Cisco Optical Networking Solution

Security Target

Version 1.0

August 11, 2014

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

List of Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
CTC	Cisco Transport Controller
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
DWDM	Dense Wavelength-Division Multiplexing
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ISDN	Integrated Services Digital Network
IT	Information Technology
MSTP	Multiservice Transport Platform
NDPP	Network Device Protection Profile
OEO	Optical-electrical-optical (conversion of data)
ONS	Optical Network Solution
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
HTTPS	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TDM	Time-Division Multiplexing
TOE	Target of Evaluation
TNC	Transport Node Controller
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Optical Networking Solution (ONS). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 2 ST and TOE Identification

Name	Description
ST Title	Cisco Optical Networking Solution Security Target
ST Version	1.0
Publication Date	August 11, 2014
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Optical Networking Solution
TOE Hardware Models	Cisco ONS 15454-M2-SA, ONS 15454-M6-SA
TOE Software Version	ONS 9.8.1.2
Keywords	Optical, Data Protection, Authentication, Networking

1.2 TOE Overview

The Cisco Optical Networking Solution (ONS) TOE is the Multiservice Transport Platform (MSTP) that provides dense wavelength-division multiplexing (DWDM) and time-division multiplexing (TDM) solutions.

The Optical Encryption Line Card provides the secure transport capability of the TOE. The card provides data confidentiality and data integrity over a fiber optic communication channel through the combination of cryptography and product architecture.

The services include service transparency, flexible topology, completely reconfigurable traffic pattern, and simplified operations. The platform supports a variety of modules to enable wide deployment scenarios including access, metro, regional, and ultra-long-haul networks. The traditional transport services such as Ethernet and IP are also supported by the TOE. The TOE includes the hardware models as defined in Table 2 in section 1.1.

The Cisco Transport Controller (CTC) is a GUI-based application used to configure and manage ONS 15454 MSTP systems, including the optical encryption card. It offers these features:

- User management: Role-based access control and complete separation of privileges between users from the transport domain and those from the security domain
- Key management: Key generation and key change interval
- Cryptographic lifecycle management: The card-to-card authentication and card authorization between two encryption cards that must succeed prior to key exchange
- Performance management: Alarms to detect an active or a passive intrusion, as well as the failure of any security function

1.2.1 TOE Product Type

The Cisco ONS 15454 MSTPs solution offers the choice of multiservice aggregation, wavelength aggregation, and wavelength transport, combined with integrated, intelligent DWDM transmission in a single platform to minimize network costs for any mix of service types.

The Cisco ONS 15454 MSTPs supports direct interconnection with DWDM interfaces from Layer 2, Layer 3, and SAN devices. This element integration eliminates the need for costly and complex Optical-Electrical-Optical (OEO) conversions at the boundaries of the network or where the traffic simply needs to pass through a site without having to terminate on an upper-layer device. The Optical Encryption Line Card offers six different modes of operation that can be applied independently on each client-trunk pair: Encryption and Authentication, Encryption only, Authentication only, Unencrypted (normal) transponder, Ultra Low Latency transponder, and OEO regenerator.

The management workstation that runs the CTC software and is used to manage ONS can be directly connected or via Local Area Network (LAN) connection. The connection is secured using HTTPS. The CTC management window appears after successful login. The management window includes a menu bar, toolbar, and a top and bottom pane. The top pane displays status information about the selected objects and a graphic of the current view. The bottom pane displays tabs and subtabs, which are used to view ONS 15454 information and perform ONS 15454 provisioning and maintenance. From this window the display can be set to display three ONS 15454 views:

- Network - allows you to view and manage ONS 15454s that have Data Communications Channel (DCC) connections to the node that you logged into and any login node groups you may have selected. DCC connections can be green (active) or gray (fail). The lines can also be solid (circuits can be routed through this link) or dashed (circuits cannot be routed through this link).
- Node - is the first view displayed after you log into an ONS 15454. The login node is the first node displayed, and it is the "home view" for the session. Node view allows you to view and manage one ONS 15454 node. The status area shows the node name; IP address; session boot date and time; number of critical (CR), major (MJ), and minor (MN) alarms; the name of the current logged-in user; and security level of the user.
- Card - displays information about individual ONS 15454 cards. Use this window to perform card-specific maintenance and provisioning. A graphic showing the ports on the card is shown in the graphic area. The status area displays the node name, slot, number of alarms, card type, equipment type, and the card status (active or standby), card state or

port state. The information that is displayed and the actions you can perform depend on the card.

The ONS 15454 generates and stores a human-readable audit trail of all system actions, such as circuit creation or deletion, and security events such as login and log outs. The administrator can access the log by clicking the Maintenance > Audit tabs. The ONS 15454 has a log capacity of 640 entries; when this limit is reached, the oldest entries are overwritten with new events. When the log is 80% full, an AUD-LOG-LOW condition is raised. When the log is full and entries are being overwritten, an AUD-LOG-LOSS condition occurs. The administrator can also archive this log in text form to a syslog server.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS or TACACS+ AAA Server	No	If configured, this includes any authentication server (RADIUS RFC 2865, 2866, 2869 and RFC 3162 (IPv6) and TACACS+ RFC 1492)) that can be leveraged for remote user authentication.
Management Workstation	Yes	This includes any IT Environment Management workstation installed with Cisco Transport Controller (CTC), the software interface for Cisco ONS 15454, Cisco ONS 15454 M2, and Cisco ONS 15454 M6 that is used by the TOE administrator to support TOE administration through HTTPS protected channels.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.
NTP Server	No	If configured, this includes time synchronization with an NTP server.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Optical Networking Solution (ONS) Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following:

- Chassis:
  - 15454-M2-SA
  - 15454-M6-SA
- Controller Cards:
  - 15454-M-TNC-K9
  - 15454-M-TSC-K9
  - 15454-M-TNCE-K9
  - 15454-M-TSCE-K9
- Encryption Card:
  - 15454-M-WSE-K9

The front door of the ONS 15454 allows access to the shelf assembly, fan-tray assembly, and cable-management area. From the front door, the Critical, Major, and Minor alarm LEDs are visible that indicate whether a critical, major, or minor alarm is present anywhere on the ONS

15454. These LEDs must be visible so technicians can quickly determine if any alarms are present on the ONS 15454 shelf or the network.

The backplanes provide access to alarm contacts, external interface contacts, power terminals, and BNC[1]/SMB[2] connectors. The lower section of the ONS 15454 backplane is covered by a clear plastic protector cover to protect access to the alarm interface panel (AIP), alarm pin fields, frame ground, and power terminals. The ONS 15454 also has an optional clear plastic rear cover. This clear plastic cover provides additional protection for the cables and connectors on the backplane.

The card slot requirement for each card is marked with a symbol that corresponds to a slot (or slots) on the ONS 15454 shelf assembly. The cards are then installed into slots displaying the same symbols. For example:

Symbol Color/Shape Definition

Orange/Circle
Slots 1 to 6 and 12 to 17. Only install cards with a circle symbol on the faceplate.

Blue/Triangle
Slots 5, 6, 12, and 13. Only install cards with circle or a triangle symbol on the faceplate.

Purple/Square
TCC2/TCC2P/TCC3 slot, Slots 7 and 11. Only install cards with a square symbol on the faceplate.

Green/Cross
Cross-connect (XC/XCVT/XC10G) slot, Slots 8 and 10. Only install ONS 15454 cards with a cross symbol on the faceplate. Note Cross-connect cards are not required in DWDM applications. Install a FILLER card or blank card if not using Slots 8 and 10.

The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release 9.8.1.2. The TOE is managed using the Cisco Transport Controller (CTC) software that is installed on the Management Workstation during the setup and installation of the TOE. The CTC is a web-based graphical user interface (GUI) application capable of managing all of the security functions, as well as performing the provisioning and administration functions of the Controller Card.

The Cisco ONS 15454 MSTPs provide features such as multilayer graphical network, node, and card visibility; comprehensive network-based service provisioning; and graphical software wizards to simplify and speed user operations for such tasks as initial network turn-up, service

[1] BNC connector (Bayonet Neill–Concelman) is a miniature quick connect/disconnect RF connector used for coaxial cable. A RF connector is an electrical connector designed to work at radio frequencies in the multi-megahertz range.

[2] SMB (SubMiniature version B) connectors are coaxial RF connectors developed in the 1960s. SMB connectors are smaller than SMA connectors. SMA connectors are semi-precision coaxial RF connectors developed in the 1960s as a minimal connector interface for coaxial cable with a screw type coupling mechanism.

provisioning, and network, node, and bandwidth upgrades. The Cisco ONS 15454 MSTPs use the embedded software architecture and control plane to introduce a level of operational simplicity exceptional in DWDM networks.

The Cisco ONS 15454 MSTPs deliver a comprehensive set of features, allowing customers worldwide to support the requirements of next-generation transport networks.

The Optical Networking Solution primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation.

The CTC software is preloaded on the ONS 15454 cards. CTC is downloaded to the management workstation during the configuration and of the ONS 15454. Although the CTC software performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

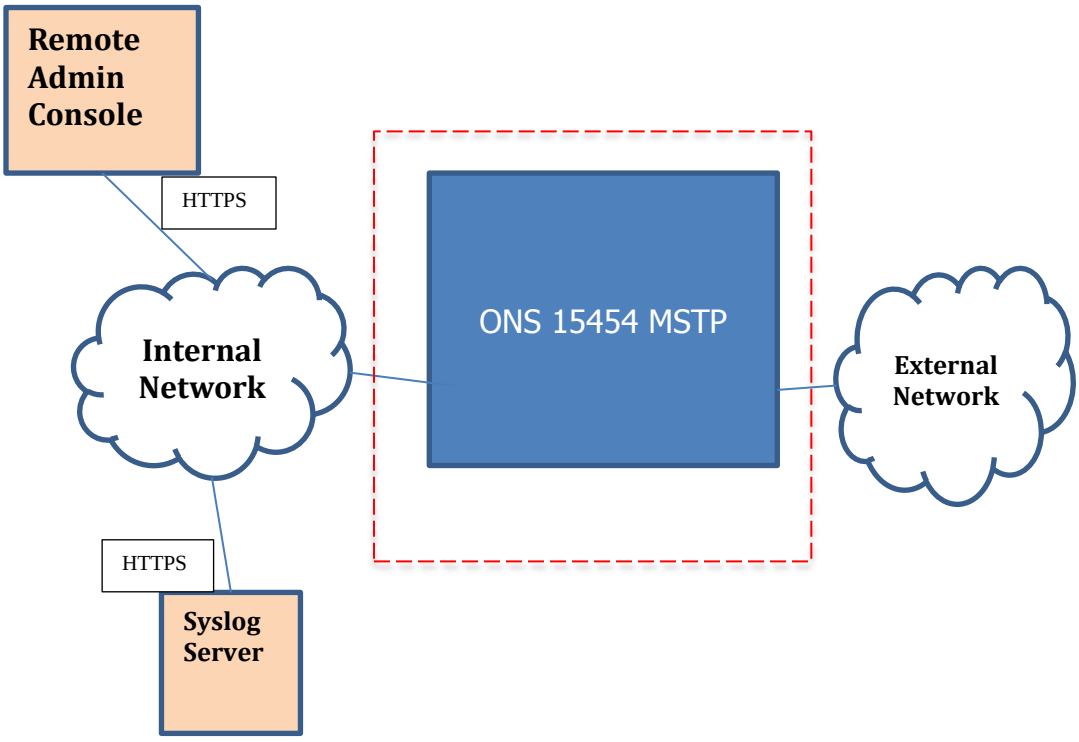


Figure 1 TOE Example Deployment

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco CTC software.

The Cisco Transport Node Controller (TNC) and Transport Shelf Controller (TSC) and the enhanced versions (TNCE and TSCE, respectively) are next-generation system processors for the Cisco ONS 15454-M6-SA and ONS 15454-M2-SA Multiservice Transport Platforms (MSTPs). The Cisco TNC, TNCE, TSC, and TSCE cards perform system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection and resolution, SONET and SDH data-communications-channel (DCC) termination, system DC input-voltage monitoring, and system fault detection, and they support multishelf connections. The TNC and TNCE cards also have two optical service channels that support a supervisory data channel (SDC), distribution of synchronous clocking, and a 100-Mbps user data channel (UDC). The enhanced versions, TNCE and TSCE, support the IEEE1588v2 Precision Timing Protocol (PTP) and time of day (ToD) with pulse per second (PPS), in addition to support for Synchronous Ethernet (SyncE)/Source Specific Multicast (SSM) and traditional Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) Building Integrated Timing Supply (BITS) timing, which the TNC and TSC also support.

Figure 2 Cisco ONS 15454 TNC Card and ONS 15454 TSC Card

The Cisco ONS 15454 10G Optical Encryption Card brings secure transport capability to the ONS 15454 MSTP product family by providing data confidentiality and data integrity over a fiber optic communication channel through the combination of Cryptography and Trusted Product Architecture. Each SFP+ (enhanced small form-factor pluggable) port can accept gray or DWDM pluggable optics, with trunk ports supporting G.709 Digital Wrapper for carrier class OAM, plus Forward Error Correction (FEC) for longer reach. The single slot card is compatible with the ONS 15454 MSTP M6 and M2 chassis, allowing up to 30 encrypted 10G streams in a 6RU footprint.

Figure 3 Optical Encryption Line Card

The Cisco ONS 15454 provisioning and administration is performed using the CTC software. CTC is a Java application that is downloaded to the management workstation the first log onto the ONS 15454. If the TOE is remotely administered, HTTPS as defined herein, must be used to secure the connections.

Figure 4 Node View (Default Login View for Single-Shelf Mode)

In the evaluated configuration, the TOE will also transmit audit logs to a remote syslog server via HTTPS secure connection.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the ONS 15454 MSTPs as follows:

1.5.1 Evaluated Configuration

The validated platforms consist of the following components:

- Chassis (one or more):
  - 15454-M2-SA
  - 15454-M6-SA
- Controller (Management) Cards (one or more):
  - 15454-M-TNC-K9
  - 15454-M-TSC-K9
  - 15454-M-TNCE-K9
  - 15454-M-TSCE-K9
- Encryption (Traffic Data) Card:
  - 15454-M-WSE-K9
- Software
  - ONS 9.8.1.2

The following pictures are representative each of the hardware model

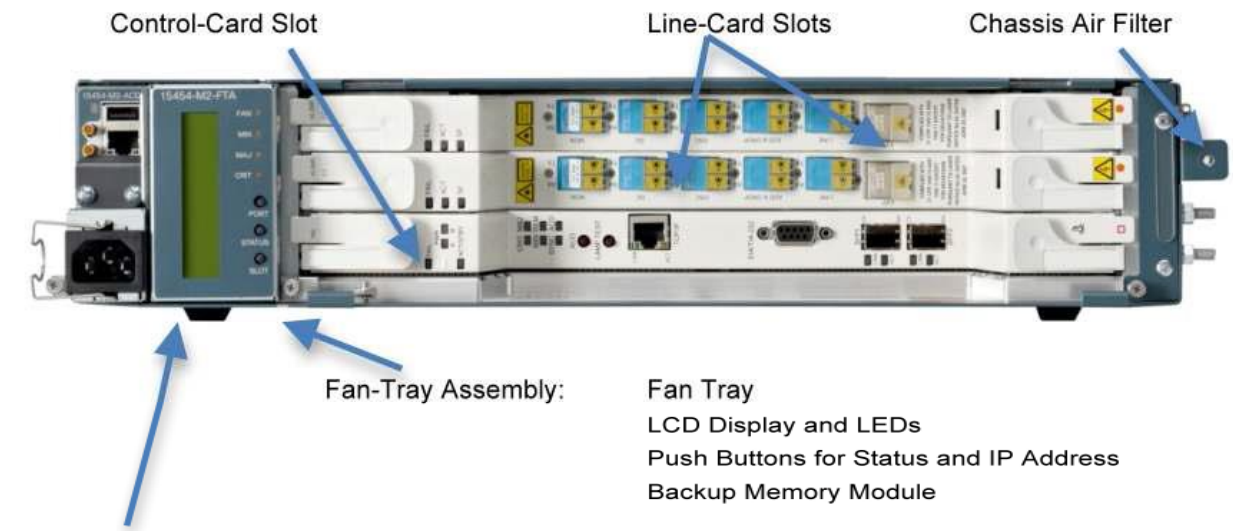


Figure 5 Cisco ONS 15454 M2 Multiservice Transport Platform (with and without covers)

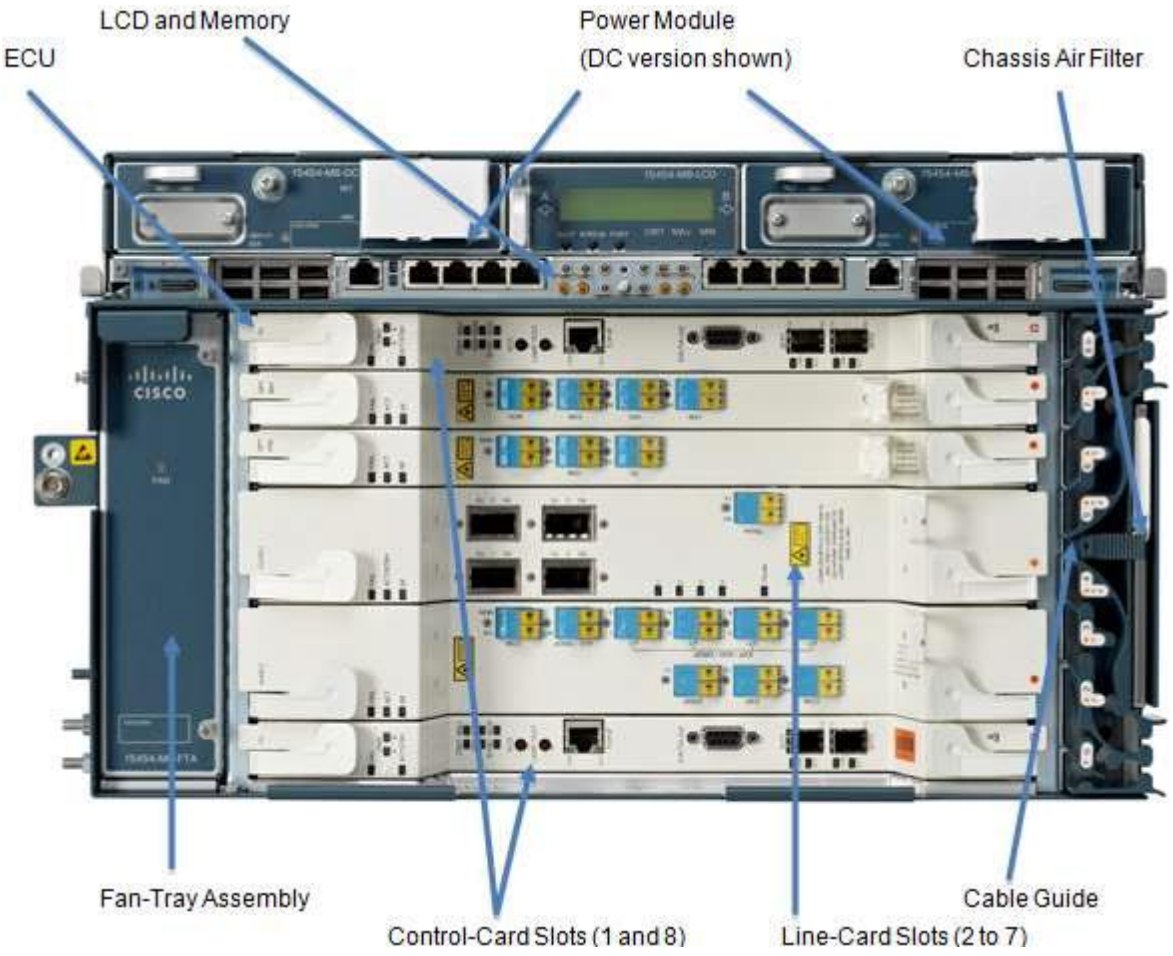


Figure 6 Cisco ONS 15454 M6 Multiservice Transport Platform (with and without front cover)

Table 4 FIPS References

Chassis	Controller Cards	Encryption Card
15454-M2-SA	**Single** 15454-M-TNC-K9	**Up to two (2)** 15454-M-WSE-K9
	Single 15454-M-TSC-K9	**Up to two (2)** 15454-M-WSE-K9
	Single 15454-M-TNCE-K9	**Up to two (2)** 15454-M-WSE-K9
	Single 15454-M-TSCE-K9	**Up to two (2)** 15454-M-WSE-K9
15454-M6-SA	**Single** 15454-M-TNC-K9	**Up to six (6)** 15454-M-WSE-K9
	Single 15454-M-TSC-K9	**Up to six (6)** 15454-M-WSE-K9

Chassis	Controller Cards	Encryption Card
	Single 15454-M-TNCE-K9	**Up to six (6)** 15454-M-WSE-K9
	Single 15454-M-TSCE-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TNC-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TSC-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TNCE-K9	**Up to six (6)** 15454-M-WSE-K9
	Dual 15454-M-TSCE-K9	**Up to six (6)** 15454-M-WSE-K9

1.6 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Full Residual Information Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDPP v1.1 as necessary to satisfy the assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco Optical Networking Solution provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Optical Networking Solution generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. Auditing is always on to audit all events and therefore the administrator is only coupled with the management of the audit data storage and archive of the log files. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are archived over secure HTTPS/TLS connection to an external audit server.

1.6.2 Cryptographic Support

ONS is a FIPS validated product.

The TOE also provides cryptography in support of other Cisco ONS security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 (see Table 5 for certificate references).

Table 5 FIPS References

Algorithm	ONS Controller (Management) Card Cert. #	ONS Encryption (Traffic) Card Cert. #
AES	2886	2887
Triple-DES	1721	N/A
SHS	2427	2428
HMAC	1820	1821
RSA	1526	1527
DRBG	521	522
SP 800-108 KDF	N/A	29

1.6.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

1.6.4 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters, password expiration as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database using the GUI interface accessed via secure HTTPS connection. The TOE may also be configured to support remote authentication via RADIUS or TACACS+.

1.6.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS session or via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;

- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE; and
- Update to the TOE.

Administrative users can be assigned one of the following security levels:

- Retrieve-Users can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance-Users can access only the ONS 15454 maintenance options.
- Provisioning-Users can access provisioning and maintenance options.
- Superusers-Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. Superusers can also provision security policies on the TOE. These security policies include idle user timeouts, password changes, password aging, and user lockout parameters.

Administrators can also create configurable login banners to be displayed at time of login.

1.6.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco ONS is not a general-purpose operating system and access to Cisco ONS memory space is restricted to only Cisco ONS functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. The TOE may also be configured to synchronize time with an NTP server.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

1.6.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also be configured to display an Authorized Administrator specified banner on the GUI management interface prior to accessing the TOE.

1.6.8 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over HTTPS and initiates secure HTTPS connections to transmit audit messages to remote syslog servers.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 6 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.6.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 7 below:

Table 7 Protection Profiles

Protection Profile	Version	Date
U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP); including the latest Errata#2	1.1	June 8, 2012

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile:

- U.S. Government Protection Profile for Security Requirements for Network Devices, Version 1.1

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDPPv1.1, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDPPv1.1, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements

included in this Security Target are identical to the Security Assurance Requirements included in section 4.3 of the NDPPv1.1.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 8 TOE Assumptions

Assumption	Assumption Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
A.NO_GENERAL_PURPOSE	It is assumed that 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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

The following table lists the threats addressed by the TOE and the operational Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 9 Threats

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

Threat	Threat Definition
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 10 Organizational Security Policies

Policy Name	Policy Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 SECURITY OBJECTIVES

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 11 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
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.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
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.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.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 12 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
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.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDPP itself, the formatting used in the NDPP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the NDPP.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 13 Security Functional Requirements

Class Name	Component Identification	Component Name
Security Functional Requirements Drawn from NDPP		
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_HTTPS_EXT.1	Explicit: HTTPS
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	Explicit: TLS
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection

Class Name	Component Identification	Component Name
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
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_TUD_EXT.1	Extended: Trusted Update
	FPT_TST_EXT.1	TSF Testing
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Trusted Channel
	FTP_TRP.1	Trusted Path

5.3 SFRs Drawn from NDPP

5.3.1 Security audit (FAU)

5.3.1.1 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) *All administrative actions*;
d) [*Specifically defined auditable events listed in* Table 14].

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 14].

Table 14 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
Audit Events and Details from NDPP		
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM_EXT.4	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session. Establishment/Termination of an HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	None.
FCS_TLS_EXT.1	Failure to establish an TLS session Establishment/Termination of an TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	None.
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MTD.1	None.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

5.3.1.2 FAU_GEN.2 User Identity Association

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.

5.3.1.3 FAU_STG_EXT.1 External Audit Trail Storage

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/HTTPS] protocol.

5.3.2 Cryptographic Support (FCS)

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

FCS_CKM.1.1 Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with

[

- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;
- 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.*

5.3.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

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

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 no other modes***]] and cryptographic key sizes 128-bits *and* 256-bitsthat meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[NIST SP 800-38A, NIST SP 800-38D]**

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

FCS_COP.1.1(2) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [

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

]

that meets the following:

~~**Case: Digital Signature Algorithm**~~

- ~~**FIPS PUB 186-3, "Digital Signature Standard"**~~

Case: RSA Digital Signature Algorithm

- **FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"**

~~**Case: Elliptic Curve Digital Signature Algorithm**~~

- ~~**FIPS PUB 186-3, "Digital Signature Standard"**~~
- ~~**The TSF shall implement "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard").**~~

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

FCS_COP.1.1(3) **Refinement:** The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-512] **and message digest sizes** [160, 256, 512] **bits** that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

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

FCS_COP.1.1(4) Refinement: The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm HMAC-[SHA-1, SHA-256, SHA-512], **key size** [**160, 256, 512** ***key size (in bits) used in HMAC***], **and message digest sizes** [160, 256, 512] **bits** that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*

5.3.2.7 FCS_HTTPS_EXT.1 Explicit: HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

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

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using [CTR_DRBG (AES)] seeded by an entropy source that accumulated entropy from [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.

5.3.2.9 FCS_TLS_EXT.1 Explicit: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246)] 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
].

5.3.3 User data protection (FDP)

5.3.3.1 FDP_RIP.2 Full Residual Information Protection

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.

5.3.4 Identification and authentication (FIA)

5.3.4.1 FIA_PMG_EXT.1 Password Management

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 the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [no *other characters*]];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

5.3.4.2 FIA_UIA_EXT.1 User Identification and Authentication

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;
- [no other actions].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

5.3.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [none] to perform administrative user authentication.

5.3.4.4 FIA_UAU.7 Protected Authentication Feedback

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.

5.3.5 Security management (FMT)

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

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the *TSF data* to the *Security Administrators*.

5.3.5.2 FMT_SMF.1 Specification of Management Functions

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 cryptographic functionality*].

5.3.5.3 FMT_SMR.2 Restrictions on Security Roles

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.

5.3.6 Protection of the TSF (FPT)

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

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.6.2 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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.

5.3.6.3 FPT_STM.1 Reliable time stamps

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

5.3.6.4 FPT_TST_EXT.1: TSF Testing

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.

5.3.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

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 [published hash] prior to installing those updates.

5.3.7 TOE Access (FTA)

5.3.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

lock the session - disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session

].

after a Security Administrator-specified time period of inactivity.

5.3.7.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 Refinement: The TSF shall terminate **a remote** interactive session after a [*Security Administrator-configurable time interval of session inactivity*].

5.3.7.3 FTA_SSL.4 User-initiated Termination

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

5.3.7.4 FTA_TAB.1 Default TOE Access Banners

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.

5.3.1 Trusted Path/Channels (FTP)

5.3.1.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **use [TLS/HTTPS]** to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [no other capabilities]]** 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 [*communications with the audit server using HTTPS*].

5.3.1.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** [**TLS/HTTPS**] 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.*

5.4 Extended Components Definition

This Security Target includes Security Functional Requirements (SFR) that are not drawn from existing CC Part 2. The Extended SFRs are identified by having a label '_EXT' as part of the requirement name for TOE SFRs. The structure of the extended SFRs is modelled after the SFRs included in CC Part 2. The structure is as follows:

A. Class – The extended SFRs included in this ST are part of the identified classes of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST below.

Extended Requirements Rationale:

FAU_STG_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement to export audit records outside the TOE.

FCS_CKM_EXT.4:

This SFR was taken from NDPP – where it is defined as a requirement for immediate zeroization when keys and CSPs are no longer required.

FCS_HTTPS_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement specific to HTTPS.

FCS_RBG_EXT.1:

his SFR was taken from NDPP – where it is defined as a requirement specific to random bit generation.

FCS_TLS_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement specific to TLS.

FIA_PMG_EXT.1:

This SFR was taken from NDPP – where it is defined as a requirement for specific password composition and aging constraints. Note that "Security Administrator" has been replaced with "Authorized Administrator".

FIA_UAU_EXT.2:

This SFR was taken from NDPP – where it is defined as a requirement allowing local and other authentication mechanisms.

FIA_UIA_EXT.1:	This SFR was taken from NDPP – where it is defined as a requirement combining both identification and authentication requirements.
FPT_SKP_EXT.1:	This SFR was taken from NDPP –where it is defined as a requirement specifically disallowing access to pre-shared keys, symmetric keys, and private keys.
FPT_APW_EXT.1:	This SFR was taken from NDPP – where it is defined as a requirement specifically disallowing access to passwords.
FPT_TST_EXT.1:	This SFR was taken from NDPP – where it is defined as a requirement for TSF self tests during initialization.
FPT_TUD_EXT.1:	This SFR was taken from NDPP – where it is defined as a requirement for secure TOE update capabilities. Note that "Security Administrator" has been replaced with "Authorized Administrator".
FTA_SSL_EXT.1:	This SFR was taken from NDPP – where it is defined as a requirement for behavior after local terminal session inactivity. Note that "Security Administrator" has been replaced with "Authorized Administrator".

5.5 TOE SFR Dependencies Rationale

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDPPv1.1. As such, the NDPP SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.6 Security Assurance Requirements

5.6.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDPP which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 15: Assurance Measures

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_FSP.1	Basic Functional Specification
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

5.6.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDPPv1.1. As such, the NDPP SAR rationale is deemed acceptable since the PP itself has been validated.

5.7 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 16 Assurance Measures

Component	How requirement will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behaviour of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and start-up procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-

Component	How requirement will be met
ALC_CMS.1	user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

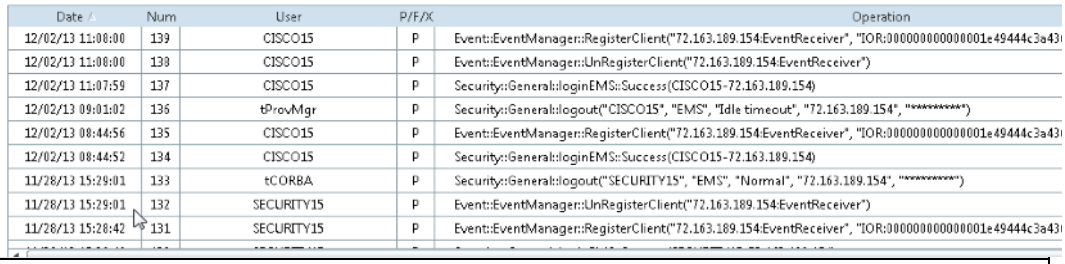
6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 17 How TOE SFRs Are Met

TOE SFRs	How the SFR is Met
Security Functional Requirements Drawn from NDPP	
FAU_GEN.1	The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 14). Each of the events is specified in the audit record in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the start-up of the audit functionality is audited. The audit function automatically starts when the TOE is booted and becomes operational. The TOE does not offer the ability to shutdown auditing as it is always in an auditing mode. However when the TOE is shutdown, a record is generated to indicate the TOE is shutting down. Audit trail records also captures the following information and activities: • User-Name of the user performing the action • Host-Host from where the activity is logged • Device ID-IP address of the device involved in the activity • Application-Name of the application involved in the activity • Task-Name of the task involved in the activity (view a dialog box, apply configuration, and so on) • Connection Mode-Telnet, Console, • Category-Type of change: Hardware, Software, Configuration • Status-Status of the user action: Read, Initial, Successful, Timeout, Failed • Time-Time of change • Message Type-Denotes whether the event is Success/Failure type • Message Details-Description of the change Example audit events are included below: 25 11/26/13 15:37:48 Event::EventManager::RegisterClient("72.163.189.154:EventReceiver", "IOR:000000000000001e49444c3a43616 1 P CISCO15 26 11/26/13 15:50:38 Security::General::loginTL1::Success(CISCO15-10.105.38.127) 0 P CISCO15 27 11/26/13 15:50:40 Security::General::logout("CISCO15", "TL1", "Normal", "10.105.38.127", "**********") 1 P tTl1Agt1 28 11/26/13 15:55:11 Event::EventManager::UnRegisterClient("72.163.189.154:EventReceiver") 1 P CISCO15 29 11/26/13 15:55:11 Security::General::logout("CISCO15", "EMS", "Normal", "72.163.189.154", "**********") 1 P tCORBA 30 11/26/13 16:26:14 Security::General::loginEMS::Success(CISCO15-72.163.189.154) 0 P CISCO15 31 11/26/13 16:26:31 Event::EventManager::RegisterClient("72.163.189.154:EventReceiver", "IOR:000000000000001e49444c3a43616 1 P CISCO15 32 11/26/13 16:30:49 Node::General::_set_name("swmanjun-M6-62") 1 P CISCO15 33 11/26/13 16:30:50 Node::General::setSntpHost(0.0.0.0, 0.0.0.0) 1 P CISCO15
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below:

TOE SFRs	How the SFR is Met
	

Date	Num	User	P/F/X	Operation
12/02/13 11:08:00	139	CISCO15	P	Event::EventManager::RegisterClient("72.163.189.154:EventReceiver", "IOR:000000000000001e49444c3a43
12/02/13 11:08:00	138	CISCO15	P	Event::EventManager::UnRegisterClient("72.163.189.154:EventReceiver")
12/02/13 11:07:59	137	CISCO15	P	Security::General::loginEMS::Success(CISCO15-72.163.189.154)
12/02/13 09:01:02	136	tProvMgr	P	Security::General::logout("CISCO15", "EMS", "Idle timeout", "72.163.189.154", "**********")
12/02/13 08:44:56	135	CISCO15	P	Event::EventManager::RegisterClient("72.163.189.154:EventReceiver", "IOR:000000000000001e49444c3a43
12/02/13 08:44:52	134	CISCO15	P	Security::General::loginEMS::Success(CISCO15-72.163.189.154)
11/28/13 15:29:01	133	tCORBA	P	Security::General::logout("SECURITY15", "EMS", "Normal", "72.163.189.154", "**********")
11/28/13 15:29:01	132	SECURITY15	P	Event::EventManager::UnRegisterClient("72.163.189.154:EventReceiver")
11/28/13 15:28:42	131	SECURITY15	P	Event::EventManager::RegisterClient("72.163.189.154:EventReceiver", "IOR:000000000000001e49444c3a43

FAU_STG_EXT.1	The TOE is able to store 640 log entries. When the log server is 80% full, an AUD-LOG-LOW condition is raised and logged. When the upper limit is reached, the oldest entries are overwritten with new events. This event indicates that audit trail records have been lost. To ensure audit records are not lost, the Administrator archives the audit records at specific internals, which are transmitted to the syslog server for storage. The TOE protects communications with an external syslog server via HTTPS. The TOE is capable of detecting when the HTTPS connection fails. The TOE is capable of storing the audit records locally on the TOE, and continues to do so if the communication with the syslog server goes down. The audit records are stored in a directory that does not allow administrators to modify the contents and only Authorized Administrators are able to archive the logs.
FCS_CKM.1	The TOE implements a FIPS-approved Deterministic Random Bit Generator for Diffie-Hellman key establishment (conformant to NIST SP 800-56A), and for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE does not implement elliptic-curve-based key establishment schemes. For Diffie-Hellman Key Establishment, the TOE implements all sections of SP 800-56A. The TOE does not perform any operation marked as “Shall Not” or “Should not” in SP 800-56A. Additionally, the TOE does not omit any operation marked as “Shall.” For RSA Key Establishment, the TOE implements the all sections of SP 800-56B. The TOE does not perform any operation marked as “Shall Not” or “Should not” in SP 800-56B. Additionally, the TOE does not omit any operation marked as “Shall.”
FCS_CKM_EXT.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form This requirement applies to the secret keys used for symmetric encryption, private keys, and CSPs used to generate keys, which are zeroized immediately after use, or on system shutdown, etc. See Section 8.1 in this ST for additional information regarding managed keys, usage, zeroization and storage location information.
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES in CBC (128, 256 bits) as described in NIST SP 800-38A and NIST SP 800-38D. Please see CAVP certificate 2886 for validation details. AES is implemented in the following protocols: HTTPS/TLS.
FCS_COP.1(2)	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-3, “Digital Signature Standard” and FIPS PUB 186-2, “Digital Signature Standard”.
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-512 as specified in FIPS Pub 180-3 “Secure Hash Standard.”
FCS_COP.1(4)	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256. HMAC-SHA-512 as specified in FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code,” and FIPS 180-3, “Secure Hash Standard.”
FCS_HTTPS_EXT.1	The TOE provides HTTPS, as specified in RFC 2818, to provide a secure interactive interface for remote administrative functions, and to support secure exchange of user authentication parameters during login. HTTPS uses TLS (as specified in FCS_TLS_EXT.1) to securely establish the encrypted remote session by certificate (key) exchange that establishes the secure

TOE SFRs	How the SFR is Met
	connection with ONS to download the executable JRE files.
FCS_TLS_EXT.1	The TOE provides TLS 1.0, conformant to RFC 2246 and supports the mandatory ciphersuites • TLS_RSA_WITH_AES_128_CBC_SHA As well as the 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 The TOE only supports standard extensions, methods, and characteristics. TLS 1.0 is used for HTTPS/TLS for management purposes and to establish encrypted sessions with IT entities to send/receive audit data. The TOE's implementation of RFC 2246 includes all of the must statements, as well as does not violate the must not statements.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. The entropy source used to seed the Deterministic Random Bit Generator (e.g. based on SP 800-90A/B/C) is a random set of bits or bytes that are regularly supplied to the DRBG from the internal on-board chip processor which produces a minimum of 256 bits of entropy This solution is available in the ONS 9.8 or later FIPS/CC approved releases of the ONS images relating to the platforms defined in 1.5 above. All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed. Though related to this, the tests are part of the FIPS validation procedures for the DBRG and are part of the NIST validations for FIPS 140-2 for the products. Any initialization or system errors during bring-up or processing of this system causes a reboot as necessary to be FIPS compliant. Finally, the system will be zeroizing any entropy seeding bytes, which will not be available after the current collection.
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from data allocated to from previous packets. Packets that are not the required length use zeros for padding. Residual data is never transmitted from the TOE. Once packet handling is completed its content is zeroized (overwritten with 0x00) before allocation to the memory buffer which previously contained the packet is reused. This process is handled by the buffer pool. The buffer space that was used by the sent packet is recalled and zerozied. When a new packet requires a buffer from the buffer pool, the new packet data is used to overwrite the buffer space. As stated above, if the packet does not require the total buffer space, the additional space is padded with zeros. This applies to both data plane traffic and administrative session traffic.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and support passwords of 15 characters or greater. Password composition rules specifying the types and number of required characters that comprise the password are settable by the Authorized Administrator.
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE's GUI. The TOE mediates all administrative actions through the GUI. Once a potential administrative user attempts to access the GUI of the TOE through either a directly connected console or remotely through an HTTPS connection, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the

TOE SFRs	How the SFR is Met
	administrative functionality of the TOE until an administrator is successfully identified and authenticated.
FIA_UAU_EXT.2	The TOE provides a local password based authentication mechanism. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via HTTPS. At initial login in the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FMT_MTD.1	The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, and security attributes. Each of the predefined and administratively configured security levels have a set of permissions that may grant them access to the TOE data, though with some security levels access is limited based on the configured privileges and policies. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged levels. For the purposes of this evaluation, users can be assigned to the following security levels and all are deemed as authorized administrators. : • Retrieve-Users can retrieve and view CTC information but cannot set or modify parameters. • Maintenance-Users can access only the ONS 15454 maintenance options. • Provisioning-Users can access provisioning and maintenance options. • Superusers-Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a security level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the GUI to perform these functions via HTTPS. The specific management capabilities available from the TOE include: • Local and remote administration of the TOE and the services provided by the TOE via the TOE GUI, as described above; • The ability to update the ONS software, and • Ability to configure the cryptographic functionality
FMT_SMR.2	The TOE platform maintains predefined and administratively configured security levels that have a set of permissions that may grant them access to the TOE data, though with some security levels access is limited based on the configured privileges and policies. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged levels. For the purposes of this evaluation, users can be assigned to the following security levels and all are deemed as authorized administrators. :

TOE SFRs	How the SFR is Met
	• Retrieve-Users can retrieve and view CTC information but cannot set or modify parameters. • Maintenance-Users can access only the ONS 15454 maintenance options. • Provisioning-Users can access provisioning and maintenance options. • Superusers-Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The security level determines the functions the user can perform; hence the Authorized Administrator with the appropriate privileges. The TOE can and shall be configured to authenticate all access to the GUI using a username and password. The TOE supports both local administration via a directly connected console cable and remote authentication via HTTPS.
FPT_SKP_EXT.1	The TOE stores all private keys in a secure directory that is not accessible to administrators via GUI page(s). All pre-shared and symmetric keys are stored in encrypted form to additionally obscure access by default. See Section 8.1 in this ST for additional information regarding managed keys, usage, zeroization and storage location information.
FPT_APW_EXT.1	The TOE ensures that plaintext user passwords will not be disclosed even to administrators. Password encryption is set by default and is not configurable. The passwords are encrypted using SHA256. See Section 8.1 in this ST for additional information regarding managed keys, usage, zeroization and storage location information.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware (i.e. a hardware clock). The hardware clock is initially set during manufacturing and can be updated to the applicable time and zone during setup and configuration at the users' organization. This date and time is also used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The TOE can optionally be set to receive clock updates from an NTP server. Instructions for how to do this are provided in the administrator guidance for this evaluation.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from the Cisco.com web site. Authorized Administrators can download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html. Digital signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The digital certificates used by the update verification mechanism are contained on the TOE. Instructions for how to do this verification are provided in the administrator guidance for this evaluation.
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, the Authorized Administrator will have to log into the GUI to determine which test failed and why. During the system bootup process (power on or reboot), all the Power on Startup Test (POST)

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:

• Encryption Card Firmware Known Answer Tests (KATs)
o AES (encrypt/decrypt) KATs
o DRBG KAT
o HMAC (HMAC-SHA-1/256/512) KATs
o RSA KAT

• Controller Card Firmware KATs
o AES (encrypt/decrypt) KATs
o DRBG KAT
o HMAC (HMAC-SHA-1/256/512) KATs
o RSA KAT
o Triple-DES (encrypt/decrypt) KATs

• Hardware (FPGA) KATs
o AES-GCM KAT
o AES-XTS KAT
• Firmware Integrity Test (32-bit CRC)

In the error state, all secure management and data transmission that is affected by the failure is halted and the module outputs status information indicating the failure. For example, if the SHA fails, the TOE will not allow any processes that use SHA to work. In an error state the Administrator may be able to log in to troubleshoot the issue.

During the POST, all ports are blocked from moving to forwarding state. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward management and data traffic. If the POST fails the TOE will continuously reboot in attempts to correct the failure. During this state no one can login, no traffic is passed, the TOE is not operational. If the problem is not corrected by the reboot, Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support.

These tests are sufficient to verify that the correct version of the TOE software is running, the TOE components are functioning as expected as well as that the cryptographic operations are all performing as expected.</td></tr>
<tr><td>FTA_SSL_EXT.1
FTA_SSL.3</td><td>An administrator can configure the idle user timeouts. Users can be idle during his or her login session for a specified amount of time before the CTC window is locked. The lockouts prevent unauthorized users from making changes. The default timeouts for the security levels are as follows, though the superuser can figure the times:

<table><tr><th>Security Level</th><th>Idle Time</th></tr><tr><td>Superuser</td><td>15 minutes</td></tr><tr><td>Provisioning</td><td>30 minutes</td></tr><tr><td>Maintenance</td><td>60 minutes</td></tr><tr><td>Retrieve</td><td>Unlimited</td></tr></table></td></tr>
<tr><td>FTA_SSL.4</td><td>An administrator is able to exit out of both local and remote administrative sessions.</td></tr>
</table>

TOE SFRs	How the SFR is Met
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the GUI management interface prior to allowing any administrative access to the TOE. This is applicable for both local and remote TOE administration.
FTP_ITC.1	The TOE protects communications between the TOE and the remote audit server using HTTPS/TLS. This provides a secure channel to transmit the log events.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted HTTPS session. The remote users are able to initiate HTTPS communications with the TOE.

7 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target (and as based on the NDPP). The following matrix is the typical display that is drawn from the information presented in Sections 2 and 3 of the NDPP.

7.1 Rationale for TOE Security Objectives

The security objectives rationale shows how the security objectives correspond to threats and organizational security policies and provides a justification of that tracing.

Table 18: Threat/Objectives/Policies Mappings

	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	T.ADMIN_ERROR	T.UNDETECTED_ACTIONS	T.USER_DATA_REUSE	T.TSF_FAILURE	P.ACCESS BANNER
O.PROTECTED_COMMUNICATIONS	X						
O.VERIFIABLE_UPDATES		X					
O.SYSTEM_MONITORING				X			
O.DISPLAY_BANNER							X
O.TOE_ADMINISTRATION			X				
O.RESIDUAL_INFORMATION_CLEARING					X		
O.SESSION_LOCK	X						
O.TSF_SELF_TEST						X	

Table 19: Threat/Policies/TOE Objectives Rationale

Objective	Rationale
Security Objectives Drawn from NDPP	

Objective	Rationale
O.PROTECTED_COMMUNICATIONS	This security objective is necessary to counter the threat: T.UNAUTHORIZED_ACCESS to ensure the communications with the TOE is not compromised
O.VERIFIABLE_UPDATES	This security objective is necessary to counter the threat T.UNAUTHORIZED_UPDATE to ensure the end user has not installed a malicious update, thinking that it was legitimate.
O.SYSTEM_MONITORING	This security objective is necessary to counter the T.UNDETECTED_ACTIONS to ensure activity is monitored so the security of the TOE is not compromised.
O.DISPLAY_BANNER	This security objective is necessary to address the Organization Security Policy P.ACCESS_BANNER to ensure an advisory notice and consent warning message regarding unauthorized use of the TOE is displayed before the session is established.
O.TOE_ADMINISTRATION	This security objective is necessary to counter the T.ADMIN_ERROR that ensures actions performed on the TOE are logged so that indications of a failure or compromise of a TOE security mechanism are known and corrective actions can be taken.
O.RESIDUAL_INFORMATION_CLEARING	This security objective is necessary to counter the threat T.USER_DATA_REUSE so that data traversing the TOE could inadvertently be sent to a user other than that intended by the sender of the original network traffic.
O.SESSION_LOCK	This security objective is necessary to counter the threat: T.UNAUTHORIZED_ACCESS to ensure accounts cannot be compromised and used by an attacker that does not otherwise have access to the TOE.
O.TSF_SELF_TEST	This security objective is necessary to counter the threat T.TSF_FAILURE to ensure failure of mechanisms do not lead to a compromise in the TSF.

7.2 Rationale for the Security Objectives for the Environment

The security objectives for the environment rationale show how the security objectives for the environment correspond to assumptions and provide a justification of that tracing.

Table 20: Assumptions/Environment Objectives Mappings

	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.TRUSTED_ADMIN
A.NO_GENERAL_PURPOSE	X		
A.PHYSICAL		X	
A.TRUSTED_ADMIN			X

Table 21: Assumptions/Threats/Objectives Rationale

Environment Objective	Rationale
OE.NO_GENERAL_PURPOSE	This security objective is necessary to address the assumption A.NO_GENERAL_PURPOSE by ensuring there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) capabilities on the TOE.
OE.PHYSICAL	This security objective is necessary to address the assumption A.PHYSICAL by ensuring the TOE and the data it contains is physically protected from unauthorized access.
OE.TRUSTED_ADMIN	This security objective is necessary to address the assumption A.TRUSTED_ADMIN by ensuring the administrators are non-hostile and follow all administrator guidance.

7.3 Rationale for requirements/TOE Objectives

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Protection Profile are mutually supportive and their combination meets the stated security objectives.

Table 22: Security Objective to Security Requirements Mappings

	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.TSF_SELF_TEST
FAU_GEN.1			X					
FAU_GEN.2			X					
FAU_STG_EXT.1			X					
FCS_CKM.1	X							
FCS_CKM_EXT.4	X							
FCS_COP.1(1)	X							
FCS_COP.1(2)	X	X						
FCS_COP.1(3)	X	X						

FCS_COP.1(4)	X							
FCS_RBG_EXT.1	X							
FCS_HTTPS_EXT.1	X							
FCS_TLS_EXT.1	X							
FDP_RIP.2						X		
FIA_PMG_EXT.1					X			
FIA_UIA_EXT.1					X			
FIA_UAU_EXT.2					X			
FIA_UAU.7					X			
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_STM.1			X					
FPT_SKP_EXT.1	X							
FPT_APW_EXT.1	X							
FPT_TUD_EXT.1		X						
FPT_TST_EXT.1								X
FTA_SSL_EXT.1					X		X	
FTA_SSL.3					X		X	
FTA_SSL.4					X			
FTA_TAB.1				X				
FTP_ITC.1	X							
FTP_TRP.1	X							

Table 23: Objectives to Requirements Rationale

Objective	Rationale
Security Functional Requirements Drawn from Security Requirements for NDPP	
O.PROTECTED_COMMUNICATIONS	The SFRs FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FPT_SKP_EXT.1, FPT_APW_EXT.1, FTP_ITC.1, FTP_TRP.1 meet this objective by ensuring the communications between the TOE and endpoints are secure by implementing the encryption protocols as defined in the SFRs and as specified by the RFCs.
O.VERIFIABLE_UPDATES	The SFRs, FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3) meet this objective by ensuring the update was downloaded via secure communications, is from a trusted source, and the update can be verified by cryptographic mechanisms prior to installation.
O.SYSTEM_MONITORING	The SFRs, FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FPT_STM.1 meet this objective by auditing actions on the TOE. The audit records identify the user associated with the action/event,

Objective	Rationale
	whether the action/event was successful or failed, the type of action/event, and the date/time the action/event occurred. The audit logs are transmitted securely to a remote syslog server. If connectivity to the remote syslog server is lost, the TOE will block new permit actions.
O.DISPLAY_BANNER	The SFR, FTA_TAB.1 meets this objective by displaying a advisory notice and consent warning message regarding unauthorized use of the TOE.
O.TOE_ADMINISTRATION	The SFRs, FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FMT_MTD.1, FMT_SMF.1, FMT_SFR.2, FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4 meet this objective by ensuring the TOE supports a password-based authentication mechanism with password complexity enforcement such as, strong passwords, password life-time constraints, providing current password when changing the password, obscured password feedback when logging in, and passwords are not stored in plaintext. The objective is further met by ensuring restrictive default values are enforced on the SFPs (authorization and flow control), that only Authorized Administrators to override the default values, that the TOE provides the management and configuration features to securely manage the TOE and that those functions are restricted to the authorized administrator, and the implementation of session termination after an administrative configurable inactivity time period whereas the user must be re-authenticated,
O.RESIDUAL_INFORMATION_CLEARING	The SFR, FDP_RIP.2 meets this objective by ensuring no left over user data from the previous transmission is included in the network traffic.
O.SESSION_LOCK	The SFRs, FTA_SSL_EXT.1, FTA_SSL.3 meet this objective by terminating a session due to meeting/exceeding the inactivity time limit.
O.TSF_SELF_TEST	The SFR, FPT_TST_EXT.1 meets this objective by performing self-test to ensure the TOE is operating correctly and all functions are available and enforced.

8 ANNEX A: ADDITIONAL INFORMATION

8.1 Cryptographic Key/CSP Management

The TOE securely stores both cryptographic keys and other critical security parameters such as passwords. The keys are also protected by the password-protection on the authorized administrator role login, and can be zeroized by the authorized administrator. All zeroization consists of overwriting the memory that stored the key.

The TOE is in the approved mode of operation (FIPS mode) only when FIPS 140-2 approved algorithms are used (except DH and RSA key transport which are allowed in the approved mode for key establishment despite being non-approved).

All Diffie-Hellman (DH)/ECDH keys agreed upon for individual tunnels are directly associated with that specific connection. RSA Public keys are entered into the TOE using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them.

8.2

8.3 Key Zeroization

The following table describes the storage location and key zeroization referenced by FCS_CKM_EXT.4 provided by the TOE.

Table 24: TOE Key Zeroization

Key/CSP Name	Description	Storage Location	Zeroization Method
DRBG entropy input	This is the entropy for SP 800-90 RNG.	SDRAM	power cycle the device
DRBG seed	This is the seed for SP 800-90 RNG.	SDRAM	power cycle the device
DRBG V	Internal V value used as part of SP 800-90 CTR_DRBG	SDRAM	power cycle the device
DRBG key	Internal Key value used as part of SP 800-90 CTR_DRBG	SDRAM	power cycle the device
Diffie-Hellman private key	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	SDRAM	Automatically after shared secret generated.
Diffie-Hellman public key	The public exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	SDRAM	Automatically after shared secret generated.
Diffie-Hellman shared secret	The shared secret used in Diffie-Hellman (DH) exchange. Zeroized after DH key agreement.	SDRAM	Automatically after key agreement.
EC Diffie-Hellman private key	The private exponent used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	SDRAM	Automatically after shared secret generated.
EC Diffie-Hellman public key	The public exponent used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	SDRAM	Automatically after shared secret generated.

Key/CSP Name	Description	Storage Location	Zeroization Method
EC Diffie-Hellman shared secret	The shared secret in Elliptic Curve Diffie-Hellman (ECDH) exchange. Zeroized after ECDH key agreement.	SDRAM	Automatically after key agreement.
HTTPS TLS server private key	1024 bit RSA private key used for SSLV3.1/TLS.	NVRAM	Zeroized by deleting binary
HTTPS TLS server public key	1024 bit RSA public key used for SSLV3.1/TLS.	SDRAM	Automatically when TLS session is terminated
HTTPS TLS pre-master secret	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	SDRAM	Automatically when TLS session is terminated
HTTPS TLS session keys	Key used to encrypt TLS session data	SDRAM	Automatically when TLS session is terminated
Optical TLS server private key	1024/1536/2048 bit RSA private key used for TLS.	NVRAM	Deleted via the GUI interface
Optical TLS server public key	1024/1536/2048 bit RSA public key used for TLS.	SDRAM	Automatically when TLS session is terminated
Optical TLS pre-master secret	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	SDRAM	Automatically when TLS session is terminated
Optical TLS key expansion master key	Optical key extracted using RFC 5705 TLS Key Extractor. Used to derive client/server keys.	SDRAM	Automatically when TLS session is terminated
Optical TLS client key	Optical traffic key derived via NIST SP 800-108 Key Derivation.	SDRAM	Automatically when TLS session is terminated
Optical TLS server key	Optical traffic key derived via NIST SP 800-108 Key Derivation.	SDRAM	Automatically when TLS session is terminated
User passwords	The password of the defined user roles. The passwords must be at least 15 characters long or greater, composed of any combination of upper and lower case, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”. The minimum required characters are configurable. The password is encrypted by default using SHA256. This password is zeroized by overwriting it with a new password.	NVRAM	Overwrite with new password

ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 25: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDPP]	U.S. Government Protection Profile for Security Requirements for Network Devices, version 1.1, June 8, 2012
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008