Cisco Aggregation Services Router (ASR) 901 Series

Security Target

Version 1.0

26 March 2015

Table of Contents

List of Tables

List of Acronyms

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

Table 1: Acronyms

Acronyms/Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
BGP	Border Gateway Protocol. An inter-domain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems)
Bridge Domain	A bridge domain is a local broadcast domain that is VLAN-ID-agnostic.
BSC	Base Station Controllers
BTS	Base Transceiver Stations
CC	Common Criteria for Information Technology Security Evaluation
CE	Carrier Ethernet
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EFP	Ethernet Flow Point. An EFP service instance is a logical interface that connects a bridge domain to a physical port or to an EtherChannel group in a router.
ENI	Enhanced Network Interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), EtherChannel Link Aggregation Control Protocol (LACP).
EtherChannel	An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.
EVC	Ethernet Virtual Connection., a conceptual service pipe within the service provider network.
FIPS	Federal Information Processing Standard
GE	Gigabit Ethernet port
HA	High Availability (device or component failover)
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IS-IS	Intermediate System to Intermediate System. An Open System Interconnection (OSI) protocol that specifies how routers communicate with routers in different domains.
IT	Information Technology
LAN	Local Area Network
MEF	Metro-Ethernet Forum. A MEF defines Ethernet Virtual Connection (EVC) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network.
MSC	Mobile Switching Center
NDPP	Network Device Protection Profile
NNI	Network Node Interfaces (NNIs) to connect to the service provider network
NTP	Network Time Protocol
OS	Operating System
OSPF	Open Shortest Path First. An interior gateway protocol (routes within a single

Acronyms/Abbreviations	Definition
	autonomous system). A link-state routing protocol which calculates the shortest path to each node.
PP	Protection Profile
RAN	Radio Access Network
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TDM	Time-division multiplexing. Is a method of putting multiple data streams in a single transmission signal, separating the signal into many segments, each having a very short duration, hence each data stream having their own time slot on the channel.
Trunk Port	A port that sends and receives tagged frames on all VLANs, except the native VLAN, if one is configured. Frames belonging to the native VLAN do NOT carry VLAN tags when sent over the trunk. Conversely, if an untagged frame is received on a trunk port, the frame is associated with the native VLAN configured on that port.
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UNI	User Network Interfaces (UNIs) to connect to customer networks.
WAN	Wide Area Network
VLAN	Virtual Local Area Network

Terminology

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer router	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 VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another router.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).

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

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- 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) 901 Series Security Target
ST Version	1.0
Publication Date	26 March 2015
Developer and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Aggregation Services Router (ASR) 901 Series
TOE Hardware Models	ASR 901 includes the following models: A901-12C-F-D, A901-12C-FT-D, A901-4C-F-D, A901-4C-FT-D, A901-6CZ-F-D, A901-6CZ-FT-D, A901-6CZ-F-A, A901-6CZ-FT-A, A901-6CZ-FS-D, A901-6CZ-FS-A
TOE Software Version	IOS 15.5(1)S1
Keywords	Audit, Authentication, Encryption, Protection, Router, Traffic

1.2 TOE Overview

The Cisco Aggregation Services Router (ASR) 901 Series TOE is a compact cell-site Radio Access Network (RAN) and Ethernet access routers that transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1/E1 circuits, including leased line, microwave, and satellite.

The RAN transport manages the backhaul traffic (both voice and data) from the cell site base transceiver stations (BTSs) to aggregation nodes and to base station controllers (BSCs), between BSCs, and between the BSC and an associated mobile switching center (MSC).

The TOE consists of any one of a number of hardware models as listed above in Table 3: ST and TOE Identification, each running the same version of IOS software. The ASR 901 Series chassis provides power, cooling, and backplane for the Ethernet interfaces and Small Form-Factor Pluggable (SFP) and enhanced SFP (SFP+) optics modules, as defined in Table 3 in Section 1.1.

Cisco IOS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing. 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 1.4.4 TOE logical scope below.

1.2.1 TOE Product Type

The Cisco Aggregation Services Router (ASR) 901 Series is a cell-site access platform specifically designed to aggregate and transport mixed-generation RAN traffic. The RAN cell sites are places of transformation between mobile radio and mobile transport networks. The Cisco ASR 901 routers are designed to minimize operating costs and optimize this radio-to-transport transformation through scalable time-division multiplexing (TDM) and IP/Ethernet interfaces for any combination of multivendor, multi-generation radios and transport networks.

The ASR 901, supports Layer2 Control Protocol Forwarding by performing analysis of incoming frames, makes forwarding decisions based on information contained in the frames, and forwards the frames toward the destination. The router also supports Layer 2 Control Protocol Tunneling for tunneling Ethernet protocol frames across Layer 2 switching domains and Carrier Ethernets (CE). In addition, the router also supports Layer 2 peering. In support of the routing capabilities, the Cisco Aggregation Services Router (ASR) 901 Series supports the listed IP routing protocols in section 1.4 for load balancing and for constructing scalable, routed backbones.

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
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
NTP Server	No	The TOE supports communications with an NTP server to synchronize date and time.
Syslog server	Yes	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides authentication services to TOE administrators.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Aggregation Services Router (ASR) 901 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 is designed for low power consumption, line rate performance for all Layer 2 and Layer 3 interfaces, the different hardware models include A901-12C-F-D, A901-12C-FT-D, A901-4C-F-D, A901-4C-FT-D, A901-6CZ-F-D, A901-6CZ-FT-D, A901-6CZ-F-A, A901-6CZ-FT-A, A901-6CZ-FS-D, A901-6CZ-FS-A. There are also flexible clocking options, and redundant power and cooling. The chassis is the component of the TOE in which all other TOE components are housed.
- Cisco IOS software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco IOS software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will prioritize and process cell-site voice, data and signaling traffic for transport across the available backhaul networks. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination. The TOE supports IPv4, IPv6, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) and Intermediate System-to-Intermediate System (IS-IS) routing, IPv4-to-IPv6 Multicast, MPLS, IPsec, Layer 2 Tunneling Protocol Version 3 (L2TPv3) and Bidirectional Forwarding Detection (BFD) protocols.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the ASR901 is to be remotely administered, then the management workstation station must be connected to an internal network, SSHv2 must be used to connect to the TOE. A syslog server is also used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

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

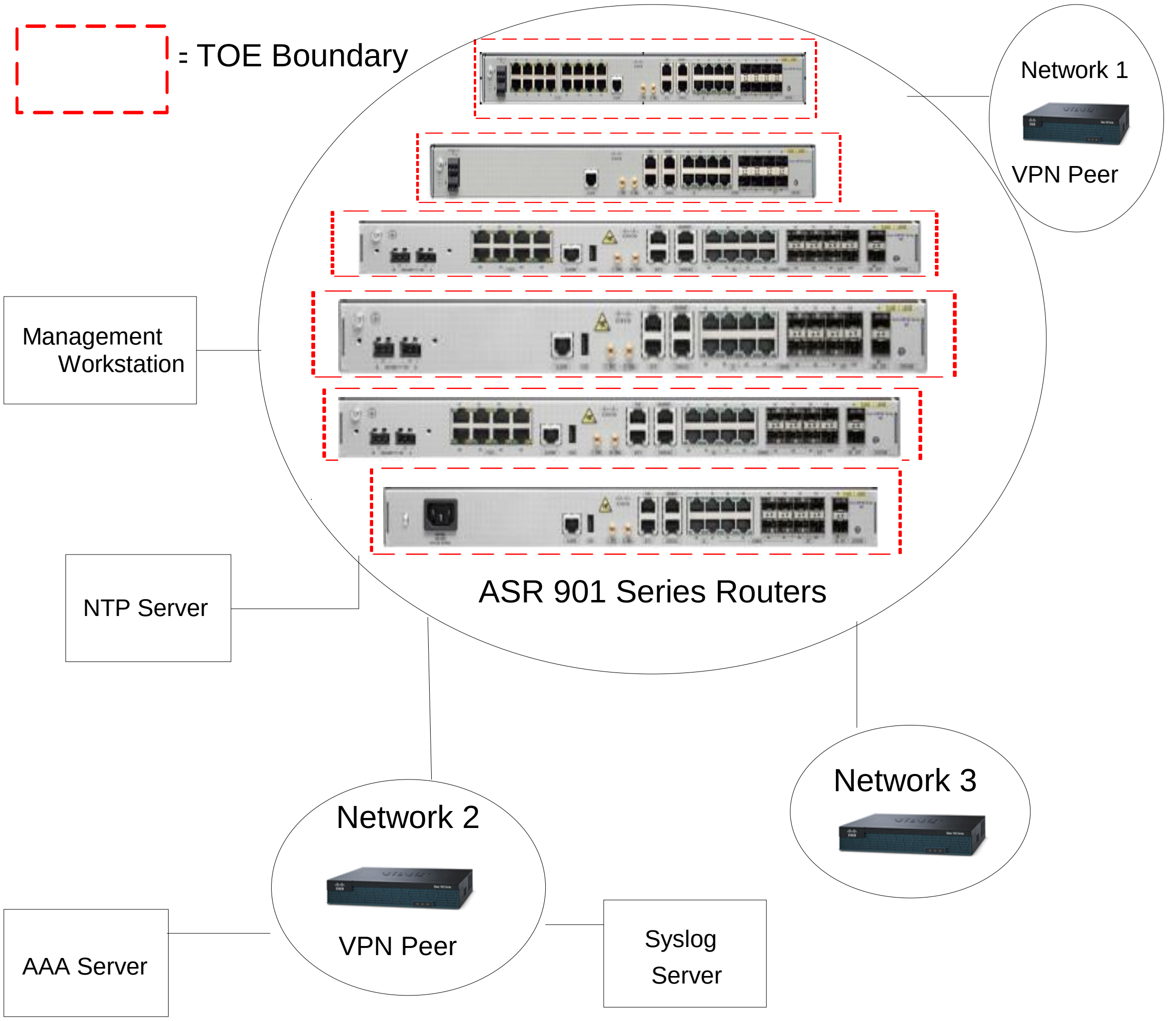


Figure 1 TOE Example Deployment

The previous figure includes the following:

- Examples of TOE Models (models listed in order of diagram)
    - Cisco ASR 901-12C-FT-D and ASR 901-4C-FT-D Routers
    - Cisco ASR 901-12C-F-D and ASR 901-4C-F-D Routers
    - Cisco ASR 901-6CZ-FT-D Router
    - Cisco ASR 901-6CZ-F-D Router
    - Cisco ASR 901-6CZ-FT-A Router
    - Cisco ASR 901-6CZ-F-A Router
- 2 - Peer Routers (IT Environment)
- Management Workstation
- Syslog Server
- AAA Server
- NTP Server

NOTE: While the previous figure includes the available TOE devices and several non-TOE IT environment devices, the TOE is only the ASR 901 device with the Cisco IOS software. Only one TOE device is required 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 shown in the figures below. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco Aggregation Services Router (ASR) 901 Series Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the http://cisco.com web site.

Figures 2 and 3 show the two basic 1-Gigabit Ethernet models of the Cisco ASR 901 Series routers

Figure 2 Cisco ASR 901-12C-FT-D and ASR 901-4C-FT-D Routers

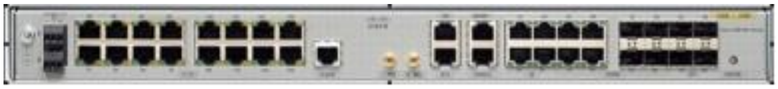
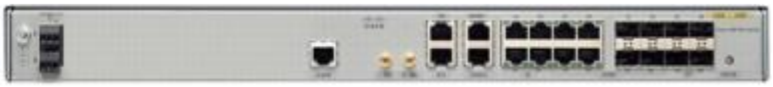


Figure 3 Cisco ASR 901-12C-F-D and ASR 901-4C-F-D Routers



Figures 4 through 7 show the four basic 10-Gigabit Ethernet models of the Cisco ASR 901 Series routers

Figure 4 Cisco ASR 901-6CZ-FT-D Router

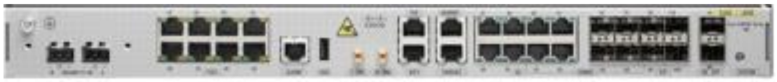


Figure 5 Cisco ASR 901-6CZ-F-D Router

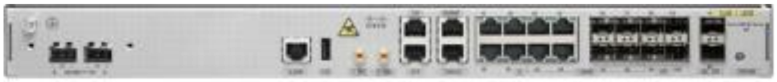


Figure 6 Cisco ASR 901-6CZ-FT-A Router

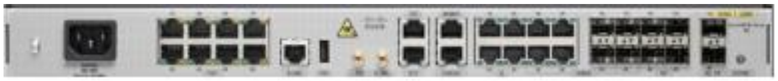
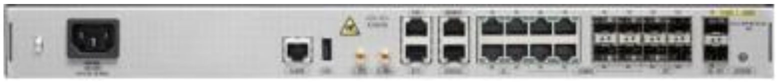


Figure 7 Cisco ASR 901-6CZ-F-A Router



The network, on which the TOE resides, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS software image Release IOS 15.5(1)S1. 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 Components for the Cisco ASR 901 Series	
Part Number	**Description**
A901-12C-F-D	Cisco ASR 901 Series Aggregation Services Router Chassis, Ethernet-only interfaces, DC power
A901-12C-FT-D	Cisco ASR 901 Series Aggregation Services Router Chassis, Ethernet and TDM interfaces, DC power
A901-4C-F-D	Cisco ASR 901 Series Aggregation Services Router Chassis, PAYG 4 GE Port, Ethernet-only interfaces, DC power
A901-4C-FT-D	Cisco ASR 901 Series Aggregation Services Router Chassis, PAYG 4 GE Port, Ethernet and TDM interfaces, DC power
A901-6CZ-F-D	Cisco ASR 901 Series Aggregation Services Router Chassis, Ethernet-only interfaces, 10 GE, DC power, USB
A901-6CZ-FT-D	Cisco ASR 901 Series Aggregation Services Router Chassis, Ethernet and TDM interfaces, 10 GE, DC power, USB
A901-6CZ-F-A	Cisco ASR 901 Series Aggregation Services Router Chassis, Ethernet-only interfaces, 10 GE, AC power, USB
A901-6CZ-FT-A	Cisco ASR 901 Series Aggregation Services Router Chassis, Ethernet and TDM interfaces, 10 GE, AC power, USB
Additional Specification Information	
Memory	Flash memory: 128 MB (onboard flash) System memory: 512 MB (DDR3)
Ethernet ports	4 100/1000 RJ-45 Gigabit Ethernet ports 4 x 1 SFP Gigabit Ethernet ports[1] 4 x 1 Gigabit Ethernet Combo ports[1] 2 x 10 Gigabit Ethernet ports (10 GE models only)
TDM ports	A901-12C-FT-D: 16 T1/E1 A901-4C-FT-D: 16 T1/E1 A901-6CZ-FT-D: 8 T1/E1 A901-6CZ-FT-A: 8 T1/E1
Console port	1 (up to 115.2 Kbps)
USB port	1 supported on the following chassis models: • A901-6CZ-FT-D • A901-6CZ-F-D • A901-6CZ-FT-A • A901-6CZ-F-A
Fans	1 GE models: dual fan, 1+1 redundancy 10 GE models: three fans, with redundancy

Power supplies	2 power supplies (DC only); module redundancy: 1:1 1 power supply (AC only)
Software	
Cisco IOS	15.5(1)S1

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. Cryptography Support
3. User Data Protection
4. Identification & Authentication
5. Security Management
6. Protection of the TSF
7. Trusted Path/Channel
8. TOE Access

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

1.6.1 Security audit

The Cisco Aggregation Services Router (ASR) 901 Series provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of an IPsec SA; establishment, termination and failure of an SSH session; modifications to the group of users that are part of the authorized administrator roles; all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, maximum sessions being exceeded, termination of a remote session and attempts to unlock a termination session; and initiation and termination of a trusted channel.

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

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

1.6.2 Cryptographic support

The TOE provides cryptography in support of other Cisco Aggregation Services Router (ASR) 901 Series security functionality. The algorithms shown in Table 6 FIPS References are implemented in the Cisco IOS Common Cryptographic Module (IC2M) Algorithm Module firmware version 2.0.

This cryptography has been validated for conformance to the requirements of FIPS 140-2 (see Table 6 for certificate references).

Table 6 FIPS References

Algorithm	Cert. #
AES	2817
DRBG	481
SHS (SHA-1, 256, 384, 512)	2361
HMAC SHA-1, 256, 384, 512	1764
RSA	1471
ECDSA	493

While the algorithm implementations listed in the preceding table were not tested on the exact processor installed within the ASR 901, the algorithm certificates are applicable to the TOE based on the following,

1. The cryptographic implementation which is tested is identical (unchanged) to the cryptographic implementation on the ASR 901s.
2. The cryptographic implementation does not depend on hardware for cryptographic acceleration I.e. there are no hardware specific cryptographic dependency. The cryptographic algorithms are implemented completely in software.
3. This is consistent with the guidance provided in NIST IG G.5 allowing portability amongst platforms as long as no software modification is required.

The ASR 901 platforms contain the following processor,

1. Freescale P2020 using the Freescale instruction set

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2. The cryptographic services provided by the TOE are described in Table 7 below.

Table 7 TOE Provided Cryptography

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

1.6.1 User Data 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.

1.6.2 Identification and Authentication

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

The TOE provides authentication services for administrative users to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. 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.

1.6.3 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage:

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

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

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

1.6.4 Protection of the TSF

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

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE’s clock manually, or can configure the TOE to use NTP to synchronize the TOE’s clock with an external time source. Finally, the TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module.

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

The TOE also supports direct connections from VPN clients, and protects against threats related to those client connections. The TOE disconnects sessions that have been idle too long, can be configured to deny sessions based on IP, time, and day, and can be configured to NAT external IPs of connecting VPN clients to internal network addresses.

1.6.5 TOE Access

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

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

1.6.6 Trusted path/Channels

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

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet sends authentication data in the clear. This feature is enabled by default and must be disabled in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target. The exclusion of this feature has no effect on the operation of the TOE. Refer to the Guidance documentation for configuration syntax and information

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 with Security Requirements for Network Devices Errata#2.

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 Protection Profiles as listed in Table 9 below:

Table 9 Protection Profiles

Protection Profile	Version	Date
None (NDPP)	Protection Profile for Network Devices (NDPP)	June 8, 2012
Security Requirements for Network Devices Errata	#2	13 January 2013

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

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

2.3.2 TOE Security Problem Definition Consistency

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

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

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDPPv1.1, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in section 4.3 of the NDPPv1.1.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

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

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

3.1 Assumptions

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

Table 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.

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

3.3 Organizational Security Policies

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

Table 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:

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

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

5.2 TOE Security Functional Requirements

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

Table 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_IPSEC_EXT.1	Explicit: IPSEC

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

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1: Audit data generation

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) *All administrative actions*;
d) [*Specifically defined auditable events listed in* Table 16].

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 16].

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.
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_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session.	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_PSK_EXT	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.

SFR	Auditable Event	Additional Audit Record Contents
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.

5.2.1.2 FAU_GEN.2 User Identity Association

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

5.2.1.3 FAU_STG_EXT.1 External Audit Trail Storage

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

5.2.2 Cryptographic Support (FCS)

5.2.2.1 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 800-56B, “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.

5.2.2.2 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.

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

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

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

5.2.2.4 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 [(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater] that meets the following:

[Case: Digital Signature Algorithm

- **FIPS PUB 186-3, "Digital Signature Standard"].**

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

FCS_COP.1.1(3) Refinement: The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512**] and message digest sizes [**160, 256, 384, 512**] bits** that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

5.2.2.6 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."*

5.2.2.7 FCS_IPSEC_EXT.1 Explicit: IPSEC

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

FCS_IPSEC_EXT.1.2 The TSF shall implement [tunnel mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602)].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [no other RFCs for hash functions]].

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

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [IKEv1 SA lifetimes can be established based on [number of packets/number of bytes and length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [*no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [RSA] algorithm and [Pre-shared Keys].

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

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

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

5.2.2.9 FCS_SSH_EXT.1 Explicit: SSH

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

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

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535 bytes*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [no other algorithms].

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

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha1-96].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [no other methods] are the only allowed key exchange method used for the SSH protocol.

5.2.3 User data protection (FDP)

5.2.3.1 FDP_RIP.2 Full Residual Information Protection

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

5.2.4 Identification and authentication (FIA)

5.2.4.1 FIA_PMG_EXT.1 Password Management

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

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

5.2.4.2 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [up to 128 characters];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [AES] and be able to [accept bit-based pre-shared keys].

5.2.4.3 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 services].

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

5.2.4.4 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

5.2.4.5 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.

5.2.5 Security management (FMT)

5.2.5.1 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*.

5.2.5.2 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;*
  - *[Ability to configure the cryptographic functionality*].

5.2.5.3 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.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 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.

5.2.6.2 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.

5.2.6.3 FPT_STM.1 Reliable time stamps

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

5.2.6.4 FPT_TST_EXT.1: TSF Testing

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

5.2.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

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

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

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [digital signature mechanism] prior to installing those updates.

5.2.7 TOE Access (FTA)

5.2.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.2.7.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.7.3 FTA_SSL.4 User-initiated Termination

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

5.2.7.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.1 Trusted Path/Channels (FTP)

5.2.1.1 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]** 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 [*remote authentication with RADIUS and TACACS+ servers (over IPsec), audit storage with syslog server (over IPsec) and time synchronization with NTP server (over IPsec)*].

5.2.1.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** [**SSH]** 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 TOE SFR Dependencies Rationale for SFRs Found in NDPP

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

5.4 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
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

5.4.2 Security Assurance Requirements Rationale

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

5.5 Assurance Measures

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

Table 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 behaviour of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 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 identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated (e.g. user identity, MAC address, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. The audit trail consist of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes [at least] all of the required information. Additional information can be configured and included if desired. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The logging buffer size can be configured from a range of 4096 (default) up to 2147483647 bytes. It is noted, not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The 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. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The logs can be saved to flash memory so records are not lost in case of failures or restarts. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<p>functionality of the switch is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information; switch functionality is not affected.</p>
<p>To configure the TOE to send audit records to a syslog server, the ‘set logging server’ command is used. A maximum of three syslog servers can be configured. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The audit records are transmitted using IPsec tunnel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established.</p>
<p>The FIPS crypto tests performed during startup, the messages are displayed only on the console. Once the box is up and operational and the crypto self-test command is entered, then the messages would be displayed on the console and will also be logged. For the TSF self-test, successful completion of the self-test is indicated by reaching the log-on prompt. If there are issues, the applicable audit record is generated and displayed on the console.</p>
<table>
<tr><th>Auditable Event</th><th>Rationale</th></tr>
<tr><td>All use of the user identification and authentication mechanism.</td><td>Events will be generated for attempted identification/authentication, and the username attempting to authenticate and the origin of the attempt will be included in the log record.</td></tr>
<tr><td>All use of the authentication mechanism.</td><td>Events will be generated for attempted identification/authentication, and the username attempting to authenticate will be included in the log record, along with the origin or source of the attempt.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Failure on invoking cryptographic functionality to include, asymmetric key generation, key zeroization, cryptographic signature, cryptographic hashing, keyed-hash message authentication and Random Bit Generation</td><td>The audit record will include the default required information for each of the failures when triggered, no additional required</td></tr>
<tr><td>Detection of replay attacks</td><td>Attempts of replaying data previously transmitted and terminated at the TOE are logged, along with the origin or source of the attempt.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td>Changes to the time.</td><td>Changes to the time are logged, including the old and new values for the time along with the origin of the attempt</td></tr>
<tr><td>Updates</td><td>An audit record will be generated on the initiation of updates (software/firmware)</td></tr>
<tr><td>Failure to establish and/or establishment/failure of an IPsec session</td><td>Attempts to establish an IPsec session or the failure of an established IPsec is logged.</td></tr>
<tr><td>Attempts at unlocking interactive sessions</td><td>Any attempt to unlock an inactive sessions is logged</td></tr>
<tr><td>Termination of a remote session by locking the session</td><td>When a session is locked, the session is terminated, thus generating an audit record</td></tr>
<tr><td>Indication that TSF self-test was completed.</td><td>During boot-up, if the self-test fails, the failure is logged.</td></tr>
<tr><td>Trusted channels</td><td>The initiation, termination, and failure related to trusted channel sessions with the remote administration console, syslog server, remote authentication server and if connected the NTP server. The initiator and the target of the trusted channel is identified and included in the audit record.</td></tr>
</table>
</td></tr>
<tr><td>FAU_GEN.2</td><td>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</td></tr>
<tr><td>FAU_STG_EXT.1</td><td>The TOE is configured to export syslog records to a specified, external syslog server. 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.
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. If the IPsec connection fails, the TOE will buffer the audit records on the TOE when it</td></tr>
</table>

TOE SFRs	How the SFR is Met
	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. This buffer store is separate from the local logging buffer, which could be set to a different level of logging then what is to be sent via syslog. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1	The TOE implements a random number generator for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE can create a RSA public-private key pair that can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The key pair generation portions of "The RSA Validation System" for FIPS 186-2 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.
FCS_CKM_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. See 1.1 Key Zeroization for more information on the key zeroization.
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described in NIST SP 800-38A and NIST SP 800-38D. AES is implemented in the following protocols: IPSEC and SSH. The relevant FIPS certificate numbers are listed in Section 1.6.2
FCS_COP.1(2)	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-3, "Digital Signature Standard" and FIPS PUB 186-3, "Digital Signature Standard". The relevant FIPS certificate numbers are listed in Section 1.6.2
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in FIPS Pub 180-3 "Secure Hash Standard." For IKE (ISAKMP) hashing, administrators can select any of SHA-1, SHA-256, SHA-384, and/or SHA-512 (with message digest sizes of 160, 256, 384, and 512 bits respectively) to be used with remote IPsec endpoints. Both SHA-1 and SHA-256 hashing are used for verification of software image integrity. The relevant FIPS certificate numbers are listed in Section 1.6.2
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."
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 in tunnel mode to provide authentication, encryption and anti-replay

TOE SFRs	How the SFR is Met
	services using AES-CBC-128 and AES-CBC-256 together with HMAC-SHA1. The TOE uses IPsec to secure communications with the remote syslog server, with AAA servers (RADIUS and TACACS+) for remote authentication if configured and with NTP servers if configured. IPsec Internet Key Exchange (IKEv1, 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. Phase 1 establishes the secure channel using Diffie-Hellman (DH) key exchange in which the TOE generates the 'secret value' ("x" in "gx mod p") using a random bit generator (RBG) to ensure the length of "x" is at least 256 bits. 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. A crypto map (the Security Policy Definition) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence – the TOE attempts to match the packet to the access list (acl) specified in that entry. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit acls would then flow through the IPsec tunnel and be classified as "PROTECTED". Traffic that does not match a permit crypto map acl and does not match a non-crypto permit acl on the interface would be DISCARDED. Traffic that does not match a permit acl in the crypto map, but does match a non-crypto permit acl would be allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic. 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 will be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode. The TOE will be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption.

TOE SFRs	How the SFR is Met
	The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs The TOE supports Diffie-Hellman Group 14 (2048-bit keys) Peer authentication uses rDSA (RSA), and can be configured to use pre-shared keys. Pre-shared keys include a combination of upper and lower case letters, numbers, and special characters and can be 22 characters or longer. Pre-shared keys are generated and applied to the TOE by the TOE administrator in coordination with the administrator of the remote IPsec endpoint (e.g. AAA server, syslog server, NTP server, or VPN Gateway located between the TOE and those remote servers).
FCS_SSH_EXT.1	The TOE implementation of SSHv2 supports the following: • Compliance with RFCs 4251, 4252, 4253, and 4254; • Dropping packets greater than 65,535 bytes, as such packets would violate the IP packet size limitations; • Encryption algorithms AES-CBC-128, and AES-CBC-256 to ensure confidentiality of the session; • Use of the SSH_RSA public key algorithms for authentication • Password based authentication • Hashing algorithm hmac-sha1 and hamc-sha1-96to ensure the integrity of the session and • Enforcement of DH Group 14 (diffie-hellman-group-14-sha1) as the only allowed key exchange method.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. The entropy source used to seed the Deterministic Random Bit Generator (e.g. based on SP 800-90A/B/C) is a random set of bits or bytes that are regularly supplied to the DRBG by randomly poll the General Purpose Registers and capture entropy from it. This solution is available in the 15.4(4)S or later FIPS/CC approved releases of the IOS images relating to the platforms mentioned above. All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed. Though related to this, the tests are part of the FIPS validation procedures for the DBRG and are part of the NIST validations for FIPS 140-2 for the products. Any initialization or system errors during bring-up or processing of this system causes a reboot as necessary to be FIPS compliant. Finally, the system will be zeroizing any entropy seeding bytes, which will not be available after the current collection.
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros for padding. Residual data is never transmitted from the TOE. Once packet handling is completed its content is overwritten before 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,

TOE SFRs	How the SFR is Met
	numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters.
FIA_PSK_EXT.1	The TOE supports use of IKEv1 (ISAKMP) pre-shared keys for authentication of IPsec tunnels. Pre-shared keys can be entered as ASCII characters (from 22 and up to 128 characters long) using the “crypto isakmp key” command and are conditioned by the TOE (using AES) to a bit-based string used by IKE. Pre-shared keys can also be entered as HEX (“bit-based”) values using the “key-string” command.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the TOE’s CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 connection, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password based authentication mechanism as well as RADIUS and TACACS+ authentication, if configured. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server, if configured. Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via SSHv2. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only ‘*’ characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FMT_MTD.1	The TOE provides the ability for Security Administrators (a.k.a Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds and updates. Each of the predefined and administratively configured privilege level has a set of permissions that will grant them access to the TOE data, though with some privilege levels, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged levels. For the

TOE SFRs	How the SFR is Met
	purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged level equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Security Administrators (a.k.a Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via SSHv2, a terminal server, or at the local console. The specific management capabilities available from the TOE include: • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above; • The ability to update the IOS software (image integrity verification is provided using SHA-256 digital signature) • Ability to configure the cryptographic functionality; • Ability to configure the IPsec functionality, • Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE via the CLI.
FMT_SMR.2	The TOE maintains Authorizer Administrators that include privileged and semi-privileged administrator roles to administer the TOE locally and remotely. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. Note: the levels are not theoretically hierarchical. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The privilege level determines the functions the user can perform; hence the Authorized Administrator with the appropriate privileges. The TOE can and shall be configured to authenticate all access to the command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote authentication via SSH.
FPT_SKP_EXT.1 and	The TOE includes CLI command features that can be used to configure the TOE to

TOE SFRs	How the SFR is Met
FPT_APW_EXT.2	encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The command is the *password encryption aes* command used in global configuration mode. The TOE can also be configured to not display configured keys as part of configuration files using the 'hidekeys' command. The command *service password-encryption* applies encryption to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords. This ensures that plaintext user passwords will not be disclosed even to administrators. The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additional, all pre-shared and symmetric keys are stored in encrypted form to prevent access. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from an NTP server. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.
FPT_TUD_EXT.1	Authorized Administrator can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the software.Cisco.com. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded.
FPT_TST_EXT.1	As a FIPS 140-2 validated product, the TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, the Authorized Administrator will have to log into the CLI to determine which test failed and why. During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO.

TOE SFRs	How the SFR is Met
FTA_SSL_EXT.1 and FTA_SSL.3	An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "session-timeout" setting applied to the console and virtual terminal (vty) lines. The configuration of the vty lines sets the configuration for the remote console access. The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period of time, the session will be locked and will require re-authentication to unlock the session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the "exec-timeout" setting.
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions.
FTA_TAB.1	Authorized administrators define a custom login banner that will be displayed at the CLI (local and remote) prior to allowing Authorized Administrator access through those interfaces.
FTP_ITC.1	The TOE protects communications with authorized IT entities with IPsec. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE.

1 ANNEX A: KEY ZEROIZATION

1.1 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	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in DRAM.	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	The function returns the value to the RP and then calls the function to perform the zeroization of the generated key pair (p_dh_kepair) and then calls the standard Linux free (without the poisoning). These values are automatically zeroized after generation and once the value has been provided back to the actual consumer. This key is stored in DRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
skeyid	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This information and keys are stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This information and keys are stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid,	Automatically after IKE session terminated. Overwritten with: 0x00

Name	Description	Zeroization
	skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's. This key is stored in DRAM.	
ISAKMP preshared	The function calls the free operation with the poisoning mechanism that overwrites the value with 0x0d. This key is stored in DRAM.	Zeroized using the following command: # no crypto isakmp key Overwritten with: 0x0d
IKE RSA Private Key	The operation uses the free operation with the poisoning mechanism that overwrites the value with 0x0d. (This function is used by the module when zeroizing bad key pairs from RSA Key generations.) This key is stored in NVRAM.	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x0d
IPsec encryption key	The function zeroizes an _ike_flow structure that includes the encryption and authentication keys. The entire object is overwritten by 0's using memset. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
IPsec authentication key	The function zeroizes an _ike_flow structure that includes the encryption and authentication keys. The entire object is overwritten by 0's using memset. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
RADIUS secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory. This key is stored in NVRAM.	Zeroized using the following command: # no radius-server key Overwritten with: 0x0d
TACACS+ secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory. This key is stored in NVRAM.	Zeroized using the following command: # no tacacs-server key Overwritten with: 0x0d
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM.	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	The results zeroized using the poisioning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended. . This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00

Name	Description	Zeroization
User Password	This is a Variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password
Enable Password (if used)	This is a Variable 15+ character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM.	Zeroized by overwriting with new password
RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device

2 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 21: 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]	None, version 1.1, June 8, 2012
[ERRATA#2]	Security Requirements for Network Devices Errata #2, 13 January 2013
[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