Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series

Security Target

Version 1.0

27 January 2016

EDCS - 1513391

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

Table of Contents

1 SECURITY TARGET INTRODUCTION 7
1.1 ST and TOE Reference 7
1.2 TOE Overview 7
1.2.1 TOE Product Type 8
1.2.2 Supported non-TOE Hardware/ Software/ Firmware 9
1.3 TOE DESCRIPTION 10
1.4 TOE Evaluated Configuration 11
1.5 Physical Scope of the TOE 12
1.6 Logical Scope of the TOE 17
1.6.1 Security Audit 18
1.6.2 Cryptographic Support 18
1.6.3 Full Residual Information Protection 18
1.6.4 Identification and authentication 19
1.6.5 Security Management 19
1.6.6 Protection of the TSF 19
1.6.7 TOE Access 20
1.6.8 Trusted path/Channels 20
1.7 Excluded Functionality 20
2 Conformance Claims 21
2.1 Common Criteria Conformance Claim 21
2.2 Protection Profile Conformance 21
2.2.1 Protection Profile Additions 21
2.3 Protection Profile Conformance Claim Rationale 21
2.3.1 TOE Appropriateness 21
2.3.2 TOE Security Problem Definition Consistency 21
2.3.3 Statement of Security Requirements Consistency 22
3 SECURITY PROBLEM DEFINITION 23
3.1 Assumptions 23
3.2 Threats 23
3.3 Organizational Security Policies 24
4 SECURITY OBJECTIVES 25
4.1 Security Objectives for the TOE 25
4.2 Security Objectives for the Environment 26
5 SECURITY REQUIREMENTS 27
5.1 Conventions 27
5.2 TOE Security Functional Requirements 27
5.3 SFRs Drawn from NDPP 28
5.3.1 Security audit (FAU) 28
5.3.2 Cryptographic Support (FCS) 30
5.3.3 User data protection (FDP) 32
5.3.4 Identification and authentication (FIA) 32
5.3.5 Security management (FMT) 33
5.3.6 Protection of the TSF (FPT) 33

5.3.7 TOE Access (FTA) 34
5.3.1 Trusted Path/Channels (FTP) 35
5.4 TOE SFR Dependencies Rationale 36
5.5 Security Assurance Requirements 36
5.5.1 SAR Requirements 36
5.5.2 Security Assurance Requirements Rationale 36
5.6 Assurance Measures 36
6 TOE Summary Specification 38
6.1 TOE Security Functional Requirement Measures 38
7 Annex A: Additional Information 46
7.1 Cryptographic Key/CSP Management 46
7.2 Key Zeroization 46
7.3 Sample Audit Records 48
Annex B: References 56

List of Tables

TABLE 1 ACRONYMS......5
TABLE 2 TERMS......6
TABLE 3 ST AND TOE IDENTIFICATION......7
TABLE 4 IT ENVIRONMENT COMPONENTS......9
TABLE 5 CAVP REFERENCES......18
TABLE 6 EXCLUDED FUNCTIONALITY......20
TABLE 7 PROTECTION PROFILES......21
TABLE 8 TOE ASSUMPTIONS......23
TABLE 9 THREATS......23
TABLE 10 ORGANIZATIONAL SECURITY POLICIES......24
TABLE 11 SECURITY OBJECTIVES FOR THE TOE......25
TABLE 12 SECURITY OBJECTIVES FOR THE ENVIRONMENT......26
TABLE 13 SECURITY FUNCTIONAL REQUIREMENTS......27
TABLE 14 AUDITABLE EVENTS......28
TABLE 15: ASSURANCE MEASURES......36
TABLE 16 ASSURANCE MEASURES......36
TABLE 17 HOW TOE SFRS ARE MET......38
TABLE 18: TOE KEY ZEROIZATION......46
TABLE 19: GENERAL AUDITABLE EVENTS......48
TABLE 20: REFERENCES......56

List of Figures

FIGURE 1 TOE EXAMPLE DEPLOYMENT......11
FIGURE 2 CISCO ONS 15454 M2 (WITH AND WITHOUT FRONT COVER)......13
FIGURE 3 CISCO ONS 15454 M6 (WITH AND WITHOUT FRONT COVER)......14
FIGURE 4 CISCO NCS 2015, NCS 2006, AND NCS 2002......14
FIGURE 5 CISCO NCS 2015......15
FIGURE 6 CISCO NCS 2015 EXTERNAL CONNECTION UNIT......15
FIGURE 7 CISCO NCS 2006......16
FIGURE 8 CISCO NCS 2006 EXTERNAL CONNECTION UNIT......16
FIGURE 9 CISCO NCS 2002......17

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
EPN	Evolved Programmable Network
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
NCS	Network Convergence System
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
ROADM	reconfigurable optical add/drop multiplexer
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

Acronyms / Abbreviations	Definition
WIC	WAN Interface Card

Terminology

The following terminology may be used in this Security Target:

Table 2 Terms

Teminology	Definition
CTC	The CTC (Cisco Transport Controller) is the GUI-based management application that is used to configure and manage ONS and NCS systems. The CTC is a JRE file that is part of the TOE software installed on the controller card. The JRE file is downloaded and installed on a management workstation during the install setup and configuration of the TOE. The software version is the same for all of the TOE components.
Muxponder	A muxponder is the element that sends and receives the optical signal on a fiber that also includes multiplexing multiple sub-rate client interfaces onto the line interface
Transponder	A transponder gathers signals over a range of uplink frequencies and re-transmits them on a different set of downlink frequencies

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) and Network Convergence System (NCS) 2000 Series. 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 3 ST and TOE Identification

Name	Description
ST Title	Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series Security Target
ST Version	1.0
Publication Date	27 January 2016
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series
TOE Hardware Models	Cisco ONS 15454-M2, ONS 15454-M6, NCS 2002, NCS 2006, and NCS 2015
TOE Software Version	ONS/NCS 10.5 Release software version consists of • MSTPR and NCS2K Note: The only difference in the software images is the new ROADM cards are only supported in NCS2K packages and the older Transponder cards are only supported in MSTP packages. The differences in the cards do not affect any of the security claims or any of the security functional requirements that are claimed in this Security Target
Keywords	Optical, Data Protection, Authentication, Networking

1.2 TOE Overview

The Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series TOE provides dense wavelength-division multiplexing (DWDM) and time-division multiplexing (TDM) solutions and the evolved flex-spectrum reconfigurable optical add/drop multiplexer (ROADM) capabilities.

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 enterprise and ultra-long-haul optical 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 3 in section 1.1 ST and TOE Reference.

The Cisco Transport Controller (CTC) is a GUI-based application used to configure and manage ONS and NCS 2000 Series 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 and NCS 2000 Series product type is optical networking. Products of this type provide optical network technology that relies on a combination of optical amplifiers, lasers, LEDs and wave division multiplexing (WDM) to transmit large quantities of data across fiber-optic cables.

The Cisco ONS and NCS 2000 Series solution offers the choice of multiservice aggregation, wavelength aggregation, and wavelength transport, combined with integrated, intelligent Dense Wavelength-Division Multiplexing (DWDM) transmission in a single platform to minimize network costs for any mix of service types. The NCS 2000 Series also includes reconfigurable optical add/drop multiplexer (ROADM) technology supports touchless re-configurability networks through colorless, omni-directional, and contention-less add/drop configurations that can instantly respond to new bandwidth requests, route around network failures, and dynamically adjust their topology.

The Cisco ONS and NCS 2000 Series 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 Cisco ONS and NCS 2000 Series 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 Cisco ONS and NCS 2000 Series information and perform Cisco ONS and NCS 2000 Series provisioning and maintenance. From this window the display can be set to display three Cisco ONS and NCS 2000 Series views:

- Network - allows you to view and manage Cisco ONS and NCS 2000 Series 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 a Cisco ONS and NCS 2000 Series. 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 Cisco ONS and NCS 2000 Series 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 Cisco ONS and NCS 2000 Series 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 Cisco ONS and NCS 2000 Series 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 Cisco ONS and NCS 2000 Series 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 the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All of the following environment components are supported by all TOE evaluated configurations.

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation	Yes	This includes any IT Environment Management workstation installed with Cisco Transport Controller (CTC), the software interface for Cisco NCS 2000 Series that is used by the TOE administrator to support TOE administration through HTTPS protected channels.

Component	Required	Usage/Purpose Description for TOE performance
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages over TLS.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco ONS and NCS 2000 Series Target of Evaluation (TOE).

The Cisco ONS and NCS 2000 Series includes the one or more of the following Chassis (Shelves):

- ONS:
    - 15454-M2
    - 15454-M6
- NCS 2000 Series
    - NCS 2002
    - NCS 2006
    - NCS 2015

Each of the Chassis support the following cards, except where specifically noted. In the evaluated configuration the chassis must include at least one controller card, at least one encryption care and at least one line card.

- Controller Cards (Management) (one or more):
    - 15454-M-TNC-K9
    - 15454-M-TSC-K9
    - 15454-M-TNCE-K9
    - 15454-M-TSCE-K9
    - NCS2K-TNCS-O-K9
    - NCS2K-TNCS-K9 (only supported on the NCS 2015 chassis)
- Encryption Cards (Data Traffic traversing the TOE):
    - 15454-M-WSE-K9
    - NCS2K-MR-MXP-LIC
    - Pluggable optics used
        - ONS-SC+-10G-SR=
        - CPAK-100G-SR10
        - QSFP-4x10G-LR-S=
- Line Cards (Data Traffic traversing the TOE; no encryption):
    - 15454-M-10X10G-LC
    - NCS2K-200G-CK-LIC=

The software is comprised of the Cisco's ONS/NCS 10.5 Release software version that consists of two images; MSTPR and NCS2K. The only difference in the software images is the new ROADM cards are only supported in NCS2K packages and the older Transponder cards are only supported in MSTP packages. The differences in the cards do not affect any of the security claims or any of the security functional requirements that are claimed in this Security Target.

While these cards are the controllers cards that are used to manage the TOE, the difference are simply how the data that transverse the TOE is transmitted. All of the TOE management and administrative traffic is protected and secured using HTTPS/TLS. All of the security management functions are the same in both packages.

The TOE is managed using the Cisco Transport Controller (CTC) management software that is installed on a Management Workstation (depicted as CTC (Admin Console) in the figure below) 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 following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

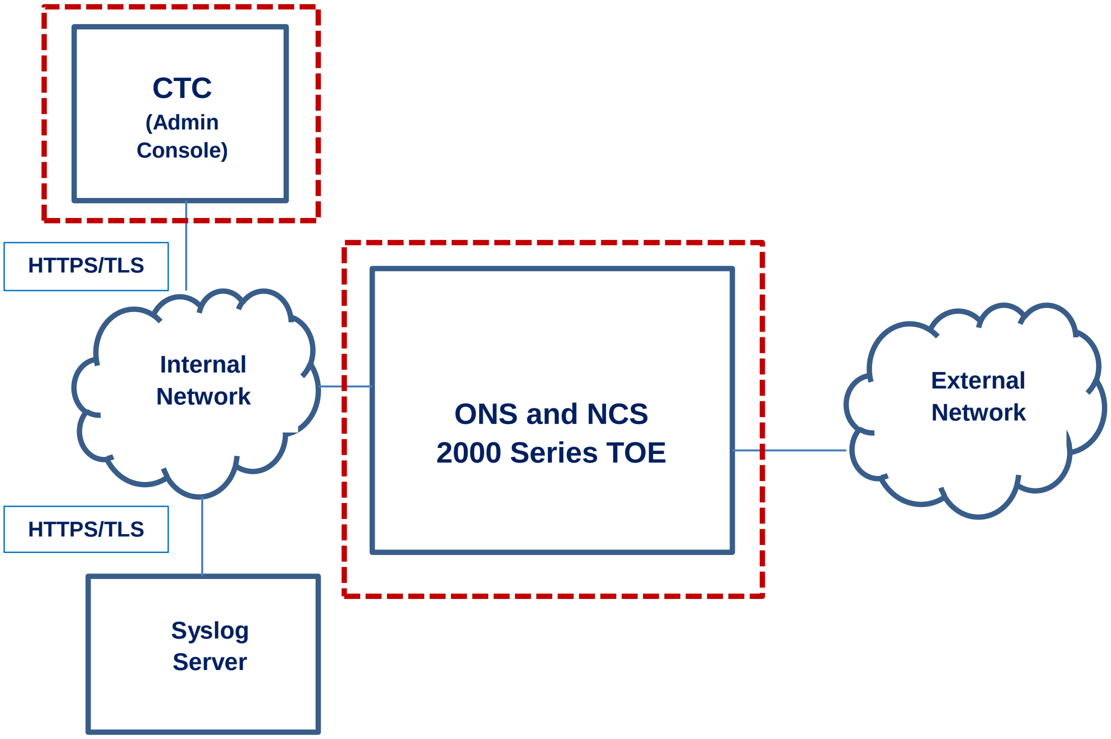


Figure 1 TOE Example Deployment

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices including the controller, encryption and line cards and software as described below.

- Chassis (one or more):

    - 15454-M2
    - 15454-M6
    - NCS 2002
    - NCS 2006
    - NCS 2015
- Controller Cards (Management) (one or more):
    - 15454-M-TNC-K9
    - 15454-M-TSC-K9
    - 15454-M-TNCE-K9
    - 15454-M-TSCE-K9
    - NCS2K-TNCS-O-K9
    - NCS2K-TNCS-K9 (only supported on the NCS 2015 chassis)
- Encryption Cards (Data Traffic traversing the TOE):
    - 15454-M-WSE-K9
    - NCS2K-MR-MXP-LIC
    - Pluggable optics used
        - ONS-SC+-10G-SR=
        - CPAK-100G-SR10
        - QSFP-4x10G-LR-S=
- Line Cards (Data Traffic traversing the TOE; no encryption):
    - 15454-M-10X10G-LC
    - NCS2K-200G-CK-LIC=
- CTC Management
- Software
    - ONS/NCS 10.5 Release software version

The CTC software is included in the ONS/NCS 10.5 Release software version and is preloaded on the ONS and NCS 2000 Series controller cards. CTC software is downloaded to the management workstation during the initial setup and configuration of the ONS and NCS 2000 Series. 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.

1.5 Physical Scope of the TOE

The Cisco ONS 15454 M2 chassis has one slot for the control card and two slots for service cards. These two line-card slots provide increased power and cooling capability and a usable high-speed backplane for future applications. The M2 chassis can be configure with integrated DC or AC power inputs. The DC power module has inputs for redundant A and B feeds. The integrated AC power module has a single input and is universal in that it accepts a power input ranging from 110to 240VAC, 50 to 60 Hz. With its front-facing connections, the M2 is ideal for cabinet installations and ETSI front-connection requirements, making this platform truly global.

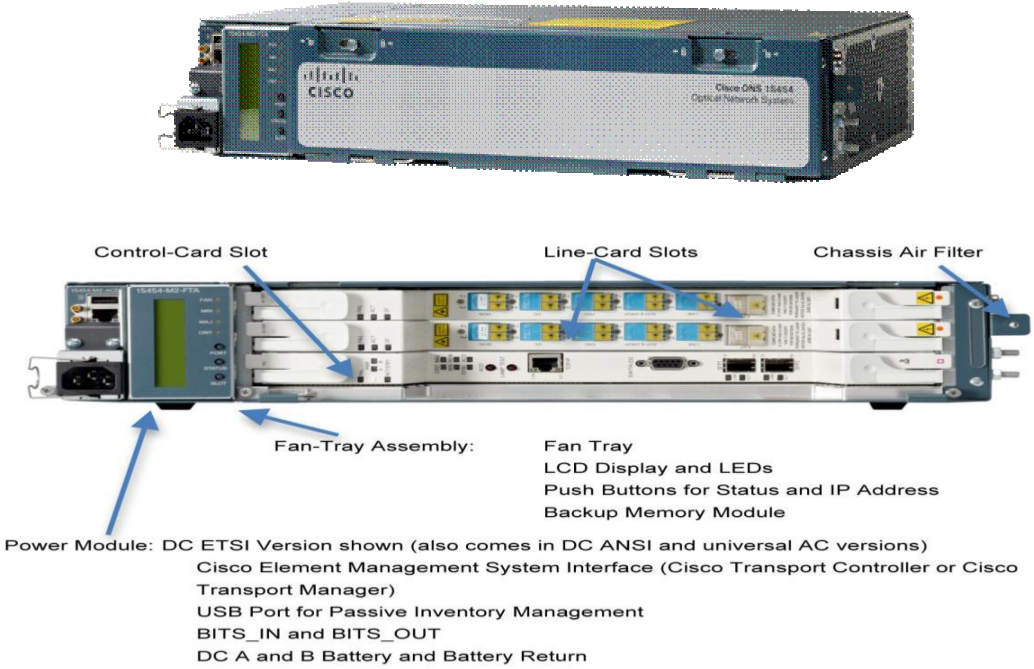

cisco
Cisco ONS 15454 Optical Network System
Control-Card Slot
Line-Card Slots
Chassis Air Filter
Fan-Tray Assembly:
Fan Tray
LCD Display and LEDs
Push Buttons for Status and IP Address
Backup Memory Module
Power Module: DC ETSI Version shown (also comes in DC ANSI and universal AC versions)
Cisco Element Management System Interface (Cisco Transport Controller or Cisco Transport Manager)
USB Port for Passive Inventory Management
BITS_IN and BITS_OUT
DC A and B Battery and Battery Return

Figure 2 Cisco ONS 15454 M2 (with and without front cover)

The Cisco ONS 15454 M6 chassis has two slots for redundant control cards and six slots for service cards. These six line card slots provide increased power and cooling capability and a high-speed backplane for card-to-card interconnection. The M6 chassis can be configured with integrated and redundant DC or AC power inputs or a single power module for low-power and low-cost configurations. The Electrical Connection Unit (ECU) is a narrow, front-facing termination panel for all management, alarm, and multi-shelf connections. With all connections to the M6 chassis located on the front, this platform is ideal for cabinet installations and ETSI front connection requirements, making it truly global in its appeal. The ECU comes in two versions; the ECU2 version includes an RJ-45 connector for time-of-day (ToD) input and pulse-per-second (PPS) input.

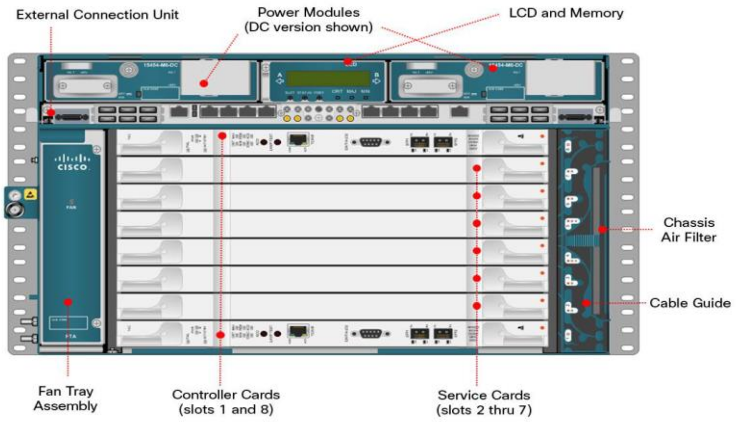


Figure 3 Cisco ONS 15454 M6 (with and without front cover)

The Cisco NCS 2000 Series offers three chassis variants to meet varying scale and space requirements. The Cisco NCS 2015 has 15 slots for service cards and is 14 rack units (14RU) high, allowing three chassis to fit into one standard rack. The Cisco NCS 2006 chassis is 6RU and has 6 slots for service cards. The NCS 2002 is 2RU and has 2 slots for service cards. Multishelf management allows multiple (up to 50) NCS 2015 and NCS 2006 shelves to be managed as a single network element, with a single target identifier (TID) and IP address, facilitating the construction of nodes with a very large number of ROADM degrees and/or service cards.

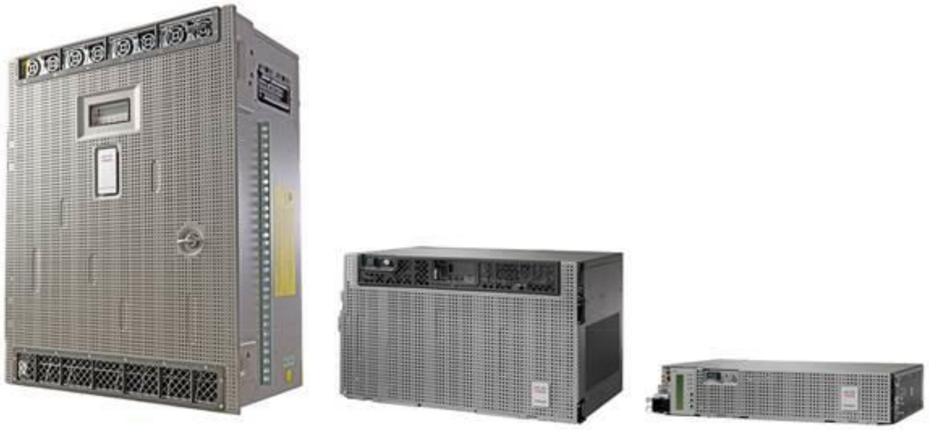


Figure 4 Cisco NCS 2015, NCS 2006, and NCS 2002

The Cisco NCS 2015 chassis support AC or DC power applications. Four slots accommodate up to four power modules in a 3 + 1 redundant configuration, which is common in the NCS 2000 Series. Power-cabling connectors are decoupled from the power modules themselves, allowing easy replacement of a module with no impact on cabling.

Airflow through the chassis is front-to-back, facilitating hot-aisle/cold-aisle installations. A replaceable fan tray containing eight fans divided among two separate circuits sits above the line cards, and also houses timing and alarm input and output connectors. Air is drawn in through a 2-inch input plenum at the bottom of the chassis, and expelled at the top-rear.

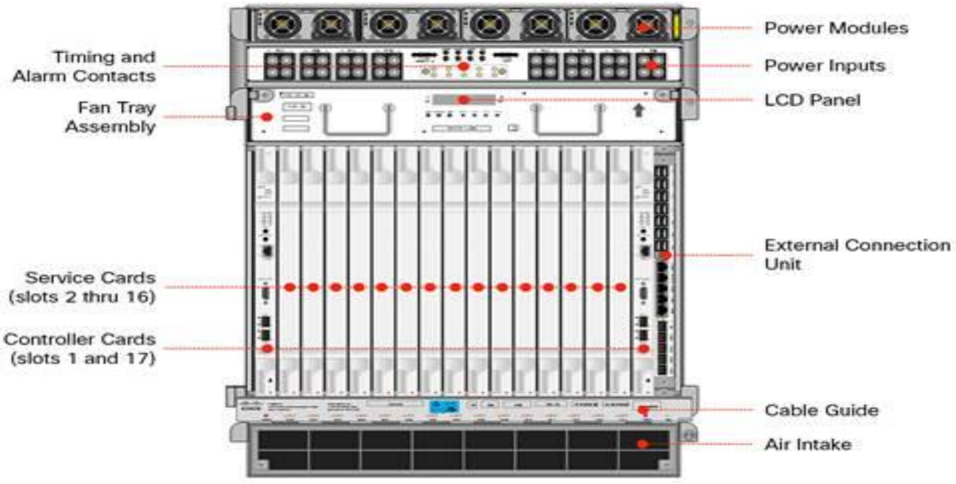


Figure 5 Cisco NCS 2015

The NCS 2015 electrical connection unit (ECU) is a replaceable module that provides interfaces for passive device inventory and management, multishelf management, and element management. Both RJ-45 and SFP interfaces are provided for multishelf and element management, allowing the convenience of copper as well as the distance flexibility of optical connections. Fourteen USB ports connect to passive devices, two of which are USB 3.0 ports capable of powering a USB hub to increase device fan-out and simplify cabling.

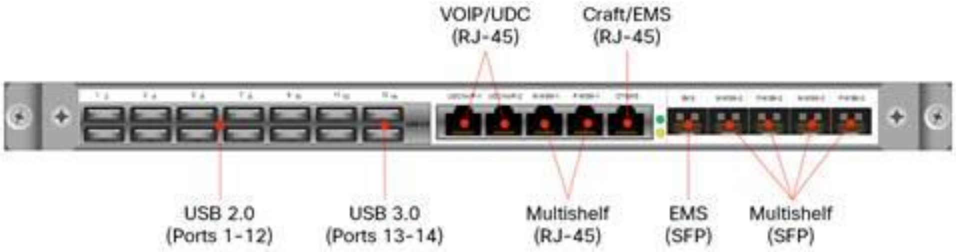


Figure 6 Cisco NCS 2015 External Connection Unit

At 6 Rack Unit (RU) with 6 service slots, the Cisco NCS 2006 chassis is versatile. Metro/edge locations can minimize footprint while still accommodating multiple ROADM degrees and/or service line cards, and large core nodes can scale as large as necessary by using multishelf configurations.

The Cisco NCS 2006 chassis can be configured with DC or AC power inputs. The DC power module has connectors for both American National Standards Institute (ANSI) and International Electrotechnical Commission (ETSI) style battery connections, making it universal. The AC power modules have a single input and are universal in that they accept a power input ranging from 110 to 240 VAC, 50 to 60 Hz.

The Cisco NCS 2006 can be mounted into 19-, 21-, or 23-inch racks or cabinets. Brackets come with the shelf assembly and can also be ordered as spares. You can use optional air deflectors in 21- and 23-inch installations. Airflow is side-to-side, but you can add deflectors for front-to-back and front-to-front airflow. In the 21-inch configuration airflow could also be front-to-top. Additionally, an air plenum is available that you can be used for front to back airflow in 19-inch rack configurations.

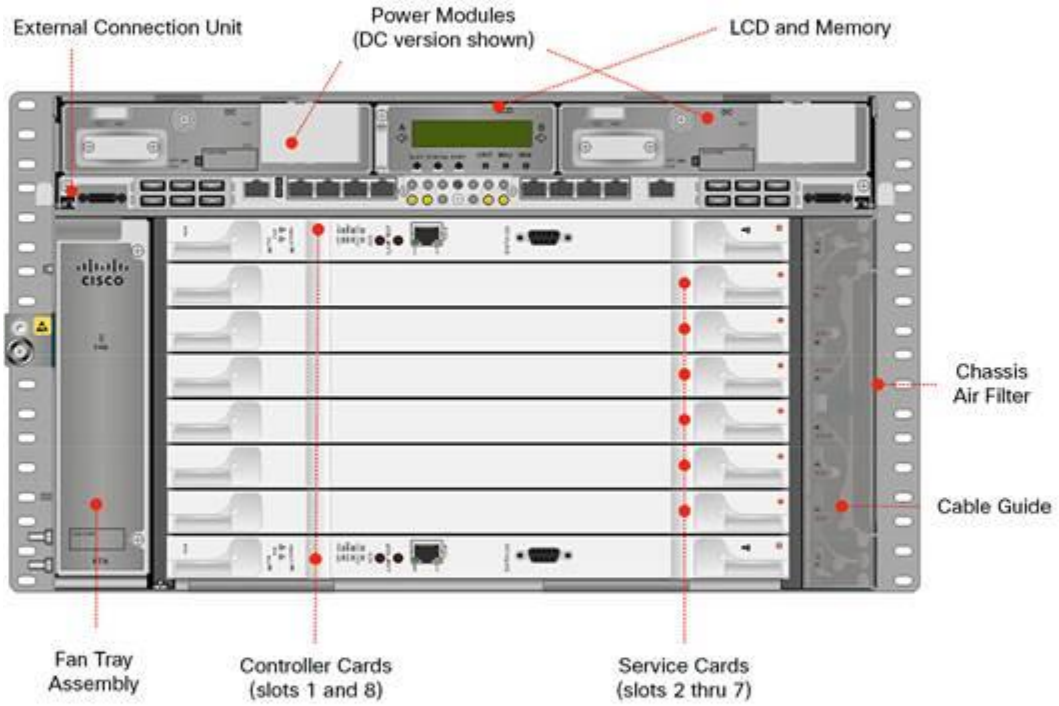


Figure 7 Cisco NCS 2006

The Cisco NCS 2006 electrical connection unit (ECU) is a replaceable module that provides interfaces for multishelf management, element management, passive device management, external alarm inputs and outputs, and timing. RJ-45 ports provide multishelf and element-management connectivity, and 12 USB ports connect to passive devices for inventory and management.

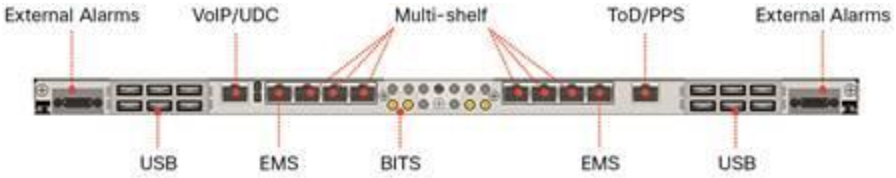


Figure 8 Cisco NCS 2006 External Connection Unit

The Cisco NCS 2002 is ideally suited to line amplifier configurations, a 2-degree ROADM node, or anywhere that only 2 slots are required for transponder or muxponder services. The NCS 2002 features 1 slot for the control card and 2 slots for service cards. The NCS 2002 can be configured with a single DC or AC power module. The DC power module has inputs for redundant A and B feeds. The integrated AC power module has a single input and is universal in that it accepts a power input ranging from 110 to 240 VAC, 50 to 60 Hz.

Although a single processor card controls the node, the NCS 2002 contains a built-in memory module to back up the software package, IP address, and circuit database. This backup capability improves mean time to repair (MTTR) and increases operational simplicity. Integrated RJ-45 and USB ports provide management connectivity and passive device connectivity, respectively. Timing inputs and outputs are also present.

The NCS 2002 can be mounted in 19-, 21-, or 23-inch racks or cabinets. Brackets come with the shelf assembly and can also be ordered as spares. Optional air deflectors in 21- and 23-inch can be used in the installations. With 19-inch brackets, the airflow is right-to-left; with 21-inch brackets, airflow can be selected as right-to-left; right-front-in, and left-front-out; left-up-out; or left-back-out. With 23-inch brackets, airflow is from right-front-in to left-back-out.

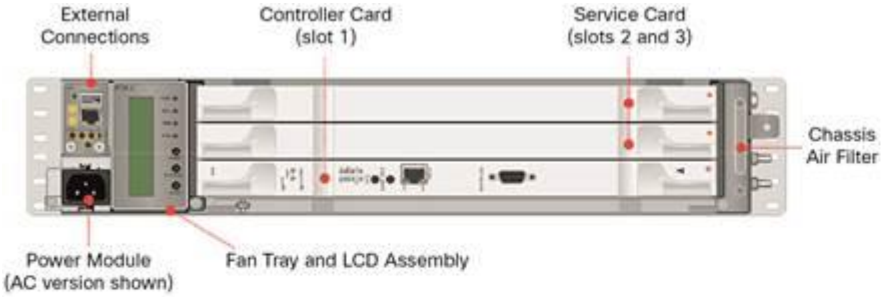

External Connections
Controller Card (slot 1)
Service Card (slots 2 and 3)
Chassis Air Filter
Power Module (AC version shown)
Fan Tray and LCD Assembly

Figure 9 Cisco NCS 2002

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 U.S. Government Protection Profile for Security Requirements for Network Devices, version 1.1, June 8, 2012 Version 1.1 with Errata#3 as necessary to satisfy the assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco ONS and NCS 2000 Series provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco ONS and NCS 2000 Series 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 connection to an external audit server.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of HTTPS/TLS connections for remote administrative management and transmission of audit records. The cryptographic services provided by the TOE are described in Table 5 CAVP References below.

Table 5 CAVP References

Algorithm	ONS and NCS 2000 Series Controller (Management) Card CAVP Cert. #
AES	3771
Triple-DES	2098
SHS	3141
HMAC	2471
RSA	1941
DRBG	1041

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+, though not required in the evaluated configuration.

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 directly connected PC. 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 and NCS 2000 Series 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
- Security Super User-Users can set encryption and card authentication parameters. The security super user creates security users and associates each user with an encryption card. By default, at least one security super user must exist.
- Security User-Users can enable or disable card authentication and payload encryption.

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

1.6.6 Protection of the TSF

The TOE protects the communications between the CTC and the node using TLS for a secure connection. The TOE also 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 and NCS 2000 Series is not a general-purpose operating system and access to Cisco ONS and NCS 2000 Series memory space is restricted to only Cisco ONS and NCS 2000 Series 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 TLS 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 mode of operation	This mode of operation includes non-FIPS mode 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, June 8, 2012, with Errata#3.

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 5.5 Security Assurance Requirements.

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)	V1.1	June 8, 2012
Security Requirements for Network Devices Errata	#3	3 November 2014

2.2.1 Protection Profile Additions

The ST claims exact conformance to the NDPP v1.1, with Errata#3 and does not include any additions to the functionality described in the Protection Profile.

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, June 8, 2012
- Security Requirements for Network Devices Errata #3

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, with Errata #3 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, with Errata#3 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, with Errata#3, 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, with Errata#3.

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
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
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.
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.

Threat	Threat Definition
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
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
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
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 <u>underlined</u> 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
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
FIA: Identification and	FIA_PMG_EXT.1	Password Management

Class Name	Component Identification	Component Name
authentication	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_ITT.1	Basic Internal TSF Data Transfer Protection
	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
FAU_GEN.1	Start of audit Shutdown of audit.	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_ITT.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] 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-bits that 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: RSA Digital Signature Algorithm

- **FIPS PUB 186-2 or 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 1.2 (RFC 5289)] supporting the following ciphersuites:

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:
[
TLS_RSA_WITH_AES_256_CBC_SHA

].

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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [”+”]];
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_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 Refinement: The TSF shall protect TSF data from *disclosure and detect its modification* when it is transmitted between separate parts of the TOE **through the use** [TLS/HTTPS].

5.3.6.2 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.

5.3.6.3 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.

5.3.6.4 FPT_STM.1 Reliable time stamps

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

5.3.6.5 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.

5.3.6.6 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] 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 TLS*].

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 TOE SFR Dependencies Rationale

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDPPv1.1 with Errata#3. As such, the NDPP SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.5 Security Assurance Requirements

5.5.1 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

5.5.2 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.

5.6 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.

Component	How requirement will be met
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-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.
ALC_CMS.1	
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
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 (not supported in the evaluated configuration), HTTPS, Console (e.g. directly connected PC), Simple Network Management Protocol (SNMP) (not supported in the evaluated configuration • 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 Examples of audit events are included in Section 7.3 Sample Audit Records in this document.
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. Examples of audit events are included in Section 7.3 Sample Audit Records in this document.
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

TOE SFRs	How the SFR is Met
	internals, which are transmitted to the syslog server for storage. The TOE protects communications with an external syslog server via TLS/HTTPS. The TOE is capable of detecting when the TLS/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. Refer to Section 7.3 Sample Audit Records for sample of the required auditable events.
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 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 7Annex A: Additional Information 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 3771 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 connection with ONS to download the executable JRE files.
FCS_TLS_EXT.1	The TOE provides TLS 1.2, conformant to RFC 5289 and supports the mandatory ciphersuites TLS_RSA_WITH_AES_128_CBC_SHA The TOE also supports the following optional ciphersuites: TLS_RSA_WITH_AES_256_CBC_SHA

TOE SFRs	How the SFR is Met
	The TOE only supports standard extensions, methods, and characteristics. TLS 1.2 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 5289 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 10.2 or later 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. Any initialization or system errors during bring-up or processing of this system causes a reboot. 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 ")"and "+". Minimum password length is settable by the Authorized Administrator, and support passwords of 15 characters or greater, up to 80 characters. 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 PC 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 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 PC 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

TOE SFRs	How the SFR is Met
	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 (e.g. directly connected PC), 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. The ONS CTC allows up to 500 user IDs on one ONS or NCS 2000 series. Each CTC user 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. • Security Super User-Users can set encryption and card authentication parameters. The security super user creates security users and associates each user with a WSE card. By default, at least one security super user must exist. • Security User-Users can enable or disable card authentication and payload encryption. 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. There are no administrative functions or capabilities available prior to successfully logging into the TOE.
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

TOE SFRs	How the SFR is Met
	evaluation, users can be assigned to the following security levels and all are deemed as authorized administrators. The ONS CTC allows up to 500 user IDs on one ONS or NCS 2000 series. Each CTC user 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. • Security Super User-Users can set encryption and card authentication parameters. The security super user creates security users and associates each user with a WSE card. By default, at least one security super user must exist. • Security User-Users can enable or disable card authentication and payload encryption. • 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 PC and remote authentication via HTTPS.
FPT_ITT.1	The TOE protects communications between the CTC and the node using HTTPS/TLS. This provides a secure channel for administrative management.
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 7 Annex A: Additional Information 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 protection is set by default and is not configurable. The passwords are protected by secure hash using SHA256. See Section 7 Annex A: Additional Information 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, however usage of an NTP server is not a required element of the evaluated configuration. 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

TOE SFRs	How the SFR is Met
	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. The TOE includes many security features to ensure the TOE hardware and software has not been tampered. The features include secure boot of the hardware that ensures authentic Cisco software boots up on the Cisco platform, and provides tamper and cloning resistance. After the secure boot, the Digital Image Signing ensures that the software that runs on Cisco devices is authentic. If there is an issue during the boot and verification process, call Cisco TAC immediately to obtain Technical Assistance. Instructions for how to do this verification are provided in the administrator guidance for this evaluation.
FPT_TST_EXT.1	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) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include and for each of the KATs listed below, the following takes place: • Encryption Card Firmware Known Answer Tests (KATs) o AES (encrypt/decrypt) KATs - - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. o DRBG KAT - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly. o HMAC (HMAC-SHA-1/256/512) KATs - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. o RSA KAT - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. • Controller Card Firmware KATs o AES (encrypt/decrypt) KATs - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted

TOE SFRs	How the SFR is Met
	value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. o DRBG KAT - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly. o HMAC (HMAC-SHA-1/256/512) KATs - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. o RSA KAT - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. o Triple-DES (encrypt/decrypt) KATs - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. • Hardware (FPGA) KATs o AES-GCM KAT - This test uses several values, including, a key, an IV, a plaintext data, and an input for additional authenticated data (AAD) to output an encrypted value and an authentication tag. The encrypted value and the authentication tag are compared to a known encrypted value and authentication tag to verify correct operation. o AES-XTS KAT - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. • Firmware Integrity Test (32-bit CRC) - This test takes a CRC of the TOE software and compares it to a known value to ensure the software has not been corrupted. 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 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.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>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</td><td rowspan="2">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.3</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>
<tr><td>FTA_TAB.1</td><td>The TOE displays a privileged Administrator specified banner on the GUI management interface prior to allowing any administrative access to the TOE. This banner is displayed both when connecting to the TOE remotely through HTTPS and when directly connecting to the management port on the TOE. In both instances the administrator accesses the same graphical interface.</td></tr>
<tr><td>FTP_ITC.1</td><td>The TOE protects communications between the TOE and the remote audit server using TLS. This provides a secure channel to transmit the log events.</td></tr>
<tr><td>FTP_TRP.1</td><td>All remote administrative communications take place over a secure encrypted HTTPS session. The remote users are able to initiate HTTPS communications with the TOE.</td></tr>
</table>

7 ANNEX A: ADDITIONAL INFORMATION

7.1 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 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.

7.2 Key Zeroization

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

Table 18: 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 overwritten by '0x00'
DRBG seed	This is the seed for SP 800-90 RNG.	SDRAM	power cycle the device overwritten by '0x00'
DRBG V	Internal V value used as part of SP 800-90 CTR_DRBG	SDRAM	power cycle the device overwritten by '0x00'
DRBG key	Internal Key value used as part of SP 800-90 CTR_DRBG	SDRAM	power cycle the device overwritten by '0x00'
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. overwritten by '0x00'
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. overwritten by '0x00'
Diffie-Hellman shared secret	The shared secret used in Diffie-Hellman (DH) exchange. Zeroized after DH key agreement.	SDRAM	Automatically after key agreement. overwritten by '0x00'

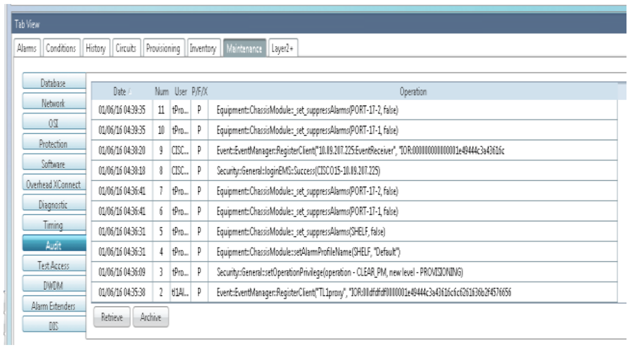
Key/CSP Name	Description	Storage Location	Zeroization Method
HTTPS TLS server private key	20148 bit RSA private key used for SSLV3.1/TLS.	NVRAM	Zeroized by deleting binary overwritten by '0x00'
HTTPS TLS server public key	2048 bit RSA public key used for SSLV3.1/TLS.	SDRAM	Automatically when TLS session is terminated overwritten by '0x00'
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 overwritten by '0x00'
HTTPS TLS session keys	Key used to encrypt TLS session data	SDRAM	Automatically when TLS session is terminated overwritten by '0x00'
Optical TLS server private key	1024/1536/2048 bit RSA private key used for TLS.	NVRAM	Deleted via the GUI interface overwritten by '0x00'
Optical TLS server public key	1024/1536/2048 bit RSA public key used for TLS.	SDRAM	Automatically when TLS session is terminated overwritten by '0x00'
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 overwritten by '0x00'
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 overwritten by '0x00'
Optical TLS client key	Optical traffic key derived via NIST SP 800-108 Key Derivation.	SDRAM	Automatically when TLS session is terminated overwritten by '0x00'
Optical TLS server key	Optical traffic key derived via NIST SP 800-108 Key Derivation.	SDRAM	Automatically when TLS session is terminated overwritten by '0x00'
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: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” and “+”. 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

7.3 Sample Audit Records

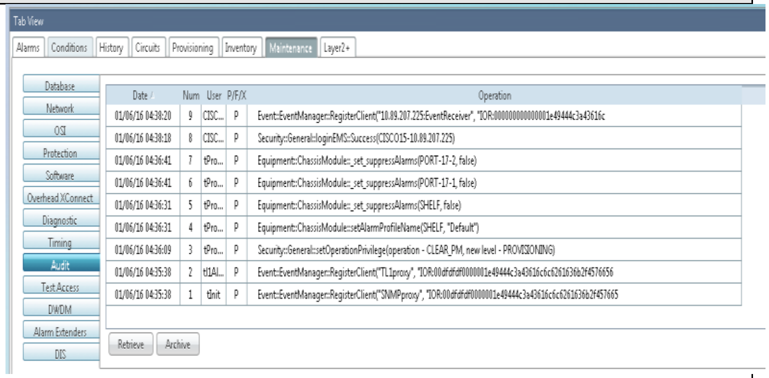
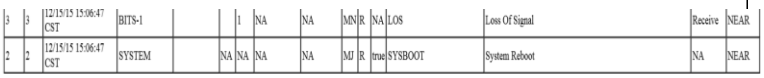
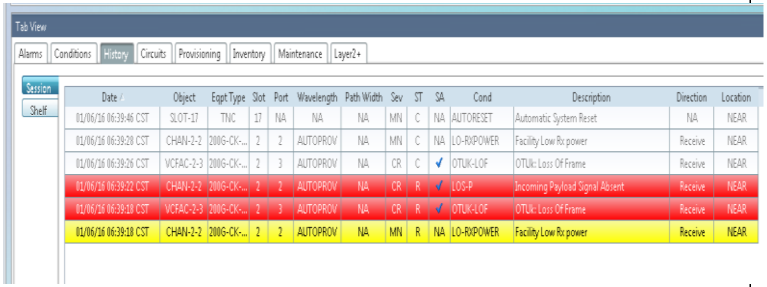
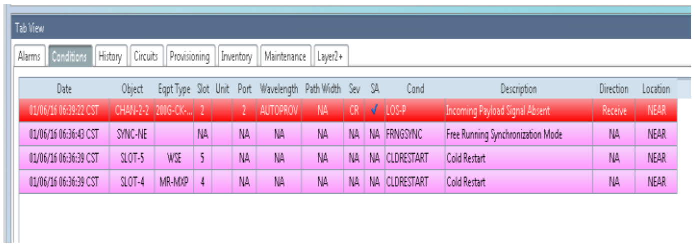
The tables below include the security relevant events that are applicable to the TOE. Audit trail records capture the following information/activities:

- 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 (not supported in the evaluated configuration), HTTPS, Console (directly connected PC), Simple Network Management Protocol (SNMP) (not supported in the evaluated configuration)
- 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

Table 19: General Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FAU_GEN.1	Start-up and shutdown of audit functions. Note: auditing starts automatically when the TOE is powered on and shutdown when the TOE is powdered off. There is no interface to start or stop auditing. Auditing is	No additional information.	

Date	Num	User	P/F/X	Operation
01/06/16 04:39:35	11	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-2, false)
01/06/16 04:39:35	10	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-1, false)
01/06/16 04:38:20	9	CISC...	P	Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c
01/06/16 04:38:18	8	CISC...	P	Security::General::loginEMS::Success(CISCO15-10.89.207.225)
01/06/16 04:36:41	7	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-2, false)
01/06/16 04:36:41	6	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-1, false)
01/06/16 04:36:31	5	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(SHELF, false)
01/06/16 04:36:31	4	tPro...	P	Equipment::ChassisModule::setAlarmProfileName(SHELF, "Default")
01/06/16 04:36:09	3	tPro...	P	Security::General::setOperationPrivilege(operation - CLEAR_PM, new level - PROVISIONING)
01/06/16 04:35:38	2	tl1Al...	P	Event::EventManager::RegisterClient("TL1proxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f4576656

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	not configurable .		   
FAU_GEN.2 User Identity Association	None	None	None
FAU_STG_EXT.1 External Audit Trail Storage	Administrative Actions: Configuration of syslog export settings	No additional information.	100 01/28/15 23:25:57 Event::AuditTrailArchiveSession::complete(true) 1 P CISCO15

Date	Num	User	P/F/X	Operation
01/06/16 04:38:20	9	CISC...	P	Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c
01/06/16 04:38:18	8	CISC...	P	Security::General::loginEMS::Success(CISCO15-10.89.207.225)
01/06/16 04:36:41	7	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-2, false)
01/06/16 04:36:41	6	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-1, false)
01/06/16 04:36:31	5	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(SHELF, false)
01/06/16 04:36:31	4	tPro...	P	Equipment::ChassisModule::setAlarmProfileName(SHELF, "Default")
01/06/16 04:36:09	3	tPro...	P	Security::General::setOperationPrivilege(operation - CLEAR_PM, new level - PROVISIONING)
01/06/16 04:35:38	2	tl1Al...	P	Event::EventManager::RegisterClient("TL1proxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f4576656
01/06/16 04:35:38	1	tInit	P	Event::EventManager::RegisterClient("SNMPproxy", "IOR:00dfdfdf0000001e49444c3a43616c6c6261636b2f457665

3	3	12/15/15 15:06:47 CST	BITS-1			1	NA	NA	MN	R	NA	LOS	Loss Of Signal	Receive	NEAR
2	2	12/15/15 15:06:47 CST	SYSTEM		NA	NA	NA	NA	MJ	R	true	SYSBOOT	System Reboot	NA	NEAR

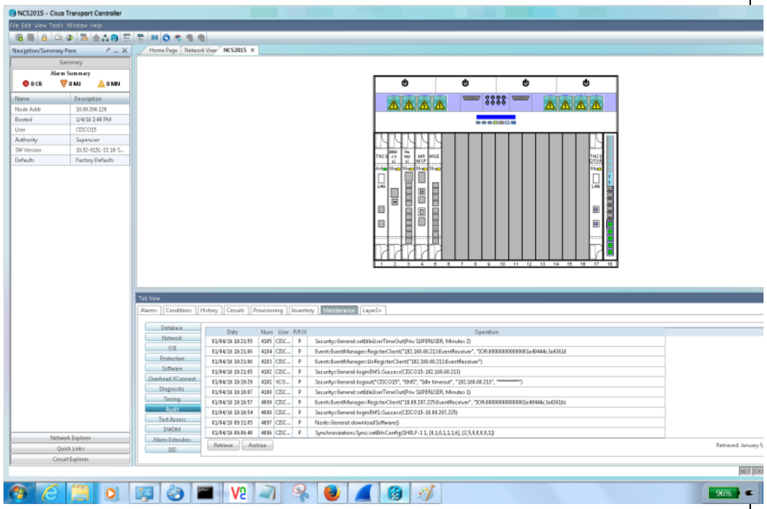
Date	Object	Eqpt Type	Slot	Port	Wavelength	Path Width	Sev	ST	SA	Cond	Description	Direction	Location
01/06/16 06:39:46 CST	SLOT-17	TNC	17	NA	NA	NA	MN	C	NA	AUTORESET	Automatic System Reset	NA	NEAR
01/06/16 06:39:28 CST	CHAN-2-2	200G-CK-...	2	2	AUTOPROV	NA	MN	C	NA	LO-RXPOWER	Facility Low Rx power	Receive	NEAR
01/06/16 06:39:26 CST	VCFAC-2-3	200G-CK-...	2	3	AUTOPROV	NA	CR	C	✓	OTUK-LOF	OTUk: Loss Of Frame	Receive	NEAR
01/06/16 06:39:22 CST	CHAN-2-2	200G-CK-...	2	2	AUTOPROV	NA	CR	R	✓	LOS-P	Incoming Payload Signal Absent	Receive	NEAR
01/06/16 06:39:18 CST	VCFAC-2-3	200G-CK-...	2	3	AUTOPROV	NA	CR	R	✓	OTUK-LOF	OTUk: Loss Of Frame	Receive	NEAR
01/06/16 06:39:18 CST	CHAN-2-2	200G-CK-...	2	2	AUTOPROV	NA	MN	R	NA	LO-RXPOWER	Facility Low Rx power	Receive	NEAR

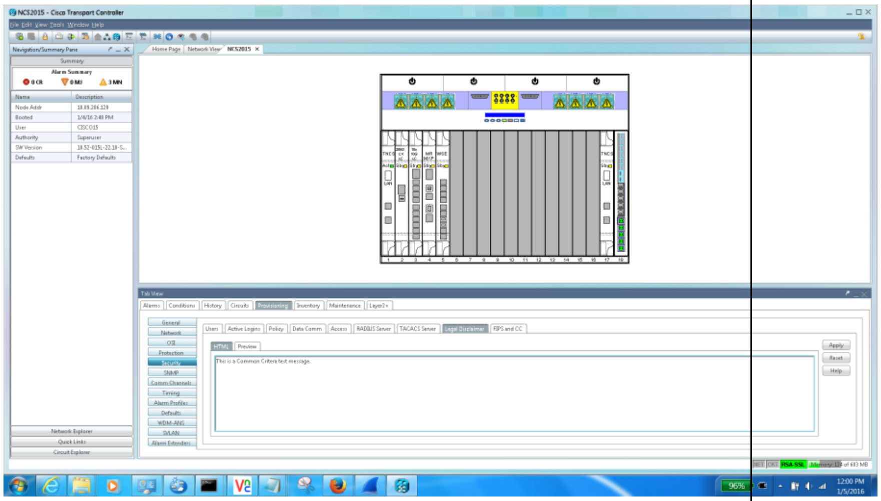
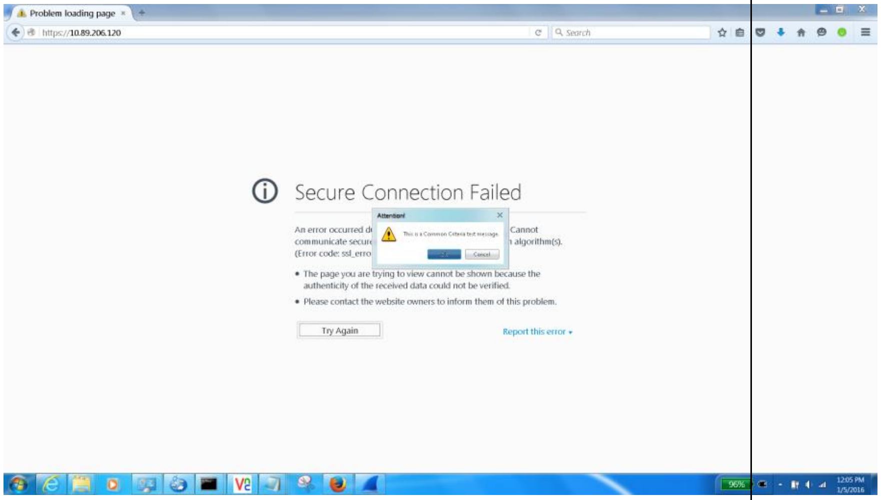
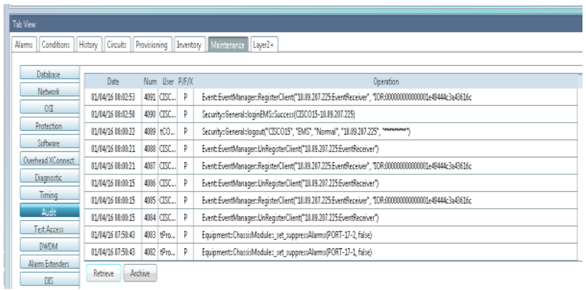
Date	Object	Eqpt Type	Slot	Unit	Port	Wavelength	Path Width	Sev	SA	Cond	Description	Direction	Location
01/06/16 06:39:22 CST	CHAN-2-2	200G-CK-...	2		2	AUTOPROV	NA	CR	✓	LOS-P	Incoming Payload Signal Absent	Receive	NEAR
01/06/16 06:36:43 CST	SYNC-NE		NA		NA	NA	NA	NA	NA	FRNGSYNC	Free Running Synchronization Mode	NA	NEAR
01/06/16 06:36:39 CST	SLOT-5	WSE	5		NA	NA	NA	NA	NA	CLDRESTART	Cold Restart	NA	NEAR
01/06/16 06:36:39 CST	SLOT-4	MR-MXP	4		NA	NA	NA	NA	NA	CLDRESTART	Cold Restart	NA	NEAR

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_CKM.1	None	None	None
FCS_CKM._EXT.4	None	None	None
FCS_COP.1(1)	None	None	None
FCS_COP.1(2)	None	None	None
FCS_COP.1(3)	None	None	None
FCS_COP.1(4)	None	None	None
FCS_RBG_EXT.1	None	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.	**Open and close HTTPS session:** 4122 01/04/16 12:45:13 Security::General::loginEMS::Success(CISCO15-10.89.207.225) 0 P CISCO15 4123 01/04/16 12:45:15 Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:0000000000000001e49444c3a43616c 1 P CISCO15 4124 01/04/16 12:47:28 Event::EventManager::UnRegisterClient("10.89.207.225:EventReceiver") 1 P CISCO15 4125 01/04/16 12:47:28 Security::General::logout("CISCO15", "EMS", "Normal", "10.89.207.225", "*********") 1 P tCORBA **Failure to establish an HTTPS session:** 251 01/31/15 18:13:27 Security::General::loginEMS::Fail(Password)(CISCO15-10.89.207.225) 0 F CISCO15
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS Session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes	251 01/31/15 18:13:27 Security::General::loginEMS::Fail(Password)(CISCO15-10.89.207.225) 0 F CISCO15

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
		and failures.	
FDP_RIP.2	None	None	
FIA_PMG_EXT.1	Administrative Actions: Setting length requirement for passwords.	None.	259 01/31/15 18:27:59 Security::General::setPasswordCharsRule(Rule = 0) 1 P CISCO15
FIA_UIA_EXT.1	All use of the identification and authentication mechanism. Administrative Actions: Logging into TOE.	Provided user identity, origin of the attempt (e.g., IP address).	Same as FCS_HTTPS
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	Same as FCS_HTTPS
FIA_UAU.7	None	None	
FMT_MTD.1	None.	None	
FMT_SMF.1	None.	None	
FMT_SMR.2	None.	None	255 01/31/15 18:16:29 Security::General::setUserSecurityLevel("bad3", level = MAINTENANCE) 1 P CISCO15
FPT_SKP_EXT.1	None.	None	
FPT_APW_EXT.1	None	None	
FPT_STM.1	Changes to the time. Administrative Actions: Changes to NTP settings. Manual changes to the system	The old and new values for the time. Origin of the attempt (e.g., IP address).	120 01/29/15 00:14:22 Node::General::setTime(11:33:11, 2015/1/30 dst=0) 1 P CISCO15

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	time.		
FPT_TUD_EXT.1	Initiation of update. Administrative Actions: Software updates	No additional information.	17 08/28/14 12:38:14 Node::General::downloadSoftware() 1 F CISCO15
FPT_TST_EXT.1	None	None	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session. Administrative Actions: Specifying the inactivity time period.	No additional information.	4106 01/04/16 12:26:47 Event::AuditTrailArchiveSession::complete(true) 1 P CISCO15 4107 01/04/16 12:27:02 Security::General::setIdleUserTimeOut(Priv SUPERUSER, Minutes 15) 1 P CISCO15 4108 01/04/16 12:27:10 Event::EventManager::UnRegisterClient("10.89.207.225:EventReceiver") 1 P CISCO15 4109 01/04/16 12:27:10 Security::General::logout("CISCO15", "EMS", "Normal", "10.89.207.225", "*********") 1 P tCORBA 4110 01/04/16 12:30:44 Security::General::loginEMS::Success(CISCO15-10.89.207.225) 0 P CISCO15 4111 01/04/16 12:30:46 Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:0000000000000001e49444c3a43616c 1 P CISCO15 4112 01/04/16 12:31:30 Security::General::setIdleUserTimeOut(Priv SUPERUSER, Minutes 1) 1 P CISCO15 4113 01/04/16 12:32:48 Security::General::logout("CISCO15", "EMS", "Idle timeout", "192.168.68.213", "*********") 1 P tCORBA 4114 01/04/16 12:32:55 Security::General::loginEMS::Success(CISCO15-192.168.68.213) 0 P CISCO15 4115 01/04/16 12:32:55 Event::EventManager::UnRegisterClient("192.168.68.213:EventReceiver") 1 P CISCO15

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			4116 01/04/16 12:32:55 Event::EventManager::RegisterClient("192.168.68.213:EventReceiver", "IOR:000000000000001e49444c3a43616 1 P CISCO15 4117 01/04/16 12:33:49 Security::General::setIdleUserTimeOut(Priv SUPERUSER, Minutes 2) 1 P CISCO15  NCS2015 - Cisco Transport Controller Name / Description: Node Addr 10.89.206.128; Booted 1/4/16 2:48 PM; User CISCO15; Authority Superuser; SW Version 10.52-015L-22.18-S...; Defaults Factory Defaults Date / Num / User / P/F/X / Operation 01/04/16 10:21:55 4185 CISC... P Security::General::setIdleUserTimeOut(Priv SUPERUSER, Minutes 2) 01/04/16 10:21:06 4184 CISC... P Event::EventManager::RegisterClient("192.168.68.213:EventReceiver", "IOR:000000000000001e49444c3a43616 01/04/16 10:21:06 4183 CISC... P Event::EventManager::UnRegisterClient("192.168.68.213:EventReceiver") 01/04/16 10:21:05 4182 CISC... P Security::General::loginEMS::Success(CISCO15-192.168.68.213) 01/04/16 10:19:29 4181 tCO... P Security::General::logout("CISCO15", "EMS", "Idle timeout", "192.168.68.213", "*********") 01/04/16 10:18:07 4180 CISC... P Security::General::setIdleUserTimeOut(Priv SUPERUSER, Minutes 1) 01/04/16 10:16:57 4099 CISC... P Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c 01/04/16 10:16:54 4098 CISC... P Security::General::loginEMS::Success(CISCO15-10.89.207.225) 01/04/16 09:31:05 4097 CISC... P Node::General::downloadSoftware() 01/04/16 09:06:40 4096 CISC... P Synchronization::Sync::setBitsConfig(SHELF-1 1, [0,1,0,1,1,1,6], [2,5,0,0,0,0,1])
FTA_SSL.3	The termination of a remote session by the session locking mechanism. Administrative Actions: Specifying the inactivity time period.	No additional information.	Same as FTA_SSL_EXT.1
FTA_SSL.4	The termination of an interactive session.	No additional information.	3657 01/04/16 08:39:52 Security::General::logout("CISCO15", "EMS", "Normal", "10.152.21.130", "*********") 1 P tCORBA
FTA_TAB.1	Administrati	None	4161 01/05/16 06:43:22 Security::General::setDisclaimer() 1 P CISCO15

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	ve Action: Configuring the banner displayed prior to authentication.		 
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.	

NCS2015 - Cisco Transport Controller

Alarm Summary: 0 CR 0 MJ 3 MN

Name	Description
Node Addr	10.89.206.128
Booted	1/4/16 2:48 PM
User	CISCO15
Authority	Superuser
SW Version	10.52-015L-22.18-S...
Defaults	Factory Defaults

Provisioning > Security > Legal Disclaimer > HTML:

This is a Common Criteria test message.

Problem loading page

https://10.89.206.120

Secure Connection Failed

An error occurred d... Cannot communicate secure... ...algorithm(s). (Error code: ssl_erro...

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Attention!

This is a Common Criteria test message.

Tab View

Date	Num	User	P/F/X	Operation
01/04/16 08:02:53	4091	CISC...	P	Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c
01/04/16 08:02:50	4090	CISC...	P	Security::General::loginEMS::Success(CISCO15-10.89.207.225)
01/04/16 08:00:22	4089	tCO...	P	Security::General::logout("CISCO15", "EMS", "Normal", "10.89.207.225", "*******")
01/04/16 08:00:21	4088	CISC...	P	Event::EventManager::UnRegisterClient("10.89.207.225:EventReceiver")
01/04/16 08:00:21	4087	CISC...	P	Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c
01/04/16 08:00:15	4086	CISC...	P	Event::EventManager::UnRegisterClient("10.89.207.225:EventReceiver")
01/04/16 08:00:15	4085	CISC...	P	Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c
01/04/16 08:00:15	4084	CISC...	P	Event::EventManager::UnRegisterClient("10.89.207.225:EventReceiver")
01/04/16 07:58:43	4083	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-2, false)
01/04/16 07:58:43	4082	tPro...	P	Equipment::ChassisModule::_set_suppressAlarms(PORT-17-1, false)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
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.	184 01/30/15 18:54:55 Event::EventManager::UnRegisterClient("10.89.207.225:EventReceiver") 1 P CISCO15 185 01/30/15 18:54:55 Security::General::logout("CISCO15", "EMS", "Normal", "10.89.207.225", "*********") 1 P tCORBA 186 01/30/15 19:24:03 Security::General::loginEMS::Success(CISCO15-10.89.207.225) 0 P CISCO15 187 01/30/15 19:24:06 Event::EventManager::RegisterClient("10.89.207.225:EventReceiver", "IOR:000000000000001e49444c3a43616c 1 P CISCO15

ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 20: 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
[ERRATA#3]	Security Requirements for Network Devices Errata #3, 3 November 2014
[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 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