Brocade Communications Systems, Inc. VDX Product Series (NDPP11e3) Security Target

Version 0.7
May 11, 2015

Prepared for:

Brocade Communications 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 the Brocade Communications Systems, Inc. VDX Product Series. The TOE is being evaluated as a network infrastructure device.

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.

Acronyms and Terminology

This following acronyms and terms are used throughout this document.

ACL	Access Control List
AUT	Authentication
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CLI	Command Line Interface
EAL	Evaluation Assurance Level

FC-SP	Fibre Channel Security Protocols
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FSP	Functional Specification
HLD	High Level Design
ISO 15408	Common Criteria 2.1 ISO Standard
IT	Information Technology
KDF	Key Distribution Function
MOF	Management of Functions
MTD	Management of TSF Data
NOS	Network operating system
OSP	Organization Security Policy
PP	Protection Profile
QSFP	Quad Small Form-factor Pluggable
SAR	Security Assurance Requirement
SCP	Secure copy
SFP	Security Function Policy
SFP+	enhanced small form-factor pluggable
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
SSH	Secure Shell
ST	Security Target
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

1.1 Security Target Reference

ST Title – Brocade Communications Systems, Inc. VDX Product Series

ST Version – Version 0.7

ST Date – May 11, 2015

1.2 TOE Reference

TOE Identification – Brocade Communications Systems, Inc. VDX Product Series operating with NOS version 5.0.1b1, including the following series and models

- VDX 6710-54
- VDX 6720-24
- VDX 6720-60
- VDX 6730-32
- VDX 6730-76
- VDX 6740

- VDX 6740T
- VDX 6740T-1G
- VDX 8770-4, and
- VDX 8770-8.

TOE Developer – Brocade Communications Systems, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is the VDX Product Series family of products provided by Brocade Communications Systems, Inc. VDX Product Series are hardware network devices that implement what is called a 'Storage Area Network' or 'SAN'. SANs provide physical connections between servers that are located in the environment and storage devices such as disk storage systems and tape libraries that are also located in the environment.

1.4 TOE Description

The Target of Evaluation (TOE) is the VDX Product Series. The VDX Product Series are hardware appliance with embedded software installed on a management processor. Optionally, a number of co-located appliances can be connected in order to work as a unit with a common security policy. The embedded software is a version of Brocades' proprietary Multiservice Network Operating System (NOS). The NOS controls the switching and routing of network frames and packets among the connections available on the hardware appliances. These switch/routers include virtual cluster switch (VCS), which allows users to create flatter, virtualized and converged data center networks. These VCS fabrics are scalable, permitting users to expand at their own pace, and simplified, allowing users to manage the fabric as a single entity. VCS-based Ethernet fabrics are convergence-capable, with technologies such as Fibre Channel over Ethernet (FCoE) for storage.

All TOE appliances are configured at the factory with default parameters and an admin and user account with default passwords. Users must login to access the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration 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 SSH. The TOE uses SCP to download/compare software images. All of the remote management interfaces are protected using encryption as explained later in this ST.

The VDX 6710 switch is a fixed port switch with 48 1-Gigabit Ethernet copper interfaces and six 10 Gigabit Ethernet SFP+ interfaces. The VDX 6720 switches are also fixed port switches with either 24 10-Gigabit LAN ports or 60 10-Gigabit LAN ports, depending on the model. The VDX 6730 switch is a 10-Gigabit Ethernet fixed port switch with LAN and native Fibre Channel ports. Depending on the model, it either provides 24 10-Gigabit Ethernet LAN ports and eight 8-Gbps native Fibre Channel ports, or 60 10-Gigabit Ethernet LAN ports and 16 8-Gbps native Fibre Channel ports. The 6710, 6720 and 6730 hardware platforms that support the TOE have a number of common hardware characteristics:

- A system motherboard that features a Reduced Instruction Set Computer (RISC) CPU running at 1.3 GHz with integrated peripherals
- Extensive diagnostics and system-monitoring capabilities for enhanced high Reliability, Availability, and Serviceability (RAS)
- A USB port for firmware upgrades and system log downloads
- Support for long-range and short-range SFP+ 10-Gigabit Ethernet transceivers

The VDX 8770-4 switch provides up to 192 10-Gigabit Ethernet or 1 Gigabit Ethernet external ports or 48 40-Gigabit Ethernet external ports, while the VDX 8770-8 switch provides up to 384 10-Gigabit Ethernet or 1 Gigabit

external ports or 96 40-Gigabit Ethernet external ports. The 8770 hardware platforms that support the TOE have a number of common hardware characteristics:

- Dual, redundant management modules
- Serial (console), Ethernet, and USB connections for management modules (though only Brocade-branded USB devices are supported)
- Support for short-range and long-range 1 Gbps SFP transceivers
- Support for short-range and long range 10 Gbps SFP+ transceivers
- Support for 40 Gbps QSFP transceivers

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, or dropped in accordance with a configured policy.

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 NOS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). NOS enforces applicable security policies on network information flowing through the hardware appliance.

1.4.1.1 Physical Boundaries

Each TOE appliance runs a version of the Brocades NOS 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 a syslog server in the 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 NTP server in the operational environment.

1.4.1.2 Logical Boundaries

The TOE logical boundary consists of the security functionality of VDX appliances summarized in the following subsections:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management

- 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 and not modify any security related configuration settings.
2. Web Management Access is assumed to be **disabled** in the evaluated configuration.
3. Telnet access is assumed to be **disabled** for remote/network access to the TOE.
4. The *Strict Password Enforcement* setting is assumed to be **enabled** in the evaluated configuration.
5. The TACACS+ external authentication service is assumed to be **disabled** in the evaluated configuration.
6. The TOE will be operated in a CC-compliant configuration.

Given that this Security Target conforms to the NDPP, the security claims focus on the TOE as a secure network infrastructure device and do not focus on other key functions provided by the TOE, such as controlling the flow of network packets among the attached networks. However, those functions can be freely used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

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 SYSLOG servers in its environment to export audit data. The TOE is designed to interact with SYSLOG servers in accordance with their respective protocols, including security capabilities where applicable.

1.4.1.2.1 Security audit

The TOE generates audit events for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware. When the syslog server writes the audit record to the audit trail, it applies its own time stamp, placing the entire TOE-generated syslog protocol message MSG contents into an encapsulating syslog record.

1.4.1.2.2 Cryptographic support

The TOE contains FIPS-certified cryptographic implementations 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 SSH and TLS.

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 authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. Either the TOE performs the validation of the login credentials or the information is passed to a RADIUS or LDAP Server to perform the validation and the TOE enforces the decision. The administrator can configure the order in which order the external authentication provider and the local credentials are checked.

1.4.1.2.5 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. Security management commands are limited to authorized users (i.e., administrators) and available 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 Authorized Administrator role can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

1.4.1.2.6 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 or a closely grouped (e.g., in the same rack) collection of appliances acting as a unit. 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.

1.4.1.2.7 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.

1.4.1.2.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access, ensuring both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs. SSH v2 is used to support SCP which the TOE uses for secure download of TOE updates.

1.4.2 TOE Documentation

Brocade offers a series of documents that describe the installation process for the TOE 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 VDX 6710-54 Hardware Reference Manual, 53-1002390-07
- Brocade VDX 6720 Hardware Reference Manual, 53-1002084-05
- Brocade VDX 6730 Hardware Reference Manual, 53-1002389-05
- Brocade VDX 6740 and VDX 6740T Hardware Reference Manual, 53-1002829-01
- Brocade VDX 8770-4 Hardware Reference Manual, 53-1002563-02
- Brocade VDX 8770-8 Hardware Reference Manual, 53-1002564-02
- Network OS Administrator's Guide, 53-1002840-01
- Network OS Command Reference, 53-1002841-01
- Network OS Common Criteria Configuration Guide, 53-1003789-01

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
- ST conforms to the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #2, 13 January 2014.
- Package Claims:
    - Assurance Level: EAL 1 conformant

2.1 Conformance Rationale

The ST conforms to the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #2, 13 January 2014. 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 *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #2, 13 January 2014 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDPP offers additional information about the identified security objectives, but that has not been reproduced here and the Protection Profile should be consulted if there is interest in that material.

In general, the NDPP has defined Security Objectives appropriate for network infrastructure devices and as such are applicable to the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #2, 13 January 2014.

3.1 Security Objectives for the TOE

O.DISPLAY_BANNER

The TOE will display an advisory warning regarding use of the TOE.

O.PROTECTED_COMMUNICATIONS

The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

O.RESIDUAL_INFORMATION_CLEARING

The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

O.SESSION_LOCK

The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.

O.SYSTEM_MONITORING

The TOE will provide the capability to generate audit data and send those data to an external IT entity.

O.TOE_ADMINISTRATION

The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.

O.TSF_SELF_TEST

The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

O.VERIFIABLE_UPDATES

The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

3.2 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.

4. Extended Components Definition

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

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS_SSH_EXT.1: Explicit: SSH
- FCS_TLS_EXT.1: Explicit: TLS
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- 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 Protection Profile (PP): *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP) with Errata #2, 13 January 2014. The refinements and operations already performed in the PP are not identified (e.g., highlighted) here, rather the requirements have been copied from the PP and any residual operations have been completed herein. Of particular note, the PP 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 NDPP which includes all the SARs for EAL 1 as defined in the CC. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the PP that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. As such, those assurance activities have been reproduced in this ST to ensure they are included within the scope of the evaluation effort.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Brocade Communications Systems, Inc. Brocade Directors and Switches 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_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1: Explicit: SSH
	FCS_TLS_EXT.1: Explicit: TLS
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	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
FPT: Protection of the TSF	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	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 5-1 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 1 (in the NDPP).

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 of Table 1 (in the NDPP).

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 [***TLS***] 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 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' for RSA-based key establishment schemes] 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 [***CBC***] and cryptographic key sizes 128-bits and 256-bits that meets the following:
- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- [***NIST SP 800-38A***].

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 [
(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater

that meets the following:

[***Case: RSA Digital Signature***
Algorithm - FIPS PUB 186-2 or 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-1, SHA-256***] and message digest sizes [***160, 256***] 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-1***], key size [**equal to the input block size**], and message digest sizes [***160***] 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: 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 [***FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES***] seeded by an entropy source that accumulated entropy from [***selection: 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.

5.1.2.8 Explicit: SSH (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1
The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [***no other RFCs***].

FCS_SSH_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**256k**] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [***no other algorithms***].

FCS_SSH_EXT.1.5
The TSF shall ensure that the SSH transport implementation uses [***SSH_RSA***] and [***no other public key algorithms***] as its public key algorithm(s).

FCS_SSH_EXT.1.6
The TSF shall ensure that data integrity algorithms used in SSH transport connection is [***HMAC-SHA1 and HMAC-SHA2-256***].

FCS_SSH_EXT.1.7
The TSF shall ensure that diffie-hellman-group14-sha1 and [***no other methods***] are the only allowed key exchange methods used for the SSH protocol.

5.1.2.9 Explicit: TLS (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1
The TSF shall implement one or more of the following protocols [***TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5289)***] supporting the following ciphersuites:
Mandatory Ciphersuites:
- TLS_RSA_WITH_AES_128_CBC_SHA
Optional Ciphersuites:
- [***TLS_RSA_WITH_AES_256_CBC_SHA***
- ***TLS_DHE_RSA_WITH_AES_128_CBC_SHA***
- ***TLS_DHE_RSA_WITH_AES_256_CBC_SHA***
- ***TLS_RSA_WITH_AES_128_CBC_SHA256***
- ***TLS_RSA_WITH_AES_256_CBC_SHA256***].

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 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.

5.1.4.2 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.

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

FIA_UAU_EXT.2.1

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

5.1.4.4 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 and SAN 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.

5.1.5 Security management (FMT)

5.1.5.1 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.

5.1.5.2 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***] capability prior to installing those updates;
- [***- Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1,***
- Ability to configure the cryptographic functionality].

5.1.5.3 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 Protection of the TSF (FPT)

5.1.6.1 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.

5.1.6.2 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.

5.1.6.3 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1
The TSF shall be able to provide reliable time stamps for its own use.

5.1.6.4 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.

5.1.6.5 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***] prior to installing those updates.

5.1.7 TOE access (FTA)

5.1.7.1 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.

5.1.7.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1
The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.7.3 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.

5.1.7.4 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.

5.1.8 Trusted path/channels (FTP)

5.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1

Refinement: The TSF shall use [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***authentication server, [LDAP 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 [**transfer of audit records, verification of user identity via remote authentication server**].

5.1.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1

Refinement: The TSF shall use [***SSH***] 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 5-2 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
- 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; adding and deleting user accounts; modification, addition and deletion of ACLs; and violations of the ACL rules). 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 are provided) or otherwise access them. The protection results from the fact that the logs can be accessed only after a user logs in (see section 6.4 below).

The log stores up to 1024 entries after which the audit entries will be overwritten, oldest first. The administrator (with Authorized Administrator privilege) can (and should) choose to configure one or more external syslog servers where the TOE will send a copy of the audit records if so desired. The TOE can be configured to use TLS 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.

Requirement	Auditable Events	Additional Audit Record Contents	Event ID
FAU_GEN.1	Startup of audit		RAS-2003
	Shutdown of audit		RAS-2003
FCS_SSH_EXT.1	Failure to establish an SSH session. Establishment/Termination of an SSH session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.	SEC-1203 SEC-3021
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	DCM-1006
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	SEC-1203 SEC-3021
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	See FIA_UIA_EXT.1

Requirement	Auditable Events	Additional Audit Record Contents	Event ID
FMT_SMF.1	All administrator actions		DCM-1006
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).	TS-1010
FPT_TUD_EXT.1	Initiation of update.	No additional information.	SULB-1000
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.	See FTA_SSL.3
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.	SEC-3022
FTA_SSL.4	The termination of an interactive session.	No additional information.	DCM-1013 SEC-3022
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.	See FCS_TLS_EXT.1 for syslog, and remote auth server connection events.
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.	See FIA_UIA_EXT.1 for SSH and HTTPS events – the user is identified in each case.

Table 6-1 Audit Events

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 6-1 and section 5.1.1. 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 section 5.1.1.
- 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 TLS.

6.2 Cryptographic support

The TOE includes a FIPS 140 certified cryptomodule providing supporting cryptographic functions (Certificate # 2322). The evaluated configuration requires that the TOE be configured in FIPS mode to ensure FIPS certified functions are used.

The following functions have been FIPS certified in accordance with the identified standards.

Functions	Standards	Cert VDX 6710, 6720, 6730	VDX 6740, 6740T, 8770
Encryption/Decryption			
• AES CBC (128 and 256 bits)	FIPS Pub 197 NIST SP 800-38A	2283	2285
Cryptographic signature services			
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS Pub 186-4	1358, 1359	1356, 1357
Cryptographic hashing			
• SHA-1, SHA-256 (digest sizes 160 and 256 bits)	FIPS Pub 180-3	1965	1966
Keyed-hash message authentication			
• HMAC-SHA-1(digest size 160)	FIPS Pub 198-1 FIPS Pub 180-3	1399	1400
Random bit generation			
• ANSI X9.31 AES-128 RBG	FIPS Pub 186-2 ANSI X9.31	1135	1136
Key Derivation Functions			
• TLS and SSH	NIST SP 800-135	131	130

While the TOE generally fulfills all of the NIST SP 800-56B requirements without extensions, the following table specifically identifies the "should", "should not", and "shall not" conditions from the publication along with an indication of how the TOE conforms to those conditions.

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented?	Rationale for deviation
5.6	Should	Yes	Not applicable
5.8	shall not	No	Not applicable
5.9	shall not (first occurrence)	No	Not applicable
5.9	shall not (second occurrence)	No	Not applicable
6.1	should not	No	Not applicable
6.1	should (first occurrence)	Yes	Not applicable
6.1	should (second occurrence)	Yes	Not applicable
6.1	should (third occurrence)	Yes	Not applicable
6.1	should (fourth occurrence)	Yes	Not applicable
6.1	shall not (first occurrence)	No	Not applicable
6.1	shall not (second occurrence)	No	Not applicable
6.2.3	Should	Yes	Not applicable
6.5.1	Should	Yes	Not applicable
6.5.2	Should	Yes	Not applicable
6.5.2.1	Should	Yes	Not applicable
6.6	shall not	No	Not applicable
7.1.2	Should	Yes	Not applicable
7.2.1.3	Should	Yes	Not applicable
7.2.1.3	should not	No	Not applicable
7.2.2.3	should (first occurrence)	Yes	Not applicable
7.2.2.3	should (second occurrence)	Yes	Not applicable

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented?	Rationale for deviation
7.2.2.3	should (third occurrence)	Yes	Not applicable
7.2.2.3	should (fourth occurrence)	Yes	Not applicable
7.2.2.3	should not	No	Not applicable
7.2.2.3	shall not	No	Not applicable
7.2.3.3	should (first occurrence)	Yes	Not applicable
7.2.3.3	should (second occurrence)	Yes	Not applicable
7.2.3.3	should (third occurrence)	Yes	Not applicable
7.2.3.3	should (fourth occurrence)	Yes	Not applicable
7.2.3.3	should (fifth occurrence)	Yes	Not applicable
7.2.3.3	should not	No	Not applicable
8	Should	Yes	Not applicable
8.3.2	should not	No	Not applicable

Table 6-2 NIST SP800-56B Conformance

The TOE uses a software-based random bit generator that complies with ANSI X9.31 using AES when operating in the FIPS mode. SHA-256 is used in conjunction with a minimum of 440 bits of entropy accumulated from the timing of disk I/O completion events.

Additionally, the TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. This function has also been subject to FIPS 140 certification. Note that 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 zeroes.

The following Critical Security Parameters are contained in the module:

- DH Private Keys for use with 2048 bit modulus in SSHv2.
- SSH Session Keys- 128 and 256 bit AES CBC
- SSH Authentication Keys - 2048 bit RSA private/public key pair
- SSH KDF Internal State
- SSH DH Shared Secret Key – 2048 bit key size
- TLS Private Key (RSA 1024)
- TLS Pre-Master Secret – 48 byte key size
- TLS Master Secret – 48 byte key size
- TLS PRF Internal State
- TLS Session Key – 128 bit AES
- TLS Authentication Key for HMAC-SHA-1/HMAC-SHA-256
- Approved RNG Seed Material
- ANSI X9.31 DRNG Internal State
- Passwords

These supporting cryptographic functions are included to support the SSHv2 (compliant with RFCs 4251, 4252, 4253, and 4254) and TLSv1.0, TLSv1.1, and TLSv1.2 (compliant with RFCs 2246, 4346, and 5289) secure communication protocols.The TOE supports the TLS ciphersuites identified in section 5.1.2.9.

The TOE supports SSHv2 with AES (CBC) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1, HMAC-SHA2-256, and RSA (with diffie-hellman-group14-sha1 for the key exchange method). While other ciphers and hashes are implemented in the product, they are disabled while the TOE is operating in FIPS mode.

The SSHv2 authentication timeout period is 120 seconds allowing clients to retry only 5 times; both public-key and password based authentication can be configured; and packets are limited to 256K bytes. Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (256K bytes) the packet will be dropped.

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

- FCS_CKM.1: See table above.
- FCS_CKM_EXT.4: Keys are zeroized when they are no longer needed by the TOE by executing the "fips zeroize" command.
- FCS_COP.1(1): See table above.
- FCS_COP.1(2): See table above.
- FCS_COP.1(3): See table above.
- FCS_COP.1(4): See table above.
- FCS_RBG_EXT.1: See table above.
- FCS_SSH_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.
- FCS_TLS_EXT.1: The TOE supports TLS sessions for exporting audit data.

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 a network packet is sent, the buffer used by the packet is recalled and managed by the buffer pool. After that, if a new packet acquires a buffer from the buffer pool, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, and additional space will be overwritten (padded) with zeros.

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 warning banners and to permit network traffic to flow through the TOE without identification or authentication so long as it conforms to the information flow policy rules. The TOE authenticates TOE Users against their user name and password or through public-key based authentication.

The Authorized Administrator is able to define 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 to decide whether or how to use these legacy accounts. Note however, that each has an identity, password, and privilege level.

While the Authorized Administrator 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 32 characters. Password enforcement mechanisms may be applied to local user accounts only. Passwords can be created using any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1). Also, the TOE can be configured to lock accounts, excluding the Authorized Administrator, after a pre-configured number of failed logon attempts. These functions are also restricted to the Authorized Administrator as is the ability to unlock locked accounts.

Alternative 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 Local User Accounts configured on the device. Local authentication methods include both password-based and public-key-based authentication. When authentication is successful, the TOE provides the associated user with applicable (role-based) privileges.

The Authentication Method List is ordered so that it will be processed from first to last. In each case, the user authentication will succeed, fail, or result in an error. Only in the case of an error (e.g., an external server is unavailable) will processing proceed to the next authentication method in the list. If a given authentication method succeeds, the user will be logged in and will be able to perform functions according to their privilege level. If a given authentication mechanism fails, the user will be denied a login session. If the point is reached where every authentication method on the list fails, only an authorized administrator whose password is not rejected will succeed in logging in to the system.

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

- FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.
- 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 use local password-based authentication or public key-based authentication.
- FIA_UIA_EXT.1: The TOE provides a password-based authentication mechanism and also permits authentication to occur using a third-party RADIUS or LDAP Server. The order in which these authentication providers are checked is determined by an administrator.

6.5 Security management

The TOE associates each defined user account with a privilege level. The most privileged level is Authorized Administrator(with regards to the requirements in this Security Target users with lesser privilege levels are referred to collectively simply as TOE users). 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 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 Authorized Administrator role, 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" 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 SSH. These command line functions can be used to effectively manage every security policy, as well as the non-security relevant aspects of the TOE.

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

- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Authorized Administrator (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, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes roles associated with privileges. 'Authorized Administrator' corresponds to the required 'Authorized Administrator' also referred to as 'Security Administrator' in some requirements.

6.6 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 is addressed in section 6.8 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. All cryptographic keys are stored in an area of the filesystem not accessible to users and no user interface is provided to access the cryptographic keys. Dynamically generated cryptographic keys, such as for SSH sessions, are stored in RAM only.cryptographic keys that are stored in the filesystem are stored in plaintext or base64 encoding and are protected using standard Linux filesystem and access control mechanisms.

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 clock is used to provide timestamp for audit records, measuring session inactivity, and 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 built-in self tests include:

1) RAM test – a known value is written to each RAM location and read back to ensure it is identical.
2) Port loopback test – internal and external loopback tests at each supported speed are performed on each port present in the system. The loopback test verifies that the frame generated is the same as the frame received through the loopback.
3) Backend connection test – in chassis systems only, the connection between port blades and core blade is tested by passing a set of fixed data patterns between the port blade and core blade.
4) Port LED test – the LED for each port is cycled through a sequence to display the amber and green colors.

The TOE performs cryptographic algorithm tests, firmware integrity and load tests, and critical function tests. Furthermore, the TOE is designed to query each pluggable module which in turn includes its own diagnostics that will serve to help identify any failing modules. When operating in FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self testing.

The TOE supports loading a new software image either automatically (when so configured) or manually by the administrator using CLI commands. When automatic updates are configured, each time the TOE boots it will attempt to connect to a configured TFTP server in order to compare the current software image name to those available. If a new software version is available it will be automatically downloaded to the TOE. From the CLI, an administrator can use either TFTP or SCP in order to download a software image. In either case, prior to actually installing and using the new software image, its digital certificate is verified by the TOE using the public key in the certificate configured in the TOE. The certificate is stored in an area of the filesystem not accessible to users and no

user interface is provided to access the certificate. 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_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- 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_STM.1: The TOE includes its own hardware clock.
- FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics and cryptographic self-tests that will serve to ensure the TOE is functioning properly. The tests include cryptographic algorithm tests, firmware load and integrity tests, 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.

6.7 TOE access

The TOE can be configured to display a login banner. The login banner can be configured to display welcome information in conjunction with login prompts. It will be displayed when accessing the TOE via the console and SSH.

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 local or remote client) for the defined timeout value will be terminated.

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.

6.8 Trusted path/channels

The TOE implements SSHv2 which is 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. Furthermore, the TOE maintains a list of users that are allowed to access the TOE remotely. As such, even when a session can be negotiated, the TOE then checks to ensure the user is authorized for remote administration and if not the session is dropped.

When a client attempts to connect using SSH, the TOE and the client will negotiate the most secure algorithms available at both ends to protect that session.

In each case, AES-CBC with 256- or 128-bit keys is implemented for encryption and decryption RSA using up to 2048-bit keys are implemented for key exchange and authentication (i.e., distribution).

Note that the product includes other cryptographic algorithms, but since they are not FIPS certified they are not recommended for use and excluded from the scope of evaluation.

Remote connection to SYSLOG servers is protected using TLS.

When a client attempts to download a TOE update though SCP, the TOE uses SSH (which underpins SCP) for secure download of the TOE updates.

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 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 TLS 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 SSH, 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 FIPS certified cryptographic operations, and all remote security management functions require the use of one of these secure channels.