FIPS 140-2 Level 2 Security Policy

For

Thunder Series TH3040S, TH5440S, TH5840S, and TH7440S-11

Document Version 1.4

This security policy describes the FIPS 140-2 compliance of the module

Table of Contents

1 Module Description

A10 Networks, Inc.'s Thunder Series are an outgrowth or evolution of Traffic Manager and Application Delivery Controller (ADC) systems and technologies. These A10 Thunder Series systems are advanced load balancers for ADC needs and sophisticated address translators for IPv6 migration, while being able to secure and control the traffic directed through the system for enterprise, ISP, and mobile networks. These systems include full proxies able to encrypt, decrypt, and inspect traffic for these networks.

The foundation of A10 Thunder systems is the A10 Networks' proprietary A10 Core Operating System (ACOS). ACOS is a software framework for maximized networks traffic processing performance that supports a common management and control plane architecture across a range of infrastructures; from data centers to cloud to multi-cloud.

These systems (subsequently referred to as "the module") support SSH, HTTPS, and console management interfaces. For the purposes of FIPS 140-2 the A10 Thunder Series is classified as multi-chip standalone module.

FIPS 140-2 conformance testing of the module was performed at Security Level 2. The following configurations were tested:

Table 1: Configurations tested by the lab

Module Name and Version	Firmware versions
Thunder Series TH3040S	4.1.4-GR1-P5
Thunder Series TH5440S	4.1.4-GR1-P5
Thunder Series TH5840S	4.1.4-GR1-P5
Thunder Series TH7440S-11	4.1.4-GR1-P5

Table 2: Module Security Level Statement

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

2 Cryptographic Boundary

The hardware and firmware components of the module are enclosed in a metal enclosure which is the cryptographic boundary of the module. The removable panels of the enclosure are protected by tamper-evident labels. The enclosure is opaque within the visible spectrum.

Images of the module is provided below:

Figure 1. Thunder Series TH3040S

Figure 2. Thunder Series TH5440S

Figure 3. Thunder Series TH5840S

Figure 4. Thunder Series TH7440S-11

3 Security Functions

The table below lists approved cryptographic algorithms employed by the module.

Table 3: Approved Cryptographic Functions

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1198	A10 Networks SSL FIPS Library	AES	FIPS 197, SP 800-38D	ECB, CBC, CTR, CFB1, CFB128, CFB8, OFB, GCM[1]	128, 192, 256	Data Encryption/ Decryption KTS[6]
C1194	A10 Networks Data Plane FIPS Software Library					
C1240	A10 Networks Data Plane FIPS Library					
C1241						
C1198	A10 Networks SSL FIPS Library	DRBG	SP 800-90A	HASH_Based DRBG HMAC_Based DRBG CTR_DRBG		Deterministic Random Bit Generation[2]
C1194	A10 Networks Data Plane FIPS Software Library					
C1240	A10 Networks Data Plane FIPS Library	CVL Partial EC-DH	SP 800-56A	ECC	P-256 P-384 P-521	Shared Secret Computation
C1241						
C1240	A10 Networks Data Plane FIPS Library	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication KTS[6]
C1241						
C1198	A10 Networks SSL FIPS Library					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1240 C1241	A10 Networks Data Plane FIPS Library	Triple-DES	SP 800-67	TCBC	168	Data Encryption/ Decryption[3]
C1240 C1241	A10 Networks Data Plane FIPS Library	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384 SHA-512		Message Digest
C1198	A10 Networks SSL FIPS Library					
C1198 C1240 C1241	A10 Networks SSL FIPS Library A10 Networks Data Plane FIPS Library	RSA	FIPS 186-4, FIPS 186-2[4]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 ANSIX9.31; PKCS1 v1.5	1024 (verification only), 1536 (verification only), 2048, 3072, 4096	Digital Signature Generation and Verification
C1198 C1240 C1241	A10 Networks SSL FIPS Library A10 Networks Data Plane FIPS Library	ECDSA	FIPS 186-4		P-256, P-384, P-521	Digital Signature Generation and Verification

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
C1240	A10 Networks Data Plane FIPS Library	CVL SNMP, TLS 1.0, 1.1 and 1.2, SSH	SP 800-135			Key Derivation[5]
C1241						
C1198	A10 Networks SSL FIPS Library					
CKG (vendor affirmed)	A10 Networks SSL FIPS Library A10 Networks Data Plane FIPS Software Library	Cryptographic Key Generation	SP 800-133			Key generation[2]

Note 1: 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.

Note 2: not all CAVS tested modes of the algorithms are used in this module.

[1] The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from SP 800-52, Section 3.3.1. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key. New AES-GCM keys are generated by the module if the module loses power.
[2]The module directly uses the output of the DRBG
[3] Operators are responsible for ensuring that the same Triple-DES key is not used to encrypt more than 2^{16} 64-bit data blocks
[4] Signature generation with key length of 4096 bit and signature verification..
[5] No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.
[6] KTS (AES Cert. #C1198; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (AES Cert. #C1198 and HMAC Cert. #C1198; key establishment methodology provides between 128 and 256 bits of encryption strength).

The module implements the following non-Approved cryptographic algorithms that are allowed in the Approved mode for protection of sensitive data:

Table 4: Non-FIPS Approved But Allowed Cryptographic Functions

Algorithm	Caveat	Use
RSA Key Wrapping using key ≥ 2048 bits key	Provides between 112 and 256 bits of encryption strength.	Used for key establishment in TLS handshake
DH using ≥ 2048 bits key	Provides between 112 and 256 bits of encryption strength.	Used for key establishment in SSH and TLS handshakes.
EC DH	Provides between 128 and 256 bits of encryption strength	Used for key establishment in TLS handshake.
NDRNG		Used to seed SP 800-90A DRBG.

The module also implements other cryptographic algorithms:

Table 5: Other Cryptographic Algorithms

Algorithm	Usage
MD5	Used by RADIUS*

* Note: RADIUS must not be used in the Approved Mode of Operation.

4 Ports and Interfaces

The module includes the following physical ports and logical interfaces.

Table 6: Ports and Interfaces

Port Name	Count	Interface(s)
Ethernet Port	TH3040S:14 1 GE Copper: 8 1 GE Fiber (SFP): 2 1/10 GE Fiber (SFP+): 4	Data Input, Data Output, Control Input, Status Output
	TH5440S/TH5840S: 30 1 GE Copper: 2 1/10 GE Fiber (SFP+): 24 40 GE Fiber (QSFP+): 4	
	TH7440S-11: 54 1 GE Copper: 2 1/10 GE Fiber (SFP+): 48 100 GE Fiber (CXP): 4	
Serial Console Port	1	Control Input, Status output, Data Output
USB Ports	1	Disabled

Port Name	Count	Interface(s)
Power Switch	1	Control Input
Power Port	TH3040S: 2	Power Input
	TH5440S/TH5840S: 2	
	TH7440S-11: 2	
LEDs[1]	3	Status Output

5 Roles, Services and Authentication

The module provides the following roles: a User role and Crypto Officer role. The Crypto Officers initialize and manage the module. Users employ the cryptographic services provided by the module.

The table below provides information on authentication mechanisms employed by each role.

Table 7.1: Authentication Mechanisms

Role	Authentication Mechanism
User	User authentication is certificate based with an RSA key of at least 2048 bits, which corresponds to 112-bit security or a probability of one successful attempt equal to 2^{-112} or ca. $2*10^{-34}$ probability of success. The modules support the maximum of 200,000 user connections per second, even assuming that authentication occurs instantly, this translates to 12,000,000 authentication attempts per minute, and the maximum probability of success is $2.4*10^{-27}$.
Crypto Officer	The minimum requirement for the password strength is eight characters. Any of the 89 characters can be used in any place. Thus, the probability of successfully guessing the password is 89^{-8} or ca. $3*10^{-16}$ per attempt. The modules support three interfaces for password authentication: console and remote (SSH and GUI/HTTPS). In the worst-case scenario console attack can be combined with the most efficient of the two remote interfaces. The probability of succeeding after 1 minute of attempts is computed as the number of guesses within one minute divided

[1] Also each Ethernet port uses 2 LEDs

Role	Authentication Mechanism
	by the total number of possible password combinations (still using the minimum password requirements as the reference). *Console access*: console bandwidth is 9600bps (1200Bps). Given an 8-bite password length, this translates to, 150 (=1200/8) guesses per second or *9,000* (=150*60) guesses per minute. *GUI/HTTPS*: the port supports 1Gbps (1,073,741,824bps). One password GUI transaction consumes at least 8,322 bytes (66,576 bits). Thus, the bandwidth supports 967,684 password guesses per minute (1,073,741,824*60/66,576). However, if we take the time of transactions into consideration, we find that each password transaction in testing took at least .29 seconds. Even assuming a 1000 times faster processing rate, the number of transactions per minute is limited to 206,896 attempts (60/.00029). Thus, GUI/HTTPS can handle at most *206,896* attempts per minute. *SSH*: one SSH session takes at least 6,614 bytes. SSH forces termination after three bad attempts at most in a single session. SSH protocol goes over 1Gbps connection. The maximum number of password attempts per minute is 3,652,735 (=1,073,741,824*60*3/(6,614*8)). *The overall number of attempts per minute* is at most 3,661,735 (3,652,735+9,000) using simultaneously console and SSH authentication. The overall 1-minute probability is at most $3{,}661{,}735*89^{-8}$ or ca. $9.3*10^{-10}$.

The module provides the following services to the operators:

Table 7.2: Roles and Services

Service	Role	Access to Cryptographic Keys and CSPs R- read; W – write or generate; E-execute
Installation of the Module	Crypto Officer	Password: W TLS server certificate: W SSH keys: E DRBG seed: E
Login	Crypto Officer	Password: E SSH Keys: E TLS Keys: E DRBG seed: E

Service	Role	Access to Cryptographic Keys and CSPs R- read; W – write or generate; E-execute
Device Management	Crypto Officer	Password: E SSH Keys: E TLS Keys: E DRBG seed: E
SSH	Crypto Officer	Password: E SSH Keys: E DRBG seed: E
HTTPS	Crypto Officer	Password: E TLS Keys: E DRBG seed: E
Run self-test	Crypto Officer	N/A
Show status	Crypto Officer	N/A
Reboot	Crypto Officer	N/A
Update firmware	Crypto Officer	Firmware load verification HMAC SHA-1 firmware load verification key: E
Zeroize	Crypto Officer	All keys: W
Establishment of secure TLS network connection	User	TLS keys: E TLS Certificate: E DRBG seed: E

6 Key Management

The following cryptographic keys and CSPs are supported by the module.

Table 8: Cryptographic Keys and CSPs

Name and type	Usage	Storage
TLS master secret	Used to derive TLS data encryption key and TLS HMAC key	Plaintext in RAM
TLS Triple-DES or AES encryption key	Used to encrypt data in TLS protocol	Plaintext in RAM
TLS HMAC key	Used to protect integrity of data in TLS protocol	Plaintext in RAM

Name and type	Usage	Storage
TLS server RSA or ECDSA certificate and private key	Used to encrypt the TLS master secret during the TLS handshake	Plaintext in RAM Plaintext in flash
TLS Diffie-Hellman keys	Used for key establishment during the handshake	Plaintext in RAM
TLS EC Diffie-Hellman keys	Used for key establishment during the handshake	Plaintext in RAM
SSH Diffie-Hellman keys	Used for key establishment during the handshake	Plaintext in RAM
Certification Authority RSA Certificate	Used to verify client certificate during the TLS handshake	Plaintext in RAM Plaintext in flash
SSH RSA keys	Used for authentication during the SSH handshake	Plaintext in RAM Plaintext in flash
SSH master secret	Used to derive SSH encryption key and SSH HMAC key	Plaintext in RAM
SSH AES encryption key	Used to encrypt SSH data	Plaintext in RAM
SSH HMAC keys	Used to protect integrity of SSH data	Plaintext in RAM
CTR_DRBG CSPs: entropy input, V and Key Hash_DRBG CSPs: entropy input, V and C HMAC_DRBG CSPs: entropy input, V and Key	Used during generation of random numbers	Plaintext in RAM
Firmware load verification HMAC SHA-1 Key	Used to verify firmware components	Plaintext in RAM Plaintext in flash
Passwords	Used to authenticate users	Plaintext in RAM Plaintext in flash
SNMP Secret	Used to authenticate Crypto Officers accessing SNMP management interface	Plaintext in RAM Plaintext in flash

7 Self Tests

The module runs a set of self-tests on power-up. If one of the self-tests fails, the module transitions into an error state where all data output and cryptographic operations are disabled.

The module runs power-up self-tests for the following algorithms:

Table 9.1: Power-up Self-Tests

Algorithm	Test
AES	Known Answer Test using GCM, ECB and CBC modes (encrypt/decrypt)
TDES	Known Answer Test using ECB mode (encrypt/decrypt)
SHS	Known Answer Test as a part of the HMAC KAT. Also SHA1 and SHA256 are tested separately.
HMAC	Known Answer Test using SHA1, SHA224, SHA256, SHA384 and SHA512 to also cover SHA POST
SP800-90A DRBG	Known Answer Test: CTR_DRBG: AES HASH_DRBG: SHA256 HMAC_DRBG: SHA256
RSA	Known Answer Test using 2048 bit key, SHA-256
ECDSA	Pairwise Consistency Test (sign/verify) using P-224, K-233 and SHA512
Firmware integrity	MD5 of the firmware image

During the module operation the following conditional self-tests are performed:

Table 9.1: Conditional Self-Tests

Condition	Test
Random Number Generation /DRBG	Continuous RNG Test
Random Number Generation /NDRNG	Continuous RNG Test
Firmware Load	Firmware Load Test using HMAC SHA1

8 Physical Security

The module consists of production-grade components enclosed in a metal enclosure. The enclosure is opaque within the visible spectrum. Sealed containers are used during the shipping of the module. The integrity of the firmware is protected.

The module is protected by tamper evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements. The tamper evident labels are applied at the factory to provide evidence of tampering if a panel is removed.

The Crypto Officer must note the locations of the tamper evidence labels upon receipt of the module. The Crypto Officer must check the integrity of the tamper evident labels periodically thereafter. Upon discovery of tampering the Crypto Officer must immediately disable the module and return the module to the manufacturer.

9 Secure Operation

9.1 Approved Mode of Operation

The module is intended to always operate in the Approved Mode of Operation. Module documentation provides detailed setup procedures and guidance for the users and administrators.

Crypto Officer must execute the following command to enable the approved mode of operation

- system fips enable

Crypto Officer must change its password during the installation.

Module users and administrators shall keep all authentication data confidential and shall not allow unauthorized access to the module.

10 References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001

Reference	Specification
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions