Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351)

Security Target

Version 1.0
EDCS - 1428573

10 December 2015

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

Table of Contents

List of Tables

List of Figures

List of Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
ISDN	Integrated Services Digital Network
ISR	Integrated Service Router
IT	Information Technology
NDPP	Network Device Protection Profile
OS	Operating System
PoE	Power over Ethernet
POP3	Post Office Protocol
PP	Protection Profile
PROM	Programmable read-only memory
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
SPI	Serial Peripheral Interface
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

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 Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 2 ST and TOE Identification

Name	Description
ST Title	Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) Security Target
ST Version	1.0
Publication Date	10 December 2015
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351)
TOE Hardware Models	Cisco ISR 4321, 4331 and 4351
TOE Software Version	IOS XE 3.13.2
Keywords	Router, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device

1.2 TOE Overview

The Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) TOE is a purpose-built, routing platform that provides feature-rich Layer 2 and Layer 3 WAN/LAN connections with VPN capabilities.

The TOE includes the Cisco ISR 4000 Family Router models 4321, 4331 and 4351 running the same IOS XE 3.13.2 software as defined in Table 2 in section 1.1.

1.2.1 TOE Product Type

The Cisco ISR 4000 Family Routers are a routing platform that provides connectivity and security services onto a single, secure device for mid-range enterprise space customers. The Cisco ISR 4000 Family Routers offers to 600Mbps of forwarding for 4351 model, 400Mbps of

forwarding for 4331 model and 200Mpbs of forwarding for 4321 model. The Cisco ISR 4000 Family Routers provide services including on-board applications as well as extended Service Modules (SM-x), Network Interface modules (NIMs), and Internal Service Cards (ISCs).

In addition, the Cisco ISR 4000 Family Routers supports a single CPU system running the Cisco IOS-XE software, where the control and data plane are co-resident on a multi-core CPU, thus serving as a lower cost general purpose platform for routing and security designed to scale for mid-range next-generation service router products.

In support of the routing capabilities, the Cisco ISR 4000 Family Routers provides IPsec connection capabilities for VPN enabled clients connecting through the TOE.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All of the following environment components are supported by all TOE evaluated configurations.

Table 3 IT Environment Components

Component	Required	TOE Interface	Usage/Purpose Description for TOE performance
RADIUS or TACACS+ AAA Server	No	Management Port	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. This can be any RADIUS or TACACS+ AAA server that provides single-use authentication. The TOE, if configured for remote authentication, correctly leverages the services provided by the AAA server to provide single-use authentication to administrators.
Management Workstation with SSH Client	Yes	Management Port	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration and management through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	Serial Console Port	This includes any IT Environment Console that can be directly connected to the TOE via the Serial Console Port and may be used by the TOE administrator to support TOE administration and management.
Certification Authority	No	Network Interface Port	This includes any IT Environment Certification Authority on the TOE network. If configured, this can be used to provide the TOE with a valid certificate during certificate enrolment.
Remote VPN Endpoint	Yes	Network Interface Port	This includes any VPN peer or client with which the TOE participates in VPN communications. Remote VPN Endpoints may be any device or software client that supports IPsec VPN communications. Both VPN clients and VPN gateways are considered to be Remote VPN Endpoints by the TOE.

Component	Required	TOE Interface	Usage/Purpose Description for TOE performance
VPN Peer	No	Network Interface Port	This includes any peer with which the TOE participates in VPN communications. VPN peers may be any device or software client that supports IPsec communications. Both VPN clients and VPN gateways are considered to be VPN peers by the TOE.
NTP Server	No	Management Port	The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server's date and time. If configured, a solution must be used that supports secure communications with up to a 32 character key.
Syslog Server	Yes	Management Port	This includes any syslog server to which the TOE would transmit syslog messages.
USB token	No	USB port	A USB token is a smart card with a USB interface. The token can securely store any type of file within its available storage space (32 KB). Configuration files that are stored on the USB token can be encrypted and accessed only via a user PIN. The device does not load the configuration file unless the proper PIN has been configured for secure deployment of device configuration files.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware model included in the evaluation is: 4321, 4331 and 4351. The software is comprised of the Cisco IOS-XE 3.13.2 software version.

The Cisco ISR 4000 Family Routers that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The Cisco ISR 4000 Family Routers' primary features include the following:

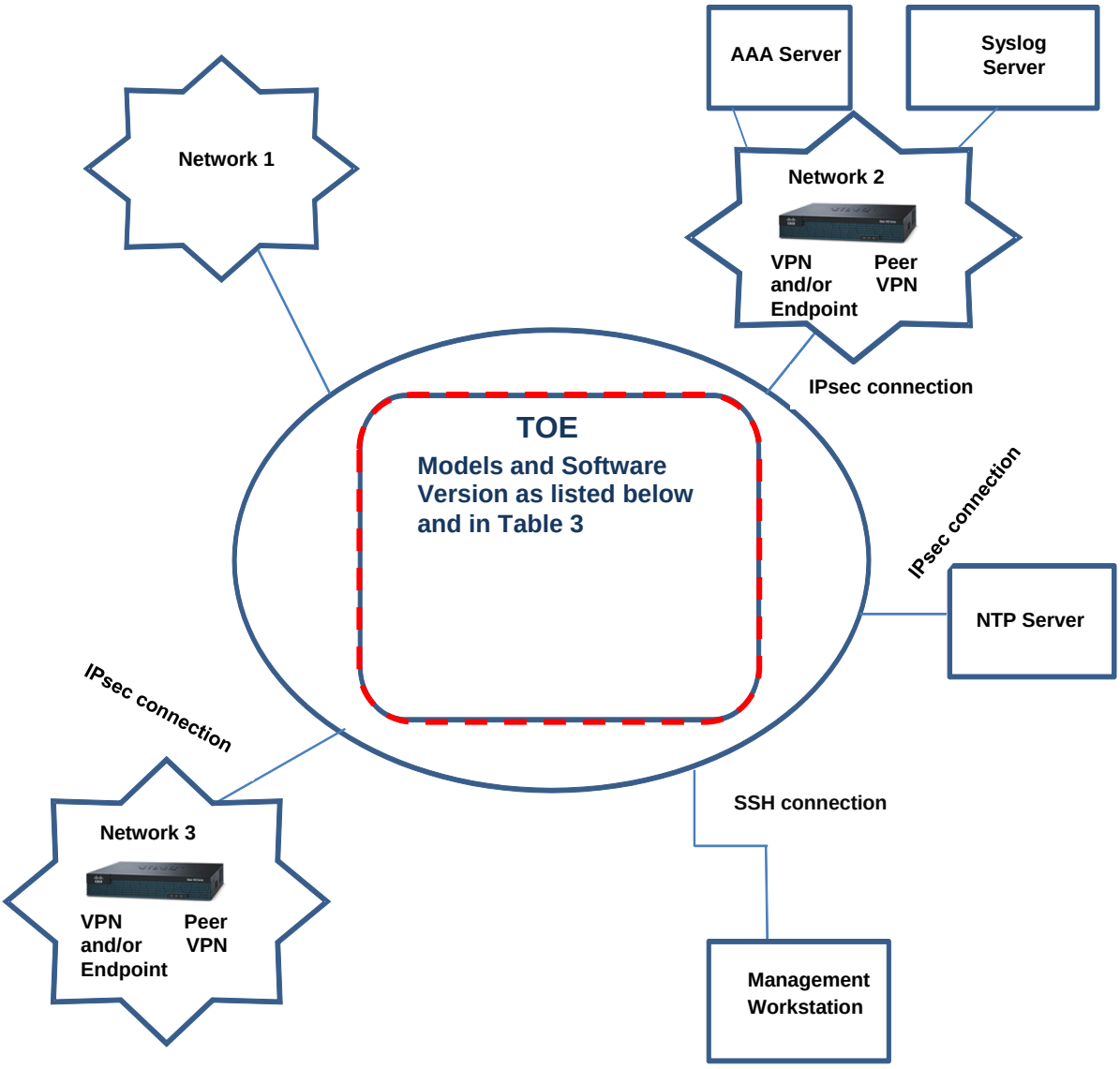
- Central processor that supports all system operations;
- DRAM memory maximum capacity of each DIMM is 8GB for a 16GB total memory
  - 4351 and 4331 has 2, 2GB DIMMs for a 4GB total
  - 4321 has a 4GB soldered down on a single channel with a DIMM socket on the second memory channel for upgrade to 8GB maximum capacity with the addition of a 4GB DIMM
- Dynamic memory, used by the central processor for system operation.
- Network Interface Modules (NIMs); each NIM slot offers high-data-throughput capability up to 2 Gbps toward the router processor and to other module slots
  - 4351 has three integrated NIM slots
  - 4351 has two integrated NIM slots
  - 4321 has two integrated NIM slots
- Services Module (SM); each service-module slot offers high data-throughput capability up to 10 Gbps toward the router processor and to other module slots. Support for both single and doublewide service modules provides flexibility in deployment options

  - 4351 has two single wide SM slots that may be combined into one double wide SM slot
  - 4331 has one single SM
- Integrated Services Card (ISC); ISC natively supports the new Cisco High-Density Packet Voice Digital Signal Processor Modules (PVDM4s), which has been optimized for concurrent voice and video support. The Cisco ISR 4000 Family Routers supports onboard ISC slots, however this functionality is not included in the evaluated configuration.
- USB port (note, none of the USB devices are included in the TOE).
  - Type A for Storage
  - Type mini-B console port
- Physical network interfaces. The only difference is in the number of ports available.
  - 1 10/100/1000 RJ-45 Ethernet port for system managements (labeled "GE mgmt")
  - 10/100/1000 RJ-45 Ethernet ports (labeled “GE 0/1/2/…….”)
  - 100/1000 SFP Ethernet ports (labeled “SFP 0/1/2/……”).
- 1 RJ45 Console
- 1 RJ45 AUX port with full modem control signals
- On board real-time clock
- PoE power supply support
- LEDs for Ethernet and console status
- Embedded IPsec VPN Hardware Acceleration

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

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

Figure 1 TOE Example Deployment



The previous figure includes the following:

- Cisco Integrated Services Routers (ISR) 4000 Family Routers (4321, 4331 and 4351)
- The following are considered to be in the IT Environment:
  - (2) VPN Peers and/or VPN Endpoints
  - Management Workstation
  - AAA Server
  - NTP Server
  - Syslog Server

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices of the Cisco ISR 4000 Family Routers as specified in section 1.5 below and the Cisco IOS-XE software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco

IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

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

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the ISR 4000 Family Routers (4321, 4331 and 4351). The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 3.13.2. The software image is also downloadable from the Cisco web site. A login id and password is required to download the software image.

The Integrated Services Routers (ISR) 4000 Family Routers (4321, 4331 and 4351) CC Configuration Guide (AGD) is considered to be part of the TOE in addition to the TOE product documentation that can be found listed in Table 5 and is downloadable from the http://cisco.com web site.

Figure 2 Cisco ISR 4000 Family Routers (4321, 4331 and 4351)

The TOE is comprised of the following physical specifications as described in Table 4 below:

Table 4 Specifications of ISR 4000 Family Routers (4321, 4331 and 4351)

Technical Specification	4351	4331	4321
Dimensions (H x W x D)	3.5 x 17.25 x 18.5 in (88.9 x 438.15 x 469.9 mm)	1.75 x 17.25 x 17.25 in (44.45 x 438.15 x 438.15 mm)	1.75 x 14.55 x 11.60 in (44.55 x 369.57 x 294.64 mm)
Typical weight (fully loaded with modules)	37.7 lb (17.1 kg)	14.6 lb (6.6 kg)	9.14 lb (4.15 kg) + 1.2 lb (55 kg) external PS
Power-supply options	Internal: AC, DC, and PoE	Internal: AC and PoE	External: AC and PoE
AC input voltage	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging
Maximum power with AC power supply (watts)	430	250	125
Maximum power with PoE power supply (platform only) (watts)	990	530	260
Airflow	I/O side to bezel side	I/O side to bezel side	Right I/O side to Left I/O side

Table 5 Guidance Documentation

#	Title
[1]	Release Notes for the Cisco 4000 Series ISRs (4321, 4331 and 4351) http://www.cisco.com/c/en/us/td/docs/routers/access/4400/release/notes/isr4451rn.html
[2]	Hardware Installation Guide for the Cisco 4000 Series Integrated Services Router (4321, 4331 and 4351) http://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html
[3]	Cisco 4000 Series ISRs Software Configuration Guide (4321, 4331 and 4351) http://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg.html

1.6 Logical Scope of the TOE

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

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDPP v1.1, with Errata#2 and VPN EP v1.01 as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the audit trail protection by providing remote backup to a syslog server over an encrypted channel.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) security functionality. This IOS-XE software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) which has been validated for conformance to the requirements of FIPS 140-2 Level 2 certificate #2388 (see Table 6 for algorithm certificate references).

Table 6 FIPS References

Algorithm	CAVP Certificate Numbers
AES	Cert #2817
Triple-DES	Cert #1688, #1670
SHS (SHA-1, 256, 384, and 512)	Cert #2361
HMAC SHA	Cert #1764
RSA	Cert #1471
ECDSA	Cert #493

Algorithm	CAVP Certificate Numbers
DRBG	Cert #481

While the algorithm implementations listed in the preceding table were not tested on the exact processor installed within the Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351), the algorithm certificates are applicable to the TOE based on the following,

- The cryptographic implementation which is tested is identical (unchanged) to the cryptographic implementation on the Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351).
- The cryptographic implementation does not depend on hardware for cryptographic acceleration i.e. there is no hardware specific cryptographic dependency. The cryptographic algorithms are implemented completely in software.
- The IOS-XE software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) for the cryptographic operations.

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

Table 7 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA/DSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing
SP 800-90 RBG	Used in IPsec session establishment. Used in SSH session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.

The TOE can act as a certification authority thus signing and issuing certificates to other devices. The TOE can also use the X.509v3 certificate for securing IPsec and SSH sessions.

1.6.3 Full Residual Information Protection

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

1.6.4 Identification and authentication

The TOE performs two types of authentication: device-level authentication of 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 TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters 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.

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

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

1.6.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure 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.

All of these management functions are restricted to authorized administrators of the TOE.

All management functions are restricted to the authorized administrator of the TOE. The term "authorized administrator" is used in this ST to refer to any user account that 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.

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.

1.6.6 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

1.6.7 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. Furthermore, Cisco IOS-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

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

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

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

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.

1.6.8 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.

1.6.9 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	This mode of operation includes non-FIPS allowed operations.
Telnet for management purposes.	Telnet passes authentication credentials in clear text. SSHv2 is to be used instead.
HTTP and HTTPS protocol and servers	HTTP and HTTPS protocol and servers were not evaluated and must be disabled
SNMP for management proposes and protocol	SNMP protocol and server was not evaluated and must be disabled

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices v1.1, with Errata#2 or the U.S. Government Network Device Protection Profile Extended Package VPN Gateway v1.1.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.5.

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
U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP)	1.1	June 8, 2012
Security Requirements for Network Devices Errata	#2	13 January 2013
Network Device Protection Profile Extended Package VPN Gateway (VPNEP)	1.1	12 April 2013

2.2.1 Protection Profile Additions

The ST claims exact conformance to the NDPP v1.1, with Errata#2, exact conformance to VPNEP v1.1 and does not include any additions to the functionality described in the Protection Profiles.

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, with Errata #2
- U.S. Government Network Device Protection Profile Extended Package VPN Gateway, 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 and Network Device Protection Profile Extended Package VPN Gateway 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 and VPN EPv1.1 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 and VPN EPv1.1 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 as well as section 5.2 of the VPN EPv1.1.

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
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1	
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.
Reproduced from U.S. Government Approved Protection Profile - Network Device Protection Profile (NDPP) Extended Package VPN Gateway Version 1.1	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

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

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
Reproduced from U.S. Government Approved Protection Profile - Network Device Protection Profile (NDPP) Extended Package VPN Gateway Version 1.1	
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.TSF_FAILURE	Security mechanisms of the TOE mail fail, leading to a compromise of the TSF.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.

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
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1	
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.
Reproduced from U.S. Government Approved Protection Profile - Network Device Protection Profile	

TOE Objective	TOE Security Objective Definition
(NDPP) Extended Package VPN Gateway Version 1.1	
O.ADDRESS_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination addresses.
O.AUTHENTICATION	The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE
O.FAIL_SECURE	Upon a self-test failure, the TOE will shutdown to ensure data cannot be passed while not adhering to the security policies configured by the administrator.
O.PORT_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination transport layer ports.

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
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1	
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.
Reproduced from U.S. Government Approved Protection Profile - Network Device Protection Profile (NDPP) Extended Package VPN Gateway Version 1.1	

Environment Security Objective	IT Environment Security Objective Definition
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

5 SECURITY REQUIREMENTS

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

5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDPP itself, the formatting used in the NDPP v1.1 and VPNGW EPv1.1 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 v1.1 and VPNGW EPv1.1.

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(1)	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.1(2)	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)

Class Name	Component Identification	Component Name
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1	Extended: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_SSH_EXT.1	Explicit: SSH
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Handling
	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	Extended: Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1	Extended: X.509 Certificates
FMT: Security management	FMT_MOF.1	Management of Security Functions Behavior
	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
FPF: Packet Filtering	FPF_RUL_EXT.1	Packet Filtering
FPT: Protection of the TSF	FPT_FLS.1	Fail Secure
	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	Extended: TSF Testing

Class Name	Component Identification	Component Name
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

5.3 SFRs from NDPP and VPN Gateway EP PP

5.3.1 Security audit (FAU)

5.3.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up of the audit functions;
b) All auditable events for the not specified level of audit; and
c) *All administrative actions*;
d) [*Specifically defined auditable events listed in Table 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(1)	None.	None.
FCS_CKM.1(2)	None.	None.
FCS_CKM_EXT.4	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
	Establishment/Termination of an IPsec SA.	Non-TOE endpoint of connection (IP address) for both successes and failures.
	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment
FCS_RBG_EXT.1	None.	None.
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure.
	Establishment/Termination of an SSH session.	Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	None.
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1	Establishing session with CA	Entire packet contents of packets transmitted/received during session establishment
FMT_MOF.1	None.	None.
FMT_MTD.1	None.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPF_RUL_EXT.1	Application of rules configured with the ‘log’ operation	Source and destination addresses Source and destination ports

SFR	Auditable Event	Additional Audit Record Contents
		Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets
FPT_FLS.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	Indication that TSF self-test was completed.	Any additional information generated by the tests beyond “success” or “failure”.
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.	Identification of the initiator and target of failed trusted channels establishment attempt
	Termination of the trusted channel.	
	Failure of the trusted channel functions.	
FTP_TRP.1	Initiation of the trusted channel.	Identification of the claimed user identity.
	Termination of the trusted channel.	
	Failures of the trusted path functions	

5.3.1.2 FAU_GEN.2 User Identity Association

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

5.3.1.3 FAU_STG_EXT.1 External Audit Trail Storage

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

5.3.2 Cryptographic Support (FCS)

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

FCS_CKM.1.1(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.*

5.3.2.2 FCS_CKM.1(2) Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1(2) Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a:

[

- *FIPS PUB 186-3, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes;*]

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

5.3.2.3 FCS_CKM_EXT.4 Cryptographic Key Zeroization

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

5.3.2.4 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* **GCM, CBC,** [*no other modes*] and cryptographic key sizes 128-bits, 256-bits that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **NIST SP 800-38D, NIST SP 800-38A [**no other standards**]**

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

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

- [RSA Digital Signature Algorithm (RSA) with a key size (modulus) of 2048 bits or greater that meets FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard",

- Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater that meets FIPS PUB 186-3, "Digital Signature Standard" with "NIST curves" P-256, P-384 and **[**no other curves**]** (as defined in FIPS PUB 186-3, "Digital Signature Standard")]**.**

5.3.2.6 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."*

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

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

5.3.2.8 FCS_IPSEC_EXT.1 Extended: Internet Protocol Security (IPsec) Communications

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, transport 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-GCM-128, AES-GCM-256 as specified in RFC 4106, [AES-CBC-128, AES-CBC-256 (both specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers] and [RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23) and [RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-128, 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 [IKEv2 SA lifetimes can be configured by an Administrator based on number of packets or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs, IKEv1 SA lifetimes can be configured by an Administrator based on number of packets or 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 generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16)*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^ [*128*].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), and [24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), [*15 (3072 bit MODP), and 16 (4096-bit MODP)*]]

FCS_IPSEC_EXT.1.12 The TSF shall ensure that all IKE protocols perform peer authentication using a [RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

FCS_IPSEC_EXT.1.13 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD_SA] connection.

5.3.2.9 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 accumulates entropy from a TSF-hardware based noise source, and [no other 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 bit length of the keys and authorization factors that it will generate.

5.3.2.10 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 [*35000*] 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 methods used for the SSH protocol.

5.3.3 User data protection (FDP)

5.3.3.1 FDP_RIP.2 Full Residual Information Protection

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

5.3.4 Identification and authentication (FIA)

5.3.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 Refinement: The TSF shall detect when **an Administrator configurable positive integer of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall [prevent the offending remote administrator from successfully authenticating until [*an authorized administrator unlocks the locked user account*] is taken by a local Administrator].

5.3.4.2 FIA_PMG_EXT.1 Password Management

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

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

5.3.4.3 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 [*any combination of alphanumeric or special characters up to 128 bytes*];
- 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 [SHA-1] and able to [accept bit-based pre-shared keys].

5.3.4.4 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

5.3.4.5 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

5.3.4.6 FIA_UAU.7 Protected Authentication Feedback

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

5.3.4.7 FIA_X509_EXT.1 Extended: X.509 Certificates

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [SSH] connections.

FIA_X509_EXT.1.2 The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.1.3 The TSF shall provide the capability for authenticated Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

FIA_X509_EXT.1.4 The TSF shall generate a Certificate Request Message as specified in RFC 2986 and be able to provide the following information in the request: public key, Common Name, Organization, Organizational Unit, and Country.

FIA_X509_EXT.1.5 The TSF shall validate the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].

FIA_X509_EXT.1.6 The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates.

FIA_X509_EXT.1.7 The TSF shall not treat a certificate as a CA certificate if the basicConstraints extension is not present or the cA flag is not set to TRUE.

FIA_X509_EXT.1.8 The TSF shall not establish an SA if a certificate or certificate path is deemed invalid.

FIA_X509_EXT.1.9 The TSF shall not establish an SA if the distinguished name (DN) contained in a certificate does not match the expected DN for the entity attempting to establish a

connection.

FIA_X509_EXT.1.10 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall, at the option of the administrator, establish an SA or disallow the establishment of an SA.

5.3.5 Security management (FMT)

5.3.5.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this EP to an authenticated Administrator.

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

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

5.3.5.3 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to update the TOE, and to verify the updates using [digital signature, published hash] capability prior to installing those updates;*
- *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 identified in this EP to the Administrator,*
- *Ability to configure all security management functions identified in other sections of this EP.*

5.3.5.4 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Authorized Administrator.**

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

5.3.6 Packet Filtering (FPF)

5.3.6.1 FPF_RUL_EXT.1 Packet Filtering

FPF_RUL_EXT.1.1 The TSF shall perform Packet Filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2 The TSF shall process the following network traffic protocols:

- Internet Protocol (IPv4)
- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

FPF_RUL_EXT.1.3 The TSF shall allow the definition of Packet Filtering rules using the following network protocol fields:

- IPv4
  - Source address
  - Destination Address
  - Protocol
- IPv6
  - Source address
  - Destination Address
  - Next Header (Protocol)
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

and distinct interface.

FPF_RUL_EXT.1.4 The TSF shall allow the following operations to be associated with Packet Filtering rules: permit, deny, and log.

FPF_RUL_EXT.1.5 The TSF shall allow the Packet Filtering rules to be assigned to each distinct network interface.

FPF_RUL_EXT.1.6 The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF_RUL_EXT.1.5) in the following order: Administrator-defined.

FPF_RUL_EXT.1.7 The TSF shall deny packet flow if a matching rule is not identified.

5.3.7 Protection of the TSF (FPT)

5.3.7.1 FPT_FLS.1 Fail Secure

FPT_FLS.1.1 Refinement: The TSF shall **shutdown** when the following types of failures occur: failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.

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

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

5.3.7.3 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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

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

5.3.7.4 FPT_STM.1 Reliable time stamps

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

5.3.7.5 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 and [published hash] prior to installing those updates.

5.3.7.6 FPT_TST_EXT.1: Extended: 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.

FPT_TST_EXT.1.2 The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1(2).

5.3.8 TOE Access (FTA)

5.3.8.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, lock the session - disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session; after a Security Administrator-specified time period of inactivity.

5.3.8.2 FTA_SSL.3 TSF-initiated Termination

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

5.3.8.3 FTA_SSL.4 User-initiated Termination

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

5.3.8.4 FTA_TAB.1 Default TOE Access Banners

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

5.3.9 Trusted Path/Channels (FTP)

5.3.9.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **use IPsec, and [SSH]** to provide a **trusted** communication channel between itself and **all authorized IT entities** 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
[

- *external audit servers using IPsec,*
- *remote AAA servers using IPsec,*
- *remote VPN gateways/peers using IPsec,*
- *another instance of the TOE using SSH or IPsec*

].

5.3.9.1 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.*

5.4 TOE SFR Dependencies Rationale for SFRs Found in NDPP

The NDPPv1.1 and VPN EPv1.1 contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP itself has been approved.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDPP v1.1 and VPNGW EPv1.1 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

5.5.2 Security Assurance Requirements Rationale

This Security Target claims conformance to the NDPP v1.1 and the VPNGW EP v1.1 which essentially is an EAL1 conformance claim. This target was chosen to ensure that the TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks.

5.6 Assurance Measures

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

Table 18 Assurance Measures

Component	How requirement will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1 ALC_CMS.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s) identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 19 How TOE SFRs Measures

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FAU_GEN.1</td><td>The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include: startup of the audit mechanism, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, “Auditable Events Table”). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup of the audit functionality is audited.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server or all of the above. For instance all emergency, alerts, critical, errors, and warning messages can be sent to the console and local buffer alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the TOE is affected. All notifications and information type message can be sent to the syslog server. The audit records are transmitted using IPsec channel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established.

The local logging buffer size can be configured from a range of 4096 (default) to 4,294,967,295 bytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount.

The local logging 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 local buffer, to set the logging level, etc.

<table>
<tr><th>Auditable Event</th><th>Rationale</th></tr>
<tr><td>All use of the user identification mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate and source address or interface will be included in the log record.</td></tr>
<tr><td>Any use of the authentication mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Met	
		attempting to authenticate will be included in the log record, along with the origin or source of the attempt.
	Management functions	The use of the security management functions is logged; modifications of the behavior of the functions in the TSF and modifications of default settings.
	Changes to the time.	Changes to the time are logged.
	Failure to establish and/or establishment/termination of an IPsec session	Attempts to establish an IPsec tunnel or the failure of an established IPsec tunnel is logged as well as successfully established and terminated IPsec sessions.
	Establishing session with CA	The connection to CA's for the purpose of certificate verification is logged.
	Failure to establish and/or establishment/termination of an SSH session	Attempts to establish a SSH session or the failure of an established SSH session is logged as well as successfully established and terminated sessions.
	Application of rules configured with the 'log' operation	Logs are generated when traffic matches acls that are configured with the log operation.
	Indication of packets dropped due to too much network traffic	Logs are generated when traffic that exceeds the settings allowed on an interface is received.
	Indication that TSF self-test was completed.	During bootup, if the self-test fails, the failure is logged.
	Initiation of update	Audit event is generated for the initiation of a software update.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td>Any attempts at unlocking of an interactive session.</td><td>Audit event is generated after a user's session is locked and the admin user is required to re-authenticate.</td></tr>
<tr><td>Once a remote interactive session is terminated after a Security Administrator-configurable time interval of session inactivity.</td><td>An audit event is generated by when sessions are terminated after exceeding the inactivity settings.</td></tr>
<tr><td>The termination of an interactive session.</td><td>An audit event is generated by an authorized administrator when the exit command is used.</td></tr>
<tr><td>Initiation of the trusted channel/ path.
Termination of the trusted channel/ path.
Failure of the trusted channel/ path functions.</td><td>See the rows for IPsec and SSH above.</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.</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 protects communications with an external syslog server via IPsec. The TOE transmits its audit events to all configured syslog servers at the same time logs are written to the local log buffer and to the console. The TOE is capable of detecting when the IPsec connection fails. The TOE also stores the set of audit records locally on the TOE, and continues to do so if the communication with the syslog server goes down. The local audit buffer size can be configured from a range of 4096 (default) to 4,294,967,295 bytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks. If the IPsec connection fails, the TOE can be configured to record messages associated with the syslog history. The level of the audit records and the number of audit records that can be stored in the syslog history can also be configured using the logging history command in the configuration mode. The audit records in the history table include the table size, the status of messages, and the text of the messages stored in the table. For example the logging history can be set to store the last 500 syslog messages with the severity less than warning messages. The TOE will transmit the local log buffer contents when connectivity to the syslog server is restored. The logging history table is separate from the local logging buffer.</td></tr>
</table>

TOE SFRs	How the SFR is Met
	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(1) FCS_CKM.1(2)	The TOE implements a random number generator for Diffie-Hellman and Elliptic curve key establishment (conformant to NIST SP 800-56A), and for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE 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 X.509v3 certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The IOS-XE Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. In addition, the IOS-XE Software includes an embedded certificate server, allowing the router to act as a certification authority on the network. The TOE can act as a certification authority thus digitally signing and issuing certificates to both the TOE and external entities. The TOE can also use the X.509v3 certificate for securing IPsec and SSH, sessions.
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 refer to Table 20 TOE 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 and GCM mode (with key sizes 128, 192 and 256 bits) as described in NIST SP 800-38A and NIST SP 800-38D. AES is implemented in the following protocols: IPSEC and SSH.
FCS_COP.1(2)	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-3, "Digital Signature Standard" and FIPS PUB 186-2, "Digital Signature Standard". In addition, the TOE will provide cryptographic signature services using ECDSA with key size of 256 and greater as specified in FIPS PUB 186-3, "Digital Signature Standard". The TOE provides cryptographic signature services using ECDSA that meets FIPS 186-3, "Digital Signature Standard" with NIST curves P-256 and P-384.
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."
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 IPsec implementation provides both VPN peer-to-peer and VPN client to TOE capabilities. The VPN peer-to-peer tunnel allows for example the TOE and another router to establish an IPsec tunnel to secure the passing of route tables (user data). Another configuration in the peer-to-peer configuration is to have the TOE be set up with an IPsec tunnel with a VPN peer to secure the session between the TOE and syslog server. The VPN client to TOE configuration would be where a remote VPN

TOE SFRs	How the SFR is Met
	client connects into the TOE in order to gain access to an authorized private network. Authenticating with the TOE would give the VPN client a secure IPsec tunnel to connect over the internet into their private network. In addition to tunnel mode, which is the default IPsec mode, the TOE also supports transport mode, allowing for only the payload of the packet to be encrypted. If tunnel mode is explicitly specified, the router will request tunnel mode and will accept only tunnel mode. The TOE implements IPsec to provide both certificates and pre-shared key-based authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. Preshared keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The IKE protocols implement Peer Authentication using the RSA, ECDSA algorithm with X.509v3 certificates, or preshared keys. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), • The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and • The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE supports both IKEv1 and IKEv2 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the 'crypto isakmp aggressive-mode disable' command. The TOE can be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using "lifetime" command. The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour, but it is configurable to 8 hours. The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum

TOE SFRs	How the SFR is Met
	configurable value. The maximum configurable value is 4GB. The TOE provides AES-GCM-128, AES_GCM-256, AES-CBC-128, and AES-CBC-256 for encrypting the IKEv1 and IKEv2 payloads. The administrator is instructed in the AGD to ensure that the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload. The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, and the following corresponding key sizes (in bits) are used: 320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20), 424 (for DH Group 15), and 480 (bits for DH Group 16)] bits. The DH group can be configured by issuing the following command during the configuration of IPsec: TOE-common-criteria (config-isakmp)# group 14 This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072 bit MODP), and 16 (4096-bit MODP) are also allowed and supported. This sets the DH group offered during negotiations. The TOE generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in gx mod p) using the NIST approved DRBG specified in FCS_RBG_EXT.1 and having possible lengths of 256, 320, 384, 424, or 480 bits. When a random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2128. The nonce is likewise generated using the AES-CTR DRBG. IPsec provides secure tunnels between two peers, such as two routers and remote VPN clients. An authorized administrator defines which packets are considered sensitive and should be sent through these secure tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers or between the TOE and remote VPN client. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per security protocol (AH or ESP). In the evaluated configuration only ESP will be configured for use. A crypto map (the Security Policy Definition (SPD)) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the router attempts to match the packet to the access list (acl) specified in that entry. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit acls would then flow through the IPsec tunnel and be classified as "PROTECTED". Traffic that does not match a permit crypto map acl and does not match a non-crypto permit acl on the interface would be DISCARDED. Traffic that does not match a permit acl in the crypto map, but does match a non-crypto permit acl would be allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp

TOE SFRs	How the SFR is Met
	would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR and using cryptographic algorithms AES-GCM-128, AES-GCM-256, AES-CBC-128 and AES-CBC-256 together with HMAC-SHA1) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. In IOS the negotiations of the IKE SA adheres to configuration settings for IPsec applied by the administrator. For example in the first SA, the encryption, hash and DH group is identified, for the Child SA the encryption and the hash are identified (unless GCM is the encryption method, then no hash is listed). The administrator configures the first SA to be as strong as or stronger than the child SA; meaning if the first SA is set at AES 128, then the Child SA can only be AES128. If the first SA is AES256, then the Child SA could be AES128 or AES256. During the negotiations, if a non-match if encountered, the process stops and an error message is received.
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSHv2 sessions are limited to a configurable session timeout period of 120 seconds, a maximum number of failed authentication attempts limited to 3, and will be rekeyed upon request from the SSH client. SSH connections will be dropped if the TOE receives a packet larger than 35,000 bytes. Large packets are detected by the SSH implementation, and dropped internal to the SSH process. The DH group 14 is a configurable option in the TOE which is used to set the minimum DH key size that can be used to establish the session. When the administrator attempts to connect to the TOE, ciphers are offered, and if the cipher presented is less than what is set on the TOE, the TOE will not negotiate the session and the connection is dropped. If the cipher matches the allowed key size, the TOE negotiates the session, validates the users' identity and password credentials and establishes the session. • The TOE implementation of SSHv2 supports the following public key algorithms for authentication: RSA Signature Verification. • The TOE also supports password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server. • The TOE implementation of SSHv2 supports the following encryption algorithms, AES-CBC-128, AES-CBC-256 to ensure confidentiality of the session. • The TOE's implementation of SSHv2 supports hashing algorithms hmac-sha1 and hmac-sha1-96to ensure the integrity of the session. • The TOE's implementation of SSHv2 can be configured to only allow Diffie-Hellman Group 14 (2048-bit keys) Key Establishment, as required by the PP.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit

TOE SFRs	How the SFR is Met
	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. Each of the ISR 4000 series models has the Quack (ACT) chip. Included as part of the TOE is the Quack (ACT) processor that is the primary entropy source. This solution is available in the IOS XE 3.13.2 or later FIPS/CC approved releases of the 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 data allocated to or deallocated from previous packets. Packets that are not the required length use a four-byte repeating pattern for padding. Residual data is never transmitted from the TOE. Once packet handling is completed, its content is overwritten by a fixed pattern before allocation to or deallocation from the memory buffer which previously contained the packet is reused. This applies to both data plane traffic and administrative session traffic.
FIA_AFL.1	The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts (between 1 and 25) before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command, *aaa local authentication attempts max-fail [number of failures]* in the configuration mode. The number of failures is the number of consecutive failures that will trigger locking of the account. When a privileged administrator or non-privileged administrator attempting to log into the administrative CLI reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until a privileged administrator resets the user's number of failed login attempts through the administrative CLI using *the clear aaa local user fail-attempts username [user]* in the configuration mode. Note, this applies to consecutive failures, and is not affected by the SSH session disconnections after their default number of failures. In other words, if this lockout command is set to 5 failures, and SSH disconnects after 3 failed attempts, if the user attempts another SSH session and enters the wrong credentials two additional times, the account will lock and remains locked until a privileged administrator resets the user's number of failed login attempts through the administrative CLI. When the user lockout is configured, the TOE authentication mechanism tracks each time a user attempts to login. If the user presents the wrong password credentials, the count is increased by one each time the user attempts to login with the wrong credentials. If the failed login number is reached, the account is locked until a privileged administrator resets the user's number of failed login attempts through the administrative CLI. If the user presents the correct password credentials, the user is successfully logged in and the count remains at zero. The counter is reset to zero

TOE SFRs	How the SFR is Met
	when the user logs out. For IKE peers, the TOE denies access to the TOE based on failed Phase 1 authentication attempts when negotiating the Internet Key Exchange Protocol.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of up 15 characters.
FIA_PSK_EXT.1	The TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. Preshared keys can be entered as ASCII character strings, or HEX values. The TOE supports keys that are from 22 characters in length up to 128 bytes in length. The data that is input is conditioned prior to use via SHA-1.
FIA_UIA_EXT.1	The TOE displays an administratively configured warning banner prior to administrative identification and authentication and provides no access to the administrative capabilities of the TOE prior to the administrative user presenting the authentication credentials.
FIA_UAU_EXT.2	The TOE provides a local password-based authentication mechanism as well as support for RADIUS and TACACS+ authentication. When the TOE is configured to authenticate users to either RADIUS or TACACS+, the Interface is invoked. When the CLI user login is displayed, the user enters the information (usually just a username and password), and sends it to the AAA server, tunneled over IPsec. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. The TOE can be configured to try one or more remote authentication servers, and optionally fallback to the local user database if the remote authentication servers are inaccessible. The TOE correctly invokes an external authentication server to provide a remote authentication mechanism, or password-based authentication by forwarding the authentication requests to the external authentication server. 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 in the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console or via SSH, the TOE does not echo any characters of the password or any representation of the characters.
FIA_X509_EXT.1	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec, and SSH connections. Public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates can be stored in a specific location on the router, such as NVRAM and flash memory or on a USB eToken 64 KB smart card. Note, only Authorized Administrator can

TOE SFRs	How the SFR is Met
	configure the storage location, import/load certificates and delete certificates. During run time setup and configuration, the Authorized Administrator will specify what active local storage device will be used to store certificates. For example, the command to specify the storage location is 'crypto pki certificate storage *location-name'*. If the storage location is to be a directory (cert) on flash, the command would be entered as **crypto pki certificate storage flash:/certs.** Once set, the certificates will be stored in *disk0:/certs/* .Once the storage location has been configured, the Authorized Administrator can import the certificates for storage in the configured storage location. The certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. The physical security of the router (A.Physical) protects the router and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE. USB tokens provide for secure configuration distribution of the digital certificates and private keys. RSA operations such as on-token key generation, signing, and authentication, and the storage of Virtual Private Network (VPN) credentials for deployment can be implemented using the USB tokens. Both OSP and CRL are configurable and may be used for certificate revocation. Checking is also done for the basicConstraints extension and the cA flag to determine whether they are present and set to TRUE. If they are not, the certificate is not accepted
FMT_MOF.1 FMT_MTD.1	The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds. Each of the predefined and administratively configured privilege level has default 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 semi-privileged and privileged levels. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI, which is the default access for IOS-XE 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 and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include, • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI • The ability to update the IOS-XE software • Ability to configure the cryptographic functionality; • Ability to configure the IPsec functionality,

TOE SFRs	How the SFR is Met
	• Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE via the CLI,
FMT_SMR.2	The term "authorized administrator" is used in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges. Refer to the Guidance documentation and IOS Command Reference Guide for available commands and associated roles and privilege levels. The TOE can and shall be configured to authenticate all access to the command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote authentication via SSH.
FPF_RUL_EXT.1	An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to interfaces using access and crypto map sets. The rules (access control list entries) within an access-list applied to a crypto map determine whether the traffic is to be encrypted/decrypted. If traffic is not defined within the crypto map access-list, encryption/decryption will not be applicable to that traffic flow, and access-lists applied to interfaces (not to crypto maps) will determine whether the traffic will be permitted/denied through the TOE (without encryption/decryption by the TOE). Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. The TOE interfaces are the external network Ethernet ports that network traffic within the suite of the IP protocol family traverses. All such data is subject to internal filtering rules which restrict the flow of Layer 3 network traffic to and from each TOE interface. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging. These rules control whether a packet is transferred from one interface to another based on: • IP address of source (as defined in the packet header) • IP address of destination (as defined in the packet header) • IP protocol Transport layer protocol (or next header in IPv6) • Service used (UDP or TCP ports, both source and destination) • Network interface on which the connection request occurs These rules are supported for the following protocols: RFC 791(IPv4); RFC 2460 (IPv6); RFC 793 (TCP); RFC 768 (UDP). TOE compliance with these protocols is verified via regular quality assurance, regression, and interoperability testing. Packets will be dropped unless a specific rule has been set up to allow the packet to

TOE SFRs	How the SFR is Met
	pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). The TOE also keeps track of the network connections that may include details such as the IP addresses, ports, and sequence numbers of the packets traversing the connections. For TCP packets, this is a quick process to determine if the packet belongs to an existing pre-screened session so that packets associated with these sessions are permitted to pass. Simultaneously, the TOE will drop packets which are not associated with the session to prevent unsolicited connections. For UDP packets, the TOE tracks the session through addresses and ports of the following packets' source and destination, By default, packets will not be encrypted/decrypted unless a specific rule matching that traffic flow has been applied to a crypto map, and that crypto map applied to the applicable interface. Whether or not packets match a crypto map, the packets need to be permitted by any access-list applied to inbound or outbound interfaces. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. These rules are entered in the form of access lists at the CLI via the 'access-list' command, and applied to interfaces via the 'access group' command or the 'match' command. These rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/ startup that the access lists are not enforced on an interface. In the event of an IOS software packet processing subsystem (control (management) and data (routing and forwarding) planes) failure to the TOE or other process failures including memory buffer overflow or failure of TOE components during Power On Self-Test (POST) or during the execution of a self-test, network traffic would not be forwarded. In the event of a failure of one or more network interfaces, traffic would not flow across the failed interface, but would continue to flow across other interfaces as long as no failed interfaces is part of the traffic path through the TOE. This is to ensure that all traffic is subjected to the rules as described above In summary, assuming the TOE, processes and all components are functioning correctly, the basic packet processing algorithms is realized by the control plane and the data plane that looks at either the control information contained in the packet and is used to transfer the packet to its destination or the data content (payload) that is used to provide some specific action and to ensure packets that are part of an established session, the header, payload and trailer information is processed to ensure the packets are routed and assembled correctly, in addition to any applicable rule set. In a condensed view, the packets are processed as follows, though noting the rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/ startup that the access lists are not enforced on an interface and all of this ensures all traffic is subjected to the rules: Inbound access lists — when the access list is applied to inbound packets on an interface, when the TOE receives those packets they are processed by the Cisco IOS software that checks the criteria statements of the access list for a match before being routed to the outbound interface. If the packet is permitted, the IOS software continues to process the packet. Any packets that are denied will not be routed since they are discarded before the routing process is invoked; hence the packet is denied and the IOS software

TOE SFRs	How the SFR is Met
	discards the packet. Outbound access lists — when an access list is applied to outbound packets on an interface, those packets are routed to the outbound interface and the processed by the Cisco IOS software through the access list for a match. If the packet is permitted, the IOS software transmits the packet accordingly. If the packet is denied, the IOS software discards the packet.
FPT_FLS.1	Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE. The TOE reloads and will continue to reload as long as the failures persist. This functionally prevents any failure of power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests from causing an unauthorized information flow. There are no failures that circumvent this protection.
FPT_SKP_EXT.1	The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. This functionality is configured on the TOE using the 'password encryption aes' command. The TOE is configured to not display configured keys as part of configuration files using the 'hidekeys' command.
FPT_APW_EXT.1	The TOE includes CLI command features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The command is the password encryption aes command used in global configuration mode. The 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.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The TOE has two clocks: a battery-powered hardware clock (referenced in CLI commands as the "calendar") and a software clock (referenced in CLI commands as the "clock"). These two clocks are managed separately. The primary source for time data on the TOE is the software clock. This clock runs from the moment the system starts up and keeps track of the current date and time. The software clock can be set from a number of sources. When the hardware clock is initialized or rebooted, the software clock is initially set based on the time in the hardware clock. The software clock can then be updated by manual configuration using the hardware clock or by NTP if configured. Since the software clock can be dynamically updated it has the potential to be more accurate than the hardware clock. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. This system clock is also used for cryptographic functions.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from the Cisco.com web site. Authorized Administrators can download the Common Criteria evaluated software image file

TOE SFRs	How the SFR is Met
	from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html. Digital signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The digital certificates used by the update verification mechanism are contained on the TOE. Instructions for how to do this verification are provided in the administrator guidance for this evaluation.
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 security administrator will have to log into the CLI to determine which test failed and why. During the system boot-up 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). If the tests pass successfully the login prompt is displayed and the administrator will be able to login and administer the TOE. If the POST fails the TOE will reboot in attempts to correct the failure. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. If the problem is not corrected by the reboot, Cisco Technical Support provides 24-hour-a-day technical assistance. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure all the TOE hardware and software components are available and operating correctly. If all components pass the tests, the login prompt will be displayed. If any of the tests fail, the TOE will reboot in attempts to correct the failure. Refer to the Guidance documentation for installation configuration settings and information and troubling shooting if issues are identified. If the problem is not corrected by the reboot, Cisco Technical Support provides 24-hour-a-day technical assistance.
FTA_SSL_EXT.1 FTA_SSL.3	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "session-timeout" setting applied to the console. If a local user session is inactive for a configured period of time, the session will be locked and will require re-authentication to unlock the session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the "exec-timeout" setting.
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions.

TOE SFRs	How the SFR is Met
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This is applicable for both local and remote TOE administration.
FTP_ITC.1	The TOE protects communications with peer or neighbour routers using keyed hash as defined in FCS_COP.1.1(4) and cryptographic hashing functions FCS_COP.1.1(3). This protects the data from modification of data by hashing that verify that data has not been modified in transit. In addition, encryption of the data as defined in FCS_COP.1.1(1) is provided to ensure the data is not disclosed in transit. The TOE also requires that peers and other TOE instances establish an IKE/IPsec connection in order to forward routing tables used by the TOE. In addition, the TOE can establish secure VPN tunnels with IPsec VPN clients. The TOE can also secure communication with other instances of the TOE using SSH. The TOE protects communications between the TOE and the remote audit server using IPsec. This provides a secure channel to transmit the log events. Likewise communications between the TOE and AAA servers are secured using IPsec.
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.

7 ANNEX A:

7.1 Key Zeroization

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

Table 20 TOE Key Zeroization

Name	Description	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.	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.	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.	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.	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.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	The function calls the operation ike_free_ike_sa_chunk, which performs the zeroization of the IKE structure. This structure contains all of the SA items, including the skeyid, skeyid_d, IKE Session Encryption Key and IKE Session Authentication Key. All values overwritten by 0's.	Automatically after IKE session terminated. Overwritten with: 0x00

Name	Description	Zeroization
ISAKMP preshared	The function calls the free operation with the poisoning mechanism that overwrites the value with 0x0d.	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.)	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.	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.	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.	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.	Zeroized using the following command: **# no tacacs-server key** Overwritten with: 0x0d
SSH Private Key	Once the function has completed the operations that require 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.	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.	Automatically when the SSH session is terminated. Overwritten with: 0x00

8 APPENDIX B

8.1 FIPS PUB 186-3, Compliance

The TOE is compliant to FIPS Pub 186-3 as described in Table 21 below.

Table 21 FIPS PUB 186-3, Compliance

Section	Exceptions to Shall/Shall Not Statement(s)	Exceptions to Should Statements	TOE Compliant?	Rationale
B.1 FFC Key Pair Generation	Not Implemented.	N/A	Yes	FFC Key Pair Generation Not Implemented
B.1.1 Key Pair Generation Using Extra Random Bits	Not Implemented.	N/A	Yes	Not Implemented.
B.1.2 Key Pair Generation by Testing Candidates	Not Implemented.	N/A	Yes	Not Implemented.
B.2 FFC Per-Message Secret Number Generation	Not Implemented.	N/A	Yes	Not Implemented.
B.2.1 Per-Message Secret Number Generation Using Extra Random Bits	Not Implemented.	N/A	Yes	Not Implemented.
B.2.2 Per-Message Secret Number Generation by Testing Candidates	Not Implemented.	N/A	Yes	Not Implemented.
B.3 IFC Key Pair Generation	N/A	N/A	Yes	N/A
B.3.1 Criteria for IFC Key Pairs	None.	N/A	Yes	N/A
B.3.2 Generation of Random Primes that are Provably Prime	Not Implemented.	N/A	Yes	TOE does not implement this prime generation method, but does method in Section B.3.4
B.3.2.1 Get the Seed	None.	N/A	Yes	N/A
B.3.2.2 Construction of the Provable Primes	Not Implemented.	N/A	Yes	TOE does not implement this

Section	Exceptions to Shall/Shall Not Statement(s)	Exceptions to Should Statements	TOE Compliant?	Rationale
p and q				prime generation method, but does method in Section B.3.4
B.3.3 Generation of Random Primes that are Probably Prime	Not Implemented.	N/A	Yes	TOE does not implement this prime generation method, but does method in Section B.3.4
B.3.4 Generation of Provable Primes with Conditions Based on Auxiliary Provable Primes	None.	N/A	Yes	N/A
B.3.5 Generation of Probable Primes with Conditions Based on Auxiliary Provable Primes	Not Implemented.	N/A	Yes	TOE does not implement this prime generation method, but does method in Section B.3.4
B.3.6 Generation of Probable Primes with Conditions Based on Auxiliary Probable Primes	Not Implemented.	N/A	Yes	TOE does not implement this prime generation method, but does method in Section B.3.4
B.4 ECC Key Pair Generation	None.	N/A	Yes	N/A
B.4.1 Key Pair Generation Using Extra Random Bits	None.	On error, invalid values for d and Q are not returned; instead, no key at all is returned.	Yes	The structure of the code doesn't return values for d and Q; instead, on success, the generated keys are installed.
B.4.2 Key Pair Generation by Testing Candidates	Not Implemented.	None.	Yes	TOE does not implement this prime generation method.
B.5 ECC Per-Message Secret Number Generation	None.	N/A	Yes	N/A

Section	Exceptions to Shall/Shall Not Statement(s)	Exceptions to Should Statements	TOE Compliant?	Rationale
B.5.1 Per-Message Secret Number Generation Using Extra Random Bits	None.	On error, invalid values of k and k^-1 are not returned	Yes	On error, k and k^-1 aren't used.
B.5.2 Per-Message Secret Number Generation by Testing Candidates	Not Implemented.	None.	Yes	TOE does not implement this method of ECC Signature Generation

ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 22: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDPP]	U.S. Government Protection Profile for Security Requirements for Network Devices, version 1.1, June 8, 2012
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008