link between clustered switch appliances. Normally clustered components are co-located and connected via a link that would not be exposed outside of the same physical environment. As such, no additional protection (e.g., encryption) should be necessary in most operational environments.

While the administrative interface is function rich, the TOE is designed specifically to not provide access to locally stored passwords (which are protected using MD-5 hashing) and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE. The TOE is a hardware appliance that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The TOE can be configured to periodically synchronize its clock with a time server, but the TOE can only ensure its own reliability and not that of an external time mechanism. The TOE also implements the timing elements through timeout functionality due to inactivity for terminating both local and remote sessions. Note that the clock is used primarily to provide timestamp for audit records, but is also used to supporting timing elements of cryptographic functions.

The TOE includes a number of built in diagnostic tests that are run during start-up to determine whether the TOE is operating properly. An administrator can configure the TOE to reboot or to stop, with errors displayed, when an error is encountered. The module performs Cryptographic algorithm known answer tests, firmware integrity tests using RSA signature verification and conditional self-tests for DRBG, Hardware RNG, Pair-wise consistency tests on generation of RSA keys, and a Firmware load test (RSA signature verification). Upon failing any of its FIPS mode power-on self-tests, the TOE will refuse to boot.

The TOE supports loading a new software image manually by the administrator using CLI commands. From the CLI, an administrator can use SCP in order to download a software image from the Brocade web site, and the TOE, prior to actually installing and using the new software image, will verify its digital certificate using the public key in the certificate configured in the TOE. An unverified image cannot be installed. Note that the TOE comes preinstalled with an applicable Brocade public certificate.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Furthermore, locally defined passwords are not stored in plaintext form.
- FPT_FLS.1: Upon failing any of its FIPS mode power-on self-tests, the TOE will refuse to boot.
- FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_STM.1: The TOE includes its own hardware clock and can be configured to synchronize with a NTP server.
- FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics that will serve to ensure the TOE is functioning properly. The tests include ensure memory and flash can be accessed as expected, to ensure that software checksums are correct, and also to test the presence and function of plugged devices.
- FPT_TUD_EXT.1: The TOE provides function to query the version and upgrade the software embedded in the TOE appliance. When installing updated software, digital signatures are used to authenticate the update to ensure it is the update intended and originated by Brocade.

6.8 TOE access

The TOE can be configured to display an administrator-configured message of the day banner that will be displayed before authentication is completed (before the user enters his password). The banner will be displayed when accessing the TOE via the console, or the GUI interface.

The TOE can be configured by an administrator to set a session timeout value (any value up to 240 minutes, with 0 disabling the timeout) – the default timeout is disabled. A session (local or remote) that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. Upon exceeding the session timeout (if set), the TOE logs the user off, but leaves the user's console displaying the last contents.

The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination. Of course, administrators can logout of local or remote sessions at any time.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: The TOE provides the function to logout (or terminate) the both local and remote user sessions as directed by the user.
- FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE, allowing administrators to terminate their session prior to performing any functions.

6.9 Trusted path/channels

The TOE implements IPsec and HTTPS over IPsec which are required to be used for remote administration. When an administrator attempts to connect to the TOE, the TOE attempts to negotiate a session. If the session cannot be negotiated, the connection is dropped.

Remote connections to SYSLOG servers and authentication servers (i.e. RADIUS or TACACS+ are protected using IPsec (as specified earlier).

In all cases, the endpoints are assured by virtue of the certificates installed, trusted, and reviewable when connecting and by virtue of user authentication.

The TOE update service is secured using SCP, as when operating in FIPS (or Common Criteria) Mode, the TOE prevents the use of TFTP to retrieve a new TOE firmware image.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use IPsec to ensure that any authentication operations and exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides IPsec, based on its embedded cryptomodule, to ensure secure remote administration. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using CAVP tested cryptographic operations, and all remote security management functions require the use of one of these secure channels