Cisco ASR 9000 Aggregated Services Routers

Firmware version:

IOS-XR 7.1.2

- **ASR-9006-SYS, ASR-9010-SYS, ASR-9901, ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922**
- **RSPs A9K-RSP880-TR, A99-RP3-TR, A9K-RSP5-TR**
- **LCs: A99-8X100GE-TR, A99-12X100GE, A9K-16X100GE-TR, A99-32X100GE-TR**
- **MACSEC: ASR-9901**

FIPS-140 Non-Proprietary Security Policy- Security Level 1

Document Version 1.1

Cisco Systems, Inc.

Table of Contents

List of Figures

List of Tables

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for Cisco ASR 9000 Aggregated Services Routers; referred to in this document as ASR9k or the module. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at https://csrc.nist.gov/groups/STM/cmvp/index.html.

1.1 References

This document deals only with operations and capabilities of the module, in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.
- The NIST Cryptographic Module Validation Program website (https://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.2 FIPS 140-2 Submission Package

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco ASR 9000 Aggregated Services Routers and explains the secure configuration and operation of the module. This introduction section is followed by Section 2 through Section 8, which details the general features and functionality of the appliances. Section 9 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Module Description

ASR 9000 Series Aggregated Services Routers (9006, 9010, 9901,9904, 9906, 9910, 9912, 9922)

Networks are pressured to evolve more rapidly to keep pace with the increasing demand for ultra-low latency connections across both mobile and wireline networks. Edge networks need the capacity to scale, and feature-richness to support a wide array of high demand applications such as distributed provider edge, Internet peering, and metro aggregation. By delivering unparalleled feature richness and with the ability to scale in support of 400 GbE, the Cisco ASR 9000 series is changing the architectural economics for edge networks. Edge network architectures are becoming more distributed to enable new revenue generating services and bring edge compute and storage closer to the end user. This edge evolution requires both hardware and software to deliver scale, simplicity, trust, and security - a combination that can only be found in the Cisco portfolio.

Figure 1 - ASR-9006-SYS

Figure 2 - ASR-9010-SYS

Figure 3 - ASR-9901

Figure 4 - ASR-9904

Figure 5 - ASR-9906

Figure 6 - ASR-9910

Figure 7 - ASR-9912

Figure 8 - ASR-9922

2.1 Line Card and Route Processor for Modular Chassis

The Cisco ASR 9000 Series Aggregated Services Routers RSPs and LCs included with this module are as follows:

Figure 9 - A9K-RSP880-TR

Figure 10 - A99-RP3-TR

Figure 11 - A9K-RSP5-TR

Figure 12 - A99-8X100GE-TR

Figure 13 - A99-12X100GE

Figure 14 - A9K-16X100GE-TR

Figure 15 - A99-32X100GE-TR

The validated platforms consist of the following components:

Chassis	Hardware Configuration	
	Route Processor	Line Cards
ASR-9901	Fixed Chassis	Fixed Chassis
ASR-9006-SYS	A9K-RSP880-TR, A99-RP3-TR, A9K-RSP5-TR	A99-8X100GE-TR, A99-12X100GE, A9K-16X100GE-TR, A99-32X100GE-TR
ASR-9010-SYS		
ASR-9904		
ASR-9906		
ASR-9910		
ASR-9912		
ASR-9922		

Table 1 - Module Validation List

2.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**1**

Table 2 - Module Validation Level

2.4 FIPS and non-FIPS modes of operation

The Cisco ASR 9000 Aggregated Services Routers supports a FIPS and non-FIPS mode of operation. The non-FIPS mode of operation is not a recommended operational mode but because the module allows for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exists. The following services are available in both a FIPS and a non-FIPS mode of operation:

- SSH
- SNMPv3
- TLS
- MACsec

When the services are used in non-FIPS mode they are considered to be non-compliant. To determine the mode of operation, the Cryptographic Officer should run the following command:

- Use the "`show logging | i fips`" command to filter FIPS specific logging messages.

If the device is in the non-FIPS mode of operation, the Cryptographic Officer must follow the instructions in Section 10 of this security policy to transfer the module into a FIPS approved mode of operation. The FIPS Approved mode supports the approved and allowed algorithms, functions and protocols identified in Sections 5 and 7 of this document. The FIPS Approved mode of operation is entered when the module is configured for FIPS mode (detailed in Section 10) and successfully passes all the power on self-tests (POST).

In the FIPS mode of operation, there are two Approved modes of operation as follows:

- Standard Mode
- Recovery Mode

The FIPS Standard mode of operation is entered when the module is configured for FIPS mode and successfully passes all the power on self-tests (POST). The FIPS Standard Mode supports the approved and allowed algorithms, functions and protocols identified in Sections 5 and 7 of this document.

The FIPS Recovery mode of operation is entered when the module is configured for FIPS mode passes all the power on self-tests (POST) with the exception being that the POSTs related to the MACsec functionality fail. If the module is configured with more than one MACsec line card, then failure of any POST on a line card will cause that line card to be disabled, thus there is the potential for at least some of the MACsec functionality to be available to the module. If module does not have the capability to have more than one MACsec line card, or only has one MACsec line card and a POST failure is detected (related to the MACsec functionality) then the module may still operate except now all MACsec hardware is disabled but the remained crypto functionality and services are still available to the module.

Anyone of these modules, which has MACsec capability, can take on the role of either the Peer or the Authenticator in reference to the MACsec protocol. The link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

When supporting the MACsec protocol in the FIPS approved modes of operation, the module should only be used together with other CMVP-validated modules providing either the remaining Peer or Authenticator functionality.

It should be noted that the module contains two separate and independent versions of the FIPS-approved AES-GCM algorithm.

The implementation contained in firmware (see CAVP cert A2414) conforms to IG A.5, scenario #3, when operating in a FIPS approved mode of operation. AES GCM IVs are generated both internally and deterministically and are a minimum of 96-bits in length as specified in SP 800-38D, Section 8.2.1.

The implementation contained in hardware (see CAVP cert AES 4369) is used in support of line rate MACsec functionality and conforms to IG A.5, scenario #2, when operating in a FIPS-approved mode of operation. AES GCM IVs are generated externally (to the AES-GCM implementation on the chip but still within the module's boundary) using the module's FIPS-approved DRBG (CAVP algorithm cert A2414) and are a minimum of 96-bits in length as specified in SP 800-38D, Section 8.2.2.

3 Cryptographic Boundary

The cryptographic boundary for the Cisco ASR 9000 Aggregated Services Routers is defined as encompassing the "top," "bottom," "front," "back," "left" and "right" surfaces of the case. Included in this physical boundary is the ACT2Lite module (certificate #3637). ACT2Lite module is solely used as NDRNG (entropy source) and is neither used for directly generating any symmetric keys or seed for asymmetric keys nor used for any services implemented by the module. The minimum number of bits of entropy generated by the ACT2Lite module is 256 bits.

4 Cryptographic Module Ports and Interfaces

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following tables:

A9K-RSP880-TR Physical Interfaces	A9K-RSP880-TR Logical Interfaces
- 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - SFP+ External Interfaces (4)	Data Input Interface Data Output Interface
- 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 port - EIA/TIA-232 RJ232 serial RJ-45 ports—one each for Console and Auxiliary modem ports - USB Port (not used) - IEEE1588 RJ-45 Timestamp port - 10 MHz and 1 PPS clock input SMB ports - Alarm Cut Off (ACO) and Lamp Test momentary push buttons - SFP+ External Interfaces (4)	Control Input Interface
- Alarm Output DB9 port - 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port - EIA/TIA-232 RJ232 serial RJ-45 ports—one each for Console and Auxiliary modem ports - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - four-character 5x7 LED dot matrix display and discrete status LEDs - Status LED indicators (9)	Status Output interface

Table 3 - A9K-RSP880-TR Interfaces

A9K-RSP5-TR Physical Interfaces	A9K-RSP5-TR Logical Interfaces
- Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port	Data Input Interface Data Output Interface
- RJ-45 Sync timing ports with Link and Fault LEDs built into the RJ-45 (2) - IEEE1588 RJ-45 Timestamp port - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - 10 MHz and 1 PPS clock input SMB ports - External USB2, class-A port - 100/1000BASE-T (RJ-45) Management Ethernet (2) - EIA/TIA-232 RJ232 serial RJ-45 ports—one each for Console and Auxiliary modem ports - Alarm Cut Off (ACO) and Lamp Test momentary push buttons	Control Input Interface
- RJ-45 Sync timing ports with Link and Fault LEDs built into the RJ-45 (2) - Alarm Output DB9 port with three alarm outputs - 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - EIA/TIA-232 RJ232 serial RJ-45 ports—one each for Console and Auxiliary modem ports - four-character 5x7 LED dot matrix display and discrete status LEDs - Status LED indicators (9)	Status Output interface

Table 4 - A9K-RSP5-TR Interfaces

A99-RP3-TR Physical Interfaces	A99-RP3-TR Logical Interfaces
- Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port	Data Input Interface Data Output Interface
- RJ-45 Sync timing ports with Link and Fault LEDs built into the RJ-45 (2) - IEEE1588 RJ-45 Timestamp port - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - 10 MHz and 1 PPS clock input SMB ports - External USB2, class-A port - 100/1000BASE-T (RJ-45) Management Ethernet (2) - EIA/TIA-232 RJ232 serial RJ-45 ports—one each for Console and Auxiliary modem ports - Alarm Cut Off (ACO) and Lamp Test momentary push buttons	Control Input Interface
- RJ-45 Sync timing ports with Link and Fault LEDs built into the RJ-45 (2) - Alarm Output DB9 port with three alarm outputs - 100/1000BASE-T (RJ-45) Management Ethernet (2) - Connectivity Management Processor (CMP) port - Inter-Chassis Sync ports—nVSync1 is shared with RS232/422 GPS TOD RJ-45 ports (2) - EIA/TIA-232 RJ232 serial RJ-45 ports—one each for Console and Auxiliary modem ports - four-character 5x7 LED dot matrix display and discrete status LEDs - Status LED indicators (9)	Status Output interface

Table 5 - A99-RP3-TR Interfaces

A99-8X100GE-TR Physical Interfaces	A99-8X100GE-TR Logical Interfaces
100 GE QSFP28 Connectors (6) 400 GE QSFP-DD Connectors (2)	Data Input Interface Data Output Interface
100 GE QSFP28 Connectors (6) 400 GE QSFP-DD Connectors (2)	Control Input Interface
LEDs	Status Output interface

Table 6 - A99-8X100GE-TR Interfaces

A99-12X100GE Physical Interfaces	A99-12X100GE Logical Interfaces
100 GE QSFP28 Connectors (12)	Data Input Interface Data Output Interface
100 GE QSFP28 Connectors (12)	Control Input Interface
LEDs	Status Output interface

Table 7 - A99-12X100GE Interfaces

A9K-16X100GE-TR Physical Interfaces	A9K-16X100GE-TR Logical Interfaces
100 GE QSFP28/QSFP+ Connectors (16)	Data Input Interface Data Output Interface
100 GE QSFP28/QSFP+ Connectors (16)	Control Input Interface
LEDs	Status Output interface

Table 8 - A9K-16X100GE-TR Interfaces

A99-32X100GE-TR Physical Interfaces	A99-32X100GE-TR Logical Interfaces
100 GE QSFP28 Connectors (32)	Data Input Interface Data Output Interface
100 GE QSFP28 Connectors (32)	Control Input Interface
LEDs	Status Output interface

Table 9 - A99-32X100GE-TR Interfaces

ASR-9901 Physical Interfaces	ASR-9901 Logical Interfaces
- RJ-45 Console port - RJ-45 Auxiliary Port - 100/1000BASE-T (RJ-45) Management Ethernet (2) - 1G SFP Ports (16) - 1G/10G Dual Rate SFP Ports (24) - 100G SFP Ports (2)	Data Input Interface Data Output Interface

ASR-9901 Physical Interfaces	ASR-9901 Logical Interfaces
- External USB port - Fixed SFP+ ports (2) - RJ-45 Console port - RJ-45 Auxiliary Port - RJ-45 Service LAN - RJ-45 ToD port - SYNC (BITS/J.211) ports (2) - 10MHz and 1PPS ports - 100/1000BASE-T (RJ-45) Management Ethernet (2) - SFP Cluster ports (2) - 1G SFP Ports (16) - 1G/10G Dual Rate SFP Ports (24) - 100G SFP Ports (2)	Control Input Interface
- Status LED indicators (9) - four-character 5x7 LED dot matrix - 100/1000BASE-T (RJ-45) Management Ethernet (2)	Status Output interface
AC/DC Power connections (2)	Power Interface

Table 10 - ASR-9901 Interfaces

5 Roles, Services, and Authentication

The module supports identity-based authentication. There are two roles in the module that the operators may assume in the FIPS mode: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. A complete description of all the management and configuration capabilities of the modules can be found in the Cisco ASR 9000 Series Aggregated Services Routers Software Configuration Guide Manual[1] and in the online help for the modules.

It should be noted that the same services are available to both Users and Crypto-officer, regardless of whether or not they are in a non-FIPS approved mode of operation or a FIPS approved mode of operation.

5.1 User Services

A User enters the system by accessing the console port with a terminal program or SSH v2 session to a LAN port or the management Ethernet port. The module prompts the User for their username/password combination. If the username/password combination is correct, the User is allowed entry to the module management functionality. The services available to the User role consist of the following:

The services available to the User role consist of the following:

Services & Access	Description	Keys & CSPs
System Status	• The LEDs show the network activity (“Green” if the interfaces are up and running, “Flashing yellow” if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), view state of interfaces, protocols and firmware version.	N/A
Random Number Generation	• Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	• Key exchange as per SP800-56Arev3 over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
Module Read-only Configuration	• Viewing of configuration settings	N/A

Table 11 - User Services (r = read, w = write, d = delete)

[1] Software configuration guides are linked in Section 10.

5.2 Cryptographic Officer Services

A Crypto Officer enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the management Ethernet port. The Crypto Officer authenticates in the same manner as a User. The Crypto Officer is identified by accounts that are part of the usergroup "root-lr". A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

Services & Access	Description	Keys & CSPs
Self-Test and Initialization	• Cryptographic algorithm tests, firmware integrity tests, module initialization.	N/A (No keys are accessible)
System Status	• The LEDs show the network activity ("Green" if the interfaces are up and running, "Flashing yellow" if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), overall operational status ("Red" indicates module failure and "Green" indicates that module is operational) and the command line "status commands" output system status (indicates whether the module is in FIPS mode or not).	N/A (No keys are accessible)
Define Rules and Filters	• Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	Operator password – r, w, d
Random Number Generation	• Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	• Key exchange as per SP800-56Arev3 over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d

Zeroization	• Zeroize CSPs and cryptographic keys by cycling power to zeroize all cryptographic keys stored in DRAM. The CSPs stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed – d
Module Configuration	• Selection of non-cryptographic configuration settings	N/A
Power Cycle	• Reboot/reloading the module	All ephemeral Keys and CSPs will be destroyed - d
Secured Dataplane	• Secure communications at data link layer between module and peer device using MACsec.	MACsec Security Association Key (SAK), MACsec Connectivity Association Key (CAK), MACsec Key Encryption Key (KEK), MACsec Integrity Check Key (ICK), Pairwise Master Key (PMK), Pairwise Transient Key (PTK) – r, w, d
SNMPv3	• Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – w, d
SSH	• Establishment and subsequent data transfer of a SSH session for use between the module and the CO.	SSH encryption key, SSH integrity key, SSH RSA private key – r, w, d
HTTPS/TLS (Client)	• Establishment and subsequent data transfer using a TLS session. • Protection of syslog messages	HTTPS/TLS Pre-Master secret, HTTPS/TLS Master secret, HTTPS/TLS Encryption Key, HTTPS/TLS Integrity Key, HTTPS/TLS RSA/ECDSA private key – w, d

Table 12 - Crypto-Officer Services (r = read, w = write, d = delete)

User and CO Authentication

The Crypto Officer role is assumed by an authorized CO connecting to the module via CLI and SSH. The OS prompts the CO for their username and password, if the password is validated against the CO's password in memory, the operator is allowed entry to execute CO services. Each username is unique and configurable by Crypto-Officer. The password feedback mechanism does not provide information that could be used to determine the authentication data. The User role monitors the module via CLI and SSH.

The Crypto Officer and User passwords and all shared secrets must each be at least eight (8) characters long, including at least one (1) special character and at least one (1) number, in length (enforced procedurally by policy) along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. See the Secure Operation section for more information. If six (6) special/alpha/number characters, one (1) special character and one (1) alphabet are used without repetition for an eight (8) character long, the probability of randomly guessing the correct sequence is one (1) in 164,290,949,222,400 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. Since it is claimed to be for 8 digits with no repetition, then the calculation should

be 32x10x92x91x90x89x88x87). Therefore, for each attempt to use the authentication mechanism, the associated probability of a successful random attempt is approximately 1 in 164,290,949,222,400, which is less than the 1 in 1,000,000 required by FIPS 140-2. The maximum number of possible attempts per minute is 5 for Password Authentication via console. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is 5/164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

The module only supports sixteen (16) concurrent SSH sessions and maximum number of possible attempts per minute is 8 for each SSH session. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is (8*16)/ 164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

SSH Public-key Authentication: The CO and User role also supports public key authentication for remotely accessing the module via SSH. RSA has modulus size of 2048 bit, thus providing 112 bits of strength. An attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million-chance required by FIPS 140-2. The fastest network connection supported by the modules over management interfaces are 10 Gb/s. Hence, at most $10 \times 10^9 \times 60s = 6 \times 10^{11}$ = 600,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed, or a false acceptance will occur in one minute is:

$$1:(2^{112} \text{ possible keys}/(6 \times 10^{11} \text{ bits per minute})/112 \text{ bits per key}))$$
$$1:(2^{112} \text{ possible keys}/5,357,142,857 \text{ keys per minute})$$
$$1:9.7\times10^{23}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in 9.7×10^{23}, which is less than the 1 in 100,000 required by FIPS 140-2.

5.3 Unauthenticated User Services

The following are the list of services for Unauthenticated Operator:

System Status: An unauthenticated operator may observe the System Status by viewing the LEDs on the module, which show network activity and overall operational status. Unauthenticated operator can also view boot up/power on self-test logs on console port which does not disclose any security relevant information.

Power Cycle: This operator can power cycle the module. A solid green LED indicates normal operation and the successful completion of self-tests.

The module does not support a bypass capability.

6 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the Crypto Officer operator logins and can be zeroized by the Crypto Officer.
The module supports the following critical security parameters (CSPs):

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
DRBG entropy input	SP 800-90A CTR_DRBG	HW-based entropy source output used to construct seed.	256-bits	DRAM	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from a hardware-based entropy source.	384 bits	DRAM	Power cycle
DRBG V	SP 800-90A CTR_DRBG	Internal V value used as part of SP 800-90A CTR_DRBG	128 bits	DRAM	Power cycle
DRBG Key	SP 800-90A CTR_DRBG	This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG..	256 bits	DRAM	Power cycle
Diffie-Hellman public key	Diffie-Hellman	The public key used in Diffie-Hellman (DH) Exchange.	2048-8192 bits	DRAM	Power cycle
Diffie-Hellman private key	Diffie-Hellman	The private key used in Diffie-Hellman (DH) Exchange.	224-384 bits	DRAM	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman	The shared key used in Diffie-Hellman (DH) Exchange. Created per the Diffie-Hellman Protocol.	2048-8192 bits	DRAM	Power cycle
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19, 20 and 21)	P-256, P-384 public key used in EC Diffie-Hellman exchange. This key is derived per the Diffie-Hellman key agreement.	P-256, P-384 and P-521	DRAM (plaintext)	Power cycle
EC Diffie-Hellman private key	Diffie-Hellman (Groups 19, 20 and 21)	P-256 and P-384 private key used in EC Diffie-Hellman exchange. Generated by calling the SP 800-90A CTR-DRBG.	P-256, P-384 and P-521	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroizatio n
EC Diffie-Hellman shared secret	Diffie-Hellman (Groups 19, 20 and 21)	P-256 and P-384 shared secret derived in EC Diffie-Hellman exchange.	P-256, P-384 and P-521	DRAM (plaintext)	Power cycle
Operator password	Shared Secret, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	Variabl e (8+ characte rs)	Flash (plaintext)	Overwrite with new password
snmpEngineID	Shared secret	Unique string to identify the SNMP engine.	32-bits	Flash (plaintext)	Overwrite with new engine ID
SNMPv3 Password	Shared Secret	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	32 bytes	Flash (plaintext)	Overwrite with new password
SNMPv3 session key	AES-CFB	Encrypts SNMPv3 traffic.	128-bit	DRAM (plaintext)	Power cycle
SSH Encryption Key	AES-CTR and AES CBC	Symmetric AES key for encrypting SSH.	128-256-bits AES	DRAM (plaintext)	Power cycle
SSH Integrity Key	HMAC	Used for SSH integrity protection.	160/256 /512 bits	DRAM (plaintext)	Power cycle
SSH Public/Private Key Pair	RSA and ECDSA	PKCS#1 v.1.5, P-256/384/521 generated by calling the SP 800-90A CTR-DRBG.	MOD 2048/30 72/4096 P-256/384 /521	Flash (plaintext)	SSH private/public key is zeroized by either deletion (via # crypto key zeroize rsa or ecdsa) or by overwriting with a new value of the key
HTTPS/TLS Pre-Master secret	Shared secret	Internal generation by FIPS-approved DRBG. Used to establish HTTPS/TLS Master Secret .	48 bytes	DRAM (plaintext)	Power cycle
HTTPS/TLS Master secret	Shared secret	Derived from the HTTPS/TLS Pre-Master Secret. Used for computing the Encryption and Integrity Keys.	48 bytes	DRAM (plaintext)	Power cycle

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroizatio n
HTTPS/TLS Encryption Key	AES-CBC, AES-GCM.	AES key used to encrypt TLS data.	128 and 256 bits	DRAM (plaintext)	Power cycle
HTTPS/TLS Integrity Key	HMAC	HMAC key used for HTTPS integrity protection.	160-384 bits	DRAM (plaintext)	Power cycle
HTTPS/TLS public/private key	ECDSA, RSA	PKCS#1 v.1.5, P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	ECDSA (P-256 and P-384) RSA (MOD 2048/30 72)	Flash (plaintext)	HTTPS/TLS Server RSA private/public key is zeroized by either deletion (via # crypto key zeroize rsa or crypto key zeroize ecdsa nistp(256/384 /521) or by overwriting with new value of the key.
MACsec Connectivity Association Key (CAK)	Hex string	A CO configured pre-shared secret key possessed by members of a MACsec connectivity association to secure control plane traffic.	16 or 32 bytes	NVRAM (plaintext)	Overwritten with new a key.
MACsec Integrity Check Key (ICK)	AES-GCM	Used to prove an authorized peer sent the message. Derived from the CAK using the SP800-108 KDF.	128/25 6 bits	DRAM (plaintext)	Automatical ly when session expires or power cycle.
MACsec Key Encryption Key (KEK)	AES-CMAC	Used to transmit Security Association Key (SAK) to other peers of a MACsec connectivity association. Derived from the CAK using the SP800-108 KDF.	128/25 6 bits	DRAM (plaintext)	Automatical ly when session expires or power cycle.
MACsec Security Association Key (SAK)	AES-GCM	Derived from the CAK and used by the device network ports for securing User network traffic.	128/25 6bits	DRAM (plaintext)	Automatical ly when session expires or power cycle

Table 13 - Keys and CSPs

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco ASR 9000 Series Aggregated Services Routers support many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. The following table identifies the approved algorithms included in the ASR 9000 Series Aggregated Services Routers for use in the FIPS mode of operation. Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module.

Algorithm	Supported Mode	Cert. #
CiscoSSL FOM 6.2b		
AES	ECB (128, 192, 256); CBC (128, 192, 256); CFB128 (128, 192, 256), CTR (128, 192, 256), GCM (128, 192, 256)	**A2414**
SHS	SHA-1, -256, -384, and -512 (Byte Oriented)	
HMAC SHS	SHA-1[2], -256, -384, and -512	
DRBG	CTR (using AES-256)	
ECDSA	Key Generation (P-256, P-384 and P-521) Key Verification (P-256, P-384 and P-521) Signature Generation (P-256 with SHA2-256, SHA2-384, SHA2-512, P-384 with SHA2-384, SHA2-512 and P-521 with SHA2-521) Signature Verification (P-256 with SHA2-256, SHA2-384, SHA2-512, P-384 with SHA2-384, SHA2-512 and P-521 with SHA2-521)	
RSA	FIPS186-4 RSA Key Generation**:** MOD 2048 with SHA2-256, MOD 3072 with SHA2-256 PKCS#1 v.1.5, 2048-3072 bit key SigGen, MOD: 2048, 3072 SigVer, MOD 2048 – 3072.	

[2] SHA-1 is used for Digital signature verification (RSA SigVer) and Non-digital-signature applications (KDF IKEv2, KDF SP800-108, KDF SSH) as per SP800-131Ar2.

Algorithm	Supported Mode	Cert. #
CVL (SP800-135)	TLS KDF, IKEv2 KDF, SSH KDF, SNMP KDF Note: The TLS, IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	
KAS-SSC (SP800-56a rev3)	KAS FFC SSC: Mod Sizes: FB, FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, modp-2048, modp-3072, modp-4096, modp-6144, modp-8192 Scheme: dhEphem KAS ECC SSC: Curves: P-224, P-256, P-384, P-521 Scheme: Ephemeral Unified	
CKG (SP800-133rev2)	Vendor Affirmed	

Table 14 - FIPS-Approved Algorithms for use in FIPS Mode

- KTS (AES Cert. #A2414 and HMAC Cert. #A2414; key establishment methodology provides between 128 and 256 bits of encryption strength)
- KAS (KAS-SSC Cert. #A2414, CVL Cert. #A2414; key establishment methodology provides between 112 and 256 bits of encryption strength)

  The KAS FFC and KAS ECC strengths are as follows:
  - KAS-ECC-SSC: 112 and 256 bits of encryption strength
  - KAS-FFC-SSC: 112 and 200 bits of encryption strength

Note 1: The module's AES-GCM implementations conforms to IG A.5 Provision #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. Method ii) was used by the tester to demonstrate the module's compliance with the TLS provision for the AES GCM IV generation in IG A.5. The counter portion of the IV is set by the module within its cryptographic boundary. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that, a new AES GCM key is established. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established which is in accordance with scenario 3 in IG A.5.
For the SSH Encryption GCM key, the IV construction is in accordance with RFC 5647 Section 7. A 96-bit IV is constructed using a 32-bit fixed field and a 64-bit invocation counter field. The invocation field is treated as a 64-bit integer and is incremented after each invocation of AES-GCM to process a binary packet. A 32-bit block counter is also used. The counter is initially set to 1 and incremented as each keystream block of 128-

bits is produced. The counter portion of the IV is set by the module within its cryptographic boundary. The use of AES GCM for SSH meets FIPS 140-2 IG A.5 scenario #4.
Note 2: CVL Cert. #A2414 support the KDF (key derivation function) used in each of TLS, SSH and SNMPv3 protocols. TLS, SSH and SNMPv3 protocols have not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.
Note 3: CKG (vendor affirmed) Cryptographic Key Generation; SP 800-133rev2. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133rev2. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.
Note 4: There are algorithms, modes, and keys that have been CAVP tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are implemented by the module.

7.2 Non-Approved Algorithms allowed for use in FIPS-mode

The Cisco ASR 9000 Series Aggregated Services Routers cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- RSA[3] (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength. RSA with less than 112-bit of security strength is non-compliant and may not be used).
- NDRNG

7.3 Non-Approved Algorithms

The Cisco ASR 9000 Series Aggregated Services Routers cryptographic module, in addition to the above listed FIPS approved algorithms, can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFCs for the following protocols allow for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exist. So those services listed above with their FIPS approved algorithms in addition to the following services with their non-approved algorithms and non-approved keys sizes are available to the User and the Crypto Officer. Prior to using any of the non-Approved services, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

The Cisco ASR 9000 Series Aggregated Services Routers cryptographic module implements the following non-approved algorithms that are not permitted for use in FIPS 140-2 mode of operations:

[3] As per IG D.9, the RSA Key Wrapping uses RSA modulus of 2048 and 3072 bit long that uses PKCS#1-v1.5 scheme and is not complaint with any revision of SP800-56B.

Service[4]	Non-Approved Algorithm
SSH (non-compliant)	Symmetric: Triple-DES Asymmetric: 512-bit RSA,1024-bit RSA, Diffie-Hellman group 1
TLS (non-compliant)	Asymmetric: 512-bit RSA, 1024-bit RSA
SNMP (non-compliant)	Hashing: MD5, MACing: HMAC MD5

Table 15 - Non-FIPS-Approved Algorithms not to be used in FIPS Mode

8 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Power On Self-Tests Performed:

- Firmware Integrity Test 2048-bit/SHA-256 RSA

CiscoSSL FOM algorithm implementation

- AES ECB (128-bit) encryption KAT
- AES ECB (128-bit) decryption KAT
- AES GCM (256-bit) encryption KAT
- AES GCM (256-bit) decryption KAT
- HMAC SHA-1 KAT
- HMAC SHA2-256 KAT
- HMAC SHA2-384 KAT
- HMAC SHA2-512 KAT
- KAS FFC Primitive “Z” KAT using 2048 bit (SP800-56a rev3)
- KAS ECC Primitive “Z” KAT using P-256 (SP800-56a rev3)
- ECDSA P-256 sign and verify KATs
- RSA 2048 sign and verify KATs
- SP800-135 KDF KATs: IKEv2 KDF, TLS 1.2 KDF, SSH KDF, SNMP KDF
- SP 800-90A AES-CTR DRBG KAT
- SP 800-90A Section 11 Health Tests

[4] These non-approved algorithms are not to be used in FIPS mode.

As per IG 9.1 and IG 9.2, the module performs the HMAC SHA self-tests and these tests pass, thus assuring the health of underlying SHS implementations for CiscoSSL FOM algorithm implementation.

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before a role can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure.

Conditional Tests Performed:

- Continuous Random Number Generator Test for the FIPS-approved DRBG
- Repetition Count Test and APT on digitized output of the noise source
- ECDSA pairwise consistency test
- RSA pairwise consistency test
- Firmware Load test using a 2048-bit/SHA-256 RSA-Based integrity test to verify firmware to be loaded into the module.

9 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 1 physical security requirements.

10 Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the module is shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Upon initial boot from the factory, the module is in a non-FIPS mode of operation. To transition from a non-FIPS mode of operation to a FIPS mode of operation, the Crypto-Officer must follow all steps detailed in section 10.1 of this security policy.

10.1 System Initialization and Configuration

Step 1 - Initially the router does not have any user configuration. The system prompts you to specify the username of the root user as well as a secret (password).

- `Enter root-system username: [USERNAME]`
- `Enter secret: [PASSWORD]`
- `Enter secret again: [PASSWORD]`

Enter the root-system username and password.

- `Username: [USERNAME]`
- `Password: [PASSWORD]`

Step 2- CO assigns passwords to users for Identification and Authentication.

- `Configure Terminal`
- `line con 0`
- `password [PASSWORD]`
- `Login Local`

Step 3 - Configure Management port

- `configure terminal`
- `interface MgmtEth [rack/slot/port]`
- `ipv4 address [ipv4-address subnet-mask]`
- `no shutdown`
- `exit`
- `router static address-family ipv4 unicast [0.0.0.0/0 default-gateway]`
- `commit`

Step 4 - Configure SSH

- `configure terminal`
- `hostname [hostname]`
- `domain-name [domain-name]`
- `commit`

```
- exit
- crypto key generate rsa [keypair-label]
- configure terminal
- ssh server v2
- commit
```

Step 5 - Enable FIPS 1402- logging

```
- configure Terminal
- logging buffered debugging
- commit
```

Step 6 - Enable FIPS mode.

```
- configure terminal
- crypto fips-mode
- commit
- reload location all
```

On either reboot or reload the device will be in the FIPS Approved Mode of Operation.

NOTE: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

To transition from a FIPS mode of operation to a non-FIPS mode of operation, the Cryptographic Officer shall zeroize all keys and CSP's that were generated and remove the FIPS mode command from the configuration. For key zeroization, please refer to the "Zeroization" column in Section 6 of this security policy. To remove the FIPS mode command from the configuration, follow the steps below:

To disable FIPS mode

```
- configure terminal
- no crypto fips-mode
- commit
- reload location all
```

On reboot/reload device will be in the non-FIPS Approved Mode of Operation.

10.2 Remote Access

SSH access to the module is allowed in FIPS approved mode of operation, using SSH v2 and a FIPS approved algorithm.
SNMPv3 communications with the module are allowed in FIPS approved mode.

10.3 Key Strength

Key sizes with security strength of less than 112-bits shall not be used in FIPS mode of operation.

11 Related Documentation

This document deals only with operations and capabilities of the security appliances in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the security appliances from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (https://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.

For LED related information, please review the following document:

- Hardware Installation Guide for ASR 9000 Series Aggregated Services Routers Modular Routers. Chapter: LEDs (https://www.cisco.com/c/en/us/td/docs/iosxr/asr9000/hardware-install/hig/b-asr9k-hardware-installation-guide/b-asr9k-hardware-installation-guide_chapter_010.html

12 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

12.1 Cisco.com

You can access the most current Cisco documentation at this URL:
https://www.cisco.com/techsupport

You can access the Cisco website at this URL:
https://www.cisco.com

You can access international Cisco websites at this URL:
https://www.cisco.com/public/countries_languages.shtml

12.2 Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.
The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.
The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:
https://www.cisco.com/go/marketplace/

12.3 Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:
https://www.cisco.com/go/marketplace/
Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

13 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.
You can send comments about Cisco documentation to bug-doc@cisco.com.
You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

14 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:
https://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:
https://www.cisco.com/go/psirt
If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:
https://tools.cisco.com/security/center/rss.x?i=44

14.1 Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered non-emergencies.

- Non-emergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
https://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
The link on this page has the current PGP key ID in use.

15 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

15.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:
https://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:
https://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location

highlighted. Locate the serial number label on your product and record the information before placing a service call.

15.2 Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:
https://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: +1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:
https://www.cisco.com/techsupport/contacts

15.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.
Severity 1 (S1) – Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

16 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

https://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

https://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

https://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

https://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

https://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

https://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

https://www.cisco.com/en/US/learning/index.html

17 Definitions List

ACL	Access Control List
AES	Advanced Encryption Standard
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DRAM	Dynamic RAM
DRBG	Deterministic Random Bit Generator
EDC	Error Detection Code
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GigE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
ISSU	In-service software upgrade
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
PIN	Personal Identification Number
RAM	Random Access Memory
RNG	Random Number Generator
RP	Route Processor
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
VPN	Virtual Private Network