FIPS 140-2 Level 2 Security Policy

For

AX Series Advanced Traffic Manager AX2500, AX2600-GCF, AX3000-GCF, AX5100 and AX5200

Document Version 0.3

Table of Contents

1 Module Description

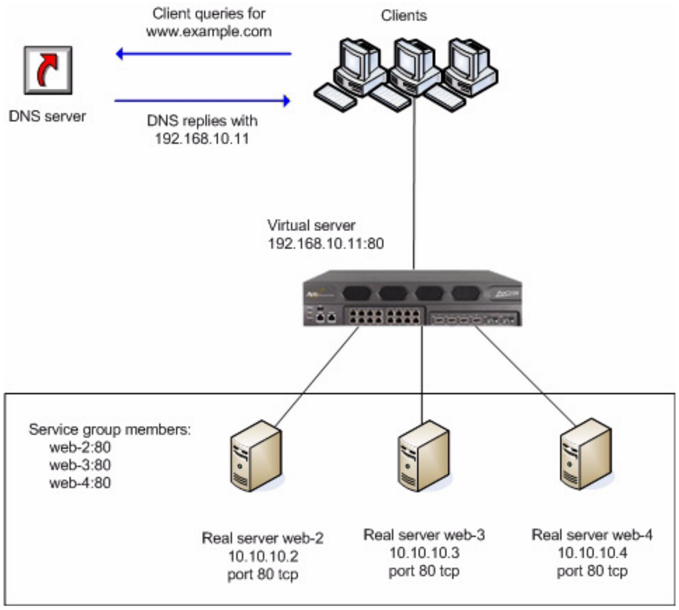
A10 Networks' AX Series is a traffic manager designed to help enterprises and ISPs with application availability through a Web Application Delivery Platform. These AX Series appliances are integrated 64-bit models.

Commonly, clients and servers use Transport Layer Security (TLS) 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. The AX devices support TLS version 1.0.

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 TLS handshake. The AX device will respond with a digital certificate. From the client’s perspective, this certificate comes from the server. Once the TLS handshake is complete, the client begins an encrypted client-server session with the AX device.

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 an AX device. There is no need to wait for DNS entries to propagate for new servers. A new server can be added to the AX configuration for the virtual server, and the new real server should then become accessible immediately.

The TOE supports SSH and HTTPS management interfaces.


Client queries for www.example.com
Clients
DNS server
DNS replies with 192.168.10.11
Virtual server 192.168.10.11:80
Service group members:
web-2:80
web-3:80
web-4:80
Real server web-2 10.10.10.2 port 80 tcp
Real server web-3 10.10.10.3 port 80 tcp
Real server web-4 10.10.10.4 port 80 tcp

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

For the purposes of FIPS 140-2 the AX Series Advanced Traffic Manager 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**
AX Series Advanced Traffic Manager AX2500	2.6.1-P2 build 28
AX Series Advanced Traffic Manager AX2600-GCF	2.6.1-P2 build 28
AX Series Advanced Traffic Manager AX3000-GCF	2.6.1-P2 build 28
AX Series Advanced Traffic Manager AX5100	2.6.1-P2 build 28
AX Series Advanced Traffic Manager AX5200	2.6.1-P2 build 28

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 1. AX Series Advanced Traffic Manager AX2500

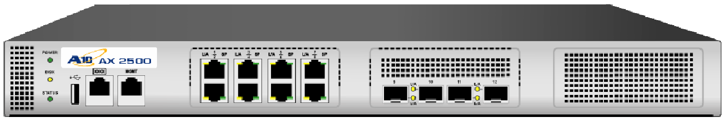


Figure 2. AX Series Advanced Traffic Manager AX2600-GCF

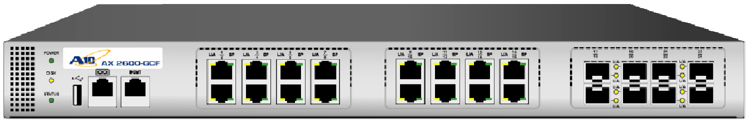


Figure 3. AX Series Advanced Traffic Manager AX3000-GCF

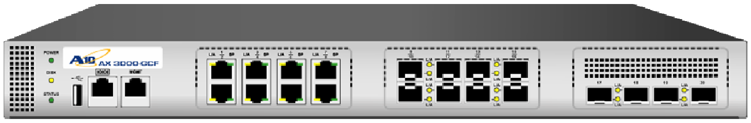


Figure 4. AX Series Advanced Traffic Manager AX5100

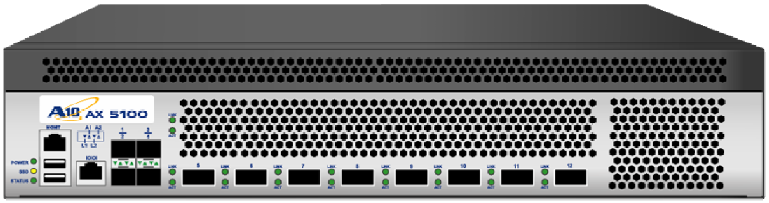
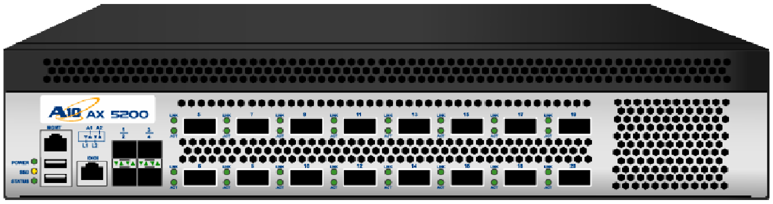


Figure 5. AX Series Advanced Traffic Manager AX5200



3 Ports and Interfaces

The module includes the following physical ports and logical interfaces.

Port Name	Count	Interface(s)
Ethernet Port	AX2500: 13	Data Input, Data Output, Control Input, Status Output
	AX2600-GCF: 25	
	AX3000-GCF: 21	
	AX5100: 13	
	AX5200: 21	
Serial Console Port	1	Control Input, Status output, Data Output

Port Name	Count	Interface(s)
USB Ports	AX2500: 1	Disabled
	AX2600-GCF: 1	
	AX3000-GCF: 1	
	AX5100: 2	
	AX5200: 2	
Power Switch	1	Control Input
Alarm off button	1	Control Input
Power Port	2	Power Input

LEDs correspond to the Status output interface.

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 1024 bit RSA key, which corresponds to 80 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. The module uses passwords of at least 8 characters, 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 ANSI X9.31 seed and key: E
Login	Crypto Officer	Password: E SSH Keys: E TLS Keys: E ANSI X9.31 seed and key: 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 network connection	User	TLS keys: E TLS Certificate: E ANSI X9.31 seed and key: E

5 Security Functions

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

Algorithm	Certificate Number
SHS	1480, 1519, 1524, 1525
HMAC	985, 1011, 1016, 1017
Triple DES	1092, 1124, 1128, 1129
AES	1693
AES[1]	1739, 1740
RSA Sign/verify	829, 858, 862, 863
ANSI X9.31 PRNG	900, 933

[1] The maximum allowed key length is 128 bits. Larger AES key sizes shall not be used.

The table below lists non-Approved cryptographic algorithms employed by the module

Algorithm	Usage
MD5	Used by RADIUS Used during TLS handshake Used by the SNMP[2] protocol
HMAC-MD5	Used by the SNMP[2] protocol
Diffie-Hellman	Used for key establishment in SSH version 2 handshake. Provides between 80 and 112 bits of encryption strength.
RSA encrypt/decrypt	Used for key establishment in TLS handshake. Provides 80 bits of encryption strength.

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 certificate and private key	Used to encrypt the TLS master secret during the TLS handshake	Plaintext in RAM Plaintext in flash
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 EAP-TLS handshake	Plaintext in RAM Plaintext in flash
SSH RSA key pair	Used to authenticate the module to the SSH client 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

[2] Non-sensitive data only .

Name and type	Usage	Storage
ANSI X9.31 PRNG1 Seed and Seed Key	Used to initialize the PRNG to a random state	Plaintext in RAM
ANSI X9.31 PRNG2 Seed and Seed Key	Used to initialize the PRNG to a random state	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
TDES	Known Answer Test
SHS	Known Answer Test
HMAC	Known Answer Test
ANSI X9.31 PRNG	Known Answer Test
RSA	Known Answer Test
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	Continuous PRNG Test
Firmware Load	Firmware Load Test using HMAC SHA1
RSA Key Pair generation	Pairwise Consistency Check (Sign/Verify, Encrypt/Decrypt)

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 check the integrity of the tamper evident labels upon receipt of the module and 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.

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

Module users shall not use AES key sizes larger than 128 bits.