SonicWall Capture Security Appliance (CSa) 1000

Module HW Version 101-500644-50 Rev A/ FW Version 1.2

FIPS 140-2 Non-Proprietary Security Policy

Document Version : 1.9

Date : March 21, 2023

Table of Contents

List of Tables

List of Figures

Copyright Notice

1. Introduction

Product Overview

The SonicWall Capture Security Appliance™ (CSa) series bring Capture Advanced Threat Protection™ (ATP) and sandboxing malware analysis to on-premises deployment scenarios for customers with compliance and policy restrictions against sending files to cloud analysis, or who prefer for all of their data to remain inside their organization. The CSa series use a combination of reputation-based checks, static file analysis and SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) engine for dynamic analysis to deliver verdicts and reports on threat analysis.

The SonicWALL CSa 1000, the first in this series, also referred to as "the Module", is a multi-chip standalone cryptographic module enclosed in hard, commercial grade metal cases. The cryptographic boundary for the Module is the enclosure; however, the removable fans and the removable power supplies are outside the cryptographic boundary. The primary purpose of the Module is to provide secure remote access to internal resources via the Internet Protocol (IP). The Module provides network interfaces for data input and output. All traffic is encrypted using FIPS Approved Transport Layer Security (TLS) algorithms to protect from unauthorized users.

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates, using FIPS Allowed Integrity mechanisms.
New firmware versions within the scope of this validation must be validated to FIPS 140-2 through the CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

Module	HW P/N and Version	FW Version
CSa 1000	101-500644-50 Rev A	1.2

Table 1 - Cryptographic Module Configuration

The Module meets the below FIPS 140-2 security level requirements:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Security Level of Security Requirements

1.1 Hardware

The figure below depicts the physical form of the Module:

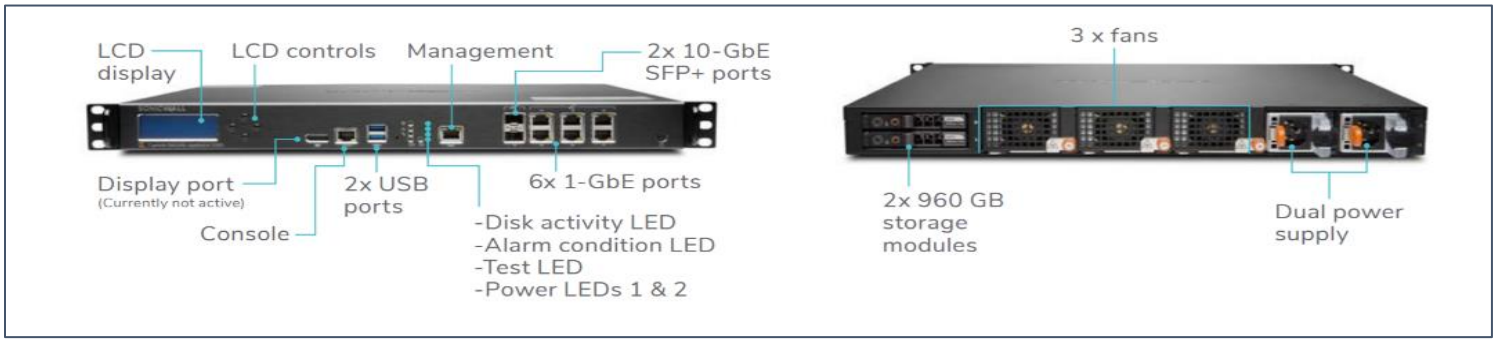

Figure 1 – Physical form of Module Configuration

Port	Description	Logical Interface Type
Console	Serial port (RS 232 115200n8)	Control in, Status out
Ethernet	Network traffic connections. (6 * 1G ports)	Control in, Data in, Data out, Status out
Display	LCD display for basic status information.	Status out
LEDs	Unit level: Disk Activity, Test, Alarm and Power (1 or 2 LEDs). Ethernet: Link and Activity LEDs.	Status out
Power	AC power, inclusive of switch, dual (redundant) power supplies.	Power
USB	Two (2) USB ports, used for disaster recovery mainly.	Read-only as a backup for firmware installation and update images

Table 3 - Ports and Interfaces

1.2 Modes of Operation

FIPS 140-2 Approved Mode

The Module can be configured to operate in FIPS Mode via its WebUI Management Console, under *System>Configuration->Settings->FIPS Mode*.

Attempts to enable FIPS Mode via the *Turn on FIPS Mode* toggle button and clicking the *Save* button next to it, cause the Module to:

- execute a FIPS Approved mode Compliance Checking tool which enforces the use of solely FIPS Approved mode ciphers
- prompt for a password change if the compliance requirements are not already met
- reboot to enforce module boot integrity checks and self-tests as well
- disable features such as remote debugging via SSH

Note that FIPS operations require a new user with admin role to be created and the default admin user to be disabled.
In addition, users are recommended to upload a CA signed RSA certificate, distinct for FIPS mode, and using keys of length 2048 bit or larger.

When successfully enabled, the *Turn on FIPS Mode* button on the said WebUI System Configuration page would turn 'green', indicating that the Module is in FIPS Mode.
Errors, if caused due to failed cryptographic health checks during reboot, would cause the Module to transition through the error state into Safe Mode, and messages indicating the same would be displayed on the LCD display.

Toggling the *Turn on FIPS Mode* toggle button will revert the module configuration back to non-Approved mode, removing all configured CSPs, and when FIPS mode is successfully disabled the *Turn on FIPS Mode* button on the said WebUI System Configuration page would no longer be 'green'. Approved mode may then be configured once again via the process noted above. In the non-Approved mode, the features cited in the bullets below are available for use. See Section 9, Security Rules and Guidance for additional Approved mode operation guidance.

Non-Approved Mode

In the Non-Approved mode, the features cited below are available for use:

- Remote SSH debugging
- Safe Mode Console for System Recovery

Note that the corresponding protocols for the above are used solely in the non-approved mode of operation, and in particular, none of the keys derived using the inherent key derivation functions can be used in the approved mode.

2. Cryptographic Functionality

The TLS Cipher suites below constitute the cryptographic protocols and primitives implemented and used by the Module in the Approved mode:

Cipher Suite String (IETF enumeration)	TLS	Key Exchange	Cipher	Auth
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	1.2	ECDHE	AES-128-CBC	HMAC-SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	1.2	ECDHE	AES-128-CBC	HMAC-SHA-256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1.2	ECDHE	AES-128-GCM	N/A (handled by AES GCM)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	1.2	ECDHE	AES-256-CBC	HMAC-SHA-1

Table 4 – TLS Cipher suites used in the Approved mode

The overall list of approved and allowed algorithms is enumerated below:

CAVP Cert #	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
A1906	AES	FIPS 197, SP 800-38A	ECB, CBC, GCM*	128, 256	Data Encryption/Decryption
A1906	RSA	FIPS 186-4		2048, 4096	Key Generation
			PKCS1 v1.5, PSS	2048, 3072, 4096 - SHA-256	Signature Generation
			PKCS1 v1.5, PSS	2048, 3072, 4096 - SHA-1, SHA-256	Signature Verification

A1906	ECDSA	FIPS 186-4		B-571, P-224	Ephemeral key generation for KAS-ECC-SSC
A1906	KAS ECC-SSC	SP 800-56Arev3	ECC	B-571, P-224	Key Agreement
A1906	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256	160, 256	Message Authentication
A1906	SHS	FIPS 180-4	SHA-1**, SHA-256		
A1906	CVL (TLS 1.2 KDF)	SP 800-135rev1	SHA-256		Key Derivation***
AES A1906 & HMAC A1906	KTS	SP 800-38F	CBC, GCM, HMAC SHA-1, HMAC SHA-256	128, 256	Key Transport****
A1906	DRBG	SP 800-90Ar1	ctr AES-256		Random number generation
Vendor Affirm	CKG*****	SP 800-133rev2			Key Generation
	ENT (P)	SP 800-90B		DRBG seeded with at least 128 bits of entropy.	Entropy Input to Approved DRBG

Table 5 – Algorithms used in the Approved mode

**As described in RFCs 5116, 5246, 5288, and 5289 provisions; the cipher suites utilizing AES GCM are from SP 800-52 Rev 1, Section 3.3.1. When nonce_explicit is exhausted the module will initiate a new TLS handshake to establish a new encryption key.*

*** SHA-1 is used only for HMAC SHA-1 and for legacy use verification of existing RSA signatures.*

****Note that no parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.*

*****Key establishment methodology provides 128 or 256 bits of encryption strength*

****** The generated seed is an unmodified output from a DRBG*

Algorithm	Use
Error detection code hash -- SHA-256 (non-compliant)	Boot-up Firmware Integrity Verification

Table 6 – Allowed Algorithms

2.1 Critical Security Parameters and Public Keys

Key/CSP name	Algorithm & Key Size(s)	Generated	Derived	Established & Minimum security strength	Input	Output	Cryptographically Associated Keys	Storage	Zeroization	Use
TLS Server Private key	RSA 2048-4096 bit	FIPS 186-4	N/A		KTS via Web GUI	N/A	TLS Server Public key	Plaintext, Persistent on Disk	On-demand, or on factory-reset.	Server identification for TLS
TLS Server Public key	RSA 2048-4096	FIPS 186-4	N/A	-	KTS via Web GUI	Plaintext during TLS handshake	TLS Server Private key	Plaintext, Persistent on Disk	N/A	Server identification for TLS
TLS Key Agreement Private Key	KAS-ECC-SSC B-571	FIPS 186-4	N/A	256 bits	N/A	N/A	TLS Key Agreement Public Key & TLS Master Secret	Ephemeral in RAM	Automatic when session ends, or on power off.	TLS Key Establishment
TLS Key Agreement Public Key	KAS-ECC-SSC B-571	FIPS 186-4	N/A	256 bits	N/A	Plaintext during TLS handshake	TLS Key Agreement Public Key & TLS Master Secret	Ephemeral in RAM	Automatic when session ends, or on power off.	TLS Key Establishment

TLS Key Agreement Client Public Key	KAS-ECC-SSC B-571	External	N/A	256 bits	Plaintext during TLS handshake	N/A	TLS Key Agreement Public Key & TLS Master Secret	Ephemeral in RAM	Automatic when session ends, or on power off.	TLS Key Establishment
TLS Pre-Master & Master Secret	N/A	SP 800-56Arev3 key agreement	-	-	N/A	N/A	TLS Session Encryption Key & TLS Session Authentication Key	Ephemeral in RAM	Automatic when session ends, or on power off.	TLS Key Establishment
TLS Session Encryption Key	AES CBC, GCM 128, 256	SP800-135 TLS 1.2 KDF	N/A	128 or 256 bits	N/A	N/A	TLS Master Secret	Ephemeral in RAM	Automatic when session ends, or on power off.	TLS Session Encryption &
TLS Session Authentication Key	HMAC 160, 256	SP800-135 TLS 1.2 KDF	N/A	-	N/A	N/A	TLS Master Secret	Ephemeral in RAM	Automatic when session ends, or on power off.	TLS Data Authentication & KTS
DRBG V and Key	CTR_DRBG	-	N/A	-	N/A	N/A	N/A	Ephemeral in RAM	On power off.	Random Number Generation and input to Key Generation
DRBG Seed	CTR_DRBG	From 90B ENT (P)	N/A	-	N/A	N/A	N/A	Ephemeral in RAM	On power off.	Random Number Generation and input to Key Generation

Authentication Passwords	-	-	-	-	Encrypted via TLS or plaintext via console	N/A	N/A	Hashed, Persistent on Disk	On-demand, or on factory-reset.	Password authentication
API Key	-	-	-	-	Encrypted via TLS	Encrypted via TLS in WebGUI	N/A	Persistent on Disk	On-demand, or on factory-reset.	Known secret authentication
Firmware Integrity Verification Key	RSA 4096 public key	External	N/A	N/A	Factory loaded	N/A	N/A	Plaintext, Persistent on Disk	N/A	Validation of firmware update

Table 7 – CSPs and Public Keys

3. Roles, Authentication and Services

3.1 Assumption of Roles

Role		**Authentication**
ID	**Description**	**Type**
(A) Admin [FIPS Crypto Officer role]	Root/Admin User – virtually omnipotent, with unrestricted access to configuration and administration of all system resources e.g. security, networking, dashboards, logs, reports, APIs, etc. The first/default admin created with this role is the singular super user and cannot be modified or deleted.	Identity-based (using *Local password verification*)
(RO)Read-Only System Admin	Non-Admin User – access restricted to read-only privileges, configured/assigned by the admin, typically all admin rights with view privileges granted and all edit privileges denied.	Identity-based (using *Local password verification*)
(SA) Security Analyst [FIPS User role]	Non-Admin User – access restricted per delegated rights, configured/assigned by the admin, typically a subset of the admin rights, and pertaining in particular to security/threat analysis.	Identity-based (using *Local password verification*)

Table 8 – Roles Description

3.2 Authentication Methods

- The *Local password verification* method requires an 8 character minimum password, max length 50, using characters in the printable character set. The maximum rate for local password authentication is conservatively estimated to be approximately one (1) attempt per microsecond. Hence the probability of false authentication is less than the required 1/1,000,000: 1/(95^8) = **1.5E-16** And the probability of false authentication in a one minute period is less than the required 1/100,000: (60*10^6)/(95^8) = **9.0E-9.**
- In addition, an *API key* can also be used to authenticate API connections and are an alternate way available for each role to interact with the Module. API keys are 256 bits in length. The maximum API requests per device are limited to 100 per minute, thus ensuring the probability of false authentication in a one minute period is again less than the required 1/100,000. And the probability of false authentication in a one minute period is less than the required 1/100,000: (100)/(2^256) = **8.6E-76.**

4. Authenticated/Secured Services

The Module constitutes the below authenticated services with RW (Read/Write), RO (Read Only) or N/A permissions enforced per Role, these are mapped to the CSP using activities of table 10:

Service [Activity]	Description	A	RO	SA
Management Portal [1]	WebGUI facilitated, over an encrypted session established via an HTTPS (OpenSSL TLS 1.2) interface.	RW	R	R
User Administration [2]	Management portal facilitated, creation and management of new/existing users and associated roles, configurable access rights, password (re)sets, etc.	RW	R	N/A
Network/System Configuration [3,5]	Management portal facilitated, configurable system resources e.g. networking, ability to whitelist/blacklist based on hash/domain, configure digital certificates, configure allowed devices, schedule backups, restores, cloud hash lookup, etc.	RW	R	N/A
Scheduled Reporting/Report History	Management portal facilitated, configurable system setting that enables the Module to schedule reports and view report archives over a given span.	RW	R	N/A
Alerting	Management portal facilitated, configurable resource usage alerts e.g. CPU, memory, disk usage and malicious file detection	RW	R	N/A
Logging	Management portal facilitated, menu based log views for time based result analysis and for typically viewing the status of recently submitted files.	RW	R	R
System Monitoring/Diagnostics	Management portal facilitated, read-only access to all the above resource dashboards, scanning history, logs and alerts.	R	R	N/A

REST API support for file submission and analysis [6]	REST API interface for file submission and result querying via scripting, samples available here: https://github.com/sonicwall/sonicwall-capture-api-python	R	R	R
Licensing and Software/firmware updates [4]	Management portal facilitated, licensing and there forth periodic updation of intelligence software and firmware updates.	RW	R	N/A

Remote System Maintenance/Support services (non-FIPS mode only)	• Safe Mode UI
	  ○ Authentication using a MSW maintenance key/password derived from a unique trio across each device - serial number, authcode and regcode.
	• Remote SSH (using OpenSSH based off OpenSSL) console access via DMZ and secure tunnel
	  ○ Authentication to the remote SSH server is done using a private key and host/root certificate generated using RSA(key length 4096)
		RW	N/A	N/A

Table 9 - Authenticated Services

Activity	Critical Security Parameter Access												
	TLS Server Private key	TLS Server Public key	TLS Key Agreement Private Key	TLS Key Agreement Public Key	TLS Key Agreement Client Public Key	TLS Master Secret	TLS Session Encryption Key	TLS Session Authentication Key	DRBG V and Key	DRBG Seed	Authentication Passwords	API Key	Firmware Integrity Verification Key
1 - Login via Web GUI	(X)	(O)	(G,X)	(G,O)	(I, X)	(G,X)	(D,X)	(D,X)	(X)		(I,X)		
2 - Password (re)set							(X)	(X)			(I)		
3 - Certificate Management	(I)	(I)					(X)	(X)					
4 - Firmware update							(X)	(X)					(X)
5 - API Key Creation/Management							(X)	(X)				(G, O)	
6 - REST API Operations	(X)	(O)	(G,X)	(G,O)	(I, X)	(G,X)	(D,X)	(D,X)	(X)			(I, X)	

Table 10 – CSP Access by Activity

[G = generate, D = derive, I = input, O = output, X = execute]

5. Self-Tests

Enabling FIPS mode causes the Module to reboot and initiate the following FIPS compliance Self Tests, else as indicated:

Power-up

- Firmware integrity test (Non-cryptographic error detection code based integrity test)
- DRBG health tests from SP 800-90A section 11.3
- RSA signature and verification known answer tests (KATs)
- KAS-ECC-SSC shared secret computation known answer tests (KATs)
- AES GCM encryption and decryption known answer tests (KATs)
- AES ECB encryption and decryption known answer tests (KATs)
- HMAC generation known answer test (KAT)
- SHA-1 hashing known answer test (KAT)
- SHA-256 hashing known answer test (KAT)
- SP 800-90B ENT (P) start-up health tests; run over 65536 consecutive samples

Conditional

- Firmware Integrity test (Signature Verification)
- RSA key generation pairwise consistency test
- SP 800-56Arev3 ECC Full Public-Key Validation
- SP 800-56Arev2 ECC Recipient Partial Public-Key Validation
- DRBG continuous RNG test
- SP 900-90B ENT (P) continuous health tests

6. Physical Security Policy

Each cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper-evident material and seals
- Protected vents

Some module components (e.g., hard drives) are field replaceable. Hard drives shall not be replaced in the FIPS module, an appliance with a failed hard drive must be returned for RMA. The removable fans of the Module and the removable power supplies of the same can be field replaced without issues because they are outside the cryptographic boundary, and aren't covered by tamper labels. The location and placement of tamper seals for each configuration are shown in the figures below. The tamper-evident seals shall remain installed for the Module to operate in a FIPS mode of operation. The two (2) seals required are shown below.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-evident Seals	Inspect tamper-evident seals monthly.	On need basis.

Table 11 – Physical Security Inspection Guidelines

If evidence of tampering is detected remove the module from service and return for RMA.

Figure 2 - CSa 1000 Tamper Seal #1 - Chassis Seam

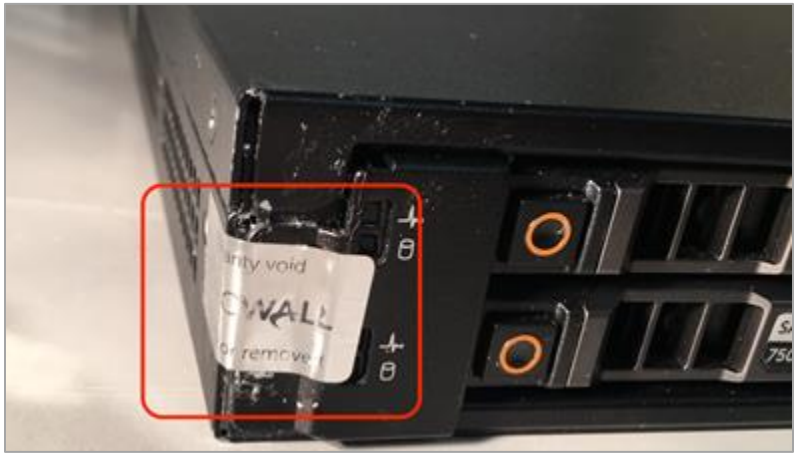

Figure 3 - CSa 1000 Tamper Seal #2 (over drive bay protected plate)

7. Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions as cited in the Introduction.

8. Mitigation of Other Attacks Policy

N/A

9. Security Rules and Guidance

- Approved TLS/https communication for all external communication/data transfers
- If power is lost, upon restoration the module will perform a new TLS handshake to establish a new AES GCM encryption key.
- All firmware updates encrypted and signed at source for integrity, and verified at destination using FIPS Approved and Allowed algorithms.

References

- Bring the Power of RTDMI Analysis On-Premises with CSa 1000
- NIST references
  - FIPS Validation Lists
  - FIPS 140-2 Approved Security Functions Annex A
  - FIPS 140-2 Approved Random Number Generators Annex C
  - FIPS 140-2 Approved Key Establishment Techniques
  - FIPS Implementation Guidance for Validation
  - SP 800-133r2 Key Recommendations for Key Generation
  - SP 800-135 Rev. 1 Recommendation for Existing Application-Specific Key Derivation Functions
  - SP800-90B Recommendation for the Entropy Sources Used for Random Bit Generation