Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9

Common Criteria Security Target

ST Version 1.0

11 October 2019

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

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Table of Contents

List of Tables

List of Figures

Acronyms

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

Table 1: Acronyms and Abbreviations

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AC	Alternating Current
ACL	Access Control Lists
AES	Advanced Encryption Standard
AGD	Guidance Documents
ACSII	American Standard Code for Information Interchange
ASR	Aggregation Services Router
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Circuit Emulation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CSR	Certificate Signing Request
DC	Direct Current
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ESP	Encapsulating Security Payload
FFC	Finite Field Cryptography
ECD	Extended Component Definition
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GCM	Galois Counter Mode
GE	Gigabit Ethernet port
HMAC	Hash-based Message Authentication Code
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IC2M	IOS Common Crypto Module
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IFS	IOS File System
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol

Acronyms / Abbreviations	Definition
ISAKMP	IPsec Internet Key Exchange
ISO	International Organization for Standardization
IT	Information Technology
KAS	Key-Agreement Scheme
KAT	Known Answer Test
LAN	Local Area Network
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NCS	Network Convergence System
NDcPP	collaborative Protection Profile for Network Devices
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OS	Operating System
OSP	Organizational Security Policy
OTN	Optical Transport Network
PHY	Physical Layer Device
PIN	Personnel Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POST	Power-on self-test
PP	Protection Profile
PPC	PowerPC
PRF	Pseudo-random function
PS	Power Supply
PSU	Power Supply Unit
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments (associated with the IETF)
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adelman
RSP	Route Switch Processor
RU	Rack Unit (1.75 inches)
SA	Security Association
SAN	Subject Alternative Name
SCEP	Simple Certificate Enrolment Protocol
SFP	Small-form-factor pluggable port
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SPD	Security Problem Definition
SSH	Secure Shell
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TD	Technical Decision
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
VPNGWEP	Device Protection Profile Extended Package VPN Gateway
WAN	Wide Area Network

Acronyms / Abbreviations	Definition
WIC	WAN Interface Card
XFP	Ten Gigabit Small Form Factor

Terminology

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

Table 2: Terminology

Term	Definition
Authorized Administrator	Any user that has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.
Peer	Another router on the network that the TOE interfaces.
Privilege level	Assigns a user specific management access to the TOE to run specific commands. The privilege levels are from 1-15 with 15 having full administrator access to the TOE similar to root access in UNIX or Administrator access on Windows. Privilege level 1 has the most limited access to the CLI. By default, when a user logs in to the Cisco IOS-XE, they will be in user EXEC mode (level 1). From this mode, the administrator has access to some information about the TOE, such as the status of interfaces, and the administrator can view routes in the routing table. However, the administrator can't make any changes or view the running configuration file. The privilege levels are customizable so that an Authorized Administrator can also assign certain commands to certain privilege levels.
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another router.
Role	An assigned role gives a user varying access to the management of the TOE. For the purposes of this evaluation the privilege level of user is synonymous with the assigned privilege level.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).

DOCUMENT INTRODUCTION

Prepared By:

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Aggregation Services Routers (ASR) 900 Series and Network Convergence System (NCS) 4200 Series running IOS-XE 16.9. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE, which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

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

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

1.1 ST and TOE Reference

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

Table 3: ST and TOE Identification

Name	Description
ST Title	Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9
ST Version	1.0
Publication Date	11 October 2019
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco ASR900 Series and NCS4200 Series
TOE Hardware Models	ASR902, ASR903, ASR907, ASR920 and NCS4201, NCS4202, NCS4206, NCS4216
TOE Software Version	IOS-XE 16.9
Keywords	Audit, Authentication, Encryption, Network Device, Router, Secure Administration, Virtual Private Network (VPN), VPN Gateway

1.2 TOE Overview

The Cisco Aggregation Services Routers (ASR) 900 Series and Network Convergence System (NCS) 4200 Series running IOS-XE 16.9 (herein after referred to as ASR900 Series and NCS4200 Series). The ASR900 Series and NCS4200 Series are purpose-built routing and switching platforms with OSI Layer2 and Layer3 traffic filtering capabilities, separation of the data plane and the control plane and are also capable of delivering circuit emulation (CEM) and optical transport network (OTN) capabilities over a redundant and protected packet-based network. The TOE includes the hardware models as defined in Table 3 in Section 1.1.

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. IOS-XE represents the continuing evolution of Cisco's pre-eminent IOS operating system. IOS-XE leverages the functionality that is provided by IOS, while adding new functionality and benefits, such as a set of infrastructure modules which define how software is installed, how processes are started and sequenced, how high-availability and software upgrades are performed and, lastly, how the applications are managed from an operational perspective.

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 1.6 Logical Scope of the TOE below.

1.2.1 TOE Product Type

The Cisco ASR900 Series and NCS4200 Series provide connectivity and security services onto a single, secure device. The TOE offers broadband speeds, cost-effective, modular solution based on a protocol-independent fabric architecture and simplified management to small businesses as well as metro and enterprise size business, service providers and carriers.

The Cisco ASR900 Series and NCS4200 Series are single-device security, routing and switching solutions for protecting the network. In support of their routing capabilities, both these devices provide IPsec connection capabilities to facilitate secure communications with external entities, as required and also provide VPN functionality.

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 the following environment components are supported by all TOE evaluated configurations.

Table 4: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Audit (Syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages over IPsec.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation with SSH client	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators.
TOE (VPN) Peer	Yes	This includes any TOE (VPN) peer with which the TOE participates in secure (IPsec) communications. The TOE (VPN) peer may be any device that supports secure (IPsec) communications.

1.3 TOE DESCRIPTION

This section provides an overview of the ASR900 Series and NCS4200 Series Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The TOE includes the hardware models as defined in Table 3 in Section 1.1. The software is comprised of the Universal Cisco Internetwork Operating System (IOS) XE software image Release IOS-XE 16.9.

The ASR900 Series and NCS4200 Series that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the platforms (such as throughput and amount of storage) and therefore support security equivalency of the platforms in terms of hardware.

The ASR900 Series and NCS4200 Series primary features include the following:

- Interface module slots that are designed to support a wide range of services, speeds, temperature ranges, and rich capabilities. They provide cost-effective delivery of converged circuit emulation, optical transport network and business Ethernet services. The interface modules that are supported include:
    - 100 Gigabit Ethernet Optics Supported in 1-Port 100GE CPAK Module - provides physical connectivity using a single pluggable 100GE CPAK optic
    - 40 Gigabit Ethernet Optics Supported in 2-Port 40GE QSFP Module - 2-port 40 Gigabit Ethernet QSFP module provides physical connectivity using two pluggable 40 Gigabit Ethernet optics
    - 10 Gigabit Ethernet Optics Supported in 8-Port 10GE SFP+ Module - provides eight 10 Gigabit Ethernet ports with physical connectivity, using pluggable 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) on each port. The interface module supports both the LAN and WAN physical layer (PHY).
    - Ethernet Optics Supported in 8-Port 1GE SFP and 1-Port 10GE SFP+ Module provides eight ports of Gigabit Ethernet and Fast Ethernet and one port of 10 Gigabit Ethernet interface. This module provides physical connectivity using eight SFP transceivers and one SPF+ transceiver
    - Ethernet Optics Supported in 8-Port 1GE RJ45 and 1-Port 10GE SFP+ Module provides eight ports of Gigabit and Fast Ethernet and one port of 10 Gigabit Ethernet connectivity. The module provides physical connectivity using eight RJ-45 connectors and one SFP+ transceiver slot.
    - Ethernet Optics Supported in 1-Port 10GE XFP Module provides physical connectivity using a single pluggable 10 Gigabit Ethernet XFP optic. It supports both the LAN and WAN PHY.
    - Ethernet Optics Supported in 2-Port 10GE XFP Module. That provides two 10 Gigabit Ethernet ports with physical connectivity, using either a pluggable 10 Gigabit Ethernet SFP+ optic or a pluggable 10 Gigabit Ethernet XFP optic per port. The interface module supports both LAN and WAN PHY.
    - Ethernet Optics Supported in the 8-Port 1GE SFP Module delivers eight ports of Gigabit Ethernet and Fast Ethernet connectivity.
- The Route Switch Processor (RSP) slots support:
    - Centralized network timing. Control plane and data plane elements. The RSP is the powerful centralized engine that provides these features and more for Cisco ASR 900 Series routers. The ASR 900 Series RSPs address the requirements of converged service provider networks, from Carrier Ethernet technologies to advanced services such as Multiprotocol Label Switching (MPLS).

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 1.6 Logical Scope of the TOE below.

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

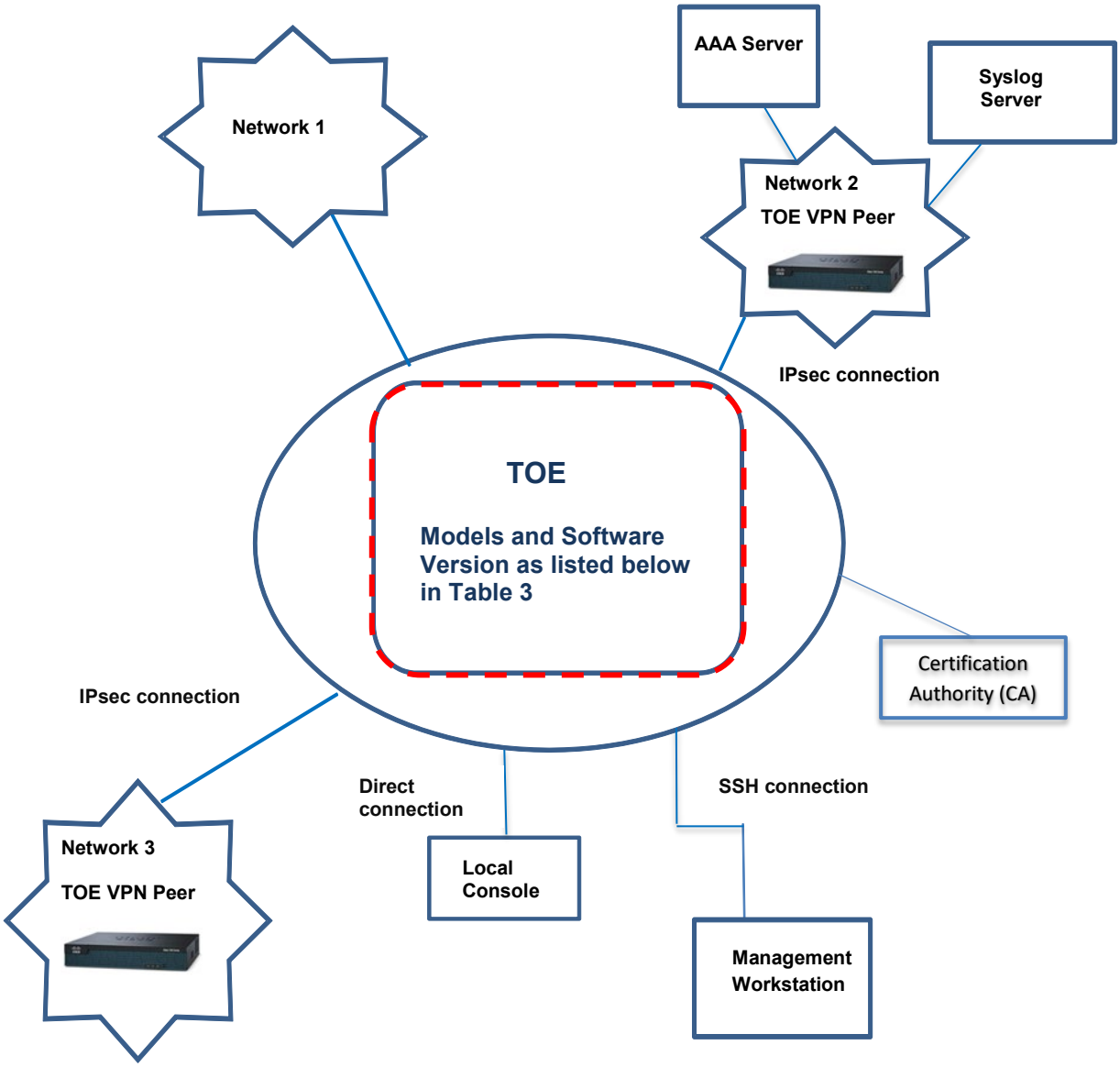


Figure 1: TOE Example Deployment

The previous figure includes the following devices, noting the TOE is only the ASR900 Series and NCS4200 Series and only one TOE device is required for the deployment of the TOE in the evaluated configuration.

- Identifies the TOE Models
  - ASR900 Series and NCS4200 Series models running Cisco IOS-XE 16.9
- Identifies the following IT entities that are considered to be in the IT Environment:
  - Authentication Server
  - Certification Authority (CA)
  - Local Console
  - Management Workstation
  - Syslog Server
  - TOE (VPN) Peers

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco IOS-XE software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The TOE 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.

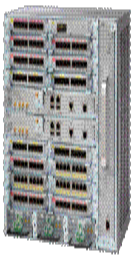
In addition, if the ASR900 Series and NCS4200 Series is to be remotely administered, then the management workstation must be connected to an internal network, where SSHv2 is used to securely connect to the TOE. A syslog server is used to store audit records, where IPsec is used to secure the transmission of the 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.

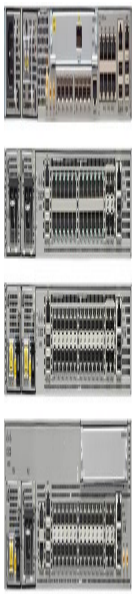
1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the router models as follows: ASR900 Series and NCS4200 Series running Cisco IOS-XE 16.9. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco ASR900 Series and NCS4200 Series Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the http://cisco.com web site. The TOE is comprised of the following physical specifications as described in Table 5 below:

Table 5: Hardware Models and Specifications

Hardware	Processor	Software	Picture	Size	Power	Interfaces
ASR902	CPU NXP P2020, CPU, Core PPC e500v2 or NXP T1042 and CPU, Core PPC e5500	Cisco IOS-XE 16.9		**Height**: 3.56in. (90.424 mm) - 2RU **Width:** 17.44 in. (443 mm) **Depth:** 9.22 in. (234.2 mm) **Weight:** 24.04 lb. (10.9 kg) with one RSP, two DC power supplies and loaded with a typical combination of interface module cards 9.48 lb. (4.3 kg) for an empty chassis	Up to 2 power supplies (AC or DC) Modules operate in load-share mode System can operate on a single power supply and supports mixing of one AC and one DC power supplies in a single chassis.	4 interface module slots 1 RSP slot

Hardware	Processor	Software	Picture	Size	Power	Interfaces
ASR903	CPU NXP P2020, CPU Core PPC e500v2	Cisco IOS-XE 16.9		**Height:** 5.22 in. (132.6 mm) - 3RU **Width:** 17.44 in. (443 mm) **Depth:** 9.22 in. (234.2 mm) **Weight:** 34.17 lb. (15.5 kg) with two RSPs, two DC power supplies, and loaded with a typical combination of interface module cards 11.2 lb. (5.1 kg) for an empty chassis	Up to 2 power supplies (AC or DC) Modules operate in load-share mode System can operate on a single power supply and supports mixing of one AC and one DC power supplies in a single chassis.	6 interface module slots 2 RSP slots
ASR907	CPU NXP T1042, CPU Core PPC e5500	Cisco IOS-XE 16.9		**Height:** 12.22 in. (310.38 mm) - 4RU **Width:** 17.44 in. (443 mm) **Depth:** 9.22 in. (234.2 mm) **Weight:** 69.32 lb. (31.4 kg) with two RSPs, two DC power supplies, and loaded with a typical combination of interface module cards 34.9 lb. (15.9 kg) for an empty chassis	Up to 3 power supplies (AC or DC) Modules operate in load share mode System can operate on a single power supply and supports mixing of AC and DC power supplies in a single chassis.	16 interface module slots 2 RSP slots

Hardware	Processor	Software	Picture	Size	Power	Interfaces
ASR920 (ASR920 series router offers multiple models with different port densities and interfaces, though these differences do not affect any of the functionality that is claimed)	CPU NXP P2020, CPU Core PPC e500v2	Cisco IOS-XE 16.9		**(H x W x D)** **ASR-920-12SZ-IM/ASR-920-12SZ-IM-CC:** 1.73 x 17.5 x 11.28 in. (44 x 444.5 x 286.54 mm), 1RU **ASR-920-24SZ-M:** 1.72 x 17.5 x 10 in. (43.7 x 444.5 x 255 mm), 1RU **ASR-920-24TZ-M**: 1.72 x 17.5 x 10 in. (43.7 x 444.5 x 255 mm), 1RU **ASR-920-24SZ-IM**: 2.6 x 17.5 x 10.6 in. (66 x 444.5 x 270 mm), 1.5RU (with IM) **Weight** **ASR-920-12SZ-IM/ASR-920-12SZ-IM-CC:** 9.25 lb. (4.2 kg) - empty chassis **ASR-920-24TZ-M:** 8.3 lb. (3.8 kg) - empty chassis **ASR-920-24SZ-M:** 8.5 lb. (3.9 kg) - empty chassis **ASR-920-24SZ-IM:** 10.3 lb. (4.7 kg) - empty chassis **ASR-920-12SZ-IM:** 13.44 lb. (6.1 kg) with two AC PSU and IM card **ASR-920-24TZ-M:** 10.5 lb. (4.8 kg) with two AC PSU **ASR-920-24SZ-M**: 10.5 lb. (4.8 kg) with two AC PSU **ASR-920-24SZ-IM:** 14.1 lb. (6.4 kg) with two AC PSUs and IM card	2 power supplies (AC or DC)	All interfaces built in, this fixed-form-factor platform is versatile and can address many deployment scenarios, including Gigabit Ethernet and 10 Gigabit Ethernet deployments.

Hardware	Processor	Software	Picture	Size	Power	Interfaces
NCS4201	CPU NXP P2020, CPU Core PPC e500v2	Cisco IOS-XE 16.9		**(H x W x D)** 1.72 x 17.5 x 11.28 in. (43.7 x 444.5 x 286.54 mm), 1RU **Weight** 8.5 lb. (3.9 kg) - empty chassis	2 power supplies (AC or DC)	Has fixed Ethernet interfaces (4X10GE + 24X GE FE 1)
NCS4202	CPU NXP T1042, CPU Core PPC e5500	Cisco IOS-XE 16.9		**(H x W x D)** 1.73 x 17.5 x 11.28 in. (44 x 444.5 x 286.54 mm), 1RU **Weight** 9.25 lb. (4.2 kg) - empty chassis	2 power supplies (AC or DC)	Has fixed Ethernet interfaces (8x1G copper + 4x1G SFP + 4x10G/1G (dual rate).
NCS4206	CPU NXP P2020, CPU Core PPC e500v2 or NXP T1042, CPU, Core PPC e5500	Cisco IOS-XE 16.9		**Height:** 5.22 in. (132.6 mm), 3 RU **Width:** 17.44 in. (443 mm) **Depth:** 9.22 in. (234.2 mm) **Weight:** 34.17 lb. (15.5 kg) with two RSPs, two DC power supplies, and loaded with a typical combination of interface module cards 11.2 lb. (5.1 kg) for an empty chassis	Up to 2 power supplies (AC or DC) Modules operate in load-share mode System can operate on a single power supply and supports mixing of one AC and one DC power supplies in a single chassis	6 interface module slots 2 RSP slots
NCS4216	CPU NXP T1042, CPU Core PPC e5500	Cisco IOS-XE 16.9		**Height:** 12.22 in. (310.38 mm), 7 RU **Width:** 17.44 in. (443 mm) **Depth:** 9.22 in. (234.2 mm) **Weight:** 69.32 lb. (31.4 kg) with two RSPs, two DC power supplies, and loaded with a typical combination of interface module cards 34.9 lb. (15.9 kg) for an empty chassis	Up to 3 power supplies (AC or DC) Modules operate in load-share mode System can operate on a single power supply and supports mixing of AC and DC power supplies in a single chassis	16 interface module slots 2 RSP slots

1.6 Logical Scope of the TOE

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

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the collaborative Protection Profile for Network Devices Version 2.1 20180924 and VPNGWEP v2.1 as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco ASR900 Series and NCS4200 Series provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

The auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections;
- modifications to the group of users that are part of the authorized administrator roles;
- all use of the user identification mechanism;
- any use of the authentication mechanism;
- Administrator lockout due to excessive authentication failures;
- any change in the configuration of the TOE;
- changes to time;
- initiation of TOE update;
- indication of completion of TSF self-test;
- maximum sessions being exceeded;
- termination of a remote session;
- attempts to unlock a termination session, and
- initiation and termination of a trusted channel.

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

The logs can be viewed on the TOE using the appropriate IOS-XE commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not

have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other ASR900 Series and NCS4200 Series security functionality. All the algorithms claimed have CAVP certificates (Operation Environment – ASR900 Series, PPC e5500 and NCS4200 series PPC e5500 and PPC e500v2).

The TOE leverages the IOS Common Crypto Module (IC2M) Rel5 as identified in the table below. The IOS-XE software calls the IC2M, certificate 2388 that has been validated for conformance to the requirements of FIPS 140-2 Level 1.

Refer to Table 6 for algorithm certificate references.

Table 6: FIPS References

Algorithm	Description	Supported Mode	CAVP Certificate #	Module	SFR
AES	Used for symmetric encryption/ decryption	CBC (128, 192 and 256) GCM (128, 192 and 256)	AES 4583	IC2M	FCS_COP.1/DataEncryption
SHS (SHA-1, SHA-256 and SHA-512)	Cryptographic hashing services	Byte Oriented	SHS 3760	IC2M	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	HMAC 3034	IC2M	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR (using AES 256)	DRBG 1529	IC2M	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation PKCS #1 v2.1 2048 bit key	RSA 2500	IC2M	FCS_CKM.1 FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	ECDSA 1122	IC2M	FCS_CKM.1 FCS_COP.1/SigGen
CVL-KAS-ECC	Key Agreement	NIST Special Publication 800-56A	Component 1257	IC2M	FCS_CKM.2
CVL-KAS-FFC	Key Agreement	NIST Special Publication 800-56A	Component 1257	IC2M	FCS_CKM.2

The TOE provides cryptography in support of secure connections that includes remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the remote authentication servers.

The cryptographic services provided by the TOE are described in Table 7 below.

Table 7: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.
HMAC	Used for keyed hash, integrity services in SSH session establishment.
DH	Used as the Key exchange method for SSH and IPsec.
ECC	Used to provide cryptographic signature services Used in Cryptographic Key Generation and Key Establishment
Internet Key Exchange (IKE)	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA	Used in IKE protocols peer authentication. Used to provide cryptographic signature services.
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing.
SP 800-90A DRBG	Used for random number generation, key generation and seeds to asymmetric key generation 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

The ASR900 Series and NCS4200 Series platforms contain the following processors as listed in Table 8, ASR900 Series and NCS4200 Series Platform Processors

Table 8: ASR900 Series and NCS4200 Series Platform Processors

Chassis	CPU Designation
ASR902	CPU NXP P2020 with CPU Core PPC e500v2, or CPU NXP T1042 with CPU Core PPC e5500
ASR903	CPU NXP P2020 with CPU Core PPC e500v2
ASR907	CPU NXP T1042 with CPU Core PPC e5500
ASR920	CPU NXP P2020 with CPU Core PPC e500v2
NCS4201	CPU NXP P2020 with CPU Core PPC e500v2
NCS4202	CPU NXP T1042 with CPU Core PPC e5500
NCS4206	CPU NXP P2020 with CPU Core PPC e500v2, or CPU NXP T1042 with CPU Core PPC e5500
NCS4216	CPU NXP T1042 with CPU Core PPC e5500

1.6.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

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

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of authentication attempts fail has exceeded 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 connections.

1.6.4 Security Management

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

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

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. The privileged administrator is the Authorized Administrator of the TOE who has the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE as described in this document.

1.6.5 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers 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.

1.6.6 Protection of the TSF

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

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

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. The TOE provides the Authorized Administrators the capability to update the TOE's clock manually to maintain a reliable timestamp. Finally, the TOE performs testing to verify correct operation of the TOE itself and that of the cryptographic module.

1.6.7 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 be configured to lock the Authorized Administrator account after a specified number of failed logon attempts until an authorized administrator can enable the user account.

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

1.6.8 Trusted path/Channels

The TOE allows trusted channels 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 also uses the IPsec to protect communications with a CA.

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 9: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.1 20180924.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. For a listing of Assurance Requirements claimed, see section 5.4.

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

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 10 below. The following NIAP Technical Decisions (TD) have also been applied to the claims in this document. Each posted TD was reviewed and considered based on the TOE product type, the PP claims and the security functions claimed in this document.

0179, 0209, 0242, 0248, 0307, 0316, 0317, 0319, 0329, 0356, 0398, 0399, 0400, 0402, 0408, 0409, 0410, 0412, 0424, 0425, 0436, 0447, 0448, and 0449

The following NIAP Technical Decisions (TD) were reviewed, though considered not applicable based on TOE product type, the PP claims, and the security functions claimed in this document.

0395, 0396, 0397, 0401, 0407, 0411, 0423, 0450, 0451, 0452, and 0453

Table 10: Protection Profiles

Protection Profile	Version	Date
Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway (VPNGWEP)	2.1	8 March, 2017
collaborative Protection Profile for Network Devices (NDcPP)	2.1	24 September 2018

2.2.1 Protection Profile Additions

The ST claims exact conformance to both the collaborative Protection Profile for Network Devices (NDcPP) 20180924, Version 2.1 and to the Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway (VPNGWEP), and does not include any additions to the functionality described in the Protection Profile.

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the:

- collaborative Protection Profile for Network Devices (NDcPP) 20180924, Version 2.1
- Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway (VPNGWEP), Version 2.1

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 collaborative Protection Profile for Network Devices (NDcPP) 20180924, Version 2.1 and Network Device collaborative Protection Profile Extended Package VPN Gateway (VPNGWEP) Version 2.1 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 NDcPPv2.1 and VPNGWEP v2.1 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 NDcPP 20180924, Version 2.1 and VPNGWEPv2.1 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 NDcPP 20180924, Version 2.1 and the VPNGWEP v2.1.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

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

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

3.1 Assumptions

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

Table 11: TOE Assumptions

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

Assumption	Assumption Definition
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
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 12: Threats

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

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

Threat	Threat Definition
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.

Threat	Threat Definition
T. NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link.
T.NETWORK_MISUSE	Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.

Threat	Threat Definition
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome. • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these modifications.
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a 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 13: 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 14: Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.ADDRESS_FILTERING	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) and/or receiving (destination) applicable network traffic as well as on established connection information.
O.AUTHENTICATION	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.FAIL_SECURE	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF.
O.PORT_FILTERING	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.

TOE Objective	TOE Security Objective Definition
O.SYSTEM_MONITORING	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs).
O.TOE_ADMINISTRATION	Compliant TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.

4.2 Security Objectives for the Environment

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

Table 15: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
OE.CONNECTIONS	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.

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 5, dated: April 2017* 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:

- Unaltered SFRs are stated in the form used in [CC2] or their extended component definition (ECD);
- Refinement made in the PP: the refinement text is indicated with **bold text** and ~~strikethroughs~~;
- Selection wholly or partially completed in the PP: the selection values (i.e. the selection values adopted in the PP or the remaining selection values available for the ST) are indicated with underlined text
  e.g. "[selection: *disclosure, modification, loss of use*]" in [CC2] or an ECD might become "disclosure" (completion) or "[selection: disclosure, modification]" (partial completion) in the PP;
- Assignment wholly or partially completed in the PP: indicated with *italicized text*;
- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text*
  e.g. "[selection: *change_default, query, modify, delete*, [*assignment: other operations*]]" in [CC2] or an ECD might become "change_default, select_tag" (completion of both selection and assignment) or "[selection: change_default, select_tag, select_value]" (partial completion of selection, and completion of assignment) in the PP;
- Iteration: indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

Extended SFRs are identified by having a label "EXT" at the end of the SFR name.

The following conventions were used to resolve conflicting SFRs between the NDcPP and VPNGWEP EP:

- All SFRs from VPNGWEP EP reproduced as-is
- SFRs that appear in both NDcPP and VPNGWEP are modified based on instructions specified in VPNGWEP

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 16: Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage

Class Name	Component Identification	Component Name
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.1/IKE	Cryptographic Key Generation (for IKE peer authentication)
	FCS_CKM.2	Cryptographic Key Establishment (Refined)
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (for AES data encryption/decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1/Hash	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1KeyedHash	Cryptographic Operation (for keyed-hash message authentication)
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_IPSEC_EXT.1	IPsec Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
	FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
FMT: Security management	FMT_MOF.1/Services	Trusted Update - Management of TSF Data
	FMT_MOF.1(1)/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of 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_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
	FPT_TST_EXT.1	TSF Testing
	FPT_TST_EXT.3	Extended: TSF Testing
	FPT_TUD_EXT.1	Trusted Update
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_FLS.1/SelfTest	Fail Secure
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

Class Name	Component Identification	Component Name
FTP: Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1/Admin	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrator actions comprising:
- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- [no other actions]]];

d) *Specifically defined auditable events listed in* Table 17.

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 17: Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.1/IKE	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).

SFR	Auditable Event	Additional Audit Record Contents
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MOF.1/Services	Starting and stopping of services.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	None.
FMT_SMF.1	All management activities of TSF data.	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 Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TST_EXT.3	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None

5.2.1.2 FAU_GEN.2 User Identity Association

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

5.2.1.3 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

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

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

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

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

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3

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

5.2.2.2 FCS_CKM.1/IKE Cryptographic Key Generation (for IKE peer authentication)

FCS_CKM.1.1/IKE The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a:
[

- **FIPS PUB 186-4 "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes;**

- **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [no other curves]**]

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

5.2.2.3 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

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

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1";
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3;

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

5.2.2.4 FCS_CKM.4 Cryptographic Key Destruction

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

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

that meets the following: *No Standard*.

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

FCS_COP.1.1/DataEncryption The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES operating in GCM, CBC mode* and cryptographic key sizes ***128 bits, 256 bits*** **and [192 bits]** that meet the following.

5.2.2.6 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm

[

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits or greater],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits or greater]

]

that meet the following: *[*

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384]; ISO/IEC 14888-3, Section 6.4

].

5.2.2.7 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash The TSF shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-512] ~~and cryptographic key sizes~~ ~~[assignment: cryptographic key sizes]~~ and **message digest sizes** [**160, 256, 512**] bits that meet the following: [*ISO/IEC 10118-3:2004*].

5.2.2.8 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

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

5.2.2.9 FCS_RBG_EXT.1 Random Bit Generation

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

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

5.2.2.10 FCS_IPSEC_EXT.1 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 have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

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

FCS_IPSEC_EXT.1.4: Refinement: The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 4106)] and [AES-CBC-192 (specified in RFC 3602), AES-GCM-192 (specified in RFC 4106)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512, no other algorithm].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [no other RFCs for hash functions]].
- IKEv2 as defined in RFCs 5996 [with no support for NAT traversal], and [no other RFCs 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-192, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-192, AES-GCM-256 (specified in RFC 5282)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

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

  ];
- IKEv2 SA lifetimes can be configured by an Security Administrator based on [
  - length of time, where the time values can configured within [**1-24**] hours;

  ]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv1 Phase 2 SA lifetimes can be configured by an Security Administrator based on [
  - number of bytes
  - length of time, where the time values can configured within [**1-8**] hours;

  ];
- IKEv2 Child SA lifetimes can be configured by an Security Administrator based on [
  - number of bytes
  - length of time, where the time values can configured within [**1-8**] hours;

].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x 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), and 384 (for DH Group 20)] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1, IKEv2] exchanges of length [

- according to the security strength associated with the negotiated Diffie-Hellman group;
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

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), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD_SA] connection.

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

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), CN: IP address, CN: Fully Qualified Domain Name (FQDN)], Distinguished Name (DN) and [no other reference identifier type].

5.2.2.11 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254].

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

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

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

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa] as its public key algorithm(s) and rejects all other public key algorithms.

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

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

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

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management (Refinement)

FIA_AFL.1.1 The TSF shall detect when **an Administrator configurable positive integer [1-3] of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely.**

FIA_AFL.1.2 Refinement: When the defined number of unsuccessful authentication attempts has been met, the TSF shall [**prevent the offending remote Administrator from successfully authenticating until unblocking action is taken by a local Administrator**].

5.2.3.2 FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and ”)”];
b) Minimum password length shall be configurable to [*15*] and [*15*].

5.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

- Display the warning banner in accordance with FTA_TAB.1;
- *[any network packets as configured by the authorized administrator may flow through the router]*.

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

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

5.2.3.5 FIA_UAU.7 Protected Authentication Feedback

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

5.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates.**
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:

- *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
- *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
- *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
- *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

5.2.3.1 FIA_X509_EXT.2 X.509 Certificate Authentication

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

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate]

5.2.3.2 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.2.3.3 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 and [no other protocols].

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 between 22 and 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].

FIA_PSK_EXT.1.4 The TSF shall be able to [accept] bit-based pre-shared keys.

5.2.4 Security management (FMT)

5.2.4.1 FMT_MOF.1/ManualUpdate Management of security functions behaviour

FMT_MOF.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual update to Security Administrators*.

5.2.4.2 FMT_MOF.1/Services Management of Security Functions Behavior

FMT_MOF.1/Services The TSF shall restrict the ability to enable and disable **start and stop** ~~the functions~~ **services** to *Security Administrators*.

5.2.4.3 FMT_MTD. 1/CoreData Management of TSF Data

FMT_MTD.1/CoreData The TSF shall restrict the ability to manage the *TSF data to Security Administrators.*

5.2.4.4 FMT_MTD.1/CryptoKeys of TSF Data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to *manage* the *cryptographic keys* and **certificates used for VPN operation** to *Security Administrators*.

5.2.4.5 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using* ***digital signature and [*****hash comparison****] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- ***Ability to configure the cryptographic functionality;***
- ***Ability to configure the lifetime for IPsec SAs;***
- ***Ability to import X.509v3 certificates;***
- ***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;*** [
    - Ability to configure audit behavior;
    - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
    - Ability to configure thresholds for SSH rekeying;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure the reference identifier for the peer;

    ]

].

5.2.4.6 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:
- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions
- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

5.2.5 Packet Filtering (FPF)

5.2.5.1 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

FPF_RUL_EXT.1.4 The TSF shall allow the following operations to be associated with Packet Filtering rules: permit, ~~deny~~, discard 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 drop traffic if a matching rule is not identified.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_FLS.1/SelfTest Fail Secure (Self-Test Failures)

FPT_FLS.1.1/SelfTest The TSF shall **shut down** 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.]*

5.2.6.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

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

5.2.6.1 FPT_APW_EXT.1: Protection of Administrator Passwords

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

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

5.2.6.2 FPT_TST_EXT.1: TSF Testing

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

- *Power-on Self-Tests:*
  - *Firmware Integrity Test*
  - *Known Answer Tests:*
    - *AES KAT*
    - *DRBG KAT*
    - *HMAC KAT*
    - *KAS ECC KAT*
    - *KAS FFC KAT*
    - *RSA KAT*

        - *ECDSA KAT*
        - *SP 800-56B RSA key wrap/unwrap KAT*
- *Conditional Self-Tests (run periodically during normal operation):*
    - *Continuous Random Number Generator test for DRBG*
    - *Continuous Random Number Generator test for Entropy Source*
    - *RSA Pairwise Consistency Test*
    - *Bypass Test*

].

5.2.6.3 FPT_TST_EXT.3: Extended: TSF Testing

FPT_TST_EXT.3.1 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/SigGen.

5.2.6.4 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

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

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

5.2.6.5 FPT_STM.EXT.1 Reliable time stamps

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

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time].

5.2.7 TOE Access (FTA)

5.2.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- 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.

5.2.7.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.7.3 FTA_SSL.4 User-initiated Termination

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

5.2.7.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.8 Trusted Path/Channels (FTP)

5.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1: Refinement: The TSF shall use **IPsec, and [no other protocols]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, VPN communications, [authentication server, and no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

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

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

- *remote AAA servers using IPsec*
- *external audit server using IPsec*
- *remote VPN gateways/peers using IPsec,*
- *a CA server using IPsec*].

5.2.8.2 FTP_TRP.1 Trusted Path

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

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

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

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv2.1

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv2.1 and VPNGWEPv2.1. As such, the NDcPPv2.1 and VPNGWEPv2.1 SFR dependency rationale is deemed acceptable since the PP and EP themselves have been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv2.1. As such, the NDcPPv2.1 SFR dependency rationale is deemed acceptable since the PP itself has been validated.

Table 18: Assurance Measures

Assurance Class	Components	Components Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
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	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv2.1 and VPNGWEP v2.1. As such, the NDcPPv2.1 SAR rationale is deemed acceptable since the PP itself have been validated.

5.5 Assurance Measures

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

Table 19 Assurance Measures

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

Table 20: How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the key-based SFR, "Auditable Events Table"). Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated (e.g. user identity, MAC address, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the start-up and shutdown of the audit functionality is audited. The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes [at least] all of the required information. Additional information can be configured and included if desired. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. Following is the audit record format: seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n) Following is an example of an audit record: *Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) 18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) *Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, not make the buffer size too large because the 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. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc.; all of which are described in the Guidance documents and IOS-XE CLI. Refer to the Common Criteria Operational

TOE SFRs	How the SFR is Met
	User Guidance and Preparative Procedures for command description and usage information. The logs can be saved to flash memory, so records are not lost in case of failures or restarts. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance, all emergency, alerts, critical, errors, and warning message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the TOE is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information; TOE functionality is not affected. To configure the TOE to send audit records to a syslog server, the 'set logging server' command is used. A maximum of three syslog servers can be configured. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The audit records are transmitted using IPsec tunnel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established. The FIPS crypto tests performed during startup, the messages are displayed only on the console. Once the box is up and operational and the crypto self-test command is entered, then the messages would be displayed on the console and will also be logged. Following is a sample of the self-test audit records: Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software checksum ... passed) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing ... passed) Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encryption/decryption ... passed) For the TSF self-test, successful completion of the self-test is indicated by reaching the log-on prompt. If there are issues, the applicable audit record is generated and displayed on the console. When the incoming traffic to the TOE exceeds what the interface can handle, the packets are dropped at the input queue itself and there are no error messages generated.
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.
FAU_STG_EXT.1	The TOE is configured to export syslog records to a specified, external syslog server.

TOE SFRs	How the SFR is Met
	Once the configuration is complete, audit records are automatically sent to the external syslog server, in real-time as they are written to the logging buffer. The TOE protects communications with an external syslog server via IPsec. If the IPsec connection fails, the TOE will store audit records locally on the TOE when it is discovered it can no longer communicate with the configured syslog server. When the connection is restored, the TOE will transmit the buffer contents to the syslog server. For audit records stored internally to the TOE, the administrator has the ability to configure the TOE to stop all auditable events when an audit storage threshold is met (lossless auditing) or given the log file is circular, the TOE may overwrite the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space. Please refer to the Guidance documentation for configuration syntax and information. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1 FCS_CKM.1/IKE FCS_CKM.2	The TOE implements Diffie-Hellman based key establishment schemes that meets RFC 3526, Section 3. The TOE implements and uses the prime and generator specified in RFC 3526 Section 3 when generating parameters for the key exchange. The TOE also implements RSA key establishment schemes that is conformant to NIST SP 800-56B. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in the NIST SP 800-56B. The TOE can also create ECDSA key pairs that can be used to generate a CSR. The RSA public-private key pair, has a minimum RSA key size of 2048-bit. The TOE also supports RSA key size of 3072-bit, and it is recommended to use the strong key size. Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes. Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes and Appendix B.4 for ECDSA schemes (using NIST curves P-256, P-384). The TOE can create a RSA public-private key pair that can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrolment Protocol (SCEP), the TOE can send the CSR to a Certificate Authority (CA) for the CA to generate a certificate and receive its X509v3 certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The key pair generation portions of "The RSA Validation System" for FIPS 186-4 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.

TOE SFRs	How the SFR is Met
	The TOE employs RSA-based key establishment used in cryptographic operations by implementing RSAES-PKCS1-v1_5 in accordance with section 7.2 of RFC 3447. The TOE implements Diffie-Hellman (DH) group 14 (2048) bit key establishment schemes in SSH. The DH key generation meets the NIST FIPS PUB 186-4 Appendix B.1. The TOE acts as a receiver for SSH communications and as both a sender and receiver for IPsec communications. For details on each protocol, see the related SFR.
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs). See Section 7.1 Key Zeroization for more information on the key zeroization.
FCS_COP.1/DataEncryption	The TOE provides symmetric encryption and decryption capabilities using AES in GCM and CBC mode (128, 192, and 256 bits) as described in ISO 18033-3, ISO 19772 and ISO 10116. AES is implemented in the following protocols: IPsec and SSH. The relevant FIPS certificate numbers are listed in Table 6 FIPS References.
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-4, “Digital Signature Standard”. The relevant FIPS certificate numbers are listed in Table 6 FIPS References.
FCS_COP.1/Hash	The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-512 as specified in ISO/IEC 10118-3:2004. For IKE (ISAKMP) hashing, administrators can select any of SHA-1, SHA-256 and/or SHA-512 (with message digest sizes of 160, 256 and 512 bits respectively) to be used with remote IPsec endpoints. SHA-256 hashing is used for verification of software image integrity. The relevant FIPS certificate numbers are listed in Table 6 FIPS References.
FCS_COP.1/KeyedHash	The TOE uses HMAC-SHA1 message authentication as part of the RADIUS Key Wrap functionality. For IPsec SA authentication integrity options administrators can select any of esp-sha-hmac (HMAC-SHA-1), esp-sha256-hmac, or esp-sha512-hmac (with message digest sizes of 160 and 256 and 512 bits respectively) to be part of the IPsec SA transform-set to be used with remote IPsec endpoints. The block sizes of the HMAC-SHA algorithms are prescribed by the underlying FIPS documents for these algorithms (FIPS 198-1 for HMAC and FIPS 180-4 for the underlying SHA). As per Figure 1 of FIPS 180-4 the block sizes would be as follows: • SHA-1 – 512 bits • SHA-256 – 512 bits • SHA-512 – 1024 bits The relevant FIPS certificate numbers are listed in Table 6 FIPS References.
FCS_IPSEC_EXT.1	The TOE implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The IPsec implementation provides both VPN peer-to-peer 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

TOE SFRs	How the SFR is Met
	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. 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. The IPsec protocol ESP is implemented using the cryptographic algorithms AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-CBC-128, AES-CBC-192 and AES-CBC-256 together with HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512. 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 strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 1 and IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 2 or IKEv2 CHILD_SA connection. The IKE protocols implement Peer Authentication using RSA and ECDSA along with X.509v3 certificates, or pre-shared keys. When certificates are used for authentication, the TOE validates the presented identifier provided supporting the following fields and types: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), CN: IP address, and CN: Fully Qualified Domain Name (FQDN), Distinguished Name(DN). Simultaneous use of the same identifier type in both the CN and SAN fields is not supported. 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.

TOE SFRs	How the SFR is Met
	The TOE supports both IKEv1 and IKEv2 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the 'crypto ISAKMP aggressive-mode disable' command. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours, but it is configurable to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets. The TOE supports Diffie-Hellman Group 14, 19, 24, and 20. Group 14 (2048-bit keys) can be set by using the "group 14" command in the config mode. 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 2^128. The nonce is likewise generated using the AES-CTR DRBG. The secret value 'x' used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) is generated using a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG). Preshared keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment. The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. The TOE provides AES-CBC-128, AES-CBC-192 and AES-CBC-256 for encrypting the IKEv1 payloads, and AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128 and AES-GCM-256 for 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), and 20 (384-bit Random ECP), 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), and 384 (for DH Group 20) bits. IPsec provides secure tunnels between two peers, such as two routers. 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. 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) 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

TOE SFRs	How the SFR is Met
	corresponding crypto map is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit ACLs would then flow through the IPSec tunnel and be classified as "PROTECTED". Traffic that does not match a permit ACL in the crypto map, but that is not disallowed by other ACLs on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit ACL and is also blocked by other non-crypto ACLs on the interface would be DISCARDED. 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. The command "fqdn <name" can be configured within a crypto identity and applied to a crypto map in order to perform validation of the peer device during authentication. Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication.
FCS_SSHS_EXT.1	The TOE implementation of SSHv2 supports the following: • Compliance with RFCs 4251, 4252, 4253, and 4254; • Dropping packets greater than 65,535 bytes, as such packets would violate the IP packet size limitations; • Enforcement to only allow the encryption algorithms AES-CBC-128, and AES-CBC-256 to ensure confidentiality of the session; • Enforcement to only use of the SSH_RSA public key algorithms for authentication; • Local password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server; • Enforcement to only allow the hashing algorithms hmac-sha1 and hmac-sha1-96 to ensure the integrity of the session and • Enforcement of DH Group 14 (diffie-hellman-group-14-sha1) as required by the NDcPPv2.1. The TOE can also be configured to require re-key after one hour of time and after one Gb of data.

TOE SFRs	How the SFR is Met
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. The DRBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate. The entropy source used to seed the DRBG (e.g. based on SP 800-90A/B/C) is a random set of bits or bytes that are regularly supplied to the DRBG by randomly poll the General Purpose Registers and capture entropy from it. This solution is available in the IOS 15.2(4)E or later FIPS/CC approved releases of the IOS XE images relating to the platforms mentioned above. All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed. Though related to this, the tests are part of the FIPS validation procedures for the DBRG and are part of the NIST validations for FIPS 140-2 for the products. Any initialization or system errors during bring-up or processing of this system causes a reboot as necessary to be FIPS compliant. Finally, the system will be zeroizing any entropy seeding bytes, which will not be available after the current collection.
FIA_AFL.1	The TOE provides the authorized administrator the ability to specify the maximum number of unsuccessful authentication attempts (between 1 and 25) before an authorized administrator is locked out through the administrative CLI using a privileged CLI command. When an authorized 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 an authorized administrator resets the user's number of failed login attempts through the administrative CLI.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and ”)”] Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters.
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. Through the implementation of the CLI, 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 by the cryptographic module prior to use via SHA-1.
FIA_UIA_EXT.1	

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

TOE SFRs	How the SFR is Met
	• Manual cut-and-paste—The router displays the certificate request on the console terminal, allowing the administrator to enter the issued certificate on the console terminal; manually cut-and-paste certificate requests and certificates when there is no network connection between the router and CA • Enrollment profiles—The router sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode certificate server (CS). • Self-signed certificate enrollment for a trust point All of the certificates include at least the following information: public key, Common Name, Organization, Organizational Unit and Country. Public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates can be stored in a specific location on the TOE. Certificates are stored to NVRAM by default; however, some routers do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates. The certificates themselves provide protection in that they are digitally signed. If a certificate were modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. The administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates. To verify, the authorized administrator could ‘show’ the pki certificates and the pki trust points. The authorized administrator can also configure one or more certificate fields together with their matching criteria to match. Such as: • alt-subject-name • expires-on • issuer-name • name • serial-number • subject-name • unstructured-subject-name • valid-start This allows for installing more than one certificate from one or more CAs on the TOE. For example, one certificate from one CA could be used for one IPsec connection, while another certificate from another CA could be used for a different IPsec connection. However, the default configuration is a single certificate from one CA that is used for all authenticated connections.

TOE SFRs	How the SFR is Met
	The physical security of the TOE (A. PHYSICAL_PROTECTION) protects the router and the certificates from being tampered with or deleted. Only authorized administrators with the necessary privilege level can access the certificate storage and add/delete them. 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. The use of CRL is configurable and may be used for certificate revocation. The authorized administrator could use the revocation-check command to specify at least one method of revocation checking; CRL. The authorized administer sets the trust point and its name and the revocation-check method • crl --Certificate checking is performed by a CRL. This is the default option. • none --Certificate checking is ignored. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. If the connection to determine the certificate validity cannot be established, the administrator is able to choose whether or not to accept the certificate.
FMT_MOF.1/ManualUpdate FMT_MOF.1/Services FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys	The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged levels. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged level equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. The term “Authorized Administrator” is used in this ST to refer to any user 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. As such, the semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned. The TOE provides the ability for Security Administrators (a.k.a Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds, cryptographic keys and updates. Each of the predefined and administratively configured privilege level has a set of permissions that will grant them access to the TOE data, though with some privilege levels, the access is limited.

TOE SFRs	How the SFR is Met
	The TOE does not provide automatic updates to the software version running on the TOE. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates. In addition, network packets are permitted to flow, as configured by the authorized administrator, through the TOE prior to the identification and authentication of an authorized administrator. The warning and access banner is also be displayed prior to the identification and authentication of an authorized administrator.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Security Administrators (a.k.a Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via SSHv2 secured connection, a terminal server, or at the local console. The specific management capabilities available from the TOE include; • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above; • The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users; • The ability to update the IOS-XE software. The validity of the image is provided using SHA-256 and digital signature prior to installing the update; • The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold; • The ability to manage termination of a local session due to exceeding the threshold of authentication failure attempts. The account is locked until the Authorized Administrator unlocks the account; • The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to view the audit logs and to clear the audit logs; • The ability to allow any network packets as configured by the authorized administrator may flow through the router prior to the identification and authentication process; • The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2 and to configure thresholds for SSH rekeying; • The ability to configure the IPsec functionality which supports the secure connections to the audit server and the remote authentication server; • The ability to import the X.509v3 certificates and validate for use in authentication and secure connections and • The ability to configure and set the time clock.

TOE SFRs	How the SFR is Met
FMT_SMR.2	The TOE maintains Authorizer Administrators that include privileged and semi-privileged administrator roles to administer the TOE locally and remotely. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are customizable. Note: the levels are not theoretically hierarchical. 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. 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 administration via SSH or IPSec over 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. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. The access lists can be applied to all the network interfaces. The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. 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. By implementing rules that defines the permitted flow of traffic between interfaces of the TOE for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on: 1. presumed address of source 2. presumed address of destination 3. transport layer protocol (or next header in IPv6) 4. Service used (UDP or TCP ports, both source and destination) 5. 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 pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). This is the default action that occurs on an interface if no ACL rule is found. If a packet arrives that does not meet any rule, it is expected to be dropped. 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.

TOE SFRs	How the SFR is Met
	These rules are entered in the form of access lists at the CLI (via 'access list' and 'access group' commands). These interfaces reject traffic when the traffic arrives on an external TOE interface, and the source address is an external IT entity on an internal network; These interfaces reject traffic when the traffic arrives on an internal TOE interface, and the source address is an external IT entity on the external network; These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on a broadcast network; These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on the loopback network; These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination; and Otherwise, these interfaces pass traffic only when its source address matches the network interface originating the traffic through another network interface corresponding to the traffic's destination address. 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. The initialization process first initializes the operating system, and then the networking daemons including the access list enforcement, prior to any daemons or user applications that potentially send network traffic. No incoming network traffic can be received before the access list functionality is operational.
FPT_FLS.1/SelfTest	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 FPT_APW_EXT.1	The TOE includes CLI command features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The command is the *password encryption aes* command used in global configuration mode. The command *service password-encryption* applies encryption to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords. During the setup and configuration of the TOE and the generation of keys, the TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additionally, all pre-shared and symmetric keys are stored in encrypted form to prevent access. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, the Authorized Administrator will have to log into the CLI to determine which test failed and why.

TOE SFRs	How the SFR is Met

	During the system bootup process (power on or reboot), all the Power on Start-up Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:
	
	• Power-on Self-Tests:
	  ○ Firmware Integrity Test – the firmware integrity test ensures the correct operation of the device and its components.
	  ○ Known Answer Tests:
	  ▪ AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.
	  ▪ RNG/DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.
	  ▪ HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.
	  ▪ KAS ECC KAT - Also known as the 'ECC Primitive "Z" KAT', the KAT shall be performed on the point multiplication for the ECC-based protocol (per SP 800-56A Rev 3, Section 5.7.1.2). See CMVP IG 9.6 for further details as to how this test is implemented (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf).
	  ▪ KAS FFC KAT - Also known as the 'FFC Primitive "Z" KAT', the KAT shall be performed on the underlying mathematical function(s) which use modular exponentiation for an FFC-based key establishment protocol (per SP 800-56A Rev. 3, Section 5.7.1.1). See CMVP IG 9.6 for further details as to how this test is implemented (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf).
	  ▪ RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known

TOE SFRs	How the SFR is Met
	encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. ▪ SP 800-56B RSA key wrap/unwrap KAT - The module has an RSA encryption pre-computed and then, while performing a power-up self-test, the module performs the RSA encryption again and compares the newly-generated result to the pre-computed value. The module also has a separate known answer for the RSA decryption by starting with a given value representing an RSA encryption and decrypting this value using the RSA algorithm. The result of said decryption operation is compared to a pre-computed result. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. • Conditional Self-Tests (run periodically during normal operation): o Continuous Random Number Generator test for DRBG - The first n-bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block shall be compared with the previously generated block. The test shall fail if any two compared n-bit blocks are equal. o Continuous Random Number Generator test for Entropy Source - This test functions precisely the same as the CRNGT for the DRBG (described above) except that input to the test is taken from the Entropy Source output as opposed to the DRBG output. o RSA Pairwise Consistency Test - Each time a new RSA public/private keypair is generated, the public key is used to encrypt a plaintext value. The resulting ciphertext value is then compared to the original plaintext value. If the two values are equal, then the test is considered to have failed. If the two values differ, then the private key is used to decrypt the ciphertext and the resulting value is then compared to the original plaintext value. If the two values are not equal, the test is considered to have failed. o Bypass Test – the bypass test involves testing correct operation providing crypto services when a router takes place between bypass services and crypto services. In short, the crypto series, gets tested normally overtime a bypass occurs and the returns. An example is AES known answer test gets run at start.

TOE SFRs	How the SFR is Met
	Then the module moves to bypass crypto services. Then returns back to crypto devices and the AES known answer test is immediately run. The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO. The combination of these tests is sufficient to verify that the correct version of the TOE is running as well as that the cryptographic operations are all performing as expected.
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 approved image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html. Digital signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded.. Instructions for how to do this verification are provided in the administrator guidance for this evaluation.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. 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 such as limiting SAs based on times.
FTA_SSL_EXT.1	An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "session-timeout" setting applied to the console and virtual terminal (vty) lines. The configuration of the vty lines sets the configuration for the remote console access. The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period of

TOE SFRs	How the SFR is Met
FTA_SSL.3	time, the session will be locked and will require re-authentication to unlock the session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the "exec-timeout" setting. The allowable inactivity timeout range is from 1 to 65535 seconds.
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions by issuing the 'exit' command.
FTA_TAB.1	Authorized administrators define a custom login banner that will be displayed at the CLI (local and remote) prior to allowing Authorized Administrator access through those interfaces.
FTP_ITC.1	The TOE protects communications with peer or neighbour routers using keyed hash as defined in FCS_COP.1/KeyedHash and cryptographic hashing functions FCS_COP.1/Hash. 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/DataEncryption is provided to ensure the data is not disclosed in transit. The TSF allows the TSF, or the authorized IT entities to initiate communication via the trusted channel. The TOE also requires that peers and other TOE instances establish an IKE/IPSec connection in order to forward routing tables used by the TOE. The TOE also requires that peers establish an IKE/IPsec connection to a CA server for sending certificate signing requests. 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. The distinction between "remote VPN gateway/peer" and "another instance of the TOE" is that "another instance of the TOE" would be installed in the evaluated configuration, and likely administered by the same personnel, whereas a "remote VPN gateway/peer" could be any interoperable IPsec gateway/peer that is expected to be administered by personnel who are not administrators of the TOE, and who share necessary IPsec tunnel configuration and authentication credentials with the TOE administrators. For example, the exchange of X.509 certificates for certificate-based authentication.
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users (Authorized Administrators) are able to initiate SSHv2 communications with the TOE.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

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

Table 21: TOE Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in DRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
skeyid	This is an IKE intermittent value used to create skeyid_d. This information is stored in DRAM. This information and keys are stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	This is an IKE intermittent value used to derive keying data for IPsec. This information and keys are stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	This the key IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	This the key IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared	This is the configured pre-shared key for ISAKMP negotiation. This key is stored in DRAM.	Zeroized using the following command: # no crypto isakmp key Overwritten with: 0x0d
IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. The device's public key must be added into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and to enrol with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is first sent to the other device so that it can be authenticated. The other device verifies the certificate is signed by CA's signing key, and then the device sends a random secret encrypted by the device's public key in the valid device certificate. Thus,	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x0d

Name	Description	Zeroization
	establishing the trusted connection since only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM.	
IPsec encryption key	This is the key used to encrypt IPsec sessions. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
IPsec authentication key	This is the key used to authenticate IPsec sessions. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
RADIUS secret	Shared secret used as part of the Radius authentication method. The password is stored in NVRAM.	Zeroized using the following command: # no radius-server key Overwritten with: 0x0d
SSH Private Key	This is the private (secret) key of the asymmetric key pair required to establish the secure SSH session. The key is stored in NVRAM.	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents). This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00
User Password	This is a variable 15+-character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password
Enable Password (if used)	This is a variable 15+-character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM.	Zeroized by overwriting with new password
RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 22: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, April 2017, version 3.1, Revision 5, CCMB-2017-04-004
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
[800-38A]	NIST Special Publication 800-38A, December 2001 Recommendation for Block Cipher Modes of Operation: Methods and Techniques
[800-56A]	NIST Special Publication 800-56A Rev. 3, April 2018 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[800-56B Rev. 2]	NIST Special Publication 800-56B Recommendation for Pair-Wise, March 2019 Key Establishment Schemes Using Integer Factorization Cryptography
[800-90A Rev. 1]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2015
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication
[FIPS PUB 180-4]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) August 2015
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008