Cisco Aggregation Services Router (ASR) 1000 Series

Security Target

Version .15

December 3, 2013

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

Table of Contents

List of Tables

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
ISDN	Integrated Services Digital Network
IT	Information Technology
NDPP	Network Device Protection Profile
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, 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.
Remote Peer	A remote peer is another network device that the TOE sets up an IPsec connection with. This could be another router.
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 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.

REVISION HISTORY

Rev	Date	Description
.01	May 14 2012	Initial Draft
.02	June 2012	Second Internal Draft
.03	July 2012	Updated info on Entropy Seeding
.04	July 2012	Updated per internal GCT Review
.05	August 2012	Added 1002-X
.06	October 2012	Updated per internal comments
.07	October 2012	Updated per evaluator comments
.08	November 2012	Updated per evaluator comments
.09	November 2012	Updated FCS_RBG_EXT.1.2 per SP800-90; Italics in FMT_SMF.1, and bold of NDPPv1.1 to FCS_IPSEC_EXT.1
.10	February 2013	Updated per NIAP comments
.11	March 2013	Updated per NIAP comments
.12	July 2013	Updated per evaluator comments
.13	October 2013	Updated per validator comments
.14	November 2013	Updated per NIAP comments
.15	December 2013	Updated per lab feedback

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]
- Rationale [Section 7]

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 4.

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	.15
Publication Date	December 2013
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Aggregation Services Router (ASR) 1000 Series
TOE Hardware Models	Chassis: ASR 1001, ASR 1002, ASR 1002X, ASR 1004, ASR 1006, ASR 1013; Embedded Services Processors (ESPr): ESP5, ESP10, ESP20, ESP40, ESP100; Route Processor (RP): RP1, RP2
TOE Software Version	IOS XE 3.7.2t(S)
Keywords	Router, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device

1.2 TOE Overview

The Cisco Aggregation Services Router (ASR) 1000 Series TOE is a purpose-built, routing platform. The TOE includes six (6) chassis options, as defined in Table 3 in section 1.1.

1.2.1 TOE Product Type

The Cisco Aggregation Services Router (ASR) 1000 Series delivers embedded hardware acceleration for multiple Cisco IOS® XE Software services. In addition, the Cisco ASR 1000 Series Router features redundant Route and Embedded Services Processors, as well as software-based redundancy.

In support of the routing capabilities, the Cisco Aggregation Services Router (ASR) 1000 Series 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:

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that can be leveraged for remote user authentication.
Management Workstation	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration through protected channels. This management workstation must have an IPsec connection established between itself and the managed instance of ASR1K. This connection will be used to protect a tunneled protocol that will be used for user authentication and to perform ASR1K management actions. While the tunneled protocol used through IPsec is not defined by the ST and can be either SSH or telnet, it is recommended to use SSHv2.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.
NTP Server	No	The TOE supports communications with an NTP server. A solution must be used that supports MD5 hashing of communications with up to a 32 character key.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Aggregation Services Router (ASR) 1000 Series Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 2-RU, 4-RU, 6-RU and 13-RU form factors. The chassis is the component of the TOE in which all other TOE components are housed.
- Embedded Services Processor (ESPr): The Cisco ASR 1000 Series ESPrs are responsible for the data-plane processing tasks, and all network traffic flows through them.

- Route Processor (RP): The Cisco ASR 1000 Series RPs provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the Cisco ASR 1000 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.

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.6 Logical Scope of the TOE below.

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. When the ASR1k is remotely administered, management must be through an IPsec tunnel. A syslog server must be used to store audit records.

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

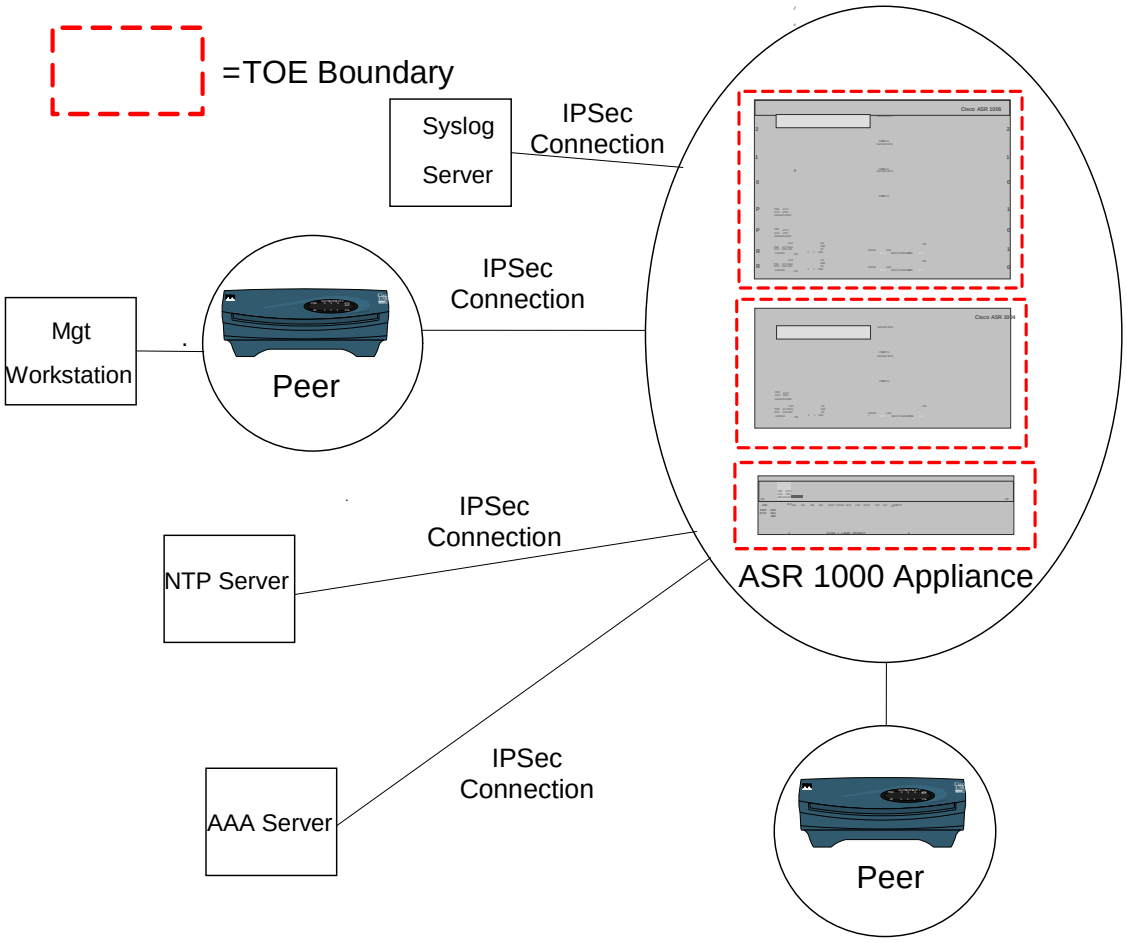

Figure 1 TOE Example Deployment

The previous figure includes the following:

- Several examples of TOE Models
  - ASR 1002
  - ASR 1004
  - ASR 1006
- 2 - Peer Routers (IT Environment)
- Management Workstation
- Syslog Server
- AAA Server
- NTP Server

NOTE: While the previous figure includes three TOE devices and several non-TOE IT environment devices, the TOE is only the ASR 1000 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 1001, ASR 1002, ASR 1002X, ASR 1004, ASR 1006, ASR 1013; Embedded Services Processors (ESPr): ESP5, ESP10, ESP20, ESP40, ESP100; 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 3.7.2t(S). 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 below:

Table 5 Hardware Models and Specifications

Hardware Model	**ASR 1001**	**ASR 1002-X**	**ASR 1002**	**ASR 1004**	**ASR 1006**	**ASR 1013**
Size	1-Rack Unit	2-Rack Units	2-Rack Units	4-Rack Units	6-Rack Units	13-Rack Units
Power	DC power: 500W AC Power: 471W	DC power: 590W AC Power: 560W	DC power: 590W AC Power: 560W	DC power: 1020W AC Power: 960W	DC power: 1700W AC Power: 1600W	DC power: 4000W AC Power: 3760W
Supported ESPrs	Integrated ESP	Integrated ESP	ESP5 ESP10	ESP10 ESP20	Dual ESP10 Dual ESP20 Dual ESP40 Dual ESP100	Dual ESP40 Dual ESP100
Supported RPs	Integrated RP1	Integrated RP1	Integrated RP1	RP1 RP2	Dual RP1 Dual RP2	Dual RP2

Supported SPAs	Cisco 1-Port Clear Channel OC3 ATM Shared Port Adapter (SPA-1XOC3-ATM-V2) Cisco 3-Port Clear Channel OC3 ATM Shared Port Adapter (SPA-3XOC3-ATM-V2) Cisco 1-Port OC12 STM Shared Port Adapter (SPA-1XOC12-ATM-V2) Cisco 2-Port T3/E3 Circuit Emulation and ATM SPA (SPA-2CHT3-CE-ATM) Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1) Cisco 4-Port Channelized T3 (DS0) Shared Port Adapter (SPA-4XCT3/DS0) Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter (SPA-2XCT3/DS0) Cisco 1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter (SPA-1XCHSTM1/OC3) Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter (SPA-2XT3/E3) Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter (SPA-4XT3/E3) Cisco 4-Port Serial Interface Shared Port Adapter (SPA-4XT-Serial) 1-port Channelized OC12 to DS0 SPA (SPA-1XCHOC12/DS0) Cisco 4-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter (SPA-4X1FE-TX-V2) Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter (SPA-8X1FE-TX-V2) Cisco 2-Port Gigabit Ethernet Shared Port Adapter (SPA-2X1GE-V2) Cisco 5-Port Gigabit Ethernet Shared Port Adapter (SPA-5X1GE-V2) Cisco 8-Port Gigabit Ethernet Shared Port Adapter (SPA-8X1GE-V2) Cisco 10-Port Gigabit Ethernet Shared Port Adapter (SPA-10X1GE-V2) Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter (SPA-1X10GE-L-V2) Cisco 1-port 10GE LAN/WAN-PHY Shared Port Adapter (SPA-1X10GE-WL-V2) Cisco Synchronous Ethernet SPA (SPA-2X1GE-SYNCE) Cisco 2-Port OC3c/STM-1c POS Shared Port Adapter (SPA-2XOC3-POS) Cisco 4-Port OC3c/STM-1c POS Shared Port Adapter (SPA-4XOC3-POS) Cisco 8-port OC3/STM4 POS Shared Port Adapter (SPA-8XOC3-POS) Cisco 1-Port OC12c/STM-4c POS Shared Port Adapter (SPA-1XOC12-POS) Cisco 2-port OC12/STM4 POS Shared Port Adapter (SPA-2XOC12-POS) Cisco 4-port OC12/STM4 POS Shared Port Adapter (SPA-4XOC12-POS) Cisco 8-port OC12/STM4 POS SPA Shared Port Adapter (SPA-8XOC12-POS) Cisco 1-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-1XOC48-POS/RPR) Cisco 2-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-2XOC48POS/RPR) Cisco 4-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-4XOC48POS/RPR) Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics (SPA-OC192POS-XFP)					
SPA Slots	1 SPA slot	1 SPA slot	3 SPA slots	8 SPA slots	12 SPA slots	24 SPA slots

Interfaces	Port Adapter Interface Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port USB Port GigE Ports (4)	Port Adapter Interface Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port USB Port GigE Ports (4)	Port Adapter Interface (3) Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port USB Port GigE Ports (4)	Port Adapter Interface (8) Console Port Auxiliary Port 10/100 Management Ethernet Port 10/100 BITS Ethernet Port (1) USB Ports (2)	Port Adapter Interface (12) Console Port Auxiliary Port (2) 10/100 BITS Ethernet Port (2) 10/100 Management Ethernet Port (2) USB Ports (4)	Port Adapter Interface (24) Console Port Auxiliary Port (2) 10/100 BITS Ethernet Port (4) 10/100 Management Ethernet Port (4) USB Ports (4)

1.6 Logical Scope of the TOE

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

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

These features are described in more detail in the subsections below.

1.6.1 Security Audit

The Cisco Aggregation Services Router (ASR) 1000 Series provide extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Aggregation Services Router (ASR) 1000 Series 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 Cisco Aggregation Services Router (ASR) 1000 Series security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 (see Table 6 for certificate references).

Table 6: FIPS References

Algorithm	Supported Mode	Cert. #
AES	CBC (128, 192, 256) ECB, CBC (128, 192, 256)	333, 2346, 2549
SHS	Byte Oriented	408, 2023, 2150
HMAC	Byte Oriented	137, 1455, 1570
RNG (ANSI X9.31)	Triple-DES (EDE)	154
Triple-DES	KO 1, CBC	397, 1170, 1469, 1543
DRBG	CTR (using AES-256)	382
RSA	PKCS#1 v.1.5, 1024-4096 bit key, FIPS 186-2 Key Gen	1304

The TOE provides cryptography in support of secure connections with other IT entities via IPSec. All keys are zeroized when no longer needed. The cryptographic services provided by the TOE include are described in the table below.

Table 7: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPSec session.
RSA Signature Services	Used in IPSec session establishment.
SP 800-90 RBG	Used in IPSec session establishment.
SHS	Used to provide IPSec traffic integrity verification
AES	Used to encrypt IPSec session traffic.

1.6.3 Full Residual Information Protection

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

1.6.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of remote IT device peers and user authentication for the Authorized Administrator of the TOE. For authentication of an Authorized Administrator, the TOE obscures the password feedback so it is not readable.

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 provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrative interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules that includes special characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or remote interfaces. The TOE optionally supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

1.6.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure IPSec session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; updates to the TOE; and TOE configuration file storage and retrieval. The TOE supports two separate administrative roles: non-privileged Administrator and privileged Administrator. Only the privileged administrator can perform all of the above security relevant management functions. The privileged Administrator is also considered to be the Authorized Administrator.

1.6.6 Protection of the TSF

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

Use of separate VLANs is used to ensure routing protocol communications between the TOE and neighbor routers including routing table updates and neighbor router authentication will be logically isolated from traffic on other VLANs.

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 malicious software.

1.6.7 Trusted Path/Channel

The TOE establishes a trusted path between the TOE and the remote management station used by the administrators to manage the TOE. This trusted path is secured using an IPSec secure connection.

The ASR1K establishes a trusted channel between itself and peer IT devices. The ASR1K sends audit logs to external syslog servers via a trusted channel. This trusted channel is secured via IPSec encryption. The ASR1K facilitates remote authentication with AAA servers. This trusted channel is secured via IPSec encryption.

1.6.8 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.

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

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.4.

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

2.2 Protection Profile Conformance

The TOE and ST are conformant with the U.S. Government Protection Profile for Security Requirements for Network Devices(NDPP).

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

Table 9: Protection Profiles

Protection Profile	Version	Date
U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP)	1.1	08 June 2012

2.2.1 Protection Profile Additions

The ST claims strict conformance to the NDPP and does not include any additions to the functionality described in the Protection Profile.

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

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

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 for which conformance is claimed verbatim.

The Security Objectives included in the Security Target represent the Security Objectives specified in the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 for which conformance is claimed verbatim. All concepts covered in the Protection Profile'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 U.S. Government Protection Profile for Security Requirements for Network Devices, Version 1.1 for which conformance is claimed verbatim. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in section 4.3 of the NDPP.

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.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

The following table lists the threats addressed by the TOE and the 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.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

Threat	Threat Definition
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Organizational Security Policies

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

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

Table 13 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security Objectives for the Environment

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

Table 14 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 SECURITY REQUIREMENTS

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

5.1 Conventions

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

- Where operations were completed in the NDPP itself, the formatting used in the NDPP has been retained;
- Assignment: Indicated by showing the value in square brackets with italicized text, [*assignment_value*];
- Refinement: Indicated with **bold** text and strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

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

5.2 TOE Security Functional Requirements

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

Table 15 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)

Class Name	Component Identification	Component Name
	FCS_IPSEC_EXT.1	Explicit: IPSEC
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
FMT: Security management	FMT_MTD.1	Management of TSF Data (for general TSF data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TUD_EXT.1	Extended: Trusted Update
	FPT_TST_EXT.1	TSF Testing
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

5.3 SFRs

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 of the audit functions;
b) All auditable events for the not specified level of audit; and
c) *All administrative actions*;
d) [*Specifically defined auditable events listed in Table 14*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 14*].

Table 16 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.

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

5.3.1.2 FAU_GEN.2 User Identity Association

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

5.3.1.3 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel implementing the IPsec protocol.

5.3.2 Cryptographic Support (FCS)

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

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

• NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;
• NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits.*

5.3.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

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

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

FCS_COP.1.1(1) Refinement: The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in* [*ECB and CBC mode*]] and cryptographic key sizes 128-bits, 256-bits, and 192 bits that meets the following:

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

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

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

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

that meets the following:

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

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

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

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

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

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

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of 256 bits of entropy at least equal to the greatest **security strength** of the keys and hashes that it will generate.

5.3.2.8 FCS_IPSEC_EXT.1: IPSEC

FCS_IPSEC_EXT.1.1 The TSF shall implement IPSec using the ESP protocol as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), no other algorithms and using IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and no other RFCs for hash functions; and no other RFCs for hash functions.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [*an administratively configurable number between 100 – 200*] MB of traffic for Phase 2 SAs.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP) and no other DH groups.

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the rDSA algorithm.

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

- Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(","), *"[and no other special characters];*
- Pre-shared keys of 22 characters and greater than 22 characters in length.

5.3.3 User data protection (FDP)

5.3.3.1 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to, deallocation of the resource from all objects.

5.3.4 Identification and authentication (FIA)

5.3.4.1 FIA_PMG_EXT.1 Password Management

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [*no other characters*];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.3.4.2 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- no other actions.

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

5.3.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

5.3.4.4 FIA_UAU.7 Protected Authentication Feedback

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

5.3.5 Security management (FMT)

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

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

5.3.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to update the TOE, and to verify the updates using* published hash *capability prior to installing those updates*;
- *Ability to configure the cryptographic functionality*;

5.3.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Authorized Administrator**.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

5.3.6 Protection of the TSF (FPT)

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

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

5.3.6.2 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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

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

5.3.6.3 FPT_STM.1 Reliable time stamps

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

5.3.6.4 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

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

5.3.6.5 FPT_TST_EXT.1: TSF Testing

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

5.3.1 TOE Access (FTA)

5.3.1.1 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.

5.3.1.2 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*].

5.3.1.3 FTA_SSL.4 User-initiated Termination

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

5.3.1.4 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Refinement: Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.3.1 Trusted Path/Channels (FTP)

5.3.1.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **use** IPsec to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server [authentication server [***remote IPsec peer* **]]** 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,*
- *remote peers using IPsec*].

5.3.1.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** IPSec provide a **trusted** communication path between itself and **remote administrators** that is logically distinct from other communication

paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.

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

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

5.3.2 TOE SFR Dependencies Rationale for SFRs Found in NDPP

This ST claims conformance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1. The NDPPv1.1 contains all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

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

Table 17: 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

5.4.2 Security Assurance Requirements Rationale

This Security Target claims conformance to the NDPP which essentially is an EAL1 conformance claim. This target was chosen to ensure that the TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.

5.5 Assurance Measures

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

Table 18: 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 ALC_CMS.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 19: How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, 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. 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: 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) 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" The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. For instance all emergency, alerts, critical, errors, and warning messages can be sent to the console and local buffer 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 channel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established. The logging buffer size can be configured from a range of 4096 (default) to

TOE SFRs	How the SFR is Met
	4,294,967,295 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. The administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc. 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. 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.
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below: 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
FAU_STG_EXT.1	The TOE is configured to export syslog records to a specified, external syslog server. The TOE protects communications with an external syslog server via IPSec. 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 2147483647-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. 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.

TOE SFRs	How the SFR is Met
	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.
FCS_CKM.1	The TOE implements a FIPS-approved Deterministic Random Bit Generator for Diffie-Hellman key establishment (conformant to NIST SP 800-56A), and for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE does not implement elliptic-curve-based key establishment schemes. For Diffie-Hellman Key Establishment, the TOE implements the following sections of SP 800-56A: 5.6.3.2.2 5.7 5.7.1 5.7.1.1 The TOE does not perform any operation marked as “Shall Not” or “Should” not in SP 800-56A. Additionally, the TOE does not omit any operation marked as “Shall.” See Table 21 for more details on the TOE’s 800-56A compliance. For RSA Key Establishment, the TOE implements the following sections of SP 800-56B: 6 6.1 6.2 6.3 The TOE does not perform any operation marked as “Shall Not” or “Should not” in SP 800-56B. Additionally, the TOE does not omit any operation marked as “Shall.” See Table 22 for more details on the TOE’s 800-56B compliance. The key pair generation portions of “The RSA Validation System” for FIPS 186-2 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.
FCS_CKM_EXT.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form.
FCS_COP.1 (1)	The TOE provides symmetric encryption and decryption capabilities using AES in ECB and CBC mode (128, 192, 256 bits) as described in NIST SP 800-38A. Please see CAVP certificate in Table 6 for validation details. AES is implemented in the following protocols: IPSEC.
FCS_COP.1(2)	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-3, “Digital Signature Standard” and FIPS PUB 186-2, “Digital Signature Standard”. Please see CAVP certificate in Table 6 for validation details.
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1 and SHA-256 as specified in FIPS Pub 180-3 “Secure Hash Standard.” 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 as specified in FIPS Pub 198-1,"The Keyed-Hash Message Authentication Code,” and FIPS 180-3, “Secure Hash Standard.” 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

TOE SFRs	How the SFR is Met
	(DRBG), as specified in SP 800-90. The DRBG is supplied with entropy from jitter from the internal OCTEON processor which produces a minimum of 256 bits of entropy.
FCS_IPSEC_EXT.1	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 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 using AES-CBC-128, AES-CBC-256, and SHA-1 hashes. IPSec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPSec Security Association (SA). The IKE protocols implement Peer Authentication using the rDSA algorithm. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPSec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPSec peers that is also used to manage IPSec connections, including: The negotiation of mutually acceptable IPSec options between peers (including peer authentication parameters, either signature based or pre-shared key based), The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE supports IKEv1 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use mainmodeusing the ‘crypto isakmp aggressive-mode disable’ command. The TOE can be configured to not allow “confidentiality only” ESP mode by ensuring the IKE Policies configured include ESP-encryption. Main mode is the default mode and the crypto isakmp aggressive-mode disable ensures all IPSec negotiations will be handled in the default main mode. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour. The TOE supports the configure of maximum traffic that is allowed to flow for a given IPSec SA using the following command, ‘crypto ipsec security-association lifetime’. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. The TOE is configured to use a range between 100-200 MB as specified in the SFR. The TOE supports Diffie-Hellman Group 14 (2048-bit keys) in support of IKE Key Establishment.

TOE SFRs	How the SFR is Met
	The TOE can be configured to use pre-shared keys with a given peer. When a pre-shared key is configured, the IPSec tunnel with be established using the configured pre-shared key provided that the peer also has the pre-shared key. Pre-shared keys used for IPSec can be constructed of essentially any alphabetic character (upper and lower case), numerals, and special characters (e.g., "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")") and can be anywhere from 1 to 128 characters in length. The TOE requires suitable keys to be entered by an authorized administrator using a CLI function. If the key pair is used for IPsec, the operational procedure to establish and use the key pair is as follows: 1. The administrator configures the device with standard IPsec configuration. Authentication via RSA Signatures is the default authentication method for the IKE proposal. 2. The administrator generates the RSA key pair via the command line "crypto key generate rsa". This key pair is used for IKE negotiation. 3. The administrator configures the PKI entity and PKI domain to retrieve and request the CA certificate and local certificate with RSA key pairs. The local certificate has public RSA key. 4. IKE negotiation will be triggered to set up SAs when there is protected subnet traffic in the device. 5. In the IKE phase 1 main mode negotiation, the 5th IKE packet has signature payload signed by RSA private key and certificate payload with RSA public key. When receiving this IKE packet, the device verifies the signature payload using the public key in the certificate payload.
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from data allocated to or deallocated from previous packets. Packets that are not the required length use a four-byte repeating pattern for padding. Residual data is never transmitted from the TOE. Once packet handling is completed, its content is zeroized (overwritten with 0x00) before allocation to or deallocation from the memory buffer which previously contained the packet is reused. This applies to both data plane traffic and administrative session traffic.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of up 15 characters.

TOE SFRs	How the SFR is Met
FIA_UIA_EXT.1/ FIA_UAU_EXT.2	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. The TOE can be configured to require local authentication and/or remote authentication via a RADIUS or TACACS+ server as defined in the authentication policy for interactive (human) users. 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. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via IPSec. 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 TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FMT_MTD.1	The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds. 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 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. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege.
FMT_SMF.1	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, Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above. The ability to update the IOS-XE software (image integrity verification is provided using SHA-256) Ability to configure the cryptographic functions
FMT_SMR.2	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 privilege level 15; and the semi-privileged role

TOE SFRs	How the SFR is Met
	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. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The privilege level determines the functions the user can perform; hence the Authorized Administrator with the appropriate privileges. Refer to the Guidance documentation and IOS Command Reference Guide for available commands and associated roles and privilege levels. The TOE can and shall be configured to authenticate all access to the command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote authentication via IPSec.
FPT_SKP_EXT.1	While the administrative CLI is function rich, the TOE is designed specifically to not disclose any keys stored in the TOE. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. For more detailed information regarding key storage see Table 20; note, while some keys occur in plain text in RAM, that is only while they are in use and are not accessible by any user from RAM. Encrypted keys are configured on the TOE using the 'password encryption aes' command. The TOE is configured to not display configured keys as part of configuration files using the 'hidekeys' command.
FPT_APW_EXT.1	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.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from an NTP server. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. 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.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from the Cisco.com web site. Authorized Administrators can download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html. The cryptographic checksums (i.e., public hashes/SHA-256) 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. Once the file is downloaded from the Cisco.com web site, verify that it was not tampered. The verification is done by using a hash utility to compute a hash value for the downloaded file and comparing this with the hash value for the image. The hash value can be displayed by hovering over the software image name under details on the Cisco.com web site. If the hashes do not match, contact Cisco Technical Assistance Center (TAC).

TOE SFRs	How the SFR is Met
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self-tests during initial start-up to verify its correct operation. 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: • 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 Known Answer Test • Triple-DES Known Answer Test • Software Integrity Test 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. 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. Entropy heath tests run at startup via the bootloader. There are no on-demand tests implemented. However, periodic continuous tests are performed to ensure that a newly generated block is compared with a previously generated saved block. If a repeated block is generated, a failure event occurs and the platform will be shut down. 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.
FTA_SSL_EXT.1 FTA_SSL.3	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. If a local user session is inactive for a configured period of time, the session will be locked and will require re-authentication to unlock the session. If a remote user session is inactive fr a configured period of time, the session will be terminated and will require authentication to establish a new session. 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.
FTA_SSL.4	Each administrator logged onto the TOE can manually terminate her 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	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 TOE also requires that peers and other TOE instances establish an IKE/IPSec connection in order to forward routing tables used by the TOE. The TOE protects communications between the TOE and the remote audit server using IPsec. This

TOE SFRs	How the SFR is Met
	provides a secure channel to transmit the log events. Likewise communications between the TOE and AAA servers are secured using IPsec.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted IPSec session. The IPSec session is encrypted using AES encryption. The remote users are able to initiate IPSec communications with the TOE.

7 ANNEX A: ADDITIONAL INFORMATION

7.1 Key Zeroization

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

Table 20: 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 ISAKMP id	This is an IKE intermittent value used to create skeyid_d. Value derived per the IKE protocol based on the peer authentication method chosen.	SDRAM (plaintext)	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d ISAKMP id	This is an IKE intermittent value used to derive keying data for IPSec. The IKE key derivation key for non ISAKMP security associations.	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	NVRAM (plaintext)	Zeroized using the following command: **# crypto key zeroize rsa** Overwritten with: 0x0d

Name	Description of Key	Storage	Zeroization
	the device. This trustpoint authenticates with the CA server to get the CA certificate and also enrolls with the CA server to generate the device certificate. 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.		
IPSec encryption key	This is the key used to encrypt IPsec sessions.	SDRAM (plaintext)	Automatically when IPSec session terminated. Overwritten with: 0x00
IPSec authentication key	This is the key used to authenticate IPsec sessions.	SDRAM (plaintext)	Automatically when IPSec session terminated. Overwritten with: 0x00
RADIUS secret	Shared secret used as part of the Radius authentication method.	NVRAM (plaintext)	Zeroized using the following command: **# no radius-server key** Overwritten with: 0x0d
TACACS+ secret	Shared secret used as part of the TACACS+ authentication method.	NVRAM (plaintext)	Zeroized using the following command: **# no tacacs-server key** Overwritten with: 0x0d

7.2 800-56 Compliance

The TOE is compliant as described in Table 21 below.

Table 21 800-56A Compliance

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5.1 Cryptographic Hash Functions	All in section	Yes	N/A
5.2 Message Authentication Code (MAC) Algorithm	All in section	Yes	N/A
5.2.1 MacTag Computation	All in section	Yes	N/A
5.2.2 MacTag Checking	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5.2.3 Implementation Validation Message	All in section	Yes	N/A
5.3 Random Number Generation	All in section	Yes	N/A
5.4 Nonces	All in section	Yes	N/A
5.5 Domain Parameters	All in section	Yes	N/A
5.5.1 Domain Parameter Generation	All in section	Yes	N/A
5.5.1.1 FFC Domain Parameter Generation	All in section	Yes	N/A
5.5.1.2 ECC Domain Parameter Generation	all in section	N/A	TOE is not using elliptic curve
5.5.2 Assurances of Domain Parameter Validity	All in section	Yes	N/A
5.5.3 Domain Parameter Management	All in section	Yes	N/A
5.6 Private and Public Keys	All in section	Yes	N/A
5.6.1 Private/Public Key Pair Generation	All in section	Yes	N/A
5.6.1.1 FFC Key Pair Generation	For the FFC schemes, each static and ephemeral private key and public key shall be generated using an Approved method and the selected valid domain parameters (p, q, g{, SEED, pgenCounter}) (see Appendix B of FIPS 186-3).	No	Prime number generation is done as described in ANSI X9.31 rather than as described.
	Each private key shall be unpredictable and shall be generated in the range [1, q-1] using an Approved random bit generator.	Yes	N/A
5.6.1.2 ECC Key Pair Generation	For the ECC schemes, each static and ephemeral private key d and public key Q shall be generated using an Approved method and the selected domain parameters (q, FR, a, b{, SEED}, G, n, h)	N/A	TOE is not using elliptic curve
	Each private key, d, shall be unpredictable and shall be generated in the range [1, n-1] using an Approved random bit generator.	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5.6.2 Assurances of the Arithmetic Validity of a Public Key	All in section	Yes	N/A
5.6.2.1 Owner Assurances of Static Public Key Validity	All in section	Yes	N/A
5.6.2.2 Recipient Assurances of Static Public Key Validity	All in section	Yes	N/A
5.6.2.3 Recipient Assurances of Ephemeral Public Key Validity	All in section	Yes	N/A
5.6.2.4 FFC Full Public Key Validation Routine	All in section	Yes	N/A
5.6.2.5 ECC Full Public Key Validation Routine	All in section	N/A	TOE is not using elliptic curve
5.6.2.6 ECC Partial Public Key Validation Routine	All in section	N/A	TOE is not using elliptic curve
5.6.3 Assurances of the Possession of a Static Private Key	All in section	Yes	N/A
5.6.3.1 Owner Assurances of Possession of a Static Private Key	All in section	Yes	N/A
5.6.3.2 Recipient Assurance of Owner's Possession of a Static Private Key	All in section	Yes	N/A
5.6.3.2.1 Recipient Obtains Assurance through a Trusted Third Party	All in section	Yes	N/A
5.6.3.2.2 Recipient Obtains Assurance Directly from the Claimed Owner	All in section	Yes	N/A
5.6.4 Key Pair Management	All in section	Yes	N/A
5.6.4.1 Common Requirements on Static and Ephemeral Key Pairs	All in section	Yes	N/A
5.6.4.2 Specific Requirements on Static Key Pairs	All in section	Yes	N/A
5.6.4.3 Specific Requirements on Ephemeral Key Pairs	All in section	Yes	N/A
5.7 DLC Primitives	All in section	Yes	N/A
5.7.1 Diffie-Hellman Primitives	All in section	Yes	N/A
5.7.1.1 Finite Field Cryptography Diffie-Hellman (FFC DH) Primitive	All in section	Yes	N/A
5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) Primitive	All in section	N/A	TOE is not using elliptic curve
5.7.2 MQV Primitives	All in section	Yes	N/A
5.7.2.1 Finite Field Cryptography MQV (FFC MQV) Primitive	All in section	Yes	N/A
5.7.2.1.1 MQV2 Form of the FFC MQV Primitive	All in section	Yes	N/A
5.7.2.1.2 MQV1 Form of the FFC MQV Primitive	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5.7.2.2 ECC MQV Associate Value Function	All in section	N/A	TOE is not using elliptic curve
5.7.2.3 Elliptic Curve Cryptography MQV (ECC MQV) Primitive	All in section	N/A	TOE is not using elliptic curve
5.7.2.3.1 Full MQV Form of the ECC MQV Primitive	All in section	N/A	TOE is not using elliptic curve
5.7.2.3.2 One-Pass Form of the ECC MQV Primitive	All in section	N/A	TOE is not using elliptic curve
5.8 Key Derivation Functions for Key Agreement Schemes	All in section	Yes	N/A
5.8.1 Concatenation Key Derivation Function (Approved Alternative 1)	All in section	Yes	N/A
5.8.2 ASN.1 Key Derivation Function (Approved Alternative 2)	All in section	Yes	N/A
6. Key Agreement	All in section	Yes	N/A
6.1 Schemes Using Two Ephemeral Key Pairs, C(2)	All in section	Yes	N/A
6.1.1 Each Party Has a Static Key Pair and Generates an Ephemeral Key Pair, C(2, 2)	All in section	Yes	N/A
6.1.1.1 dhHybrid1, C(2, 2, FFC DH)	All in section	Yes	N/A
6.1.1.2 Full Unified Model, C(2, 2, ECC CDH)	All in section	N/A	TOE is not using elliptic curve
6.1.1.3 MQV2, C(2, 2, FFC MQV)	All in section	Yes	N/A
6.1.1.4 Full MQV, C(2, 2, ECC MQV)	All in section	N/A	TOE is not using elliptic curve
6.1.1.5 Rationale for Choosing a C(2, 2) Scheme	All in section	Yes	N/A
6.1.2 Each Party Generates an Ephemeral Key Pair; No Static Keys are Used, C(2, 0)	All in section	Yes	N/A
6.1.2.1 dhEphem, C(2, 0, FFC DH)	All in section	Yes	N/A
6.1.2.2 Ephemeral Unified Model, C(2, 0, ECC CDH)	All in section	N/A	TOE is not using elliptic curve
6.1.2.3 Rationale for Choosing a C(2, 0) Scheme	All in section	Yes	N/A
6.2 Schemes Using One Ephemeral Key Pair, C(1)	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
6.2.1 Initiator Has a Static Key Pair and Generates an Ephemeral Key Pair; Responder Has a Static Key Pair, C(1, 2)	All in section	Yes	N/A
6.2.1.1 dhHybridOneFlow, C(1, 2, FFC DH)	All in section	Yes	N/A
6.2.1.2 One-Pass Unified Model, C(1, 2, ECC CDH)	All in section	N/A	TOE is not using elliptic curve
6.2.1.3 MQV1, C(1, 2, FFC MQV)	All in section	Yes	N/A
6.2.1.4 One-Pass MQV, C(1, 2, ECC MQV)	All in section	N/A	TOE is not using elliptic curve
6.2.1.5 Rationale for Choosing a C(1, 2) Scheme	All in section	Yes	N/A
6.2.2 Initiator Generates Only an Ephemeral Key Pair; Responder Has Only a Static Key Pair, C(1, 1)	All in section	Yes	N/A
6.2.2.1 dhOneFlow, C(1, 1, FFC DH)	All in section	Yes	N/A
6.2.2.2 One-Pass Diffie-Hellman, C(1, 1, ECC CDH)	All in section	N/A	TOE is not using elliptic curve
6.2.2.3 Rationale in Choosing a C(1, 1) Scheme	All in section	Yes	N/A
6.3 Scheme Using No Ephemeral Key Pairs, C(0, 2)	All in section	Yes	N/A
6.3.1 dhStatic, C(0, 2, FFC DH)	All in section	Yes	N/A
6.3.2 Static Unified Model, C(0, 2, ECC CDH)	All in section	N/A	TOE is not using elliptic curve
6.3.3 Rationale in Choosing a C(0, 2) Scheme	All in section	Yes	N/A
7. DLC-Based Key Transport	All in section	Yes	N/A
8. Key Confirmation	All in section	Yes	N/A
8.1 Assurance of Possession Considerations when using Key Confirmation	All in section	Yes	N/A
8.2 Unilateral Key Confirmation for Key Agreement Schemes	All in section	Yes	N/A
8.3 Bilateral Key Confirmation for Key Agreement Schemes	All in section	Yes	N/A
8.4 Incorporating Key Confirmation into a Key Agreement Scheme	All in section	Yes	N/A
8.4.1 C(2, 2) Scheme with Unilateral Key Confirmation Provided by U to V	All in section	Yes	N/A
8.4.2 C(2, 2) Scheme with Unilateral Key Confirmation Provided by V to U	All in section	Yes	N/A
8.4.3 C(2, 2) Scheme with Bilateral Key Confirmation	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
8.4.4 C(1, 2) Scheme with Unilateral Key Confirmation Provided by U to V	All in section	Yes	N/A
8.4.5 C(1, 2) Scheme with Unilateral Key Confirmation Provided by V to U	All in section	Yes	N/A
8.4.6 C(1, 2) Scheme with Bilateral Key Confirmation	All in section	Yes	N/A
8.4.7 C(1, 1) Scheme with Unilateral Key Confirmation Provided by V to U	All in section	Yes	N/A
8.4.8 C(0, 2) Scheme with Unilateral Key Confirmation Provided by U to V	All in section	Yes	N/A
8.4.9 C(0, 2) Scheme with Unilateral Key Confirmation Provided by V to U	All in section	Yes	N/A
8.4.10 C(0, 2) Scheme with Bilateral Key Confirmation	All in section	Yes	N/A

Table 22 800-56B Compliance

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5 Cryptographic Elements	All in section	Yes	N/A
5.1 Cryptographic Hash Functions	All in section	Yes	N/A
5.2 Message Authentication Code (MAC) Algorithm	All in section	Yes	N/A
5.2.1 MacTag Computation	All in section	Yes	N/A
5.2.2 MacTag Checking	All in section	Yes	N/A
5.2.3 Implementation Validation Message	All in section	Yes	N/A
5.3 Random Bit Generation	All in section	Yes	N/A
5.4 Prime Number Generators	Only approved prime number generation methods shall be employed in this Recommendation.	No	We are ANSI X9.31 compliant. However, the requirements in this SP have recently changed.
5.5 Primality Testing Methods	All in section	Yes	N/A
5.6 Nonces	All in section	Yes	N/A
5.7 Symmetric Key-Wrapping Algorithms	All in section	Yes	N/A
5.8 Mask Generation Function (MGF)	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
5.9 Key Derivation Functions for Key Establishment Schemes	All in section	Yes	N/A
5.9.1 Concatenation Key Derivation Function (Approved Alternative 1)	All in section	Yes	N/A
5.9.2 ASN.1 Key Derivation Function (Approved Alternative 2)	All in section	Yes	N/A
6 RSA Key Pairs	All in section	Yes	N/A
6.1 General Requirements	All in section	Yes	N/A
6.2 Criteria for RSA Key Pairs for Key Establishment	All in section	Yes	N/A
6.2.1 Definition of a Key Pair	All in section	Yes	N/A
6.2.2 Formats	All in section	Yes	N/A
6.2.3 Parameter Length Sets	All in section	Yes	N/A
6.3 RSA Key Pair Generators	All in section	Yes	N/A
6.3.1 RSAKPG1 Family: RSA Key Pair Generation with a Fixed Public Exponent	No shall statements (def of approved key pair generator)	Yes	N/A
6.3.2 RSAKPG2 Family: RSA Key Pair Generation with a Random Public Exponent	No shall statements (def of approved key pair generator)	Yes	N/A
6.4 Assurances of Validity	All in section	Yes	N/A
6.4.1 Assurance of Key Pair Validity	All in section	Yes	N/A
6.4.2 Recipient Assurances of Public Key Validity	All in section	Yes	N/A
6.5 Assurances of Private Key Possession	All in section	Yes	N/A
6.5.1 Owner Assurance of Private Key Possession	All in section	Yes	N/A
6.5.2 Recipient Assurance of Owner's Possession of a Private Key	All in section	Yes	N/A
6.6 Key Confirmation	All in section	Yes	N/A
6.6.1 Unilateral Key Confirmation for Key Establishment Schemes	All in section	Yes	N/A
6.6.2 Bilateral Key Confirmation for Key Establishment Schemes	All in section	Yes	N/A
6.7 Authentication	All in section	Yes	N/A
7 IFC Primitives and Operations	All in section	Yes	N/A
7.1 Encryption and Decryption Primitives	All in section	Yes	N/A
7.1.1 RSAEP	All in section	Yes	N/A
7.1.2 RSADP	All in section	Yes	N/A
7.2 Encryption and Decryption Operations	All in section	Yes	N/A
7.2.1 RSA Secret Value Encapsulation (RSASVE)	All in section	Yes	N/A

Section	Shall/Shall Not Statement(s)	Compliant?	Rationale
7.2.2 RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP)	All in section	Yes	N/A
7.2.3 RSA-based Key-Encapsulation Mechanism with a Key-Wrapping Scheme	All in section	Yes	N/A
(RSA-KEM-KWS)	All in section	Yes	N/A
8 Key Agreement Schemes	All in section	Yes	N/A
8.1 Common Components for Key Agreement	All in section	Yes	N/A
8.2 The KAS1 Family	All in section	Yes	N/A
8.2.1 KAS1 Family Prerequisites	All in section	Yes	N/A
8.2.2 KAS1-basic	All in section	Yes	N/A
8.2.3 KAS1 Key Confirmation	All in section	Yes	N/A
8.2.4 KAS1 Security Properties	All in section	Yes	N/A
8.3 The KAS2 Family	All in section	Yes	N/A
8.3.1 KAS2 Family Prerequisites	All in section	Yes	N/A
8.3.2 KAS2-basic	All in section	Yes	N/A
8.3.3 KAS2 Key Confirmation	All in section	Yes	N/A
8.3.4 KAS2 Security Properties	All in section	Yes	N/A
9 IFC based Key Transport Schemes	All in section	Yes	N/A
9.1 Additional Input	All in section	Yes	N/A
9.2 KTS-OAEP Family: Key Transport Using RSA-OAEP	All in section	Yes	N/A
9.2.1 KTS-OAEP Family Prerequisites	All in section	Yes	N/A
9.2.2 Common components	All in section	Yes	N/A
9.2.3 KTS-OAEP-basic	All in section	Yes	N/A
9.2.4 KTS-OAEP Key Confirmation	All in section	Yes	N/A
9.2.5 KTS-OAEP Security Properties	All in section	Yes	N/A
9.3 KTS-KEM-KWS Family: Key Transport using RSA-KEM-KWS	All in section	Yes	N/A
9.3.1 KTS-KEM-KWS Family Prerequisites	All in section	Yes	N/A
9.3.2 Common Components of the KTS-KEM-KWS Schemes	All in section	Yes	N/A
9.3.3 KTS-KEM-KWS-basic	All in section	Yes	N/A
9.3.4 KTS-KEM-KWS Key Confirmation	All in section	Yes	N/A
9.3.5 KTS-KEM-KWS Security Properties	All in section	Yes	N/A

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 23: 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
[NDPP]	U.S. Government Protection Profile for Security Requirements for Network Devices, version 1.1, June 8, 2012
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

Identifier	Description
[Security Policy]	Cisco ASR 1001 with integrated RP and integrated ESPr12.5, ASR 1002 with integrated RP1 and ESPr5 or ESPr10, ASR1002-X with integrated RP and integrated ESPr5, ASR 1004 with RP1 or RP2 and ESPr10 or ESPr20 or ESPr40, and ASR 1006 with dual RP1 or RP2 and single/dual ESPr10 or ESPr20 or ESPr40 or ESPr100, ASR 1013 with RP2 and ESPr40 or ESPr100
	Firmware version: 3.7.2 Hardware versions: ASR1001, ASR1002, ASR1002-X, ASR1004, ASR1006, ASR1013; Embedded Services Processor (ESP) Hardware versions:
	ASR1000-ESPr5, ASR1000-ESP10, ASR1000-ESPr20, ASR1000-ESPr40, ASR1000-ESPr100; Route Processor (RP) Hardware versions: ASR-1000-RP1, ASR-1000-RP2 FIPS-140 Security Policy

[1] "r" has been added in order to differentiate the Embedded Services Processor from the Encapsulating Security Payload