Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS

Common Criteria Security Target

Version 2.0

17 March 2017

EDCS – 1513388

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

Table of Contents

List of Tables

List of Figures

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
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS	The proprietary operating system developed by Cisco Systems.
IoT	Internet of Things
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Services Digital Network
IT	Information Technology
MAC	Media Access Control
NDcPP	collaborative Network Device Protection Profile
NVRAM	Non-volatile random access memory, specifically the memory in the switch where the configuration parameters are stored.
OS	Operating System
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SM	Service Module
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol

Acronyms / Abbreviations	Definition
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

Terminology

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer router/switch	Another router/switch on the network that the TOE interfaces with
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another switch/router.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

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 IoT Industrial Ethernet and Connected Grid Switches running IOS (IE2K, IE4K, IE5K and CGS). 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 IoT Industrial Ethernet and Connected Grid Switches running IOS
ST Version	2.0
Publication Date	17 March 2017
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS
TOE Hardware Models	IE2000 Series, IE4000 Series, IE4010 Series, IE5000 Series and 2500 Series CGS
TOE Software Version	IOS 15.2(4)E
Keywords	Audit, Authentication, Encryption, Protection, Switch, Traffic

1.2 TOE Overview

The Cisco IE2000 Series, IE4000 Series, IE4010 Series, IE5000 Series and 2500 Series CGS running IOS 15.2(4)E (herein after referred to as IoT Industrial Ethernet and Connected Grid Switches, IE2K, IE4K, IE5K and CGS or TOE). The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities. The TOE includes the hardware models as defined in Table 3 in Section 1.1.

Cisco IOS software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this Security Target only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 TOE logical scope below.

1.2.1 TOE Product Type

The Cisco IE2K, IE4K, IE5K and CGS are switching and routing platforms that provide connectivity and security services onto a single, secure device. These switches offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers.

The Cisco IE2K, IE4K, IE5K and CGS are single-device security and switching solutions for protecting the network.

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
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators.
Management Workstation	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 over IPsec secured connection. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
NTP Server	Yes	The TOE supports communications with an NTP server to synchronize date and time.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages over IPsec.

1.3 TOE DESCRIPTION

This section provides an overview of the IoT Industrial Ethernet and Connected Grid Switches running IOS Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following: IE2000 Series, IE4000 Series, IE4010 Series, IE5000 Series and 2500 Series CGS. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS 15.2(4)E.

The IoT Industrial Ethernet and Connected Grid Switches running IOS that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The IoT Industrial Ethernet and Connected Grid Switches running IOS primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation.
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program).
- USB port (v2.0) (note, none of the USB devices are included in the TOE).
    - Type A for Storage, all Cisco supported USB flash drives.
    - Type mini-B as console port in the front.
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.

- Non-volatile random-access memory (NVRAM) is used to store router configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100/1000 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

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

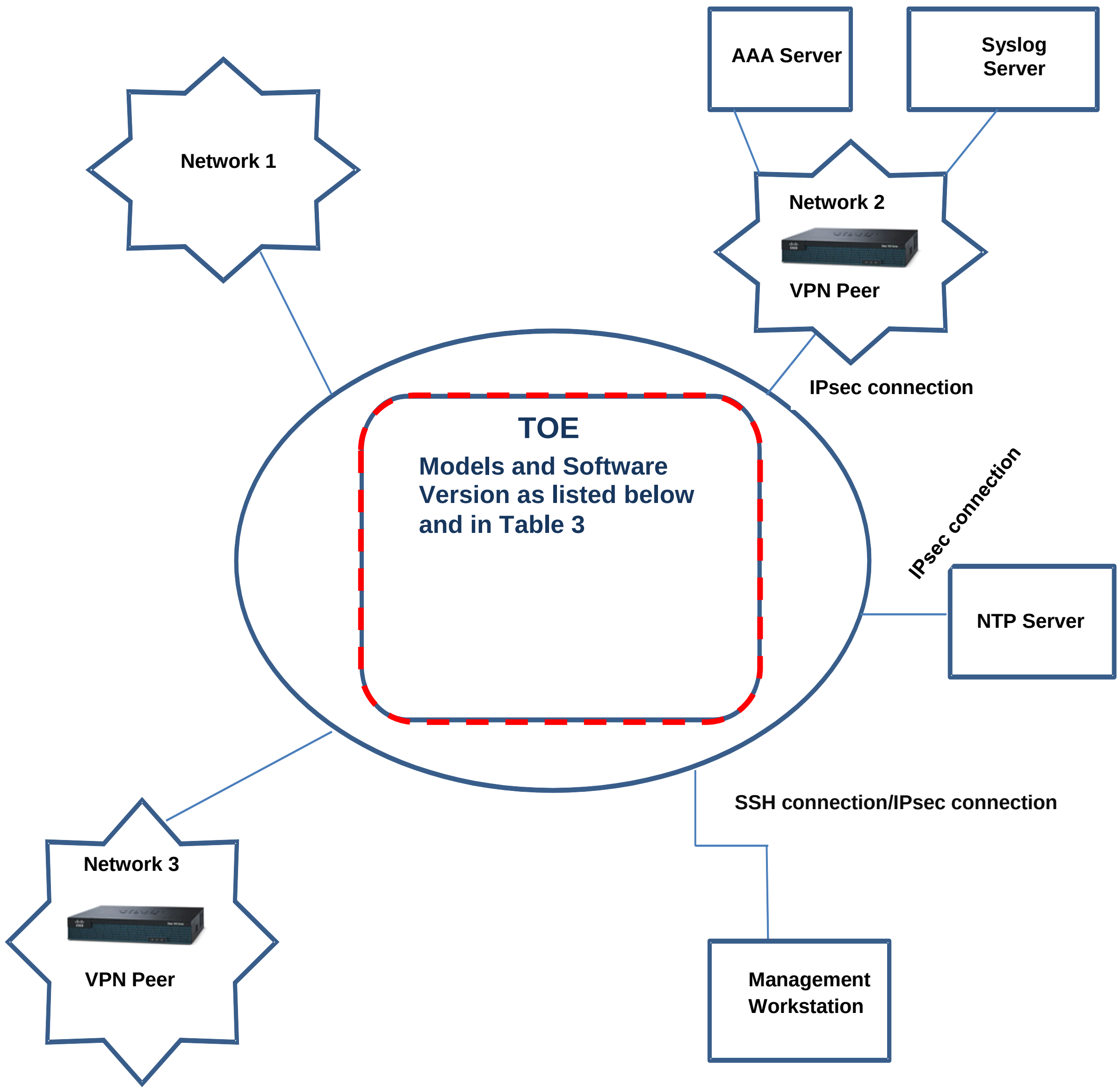

Figure 1 TOE Example Deployment

The previous figure includes the following:

- Identifies the TOE Models
  - Cisco IE2000 Series, IE4000 Series, IE4010 Series, IE5000 Series and 2500 Series CGS running Cisco IOS 15.2(4)E
- The following IT entities are considered to be in the IT Environment:
  - VPN Peers (2)
  - Management Workstation
  - Authentication Server
  - NTP Server
  - Syslog Server

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco IOS software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the IoT Industrial Ethernet and Connected Grid Switches running IOS is to be remotely administered, then the management station must be connected to an internal network, SSHv2 may be used to connect to the switch, though it must be over an IPsec secured connection. A syslog server is also used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the switch models as follows: IE2000 Series, IE4000 Series, IE4010 Series, IE5000 Series and 2500 Series CGS running Cisco IOS 15.2(4)E. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the http://cisco.com web site. The TOE is comprised of the following physical specifications as described in Table 5 below:

Table 5 Hardware Models and Specifications

Hardware	Processor	Software	Picture	Size	Power	Interfaces
IE2000 (IE-2000-16TC-G-E IE-2000-4TS-G-B IE-2000-16PTC-G-E IE-2000-16TC-L IE-2000-8TC-L)	Yeti-3 - PowerPC 405 RISC core	Cisco IOS 15.2(4)E		• IE-2000 6 ports (copper downlinks) chassis: 5.1"H x 2.95"W x 4.51"D in (130mm H x 74.9mm W x 115mm D) • IE-2000 6 ports (SFP downlinks) chassis: 5.1"H x 3.15"W x 4.51"D in (130mm H x 80mm W x 115mm D) • IE-2000 10 ports short chassis: 5.1"H x 3.6"W x 4.51"D (130mm H x 91.4mm W x 115mm D) • IE-2000 10 ports long chassis: 5.1"H x 3.6"W x 5.26"D (130mm H x 91.4mm W x 134mm D) • IE-2000 18-20 ports chassis: 5.1"H x 5.0"W x 5.26"D (130mm H x 127mm	dual-input DC power supply	four, eight or sixteen 10/100base-T Ethernet ports fixed-configuration • IE-2000-4* with a total of 6 ports (6 copper, 4 copper plus 2 SFP, or 6 fiber), RJ45 port (4FE, 6 FE, 4FE/2GE) SFP port (2FE, 2GE, 4FE/2GE)) • IE-2000-8* with a total of 10 ports (8 copper plus 2 combo ports (copper or SFP), RJ45 (8 FE), Combo ports (2 FE, 2 GE) SFP ports (2 FE)) • IE-2000-16* with a total of 20 ports (16 copper plus 2 combo ports or 16 copper ports (including 4 PoE/PoE+ ports) plus 2 combo ports), RJ45 ports (16 FE), Combo ports (2 GE) SFP ports (2 FE))

Hardware	Processor	Software	Picture	Size	Power	Interfaces
				W x 134mm D)		

IE4000 (IE-4000-4GC4GP4G-E IE-4000-16GT4G-E IE-4000-8GT8GP4G-E IE-4000-4GS8GP4G-E)	Applied Micro - APM86392 dual core PPC465	Cisco IOS 15.2(4)E		All IE 4000 models have the following dimensions: 6.12 x 6.12 x 5.09 in. (155.4 x 155.4 x 129.2 mm)	High-Density Industrial Power over Ethernet (PoE)	eight , twelve, sixteen, twenty port models:
						• All models have 4 GE combo uplink ports
						• Additional ports include additional combo ports, copper, fiber and PoE/PoE+ Ports
						  ◦ All copper Gigabit Ethernet interfaces support speed negotiation to 10/100/1000 mbps and duplex negotiation.
						  ◦ All copper Fast Ethernet interfaces support speed negotiation to 10/100 mbps and duplex negotiation

IE4010 (IE-4010-16S12P, E-4010-4S24P)	Applied Micro - APM86392 dual core PPC465	Cisco IOS 15.2(4)E	 (picture is of both models; one	All IE 4000 models have the following dimensions: 1.75 x 17.5 x 14.0 in. (4.45 x 44.5 x 35.6 cm),	Both models support PWR-RGD-AC-DC-H 150W AC 100-240V/2.0A 50-60Hz or DC 100-	• IE-4010-16S12P has 28 total ports, 4 SFP (100MB/1G) Uplinks, 12 (100/1000M) SFP Fiber ports and 12 (10/100/1000M) Copper 10/100/1000 PoE/PoE+ Ports • IE-4010-4S24P has 28 total ports, 4 SFP (100MB/1G) Uplinks

Hardware	Processor	Software	Picture	Size	Power	Interfaces
			sitting on top of the other)	1 RU (rack unit) height)	250V/2.0A AC 85-264V or DC 88-300V and PWR-RGD-LOW-DC-H 150W DC 24-60V/10A DC 18-75V with PoE/PoE+ Support	and 24 (10/100/1000M) Copper 10/100/1000 PoE/PoE+ Ports
IE5000 (IE-5000-12S12P-10G, IE-5000-16S12P)	Applied Micro - APM86392 dual core PPC465	Cisco IOS 15.2(4)E		1.75 x 17.5 x 14.0 in. (4.45 x 44.5 x 35.6 cm), 1RU (rack unit) height	PWR-RGD-AC-DC-H 150W AC 100-240V/2.0A 50- 60Hz or DC 100-250V/2.0A AC 85-264V or DC 88-300V and PWR-RGD-LOW-DC-H 150W DC 24-60V/10A DC 18-75V with PoE/PoE+ Support	• IE-5000-12S12P-10G has 28 total ports, 4 SFP/SFP+ (1G/10G) Uplinks, 12 (FE/GE) SFP Fiber ports and 12 (10/100/1000M) Copper 10/100/1000 PoE/PoE+ Ports • IE-5000-12S12P has 28 total ports, 4 SFP/SFP+ (1G) Uplinks, 12 (FE/GE) SFP Fiber ports and 12 (10/100/1000M) Copper 10/100/1000 PoE/PoE+ Ports
CGS2500 (CGS-2520-16S-8PC CGS-2520-24TC)	Yeti-3 - PowerPC 405 RISC core	Cisco IOS 15.2(4)E	 (picture is of both models; one sitting on top of the other)	1.75 x 17.5 x 14.0 in. (4.45 x 44.5 x 35.6 cm)	Both models also include PWR-RGD-LOW-DC: Low DC (24/48V) power supply module or the PWR-RGD-AC-DC: High AC/DC (88-300VDC/85-264VAC) power	• Cisco CGS-2520-24TC: Ethernet switch with 24 10/100BaseTX ports and two dual-purpose Gigabit Ethernet uplinks, two 10/100/1000BaseTX ports and two 100/1000 Small Form-Factor Pluggable (SFP) ports on board. The user can select two fiber ports, two copper ports, or a combination of fiber and copper ports. • Cisco CGS-2520-16S-8PC: Ethernet switch with 16 Fast Ethernet (FE) SFP ports, eight 10/100BaseTX/PoE

Hardware	Processor	Software	Picture	Size	Power	Interfaces
					supply module:	ports, and two dual-purpose Gigabit Ethernet uplinks.

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.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco IoT Industrial Ethernet and Connected Grid Switches running IOS provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of an IPsec SA; modifications to the group of users that are part of the authorized administrator roles; all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, maximum sessions being exceeded, termination of a remote session and attempts to unlock a termination session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE can be configured to block new permit actions.

The logs can be viewed on the TOE using the appropriate IOS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco IE2K, IE4K, IE5K and CGS security functionality. This IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) has been validated for conformance to the requirements of FIPS 140-2 Level 1 certificate #2388 (see Table 6 for algorithm certificate references).

Table 6 FIPS References

Algorithm	CAVP Cert. #
AES	2783, 2817, 3278
SHS (SHA-1, 256, 512)	2338, 2361
HMAC SHA-1 (256 and 512)	1764
DRBG	481
RSA	1471

While the algorithm implementations listed in the preceding table were not tested on the exact processor installed within the IE2K, IE4K, IE5K and CGS, the algorithm certificates are applicable to the TOE based on the following,

- The cryptographic implementation which is tested is identical (unchanged) to the cryptographic implementation on the IE2K, IE4K, IE5K and CGS.
- The cryptographic implementation does not depend on hardware for cryptographic acceleration i.e. there is no hardware specific cryptographic dependency. The cryptographic algorithms are implemented completely in software.
- The IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5
- (Firmware Version: Rel 5) for the cryptographic operations.
- This is consistent with the guidance provided in *Frequently Asked Questions for NIAP Policy #5*, 12 June 2015 allowing portability amongst platforms as long as no software modification is required. See policy posted at https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/FAQ_Policy_5.pdf.

The IE2K, IE4K, IE5K and CGS platforms contain the following processor,

- The IE2K and CGS contains the Yeti-3 - PowerPC 405 RISC core
- The IE4K and IE5K contains the Applied Micro - APM86392 dual core PPC465

The TOE provides cryptography in support of VPN connections that includes remote administrative management. The cryptographic services provided by the TOE are described in Table 7 below

Table 7 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.

Cryptographic Method	Use within the TOE
RSA/DSA Signature Services	Used in IPsec session establishment.
SP 800-90 RBG	Used in IPsec session establishment.
SHS	Used to provide IPsec traffic integrity verification
AES	Used to encrypt IPsec session traffic. .

1.6.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate 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 as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSHv2 session interfaces over IPsec secured connection. The TOE supports use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

1.6.4 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 SSHv2 session over IPsec secured connection or via a local console connection. The TOE provides the ability to securely manage:

- The TOE locally and remotely;
- Configuration of warning and consent access banners;
- Configuration of session inactivity thresholds;
- Updates of the TOE software;
- Configuration of the audit functions of the TOE;
- Configuration of the TOE provided services;
- Configuration of the cryptographic functionality of the TOE;

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

1.6.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco IOS is not a general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS 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. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of Authorized Administrator software.

1.6.6 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 display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.6.7 Trusted path/Channels

The TOE allows trusted channels to be established to itself from remote administrators that is SSHv2 sessions over IPsec secured connection, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet for management purposes.	Telnet passes authentication credentials in clear text. SSHv2 over IPsec secured connection is to be used instead of telnet.
SNMP for management proposes and protocol	SNMP protocol and server was not evaluated and must be disabled
HTTP and HTTPS protocol and servers	HTTP and HTTPS protocol and servers were not evaluated and must be disabled

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 1.0.

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: July 2009. For a listing of Assurance Requirements claimed see section 5.4.

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 9 below:

Table 9 Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices (NDcPP)	1.0	February 27, 2015

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:

- collaborative Protection Profile for Network Devices (NDcPP), Version 1.0

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 collaborative Protection Profile for Network Devices, Version 1.0 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 NDcPPv1.0, 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 NDcPPv1.0, 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 the NDcPPv1.0.

3 SECURITY PROBLEM DEFINITION

This section 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 10 TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

3.2 Threats

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

Table 11 Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat	Threat Definition
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

3.3 Organizational Security Policies

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

Table 12 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 section 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.

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v1.0 does not define any security objectives for the TOE.

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 13 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 made by PP author: Indicated with **bold text** and ~~strikethroughs~~, if necessary;
- Selection: Indicated with <u>underlined</u> text;
- Assignment within a Selection: Indicated with <u>*italicized and underlined text*</u>;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3) and/or by adding a string starting with "/"..
- Where operations were completed in the NDcPP itself, the formatting used in the NDcPP 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 NDcPPv1.0.

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 14 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	Security audit event storage
	FAU_STG.1	Security Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.2	Cryptographic Key Establishment (Refined)
	FCS_CKM.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1(3)	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(4)	Cryptographic Operation (Keyed Hash Algorithm)

Class Name	Component Identification	Component Name
	FCS_IPSEC_EXT.1	IPSEC Protocol
	FCS_RBG_EXT.1	Random Bit Generation
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: Security management	FMT_MOF.1(1)/TrustedUpdate	Management of security functions behaviour
	FMT_MTD.1	Management of 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	Trusted update
	FPT_TST_EXT.1	TSF Testing (Extended)
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Trusted Channel
	FTP_TRP.1	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 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 shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrator actions comprising:

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
- *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- *Starting and stopping services (if applicable)*
- [no other actions, [*no other uses*]];

d) [*Specifically defined auditable events listed in* Table 15].

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 15].

Table 15 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
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_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_RBG_EXT.1	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.
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1(1)/Trusted Update	Any attempt to initiate a manual update	None.
FMT_MTD.1	All management activities of TSF data	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	No additional information.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
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.

5.2.1.2 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.

5.2.1.3 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 according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall [<u>overwrite previous audit records according to the following rule:</u> [*when allotted space has reached its threshold*], [no *other action*]] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation (Refined)

FCS_CKM.1.1 Refinement: The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm:[

- <u>RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3</u>

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

5.2.2.1 FCS_CKM.2 Cryptographic Key Establishment (Refined)

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- <u>RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”</u>**;**

] ~~that meets the following: [assignment: list of standards]~~.

5.2.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- For volatile memory, the destruction shall be executed by a single direct overwrite [consisting of zeroes] followed by a read-verify.
  - If the read-verification of the overwritten data fails, the process shall be repeated again.
- For non-volatile EEPROM, the destruction shall be executed by a single, direct overwrite consisting of a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), followed by a read-verify.
  - If the read-verification of the overwritten data fails, the process shall be repeated again.
- For non-volatile flash memory, the destruction shall be executed by [a single, direct overwrite consisting of zeroes] followed by a read-verify.
  - If the read-verification of the overwritten data fails, the process shall be repeated again.
- For non-volatile memory other than EEPROM and flash, the destruction shall be executed by overwriting three or more times with a random pattern that is changed before each write.

]
that meets the following: No Standard.

5.2.2.3 FCS_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1(1) Refinement: The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [CBC] mode and cryptographic key sizes [128 bits, 256-bits] that met the following: *AES as specified in ISO 18033-3*, [CBC as specified in ISO 10116].

5.2.2.4 FCS_COP.1(2) Cryptographic Operation (Signature Generation and Verification)

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

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits*],

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

].

5.2.2.5 FCS_COP.1(3) Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1(3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-512] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ that meet the following: ISO/IEC 10118-3:2004.

5.2.2.6 FCS_COP.1(4) Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1(4) The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512] and cryptographic key sizes [**160-bit, 256-bit, 512-bit**] **and message digest sizes** [160, 256, 512] **bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

5.2.2.7 FCS_IPSEC_EXT.1 Explicit: IPSEC

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement transport mode and [tunnel mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602) and [no other algorithms] together with a Secure Hash Algorithm (SHA)-based HMAC.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [no other RFCs for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and [no other algorithm].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that

- IKEv1 Phase 1 SA lifetimes can be configured by an Security Administrator based on

[

  - length of time, where the time values can configured within [**1-24**] hours;

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that

- IKEv1 Phase 2 SA lifetimes can be configured by an Security Administrator based on

[

  - number of bytes
  - length of time, where the time values can configured within [**1-8**] hours;

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [320 (for DH Group 14)] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1] exchanges of length [320 (for DH Group 14)].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [no other DH groups].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel to peers with valid certificates.

5.2.2.8 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [**2**] hardware and software based noise source and] with minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1

5.2.3 Identification and authentication (FIA)

5.2.3.1 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;

5.2.3.2 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;
- [any network packets as configured by the authorized administrator may flow through the switch].

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.

5.2.3.3 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [*remote password-based authentication via RADIUS*] to perform administrative user authentication.

5.2.3.4 IA_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.

5.2.3.5 FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5759].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.6 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [IPsec], and [*no additional uses*].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [allow the administrator to choose whether to accept the certificate in these cases].

5.2.3.7 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security management (FMT)

5.2.4.1 FMT_MOF.1(1)/TrustedUpdate Management of security functions behaviour

FMT_MOF.1.1(1)/TrustedUpdate The TSF shall restrict the ability to enable the functions *to perform manual update* to *Security Administrators*.

5.2.4.2 FMT_MTD.1 Management of TSF Data

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

5.2.4.3 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 configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;*
- [
  - Ability to configure audit behavior;
  - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
  - Ability to configure the cryptographic functionality;

].

5.2.4.4 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security 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

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

5.2.5 Protection of the TSF (FPT)

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

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

5.2.5.2 FPT_APW_EXT.1: 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.

5.2.5.3 FPT_STM.1 Reliable time stamps

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

5.2.5.4 FPT_TST_EXT.1: TSF Testing (Extended)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [<u>during initial start-up (on power on)</u>] to demonstrate the correct operation of the TSF: [

- *Power-on Self-Tests:*
  - *Route Processor*
    - *Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, RNG KAT, RSA KAT*
    - *Firmware Integrity Test*
  - *Embedded Services Processor*
    - *Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, RNG KAT, RSA KAT*
    - *Firmware Integrity Test*
- *Conditional Self-Tests:*
  - *Route Processor*

    - *Continuous Random Number Generator test for the FIPS-approved RNG*
    - *Continuous Random Number Generator test for the non-approved RNG*
    - *Pair-Wise Consistency Test*
    - *Conditional Bypass Test*
  - *Embedded Services Processor*
    - *Continuous Random Number Generator test for the FIPS-approved RNG*
    - *Continuous Random Number Generator test for the non-approved RNG*
    - *Conditional Bypass Test*
- *Powerup bypass test*
- *Software integrity test*

].

5.2.5.5 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software as well as the most recently installed version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide a means to authenticate firmware/software updates to the TOE using a [published hash] prior to installing those updates.

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.2.6.2 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*].

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 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.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1: The TSF shall **be capable of using [<u>IPsec</u>] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [<u>authentication server</u>]** 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 **<u>the TSF, or the authorized IT entities</u>** to initiate communication via the trusted channel.

FTP_ ITC.1.3 The TSF shall initiate communication via the trusted channel for [*remote authentication with RADIUS servers (over IPsec), audit storage with syslog server (over IPsec) and time synchronization with NTP server (over IPsec)*].

5.2.7.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **be capable of using [IPsec] to** provide a communication path between itself and **<u>authorized remote administrators</u>** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from <u>disclosure</u> *and provides detection of modification of the channel data*.

FTP_TRP.1.2 The TSF shall permit **<u>remote administrators</u>** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **<u>initial administrator authentication and all remote administration actions</u>**.

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv1.0

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv1.0. As such, the NDcPPv1.0 SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPPv1.0 which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 16: 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

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv1.0. As such, the NDcPPv1.0 SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 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 17 Assurance Measures

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

Component	How requirement will be met
ALC_CMS.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.
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 section identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 18 How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated (e.g. user identity, MAC address, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. The audit trail consist of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes [at least] all of the required information. Additional information can be configured and included if desired. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc.; all of which are described in the Guidance documents and IOS CLI. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.

TOE SFRs	How the SFR is Met
	The logs can be saved to flash memory so records are not lost in case of failures or restarts. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the switch is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information; switch functionality is not affected. To configure the TOE to send audit records to a syslog server, the 'set logging server' command is used. A maximum of three syslog servers can be configured. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The audit records are transmitted using IPsec tunnel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established. The FIPS crypto tests performed during startup, the messages are displayed only on the console. Once the box is up and operational and the crypto self-test command is entered, then the messages would be displayed on the console and will also be logged. For the TSF self-test, successful completion of the self-test is indicated by reaching the log-on prompt. If there are issues, the applicable audit record is generated and displayed on the console.
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. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.
FAU_STG_EXT.1	The TOE is configured to export syslog records to a specified, external syslog server. The TOE protects communications with an external syslog server via IPsec. If the IPsec connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connectivity to the syslog server For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1	The TOE implements a random number generator for RSA key establishment schemes (conformant to NIST SP 800-56B).

TOE SFRs	How the SFR is Met
	The TOE can create a RSA public-private key pair, with a minimum RSA key size of 2048 bits. The TOE also supports larger RSA key size of 4096. The RSA key pair can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The key pair generation portions of "The RSA Validation System" for FIPS 186-2 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.
FCS_CKM.2	The TOE employs RSA-based key establishment used in cryptographic operations.
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use. The keys are destroyed by overwriting and verified through the command show crypto key mypubkey. Additionally, none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form. See 7 Annex A: Key Zeroizationfor more information on the key zeroization.
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described AES as specified in ISO 18033-3. AES is implemented in the following protocols: IPSEC and SSH. The relevant FIPS certificate numbers are listed in Table 6 FIPS References
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 186-3, "Digital Signature Standard". The relevant FIPS certificate numbers are listed in Table 6 FIPS References
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512 as specified in FIPS Pub 180-3 "Secure Hash Standard." For IKE (ISAKMP) hashing, administrators can select any of SHA-1, SHA-256, and/or SHA-512 (with key sizes and message digest sizes of 160, 256, and 512 bits respectively) to be used with remote IPsec endpoints. Both SHA-1 and SHA-256 hashing are used for verification of software image integrity. The relevant FIPS certificate numbers are listed in Table 6 FIPS References
FCS_COP.1(4)	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 (with key sizes and message digest sizes of 160, 256, and 512 bits respectively) as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"
FCS_IPSEC_EXT.1	The IPsec implementation provides both VPN peer-to-peer and VPN client to TOE capabilities. The VPN peer-to-peer tunnel allows for example the TOE and another router to establish an IPsec tunnel to secure the passing of route tables (user data). Another configuration in the peer-to-peer configuration is to have the TOE be set up with an IPsec tunnel with a VPN peer to secure the session between the TOE and syslog server. The VPN client to TOE configuration would be where a remote VPN client connects into the TOE in order to gain access to an authorized private network. Authenticating with the TOE would give the VPN client a secure IPsec tunnel to connect over the internet into their private network.

TOE SFRs	How the SFR is Met
	In addition to tunnel mode, which is the default IPsec mode, the TOE also supports transport mode, allowing for only the payload of the packet to be encrypted. If tunnel mode is explicitly specified, the router will request tunnel mode and will accept only tunnel mode. The TOE implements IPsec to provide both certificates and pre-shared key-based authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. Preshared keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The IKE protocols implement Peer Authentication using the RSA algorithm with X.509v3 certificates or preshared keys. When certificates are used for authentication, the distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), • The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and • The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE supports IKEv1 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the 'crypto isakmp aggressive-mode disable' command. The TOE can be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using "lifetime" command. The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour, but it is configurable to 8 hours.

TOE SFRs	How the SFR is Met
	The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. The TOE provides AES-CBC-128, and AES-CBC-256 for encrypting the IKEv1 payloads. The administrator is instructed in the AGD to ensure that the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload. The TOE supports Diffie-Hellman Group 14 (2048-bit keys), in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, and the following corresponding key sizes (in bits) are used: 320 (for DH Group 14) bits. The DH group can be configured by issuing the following command during the configuration of IPsec: TOE-common-criteria (config-isakmp)# group 14 This selects DH Group 14 (2048-bit MODP) for IKE This sets the DH group offered during negotiations. The TOE generates the secret value 'x' used in the IKEv1 Diffie-Hellman key exchange ('x' in gx mod p) using the NIST approved DRBG specified in FCS_RBG_EXT.1 and having possible lengths of 320 bits. When a random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2128. The nonce is likewise generated using the AES-CTR DRBG. IPsec provides secure tunnels between two peers, such as two routers and remote VPN clients. An authorized administrator defines which packets are considered sensitive and should be sent through these secure tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers or between the TOE and remote VPN client. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per security protocol (AH or ESP). In the evaluated configuration only ESP will be configured for use. A crypto map (the Security Policy Definition (SPD)) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the router attempts to match the packet to the access list (acl) specified in that entry. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit acls would then flow through the IPsec tunnel and be classified as "PROTECTED". Traffic that does not match a permit crypto map acl and does not match a non-crypto permit acl on the interface would be DISCARDED. Traffic that does not match a permit acl in the crypto map, but does match a non-crypto permit acl would be allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic.

TOE SFRs	How the SFR is Met
	The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR and using cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA1, HMAC-SHA-256, and HMAC-SHA-512) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. In IOS the negotiations of the IKE SA adheres to configuration settings for IPsec applied by the administrator. For example in the first SA, the encryption, hash and DH group is identified, for the Child SA the encryption and the hash are identified. The administrator configures the first SA to be as strong as or stronger than the child SA; meaning if the first SA is set at AES 128, then the Child SA can only be AES128. If the first SA is AES256, then the Child SA could be AES128 or AES256. During the negotiations, if a non-match is encountered, the process stops and an error message is received.
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 by randomly poll the General Purpose Registers and capture entropy from it. This solution is available in the IOS 15.2(4)E or later FIPS/CC approved releases of the IOS images relating to the platforms mentioned above. All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed. Though related to this, the tests are part of the FIPS validation procedures for the DBRG and are part of the NIST validations for FIPS 140-2 for the products. Any initialization or system errors during bring-up or processing of this system causes a reboot as necessary to be FIPS compliant. Finally, the system will be zeroizing any entropy seeding bytes, which will not be available after the current collection.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters.

TOE SFRs	How the SFR is Met
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication and any network packets as configured by the authorized administrator may flow through the switch. Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 session over IPsec secured 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. The TOE provides a local password based authentication mechanism as well as RADIUS AAA server for remote authentication. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via SSHv2 session over IPsec secured connection. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FIA_X509_EXT.1 FIA_X509_EXT.2 FIA_X509_EXT.3	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections. The TOE supports the following methods to obtain a certificate from a CA: • Simple Certificate Enrollment Protocol (SCEP)—A Cisco-developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). • Imports certificates in PKCS12 format from an external server • IOS File System (IFS)—The switch uses any file system that is supported by Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. • Manual cut-and-paste—The switch displays the certificate request on the console terminal, allowing the administrator to enter the issued certificate on the console terminal; manually cut-and-paste certificate requests and certificates when there is no network connection between the switch and CA

TOE SFRs	How the SFR is Met
	• Enrollment profiles—The switch sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode certificate server (CS). • Self-signed certificate enrollment for a trust point Public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates can be stored in a specific location on the TOE. Certificates are stored to NVRAM by default; however, some switches do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates.. The certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. The administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates. To verify, the authorized administrator could 'show' the pki certificates and the pki trust points. The authorized administrator can also configure one or more certificate fields together with their matching criteria to match. Such as: • alt-subject-name • expires-on • issuer-name • name • serial-number • subject-name • unstructured-subject-name • valid-start This allows for installing more than one certificate from one or more CAs on the TOE. For example, one certificate from one CA could be used for SSH connections, while another certificate from another CA could be used for IPsec connections. However the default configuration is a single certificate from one CA that is used for all authenticated connections. The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the router and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE.

TOE SFRs	How the SFR is Met
	USB tokens provide for secure configuration distribution of the digital certificates and private keys. RSA operations such as on-token key generation, signing, and authentication, and the storage of Virtual Private Network (VPN) credentials for deployment can be implemented using the USB tokens. The use of CRL and OCSP is configurable and may be used for certificate revocation. The authorized administrator could use the revocation-check command to specify at least one method of revocation checking; CRL or OCSP. The authorized administer sets the trust point and its name, the OCSP url, the revocation-check method • crl --Certificate checking is performed by a CRL. This is the default option. • none --Certificate checking is ignored. • ocsp --Certificate checking is performed by an OCSP server. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. If the connection to determine the certificate validity cannot be established, the administrator is able to choose whether or not to accept the certificate.
FMT_MOF.1(1)/TrustedUpdate	The TOE does not provide automatic updates to the software version running on the TOE. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.
FMT_MTD.1	The TOE provides the ability for Security Administrators (a.k.a Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds and updates. Each of the predefined and administratively configured privilege level has a set of permissions that will grant them access to the TOE data, though with some privilege levels, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged levels. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged level equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. 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. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege.

TOE SFRs	How the SFR is Met
	In addition, network packets are permitted to flow, as configured by the authorized administrator, through the switch prior to the identification and authentication of an authorized administrator.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Security Administrators (a.k.a Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via SSHv2 session over IPsec secured connection, a terminal server, or at the local console. 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 CLI, as described above; • The ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users • The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold. • The ability to update the IOS software. The validity of the image is provided using SHA-256 and/or digital signature prior to installing the update • The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs • The ability to display the log on banner and to allow any network packets as configured by the authorized administrator may flow through the switch prior to the identification and authentication process • The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2
FMT_SMR.2	The TOE maintains Authorizer Administrators that include privileged and semi-privileged administrator roles to administer the TOE locally and remotely. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. Note: the levels are not theoretically hierarchical. 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.

TOE SFRs	How the SFR is Met
	The privilege 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 command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote authentication via SSH.
FPT_SKP_EXT.1 and FPT_APW_EXT.1	The TOE includes CLI command features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The command is the *password encryption aes* command used in global configuration mode. The command *service password-encryption* applies encryption to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords. The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additional, all pre-shared and symmetric keys are stored in encrypted form to prevent access. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage 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. The TOE can optionally be set to receive clock updates from an NTP server. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. This system clock is also used for cryptographic functions.
FPT_TUD_EXT.1	Authorized Administrator can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the software.Cisco.com. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE. Detailed instructions for how to do this verification are provided in the administrator guidance for this evaluation. Briefly, the software version and digital signature information for the TOE specific image can be displayed using the following commands: The administrator in privileged EXEC mode enters Switch# show version (this displays information about the Cisco IOS software version running on the TOE the ROM Monitor and Bootflash software versions, and the hardware configuration, including the amount of system memory Switch# show software authenticity running (displays software authenticity-related information for the current ROMmon and the Cisco IOS image file used for booting)

TOE SFRs	How the SFR is Met
	Switch# show software authenticity file {flash0:*filename* | flash1:*filename* | flash:*filename* | nvram:*filename* | usbflash0:*filename* | usbflash1:*filename*} (displays digital signature and software authenticity-related information for a specific image file.) Switch# show software authenticity keys (Displays the software public keys that are in storage with the key types for digitally signed Cisco software).
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, the Authorized Administrator will have to log into the CLI 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). Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms. Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing selftests and entering FIPS mode. In the event of a power-on self-test failure, the cryptographic module will force the IOS platform to reload and reinitialize the operating system and cryptographic module. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful. These tests include: • AES Known Answer Test - 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. • HMAC Known Answer Test - 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. • RNG/DRBG Known Answer Test - 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. • SHA-1/256/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly. • RSA Signature Known Answer Test (both signature/verification) - 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.

TOE SFRs	How the SFR is Met
	• Powerup bypass test - Involves testing correct operation providing crypto services when a switch takes place between bypass services and crypto services. In short the crypto series gets tested normally overtime a bypass occurs and the returns. AN example is AES known answer test gets run at start. Then the module moves to bypass crypto services. Then returns back to crypto devices and the AES known answer test gets immediately run. The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO.
FTA_SSL_EXT.1 and FTA_SSL.3	An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "session-timeout" setting applied to the console and virtual terminal (vty) lines. The configuration of the vty lines sets the configuration for the remote console access. The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period of time, the session will be locked and will require re-authentication to unlock the session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the "exec-timeout" setting.
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions.
FTA_TAB.1	Authorized administrators define a custom login banner that will be displayed at the CLI (local and remote) prior to allowing Authorized Administrator access through those interfaces.
FTP_ITC.1	The TOE protects communications with authorized IT entities with IPsec. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted IPsec session. The IPsec implementation allows for VPN vlient to TOE capabilities. The remote users are able to initiate IPsec communications with the TOE.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE.

Table 19: TOE Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in DRAM.	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	The function returns the value to the RP and then calls the function to perform the zeroization of the generated key pair (p_dh_kepair) and then calls the standard Linux free (without the poisoning). These values are automatically zeroized after generation and once the value has been provided back to the actual consumer. This key is stored in DRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
skeyid	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This information and keys are stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This information and keys are stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared	The function calls the free operation with the poisoning mechanism that overwrites the value with 0x0d. This key is stored in DRAM.	Zeroized using the following command: # no crypto isakmp key Overwritten with: 0x0d
IKE RSA Private Key	The operation uses the free operation with the poisoning mechanism that overwrites the value with 0x0d. (This function is used by the module when zeroizing bad key pairs from RSA Key generations.). This key is stored in NVRAM.	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x0d

Name	Description	Zeroization
IPsec encryption key	The function zeroizes an _ike_flow structure that includes the encryption and authentication keys. The entire object is overwritten by 0's using memset. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
IPsec authentication key	The function zeroizes an _ike_flow structure that includes the encryption and authentication keys. The entire object is overwritten by 0's using memset. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
RADIUS secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory. The password is stored in NVRAM.	Zeroized using the following command: # no radius-server key Overwritten with: 0x0d
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	The results zeroized using the poisioning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended. This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00
User Password	This is a Variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password
Enable Password (if used)	This is a Variable 15+ character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM.	Zeroized by overwriting with new password
RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device

8 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
[NDcPP]	collaborative Protection Profile for Network Devices, Version 1.0, 27 Feb 2015