FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASR 1002f, ASR 1002 with ESP5 or ESP10, ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20, and ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20

Firmware version: 2.4.2t
Hardware versions: ASR1002f, ASR1002, ASR1004, ASR1006; Embedded Services Processor (ESP) Hardware versions: ASR1000-ESP5, ASR1000-ESP10, ASR1000-ESP20; Route Processor (RP) Hardware versions: ASR-1000-RP1, ASR-1000-RP2

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the ASR 1002f, ASR 1002 with ESP5 or ESP10, ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20, and ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20 from Cisco Systems, Inc., referred to in this document as the modules, routers, or by their specific model name. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

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 http://csrc.nist.gov/groups/STM/cmvp/index.html.

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 (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

FIPS 140-2 Submission Package

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package includes:

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

With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See “Obtaining Technical Assistance” section for more information.

Module Description

Cisco ASR (1002, 1004, and 1006)

The Cisco ASR 1000 Series Router (ASR 1002f, ASR 1002, ASR 1004, ASR 1006) is a highly scalable WAN and Internet Edge router platform that delivers embedded hardware acceleration for multiple Cisco IOS XE Software services without the need for separate service blades. In addition, the Cisco ASR 1000 Series Router is designed for business-class resiliency, featuring redundant Route and Embedded Services Processors, as well as software-based redundancy.

With routing performance and IPsec VPN acceleration around ten-fold that of previous midrange aggregation routers with services enabled, the Cisco ASR 1000 Series Routers provides a cost-effective approach to meet the latest services aggregation requirement. This is accomplished while still leveraging existing network designs and operational best practices.

The router also supports GDOI-based GetVPN services.

Embedded Services Processor (5Gbps, 10Gbps, 20Gbps)

The Cisco ASR 1000 Series Embedded Service Processors (ESPs) are based on the innovative, industry-leading Cisco QuantumFlow Processor for next-generation forwarding and queuing in silicon. These components use the first generation of the hardware and software architecture known as Cisco QuantumFlow Processor.

The 5-, 10-, and 20-Gbps Cisco ASR 1000 Series ESPs provide centralized forwarding-engine options for the Cisco ASR 1000 Series Aggregation Services Routers.

The Cisco ASR 1000 Series ESPs are responsible for the data-plane processing tasks, and all network traffic flows through them. The modules perform all baseline packet routing operations, including MAC classification, Layer 2 and Layer 3 forwarding, quality-of-service (QoS) classification, policing and shaping, security access control lists (ACLs), VPN, load balancing, and NetFlow.

Router Processor (RP1, RP2)

The Cisco ASR 1000 Series Route Processors address the route-processing requirements of carrier-grade IP and Multiprotocol Label Switching (MPLS) packet infrastructures. Not only do they provide advanced routing capabilities, but they also monitor and manage the other components in the Cisco ASR 1000 Series Aggregation Services Router.

The validated platforms consist of the following components:

- Cisco ASR 1002f – ASR1002f
- Cisco ASR 1002 – ASR1002
- Cisco ASR 1004 – ASR1004

- Cisco ASR 1006 – ASR1006
- Embedded Services Processor (5Gbps) – ASR1000-ESP5
- Embedded Services Processor (10Gbps) – ASR1000-ESP10
- Embedded Services Processor (20Gbps) – ASR1000-ESP20
- Route Processor 1 – ASR-1000-RP1
- Route Processor 2 – ASR-1000-RP2

Model	Firmware	Hardware Configuration
Cisco ASR 1002f	2.4.2t	Integrated RP Integrated ESP
Cisco ASR 1002		Integrated RP Single ESP (5Gbps)
		Integrated RP Single ESP (10Gbps)
Cisco ASR 1004		Single RP 1 Single ESP (10Gbps)
		Single RP 1 Single ESP (20Gbps)
		Single RP 2 Single ESP (10Gbps)
		Single RP 2 Single ESP (20Gbps)
Cisco ASR 1006		Dual RP 1 Dual ESP (10Gbps)
		Dual RP 1 Dual ESP (20Gbps)
		Dual RP 2 Dual ESP (10Gbps)
		Dual RP 2 Dual ESP (20Gbps)

Table 1: Module Hardware Configurations

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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2

8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**2**

Table 2: Module Validation Level

Cryptographic Boundary

The cryptographic boundary for the ASR 1002f, ASR 1002 with ESP5 or ESP10, ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20, and ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20 is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the case; all portions of the "backplane" of the case which are not designed to accommodate a removable port adapter; and space within the case that would be occupied by an installed port adapter. The cryptographic boundary includes the connection apparatus between the port adapter and the board that hosts the port adapter, but the boundary does not include the port adapter itself. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular port adapter.

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:

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (3) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Input Interface
Port Adapter Interface (3) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Output Interface
Port Adapter Interface (3) Console Port Auxiliary Port 10/100 BITS Ethernet Port (1 per RP) 10/100 Management Ethernet Port Power Switch	Control Input Interface
Port Adapter Interface (3) LEDs USB Ports (Up to 2) Console Port Auxiliary Port 10/100 Management Ethernet Port	Status Output Interface
Power Plug	Power interface

Table 3: ASR 1002f

NOTE: The ASR1002f module includes four GigE Ports in the front of the panel. These ports are covered by FIPS tamper evident labels. The ports are considered to be disabled since the tamper evident labels make them physically inaccessible.

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (3) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Input Interface
Port Adapter Interface (3) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Output Interface
Port Adapter Interface (3) Console Port Auxiliary Port 10/100 BITS Ethernet Port (1 per RP) 10/100 Management Ethernet Port Power Switch	Control Input Interface
Port Adapter Interface (3) LEDs USB Ports (Up to 2) Console Port Auxiliary Port 10/100 Management Ethernet Port	Status Output Interface
Power Plug	Power interface

Table 4: ASR 1002 with ESP5 or ESP10

NOTE: The ASR1002 with ESP5 or ESP10 module includes four GigE Ports in the front of the panel. These ports are covered by FIPS tamper evident labels. The ports are considered to be disabled since the tamper evident labels make them physically inaccessible.

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (8) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Input Interface
Port Adapter Interface (8) Console Port Auxiliary Port 10/100 Management Ethernet Port	Data Output Interface
Port Adapter Interface (8) Console Port Auxiliary Port 10/100 BITS Ethernet Port (1 per RP) 10/100 Management Ethernet Port Power Switch	Control Input Interface
Port Adapter Interface (8)	Status Output Interface

Physical Interfaces	FIPS 140-2 Logical Interfaces
LEDs USB Ports (Up to 2) Console Port Auxiliary Port 10/100 Management Ethernet Port	
Power Plug	Power interface

Table 5: ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (12) Console Port Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP)	Data Input Interface
Port Adapter Interface (12) Console Port Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) Power Switch	Data Output Interface
Port Adapter Interface (12) Console Port Auxiliary Port (1 per RP) 10/100 BITS Ethernet Port (1 per RP) 10/100 Management Ethernet Port (1 per RP)	Control Input Interface
Port Adapter Interface (12) LEDs USB Ports (Up to 2 per RP) Console Port Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP)	Status Output Interface
Power Plug	Power interface

Table 6: ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20

Roles, Services, and Authentication

Authentication is identity-based. Each user is authenticated upon initial access to the module. There are two main roles in the router that operators may assume: 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. The module supports RADIUS and TACACS+ for authentication. A complete description of all the management and configuration capabilities of the modules can be found in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide Manual and in the online help for the modules.

The User and Crypto Officer passwords and all shared secrets must each be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). See the Secure Operation section for more information. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 832,000,000. In order to successfully guess the sequence in one minute would require the ability to make over 13,000,000 guesses per second, which far exceeds the operational capabilities of the module. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence."

Additionally, when using RSA based authentication, RSA key pair has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $1.8\text{x}10^{21}$ attempts per minute, which far exceeds the operational capabilities of the modules to support.

User Services

A User enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the 10/100 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:

- Status Functions - View state of interfaces and protocols, firmware version
- Terminal Functions - Adjust the terminal session (e.g., lock the terminal, adjust flow control)
- Directory Services - Display directory of files kept in memory
- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand
- Perform Cryptography – Use the cryptography provided by the module (e.g., IPSec and GDOI)

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 10/100 management Ethernet port. The Crypto Officer authenticates in the same manner as a User. The Crypto Officer is identified by accounts that have a privilege level 15 (versus the privilege level 1 for users). 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:

- Configure the module - Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- 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 characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- Status Functions - View the module configuration, routing tables, active sessions, use get commands to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
- Manage the module - Log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manager user rights, initiate power-on self tests on demand and restore router configurations.
- Set Encryption/Bypass - Set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.
- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand

Unauthenticated User Services

The services for someone without an authorized role are to view the status output from the module’s LED pins, perform bypass services and cycle power.

Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the Crypto Officer operator logins, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE).

The module supports the following critical security parameters (CSPs):

CSP	Name	Alg.	Key Size	Description	Storage	Zeroization
#1	RNG Seed (IOS XE)	ANSI X9.31 RNG	64-bits	This RNG seed is created from several entropy sources throughout the module, including, contents of recent packets, recent statistics from the module, the exact time since boot (in microseconds), and recent RNG output.	DRAM (plaintext)	Automatically every 400 bytes, or turn off the router.
#2	RNG Seed (Nitrox)	ANSI X9.31 RNG	64-bits	This is the seed for Nitrox resident X9.31 RNG. This seed is created from Nitrox hardware entropy sources.	DRAM (plaintext)	Zeroized with generation of new seed
#3	RNG Seed Key (IOS XE)	ANSI X9.31 RNG	168-bits	This RNG seed key is created from several entropy sources throughout the module, including, contents of recent packets, recent statistics from the module, the exact time since boot (in microseconds), and recent RNG output.	DRAM (plaintext)	Automatically every 400 bytes, or turn off the router.
#4	RNG Seed Key (Nitrox)	ANSI X9.31 RNG	168-bits	This is the seed key for Nitrox resident X9.31 RNG. This seed is created from Nitrox hardware entropy sources.	DRAM (plaintext)	Zeroized with generation of new seed
#5	Diffie-Hellman Shared Secret	DH	1024 – 2048 bits	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	DRAM (plaintext)	Zeroized upon deletion.
#6	Diffie Hellman private exponent	DH	1024 – 2048 bits	The private exponent used in Diffie-Hellman (DH) exchange. This CSP is created using the ANSI X9.31 RNG (Nitrox).	DRAM (plaintext)	Zeroized upon deletion.
#7	skeyid	Keyed SHA-1	160-bits	Value derived per the IKE protocol based on the peer authentication method chosen.	DRAM (plaintext)	Automatically after IKE session terminated.
#8	skeyid_d	Keyed SHA-1	160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE

CSP	Name	Alg.	Key Size	Description	Storage	Zeroization
						session terminated.
#9	IKE session encrypt key	TDES/AES	168-bits/256-bits	The IKE session encrypt key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically after IKE session terminated.
#10	IKE session authentication key	SHA-1 HMAC	160-bits	The IKE session authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically after IKE session terminated.
#11	ISAKMP preshared	Secret	At least eight characters	The key used to generate IKE skeyid during preshared-key authentication. **# no crypto isakmp key** command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	**# no crypto isakmp key**
#12	IKE RSA Private Key	RSA (Private Key)	1024 – 2048 bits	The key used in IKE authentication. **# crypto key zeroize rsa** command zeroizes it.	NVRAM (plaintext)	**# crypto key zeroize rsa**
#13	IPSec encryption key	TDES/AES	168-bits/256-bits	The IPSec encryption key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically when IPSec session terminated.
#14	IPSec authentication key	SHA-1 HMAC	160-bits	The IPSec authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Automatically when IPSec session terminated.
#15	Operator password	Shared Secret	At least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Overwrite with new password
#16	Enable password	Shared Secret	At least eight characters	The plaintext password of the CO role. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Overwrite with new password
#17	Enable secret	Shared Secret	At least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password. The Cryptographic Operator optionally configures the module to obfuscate the Enable password. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Overwrite with new password

CSP	Name	Alg.	Key Size	Description	Storage	Zeroization
#18	RADIUS secret	Shared Secret	At least eight characters	The RADIUS shared secret. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext), DRAM (plaintext)	**# no radius-server key**
#19	TACACS + secret	Shared Secret	At least eight characters	The TACACS+ shared secret. This CSP is entered by the by the Cryptographic Officer.	NVRAM (plaintext), DRAM (plaintext)	**# no tacacs-server key**
#20	SSH Private Key	RSA	1024 – 2048 bits	The SSH private key for the module. RSA key sizes 1024 - 2048 bits.	NVRAM (plaintext)	SSH private key is zeroized by either deletion (via **# crypto key zeroize rsa**) or by overwriting with a new value of the key
#21	SSH Session Key	TDES/AES	168-bits/256-bits	The SSH session key. This key is created through SSH key establishment.	DRAM (plaintext)	Automatically when the SSH session is terminated.
#22	GDOI Data Security Key (TEK)	TDES/AES	168-bits/256-bits	This key is created using the “GROUPKEY-PULL” registration protocol with GDOI.	DRAM (plaintext)	Automatically when session terminated.
#23	GDOI Group Key Encrypting Key (KEK)	TDES/AES	168-bits/256-bits	This key is created using the “GROUPKEY-PUSH” registration protocol with GDOI.	DRAM (plaintext)	Automatically when session terminated.

Table 7: CSP Table

The services accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below.

	CSP	CSP #1	CSP #2	CSP #3	CSP #4	CSP #5	CSP #6	CSP #7	CSP #8	CSP #9	CSP #10	CSP #11	CSP #12	CSP #13	CSP #14	CSP #15	CSP #16	CSP #17	CSP #18	CSP #19	CSP #20	CSP #21	CSP #22	CSP #23
Role/Service																								
User Role																								
Network Function		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r							r	r
Status Function																								
Terminal Function																								
Directory Services																								

CO Role																								
Configure the module																								
Define Rules and Filters																								
Status Functions																								
Manage the module		d	d	d	d								d			r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d
Set Encryption/ Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w	r w d	r w d									

Table 8: Role CSP Access

Cryptographic Algorithms

Approved Cryptographic Algorithms

The Cisco ASR 1000 supports 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 1000 for use in the FIPS mode of operation.

Algorithm	Supported Mode	Cert. #
IOS XE (Route Processor 1)		
AES	CBC (128, 192, 256)	1250
SHS (SHA-1)	Byte Oriented	1147
HMAC SHA-1	Byte Oriented	730
RNG (ANSI X9.31)	Triple-DES	695
RSA	PKCS#1 v.1.5, 512-2048 bit key	599
Triple-DES	CBC	894
IOS XE (Route Processor 2)		
AES	CBC (128, 192, 256)	1250
SHS (SHA-1)	Byte Oriented	1147
HMAC SHA-1	Byte Oriented	730
RNG (ANSI X9.31)	Triple-DES	695
RSA	PKCS#1 v.1.5, 512-2048 bit key	599
Triple-DES	CBC	894
Nitrox 2420 (Embedded Services Processor (ESP5))		
AES	CBC (128, 192, 256)	333
SHS (SHA-1)	Byte Oriented	408
HMAC SHA-1	Byte Oriented	137
RNG (ANSI X9.31)	Triple-DES (EDE)	154
Triple-DES	KO 1, CBC	398
Nitrox 2435 (Embedded Services Processor (ESP10))		
AES	CBC (128, 192, 256)	333
SHS (SHA-1)	Byte Oriented	408
HMAC SHA-1	Byte Oriented	137
RNG (ANSI X9.31)	Triple-DES (EDE)	154
Triple-DES	KO 1, CBC	398
Nitrox 2450 (Embedded Services Processor (ESP20))		
AES	CBC (128, 192, 256)	333
SHS (SHA-1)	Byte Oriented	408
HMAC SHA-1	Byte Oriented	137
RNG (ANSI X9.31)	Triple-DES (EDE)	154
Triple-DES	KO 1, CBC	398

Table 9: FIPS-Approved Algorithms for use in FIPS Mode

Non-Approved Algorithms allowed for use in FIPS-mode

The ASR 1000 cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- Diffie-Hellman – provides between 80 and 156-bits of encryption strength
- RSA Key Wrapping – provides between 80 and 156-bits of encryption strength

Non-Approved Algorithms

The ASR 1000 cryptographic module implements the following non-Approved algorithms:

- ROMMON (Route Processor 1)
  - SHA-1 (non-compliant)
- ROMMON (Route Processor 2)
  - SHA-1 (non-compliant)
- ROMMON (Embedded Services Processor – ESP5/ESP10/ESP20)
  - SHA-1 (non-compliant)
- IOS XE (Route Processor 1)
  - MD5, DES, HMAC MD5, RC4 – May not be used in FIPS mode
- IOS XE (Route Processor 2)
  - MD5, DES, HMAC MD5, RC4 – May not be used in FIPS mode
- Nitrox 2420 (Embedded Services Processor (ESP5))
  - MD5, DES, HMAC MD5, RC4 – May not be used in FIPS mode
- Nitrox 2435 (Embedded Services Processor (ESP10))
  - MD5, DES, HMAC MD5, RC4 – May not be used in FIPS mode
- Nitrox 2450 (Embedded Services Processor (ESP20))
  - MD5, DES, HMAC MD5, RC4 – May not be used in FIPS mode

The modules support the following key establishment schemes[1]:

- SSH key establishment
- Internet Key Exchange Key Establishment (IKEv1)
- GDOI Key Establishment

[1] In addition to Diffie-Hellman listed above.

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 insure all components are functioning correctly. The modules implement the following power-on self-tests:

- Route Processor (RP1 and RP2)
  - Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, Triple-DES, RNG KAT, RSA KAT
  - Firmware Integrity Test (ROMMON SHS)
- Embedded Services Processor (ESP5, ESP10, ESP20)
  - Known Answer Tests: AES KAT, SHS KAT, HMAC KAT, Triple-DES, RNG KAT, RSA KAT
  - Firmware Integrity Test

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior any other operations; this prevents the module from passing any data during a power-on self-test failure. In addition, the modules also provide the following conditional self-tests:

- Route Processor (RP 1 and RP 2)
  - Continuous Random Number Generator test for the FIPS-approved RNG
  - Continuous Random Number Generator test for the non-approved RNG
  - Pair-Wise Consistency Test
  - Conditional Bypass Test
- Embedded Services Processor (ESP5, ESP10, ESP20)
  - Continuous Random Number Generator test for the FIPS-approved RNG
  - Continuous Random Number Generator test for the non-approved RNG
  - Conditional Bypass Test

Physical Security

This module is a multi-chip standalone cryptographic module.

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence. The following sections illustrate the physical security provided by the module. The module relies upon Tamper Evident Labels and Opacity Shields (Cisco Part No. ASR1002-FIPS-Kit= (ASR 1002 and ASR 1002F), ASR1004-FIPS-Kit= (ASR 1004), ASR1006-FIPS-Kit= (ASR 1006)).

Tamper Evidence

Once the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. The Crypto Officer shall be instructed to record serial numbers, and to inspect for these signs of tampering or changed numbers periodically. The modules require the following number of labels

- ASR 1002 – 11 labels
- ASR 1002f – 9 labels
- ASR 1004 – 18 labels
- ASR 1006 – 32 labels

Each module requires an additional two labels placed on the opacity shields, which are not counted in the above total. Please see the Module Opacity section below for details.

To seal the system, apply serialized tamper-evidence labels as depicted in Figures 1-8 below:

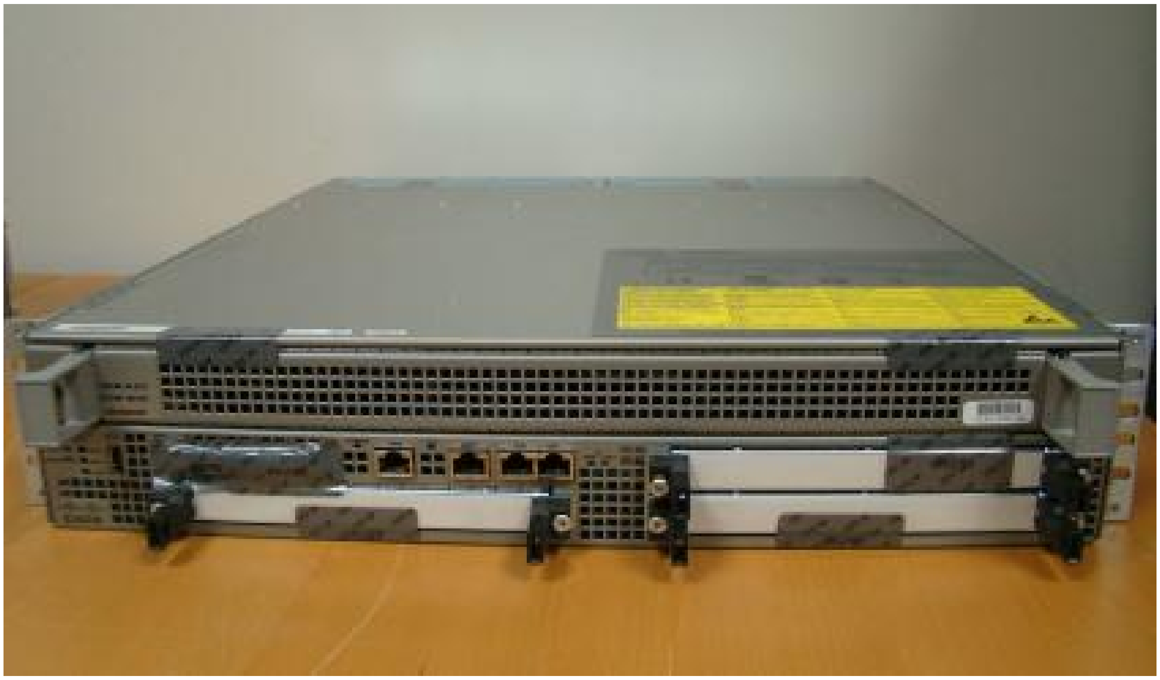

Figure 1: ASR 1002 Tamper Evident Seal Placement Front (w/o shield)

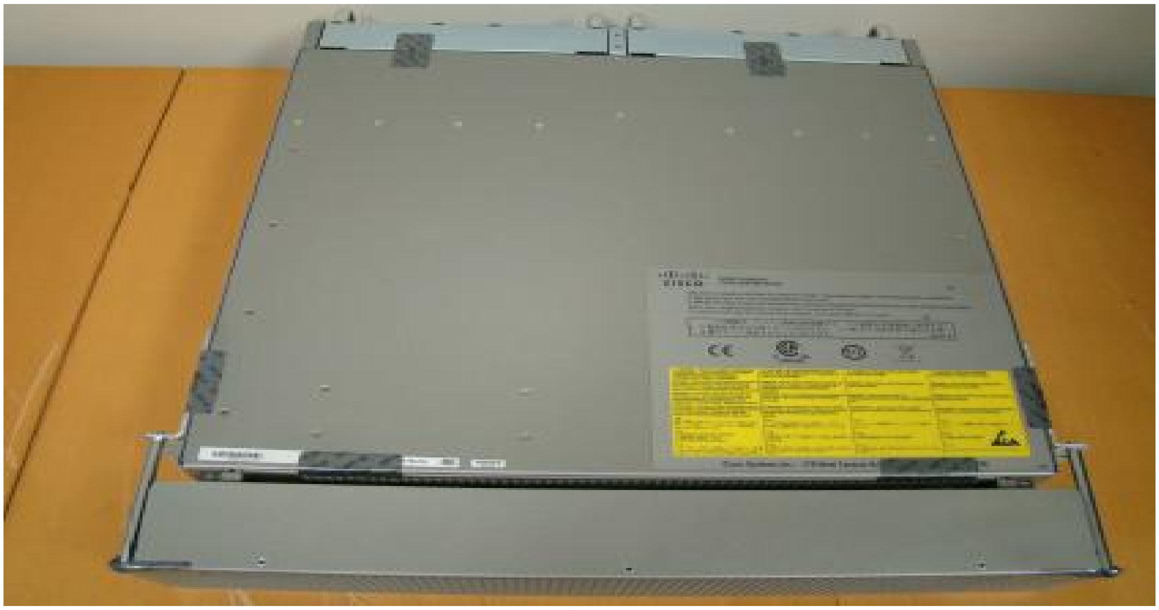

Figure 2: ASR 1002 Tamper Evident Seal Placement Top

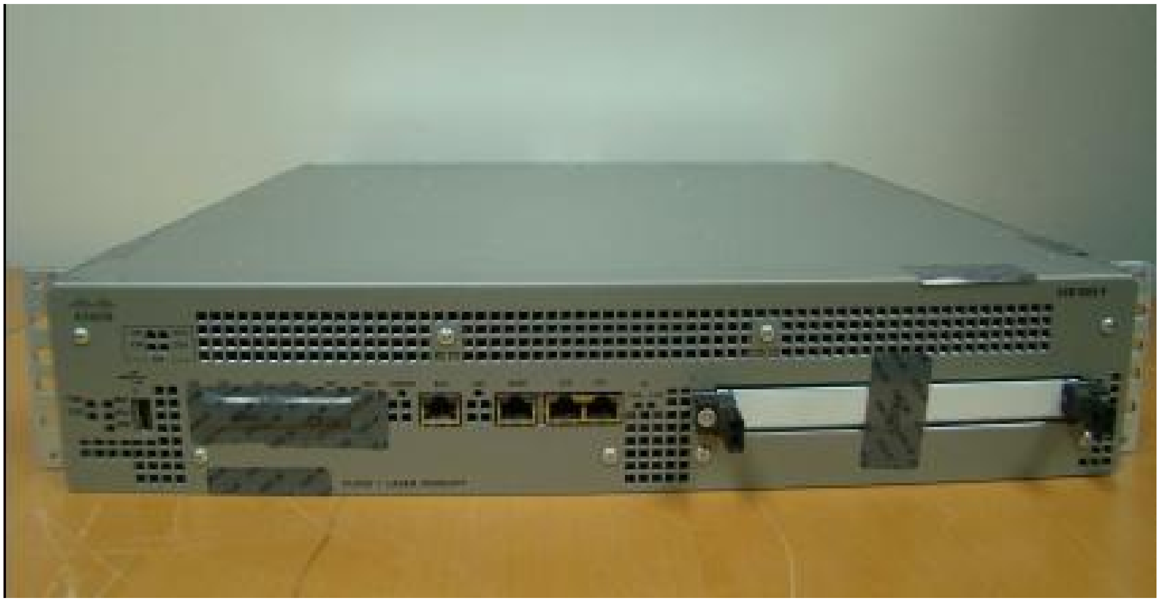

Figure 3: ASR 1002f Tamper Evident Seal Placement Front (w/o shield)

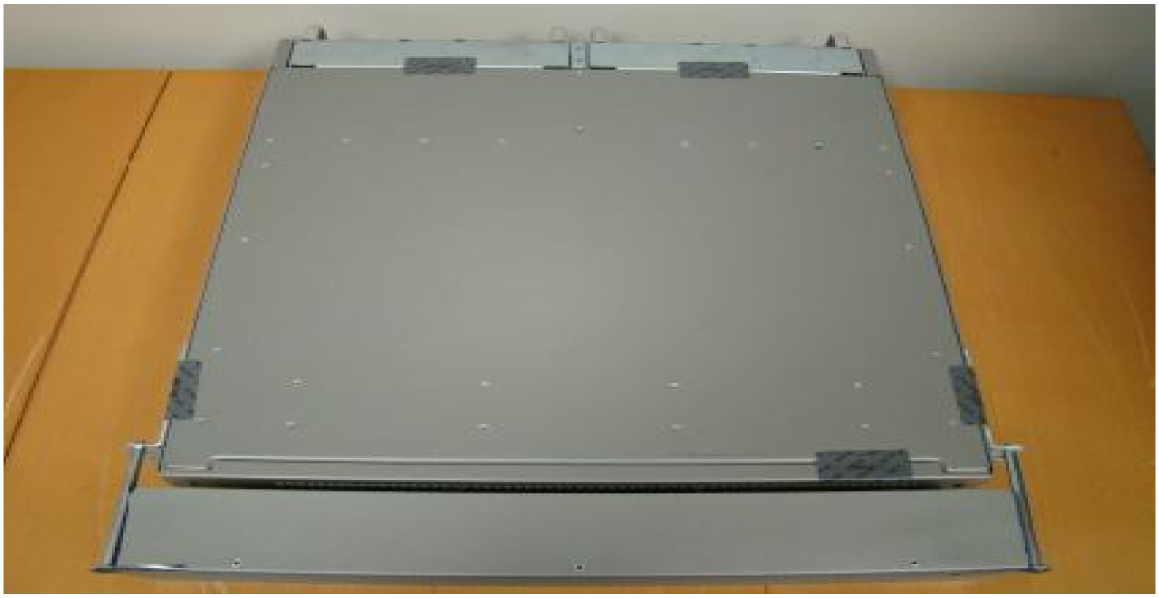

Figure 4: ASR 1002f Tamper Evident Seal Placement Top

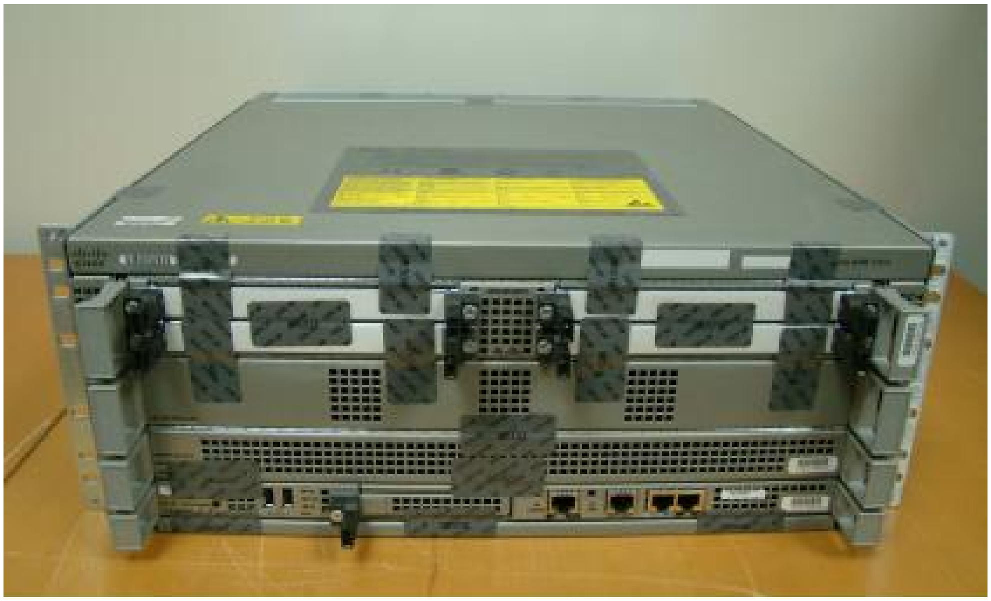

Figure 5: ASR 1004 Tamper Evident Seal Placement Front

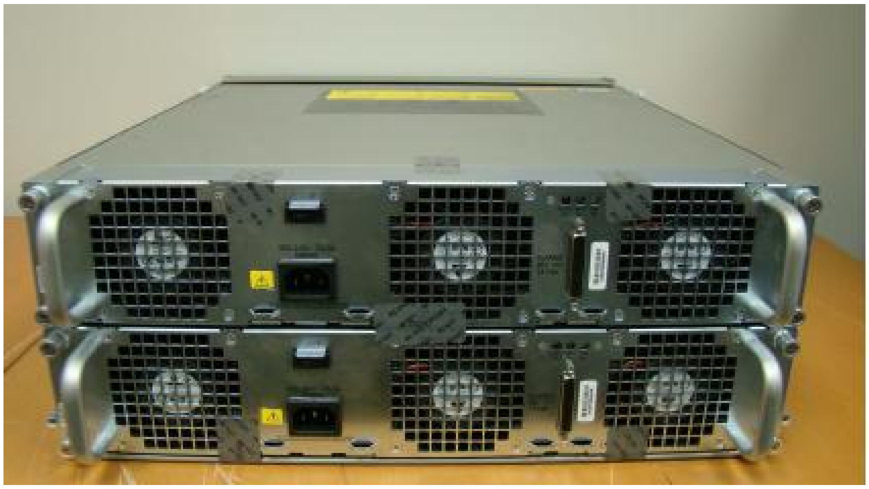

Figure 6:ASR 1004 Tamper Evident Seal Placement Back

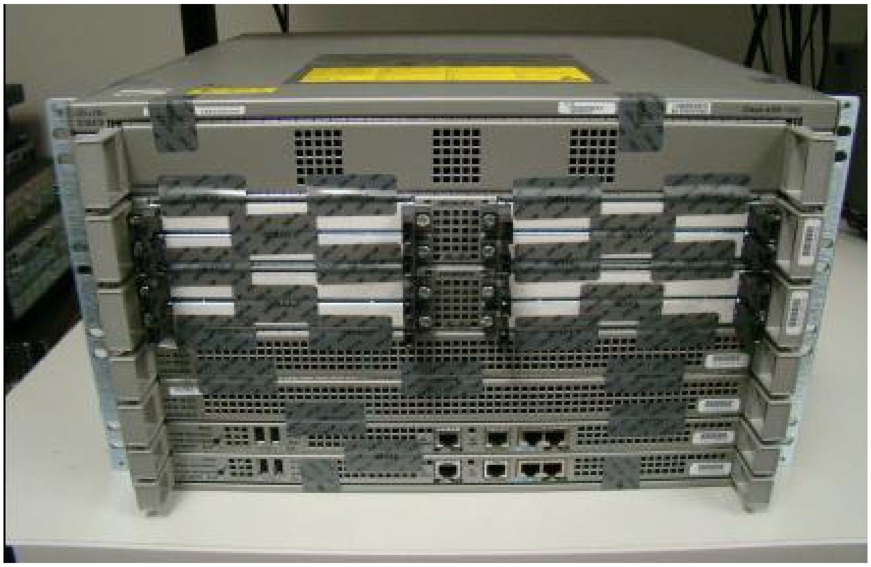

Figure 7: ASR 1006 Tamper Evident Seal Placement Front

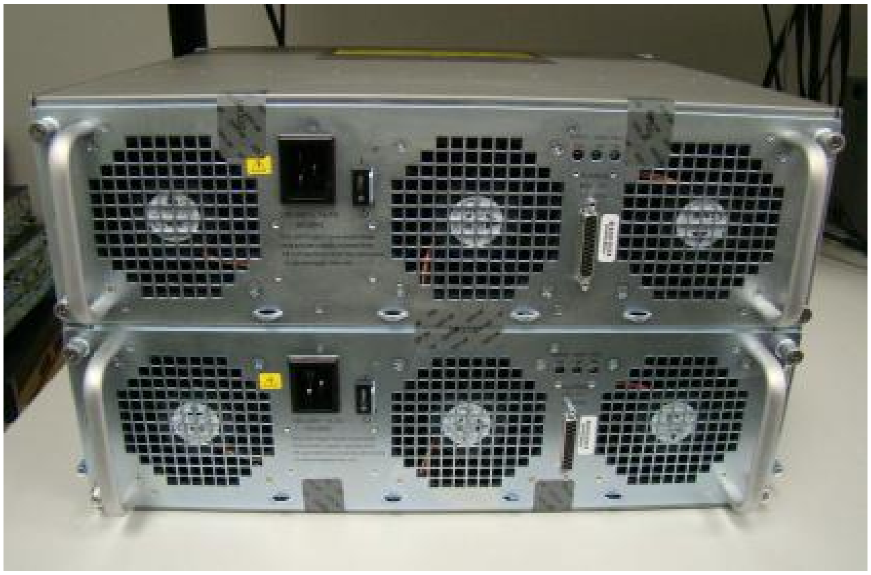

Figure 8: ASR 1006 Tamper Evident Seal Placement Back

Module Opacity

The modules require that a special opacity shield be installed over front panel of the modules in order to operate in FIPS-approved mode. The shield decreases the surface area of the vent holes, reducing visibility within the cryptographic boundary to FIPS-approved specifications.

Installing the Opacity Shield on the Cisco ASR 1002, ASR 1004, or ASR 1006

To install an opacity shield on the Cisco ASR 1002, ASR1002f, ASR 1004, or ASR 1006, follow these steps:

- Step 1: The opacity shield is designed to be installed on a Cisco ASR 1002, ASR1002f, ASR 1004, or ASR 1006 router chassis that is already rack-mounted.
- Step 2: Open the FIPS kit packaging. The kit contains the following items:
  - A packaged opacity shield assembly with installation hardware for the Cisco ASR 1002, ASR 1004, or ASR 1006, as appropriate.
  - An envelope with FIPS tamper evident labels.
  - An envelope containing a disposable ESD wrist strap.
- Step 3: Open the protective packaging and remove the opacity shield.
- Step 4: Remove the sticker cover on the back of the opacity shield.
- Step 5: Line up the opacity shield with the rack mount screw holes on the router, and press it against the chassis of the router.
- Step 6: Tighten the screws until the opacity shield is firmly attached to the module.

- Step 7: Before applying tamper evident labels (either for the first time or subsequent re-application), clean the surfaces with solvent agent (i.e. acetone) to ensure a clean, residue free surface for label application.
- Step 8: Place tamper evident labels over screws as shown in Figures 9-12.

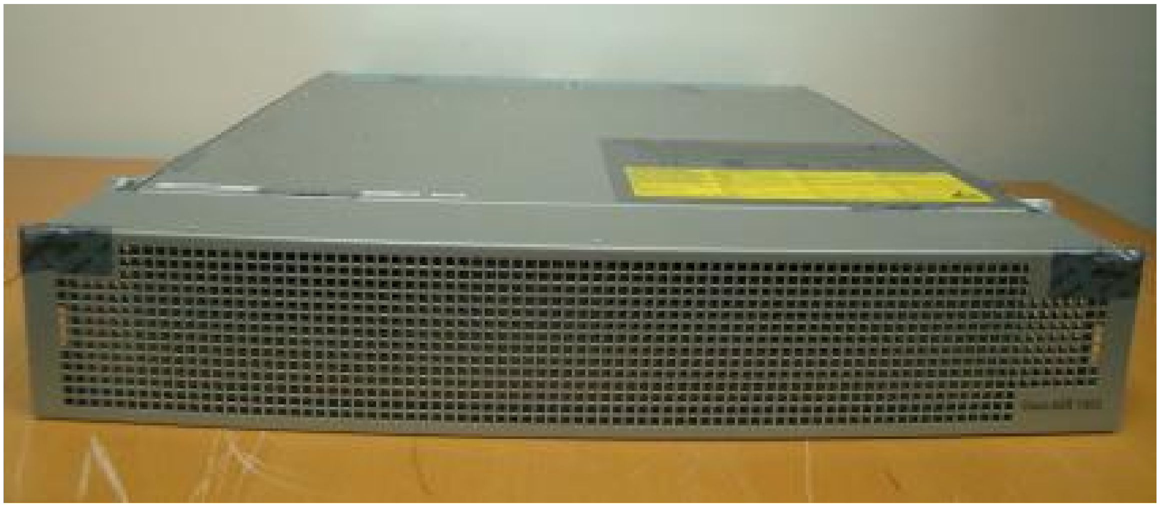

Figure 9: ASR 1002 with Opacity Shield Installed

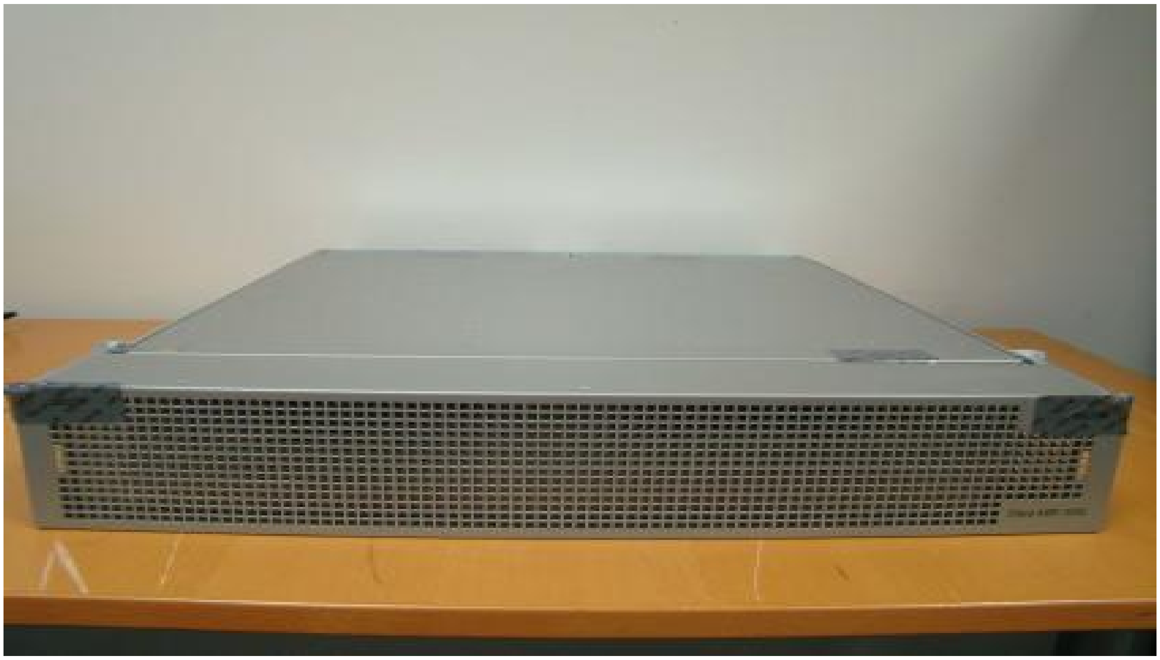

Figure 10: ASR 1002f with Opacity Shield Installed

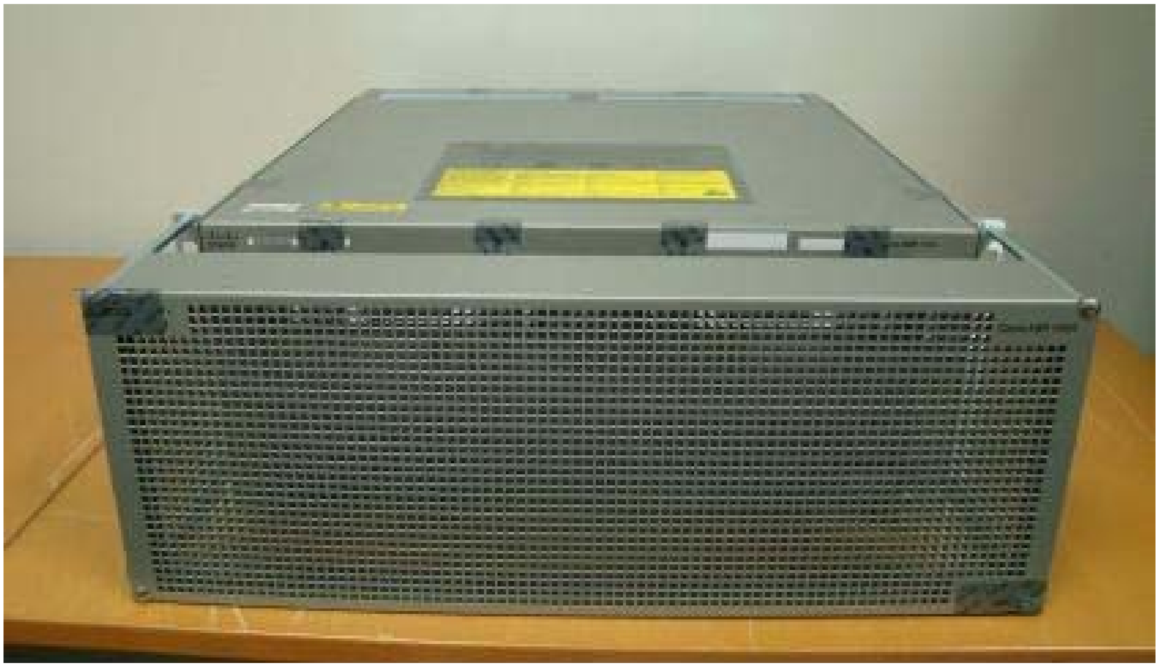

Figure 11: ASR 1004 with Opacity Shield Installed

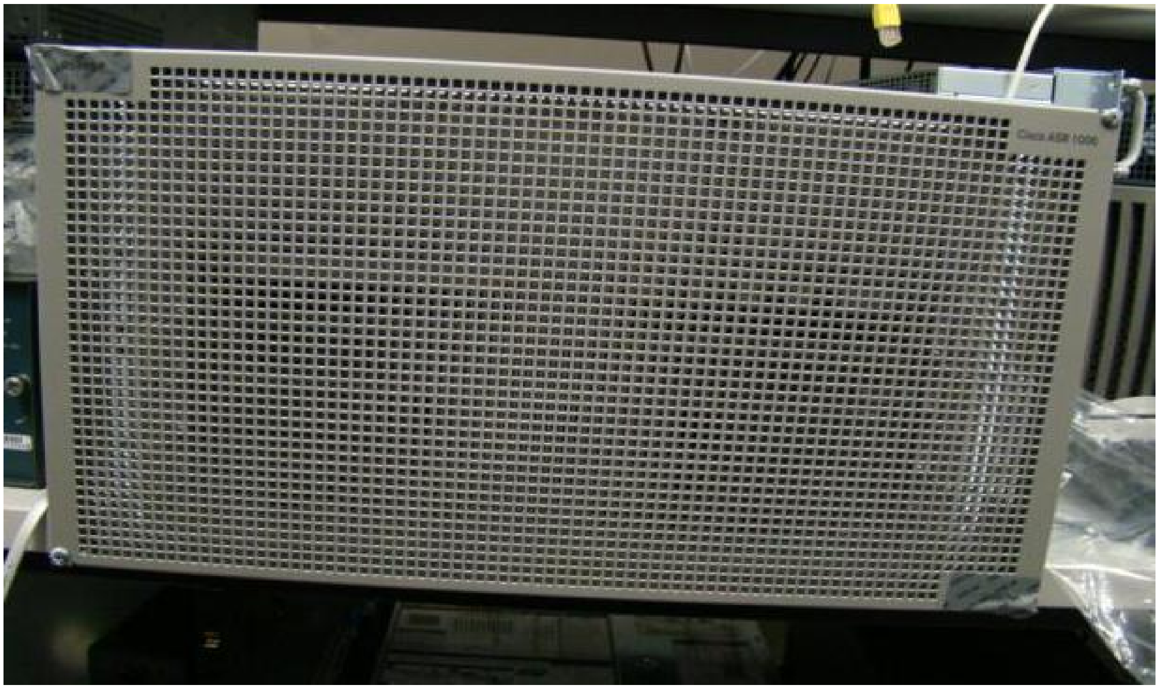

Figure 12: ASR 1006 with Opacity Shield Installed

Secure Operation

System Initialization and Configuration

Step1 - The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
config-register 0x0102
```

Step 2 - The Crypto Officer must create the "enable" password for the Crypto Officer role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

```
enable secret [PASSWORD]
```

Step 3 - The Crypto Officer must set up the operators of the module. The Crypto Officer enters the following syntax at the "#" prompt:

```
Username [USERNAME]

Password [PASSWORD]
```

Step 4 – For the created operators, the Crypto Officer must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
line con 0
password [PASSWORD]
login local
```

Step 5 - The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 8 characters long, including at least one letter and at least one number.

Step 6 - The Crypto Officer must apply tamper evidence labels as described earlier in this document.

Step 7 - Dual IOS mode is not allowed. ROMMON variable IOSXE_DUAL_IOS must be set to 0.

Step 8 - In service software upgrade (ISSU) is not allowed. The operator should not perform in service software upgrade of an ASR1000 FIPS validated firmware image

Step 9 - Use of the debug.conf file is not allowed. The operator should not create the bootflash:/debug.conf file and use it for setting environment variables values.

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.

IPSec Requirements and Cryptographic Algorithms

Step 1 - The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE).

Step 2 - Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

- ah-sha-hmac
- esp-sha-hmac
- esp-3des
- esp-aes
- esp-aes-192
- esp-aes-256

Step 3 - The following algorithms shall not be used:

- MD-5 for signing
- MD-5 HMAC
- DES

Protocols

Step 1 - SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP gets and sets. Since SNMP v2C uses community strings for authentication, only gets are allowed under SNMP v2C.

Step 2 - Secure DNS is not allowed in FIPS mode of operation and shall not be configured.

Remote Access

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

TLS communications with the module is not allowed in FIPS approved mode. TLS cannot be used in FIPS-mode of operation.

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 (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.

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.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

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:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://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.

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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://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:

http://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:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

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 a 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 nonemergencies.

- Nonemergencies — 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:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

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.

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:

http://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:

http://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.

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:

http://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 55USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

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.

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:

  http://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:

  http://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:

  http://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:

  http://www.cisco.com/ipj

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

  http://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:

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

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

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

Definition List

AES – Advanced Encryption Standard

ASR – Aggregation Services Routers

CMVP – Cryptographic Module Validation Program

CSEC – Communications Security Establishment Canada

CSP – Critical Security Parameter

FIPS – Federal Information Processing Standard

HMAC – Hash Message Authentication Code

HTTP – Hyper Text Transfer Protocol

KAT – Known Answer Test

LED – Light Emitting Diode

MAC – Message Authentication Code

NIST – National Institute of Standards and Technology

NVRAM – Non-Volatile Random Access Memory

RAM – Random Access Memory

RNG – Random Number Generator

RSA – Rivest Shamir and Adleman method for asymmetric encryption

SHA – Secure Hash Algorithm

TDES – Triple Data Encryption Standard