FIPS 140-2 Level 2 Security Policy

For

Thunder Series Application Delivery Controller TH3030S, TH4440S, TH6630S, and TH7440S

Document Version 1.4

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

Table of Contents

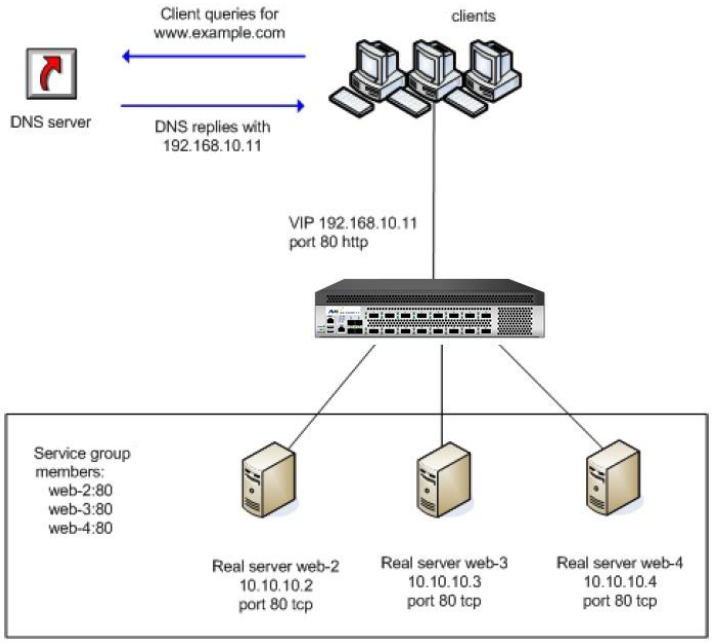
1 Module Description

A10 Networks, Inc.'s Thunder Series is a traffic manager designed to help enterprises and ISPs with application availability through a Web Application Delivery Platform. These Thunder Series appliances are integrated 64-bit models.

Commonly, clients and servers use Hypertext Transfer Protocol Secure (HTTPS) to secure traffic. Hardware acceleration is used for TLS encryption of data. For example, a client that is using a shopping application on a server will encrypt data before sending it to the server. The server will decrypt the client's data, and then send an encrypted reply to the client. The client will decrypt the server reply, and so on.

TLS works using certificates and keys. Typically, a client will begin a secure session by sending an HTTPS request to a virtual endpoint. The request begins an HTTPS handshake. The module will respond with a digital certificate. From the client's perspective, this certificate comes from the server. Once the HTTPS handshake is complete, the client begins an encrypted client-server session with the module.

Server farms can easily be grown in response to changing traffic flow, while protecting the servers behind a common virtual endpoint. From the perspective of a client who accesses services, requests go to and arrive from a single endpoint. The client is unaware that the server is in fact multiple servers managed by the module. There is no need to wait for DNS entries to propagate for new servers. A new server can be added to the configuration for the virtual server, and the new real server should then become accessible immediately.



The module supports SSH, HTTPS, and console management interfaces.

For the purposes of FIPS 140-2 the Thunder Series Application Delivery Controller 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:

Module Name and Version	Firmware versions
Thunder Series Application Delivery Controller TH3030S	4.1.1-P3
Thunder Series Application Delivery Controller TH4440S	4.1.1-P3
Thunder Series Application Delivery Controller TH6630S	4.1.1-P3
Thunder Series Application Delivery Controller TH7440S	4.1.1-P3

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.

An image of the module is provided below:

Figure 12. Thunder Series Application Delivery Controller TH3030S

Figure 13. Thunder Series Application Delivery Controller TH4440S

Figure 14. Thunder Series Application Delivery Controller TH6630S

Figure 15. Thunder Series Application Delivery Controller TH7440S

3 Ports and Interfaces

The module includes the following physical ports and logical interfaces.

Port Name	Count	Interface(s)
Ethernet Port	TH3030S:14 1 GE Copper: 8 1 GE Fiber (SFP): 2 1/10 GE Fiber (SFP+): 4	Data Input, Data Output, Control Input, Status Output
	TH4440S:30 1 GE Copper: 2 1/10 GE Fiber (SFP+): 24 40 GE Fiber (QSFP+): 4	
	TH6630S:18 1 GE Copper: 2 1/10 GE Fiber (SFP+): 12 100 GE Fiber (CXP): 4	
	TH7440S:54 1 GE Copper: 2 1/10 GE Fiber (SFP+): 48 40 GE Fiber (QSFP+): 4	
Serial Console Port	1	Control Input, Status output, Data Output
USB Ports	1	Disabled
Power Switch	1	Control Input
Power Port	TH3030S:2	Power Input
	TH4440S:2	
	TH6630S:4	
	TH7440S:2	
LEDs[1]	3	Status Output

[1] Also each Ethernet port uses 2 LEDs

4 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.

Role	Authentication Mechanism
User	Client Certificates are used for user authentication. The module uses client certificates with at least 2048 bit RSA key, which corresponds to 112 bits of security, therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur due to the authentication process performance limitation.
Crypto Officer	Passwords are used for connections via Console, SSH, and Web User Interface. RSA keys can be used for connections via SSH. The module uses passwords of at least 8 characters, or at least 2048 bit RSA key, therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. For multiple attempts to use the authentication mechanism during a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur due to the authentication process performance limitation.

The module provides the following services to the operators:

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
Device Management	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
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

5 Security Functions

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

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
4462	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 (key establishment methodology provides between 128 and 256 bits
4752	A10 Networks Data Plane FIPS Software Library					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
2329 5052 5053	A10 Networks Data Plane FIPS Library					of encryption strength)
1447	A10 Networks SSL FIPS Library	DRBG	SP 800-90A	HASH_Based DRBG HMAC_Based DRBG CTR_DRBG		Deterministic Random Bit Generation[2]
1633	A10 Networks Data Plane FIPS Software Library					
1610 1611	A10 Networks Data Plane FIPS Library	CVL Partial EC-DH	SP 800-56A	ECC	P-256 P-384 P-521	Shared Secret Computation
1444 1654	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
2961	A10 Networks SSL FIPS Library					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
1463	A10 Networks Data Plane FIPS Library	Triple-DES	SP 800-67	TECB, TCBC	168	Data Encryption/ Decryption[3] KTS (key establishment methodology provides 112 bits of encryption strength)
2396	A10 Networks SSL FIPS Library					
2013	A10 Networks Data Plane FIPS Library	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384 SHA-512		Message Digest
2236						
3674	A10 Networks SSL FIPS Library					
2438	A10 Networks SSL FIPS Library	RSA	FIPS 186-4, FIPS186-2	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
2738	A10 Networks Data Plane FIPS Library					
2739						
1087	A10 Networks SSL FIPS Library	ECDSA	FIPS 186-4		P-256, P-384, P-521	Digital Signature Generation and Verification
1187	A10 Networks Data Plane					

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
	FIPS Software Library					
143	A10 Networks Data Plane TLS KDF FIPS Library	CVL SNMP, TLS 1.0, 1.1 and 1.2, SSH	SP 800-135			Key Derivation
144						
1170	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]

[1]The module's AES-GCM implementation complies with IG A.5 scenario 1, RFC 5288 and SP 800-52. AES-GCM is only used in TLS version 1.2. New AES-GCM keys are generated by the module if the module loses power. The module uses a monotonically increasing counter to ensure uniqueness of the IV. The implementation of the module ensures by comparing the value of the counter to the maximum value that when the counter exhausts all possible values, a new key is established.

[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

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

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

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:

Algorithm	Usage
MD5	Used by RADIUS

6 Key Management

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

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
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

Name and type	Usage	Storage
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 Triple-DES or AES encryption keys	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:

Algorithm	Test
AES	Known Answer Test using 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
ECC CDH	Shared secret computation
Firmware integrity	HMAC-SHA-1 of the firmware image

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

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.

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 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
[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

Reference	Specification
[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