



Cisco Aggregation Services Router (ASR) 1000 Series

Security Target

Version 0.7

17 October 2017

Table of Contents

1	SECURITY TARGET INTRODUCTION	8
1.1	ST AND TOE REFERENCE	8
1.2	TOE OVERVIEW	8
1.2.1	<i>TOE Product Type</i>	8
1.2.2	<i>Supported non-TOE Hardware/ Software/ Firmware</i>	9
1.3	TOE DESCRIPTION	9
1.3.1	<i>Cisco Aggregation Services Router (ASR) 1000 Series</i>	9
1.4	TOE EVALUATED CONFIGURATION	10
1.5	PHYSICAL SCOPE OF THE TOE	12
1.6	LOGICAL SCOPE OF THE TOE	14
1.6.1	<i>Security Audit</i>	14
1.6.2	<i>Cryptographic Support</i>	14
1.6.3	<i>Identification and Authentication</i>	16
1.6.4	<i>Security Management</i>	16
1.6.5	<i>Protection of the TSF</i>	17
1.6.6	<i>TOE Access</i>	17
1.6.7	<i>Trusted Path/Channel</i>	18
1.7	EXCLUDED FUNCTIONALITY	19
2	CONFORMANCE CLAIMS	20
2.1	COMMON CRITERIA CONFORMANCE CLAIM	20
2.2	PROTECTION PROFILE CONFORMANCE	20
2.3	PROTECTION PROFILE CONFORMANCE CLAIM RATIONALE	21
2.3.1	<i>TOE Appropriateness</i>	21
2.3.2	<i>TOE Security Problem Definition Consistency</i>	21
2.3.3	<i>Statement of Security Requirements Consistency</i>	21
3	SECURITY PROBLEM DEFINITION	22
3.1	ASSUMPTIONS	22
3.2	THREATS	23
3.3	ORGANIZATIONAL SECURITY POLICIES	25
4	SECURITY OBJECTIVES	26
4.1	SECURITY OBJECTIVES FOR THE TOE	26
4.2	SECURITY OBJECTIVES FOR THE ENVIRONMENT	26
5	SECURITY REQUIREMENTS	28
5.1	CONVENTIONS	28
5.2	TOE SECURITY FUNCTIONAL REQUIREMENTS	28
5.3	SFRS FROM NDCPP	30
5.3.1	<i>Security Audit (FAU)</i>	30
5.3.2	<i>Cryptographic Support (FCS)</i>	33
5.3.3	<i>Identification and authentication (FIA)</i>	38
5.3.4	<i>Security management (FMT)</i>	39
5.3.5	<i>Protection of the TSF (FPT)</i>	40

5.3.6	TOE Access (FTA)	41
5.3.7	Trusted Path/Channels (FTP)	42
5.4	TOE SFR DEPENDENCIES RATIONALE FOR SFRS FOUND IN PP	43
5.5	SECURITY ASSURANCE REQUIREMENTS	43
5.5.1	SAR Requirements	43
5.5.2	Security Assurance Requirements Rationale	44
5.6	ASSURANCE MEASURES	44
6	TOE SUMMARY SPECIFICATION	45
6.1	TOE SECURITY FUNCTIONAL REQUIREMENT MEASURES	45
7	ANNEX A: KEY ZEROIZATION	57
7.1	KEY ZEROIZATION	57
8	ANNEX B: REFERENCES	59

List of Tables

TABLE 1 ACRONYMS.....	5
TABLE 2 TERMINOLOGY.....	6
TABLE 3 ST AND TOE IDENTIFICATION	8
TABLE 4 IT ENVIRONMENT COMPONENTS	9
TABLE 5 ASR1K HARDWARE MODELS AND SPECIFICATIONS	12
TABLE 7 FIPS REFERENCES	14
TABLE 8 TOE PROVIDED CRYPTOGRAPHY	15
TABLE 9 EXCLUDED FUNCTIONALITY	19
TABLE 10 PROTECTION PROFILES.....	20
TABLE 11 TOE ASSUMPTIONS	22
TABLE 12 THREATS	23
TABLE 13 ORGANIZATIONAL SECURITY POLICIES	25
TABLE 13 SECURITY OBJECTIVES FOR THE ENVIRONMENT	26
TABLE 16 SECURITY FUNCTIONAL REQUIREMENTS.....	28
TABLE 17 AUDITABLE EVENTS	31
TABLE 18 ASSURANCE MEASURES	43
TABLE 19 ASSURANCE MEASURES	44
TABLE 20 HOW TOE SFRS MEASURES.....	45
TABLE 21 TOE KEY ZEROIZATION	57
TABLE 22 DOCUMENTATION REFERENCES	59

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
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
ESPr	Embedded Services Processors
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
NDcPP	collaborative Protection Profile for Network Devices
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
ST	Security Target
TCP	Transport Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
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	Another router on the network that the TOE interfaces with.
Privilege level	Assigns a user specific management access to the TOE to run specific commands. The privilege levels are from 1-15 with 15 having full administrator access to the TOE similar to root access in UNIX or Administrator access on Windows. Privilege level 1 has the most limited access to the CLI. By default when a user logs in to the Cisco IOS-XE, they will be in user EXEC mode (level 1). From this mode, the administrator has access to some information about the TOE, such as the status of interfaces, and the administrator can view routes in the routing table. However, the administrator can't make any changes or view the running configuration file. The privilege levels are customizable so that an Authorized Administrator can also assign certain commands to certain privilege levels.
Role	An assigned role gives a user varying access to the management of the TOE. For the purposes of this evaluation the privilege level of user is synonymous with the assigned privilege level.
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). For configuration purposes vty defines the line for remote access policies to the router.

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 Cisco Aggregation Services Router (ASR) 1000 Series. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

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 3, Chapter 11.

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 Aggregation Services Router (ASR) 1000 Series Security Target
ST Version	0.7
Publication Date	17 October, 2017
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Aggregation Services Router (ASR) 1000 Series [ASR1K]
TOE Hardware Models	ASR1K – <ul style="list-style-type: none"> • 1004
TOE Software Version	IOS-XE 16.3
Keywords	Router, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device

1.2 TOE Overview

The Cisco Aggregation Services Router 1000 Series (ASR1K) TOE is a purpose-built, routing platform. The ASR1K TOE includes the ASR1004 chassis, as defined in Table 3 in section 1.1.

1.2.1 TOE Product Type

The Cisco ASR1K Series delivers embedded hardware acceleration for multiple Cisco IOS-XE Software services. In addition, the Cisco ASR1K Series Router features redundant Route and Embedded Services Processors, as well as software-based redundancy. In support of the routing

capabilities, the Cisco ASR1K provides IPsec connection capabilities to facilitate secure communications with external entities, as required.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

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

Table 4 IT Environment Components

Component	Mandatory	Usage/Purpose Description for TOE performance
RADIUS AAA Server	No	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.
Management Workstation with SSH client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. 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.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrolment.
NTP Server	No	The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server's date and time. A solution must be used that supports secure communications with up to a 32 character key.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.
Another instance of the TOE	No	Includes "another instance of the TOE" that would be installed in the evaluated configuration, and likely administered by the same personnel. Used as a VPN peer.

1.3 TOE DESCRIPTION

1.3.1 Cisco Aggregation Services Router (ASR) 1000 Series

This section provides an overview of the Cisco ASR1K Series Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE.

The hardware models included in the evaluation are: 1004. The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 4-RU form factor. The chassis is the component of the TOE in which all other TOE components are housed.
- Embedded Services Processor (ESPr): The Cisco ASR1K Series ESPs (ESP10, ESP 20, ESP40) are responsible for the data-plane processing tasks, and all network traffic flows through them.
- Route Processor (RP): The Cisco ASR1K Series RPs (RP1 and RP2) provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the Cisco ASR1K Series Aggregation Services.
- Shared Port Adaptors (SPAs): Used for connecting to networks. These SPAs interface with the TOE to provide the network interfaces that will be used to communicate on the network.

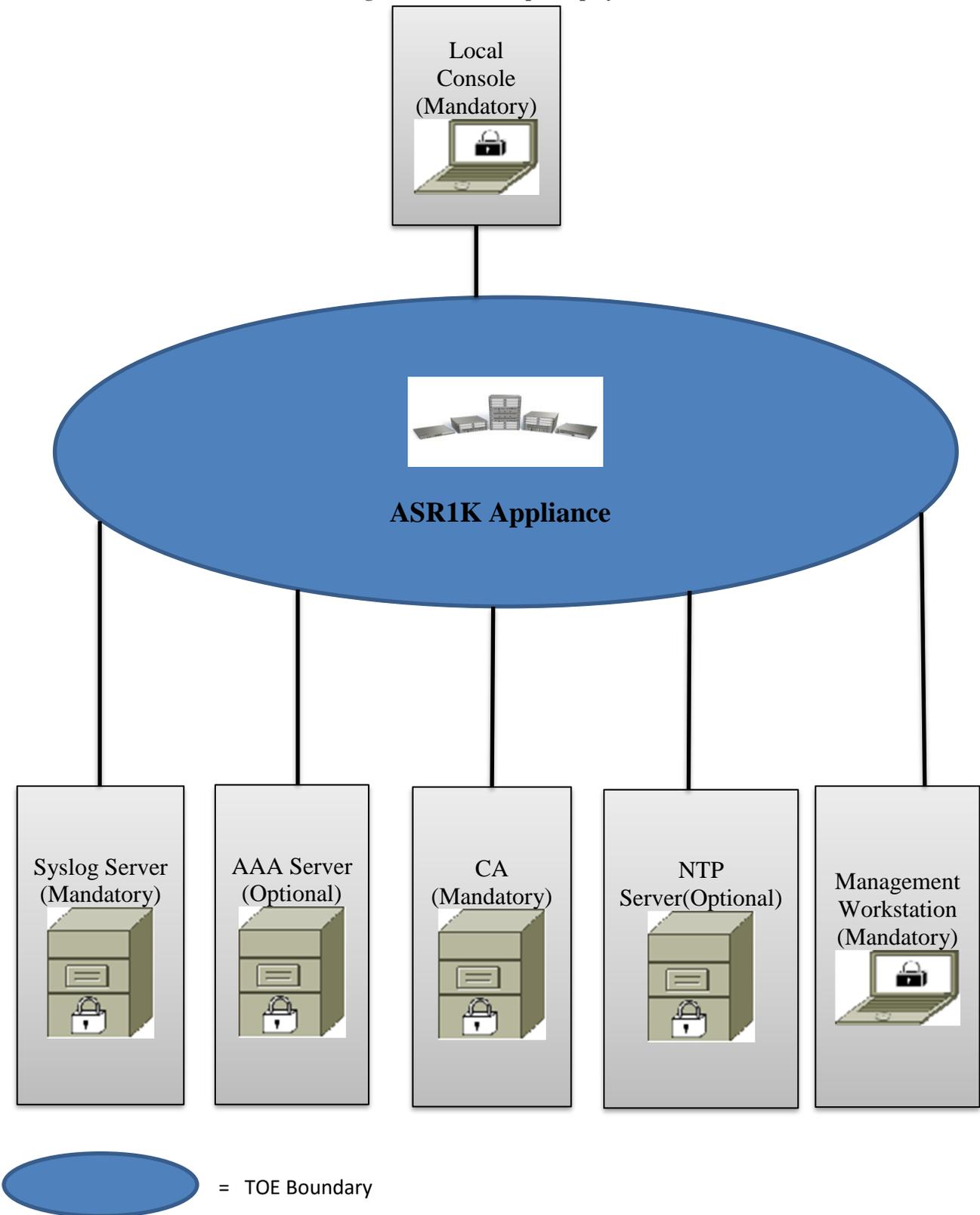
1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco IOS-XE software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE 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 for clock synchronization. A syslog server must be used to store audit records.

The following figure provides a visual depiction of an example TOE deployment.

Figure 1 TOE Example Deployment



The previous figure includes the following:

- Several examples of TOE Models
- The following are considered to be in the IT Environment:
 - Management Workstation
 - Authentication Server
 - NTP Server
 - Syslog Server
 - Local Console
 - CA

NOTE: While the previous figure includes several TOE devices and several non-TOE IT environment devices, the TOE is only the ASR1K device. Only one TOE device is required for deployment of the TOE in an evaluated configuration.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the router models as follows:

Chassis:

- ASR 1004; Embedded Services Processors (ESP): ESP20 and ESP40; Route Processor (RP): RP1, RP2

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 16.3. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image. The TOE is comprised of the following physical specifications as described in Table 5 and Table 6 below:

Table 5 ASR1K Hardware Models and Specifications

Hardware Model	ASR 1004
Dimensions (HxWxD) in inches	7 x 17.2 x 18.15
Shared Port Adapters	8
Ethernet Port Adapters	n/a
Embedded services processor slots	1
ESP Bandwidth	10 to 40 Gbps

Route processor slots	1
Built-in Gigabit Ethernet ports	0
Default memory	4-GB DRAM RP1 8-GB DRAM RP2
External USB flash memory	1-GB USB flash-memory support

1.6 Logical Scope of the TOE

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

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

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

1.6.1 Security Audit

The ASR1K provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operation Environment - Intel Xeon, MIPS64). Please see table below for certificate references.

Table 6 FIPS References

Algorithm	Supported Mode	Cert. #	SFR
AES	CBC (128, 192, 256), GCM (128, 192, 256)	4583	FCS_COP.1(1)
SHS (SHA-1, SHA-256 and SHA-512)	Byte Oriented	3760	FCS_COP.1(3)

Algorithm	Supported Mode	Cert. #	SFR
HMAC (HMAC-SHA-1)	Byte Oriented	3034	FCS_COP.1(4)
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011 CTR (using AES-256)	1529	FCS_RBG_EXT.1
RSA	PKCS#1 v.1.5, 2048 bit key, FIPS 186-4 Key Gen	2500	FCS_CKM.1 FCS_COP.1(2)
ECDSA	FIPS 186-4, Digital Signature Standard (DSS)	1122, 1241	FCS_CKM.1 FCS_COP.1(2)
CVL – KAS-ECC	NIST Special Publication 800-56A	1257	FCS_CKM.2

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2. 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.
Secure Shell Establishment	Used to establish initial SSH session.
RSA/DSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing
SP 800-90 RBG	Used in IPsec session establishment. Used in SSH session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services

Cryptographic Method	Use within the TOE
ECC	Used to provide cryptographic signature services
DH	Used as the Key exchange method for SSH

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 TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. 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 TOE's 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. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally 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.

The TOE provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts fail exceeding the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec, and SSH connections.

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 or via a local console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely;

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE and verification of the updates;
- Configuration of IPsec functionality;
- TOE configuration file storage and retrieval.

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. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authenticated administrators.

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-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE 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 router 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 unauthorized software.

Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

1.6.6 TOE Access

The TOE can terminate or lock 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. Sessions can also be terminated if an Authorized Administrator enters the “exit” command.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.6.7 Trusted Path/Channel

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2, 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, as well as to protect communications with a CA or remote administrative console.

1.7 Excluded Functionality

The following functional 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.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the NDcPP v1.0.

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: September 2012. For a listing of Assurance Requirements claimed see section 5.5.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant. The ST is also compliant to the following Technical Decisions –

- TD0090
- TD0115
- TD0116
- TD0117
- TD0130
- TD0150
- TD0153
- TD0154
- TD0156
- TD0160
- TD0164
- TD0167
- TD0168
- TD0169
- TD0181
- TD0184
- TD0185
- TD0186
- TD0187
- TD0188
- TD0189
- TD0199
- TD0201
- TD0223
- TD0224
- TD0225
- TD0228

2.2 Protection Profile Conformance

This ST claims compliance to the following Common Criteria validated Protection Profiles:

Table 9 Protection Profiles

Protection Profile	Version	Date
--------------------	---------	------

collaborative Protection Profile for Network Devices (NDcPP)	1.0	Feb 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 U.S. Government Protection Profile and extended package:

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

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in the collaborative Protection Profile for Network Devices (NDcPP) 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 section 6 of the NDcPPv1.0.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

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

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

3.1 Assumptions

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

Table 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

Assumption	Assumption Definition
	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.
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.

Threat	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	<p>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.</p> <p>An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.</p>
T.WEAK_AUTHENTICATION_ENDPOINTS	<p>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.</p>
T.UPDATE_COMPROMISE	<p>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.</p>
T.UNDETECTED_ACTIVITY	<p>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.</p>
T.SECURITY_FUNCTIONALITY_COMPROMISE	<p>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.</p>

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

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

4.1 Security Objectives for the TOE

The 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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Environment Security Objective	IT Environment Security Objective Definition
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

5 SECURITY REQUIREMENTS

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

5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDcPP, the formatting used in those documents 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 matches the formatting specified within the NDcPP.

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	Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (Refined)
	FCS_CKM.2	Cryptographic Key Establishment (Refined)
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)

Class Name	Component Identification	Component Name
	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)
	FCS_IPSEC_EXT.1	IPsec Protocol
	FCS_SSHS_EXT.1	SSH Server 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)/Trusted Update	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	Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Extended: Trusted Update
	FPT_STM.1	Reliable Time Stamps
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination

Class Name	Component Identification	Component Name
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

5.3 SFRs from NDcPP

5.3.1 Security Audit (FAU)

5.3.1.1 FAU_GEN.1 Audit data generation

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

- a) Start-up and 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];
- 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.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
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 identification and 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.

SFR	Auditable Event	Additional Audit Record Contents
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_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	No additional information.
FPT_TST_EXT.1	None.	None.
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.
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 path. Termination of the trusted path. Failure of the trusted path functions.	Identification of the claimed user identity.

5.3.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.3.1.3 FAU_STG_EXT.1 Protected Audit Event 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 [overwrite previous audit records according to the following rule: [when allotted space has reached its threshold], [no other action]] when the local storage space for audit data is full.

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_CKM.1 Cryptographic Key Generation (Refined)

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

- 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
- ECC schemes using “NIST curves” [P-256, P-384] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
-

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

5.3.2.2 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: [

- RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B Revision 1, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;

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

5.3.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

- For plaintext keys in volatile storage, the destruction shall be executed by a [selection: single overwrite consisting of [zeroes];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
 - logically addresses the storage location of the key and performs a [single-pass] overwrite consisting of [zeroes];

]

that meets the following: *No Standard*.

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

FCS_COP.1.1(1) The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm AES *used in* [CBC, GCM] mode and cryptographic key sizes [128-bits, 192-bits, 256-bits] that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772]*

5.3.2.5 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],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 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,
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing [“NIST curves” P-256, P-384]; ISO/IEC 14888-3, Section 6.4

].

5.3.2.6 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.

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

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

5.3.2.8 FCS_IPSEC_EXT.1 Extended: 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, 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 (specified by RFC 3602), AES-CBC-256 (specified by RFC 3602)] 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]].
- IKEv2 as defined in RFC 5996 and [with mandatory support or NAT traversal as specified in RFC 5996, section 2.23], and [RFC 4868 for hash functions]

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms [AES-CBC-128 (specified in RFC 3602), AES-CBC-256 (specified in RFC 3602)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv1 Phase 1 SA lifetimes can be configured by an Security Administrator based on [
 - number of bytes
 - length of time, where the time values can configured within [1-24] hours;

].

- IKEv2 SA lifetimes can be configured by an Security Administrator based on
 - [
 - number of bytes
 - length of time, where the time values can configured within [1-24] 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;
 - IKEv2 Child 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 $g^x \bmod p$) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16)] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1, IKEv2] exchanges of length [320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16)].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [14 (2048-bit MODP), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP)].

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, IKEv2 IKE_SA] 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, IKEv2 CHILD_SA] 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 if the presented identifier in the received certificate matches the configured reference identifier, where the presented and

reference identifiers are of the following types: [IP address, Fully Qualified Domain Name (FQDN), user FQDN, Distinguished Name (DN)] and [no other reference identifier type].

5.3.2.9 FCS_RBG_EXT.1 Extended: Cryptographic Operation (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 [*I*] hardware based noise source] with minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.3.2.10 FCS_SSHS_EXT.1 SSH Server Protocol

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

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

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [35,000 bytes] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc]

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [ssh_rsa] and [no other public key algorithms] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha1-96] and [no other MAC algorithms] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

5.3.3 Identification and authentication (FIA)

5.3.3.1 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- a) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!” , “@” , “#” , “\$” , “%” , “^” , “&” , “*” , “(” , “)”] ;*
- b) *Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater;*

5.3.3.2 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;
- [no other actions]

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

5.3.3.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

5.3.3.4 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress at the local console.

5.3.3.5 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 [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, 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.

5.3.3.6 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, SSH], and [code signing for system software updates, *[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].

5.3.3.7 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, Organization, Organizational Unit and Country].

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

5.3.4 Security management (FMT)

5.3.4.1 FMT_MOF.1(1)/TrustedUpdate Management of security functions behavior

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

5.3.4.2 FMT_MTD.1/AdminAct Management of TSF Data

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

5.3.4.3 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;]

5.3.4.4 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.

5.3.5 Protection of the TSF (FPT)

5.3.5.1 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.

5.3.5.2 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.3.5.3 FPT_STM.1 Reliable Time Stamps

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

5.3.5.4 FPT_TST_EXT.1: Extended: TSF Testing

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

- *AES Known Answer Test*
- *RSA Signature Known Answer Test (both signature/verification)*
- *Power up bypass test*
- *RNG Known Answer Test*
- *Diffie Hellman test*
- *HMAC Known Answer Test*
- *SHA-1/256/512 Known Answer Test*
- *Software Integrity Test*

5.3.5.5 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 and [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 [digital signature mechanism, published hash] prior to installing those updates.

5.3.6 TOE Access (FTA)

5.3.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

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

after a Security Administrator-specified time period of inactivity.

5.3.6.2 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*.

5.3.6.3 FTA_SSL.4 User-initiated Termination

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

5.3.6.4 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.

5.3.7 Trusted Path/Channels (FTP)

5.3.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall be **capable of using [IPsec]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [authentication server, [CA Server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit **the TSF, or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[communications with the following:*

- *external audit servers using IPsec,*
- *remote AAA servers using IPsec,*
- *a CA server using IPsec].*

5.3.7.2 FTP_TRP.1 Trusted Path

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

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

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

5.4 TOE SFR Dependencies Rationale for SFRs Found in PP

The NDcPPv1.0 contains all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP and EP have been approved.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP 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
TESTS	ATE_IND.1	Independent testing – conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

5.5.2 Security Assurance Requirements Rationale

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

5.6 Assurance Measures

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

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

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 18 How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	<p>The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism cryptography related events, 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 syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.</p> <p>The audit trail consists 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. Example audit events are included below:</p> <pre>Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test activated by user: lab) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software checksum ... passed) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encryption/decryption ... passed) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encryption/decryption ... passed) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing ... passed) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encryption/decryption ... passed)</pre> <p>In the above log events a date and timestamp is displayed as well as an event description “CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test)”. The subject identity where a command is directly run by a user is displayed “user: lab.” The outcome of the command is displayed: “passed”</p> <p>The logging buffer size can be configured from a range of 4096 (default) to 2,148,483,647 bytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount.</p> <p>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</p>

TOE SFRs	How the SFR is Met
	<p>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. 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.</p> <p>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 messages 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 TOE is affected. All notifications and information type message can be sent to the syslog server. 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.</p> <p>Once the box is up and operational and the crypto self test command is entered, then the result messages would be displayed on the console and will also be logged. If the TOE encounters a failure to invoke any one of the cryptographic functions, a log record is generated.</p> <p>When the incoming traffic to the TOE exceeds what the interface can handle, the packets are dropped at the input queue itself and there are no error messages generated.</p>
FAU_GEN.2	<p>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below:</p> <pre>Jun 18 11:17:20.769: AAA/BIND(0000004B): Bind i/f Jun 18 11:17:20.769: AAA/AUTHEN/LOGIN (0000004B): Pick method list 'default' Jun 18 2012 11:17:26 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 100.1.1.5] [localport: 22] at 11:17:26 UTC Mon Jun 18 2012</pre>
FAU_STG_EXT.1	<p>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. The TOE transmits its audit events to all configured syslog servers at the same time logs are written to the local log buffer and to the console. The TOE is capable of detecting when the IPsec connection fails. The TOE also stores a limited set of audit records locally on the TOE, and continues to do so if the communication with the syslog server goes down. If the IPsec connection fails, the TOE will buffer between 4096-bytes and 2,148,483,647 bytes of audit records on the TOE when it discovers it can no longer communicate with its configured syslog server, and will transmit the buffer contents when connectivity to the syslog server is restored. The exact size of the audit storage is configured using the “logging buffered” command.</p>

TOE SFRs	How the SFR is Met
	<p>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.</p> <p>For audit records stored internally to the TOE, the Authorized Administrator has the ability to configure the TOE to stop all auditable events when an audit storage threshold is met (lossless auditing) or configure the TOE to overwrite the oldest audit records when the audit trail becomes full.</p>
FCS_CKM.1	<p>The TOE implements a random number generator for Diffie-Hellman and Elliptic curve key establishment (conformant to NIST SP 800-56A), and for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in the NIST SP 800-56B. Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes and Appendix B.4 for ECDSA schemes. The TOE can create a RSA public-private key pair that can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrolment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its X.509v3 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 IOS-XE Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. In addition, the IOS-XE Software includes an embedded certificate server, allowing the router to act as a certification authority on the network. The TOE can act as a certification authority thus digitally signing and issuing certificates to both the TOE and external entities. The TOE can also use the X.509v3 certificate for securing IPsec and SSH sessions. The TOE provides cryptographic signature services using ECDSA that meets FIPS 186-3, "Digital Signature Standard" with NIST curves P-256 and P-384 and RSA that meets FIPS PUB 186-4, "Digital Signature Standard".</p>
FCS_CKM.2	
FCS_CKM_EXT.4	<p>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form. See refer to Table 19 for more information on the key zeroization.</p>
FCS_COP.1 (1)	<p>The TOE provides symmetric encryption and decryption capabilities using AES in GCM and CBC mode (128, 192 and 256 bits) as described in ISO 18033-3, NIST SP 800-38F, ISO 19772 and ISO 10116 respectively. Please see CAVP certificate in Table 6 for validation details. AES is implemented in the following protocols: IPsec and SSH.</p>
FCS_COP.1(2)	<p>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3. In addition, the TOE will provide cryptographic signature services using ECDSA with key</p>

TOE SFRs	How the SFR is Met
	size of 256 or greater as specified in FIPS PUB 186-4, “Digital Signature Standard”. The TOE provides cryptographic signature services using ECDSA that meets ISO/IEC 14888-3, Section 6.4 with NIST curves P-256 and P-384.
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512 as specified in ISO/IEC 10118-3:2004.” Please see CAVP certificate in Table 6 for validation details.
FCS_COP.1(4)	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, with key size and message digest size of 160 bits and a block size of 512 bits, as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. Please see CAVP certificate in Table 6 for validation details.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90 seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source. The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.
FCS_IPSEC_EXT.1	<p>The TOE implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. 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.</p> <p>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.</p> <p>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. The IPsec protocol ESP is implemented using the cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA-1.</p> <p>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.</p> <p>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 strength of the symmetric algorithm negotiated to protect the IKEv1 Phase</p>

TOE SFRs	How the SFR is Met
	<p>1 and IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 2 or IKEv2 CHILD_SA connection. The IKE protocols implement Peer Authentication using RSA and ECDSA along with X.509v3 certificates, or pre-shared keys. 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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>The TOE supports both IKEv1 and IKEv2 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 supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours, but it is configurable to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets. The TOE supports Diffie-Hellman Group 14, 19, 24, 20, 15 and 16. Group 14 (2048-bit keys) can be set by using the “group 14” command in the config mode. The nonces used in IKE exchanges are generated in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^{128}. The secret value ‘x’ used in the IKE Diffie-Hellman key exchange (“x” in $g^x \text{ mod } p$) is generated using a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG). 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. 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.</p> <p>The TOE provides AES-CBC-128 and AES-CBC-256 for encrypting the IKEv1 Phase 1, and AES-CBC-128, AES-CBC-256, AES-GCM-128 and AES-GCM-256 for IKEv1 Phase 2 and IKEv2 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.</p> <p>The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic</p>

TOE SFRs	How the SFR is Met
	<p>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), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16)] bits.</p> <p>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.</p> <p>A crypto map (the Security Policy Definition) 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 acl in the crypto map, but that is not disallowed by other acls on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit acl and is also blocked by other non-crypto acls on the interface would be DISCARDED.</p> <p>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.</p> <p>The command "fqdn <name>" can be configured within a crypto identity and applied to a crypto map in order to perform validation of the peer device during authentication.</p> <p>Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication.</p>
FCS_SSHS_EXT.1	<p>The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> • Public key algorithms for authentication: RSA Signature Verification. • Local password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server.

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> • Encryption algorithms, AES-CBC-128, AES-CBC-256 to ensure confidentiality of the session. • The TOE's implementation of SSHv2 supports hashing algorithms hmac-sha1 and hmac-sha1-96 to ensure the integrity of the session. • The TOE's implementation of SSHv2 can be configured to only allow Diffie-Hellman Group 14 (2048-bit keys) Key Establishment, as required by the PP. • Packets greater than 35,000 bytes in an SSH transport connection are dropped. Large packets are detected by the SSH implementation, and dropped internal to the SSH process. • Rekeying is checked by the TOE and performed based on time or number of bytes sent. When the threshold is reached for either time or bytes, the TOE will perform a rekey between the TOE and client.
FIA_PMG_EXT.1	<p>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 up to 15 characters.</p>
FIA_UIA_EXT.1	<p>The TOE displays an administratively configured warning banner prior to administrative identification and authentication and provides no access to the administrative capabilities of the TOE prior to the administrative user presenting the authentication credentials.</p>
FIA_UAU_EXT.2	<p>The TOE can be configured to require local authentication and/or remote authentication via a RADIUS server as defined in the authentication policy for interactive (human) users.</p> <p>The administrator authentication policies include, authenticated to the local user database, or have 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.</p> <p>The process for password-based authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via SSH or IPsec over SSH. At initial login in the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access or indicates that the login was unsuccessful. The SSH interface also supports authentication using SSH keys which are provided during the SSH connection request.</p>
FIA_UAU.7	<p>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. The TOE does not provide a reason for failure in the cases of a login failure.</p>

TOE SFRs	How the SFR is Met	
FIA_X509_EXT.1	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and SSH connections. Public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates can be stored in a specific location on the router, such as NVRAM and flash memory. The certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. Only authorized administrators with the necessary privilege level can access the certificate storage and add/delete them. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. The physical security of the router (A.Physical) 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. Both OCSP and CRL are configurable and may be used for certificate revocation (the TOE supports use of OCSP only when using RSA certs and not when using ECDSA certs). Checking is also done for the basicConstraints extension and the cA flag to determine whether they are present and set to TRUE. If they are not, the certificate is not accepted. If the TOE does not have the applicable CRL and is unable to obtain one, or if the OCSP server returns an error, the TOE will reject the peer's certificate--unless an administrator includes the 'none' keyword in your configuration. If the 'none' keyword is configured, a revocation check will not be performed and the certificate will always be accepted.</p> <p>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.</p> <p>The certificate chain path validation is configured on the TOE by first setting crypto pki trustpoint name and then configuring the level to which a certificate chain is processed on all certificates including subordinate CA certificates using the <i>chain-validation</i> command.</p>	
FIA_X509_EXT.2		
FIA_X509_EXT.3		
FMT_MOF.1(1)/TrustedUpdate	<p>The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and 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-XE 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</p>	

TOE SFRs	How the SFR is Met
FMT_MTD.1	<p>customizable, while levels 2-14 are undefined by default and are also customizable.</p> <p>The term “Security 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. No administrative functionality is available prior to administrative login.</p>
FMT_SMF.1	<p>The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include -</p> <ul style="list-style-type: none"> • 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-XE software. The validity of the image is provided using SHA-256 and 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	<p>The TOE platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and 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-XE 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 hierarchical.</p> <p>The term “Security 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.</p>

TOE SFRs	How the SFR is Met
	<p>The privilege level determines the functions the user can perform; hence the Security Administrator with the appropriate privileges. Refer to the Guidance documentation and IOS-XE Command Reference Guide for available commands and associated roles and privilege levels.</p> <p>The TOE can and shall be configured to authenticate all access to the command line interface using a username and password.</p> <p>The TOE supports both local administration via a directly connected console cable and remote administration via SSH or IPSec over SSH.</p>
FPT_SKP_EXT.1	<p>The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. This functionality is configured on the TOE using the ‘password encryption aes’ command.</p> <p>The TOE is configured to not display configured keys as part of configuration files using the ‘hidekeys’ command.</p>
FPT_APW_EXT.1	<p>The TOE includes a Master Passphrase feature that can be used to configure the TOE to encrypt all locally defined user passwords using AES. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. Password encryption is configured using the ‘service password-encryption’ command. There are no administrative interfaces available that allow passwords to be viewed as they are encrypted via the password-encryption service.</p>
FPT_STM.1	<p>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. The time information is also used in various routing protocols such as, OSPF, BGP, and ERF; Set system time, Calculate IKE stats (including limiting SAs based on times); determining AAA timeout, and administrative session timeout.</p>
FPT_TUD_EXT.1	<p>The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from the Cisco.com web site. Authorized Administrators can download the approved image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html. Digital signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The 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. Instructions for how to do this verification are provided in the administrator guidance for this evaluation.</p>

TOE SFRs	How the SFR is Met
FPT_TST_EXT.1	<p>The TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE is operating correctly, including checks of image integrity and all cryptographic functionality.</p> <p>During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:</p> <ul style="list-style-type: none"> • AES Known Answer Test • RSA Signature Known Answer Test (both signature/verification) • Power up bypass test • RNG Known Answer Test • Diffie Hellman test • HMAC Known Answer Test • SHA-1/256/512 Known Answer Test • Software Integrity Test <p>If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file.</p> <p>All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic.</p> <p>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behavior will be identified by the failure of a self-test.</p> <p>The integrity of stored TSF executable code when it is loaded for execution can be verified through the use of RSA and Elliptic Curve Digital Signature algorithms.</p>
FTA_SSL_EXT.1	<p>An 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. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be locked and will require authentication to establish a new session.</p>
FTA_SSL.3	<p>The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</p>

TOE SFRs	How the SFR is Met
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the “exit” command.
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This is applicable for both local and remote TOE administration.
FTP_ITC.1	<p>The TOE protects communications with peer or neighbor routers using keyed hash as defined in FCS_COP.1.1(4) and cryptographic hashing functions FCS_COP.1.1(3). This protects the data from modification of data by hashing that verify that data has not been modified in transit. In addition, encryption of the data as defined in FCS_COP.1.1(1) is provided to ensure the data is not disclosed in transit. The TSF allows the TSF, or the authorized IT entities to initiate communication via the trusted channel.</p> <p>The TOE also requires that peers and other TOE instances establish an IKE/IPSec connection in order to forward routing tables used by the TOE. In addition the TOE can establish secure VPN tunnels with IPSec VPN clients.</p> <p>The TOE also requires that peers establish an IKE/IPsec connection to a CA server for sending certificate signing requests.</p> <p>The TOE protects communications between the TOE and the remote audit server using IPsec. This provides a secure channel to transmit the log events. Likewise communications between the TOE and AAA servers are secured using IPsec.</p>
FTP_TRP.1	All remote administrative communications take place over a secure encrypted SSHv2 session which has the ability to be encrypted further using IPsec. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

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

Table 19 TOE Key Zeroization

Name	Description of Key	Storage	Zeroization
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange.	SDRAM (plaintext)	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange.	SDRAM (plaintext)	Zeroized upon completion of DH exchange. Overwritten with: 0x00
Skeyid	This is an IKE intermittent value used to create skeyid_d.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	This is an IKE intermittent value used to derive keying data for IPsec.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	This the key IPsec key used for encrypting the traffic in an IPsec connection.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	This the key IPsec key used for authenticating the traffic in an IPsec connection.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared	This is the configured pre-shared key for ISAKMP negotiation.	NVRAM (plaintext)	Zeroized using the following command: # no crypto isakmp key Overwritten with: 0x0d
IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. Afterwards, the device's public key must be put into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate	NVRAM (plaintext)	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x0d

Name	Description of Key	Storage	Zeroization
	<p>and also enrolls with the CA server to generate the device certificate.</p> <p>In the IKE authentication step, the device's certificate is firstly sent to other device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sends back a random secret encrypted by the device's public key in the valid device certificate. . Only the device with the matching device private key can decrypt the message and obtain the random secret.</p>		
IPSec encryption key	This is the key used to encrypt IPsec sessions.	SDRAM (plaintext)	<p>Automatically when IPsec session terminated.</p> <p>Overwritten with: 0x00</p>
IPSec authentication key	This is the key used to authenticate IPsec sessions.	SDRAM (plaintext)	<p>Automatically when IPsec session terminated.</p> <p>Overwritten with: 0x00</p>
RADIUS secret	Shared secret used as part of the Radius authentication method.	NVRAM (plaintext)	<p>Zeroized using the following command:</p> <p># no radius-server key</p> <p>Overwritten with: 0x0d</p>
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.	SDRAM (plaintext)	<p>Zeroized using the following command:</p> <p># crypto key zeroize rsa</p> <p>Overwritten with: 0x00</p>
SSH Session Key	The results zeroized using the poisoning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended.	SDRAM (plaintext)	<p>Automatically when the SSH session is terminated.</p> <p>Overwritten with: 0x00</p>

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 20 Documentation 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, February 27, 2015
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008