PacketLight PL2000 Series with Firmware v1.3.12c Security Target

Version 1.3

31 August 2020

Table of Contents

1 Document Introduction

This document is the Common Criteria Security Target for PacketLight PL2000 Series with Firmware v1.3.12c. It defines all the elements of a Common Criteria Security Target as defined in Common Criteria Version 3.1 Revision 5 Part 1, Part 2 and Part 3.

1.1 Version history

Version	Date	Revisions
1.3	31 August 2020	Final certification version

1.2 References

[CC Part1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model. April 2017 Version 3.1 Revision 5 CCMB-2017-04-001.

[CC Part 2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components. April 2017 Version 3.1 Revision 5 CCMB-2017-04-002.

[CC Part 3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components. April 2017 Version 3.1 Revision 5 CCMB-2017-04-003.

[CEM] Common Methodology for Information Technology Security Evaluation Evaluation methodology. April 2017 Version 3.1 Revision 5 CCMB-2017-04-004.

[140sp3529] FIPS 140-2 Non-Proprietary Security Policy v1.4, PacketLight Networks Ltd. PL-2000M, PL- 2000AD and PL-2000ADS, Hardware version: PL-2000M, PL-2000AD, PL-2000ADS, Firmware version: 1.3.12, Date: 09/05/2019.

1.3 Abbreviations

CLI	Command Line Interface
CVL	Component Validation List
ECC	Elliptic Curve Cryptography
FC	Fiber Channel
FFC	Finite Field Cryptography
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Security
IG	Implementation Guidance (for FIPS 140-2)
KTS	Key Transport Scheme
LAN	Local Area Network
LED	Light Emitting Diode
LAN	Local Area Network
MSPP	Multiple-Service Protocol Platform

OAM	Operation, Administration, Maintenance
OS	Operating System
OTN	Optical Transport Networking
OTU	OTN Signal type
PM	Performance Monitoring
PRBS	Pseudo Random Binary Sequence
RADIUS	Remote Authentication Dial-In User Service
RSTP	Rapid Spanning Tree Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
STM	Synchronous Transport Mmodule
TFTP	Trivial File Transfer Protocol

2 Security Target Introduction

2.1 ST Identification

ST Title	PacketLight PL2000 Series with Firmware v1.3.12c Security Target
ST Version	1.3
ST Release Date	31 August 2020

2.2 TOE Identification

TOE Name	PacketLight PL2000 Series with Firmware v1.3.12c
TOE Hardware	PL-2000AD, PL-2000ADS, and PL-2000M
TOE Firmware	Firmware v1.3.12c
TOE Guidance	PacketLight PL2000 Series Common Criteria Guidance Supplement v2.1

2.3 TOE overview

2.3.1 Usage and Major Security Features of the TOE

The TOE is the PacketLight PL2000 Series Layer 1 security appliance. The PL-2000AD, PL-2000M and the PL-2000ADS are three product variations of the PL-2000x clone. The product variants run the same firmware and provide the same security functions and mechanisms with minor differences in the network ports.

The PL-2000x series are a 200G multi-protocol 1U MSPP transponder/muxponder device that provides a secure transport solution for long haul (PL-2000AD), metro (PL-2000M) and short-haul (PL-2000ADS) applications. Any data communicated between two connected instances of a TOE is aggregated and encrypted at Layer-1 to ensure secure communication between two devices. The encryption can be per service or per the entire link.

The TOE can be managed locally with a Command Line Interface (CLI) over a serial port, remotely with CLI over telnet or SSHv2, and over the web using a HTTP/HTTPS connection. The TOE implements the cryptographic protocols to protect communication between itself and a remote management station. This ensures that all communication between the TOE and the remote management station is protected from active and passive eavesdropping. Users can be assured that the management commands executed by the TOE are exactly as intended by the administrators and unauthorised parties may not learn the configuration by eavesdropping on the management commands. Telnet and HTTP are considered insecure and are not used in the certified configuration.

The PL-2000 series implements a suite of SNMP protocols for remote monitoring. These include SNMPv1, SNMPv2 and SNMPv3. None of them is used by the TOE. The TOE also implements TFTP and SFTP for file transfer but neither is used by the TOE.

The TOE implements a firewall which allows administrators to restrict the protocols which are allowed for use in the management of the TOE. This allows the administrators to ensure that only connections over protocols considered secure are allowed.

A variant of the PacketLight PL-2000 series appliance with firmware v1.3.12 is FIPS 140-2 Level 2 certified. The FIPS 140-2 non-proprietary security policy for the PL-2000 appliance with firmware v1.3.12 is given in [140sp3529]. The FIPS 140-2 certification covers the essential cryptographic services and the related security functions and mechanisms provided by the appliances when operated with the FIPS mode activated.

The hardware of the TOE and the FIPS 140-2 certified variant of the appliance are identical. The firmware components implementing the cryptographic functions of the TOE and of the FIPS 140-2 certified appliance are also identical. The differences between firmware versions v1.3.12 and v1.3.12c are in the management of the users and roles, and in the protection of various configuration files.

As the cryptographic functions of the TOE are implemented with the firmware components which are identical to the corresponding modules of the FIPS 140-2 certified firmware, using the TOE with the FIPS mode enabled is a prerequisite for secure communication services to the applications. FIPS mode activation ensures that the necessary initialisation of the cryptographic functions are performed even if formally, given the differences in the firmware, the FIPS 140-2 certification is not valid for the firmware v1.3.12c.

The secure communication services, both between two instances of the TOE and between the TOE and external IT devices, are the fundamental security functions of the TOE. They are supported by additional security functions and mechanisms summarised as follows:

- The TOE generates audit records of all relevant security events and stores them for further analysis;
- The TOE implements user authentication for human users and IT devices connected to the TOE and assigns authenticated human users to roles. Access to the functions of the TOE is restricted to those network protocols deemed acceptable by the Administrator, and only to those users whose role assignment provides the necessary credentials for accessing the services. All other accesses are prevented;
- The TOE provides a well defined set of management functions accessible to authorised administrators. These management functions allow the authorised administrators to modify the behavior of the TOE to ensure suitability of the configuration for each specific application. The management functions are available either locally over a serial interface, remotely over a SSHv2 connection, or over the web using HTTPS; and
- The TOE provices physical and logical tamper evidence mechanism which allow users of the TOE to inspect the TOE for integrity. Hardware integrity can be verified by inspection of tamper-evident seals which are placed in the casing of the TOE during manufacturing. They assist in detecting if potential physical tampering of the TOE may have occurred. Integrity and authenticity of the TOE firmware can be verified by authorised users by executing self-test functions engineered to ensure that any violation of authenticity or integrity of the TOE firmware is detected.

The PL-2000M has a single 200G uplink, composed of two multiplexed 100G OTU4 signals, while the PL- 2000AD and PL-2000ADS have dual 100G uplinks. The PL-2000x serve as a multi-protocol, multi-rate, high-capacity optical transport platform for various types of client services with bit rates ranging from 10G to 100G.

The supported services are:

- 10GbE-LAN, 40GbE-LAN, 100GbE-LAN
- 8G FC, 16G FC, 32G FC

- OC-192, STM-64
- OTU2, OTU2e, OTU3, OTU4

The PL-2000x can be configured to work in the following system modes:

Mode	Characteristics
Transponder	Provides two 100G OTN transponders for 100G client services over a 200G uplink.
10G Muxponder	Provides two 100G muxponders for aggregation of 10G client services over a 200G uplink.
32G FC Muxponder	Provides two 100G muxponders for aggregation of 32G client services over a 200G uplink.
2x40G+12x10G Muxponder	Provides two 100G muxponders for aggregation of 40G and 10G client services over a 200G uplink.
4x40G+4x10G Muxponder	Provides two 100G muxponders for aggregation of 40G and 10G client services over a 200G uplink.
100G+10x10G	Provides one 100G OTN transponder for a 100G client service and one muxponder for aggregation of 10G client services over two 100G uplinks.
100G+40G+6x10G	Provides one 100G OTN transponder for a 100G client service and one muxponder for aggregation of 40G and 10G client services over two 100G uplinks.
2x32G+14x10G	Provides muxponder aggregation of 32G and 10G client services over two 100G uplinks.
100G+2x32G+4x10G	Provides one 100G OTN transponder for a 100G client service and muxponder aggregation of 32G FC client services and 10G client services over two 100G uplinks.
10x10G (PL-2000M only)	Provides muxponder for aggregation of 10G client services over 100G uplink.
100G (PL-2000M only)	Provides 100G OTN transponder for a 100G client service over 100G uplink.
40G+6x10G (PL-2000M only)	Provides muxponder for aggregation of 40G and 10G client services over 100G uplink.
2x40G+2x10G (PL-2000M only)	Provides muxponder for aggregation of 40G and 10G client services over 100G uplink.

The PL-2000x products provide several optional types of traffic fault protection:

- 1+1 optical fiber fault protection when an optional Optical Switch is installed (not available for PL-2000ADS).
- 1+1 service fault protection (not available for PL-2000M).
- Equipment fault protection per service port with two PL-2000x devices at each site.

The following management protocols are supported by the PL-2000x products and may be allowed or disallowed by the Administrators through the firewall functionality:

- Command Line Interface (CLI) over a serial interface or Telnet/Secure Shell (SSH) connection.
- Web-based HTTP/HTTPS management.
- SNMP protocol with support for SNMPv1, SNMPv2, and SNMPv3 versions.
- Remote Authentication Dial-In User Service (RADIUS) protocol for centralized remote user authentication.
- Rapid Spanning Tree Protocol (RSTP) for loop prevention of management traffic.
- File Transfer Protocols such as TFTP and SFTP for file transfer of system software, Log files, and Configuration files.
- Simple Network Time Protocol (SNTP) for network calendar timing.
- Syslog protocol for monitoring device events by a remote server.
- Virtual chassis configuration, using a single IP address for multiple nodes.

The module supports the following Operations, Administration, and Maintenance (OAM) functions over management interfaces:

- Optical parameters monitoring.
- Alarm and Event fault management.
- Layer 1 and Layer 2 Performance monitoring (PM).
- Terminal loopback and Facility loopback for optical data ports.
- Diagnostic Pseudo Random Binary Sequence (PRBS) for the optical data ports2.
- Environmental (External) Alarms.

2.3.2 TOE Type

This ST claims no conformance to any Protection Profile. Therefore, the TOE is not of type defined in any Protection Profile. Instead, TOE is a hardware cryptographic appliance with the primary function of protecting the Layer 1 communication between two instances of the TOE.

2.3.3 Non-TOE Hardware, Firmware and Software

The TOE requires the following non-TOE Hardware, Firmware and Software components to function:

Component	Description
A second instance of a TOE	The TOE is an appliance which is configured to operate pairwise. Two instances of a TOE are connected to provide the required communication service and for protecting that communication. A second instance of a TOE is required for the TOE to function in the intended setup.
Web client	The TOE requires a Web client for secure administration of the TOE over a HTTPS connection.

SSHv2 client	The TOE requires a SSHv2 client which is used for a secure connection to the TOE for remote administration.
Serial connection client	The TOE requires a serial connection client for local administration.
Other connectivity	The TOE requires connectivity for the services that use the TOE for communication, and for the two interconnected instances of the TOE.

2.4 TOE description

This section states the physical and logical scope of the TOE.

2.4.1 Physical scope of the TOE

The physical scope of the TOE consists of the following:

Component	Description
TOE Hardware	The TOE hardware is the PacketLight PL-2000 series hardware, including the following: ○ PL-2000AD intended for long haul applications; ○ PL-2000M intended for metropolitan applications; and ○ PL-2000ADS intended for short haul applications. Different hardware variants have a slightly different interfaces but they all provide identical TOE Security Functions.
TOE Firmware	TOE firmware is version v1.3.12c. The TOE is delivered with firmware installed on the hardware. The firmware may be v1.3.12c or other v1.3.12 variant. The TOE provides a function for verifying the version of the firmware and supports firmware update through ALC_FLR.1 mechanism. The user of the TOE must verify the received firmware version and ensure that if the TOE is delivered with firmware variant other than v1.3.12c, the firmware is updated to v1.3.12c in accordance with the security guidance prior to the deployment of the TOE.
Guidance Supplement	The TOE is delivered with Common Criteria Guidance supplement named as *PacketLight PL2000 Series Common Criteria Guidance Supplement v2.1.*

The TOE is delivered as an appliance with minor variants on the interfaces of different appliances. The firmware and guidance are identical on all appliances. The firmware is delivered installed on the TOE (but may need to be updated to v1.3.12c) and the guidance supplement is delivered over an email with a link from which the document may be downloaded.

The connectivity of the TOE is provided in the front panels. The front panels of PL-2000AD, PL-2000ADS and PL-2000M model appliances are illustrated in Figure 1, Figure 2, and Figure 3 respectively.

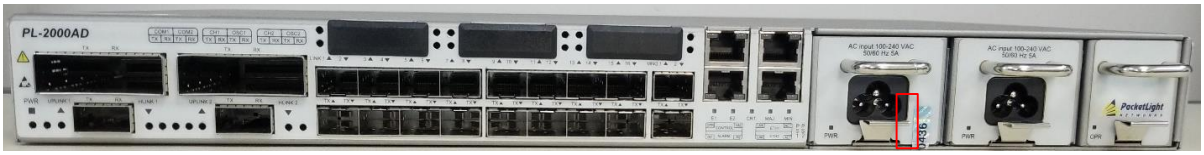

Figure 1 – Front panel of PL-2000AD

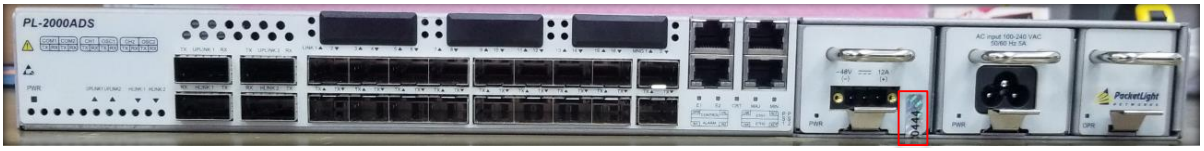

Figure 2 – Front panel of PL-2000ADS

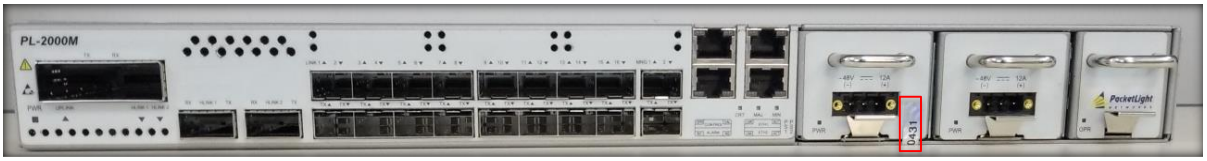

Figure 3 – Front panel of PL-2000M

The rear and side panels are identical on all versions. The right hand side of the appliance contains the fans and therefore the right hand side has the required openings for the ventilation as illustrated in Figure 4. The left hand side panel has smaller openings as illustrated in Figure 5. The rear panel only has a LED indicator as illustrated in

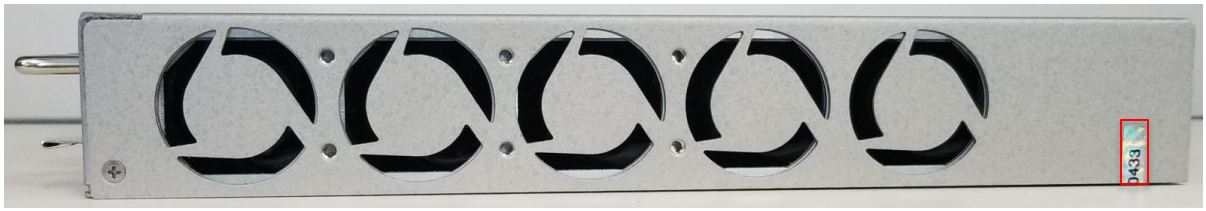

Figure 4 – The right hand side panel

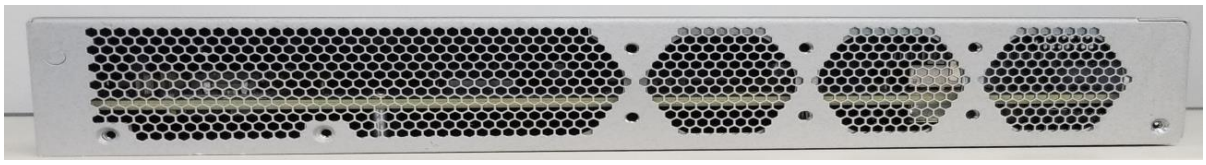

Figure 5 – The left hand side panel

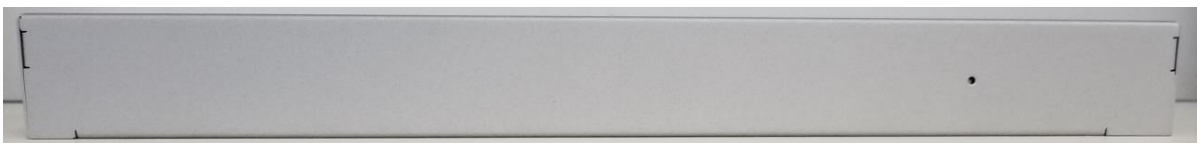

Figure 6 – The rear panel

The casing of the TOE is covered with tamper-evident seals to give basic detection of attempted physical tampering. The seals, illustrated as red rectangles in figures above, are applied at production time. Nevertheless, the intended use case scenario is that the TOE resides in a secure data center in which only authorised personnel is granted physical access to the appliance.

The user can identify different parts of the TOE as follows:

- The hardware version is identified by the model indicator in the upper left hand side corner of the front panel.
- The TOE provides a function for the authorised administrator to verify the firmware version number.
- The guidance supplement is identified by the title and the version number on the cover and each page of the supplement.

2.4.2 Logical scope of the TOE

The logical scope of the TOE consists of the security functions and mechanisms, jointly called TOE Security Functions (TSF), provided by the TOE. The TSF the TOE provides are stated in the following.

TSF	Description
Security Audit	The TOE is capable of generating audit data of relevant security events. The audit data is stored by the TOE for further analysis.
Secure communication	The TOE implements a set of cryptographic functions for two purposes: 1. to protect communication of sensitive data between itself and another instance of a TOE, and 2. to protect communication between itself and other trusted IT products. The other trusted IT product may be a remote management workstation or a web management workstation.
User management, authentication and access control	The TOE maintains a unique account for each user. Users are assigned to roles and access to TOE functions is granted based on the role of the user. Any access not deemed legitimate (i.e. in violation of the access control policies of the TOE) is prevented from occuring. Remote access to the TOE functions is only allowed using protocols which are explicitly approved by the Administrator of the TOE. The firewall of the TOE drops all other protocols. User credentials are protected from unauthorised access and can be changed by users if suspecting a compromise, or periodically as applicable. Inactive user sessions are terminated by the TOE and the users are also provided the necessary functions to terminate their sessions.
Security management	The TOE provides a set of management functions available to legitimate administrators for configuring the behavior of the TOE.
Tamper evidence	The TOE casing is protected with tamper evident seals which allows users of the TOE to visually detect attempts of physical tampering with the TOE. The TOE also implements a mechanism to verify the firmware version installed on the appliance and self tests to assist the administrators in asserting the authenticity and integrity of the critical functions of the TOE firmware and the authenticity of the firmware itself.

Some of the communication protocols implemented by the PL-2000 appliance are not considered secure and are not included in the logical scope of the TOE. The protocols implemented by the TOE are listed below and their inclusion in the logical scope of the TOE stated.

Protocol	Inclusion in the logical scope of the TOE
Command Line Interface over a serial port	Included
Command Line Interface over Telnet/SSH	Telnet excluded SSH included
Web-based HTTP/HTTPS management	HTTP not included HTTPS included
SNMP Protocol	SNMPv1 not included SNMPv2 not included SNMPv3 not included
RADIUS for remote user authentication	Not included
Rapid Spanning Tree Protocol (RSTP)	Not included
File transfer protocols	TFTP not included SFTP not included
Simple Network Time Protocol (SNTP)	Not included
Syslog protocol	Not included
Virtual chassis configuration	Not included

3 Conformance Claims

3.1 Conformance claims statement

The ST and TOE claim conformance to

- Common Criteria v3.1 Revision 5 Part 1 which is fully identified in [CC Part 1],
- Common Criteria v3.1, Revision 5 Part 2 which is fully identified in [CC Part 2], and
- Common Criteria v3.1 Revision 5 Part 3 which is fully identified in [CC Part 3].

The ST is CC Part 2 conformant.

The ST is CC Part 3 Augmented conformant.

The ST claims conformance to the following Protection Profiles and Packages: **None**.

The ST claims package conformance to the following: **Evaluation Assurance Level EAL2 Augmented with ALC_FLR.1**. ALC_FLR.1 is fully defined in [CC Part 3].

3.2 Conformance claims rationale

The ST does not claim conformance to any Protection Profile. Therefore, the Conformance Claims Rationale is not applicable.

4 Security Problem Definition

This section states the threats the TOE mitigates, the assumptions about the security environment of the TOE, and the organisational security policies that must be followed in the use and operation of the TOE and the operational environment thereof.

4.1 Threats

Threat	Description
T.AUDIT	An unauthorised user gaining access to the TOE or the environment thereof, or a legitimate user of the TOE operating the TOE in violation of security guidance succeeds in discovering a way to operate the TOE in a manner which renders illegitimate activities undetected by successfully bypassing or circumventing the audit record generation function of the TOE.
T.COMMUNICATION	An unauthorised user of the TOE succeeds in gaining access to the communication between two instances of the TOE or between a TOE and a remote IT product the TOE communicates with in order to 1. Distract the communication between two instances of the TOE to falsify the data communicated between parts of the application using the TOE; 2. Trigger an unauthorised configuration of the TOE a) by falsifying the management commands issued by a legitimate administrator of the TOE, b) by injecting unauthorised management commands into the TOE which the TOE can not differentiate from legitimate management commands, or c) by providing to administrators off the TOE false feedback on the execution outcome of management commands; or 3. Disclose the content of the communication to disclose sensitive data communicated between two instances of the TOE or the configuration of the TOE as modified by administrators.
T.ACCESS	An unauthorised party succeeds in masquerading as a legitimate administrator by 1) discovering that the TOE accepts remote management commands over an insecure protocol, or 2) by correctly guessing the authentication credentials of a legitimate administrator or by discovering a method of bypassing the authentication of human users of the TOE. **NOTE**: T.ACCESS concerns with the prevention of illegitimate accesses to the TOE through bypassing of circumventing of the the authentication, role assignment and access control functions. Gaining illegitimate access by tapping the communication between a TOE and connected devices is addressed at T.COMMUNICATION.
T.MANAGEMENT	A legitimate administrator of the TOE or an unauthorised user discovers a mechanism to change the configuration of the TOE without invoking the respective management interface of the TOE, or a mechanism which prevents without detection a management command from taking effect when issued by a legitimate administrator of the TOE.

T.TAMPERING	A legitimate or illegitimate user who succeeds (either in a legitimate or in an illegitimate manner) gaining physical access to the TOE succeeds in tampering with the TOE hardware or firmware without detection when the TOE is inspected logically by self tests or visually for signs of physical tampering by the administrators. **NOTE:** The TOE provides a mechanism for detection of attempted physical and logical tampering, not to prevent it. Consequently, the administrators must inspect the TOE physically on a regular basis to observe any tampering with the tamper-evident seals on the casing of the TOE and logically by executing the on-demand self-tests.

4.2 Assumptions

There are no assumptions governing the use of the TOE.

4.3 Organisational security policies

OSP	Description
OSP.ADMIN	The organisation utilising the TOE has in place a policy that covers the selection and training of the administrators to ensure that each administrator is trustworthy and has received sufficient training to administer the TOE in a secure manner. Administrators are committed into only using the TOE in accordance with good IT security practices and in full conformance with the security guidance of the TOE. Records are kept of the application of all selection and training procedures as well as of the expressed commitment of the administrators to operate the TOE in accordance with all security guidance.
OSP.FIPS140-2	The organisation using the TOE has in place a defined and enforced security policy requiring that the TOE is to be always used with the FIPS mode enabled and operated in full conformance with the FIPS 140-2 Security policy of PL2000 series stated in [140sp3529].
OSP.PHYSICAL	The TOE resides in a physically secure premises. The management workstation, whether local or remote, and the cabling connecting the TOE to the management workstation are to reside in the same premises. The organisation using the TOE has in place a defined and enforced policy on the minimum physical security arrangements which are, as per the user's risk assessment, sufficient for mitigating the risk of access to the TOE which would allow physical attacks which go beyond what can be reasonably expected to be detected by the tamper evident seals of the TOE casing.

5 Security Objectives

This section states the security objectives for the TOE and for the environment of the TOE. It also provides a secure objectives rationale.

5.1 Security objectives for the TOE

Objective	Objective statement
O.AUDIT	The TOE generates an accurate audit record for each relevant auditable event and assignes each audit record with a time stamp.The audit records are stored by the TOE in a manner that prevents unauthorised modification of the audit records. The audit records allow administrators to examine them and unambigiously detect any possible unauthorised operation on the TOE or successfully trace the actions to the administrators and users of the TOE.
O.COMMUNICATION	The TOE ensures that all communication 1) between two instances of a TOE, 2) between a TOE and a remote management station, and 3) between a TOE and the Web management station is protected from eavesdropping of the data streams, undetected modification of data streams, undetected injection of fabricated data into the data stream, and undetected removal of legitimate content from the data stream.
O.ACCESS	The TOE ensures that 1) the likelihood of an unauthorised party successfully masquerading as a legitimate user of the TOE is sufficiently low, and that access to the functions of the TOE is only granted to legitimate users, whether human users or other IT devices (i.e. remote or Web management station), and 2) remote administration of the TOE is only allowed over secure protocols.
O.MANAGEMENT	The TOE provides a well defined set of management functions to the administrators and ensures that each management action is fully executed when called by a legitimate administrator, and that there are not alternative methods of executing management commands or otherwise configuring the TOE.
O.TAMPERING	The TOE ensures that any attempted logical or physical tampering with the TOE is detected.

5.2 Security objectives for the environment

Objective	Objective statement
OE.ADMIN	The operational environment shall provide one or more competent administrators assigned to manage the TOE, its platform and the security of the information both of them contain. The operational environment will ensure that the administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.

OE.PHYSICAL	Physical security mechanisms, commensurate with the value of the TOE and the data it contains, are provided by the environment to prevent unauthorised access to the TOE and TSF data.

5.3 Security objectives rationale

This section provides the security objectives rationale. It first provides a tracing of security objectives to the security problem definition and then provides a justification for the tracing.

The tracing of elements in the security environment of the TOE to the security objectives of the TOE and the environment of the TOE is given below.

	O.AUDIT	O.COMMUNICATION	O.ACCESS	O.MANAGEMENT	O.TAMPERING	OE.ADMIN	OE.PHYSICAL
T.AUDIT	X						
T.COMMUNICATION		X					
T.ACCESS			X				
T.MANAGEMENT				X			
T.TAMPERING					X		
OSP.ADMIN				X		X	
OSP.PHYSICAL					X		X
OSP.FIPS140-2		X	X				

O.AUDIT concerns with ensuring that 1) the TOE generates an accurate audit record for each relevant auditable event and assigns each audit record with a time stamp, that 2) the TOE stores the generated audit records in a manner that prevents their unauthorised modification, and that 3) the audit records allow administrators to detect any possible unauthorised operation on the TOE or successfully trace the actions to the administrators and users of the TOE. T.AUDIT is prevented from occurring if

1. unauthorised and legitimate users are prevented from manipulating the TOE in a way that allows execution of TOE functions in a manner that does not generate the audit record or the audit record time stamp is falsified;
2. illegitimate and legitimate users are preventing from manipulating the TOE in a manner that prevents storage of the audit record; and

3. as a combination of the above, the users of the TOE may not reduce the quality of the audit records generated by the TOE, hence not being able to reduce the administrators' ability to investigate TOE use and trace user actions to specific users.

Jointly, the above three concerns fully address the aspects of O.AUDIT. Therefore, O.AUDIT is satisfied and enforced if T.AUDIT is prevented from occurring.

O.COMMUNICATION concerns with protection of the communication between the TOE and external entities. The external entities of concern are another instance of a TOE, a remote management station and a Web management station.

Preventing violations of the security of these communications ensures that T.COMMUNICATION is prevented from occurring. However, they alone are not sufficient for ensuring that O.COMMUNICATION is satisfied and enforced. Additionally, the TOE must at all times used so that the FIPS mode of the PL-2000 series appliance is enabled, i.e. OSP.FIPS140-2 is definied and enforced. This ensures that the appliance is used in conformance with the FIPS 140-2 certificate for the PL-2000 Cryptographic Module, and that each cryptographic algorithm is used in conformance with their respective Cryptographic Algorithm Validation Program certificates. Jointly, preventing T.COMMUNICATION from occurring and having OSP.FIPS140-2 enforced ensure that O.COMMUNICATION is satisfied and enforced and the TOE can be trusted to deliver the secure communication services to the applications.

O.ACCESS concerns with ensuring that

1. All users are authenticated prior granting access to the TOE and that the TOE only grants accesses which are in conformance with the access control policies of the TOE. O.ACCESS does not concern with the violation of communication security (which is the concern of O.COMMUNICATION) that might grant unauthorised parties access to TOE functions but with the enforcement of user authentication and well defined access control policies on all TOE accesses.
2. The TOE only accepts management commands from remote management stations over secure protocols. This is enforced when the TOE implements a firewall preventing access through protocols deemed insecure and that the TOE is operated in accordance to FIPS 140-2 certificate in which the firewall is configured to disallow insecure protocols.

These concerns are addressed if T.ACCESS is prevented from occurring and OSP.FIPS140-2 is enforced. Consequently, enforcing O.ACCESS from these parts prevents T.ACCESS from occurring and ensures that OSP.FIPS140-2 is enforced.

O.MANAGEMENT concerns with ensuring that management of the TOE only occurs through legitimate management interfaces. The TOE provides a rich set of management functions which are the only legitimate interface to the management functions. T.MANAGEMENT concerns with the users finding alternative means of managing the TOE which are not available, i.e. preventing T.MANAGEMENT from occurring partially enforces O.MANAGEMENT, and enforcing O.MANAGEMENT prevents T.MANAGEMENT from occurring. However, preventing T.MANAGEMENT alone is not sufficient for enforcing O.MANAGEMENT. The administrators of the TOE must also be committed into using the TOE in accordance with good IT Security practices and in full conformance with the security guidance. This occurs whe OSP.ADMIN is enforced by the organisation using the TOE, i.e. the administrators only use the TOE using the legitimate management interface. This also contributes to the enforcement of O.MANAGEMENT.

O.TAMPERING concerns with ensuring that any attempted physical and logical tampering with the TOE is detected with a high probability. This is enforced of T.TAMPERING is prevented from occurring. However, the TOE does not contain mechanisms for active detection of attempted tampering. Consequently, the technical measures for preventing O.TAMPERING from occurring (and preventing T.TAMPERING from occurring) must be applied together with the TOE residing in a physically secure environment. This ensures that any opportunity to physically attack the TOE occurs in a sufficiently small time window that the unauthorised presence is detected with likelihood until the physical and logical anti-tampering defenses of the TOE are overwhelmed (and the physical anti-tampering measures restored by the attacker to a state in which they can not be differentiated from intact anti-tampering measures). Consequently, O.TAMPERING is fully enforced of T.TAMPERING is prevented from occurring and OSP.PHYSICAL enforced in the environment in which the TOE is used.

OE.ADMIN concerns with ensuring that the administrators of the TOE are well behaving and always operate the TOE in accordance with good IT Security practices and in full conformance with the security guidance. This can not be enforced by TOE Security functions and mechanisms but must be addressed through personnel selection and training by the organisating using the TOE. Consequently, OE.ADMIN is fully enforced of the organisation using the TOE has defined and enforced policy OSP.ADMIN.

OE.PHYSICAL concerns with ensuring that the TOE resides in a physically secure environment in which the likelihood of unauthorised users gaining physical access to the TOE is sufficiently low. As the TOE does not contain mechanisms for preventing physical attacks beyond tamper-evident seals in teh casing and basic self-tests, it must only be used in environments which are physically secure. Therefore, OE.PHYSICAL is prevented from occurring of the organisation using the TOE has defined and enforced policy OSP.PHYSICAL.

6 Extended Components Definition

This ST defines no extended components applicable to the TOE. Therefore, this section is not applicable and is omitted.

7 Security Functional Requirements

This section defines the security requirements for the TOE. As there are no extended components defined for the ST, the security functional requirements are only defined with reference to CC Part 2. The security assurance requirements are defined with reference to a well-defined evaluation assurance package EAL2 defined in CC Part 3, augmented with ALC_FLR.1 also defined in CC Part 3.

The statement of security functional requirements utilizes operations as defined for each applicable security functional requirement in CC Part 2. The notation for identifying the operations is as follows:

Iteration is identified by repeating the identifier of the security functional requirement with a string indicating a specific iteration separated from the SFR identification by a slash (e.g. FCS_COP.1/AES, FCS_COP.1/DSIG).

Refinement is identified by a) indicating in square brackets in bold font any added text, in form of [**Refinement: added text**] and b) indicating any removed words using ~~overstrike~~ font. Whenever a refinement is used, the rationale and justification of the refinement is given immediately after the statement of the security requirement.

Selection is identified by indicating the selected values in [**square brackets using bold font**].

Assignment is identified by indicating the assigned values in [***square brackets using bold italic font***].

Application notes may be added after the formal statement of the security requirements to assist the reader in understanding the specific security requirement in the context of this particular TOE.

7.1 Statement of Security Functional Requirements

7.1.1 FAU: Security Audit

7.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [**not specified**] level of audit; and

c) [The following auditable events:

Alarm Rise: This event is generated when a new alarm is detected.

Alarm Clear: This event is generated when an alarm is cleared.

Link Up: This is an event that is generated when the operational status of a port is changed from Down to Up.

Link Down: This is an event that is generated when the operational status of a port is changed from Up to Down.

Cold Restart: This is an event that is generated after a cold restart of the node.

Warm Restart: This is an event that is generated after a warm restart of the node.

Test Status Changed: This event is generated when the loopback or PRBS test status of a port is changed.

Inventory Change: This event is generated when the node inventory is changed.

Unsolicited Event: This event is generated when an exceptional incident occurs.

Power Level Event: This event is generated when two consequtive readings of the uplink optical port power differ with more than 2dB.

Configuration Change: This event is generated when the node configuration is changed

].

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 (if applicable), 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, [***no other audit-relevant information***].

7.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**authorised users**] with the capability to read [***data, time, event and outcome (success or fail)***] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.2 FCS: Cryptographic support

7.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***CKG***] and specified cryptographic key sizes [***128 bits, 192 bits and 256 bits***] that meet the following: [***NIST SP 800-90A***].

7.1.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [***Stated in Table 1***] that meets the following: [***Standards stated in Table 1***].

Table 1 Key distribution and agreement methods

Method	Key size(s)	Standard(s)	Purpose	Use
CVL	256 bits	SHA-1, SHA- 256, SHA-384, SHA-512	TLS, SSH, KDF	Key derivation

CVL	N/A[1]	SP 800-56A	ECC CDH Component Testing	Key agreement
KTS	128 bits, 192 bits, 256 bits	IG D.9	KTS (AES GCM)	Key Transport key establishment methodology provides between 128 and 256 bits of encryption strength
CVL (FFC)	P = 2048, q = 256;	SP 800-56A	DH Ephemeral	Key agreement
CVL (ECC)	P-256, P- 384, P-521	SP 800-56A	DH Ephemeral united	Key agreement

7.1.2.3 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***Stated in table 2***] that meets the following: [***none***].

Table 2 Cryptographic key destruction methods

Key(s)	Destruction method
Ephemeral keys	Zeroized at session termination or by power-cycling the module.
Persistently stored keys	Zeroized by issuing a factory reset. This changes all values back to zero or to the default values.
SSH Host Key Pair	Zeroized by a command invoked by the Admin role at the Command Line Interface
All non-persistent keys	Zeroized prior to the TOE transitioning to/from FIPS approved mode

7.1.2.4 FCS_COP.1 Cryptographic operation

FCS_COP.1.1/HW The TSF shall perform [***Operations stated in Table 3***] in accordance with a specified cryptographic algorithm [***stated in Table 3***] and cryptographic key sizes [***stated in Table 3***] that meet the following: [***Standards stated in Table 3***].

Table 3 Hardware Cryptographic functions

Algorithm	Key size(s)	Standard(s)	Mode	Operations
AES	256 bits	SP 800-38A , FIPS PUB 197, SP 800-38D	ECB, GCM, CTR	Data encryption, decryption and authentication
KTS	256 bits	IG D.9	KTS (AES GCM)	Key Transport

[1] Partial Public Key Validation

FCS_COP.1.1/FW The TSF shall perform [***Operations stated in Table 4***] in accordance with a specified cryptographic algorithm [***stated in Table 4***] and cryptographic key sizes [***stated in Table 4***] that meet the following: [***Standards stated in Table 4***].

Table 3 Firmware Cryptographic functions

Algorithm	Key size(s)	Standard(s)	Mode	Operations
AES	128 bits, 192 bits, 256 bits	SP 800-38A, FIPS 197, SP 800-38D	CBC, CFB, ECB, GCM, CTR	Data encryption, decryption and authentication
HMAC	160 bits, 256 bits, 384 bits, 512 bits	FIPS PUB 198	SHA-1, SHA-256, SHA-384, SHA-512	Message authentication
SHS	N/A	FIPS PUB 180-4	SHA-1, SHA-256, SHA-384, SHA-512	Message digest generation
RSA	2048 bits, 3072 bits[2]	FIPS PUB 180-4	N/A	Key Generation, Signature Generation, Signature Verification

7.1.3 FDP: User data protection

7.1.3.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [***Service Access SFP***] on [
Subjects: Users,
Objects: Services,
Operations: Execution
].

7.1.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [***Service Access SFP***] to objects based on the following: [
Users: Role,
Objects: Function
].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***Executing a function is only allowed to a user in a role if the cell value of that function is 'X' for that role***].

[2] For key generation only

Function	Read-Write	Read only	Crypto officer	Admin
Initialization	X			X
Manage accounts				X
Change password	X	X	X	X
Manage encryption service			X	
Add/Change Pre-Shared Secret			X	
Lock Encrypted Service			X	
Change Provisioning Type	X			X
View Performance Monitoring	X	X	X	X
View Faults or Alarms	X	X	X	X
Configure firewall				X
Request Status Information	X	X	X	X
Set configuration data	X			X
Export backup of configuration file over HTTPS				X
View Network Topology	X	X	X	X
On-Demand Self-test	X	X	X	X
Zeroization/Factory Reset				X
Firmware Update	X			X

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***Start-up self-tests may be executed by any user***].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***].

7.1.3.3 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [***Firewall SFP***] on [
Subjects: TOE, External IT Device
Information: Network traffic
] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

7.1.3.4 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [***Firewall SFP***] based on the following types of subject and information security attributes: [
TOE: None
External IT Device: IP Address
Network traffic: Protocol, Allowed
].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [***Information flows from External IT Device to the TOE is allowed if the IP Protocol of the Network traffic is Allowed by the firewall rules***].

FDP_IFF.1.3 The TSF shall enforce the [***None***].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [***Information flow is allowed if the External IT Device is another instance of a TOE***].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [***None***].

7.1.4 FIA: Identification and authentication

7.1.4.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***Username, Password, Role***].

7.1.4.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [***execution of on-demand self-tests***] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.4.3 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [***if the session exceeds the configured timeout value***].

7.1.4.4 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [***obfuscated feedback***] to the user while the authentication is in progress.

7.1.4.5 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [***execution of on-demand self-tests***] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.1.4.6 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [***a password must be in the minimum 8 bytes and in maximum 20 bytes in length***].

7.1.5 FMT: Security management

7.1.5.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [***Firewall SFP***] to restrict the ability to [**modify**] the security attributes [***Allowed network traffic***] to [***Administrator***].

7.1.5.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [***Service Access SFP, Firewall SFP***] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***none***] to specify alternative initial values to override the default values when an object or information is created.

7.1.5.3 FMT_SMF.1 Management of TSF data

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [
Initialization;
Manage accounts;
Change password;
Manage encryption service;
Add/Change Pre-Shared Secret;
Lock Encrypted Service;
Change Provisioning Type;
View Performance Monitoring;
View Faults or Alarms;
Configure firewall;
Request Status Information;
Set configuration data;
Export backup of configuration file over HTTPS;
View Network Topology;
On-Demand Self-test;
Zeroization/Factory Reset;
Firmware Update
].

7.1.5.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [***Administrator (Admin), Crypto-Officer (CO), Read-Write, Read-Only***].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

7.1.6 FPT: Protection of the TSF

7.1.6.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [***failure of a self-test***].

7.1.6.2 FPT_PHP.1 Passive detection of physical attacks

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

7.1.6.3 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

7.1.6.4 FPT_TEE.1 Testing of external entities

FPT_TEE.1.1 The TSF shall run a suite of tests [**periodically during normal operation**] to check the fulfillment of [***Integrity of the optical link***] .

FPT_TEE.1.2 If the test fails, the TSF shall [***warn the user***] .

7.1.6.5 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests [**during initial start-up, periodically during normal operation, at the request of the authorised user**] to demonstrate the correct operation of [[***TOE Firmware, Firmware cryptographic functions, Hardware cryptographic functions, Entropy and Random Number Generators***]].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [[***Service table***]].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [[***TOE Firmware, Firmware cryptographic functions, Hardware cryptographic functions, Entropy and Random Number Generators***]].

7.1.7 FTA: TOE access

7.1.7.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after an [***administrator-configurable time limit***].

7.1.7.2 FTA_SSL.4 User-initiated termination

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

7.1.8 FTP: Trusted path/channels

7.1.8.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**modification, disclosure**].

FTP_TRP.1.2 The TSF shall permit [**remote users**] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**initial user authentication,** [***TOE Administration***]].

7.2 Security assurance requirements

Security assurance requirements for the TOE constitute the evaluation assurance package EAL2 Augmented with ALC_FLR.1 and are fully defined with reference to CC Part 3. The security assurance requirements are the following:

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description

	ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures ALC_FLR.1 Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7.3 Security requirements rationale

7.3.1 Security requirement dependency rationale

For each Security Functional Requirement applicable to the TOE, the following identifies all dependencies and states whether they are satisfied by the TOE or not. For each dependency not satisfied by the TOE, a justification is given for the non-satisfaction.

SFR	Dependencies	Rationale
FAU_GEN.1	FPT_STM.1	FPT_STM.1 by the TOE
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1 by the TOE
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 by the TOE FCS_CKM.4 by the TOE
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 by the TOE FCS_CKM.4 by the TOE

FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 by the TOE
FCS_COP.1/HW	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 by the TOE FCS_CKM.4 by the TOE
FCS_COP.1/FW	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 by the TOE FCS_CKM.4 by the TOE
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1 by the TOE
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 by the TOE FMT_MSA.3 by the TOE
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1 by the TOE
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2 by the TOE. FDP_IFC.2 is hierarchical to FDP_IFC.1 and therefore appropriate for satisfying the dependency. FMT_MSA.3 by the TOE.
FIA_ATD.1	No dependencies	N/A
FIA_UAU.1	FIA_UID.1	FIA_UID.1 by the TOE
FIA_UAU.6	No dependencies	N/A
FIA_UAU.7	FIA_UID.1	FIA_UID.1 by the TOE
FIA_UID.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 for **Service Access SFP** is not satisfied by the TOE. The access control rules for different roles to access the services are hard coded into the TOE and can not be accessed by any user. Therefore, there are no roles which are granted any access to the rules and the dependency is not applicable. FDP_IFC.1 for **Firewall SFP** by the TOE FMT_SMR.1 by the TOE FMT_SMF.1 by the TOE
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 for **Service Access SFP** is not satisfied by the TOE. The access control rules are hard coded into the TOE FW and a) there are no functions to query or otherwise access them for reading, and b) they can not be modified by users in any role. Therefore, FMT_MSA.1 is unnecessary. FMT_MSA.1 for **Firewall SFP** by the TOE. FMT_SMR.1 by the TOE
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1 by the TOE
FPT_FLS.1	No dependencies	N/A
FPT_PHP.1	No dependencies	N/A

FPT_STM.1	No dependencies	N/A
FPT_TEE.1	No dependencies	N/A
FPT_TST.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTA_SSL.4	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

7.3.2 Tracing of security objectives to Security Functional Requirements

The tracing of the security objectives for the TOE to the Security Functional Requirements is given below. The tracing shall be followed by a justification demonstrating that the Security Functional Requirements are sufficient for fulfilling the security objectives.

SFR	O.AUDIT	O.COMMUNICATION	O.ACCESS	O.MANAGEMENT	O.TAMPERING
FAU_GEN.1	X				
FAU_SAR.1	X				
FCS_CKM.1		X			
FCS_CKM.2		X			
FCS_CKM.4		X			
FCS_COP.1/HW		X			
FCS_COP.1/FW		X			
FDP_ACC.1	X		X	X	
FDP_ACF.1	X		X	X	
FDP_IFF.1			X		
FDP_IFC.1			X		
FIA_ATD.1			X		
FIA_UAU.1			X		
FIA_UAU.6			X		
FIA_UAU.7			X		
FIA_UID.1			X		
FIA_SOS.1			X		
FMT_MSA.1			X	X	
FMT_MSA.3			X	X	

FMT_SMF.1				X	
FMT_SMR.1			X	X	
FPT_FLS.1					X
FPT_PHP.1					X
FPT_STM.1	X				
FPT_TEE.1		X			
FPT_TST.1					X
FTA_SSL.3			X		
FTA_SSL.4			X		
FTP_TRP.1		X			

O.AUDIT concerns with ensuring that the TOE provides sufficient data in audit records for the administrators to examine the operation of the TOE. This is satisfied if the TOE indeed generates the necessary audit records (FAU_GEN.1) and equips them with appropriate time stamps (FPT_STM.1). Furthermore, the TOE ensures that the audit records are stored in a manner that is suitable for analysis (FAU_SAR.1) and that access to review audit records is granted to authorised parties (FPT_ACC.1 and FPT_ACF.1 - specifically row "View faults or alarms"). Jointly these SFRs ensure that O.AUDIT is fully enforced by the TOE.

O.COMMUNICATION concerns with ensuring that the communication between the TOE and external entities is sufficiently protected. This concerns with two types of communication: 1) protection of the communication between two instances of a TOE (i.e. encrypting the link or a service over a link) and 2) protection of the communication between a TOE and the various management stations.

Concern (1) is addressed by the TOE providing a) a range of cryptographic functions for key management, i.e. key generation (FCS_CKM.1), key distribution and agreement (FCS_CKM.2) and key destruction, and b) a set of cryptographic functions implemented in TOE hardware (FCS_COP.1/HW) and firmware (FCS_COP.1/FW). The TOE also implements an additional mechanism for monitoring the integrity of the optical link connecting two instances of the TOE. This is achieved by measuring and monitoring the optical power of the uplink power. A substantial change in the power between two measurements is indicative of a potential tapping of the optic link and the user is notified of the irregularity (FPT_TEE.1).

Concern (2) is addressed by the TOE providing a trusted path between itself and aremote management station, and between itself and a Web management station (FTP_TRP.1).

Jointly, addressing concerns (1) and (2) ensure that O.COMMUNICATION is fully enforced by the selected Security Functional Requirements.

O.ACCESS concerns with the TOE ensuring that access is only granted to legitimate users of the TOE. This consists of two aspects: 1) ensuring that users are identified and authenticated using sufficiently strong authentication measures and assigned to roles, 2) ensuring that access to controlled functions is only granted to users acting in well defined roles, and 3) only explicitly authorised protocols are allowed to be used in the management of the TOE.

Concern (1) is addressed is all users are assigned to well defined roles (FMT_SMR.1). The user maintains for each user security attributes Username, Password, and Role (FIA_ATD.1). The user must enter correct Username and Password for successful authentication and only shall be assigned to a role upon successful authentication. During the authentication, the TOE only provides obfuscated feedback of the password (FIA_UAU.7) to prevent unauthorised parties learning the passwords. The TOE also imposes a time limit on remote management sessions (FTA_SSL.3) and requires re-authentication to renew the session (FIA_UAU.6). The users are allowed to terminate their own sessions (FTA_SSL.4) and to select their own passwords (FDP_ACC.1, FDP_ACF.1) but the TOE imposes restrictions on the minimum quality of them (FIA_SOS.1).

Concern (2) is satisfied with the TOE ensuring that access control functions are well definied (FDP_ACC.1 and FDP_ACF.2) and that by default, access is restrictive i.e. access is not granted to any party unless properly assigned to a well defined role (FMT_MSA.3). The only exception to this is the execution of start-up self-tests of the TOE (FIA_UID.1, FIA_UAU.1). Those tests are automatically executed at the start-up of the TOE prior to any authentication and access control function is active and, therefore, are available to any user who gains physical access to the TOE.

Concern (3) is satisfied with the TOE ensuring that information flow for management of the TOE is only allowed from approved IP addresses using allowed protocols (FDP_IFC.1, FDP_IFF.1). Furthermore, all network protocols are disallowed by default (FMT_MSA.3) and any allowed protocols must be explicitly declared allowed by the Administrator (FMT_MSA.1).

Jointly, addressing concerns (1), (2) and (3) ensure that O.ACCESS is fully enforced by the selected Security Functional Requirements.

O.MANAGEMENT concerns with the TOE providing a well defined management interface which is only accessible through a legitimate management interface. To achieve this, the TOE includes a set of defined roles (FMT_SMR.1) and a well defined set of management functions (FMT.SMF.1). For each role, the TOE has a defined set of access rights to different management functions and enforces that accesses are only granted to users in those roles which have a right to access the function (FDP_ACC.1, FDP_ACF.1). By default, users have no access rights and access rights are only made available upon proper role assignment (FMT_MSA.3).

The TOE also ensures that management traffic is only allowed from authorised IP Addresses using explicitly approved network protocols. Only users acting in the Administrator role are allowed to modify the firewall rules for allowed and disallowed protocols (FMT_MSA.1). If a protocol is not explicitly declared allowed, it is by default not allowed (FMT_MSA.1).

These characteristcs ensure that the seleceted Security Functional Requirements fully enforce O.MANAGEMENT.

O.TAMPERING concerns with the TOE ensuring that any physical or logical tampering with the TOE hardware or firmware is detected. For the detection of physical tampering, the TOE hardware is equipped with tamper evident seals during the manufacturing which allow the users of the TOE to visually detected any attempted physical tampering (FPT_PHP.1). The TOE firmware also implements a set of self-tests to test the critical TOE functions and data (FPT_TST.1) and fail safety measures which trigger a secure state if any of the self-tests fails (FPT_FLS.1). Jointly these measures ensure that O.TAMPERING is fully enforced by the selected Security Functional Requirements.

7.3.3 Justification for the Security Assurance Requirements

The Security Assurance Requirements selected for the TOE constitute a well-defined evaluation assurance package EAL2 augmented with ALC_FLR.1 (Basic Flaw Remediation) and as such, are an internally consistent set of security assurance requirements. The augmentation is deemed relevant and necessary as it is plausible that from time to time the developer is required to issue bug fixes which shall be updated on the firmware running on the TOE hardware. To ensure that replacement of the entire appliances is not required, the developer has chosen to implement a mechanism to update the TOE firmware using the basic flaw remediation mechanism.

8 TOE Summary Specification

This section provides a high level descriptions of the security functions and security mechanisms implemented by the TOE.

SFR	Description of the implementation
FAU_GEN.1 FAU_SAR.1	The TOE implements a function to generate and store audit records to allow administrators to examine the operation of the TOE and, when required, examine the causes of possible security incidents. The audit function operates without intervention from the user and an audit record is generated and stored for the following events: a) Start-up and shutdown of the audit functions; b) Alarm Rise: This event is generated when a new alarm is detected; c) Alarm Clear: This event is generated when an alarm is cleared; d) Link Up: This is generated when the operational status of a port is changed from Down to Up; e) Link Down: This is generated when the operational status of a port is changed from Up to Down; f) Cold Restart: This is generated after a cold restart of the node; g) Warm Restart: This is generated after a warm restart of the node; h) Test Status Changed: This event is generated when the loopback or PRBS test status of a port is changed; i) Inventory Change: This event is generated when the node inventory is changed; j) Unsolicited Event: This event is generated when an exceptional incident occurs; and k) Configuration Change: This event is generated when the node configuration is changed. When an audit record is generated, the TOE requests a time stamp which it attaches to the audit record prior to storing it. Each audit record is also stored with and identification of the type of event, when available the identity of the subject triggering the action from which the audit record is generated, and when applicable the success or failure of the event triggering the generation of the audit record. Authorised users of the TOE are allowed to read the audit records and the TOE ensures that the records are kept in a matter which allows the reading and analysis by authorised users.
FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1/FW FCS_COP.1/HW	The TOE implements a rich set of cryptographic functionality implemented in hardware and in firmware. TOE hardware provides the high speed AES implementation and the firmware implements the mechanisms for key management, public key cryptography, has function computation and keyed HMAC computations. The primary function of the cryptography is to encrypt the link or a specific service between two instances of a TOE but cryptographic functions are also used for providing the trusted channels and trusted paths between the TOE and remote IT devices and between the TOE and remote users. The cryptographic functionality covers the whole life-cycle of cryptographic keys and implements the algorithms for the encryption of the link or the selected services between two instances of a TOE and between the TOE and remote IT products (see FTP_TRP.1). The cryptographic functions of the TOE are identical to the appliance with firmware v1.3.12 which constitutes a FIPS 140-2 cryptographic module validated to Level 2 with Certificate number #3529.

Each relevant cryptographic algorithm of the FIPS 140-2 certified appliance has also been certified under the Cryptographic Algorithm validation Program (CAVP) with relevant certificate numbers as below.

Key generation

The TOE implements an entropy-generating NDRNG which is consistent with Scenario 1 (a) described in FIPS 140-2 IG 7.14. The key generation function performs a CRNGT on the entropy input it receives. The TOE firmware requests 512-bits from the entropy buffer (which is filled by the NDRNG). The firmware uses 384 bits as seed for the CTR_DRBG. The 384-bits used to seed the DRBG will contain ~307-bits of actual entropy which is more than 256-bits of entropy required for the CTR_DRBG, per NIST SP 800-90A.

In accordance with FIPS 140-2 IG D.12, the TOE generates cryptographic keys in accordance with SP 800-133. The resulting generated symmetric keys are the unmodified output from the SP 800-90A DRBG.

The key generation functions used by in the key generation by the TOE and the CACP certificate numbers of the corresponding FIPS 140-2 certified appliance are the following:

CAVP Cert	Alg.	Key size(s)	Standard(s)	Mode	Use
C416	DRBG	256 bits	SP 800-90Arev1	AES CTR_DRBG	Random bit generation
N/A	CKG	N/A	SP800-133	N/A	Key generation

Key distribution

The key distribution mechanisms implemented by the TOE consist of mechanisms for key derivation, key transport and key agreement. The key distribution mechanisms implemented by the TOE and the CAVP certificate numbers of the corresponding FIPS 140-2 certified appliance are the following:

CAVP Cert	Alg.	Key size(s)	Standard(s)	Mode	Use
C416	CVL	SHA-1, SHA- 256, SHA-384, SHA-512	SP 800-135	TLS, SSH KDF	Key derivation
C416	CVL	Partial Public Key Validation	SP 800-56A	ECC CDH Component Testing	Key agreement
C416	KTS	128 bits, 192 bits, 256 bits	IG D.9	KTS (AES GCM)	Key Transport key establishment

C416	CVL	FFC: P = 2048, q = 256; ECC: P-256, P- 384, P-521	SP 800-56A	FFC DH Ephemeral, ECC Ephemeral Unified	Key agreement

Key destruction

The TOE implements a function to zeroize the keys which are no longer used. Depending on the types of the keys, the zeroization may occur by an authorised user executing a zeroization command, by a user terminating a session, or by the TOE being powered off. In each case, the zeroization ensures that the non-persistent keys stored in the memories of the TOE are erased and can not be recovered and reused.

Firmware cryptography

The TOE implements in firmware the following cryptographic mechanisms identical to those included in the FIPS 140-2 certified appliance as indicated by the relevant CAVP certificate number:

CAVP Cert	Alg.	Key size(s)	Standard(s)	Mode	Use
C416	HMAC	160 bits, 256 bits, 384 bits, 512 bits	FIPS PUB 198	SHA-1, SHA-256, SHA-384, SHA-512	Message authentication
C416	SHS	SHA-1, SHA- 256, SHA-384, SHA-512	FIPS PUB 180-4	SHA-1, SHA-256, SHA-384, SHA-512	Message digest generation
C416	RSA	2048, 3072 (Key Generation Only)	FIPS PUB 186-4	Key Generation, Signature Generation9.31, Signature Verification9.31, Signature Generation PKCS1.5, Signature Verification PKCS1.5, Signature Generation PSS, Signature Verification PSS	Key Generation, Signature Generation, Signature Verification

Hardware cryptography

<table>
<tr><td></td><td>The TOE implements in hardware 256-bit AES which is used for establishing keys and for encryption and decryption of the communication between two instances of the TOE.
The details of the cryptographic functions and the corresponding CAVP certificate numbers of the respective FIPS 140-2 certified appliance for the cryptographic hardware of the TOE are the following:
<table>
<tr><th>CAVP Cert</th><th>Alg.</th><th>Key size(s)</th><th>Standard(s)</th><th>Mode</th><th>Use</th></tr>
<tr><td>C221</td><td>AES</td><td>256 bits</td><td>SP 800-38A, FIPS 197, SP 800-38D</td><td>ECB, GCM, CTR</td><td>Link, service and message encryption, decryption, authentication</td></tr>
<tr><td>C221</td><td>KTS</td><td>256 bits</td><td>IG D.9</td><td>KTS (AES GCM)</td><td>Key transport</td></tr>
</table></td></tr>
<tr><td>FDP_ACC.1
FDP_ACF.1
FMT_MSA.3</td><td>For each role within the TOE (see FMT_SMR.1) and for each function of the TOE (see FMT_SMF.1), the TOE implements a mechanism to ensure that only users acting in an authorised role are granted access to the specific function.
Once a user is successfully authenticated the TOE assigns that user to a role. From here on, each access request of that user is verified against the access control rules of the TOE based on the role of the user and the function to which access is requested. Only if the access is allowed to the role in which the user is operating the TOE shall the access be granted. Otherwise, the TOE prevents the access from occurring.
For each function, the access control rules are hard coded into the firmware and no user is allowed to modify them. The TOE restricts the defaut access rights, i.e. if the authentication and role assignment fails or is not executed, no access rights are granted for functions other than executing the start-up self-tests (see FIA_UID.1 and FIA_UAU.1).</td></tr>
<tr><td>FDP_IFC.2
FDP_IFF.1
FMT_MSA.1
FMT_MSA.3</td><td>The TOE implements a firewall which controls access to the remote management functions by only allowing TOE to be accessed by specific protocols (FDP_IFC.1, FDP_IFF.1). All incoming traffic is subject to the firewall traffic filtering rules and the traffic is only allowed if explicitly declared allowed. Otherwise, the traffic is dropped.
By default, all traffic is disallowed (FMT_MSA.3) but can be modified by users acting in the role of Administrator (FMT_MSA.1) to allow specific protocols to be used to access the TOE.</td></tr>
<tr><td>FIA_ATD.1
FIA_UAU.1
FIA_UID.1</td><td>The TOE implements access control mechanism to ensure that only authentic users acting in legitimate and authorised roles are allowed to access services. Users are identified using a username and authenticated using a password. Upon successful identification and authentication, users are assigned to roles used for controlling the access to TOE functions. The TOE stores <username, password> pairs for each user persistently and performs the role assignment for each user session while the session is activate.
However, the access control function is only available once the TOE is successfully booted up and the boot sequence itself implements a number of self-tests to ensure that the TOE boots into a secure state. Consequently, the identification, authentication and access control rules can not apply to the execution of the start-up self-tests and therefore any user may execute the start-up self-tests by booting up the TOE.</td></tr>
<tr><td>FIA_UAU.6
FTA_SSL.3
FTA_SSL.4</td><td>The Admin role is authorised to manage the account settings and define the maximum session lengths for users. If the maximum session length is configured the TOE monitors the length of a session and if the time limit is reached, requires a re-authentication of that user prior to allowing continuation of the session.</td></tr>
</table>

	Each user is also allowed to terminate his/her session with the TOE using the applicable command from the interface he/she is using for accessing the TOE.
FIA_UAU.7	While a user is authenticated to the user locally (i.e. via the command line interface), the password is not displayed in a readable format when entered to the TOE.
FIA_SOS.1	The TOE allows users to select their own passwords. When doing this, the TOE examines the password candidate prior to accepting it to ensure it meets the minimum requirements for strength: each password must be a string of at least 8 bytes in length and must be no longer than 20 bytes. Depending on the character encoding the TOE is configured to use the number of bytes translates to a variable number of characters. Any password candidate not meeting these requirements is rejected and the TOE re-requests the user to enter the password.
FMT_SMF.1	The TOE implements a set of management functions available to users acting in different roles (see FDP_ACC.1, FDP_ACF.1). These management functions are well defined and can only be accessed through the GUI. This ensures that they are the only way of accessing the management functions of the TOE and that only legitimate users are granted access to the management functins. The access rights of roles to management functions are hard coded in the TOE firmware and can not be modified by any user.
FMT_SMR.1	The TOE has four predefined set of roles: Administrator (Admin), Crypto-Officer (CO), Read- Write and Read-Only. These roles are hard coded into the firmware and new roles can not be added. However, there can be 21 unique Crypto-Officer users. This allows assignment of a different CO for each service of the TOE. Once authenticated, each user is assigned to a role for the duration of the session. All access control decisions are made based on the role in which the user requesting for a service acts.
FPT_PHP.1	At the manufacturing the TOE, tamper evident seals are placed in the casing. These seals can be inspected by the users of the TOE to ensure that they are intact and to take the necessary action if the seals are not intact.
FPT_STM.1	The TOE maintains an internal clock from which various other functions may request time stamps.
FPT_TEE.1	The TOE measures the Optical Power of the uplink port(s) every 15 minutes and saves the reading in the corresponding performance management intervals. It there is a drop of more than 2dB between two consecutive measurements, a “Power Level Event” event is generated and recorded. The drop may be indicative of a physical tapping of the optic link between two instances of the TOE in which case the warns the user of the possibility.
FPT_FLS.1 FPT_TST.1	The TOE implements three types of self-tests: power-on self-tests, conditional self-tests, and critical function tests. if any of the self tests fails, the TOE will return an error code and transition to an error state where no functions can be executed. An operator can attempt to reset the state by cycling the power. However, the failure of a self-test may require the module to be replaced. Power-on self-tests are executed automatically at the start-up of the TOE when they do not require intervention of the user. Alternatively, they can be triggered by the user by requesting transition to a FIPS mode. These consist of two types of tests: a) HMAC-SHA-384 keyed hash integrity test on the module firmware, and b) Known Answer Tests (KAT) on the hardware and firmware cryptographic functions: a. Hardware AES ECB KAT (Encryption and Decryption. Size 256) b. Hardware AES GCM KAT (Encryption and Decryption. Size 256) c. Firmware SHS KAT (SHA-1, SHA-256, SHA-384 and SHA-512)

	d. Firmware HMAC KAT (HMAC-SHA-384) e. Firmware AES ECB KAT (Encryption and Decryption. Size 256) f. Firmware AES GCM KAT (Encryption and Decryption. Size 256) g. Firmware SP 800-90A CTR_DRBG KAT h. Firmware RSA (Sign and Verify. Size 2048) i. Firmware Diffie-Hellman Primitive "Z" Computation KAT j. Firmware EC Diffie-Hellman Primitive “Z” Computation KAT Conditional self-tests are executed by the TOE without intervention of the user to test critical functions of the TOE prior to execution of critical functions. These consist of the following tests: a) CRNGT on NDRNG: Continuous RNG test (CRNGT) performed on entropy input from the TRNG b) CRNGT on the DRBG: Continuous RNG test (CRNGT) for the SP800-90A DRBG c) DRBG Health Tests: Performed on DRBG, per SP 800-90A Section 11.3. Required per IG W.3. d) Pairwise Consistency Test: RSA Key Generation e) Bypass Test: SHA-384 hash on service table f) Firmware Load Test: HMAC-SHA-384 based integrity test to verify firmware to be loaded into the module Critical function tests execute at the start-up of the TOE or during operation of it: a) Hardware TRNG Health checks: The hardware-based entropy source performs health checking functions prior to providing output. b) DRBG Health Tests: Performed on DRBG, per SP 800-90A Section 11.3. Required per IG W.3.
FTP_TRP.1	There are three ways by which the TOE may be operated by human users: a) Local operation over a Command Line Interface from a console connected to the TOE over a serial port, b) Remote operation over a Command Line Interface through a workstation connected to the TOE over a SSHv2 connection, and c) Web user interface over a management workstation connected to the TOE over a TLS/HTTPS connection. Options (b) and (c) are considered non-local and for the purposes of the evaluation constitute the two types of trusted paths to the TOE. In both cases, the TOE is operated by a human user over a remote workstation. The TOE allows the user to establish a SSH connection between the remote workstation of the user and the TOE to execute commands on the TOE over the Command Line Interface. The parameters used in the SSH connection are the following: a) Operator Passwords which are used for authentication of the user (and subsequently for being assigned to a pre-defined role). The password is a string in the minimum of 8 bytes (64 bits) and in the maximum 20 bytes (160 bits) long. The password is selected by the user and is inputed to the TOE over the established SSH connection. The password is stored in the TOE non-volatile Flash memory in hashed plaintext format. It can be zeroized by factory reset or by issuing a zeroization command. b) Diffie-Hellman (DH) key pair with a private component of 160-512 bits and public component of 2048 bits used for negotiating TLS/HTTPS and SSH sessions. The key pair is generated internally using the SP 800-90A CTR_DRBG and the private component never exits the module. The public component of the peer entity is received from an external party. Both

components are stored in plaintext in volatile memory. They are destroyed when a session is terminated or the TOE powered off.

c) Elliptic Curve Diffie-Hellman (ECDH) Key Pair with the EC DH private component of 384 bits and the EC DH public key being in P-256, P-384 or P-521 used for negotiating TLS/HTTPS or SSH sessions. The key pair is generated internally using the SP 800-90A CTR_DRBG and the private component never exits the module. The public component of the peer entity is received from an external party. Both components are stored in plaintext in volatile memory. They are destroyed when a session is terminated or the TOE powered off.

d) SSH Host Key Pair (2048-bit RSA) used for SSH authentication. It is generated internally when the TOE powers up using a FIPS-Approved DRBG. The private component never leaves the module and the two components are stored in plaintext in the non-volatile Flash memory of the TOE. The host key pair can be zeroized by issuing a zeroization command.

e) SSH Session Encryption Key 128, 192 or 256 bit AES key in CBC or CTR mode) used for Encrypting SSH messages. They key is generated internally to the TOE using a FIPS-Approved DRBG. It is stored in plaintext in the volatile memory of the TOE. It is zeroized when a session is terminated or the TOE pwered down.

f) SSH Session Authentication key (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 or HMAC-SHA-512) used for data authentication for SSH sessions. The key is derived using SP800-135 KDF and is stored in plaintext in the volatile memory of the TOE. It is zeroized when a session is terminated or the TOE pwered down.

The TOE also allows administration over a Web UI when connecting over HTTPS. The remote user may establish a HTTPS connection with the TOE and operate the TOE over that connection. The TOE configuration backup may also be exported over the HTTPS connection for storage.

The AES-GCM implemention of the TOE FW conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module is compatible with TLS v1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The counter portion of the IV is set by the TOE. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the TOE loses power, a new key for use with the AES GCM encryption/decryption shall be established when the power is restored.

The following security parameters govern the HTTPS:

a) Operator Passwords which are used for authentication of the user (and subsequently for being assigned to a pre-defined role). The password is a string in the minimum of 8 bytes (64 bits) and in the maximum 20 bytes (160 bits) long. The password is selected by the user and is inputed to the TOE over the established SSH connection. The password is stored in the TOE non-volatile Flash memory in hashed plaintext format. It can be zeroized by factory reset or by issuing a zeroization command.

b) Diffie-Hellman (DH) key pair with a private component of 160-512 bits and public component of 2048 bits used for negotiating TLS/HTTPS and SSH sessions. The key pair is generated internally using the SP 800-90A CTR_DRBG and the private component never exits the module. The public component of the peer entity is received from an external party. Both components are stored in plaintext in volatile memory. They are destroyed when a session is terminated or the TOE powered off.

	c) Elliptic Curve Diffie-Hellman (ECDH) Key Pair with the EC DH private component of 384 bits and the EC DH public key being in P-256, P-384 or P-5221 used for negotiating TLS/HTTPS or SSH sessions. The key pair is generated internally using the SP 800-90A CTR_DRBG and the private component never exits the module. The public component of the peer entity is received from an external party. Both components are stored in plaintext in volatile memory. They are destroyed when a session is terminated or the TOE powered off. d) TLS Premaster Secret, a 384-bit string used for establishing the TLS Master Secret. The string is generated internally with the SP 800-90A CTR_DRBG and stored in plaintext in the volatile memory of the TOE. The TLS Premaster Secret is zeroized when the session is terminated or the TOE is powered down. e) TLS Master Secret is a 384-bit string used for establishing the TLS session key. It is derived from the TLS Pre-Master Secret and stored in plaintext in the volatile memory of the TOE. The TLS Master Secret is zeroized when the session is terminated or the TOE is powered down. f) TLS Session Key, a 128 bit or 256 bit AES key used in CBC, CTR or GCM mode for encrypting and decrypting TLS messages. The TLS Session Key is generated by the TOE via NIST SP 800-135 TLS 1.2 KDF during session negotiation and is stored as plaintext in the volatile memory of the TOE. It is zeroized when the session is terminated or the TOE is powered down. g) TLS Authentication Key is a HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 or HMAC-SHA-512 key used for authenticating TLS messages. It is generated by the TOE during a TLS session negotation and stored in plaintext in the volatile memory of the TOE. It is zeroized when the session is terminated or the TOE is powered down.