Brocade® 7840 Extension Switch

FIPS 140-2
Non-Proprietary
Security Policy

Document Version 1.0

Brocade Communications Systems, Inc.

February 15, 2018

Document History

Version	Publication Date	Summary of Changes
1.0	February 15, 2018	Initial Release

Table of Contents

Table of Tables

Table of Figures

1 Module Overview

The Brocade 7840 is a multiple-chip standalone cryptographic module, as defined by FIPS 140-2. The cryptographic boundary of the 7840 Extension Switch is the outer perimeter of the metal chassis including the removable cover. The module is a Fibre Channel and/or Gigabit Ethernet routing switch that provides secure network services and network management.

A validated module configuration is comprised of Fabric OS v8.1.0 (P/N: 63-1001736-01) installed on, a switch or backbone and a set of installed blades. The below platforms may be used in a validated module configuration:

Table 1 – Firmware Version

Firmware
Fabric OS v8.1.0

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

1.1 Brocade 7840 Switch

Figures below, illustrate the Brocade 7840 cryptographic module.

Figure 1 - Brocade 7840– Front and Top Sides

Figure 2 - Brocade 7840– Front, Left and Top sides

Figure 3 - Brocade 7840– Front, Right and Top sides

Figure 4 - Brocade 7840– Back and Top sides (showing XBR-FAN-80-R and XBR-1100WPSAC-R)

Table 2 – Brocade 7840 Switch

Switch	SKU	Part Number	Brief Description
7840	BR-7840-0002	80-1008000-01	7840 baseline 16G configuration with port side air flow - Provides 42 Ports - 24 16G Long Wave SFPS - 0 1/10/40GBE SFP - Dual hot-swappable redundant power supplies
	XBR-FAN-80-R	80-1004580-02	FRU FAN, 80MM, PORT SIDE EXHAUST AF
	XBR-1100WPSAC-R	80-1007263-01	FRU,1100W PSAC, PORTSIDE EXHAUST AF

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 3 – Module Security Level Specification

Security Requirements Section	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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

3 Modes of Operation

Module State: Non-compliant FIPS state:

An uninitialized module provides an operational environment which is not a FIPS compliant state (it is a non-compliant FIPS state). A Crypto-officer must follow the instructions in section 3.1.2 to configure the module in order to create a FIPS compliant state.

Module State: Compliant FIPS state:

A module must be configured to provide a compliant FIPS state. Section 3.1.2 provides the required detailed instructions on how to configure the module into a compliant FIPS state.

The Crypto-Officer must use the admin user-account to login to the module and configure the module into FIPS compliant state (see section 3.1.2). These configuration steps, also, configure the module to use FIPS Approved cryptographic algorithms (see Table 4, Table 5, Table 6 and Table 7).

Term Crypto-Officer in this document refers to the Crypto-Officer who has logged in using the admin user-account.

Mode of Operation: FIPS Approved mode

After module is configured to enter FIPS compliant state it must operate adhering to use only the FIPS approved cryptographic algorithms (see Table 4, Table 5, Table 6 and Table 7) and the FIPS approved services.

NOTE: Operating the module with Non-Approved FIPS cryptographic algorithms (see Table 8) or FIPS Non-Approved services (see Table 9) is in explicit violation of this Security Policy and implicitly toggles the module out of FIPS mode.

Mode of Operation: FIPS Non-Approved mode

NOTE: A module configured to operate in FIPS compliant state can be re-configured by the Crypto-Officer to use FIPS Non-Approved cryptographic algorithms (see Table 8) and/or FIPS Non-Approved services (see Table 9). Operating the module with Non-Approved FIPS cryptographic algorithms or FIPS Non-Approved services is in explicit violation of this Security Policy and implicitly toggles the module out of FIPS mode.

3.1 FIPS Compliant Approved Mode of Operation

This section provides information on how to configure the module to create a FIPS compliant state. It also describes the requirements for providing a FIPS Approved operational environment.

This section provides the following information:

A. Reference to approved algorithms and their CAVP granted certificates (section 3.1.1),

B. The initialization steps (section 3.1.2) to configure the module to operate in Approved mode of operation (FIPS enabled), and

C. Steps and procedures (section 3.1.2.3) on how to examine that the module is operating in Approved mode of operation (FIPS enabled).

Note that special attention must be paid to section, 3.2, Non-Approved mode of operation (post following steps to enable FIPS mode), to understand additional requirements for operating in Approved mode of operation.

Next page →

3.1.1 FIPS Approved Cryptographic Algorithms

3.1.1.1 Brocade 7840 – Control Plane Algorithms

Table 4 – Control Plane Algorithm Certificates

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4242	AES	FIPS 197, SP 800-38A	CBC, ECB, CTR	128, 192, and 256	Data Encryption/Decryption ([1])
4242	AES	FIPS 197, SP 800-38A	CFB	128	Data Encryption/Decryption
988	CVL, SSHv2 TLS 1.0/1.1 TLS 1.2 SNMPv3	SP 800-135rev1			Key Derivation
989	CVL, Partial ECDH	SP 800-56Arev2	ECC CDH Primitive	P-256, P-384	Shared Secret Computation ([2])
987	CVL, Partial ECDH	SP 800-56Arev2	ECC	P-256, P-384	Shared Secret Computation ([3])
987	CVL, Partial DH	SP 800-56Arev2	FFC	(2048, 256)	Shared Secret Computation
1321	DRBG	SP 800-90Arev1	CTR_DRBG	256	Deterministic Random Bit Generation
1132	DSA	FIPS 186-4		2048	Key Pair Generation, PQG(Gen) and PQG(Ver) ([4])
982	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P-256	Digital Signature Generation and Verification ([5])
2780	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication ([6])
2288	RSA	FIPS 186-4	SHA-256	2048	Digital Signature Generation and Verification ([7])
3479	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest

[1] AES (Cert. #4242) supports the ECB mode only as a pre-requisite for other implementations in the module. AES ECB mode is not invoked independently by any approved service in the FIPS Approved mode.
[2] CVL (Cert. #989); P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[3] CVL (Cert. #987); P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[4] DSA (Cert. #1132) is only used as a prerequisite for CVL (Cert. #987)
[5] ECDSA (Cert #982) P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[6] HMAC (Cert. 2780): HMAC-SHA-224 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[7] RSA (Cert. #2288): The only mode utilized by the module is RSA 2048 with SHA-256. All other modes and key sizes are latent functionality.

3.1.1.2 Brocade 7840 – Data Plane Algorithms

Table 5 – Data Plane Algorithm Certificates

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4116	AES	FIPS 197, SP 800-38A	CBC	256	Data Encryption/Decryption
4116	AES	FIPS 197, SP 800-38D	GCM	256	Data Encryption/Decryption
924	CVL, IKEv2	SP 800-135rev1			Key Derivation
923	CVL, Partial ECDH	SP 800-56Arev2	ECC	P-384	Shared Secret Computation
1239	DRBG	SP 800-90Arev1	CTR_DRBG	256	Deterministic Random Bit Generation
934	ECDSA	FIPS 186-4	PKG	P-384	Key Pair Generation
2688	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication ([8])
3386	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest

3.1.1.3 Brocade 7840 – Blitzer FPGA Algorithms

Table 6 – Blitzer FPGA Algorithm Certificates

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4145	AES	FIPS 197, SP 800-38A	ECB	256	Data Encryption
4145	AES	FIPS 197, SP 800-38D	GCM	256	Data Encryption/Decryption

For additional information on transitions associated with the use of cryptography refer to NIST Special Publication SP800-131Ar1. This document can be located on the CMVP website at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

FIPS Approved mode enables:

- HTTPS TLS v1.0/1.1 and TLS v1.2
- SSHv2
- IKEv2
- SNMPv3

[8] HMAC (Cert. 2688): HMAC-SHA-224 is latent functionality. The module does not support this mode in the FIPS Approved mode.

3.1.1.4 Non-Approved Algorithms Allowed in FIPS Mode

Following table lists all non-Approved algorithms and protocols that are allowed within the Approved mode of operation.

Table 7 – Non-Approved Algorithms Allowed in FIPS Mode

Algorithm	Caveat	Use
Diffie-Hellman (CVL Cert. #987 with CVL Cert. #988)	Key agreement; key establishment methodology provides 112 bits of encryption strength.	Key establishment within SSHv2 protocol
EC Diffie-Hellman (CVL Cert. #987 with CVL Cert. #988) Supported curves: P-256, P-384([9])	Key agreement; key establishment methodology provides 128 bits of encryption strength.	Key establishment within SSHv2 protocol
EC Diffie-Hellman (CVL Cert. #989 with CVL Cert. #988) Supported curves: P-256, P-384([9])	Key agreement; key establishment methodology provides 128 bits of encryption strength.	Key establishment within SSHv2 protocol
EC Diffie-Hellman (CVL Cert. #923 with CVL Cert. #924) Supported curve: P-384	Key agreement; key establishment methodology provides 192 bits of encryption strength.	Key establishment within IKEv2 protocol
HMAC-MD5	Used in RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)	RADIUS authentication
HMAC-SHA-1-96([10])	Used in SNMPv3 (HMAC-SHA-1-96 is not exposed to the operator)	SNMPv3
HMAC-SHA-384-192([11])	Used in IKEv2 for message integrity (HMAC-SHA-384-192 is not exposed to the operator)	IKEv2
MD5	Used in storage of passwords (MD5 is not exposed to the operator)	Storage of passwords
MD5	Used in TLS v1.0 KDF	TLS v1.0KDF
NDRNG – entropy data		Seeding for the Approved DRBG The minimum number of bits of entropy generated by the module for use in key generation is 112-bits.
RSA Key Wrapping	Key wrapping; key establishment methodology provides 112 bits of encryption strength.	Key establishment within TLS v1.0/1.1 and TLS v1.2

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

[9] P-384 is latent functionality. The module does not support this mode in the FIPS Approved mode.
[10] See HMAC Certificate #2780 in Table 4.
[11] See HMAC Certificate #2688 in Table 5.

3.1.2 Creating FIPS Compliant State and Entering FIPS Approved mode

Physical Security:

Follow instructions provided in section 9 (Physical Security Policy) to apply the required tampered seals. Validate that the tamper evident seals are applied and the module is untampered.

Module Configuration:

The cryptographic module IS NOT operating in the Approved mode of operation until the required configurations steps in this section are followed to initialize the module. When the module is yet to be initialized and configured to enter the FIPS compliant State, the module is known to be in a non-compliant FIPS state.

In such non-compliant FIPS state the module provides access to three different user accounts: root user-account, admin user-account, and user user-account. The Crypto-Officer must use the admin user-account to login to the module and configure the module as per instructions provided below to enter the Approved mode of operation (to enable FIPS mode.)

After this configuration is complete, root user-account is permanently disabled and only admin and user user-accounts are left available to login to the module.

Term Crypto-Officer in this document refers to the Crypto-Officer who has logged in using the admin user-account.

3.1.2.1 Notes and Guidance to Crypto-Officer

A. Guidance for module being upgraded to FOS 8.1.0:
    1. Only a module running FOS 7.4.0 can be upgraded to FOS 8.1.0.

B. Following features and capabilities are not supported FIPS mode. Instructions listed below must be followed by the Crypto-Officer when configuring a device to operate in FIPS mode:

    1. Do not enable FC port authentication. This level of authentication is considered as plain text and not supported in Approved mode of operation (FIPS mode). The security it provides does not meet FIPS security requirements. This includes use of Common-Certs which are not supported in FIPS Mode.

    2. The client authentication feature for TLS clients is not supported in Approved mode of operation. The Crypto-Officer must not configure client authentications for TLS connections as it is not supported in Approved mode of operation (FIPS mode).

    3. Do not configure access-time feature for any users in the FIPS mode.
    The Crypto-Officer must not configure access-time feature. Access-time feature is not supported in Approved mode of operation.

Next page →

3.1.2.2 Cryptographic module initialization

The following is the procedure to enable FIPS mode on CP and DP. Unless explicitly mentioned all commands should be executed on the Active CP. Ensure that the pre-requisites mentioned in Section 3.1.2.1 are reviewed and adhered to.

Steps:

1. Login to the switch as an authorized user

2. Verify the firmware version using *firmwareshow* command
   a. *firmwareshow*

3. User Defined roles:
User Defined role is not supported in FIPS mode. The Crypto-Officer must not use this feature. The Crypto-Officer must delete any User Defined roles which may exist prior to placing the module in FIPS mode.
   a. Examine existing User Defined roles by issuing the following CLI command:

      roleconfig --show -all

      If no User Defined roles is present then the above CLI command will report the following message:

      "There are no user-defined roles on the switch."

   b. If User Defined roles have been configured, then '*roleconfig --show -all*' command will display a list of defined roles. In this case, use the following CLI command to delete all existing User Defined roles.

      roleconfig --delete <role_name>

4. Execute *extncfg* command to configure DP *in FCIP mode.*
   a. *extncfg --appmode fcip*

      NOTE: Brocade 7840 DP shall not be configured for Hybrid mode or the cryptographic module would not be deemed as FIPS 140-2 validated.

5. Zeroize the switch
   a. Execute zeroization to zeroize all the CSP on the Switch and DP
      1. fipscfg --zeroize –dp

   b. Reboot the switch
      1. *reboot*

6. Enable the self-tests mode using the command '*fipscfg --enable selftests*'
   1. fipscfg --enable selftests –dp

NOTE: Once this step occurs the cryptographic module will perform power-up self-tests during all subsequent power-ups regardless of whether the cryptographic module is in FIPS mode or non-FIPS mode. There is no service, method, or mechanism to disable such power-up self-tests thereafter.

7. Disable the non-secure ports using *ipfilter* CLI. Follow the procedure outlined below for disabling a given port. Use the same approach to disable port 80, 23 and 897 for both Ipv4 and Ipv6 rules

   For e.g.: For Ipv4
   ipfilter --clone fips_ipv4 –from default_ipv4
   ipfilter --delrule fips_ipv4 –rule 2
   ipfilter --addrule fips_ipv4 –rule 2 –sip any –dp 23 –proto tcp –act deny –type INPUT –dip any
   ipfilter --delrule fips_ipv4 –rule 3
   ipfilter --addrule fips_ipv4 –rule 3 –sip any –dp 80 –proto tcp –act deny –type INPUT –dip any
   ipfilter --addrule fips_ipv4 –rule 7 –sip any –dp 897 –proto tcp –act deny –type INPUT –dip any
   ipfilter --addrule fips_ipv4 –rule 7 –sip any –dp 897 –proto udp –act deny –type INPUT –dip any
   ipfilter --delrule fips_ipv4 –rule 10
   ipfilter --delrule fips_ipv4 –rule 9
   ipfilter --addrule fips_ipv4 –rule 9 –sip any –dp "600-896" –proto tcp –act permit –type INPUT –dip any
   ipfilter --addrule fips_ipv4 –rule 10 –sip any –dp "898-1023" –proto tcp –act permit –type INPUT –dip any
   ipfilter --addrule fips_ipv4 –rule 11 –sip any –dp "600-896" –proto udp –act permit –type INPUT –dip any
   ipfilter --addrule fips_ipv4 –rule 12 –sip any –dp "898-1023" –proto udp –act permit –type INPUT –dip any
   ipfilter --activate fips_ipv4

   For Ipv6
   ipfilter --clone fips_ipv6 –from default_ipv6
   ipfilter --delrule fips_ipv6 –rule 2
   ipfilter --addrule fips_ipv6 –rule 2 –sip any –dp 23 –proto tcp –act deny –type INPUT –dip any
   ipfilter --delrule fips_ipv6 –rule 3
   ipfilter --addrule fips_ipv6 –rule 3 –sip any –dp 80 –proto tcp –act deny –type INPUT –dip any
   ipfilter --addrule fips_ipv6 –rule 7 –sip any –dp 897 –proto tcp –act deny –type INPUT –dip any
   ipfilter --addrule fips_ipv6 –rule 7 –sip any –dp 897 –proto udp –act deny –type INPUT –dip any
   ipfilter --delrule fips_ipv6 –rule 10
   ipfilter --delrule fips_ipv6 –rule 9
   ipfilter --addrule fips_ipv6 –rule 9 –sip any –dp "600-896" –proto tcp –act permit –type INPUT –dip any
   ipfilter --addrule fips_ipv6 –rule 10 –sip any –dp "898-1023" –proto tcp –act permit –type INPUT –dip any
   ipfilter --addrule fips_ipv6 –rule 11 –sip any –dp "600-896" –proto udp –act permit –type INPUT –dip any
   ipfilter --addrule fips_ipv6 –rule 12 –sip any –dp "898-1023" –proto udp –act permit –type INPUT –dip any
   ipfilter --activate fips_ipv6

8. Configure supported host keys for use for SSH:
   Delete the unsupported host key for SSH i.e. DSA and RSA using `sshutil delknownhost`

   `sshutil delhostkey -rsa`

   `sshutil delhostkey -dsa`

   NOTE: this action ensures that only ecdsa-sha2-nistp256 based SSHv2 host key are available for use in Approved mode of operation

9. Configuring AAA authentication:

   NOTE: TACACS+ is not supported in FIPS mode and should not be enabled.

   If AAA authentication is to be used in FIPS mode, configure the preferred and supported AAA server (LDAP/RADIUS) using *aaaconfig* CLI command.

   a. Set the initial state
      i. Set the authentication to the local database
         aaaconfig --authspec "local"

         NOTE: By default, authentication is set using the local database.

   b. Requirements for CA certificate
      i. Existence of CA certificate is mandatory for RADIUS and/or LDAP services.
         1. Ensure that the CA certificate is imported using *seccertmgmt* CLI
            a. Ex: For radius:
               seccertmgmt import -ca -server radius

            b. Ex: For ldap:
               seccertmgmt import -ca -server ldap

      ii. CA certificate also must meet the requirement listed below:
         1. All certificates must be of RSA 2048 key pair signed with SHA256 hash

   c. Add the server
      i. If RADIUS server is used, then issue the following CLI command and ensure only '*peap-mschapv2*' is configured.
         aaaconfig --add <radius-serverip> -conf radius -a peap-mschapv2

      ii. If LDAP server is used, then issue the following CLI command,
         aaaconfig --add <ldap-serverip> -conf ldap -d <domain>

   d. Set the final authentication setting
      i. If setting up a RADIUS server, then issue the following CLI command:
         aaaconfig --authspec "radius;local"

      ii. If setting up a LDAP server, then issue the following CLI command:
         aaaconfig --authspec "ldap;local"

10. If in-flight encryption feature is enabled, disable it using
    portcfgencrypt –-disable <portnum>

11. If management IP Sec feature is enabled, disable it using *ipsecconfig* CLI

12. If Inband Management feature is enabled, disable it using
    `portcfg mgmtif <port num> disable`

13. In FIPS mode http is blocked and only https is allowed. For using https in FIPS mode, configure HTTPS using the *seccertmgmt* CLI with a third-party certificate

    seccertmgmt import –ca –server https
    seccertmgmt import –cert https

14. Configure cipher using `secCryptoCfg` CLI to configure ciphers for SSH, TLS, RADIUS and LDAP

    a. Export default_strong template from the switch.
       seccryptocfg --export default_strong –server <server-ip> -name <username> -proto scp –file <filename>
    b. Edit the template to include only the ciphers as mentioned in section 3.1.1 (FIPS Approved Cryptographic Algorithms)
    c. Download the template and enable it

seccryptocfg --import <custom template name> -server <serverip> -name <username> -proto scp –file <filename>
seccryptocfg --apply <custom template name>

15. Enable secure protocols using *configurechassis* command

```
configurechassis

Configure…

  cfgload attributes (yes, y, no, n): [no] y

   Enforce secure config Upload/Download (yes, y, no, n): [no] y
```

16. SNMP configurations

    a. Disable SNMPv1 using `snmpconfig –disable snmpv1` CLI command
    b. If SNMPv3 is to be used in FIPS mode,
        i. enable SNMPv3 and sec level to auth and Priv
        ii. Passwords for all users should be of minimum length 8
        iii. Auth protocol should be SHA1
        iv. Priv protocol should be AES128
        NOTE: DES must not be configured for SNMPv3

```
E.g.: snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false]

SNMPV3 Password Encryption Enabled (true, t, false, f):
[false] true
Warning: The encrypted password cannot be decrypted. Do you
want to continue? (yes, y, no, n): [no] y

SNMPv3 user configuration(snmp user not configured in FOS
user database will have default VF context and admin role as
the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 2
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]):
(1..4) [2] 3
New Priv Passwd:
Verify Priv Passwd:
```

17. Passwords for default accounts (admin and user) must be changed after every zeroization to maintain FIPS 140-2 compliance. Change the default password for “admin” and “user” by pressing “Enter” instead of “Ctrl-C” after logging in as “admin”.

18. Modify the authutil policy in every VF present, to use hash SHA-256 and DH Group 4(use *setcontext CLI to switch to each VF and execute below command)*".

```
authutil --set -h sha256
authutil --set -g 4
```

19. Disable bootprom using the CLI *fipscfg –disable bootprom*.

    a. Bootprom account can be disabled only as root.
    b. Enable root account using following CLI
       userconfig --change root –e yes
    c. Login as "root" and disable the bootprom using
       fipscfg --disable bootprom
    d. Login as "admin" again and disable "root" using
       userconfig --change root –e no

20. Verify if the switch is configured to be FIPS compliant
    a. Execute '*fipscfg --verify fips*'
    b. Execute '*fipscfg --verify fips -dp*' if DP exists
    c. Ensure that all conditions are met and the message is displayed that FIPS mode can be enabled.

    Ex: (Indicates of both failure and pass example)

```
fipscfg --verify fips
Standby firmware supports FIPS  - PASS
SELF tests check has passed  - PASS
Root account check has passed  - PASS
Radius check has passed  - PASS
Authentication check has passed  - PASS
Inflight Encryption check has passed  - PASS
IPSec check has passed  - PASS
IPv6 policies FIPS compliant  - PASS
IPv6 policies FIPS compliant  - PASS
SNMP is in read only mode–  - PASS
SNMP User password length check - PASS
SNMP Users have no MD5 auth protocol check - PASS
Bootprom access is disabled–  - PASS
Secure config upload/download is enabled–  - PASS
SSH DSA Keys check passed  - PASS
Inband Management interface is disabled  - PASS
Ipsecconfig is disabled.  – PASS
FCIP validations - PASS
Certificates validation has passed  - PASS
SSH host key (RSA) validation has passed  - PASS
```

21. If all the tests are PASS in above step, then proceed to enable FIPS mode.

Next page →

22. Enable FIPS Mode
    - *Execute '`fipscfg --enable fips`'*

```
sw068:test> fipscfg --enable fips
FIPS mode has been set to : Enabled
```

    - *Verify that the FIPS mode has been set to '`Enabled`' using '`fipscfg --show`'*

```
Sw0068:test> fipscfg --show
FIPS mode is : Enabled
FIPS Selftests mode/status is : Enabled/None
```

    - *Execute '`fipscfg --enable fips -dp`' to enter DP FIPS mode*

```
Sw068:test> fipscfg --enable fips -dp
FIPS mode has been set to : Enabled
DP FIPS mode has been set to : Enabled
```

        - Power-cycle the chassis.

    - Login to the node as an authorized user, and verify that the self-tests mode is set to Enabled/Pass'

```
SB65:FID128:root> fipscfg –show
FIPS mode is : Enabled
FIPS Selftests mode/status is : Enabled/Pass
diffie-hellman-group-exchange-sha256 is : Enabled
DP FIPS mode is : Enabled
DP FIPS Selftests mode/status is : Enabled/Pass
SB65:FID128:root>
```

23. Enable the DH key size configuration using '*`fipscfg --enable dh`*'

24. The tamper evident seals supplied in FIPS Kit Brocade XBR-000195 (P/N: 80-1002006-02) must be installed as defined in section 12 (Appendix A: Tamper Label Application).

25. After successful completion of step 24, your switch is now in FIPS Approved mode

26. WARNING: At this point, the algorithms in Section 3.2, Table 8, are now disabled. Any use of these algorithms, or an attempt by the operator to revert the configuration in Section 3.1.2.2, is an explicit violation of this Security Policy and implicitly toggles the module out of FIPS mode.

    NOTE: Upon successful completion of all configuration steps in Section 3.1.2.2, self-tests will forevermore be enabled, even if the operator violates this Security Policy which implicitly toggles the module out of FIPS mode after configuration.

Next page →

3.1.2.3 How to determine that an Approved mode of operation is selected

After all steps specified in section 3.1.2.2 (Cryptographic module initialization) are performed, the operator shall perform the following instructions to examine the mode of operation:

1. Check for successful status of the powerup Self-Tests. For details, see section 8, Security Rules.
2. Confirm the firmware version using `firmwareshow` command
   a. *`firmwareshow`*
3. Check status of FIPS mode
   a. *`fipscfg –show`*
4. Validate that the tamper evident seals are applied and the module is untampered (see section 9.2 for details).
5. Do not configure the device to use any of the algorithms listed in section 3.2, Non-Approved mode of operation

3.2 Non-Approved FIPS cryptographic algorithms and services

This section lists all non-Approved cryptographic algorithms and all Non-Approved services which MUST NOT be used. The use of any such algorithm, and service, is an explicit violation of this Security Policy and is explicitly disallowed by this Security Policy.

The module supports a Non-Approved mode of operation. This mode of operation exists when:

A. After the module has been initialized and configured as per section 3.1, the Crypto-Officer reverts any of the configuration procedures and executes the Non-Approved services in Table 9 using the Non-Approved Algorithms in Table 8.

The algorithms marked "non-compliant" are not compliant simply because they are invoked in the Non-Approved mode of operation, by a Non-Approved mode service.

Table 8 – Non-Approved Algorithms

Algorithm	Use
AES 128, 192 and 256 (non-compliant)	Encryption / Decryption
CAMELLIA 128 and 256	Encryption / Decryption
DES	Encryption / Decryption
Diffie-Hellman (1024, 2048 and 3096) (non-compliant)	Key Establishment
DSA (non-compliant)	Digital Signature
EC-DH (2048, 256) (2048, 384) (2048, 521) (non-compliant)	Key Establishment
ECDSA (FIPS 186-4; non-compliant)	Digital Signature
HMAC-MD5	Message Authentication
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256 and HMAC-SHA-384, HMAC-SHA-512 (non-compliant)	Message Authentication
KDF (SSHv2, IKEv2, SNMPv3, TLS) (non-compliant)	Key Derivation
MD5	Message digest
PSK	Key Establishment
RC-4	Encryption / Decryption
RSA Key Wrap (non-compliant)	Key establishment
SEED	Encryption/ Decryption
SHA-1, SHA-256, SHA-384 (non-compliant)	Message Digest
Triple-DES (non-compliant)	Encryption / Decryption

These functions and services are non-compliant and disallowed in Approved mode of operation.

Table 9 – Services in Non-Approved Mode of Operation

Crypto Function/Service	User Role Change Access	Additional Details
Ciphers, Message Authentication Codes, Key Exchange, Digital Signature, and KDF algorithms for TLS	Crypto-Officer	Cipher: aes128-cbc (non-compliant), aes256-cbc (non-compliant), aes128-gcm (non-compliant), aes256-gcm (non-compliant), camellia-128, camellia-256, des , seed, rc-4, triple-des (non-compliant) Message Authentication Code: hmac-sha-1, hmac-sha-256 (non-compliant) , hmac-sha-384 (non-compliant) Key Exchange: dh-dss, dhe-dss, dhe-rsa (non-compliant) , dh-rsa (non-compliant) , ecdh (non-compliant) , ecdhe (non-compliant) , psk Digital Signature: ecdsa (non-compliant) , rsa (non-compliant) KDF: TLSv1.0/1.1 (non-compliant) , TLSv1.2(non-compliant)
Ciphers, Message Authentication Codes, Key Exchange, and KDF algorithms for SSHv2	Crypto-Officer	Cipher: aes128-ctr (non-compliant) , aes192-ctr (non-compliant) , aes256-ctr (non-compliant) , aes128-cbc (non-compliant) , 3des-cbc (non-compliant) , aes192-cbc (non-compliant) , aes256-cbc (non-compliant) Message Authentication Code: hmac-md5, hmac-sha1 (non-compliant) , hmac-sha2-256 (non-compliant) , hmac-sha2-512 (non-compliant) Key Exchange: ecdh-sha2-nistp256(non-compliant), ecdh-sha2-nistp384 (non-compliant), ecdh-sha2-nistp521 (non-compliant), diffie-hellman-group-exchange-sha256 (non-compliant), diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1 KDF: SSHv2 (non-compliant)
Common Certificates for FCAP and HTTPS	Crypto-Officer	FCAP and HTTPS are supported with certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)
SNMP	Crypto-Officer	SNMPv1 (plaintext) and SNMPv3 KDF (non-compliant); Algorithms: AES128 (non-compliant), SHA-1 (non-compliant), KDF (non-compliant) and MD5

Crypto Function/Service	User Role Change Access	Additional Details
RADIUS or LDAP	Crypto-Officer	PAP and CHAP authentication method for RADIUS (all considered as plaintext) LDAP and RADIUS is supported with CA certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant) LDAP uses TLS connections in non-FIPS mode without certificates
Telnet	Crypto-Officer	N/A – No algorithms (plaintext)
HTTP	Crypto-Officer	N/A – No algorithms (plaintext)
FTP	Crypto-Officer	Config Upload, Config Download, Support Save, FW Download, autoftp
Management IPSec	Crypto-Officer	Management Interface IPSec/IKEv2 (disabled for management interface)
In-Band Management Interface	Crypto-Officer	N/A – No algorithms (plaintext)
RSA	Crypto-Officer	RSA key size < 2048 bits for SSHv2 and TLS
Diffie-Hellman	Crypto-Officer	DH key size < 2048 bits for SSHv2
In-Flight Encryption	Crypto-Officer	DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm FCAP: Certificates with any key size signed by MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)
TACACS+ authspec mode	Crypto-Officer	PAP or CHAP authspec is supported
FC-SP Authentication	Crypto-Officer	DH-CHAP and FCAP for FC-SP Authentication DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm FCAP supported with certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

4 Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- Fiber Channel: Data Input, Data Output, Control Input, Status Output
- 1 GbE & 10 GbE: Data Input, Data Output, Control Input, Status Output
- Ethernet Ports: Control Input, Status Output
- Serial port: Control Input, Status Output
- USB: Data Input, Data Output, Status Output
- Power Supply Connectors: Power Input
- LEDs: Status Output

4.1 LED Indicators

1. Switch Extension 7840
    a. Port side:
        i. System Status LED (1 per module)
        ii. System Power LED (1 per module)
        iii. Management port Ethernet:
        iv. Ethernet Link LED (1)
        v. Ethernet Status LED (1)
        vi. FC Port Status LED (one for each FC port)
        vii. 40 GbE FCIP Port Status (one for each FCIP port)
        viii. 1/10 GbE FCIP Port Status (one for each FCIP port)

    b. Non-port side:
        i. Power supply AC input status LED (one per power supply)
        ii. Power supply DC output status LED (one per power supply)
        iii. Fan status LED (one per fan)

Table 10 – Port/Interface Quantities for Brocade 7840

Model	Port/Interface Type								
	Fibre Channel Ports	40 GbE ports	1 GbE & 10 GbE	Management port Ethernet	Serial Port	USB	Power Supply Connectors	FAN FRU	LED (total)
7840	24	2	16	1	1	1	2	3	51

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Table 11 – Port-side LED patterns during normal operation

LED name	LED color	Status of hardware
Power Status	No light	System is off or there is an internal power supply failure.
	Steady green	System is on and power supplies are functioning properly.
System Status	No light	System is off or there is no power.
	Steady green	POST and initialization is completed. System is on and functioning properly.
	Steady amber (for more than five seconds)—can take over a minute to complete POST	System is going through the power-up process.
	Steady amber (for more than a few minutes)	Unknown state, boot failed, or the system is faulty. NOTE Once POST completes and the switch has failed, steady amber may result.
	Flashing amber/green	Attention is required. A number of variables can cause this status, including a single power supply failure, a fan failure, or one or more environmental ranges has been exceeded.
Ethernet Link	No light	There is no link.
	Steady green	There is a link.
Ethernet Status/Activity	No light	No activity.
	Flashing green	There is link activity (traffic).
FC Port Status	No light	Indicates one of the following: No signal or light carrier (media or cable) detected. Blade may be currently initializing. Connected device is configured in an offline state.
	Steady green	Port is online (connected to external device) but has no traffic.
	Slow-flashing green (on 1/2 second; then off 1/2 second)	Port is online but segmented because of a loopback cable or incompatible Extension Switch connection.
	Fast-flashing green (on 1/4 second; then off 1/4 second)	Port is online and an internal loopback diagnostic test is running.
	Flickering green	Port is online and frames are flowing through the port.
	Steady amber	Port is receiving light or signal carrier, but it is not online yet.
	Slow-flashing amber (on 2 seconds; then off 2 seconds)	Port is disabled because of diagnostics or the portDisable command.
	Fast-flashing amber (on 1/2 second; then off 1/2 second)	SFP or port is faulty.
10-GbE/40-GbE Ethernet Port Status	No light (LED is off)	Port is offline. No activity.
	Steady green	Port is online and active.

Table 12 – Non-port-side LED patterns during normal operation

LED name	LED color	Status of hardware	Recommended action
Power supply AC input status (one green LED)	No light	Power supply is not receiving AC input voltage or AC input voltage is below operational limit.	Verify that the power supply is properly seated and the power cord is connected to a functioning
	Steady green	AC input voltage is within operational range.	No action required.
Power supply DC output status (one bi-color LED)	Flashing amber (1:1)	Output voltage is not enabled.	Verify that the power supply is fully seated and that the captive screw is
	Flashing amber/green (2:1)	Over temperature warning.	Verify that ambient temperature is less than 40°C (104°F) and check
	Flashing amber/green (1:1)	Internal fan is out of regulation.	Replace the power supply.
	Steady amber	Power supply is faulty or not plugged in completely.	Check the power cord, current, voltage, and temperature to determine
	Steady green	DC output is OK.	No action required.
Fan assembly status (one bi-color LED)	No light (LED is off)	Fan assembly is not receiving power.	Verify that the fan FRU is seated correctly.
	Steady green	Fan assembly is operating normally.	No action required.
	Steady amber (for more than 5 seconds)	Fan fault for one of the following reasons: A fan assembly with mismatched airflow is present. One or more of the fans in the fan assembly has failed.	Try one of the following: Replace the mismatched fan assembly with one that has the correct airflow direction. Replace the faulty fan assembly.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module supports the following operator roles listed in the table below. The cryptographic module enforces the separation of roles using role-based operator authentication. An operator must enter a username and its password to log in. The username is an alphanumeric string of maximum 40 characters. The password is an alphanumeric string of 8 to 40 characters chosen from 96 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the context of the module. At the end of a session, the operator must log-out. The module supports a maximum of 256 operators, five Radius servers and five LDAP servers that may be allocated the following roles:

Table 13 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (Crypto-Officer)	Role-based operator authentication	Username and Password
User (User role)	Role-based operator authentication	Username and Password
Security Admin	Role-based operator authentication	Username and Password
Fabric Admin	Role-based operator authentication	Username and Password
LDAP Server	Certificate based server authentication	LDAP Root CA certificate
RADIUS Server	Certificate based server authentication	RADIUS Shared Secret and RADIUS Root CA Certificate
Host/Server/Peer Switch	Role-based operator authentication	PKI (FCAP) or Shared Secret (DH-CHAP)
IKEv2 Peer	Role-based operator authentication	IKEv2 Authentication Key or PKI [ECDSA , P-384 signing (private) key]
SNMP	Role-based operator authentication	"Auth" and "Priv" passwords

Table 14 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive failed authentication attempts. If the module is not configured to restrict failed authentication attempts, then the maximum attempts possible within one minute is 20. The probability of successfully authenticating to the module within one minute is 20/96^8 which is less than 1/100,000.
Digital Signature Verification (PKI)	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112 which is less than 1/1,000,000. The module will restrict the number of consecutive failed authentication attempts to 10. The probability of successfully authenticating to the module within one minute is 10/2^112 which is less than 1/100,000.
Knowledge of a Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The maximum possible authentication attempts within a minute are 16 attempts. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
Knowledge of IKEv2 Authentication Key	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^512, which is less than 1/1,000,000. The maximum attempts allowed in a one minute period are equal to one attempt. If an authentication error is detected, the session goes into a fault state, and no new attempts are allowed. Therefore, the probability of a random success in a one minute period is 1/2^512, which is less than 1/100,000.
Knowledge of IKEv2 ECDSA P-384 Private Key	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^192, which is less than 1/1,000,000. The maximum attempts allowed in a one minute period are equal to one attempt. If an authentication error is detected, the session goes into a fault state, and no new attempts are allowed. Therefore, the probability of a random success in a one minute period is 1/2^192, which is less than 1/100,000.

Table 15 – Description of Services in Approved mode of operation

Service Name	Description	FOS Interface
FIPSCfg	Control FIPS mode operation and related functions.	fipscfg
Zeroize	Zeroize all CSPs.	fipgscfg –zeroize
FirmwareManagement	Control firmware management.	firmwarecommit firmwaredownload firmwaredownloadstatus, firmwareshow
IKEv2 Negotiation - IPsec Traffic	Negotiate IKEv2 sessions, key security associations for IPsec	portcfg ipsec-policy portcfg fciptunnel
PKI	PKI configuration functions, including FOS switch certificates, SSL certificates and IKEv2 ECDSA P-384 certificates.	seccertmgmt
RADIUS	RADIUS configuration functions.	aaaconfig
LDAP	LDAP configuration functions.	aaaconfig
UserManagement	User and password management.	passwd passwdconfig userconfig
SSHv2 and TLS	Crypto configuration	seccryptocfg
SNMPv3	SNMPv3 configuration	snmpconfig

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6 Access Control Policy

6.1 Roles and Services

Table 16 – Services Authorized for Roles

Services \ Roles	User	Admin (Crypto-Officer)	FabricAdmin	SecurityAdmin	LDAP Server	RADIUS Server	Host Server / Peer Switch	IKEV2 Peer	SNMP
FIPSCfg		X		X			X		
Zeroize		X		X					
FirmwareManagement	X	X	X	X					
PKI	X	X	X	X					
RADIUS		X		X		X			
LDAP		X		X	X				
UserManagement	X	X		X					
IKEv2 Negotiation-IPsec Traffic		X		X			X	X	
SSHv2 and TLS	X	X		X					
SNMPv3		X	X	X					X

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated by power-cycling the module.
- Show Status: This service is met through the various status outputs provided by the services provided above, as well as the LED interfaces.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6.3 Definition of Critical Security Parameters (CSPs)

DH Private Key:

- DH Private Keys for use with 2048-bit modulus

SSHv2/SCP/SFTP CSPs:

- SSHv2/SCP/SFTP Encryption Keys
- SSHv2/SCP/SFTP Authentication Key
- SSHv2 KDF Internal State
- SSHv2 DH Shared Secret Key (2048 bit)
- SSHv2 ECDH Shared Secret Key (P-256)
- SSHv2 ECDH Private Key (P-256)
- SSHv2 ECDSA Private Key (P-256)
- Value of K during SSHv2 P-256 ECDSA session

TLS CSPs:

- TLS Private Key (RSA 2048)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS KDF Internal State
- TLS Session Keys - 128, 256 bit AES CBC
- TLS Authentication Key for HMAC-SHA-1 (160 bits) and HMAC-SHA-256

CP DRBG CSPs:

- CP DRBG Seed Material
- CP DRBG Internal State (V and Key)

Passwords:

- Passwords

RADIUS Secret:

- RADIUS Secret

IKEv2 and IPsec CSPs:

- DH Private Key (256 bits) (Used in IKEv2)
- DH Shared Secret (2048 bits) (Used in IKEv2)
- IKEv2 AES-256 Encrypt/Decrypt Keys
- ESP AES-256-GCM Encrypt/Decrypt Keys
- IKEv2 KDF State
- IKEv2 Authentication Key (PSK)

- IKEv2 ECDH P-384 Private Key
- IKEv2 ECDSA P-384 Private Key
- IKEv2 Integrity Key (HMAC-SHA-384)

DRBG Internal State and Entropy Data (On Cavium)

- DRBG Internal State (V and Key) (On Cavium)
- Entropy Data (on Cavium)

SNMPv3 CSPs:

- SNMPv3 Auth and Priv password
- SNMPv3 KDF Internal State
- SNMPv3 Auth and Priv Secrets

6.4 Definition of Public Keys

DH Public Keys:

- DH Public Key (2048 bit modulus)
- DH Peer Public Key (2048 bit modulus)

TLS Public Keys:

- TLS Public Key (RSA 2048)
- TLS Peer Public Key (RSA 2048)

FW Download Public Key:

- FW Download Public Key (RSA 2048)

SSHv2 Public Keys:

- SSHv2 ECDSA Public Key (P-256)
- SSHv2 ECDSA Peer Public Key (P-256)
- SSHv2 ECDH Public Key (P-256)
- SSHv2 ECDH Peer Public Key (P-256)
- DH Public Key (2048-bit) (Used in IKEv2)
- DH Peer Public Key (2048-bit) (Used in IKEv2)

LDAP ROOT CA Public Key:

- LDAP ROOT CA certificate (RSA 2048)

RADIUS ROOT CA Public Key:

- RADIUS ROOT CA certificate (RSA 2048)

IKEv2 and IPsec Public Keys:

- IKEv2 ECDH P-384 Public Key
- IKEv2 ECDH P-384 Peer Public Key
- IKEv2 ECDSA P-384 Public Key
- IKEv2 ECDSA P-384 Peer Public Key

6.5 Definition of CSPs Modes of Access

Table below defines the relationship between access to CSPs and the different module services. Please see Section 6.3 and Section 6.4 for explicit designation of CSPs and Public Keys. The modes of access shown in the table are defined as follows:

- R: Read
- W: Write
- N: No Access
- Z: Zeroize (Session Termination and "fipscfg –zeroize" command)

Table 17 – CSP Access Rights within Roles & Services

Services \ CSPs	SSHv2/SCP/SFTP CSPs	DH Private Keys	TLS CSPs	CP DRBG Seed Material / Internal State	DRBG Internal State and Entropy Data (On Cavium)	Passwords	RADIUS Secret	IKEv2 and IPsec CSPs	SNMPv3 CSPs e
FIPSCfg	N	N	N	N	N	N	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	R	N	N	N	N	N	N	N
PKI	RW	RW	N	RW	N	N	N	N	N
RADIUS	N	N	N	N	N	RW	RW	N	N
LDAP	N	N	N	N	N	N	N	N	N
UserManagement	N	N	RW	RW	N	RW	N	N	N
IKEv2 Negotiation – IPsec Traffic	N	N	N	N	RW	N	N	RW	N
SSHv2 and TLS	RW	RW	RW	N	N	RW	N	N	N
SNMPv3	N	N	N	N	N	RW	N	N	RW

Next page →

Table 18 – Public Key Access Rights within Roles & Services

Services \ Public Keys	DH Public Keys	TLS Public Keys	Firmware Download Public Key	SSHv2 Public Keys	LDAP Root CA Certificate	RADIUS Root CA Certificate	IKEv2 and IPSEC Public Keys
FIPSCfg	N	N	N	N	N	N	N
Zeroize	N	N	N	N	N	N	N
FirmwareManagement	N	N	RW	N	N	N	N
PKI	N	RW	N	RW	N	N	N
RADIUS	N	N	N	N	N	RW	N
LDAP	N	N	N	N	RW	N	N
UserManagement	N	N	N	N	N	N	N
IKEv2 Negotiation – IPsec Traffic	RW	N	RW	N	N	N	RW
SSHv2 and TLS	RW	RW	N	RW	R	R	N
SNMPv3	N	N	N	N	N	N	N

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code RSA signed may be executed.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

8 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS140-2 Level 2 module.

1) The cryptographic module shall provide role-based authentication.
2) When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3) The cryptographic module shall perform the following tests:
   a) Power up Self-Tests:
      - AES (128,192 and 256) CBC Encrypt KAT
      - AES (128,192 and 256) CBC Decrypt KAT
      - AES (256) GCM KAT Encrypt
      - AES (256) GCM KAT Decrypt
      - HMAC SHA-1 KAT
      - HMAC-SHA-224 KAT
      - HMAC SHA-256 KAT
      - HMAC SHA-384 KAT
      - HMAC SHA-512 KAT
      - SP800-90A DRBG KAT
      - SHA-1 KAT
      - SHA-256 KAT
      - SHA-384 KAT
      - SHA-512 KAT
      - RSA 2048 SHA-256 Sign KAT
      - RSA 2048 SHA-256 Verify KAT
      - SP800-135 SSHv2 KDF KAT
      - SP800-135 TLS 1.0 KDF KAT
      - SP800-135 TLS 1.2 KDF KAT
      - SP800-135 IKEv2 KDF KAT
      - ECDSA KAT
      - ECDH KAT (Primitive "Z" Computation KAT)
      - SP800-135 SNMPv3 KDF KAT

   b) Critical Functions Tests:
      - RSA 2048 Encrypt/Decrypt

c) Message reporting for Status of Power-Up Self-Tests

- On Success, CP will display the status as below,

  <Algorithm Detail>.....successful

- On Failure, CP will display the Power-Up Self-Tests status as shown below,

  <Algorithm Detail>.....FAILED!

- On Failure in the DP, CP will display the error message as shown below,

  POST failure detected on DP<DP#>

d) Firmware Integrity Tests (128-bit EDC)

- On Failure, the following message is displayed:

  Firmware integrity check failed

- On Success, the following message is displayed:

  Firmware integrity test passed

e) Conditional Self-Tests

- Continuous Random Number Generator NDRNG test – Performed on non-Approved RNG.
- Continuous Random Number Generator test – performed on DRBG (CTR_DRBG, AES-256).
- RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)
- RSA 2048 Pairwise Consistency Test (Encrypt/Decrypt)
- ECDSA P-256 Pairwise Consistency Test (Sign/Verify)
- ECDSA P-384 Pairwise Consistency Test (Sign/Verify)
- Firmware Load Test (RSA 2048 with SHA-256 Signature Verification)
- Bypass Test: N/A
- Manual Key Entry Test: N/A

f) Message reporting for Status of Conditional Self-Tests

- On failure in Continuous Random Number Generator related tests
  - On CP

    NDRNG continuous test failed!

    or

    ERROR: DRBG Critical Failure! FIPS Drbg Health Check Failed

    or

    ERROR: DRBG Critical Failure! FIPS DRBG Init Failed
  - On DP

    Continuous health check failed on DP<DP#>
- On Failure in RSA 2048 Pairwise Consistency related Tests

  Conditional tests failed at Sign/Verify

  or

  Conditional tests failed Encrypt/Decrypt

- On Failure in ECDSA Pairwise Consistency related Tests
  ECDSA pair wise consistency test failed
- On Failure in Firmware Load Test

  Firmware download failed - Failed to download RPM package
  or
  Firmwaredownload failed because the signature for the firmware could not be validated.

g) At any time, the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.

4) Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

5) Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

6) The module does not support a maintenance role or maintenance interface.

7) The serial port may only be accessed by the Crypto-Officer when the Crypto-Officer is physically present at the cryptographic boundary, via a direct connection without any network access or other intervening systems.

8) The following protocols have not been reviewed or tested by the CAVP nor CMVP
   i) TLS v1.0/v1.1
   ii) SSHv2
   iii) TLS v1.2
   iv) IKEv2
   v) SNMPv3

9) The module complies with FIPS 140-2 Implementation Guidance, Section A.5, Key/IV Pair Uniqueness Requirements from SP 800-38D

   The AES GCM session key is established via the IKEv2 KDF (internally). The 96-bit IV is also constructed internally (deterministically) as per FIPS 140-2 IG A.5 Scenario 3. The fixed field (64-bits) is randomly generated bits from the SP 800-90A DRBG; this is an acceptable construction of the fixed field as per SP 800-38D Section 8.2.1 which states “the entire fixed field may consist of arbitrary bits when there is only one context to identify, such as when a fresh key is limited to a single session of a communications protocol”.

   Furthermore, this is satisfactory because as per the implementation guidance “just the fact that the modules can possibly have at least 2^32 different names will be sufficient to meet this requirement.” The invocation field is a separate 32-bit deterministic non-repetitive counter which increments by one. The implementation of the deterministic non-repetitive counter management logic inside the module ensures that after 2^31 operations, a new AES GCM session key and IV must be created (i.e. IKE V2 renegotiation is automatically enforced which results in new GCM Key and new IV). The IV restoration conditions are satisfied for the deterministic non-repetitive counter as per the IG A.5 bullet 3: The GCM key and IV are session specific; if the module loses power the implementation is required to renegotiate a new IKE session and thus a new GCM key and IV will be created.

10) This module complies with FIPS 140-2 Implementation Guidance, Section A.8 Use of HMAC-SHA-1-96 and Truncated HMAC

    If IKEv2 is configured to use HMAC-SHA-384-192 as specified in RFC 6379 *Suite B Cryptographic Suites for IPsec* Section 3.2. The HMAC-SHA-384-192 integrity algorithm is specified in RFC 4868 *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*. In RFC 4868 Section 2.3 the truncation of HMAC output when used as an integrity verification algorithm for IKEv2 is described. The bits used as the integrity value shall be one-half the length of the algorithm output. In this case, the message is MAC'ed using the HMAC-384 algorithm, and the digest is shortened to 192 bits by truncating the least-significant 192 bits of the digest. This use of the HMAC-SHA-384-192 as an integrity algorithm is summarized in RFC 4868 Section 2.6.

    The HMAC standard is FIPS 198-1 -*The Keyed-Hash Message Authentication Code (HMAC)*. Section 5 of that standard specifies that applications of that standard may truncate the output of the HMAC function. Per FIPS 198-1, the leftmost bits of the HMAC output shall be used as the MAC. There is no conflict in this case between FIPS 198-1 and RFC 4868. FIPS 198-1 references SP800-107 *Recommendation for Applications Using Approved Hash Algorithms*.

    In SP800-107 Section 5.3.3, the use of truncated HMAC output for integrity tags is described. This section requires that *n* leftmost bits are used as the tag, and that *n* is no less than 32 bits. This implementation adheres to RFC 4868, so the leftmost 192 bits of the 384-bit output of the HMAC are used as the MAC tag, and the requirements of SP800-107 are met.

11) When the extension platform is configured for FIPS mode, and a PSK IPSec policy is used, the operator must ensure the IKEv2 Authentication Key (PSK) is configured using a full 64 byte (512 bits) value.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- Tamper evident seals.

9.2 Operator Required Actions

The operator is required to inspect the tamper evident seals, periodically, per the guidance provided in the user documentation.

Table 19 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Tamper Evident Seals	12 months	Reference Appendix A for a description of tamper label application for all evaluated platforms.

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Table 20 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11 Definitions and Acronyms

Table 21 – Definitions and Acronyms

Acronym	Definition
0 1/10/40GBE SFP	Zero SFP devices provided
10 GbE	10 Gigabit Ethernet
AES	Advanced Encryption Standard
Blade	Any functional assembly that can be installed in a chassis, excluding power and fan FRUs
BR	Brocade
CBC	Cipher Block Chaining
CLI	Command Line interface
CP	Control Processor
CSP	Critical Security Parameter
DH	Diffie-Hellman
DP	Data Processor
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve Digital Signature Algorithm
FC	Fiber Channel
FCIP	Fiber Channel over Internet Protocol
FIPS	Federal Information Processing Standard
FOS	Fabric Operating System
FRU	Field Replaceable Unit
GbE	Gigabit Ethernet
GBE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SFP	Small form-factor pluggable
SHA	Secure Hash Algorithm
SSHv2	Secure Shell Protocol
TLS	Transport Layer Security Protocol
Triple-DES	Triple Data Encryption Standard

12 Appendix A: Tamper Label Application

For each module to operate in a FIPS approved mode of operation, the tamper evident seals supplied in FIPS Kit Brocade XBR-000195 (P/N: 80-1002006-02) must be installed.

The Crypto-Officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The Crypto-Officer shall maintain a serial number inventory of all used and unused tamper evident seals. The Crypto-Officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The Crypto-Officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The Crypto-Officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

Use ethyl alcohol to clean the surface area at each tamper evident seal placement location. Prior to applying a new seal to an area that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use ethyl alcohol to clean off any residual adhesive remover before applying a new seal.

12.1 Brocade 7840 Switch

Use ethyl alcohol to clean the surface area at each tamper evident seal placement location. Prior to applying a new seal to an area that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use ethyl alcohol to clean off any residual adhesive remover before applying a new seal.

Twenty-seven (27) tamper evident seals are required to complete the physical security requirements for the Brocade 7840. Steps 1 – 5 below, detail the tamper evident seal placement for the Brocade 7840 module.

1. Apply two (2) seals to the front side of the module. See Figure 5 for correct seal placement.
2. Apply twelve (12) seals to the back side of the module. See Figure 6 for correct seal placement.
3. Apply five (5) seals to the left side of the module. These seals will wrap around to the bottom of the module. See Figure 7 for correct seal placement.
4. Apply five (5) seals to the right side of the module. These seals will wrap around to the bottom of the module. See Figure 8 for correct seal placement.
5. Apply three (3) seals to the bottom side of the module near the front side. See Figure 9 for correct seal placement.

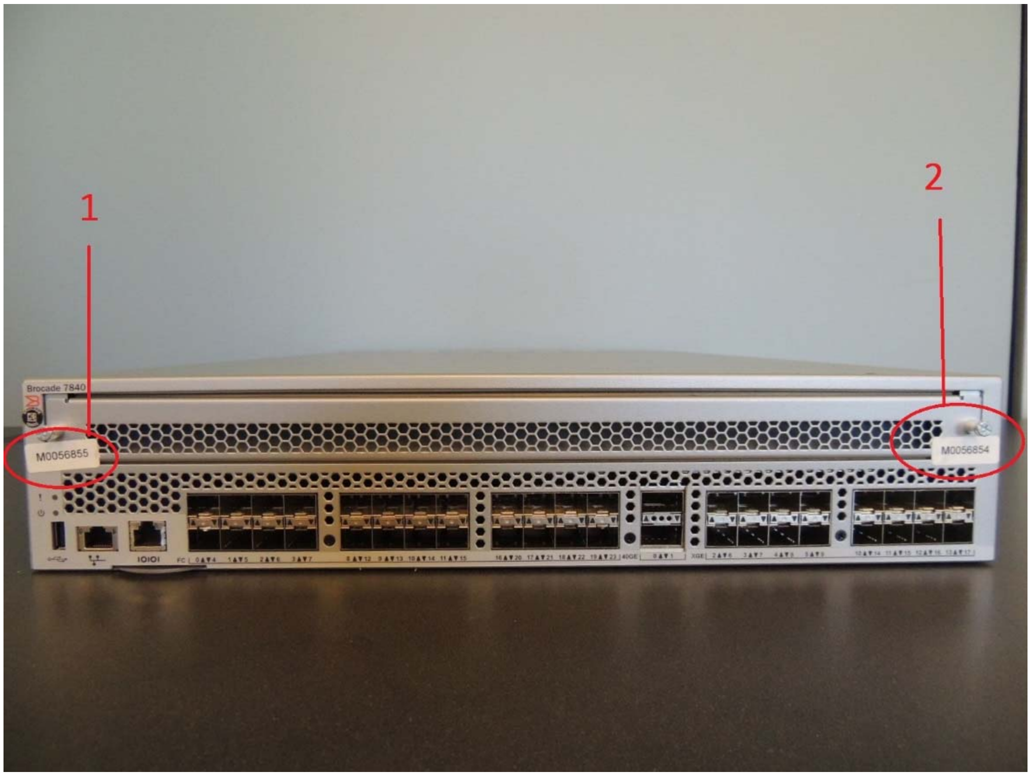

Figure 5 - Brocade 7840 front side seal locations

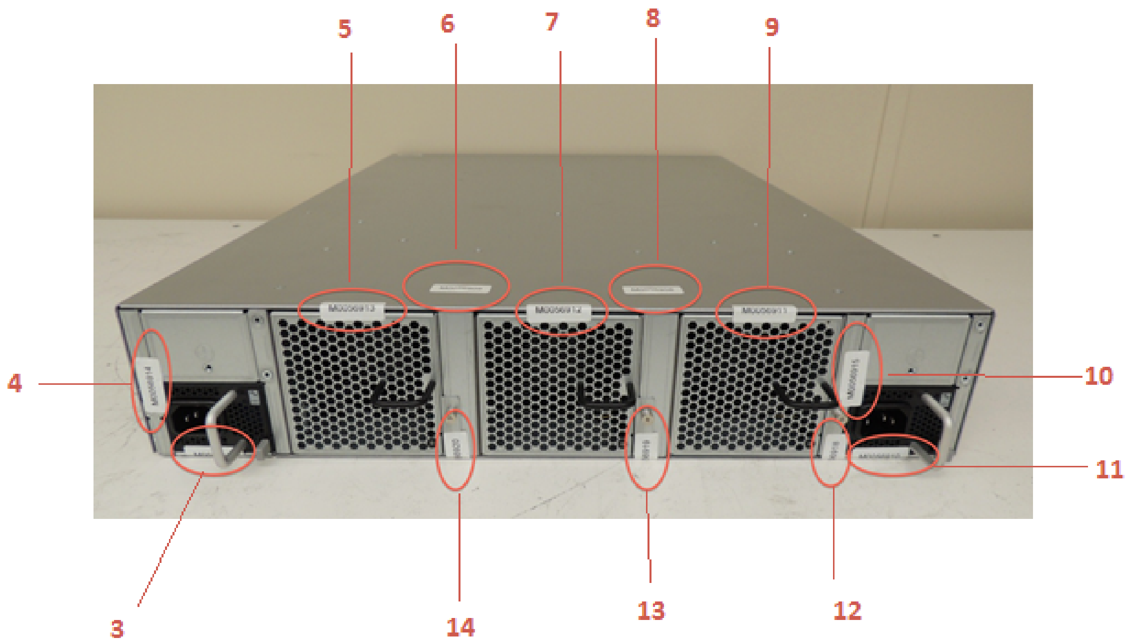

Figure 6 - Brocade 7840 back side seal locations

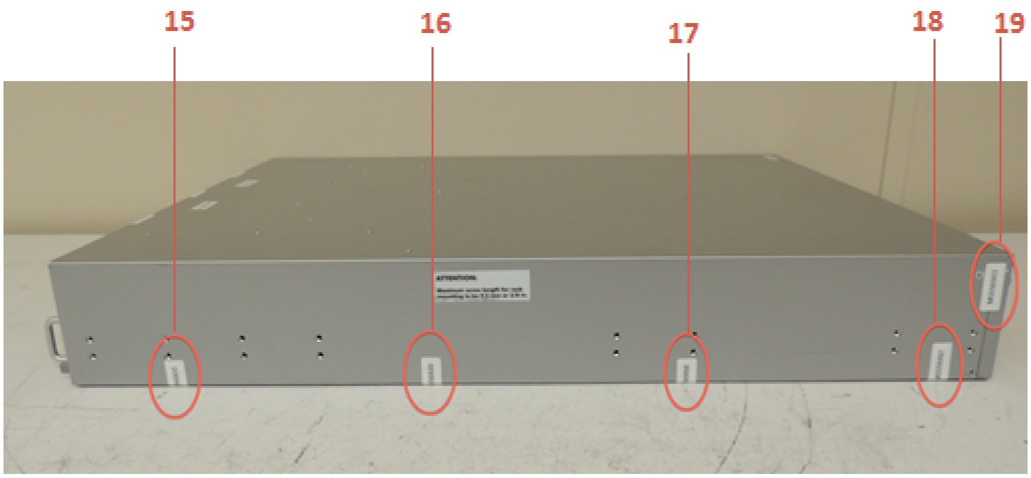

Figure 7 - Brocade 7840 left side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 8 - Brocade 7840 right side seal locations

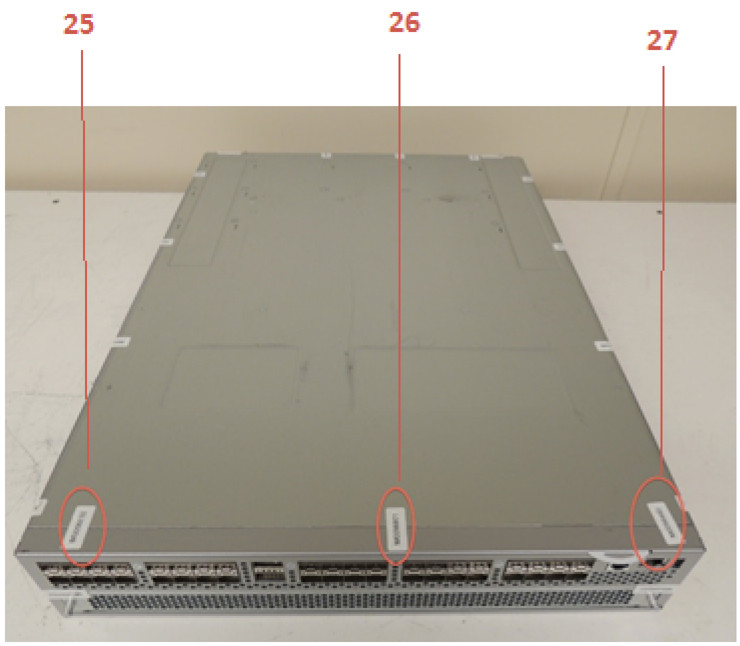

Figure 9 - Brocade 7840 bottom side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13 Appendix B: Block Diagram

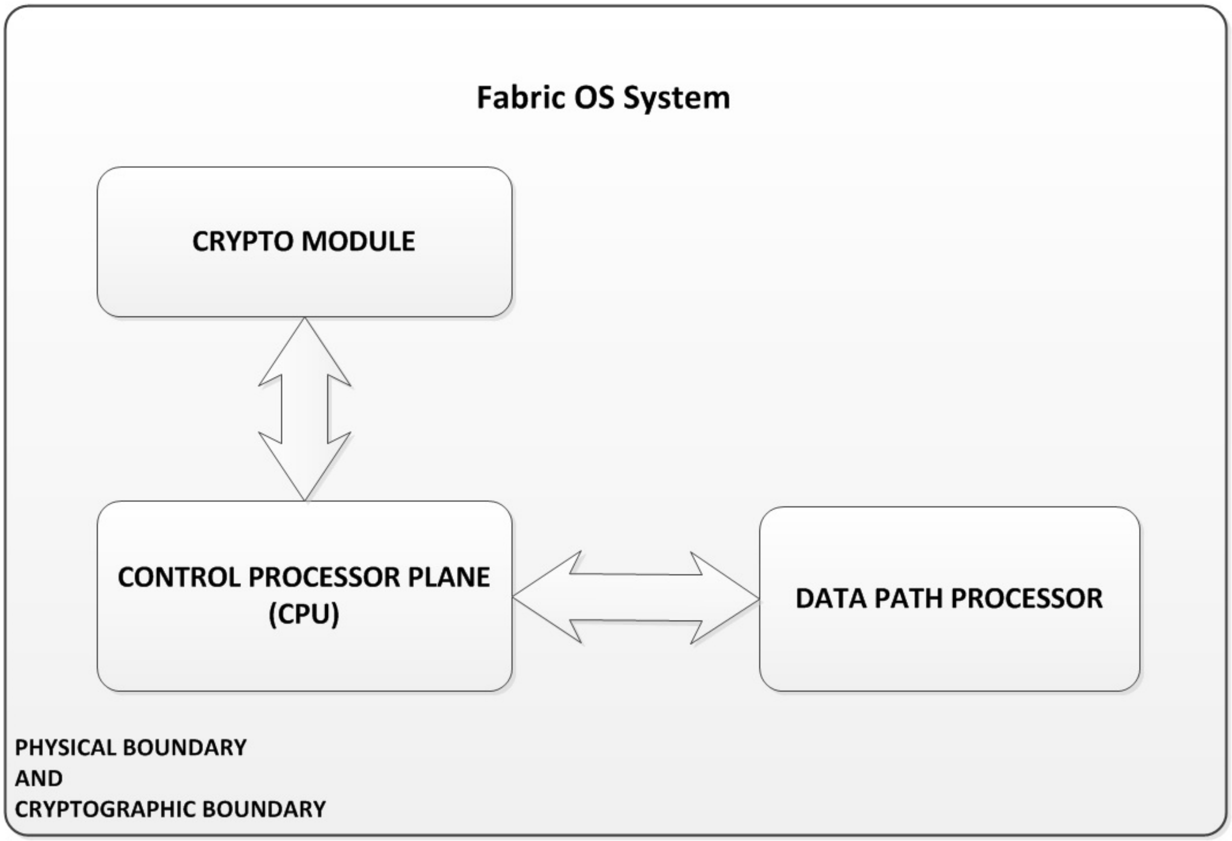

Figure 10 - Block Diagram

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

14 Appendix C: Critical Security Parameters and Public Keys

The module supports the following CSPs and Public Keys:

1. DH Private Keys for use with 2048 bit modulus
- Description: Used in SSHv2 to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination and "fipscfg --zeroize" command

2. SSHv2/SCP/SFTP Encryption Keys
- Description: AES (CBC or CTR mode) supporting 128, 192, and 256 Key sizes.
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg --zeroize" command

3. SSHv2/SCP/SFTP Authentication Key
- Description: HMAC-SHA-1 (160 bits), HMAC-SHA-256 and HMAC-SHA-512 Session authentication keys used to authenticate and provide integrity of SSHv2 session
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

4. SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

5. SSHv2 DH Shared Secret Key (2048 bit)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process

- Destruction: Session termination or "fipscfg -zeroize" command

6. SSHv2 ECDH Shared Secret Key (P-256)
- Description: Shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys
- Generation: N/A
- Establishment: SSHv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

7. SSHv2 ECDH Private Key (P-256)
- Description: ECDH private key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or performing the "fipscfg -zeroize" command

8. SSHv2 ECDSA Private Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

9. Value of K during SSHv2 P-256 ECDSA session
- Description: Used to generate keys that sign and verify
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

10. TLS Private Key (RSA 2048)
- Description: RSA key used to establish TLS sessions (decrypt padded TLS Pre-Master secret key block)
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: "fipscfg -zeroize" command

11. TLS Pre-Master Secret
- Description: 48-byte secret value used to establish the Session and Authentication key
- Generation: Approved SP800-90A DRBG

- Establishment: RSA key wrapped over TLS session; allowed as per FIPS 140-2 IG D.9
- Storage: Plaintext in RAM
- Entry: RSA key wrapped (after padding to block size) during TLS handshake
- Output: RSA key wrapped (after padding to block size) during TLS handshake
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

12. TLS Master Secret
- Description: 48 bytes secret value used to establish the Session and Authentication key
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

13. TLS KDF Internal State
- Description: Values of the KDF internal state.
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

14. TLS Session Keys - 128, 256 bit AES CBC
- Description: AES key used to secure TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination and "fipscfg -zeroize" command

15. TLS Authentication Key for HMAC-SHA-1 (160 bits) and HMAC-SHA-256
- Description: HMAC-SHA-1 or HMAC-SHA-256 key used to provide data authentication for TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination and "fipscfg -zeroize" command

16. CP DRBG Seed Material
- Description: Seed material for SP800-90A DRBG (AES-256-CTR DRBG)
- Generation: Internally generated; raw random data from NDRNG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

17. CP DRBG Internal State (V and Key)
- Description: SP800-90A DRBG (AES-256-CTR DRBG) Internal State
- Generation: SP800-90A DRBG seeded by raw random data from NDRNG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: "fipscfg -zeroize" command

18. Passwords
- Description: Password used to authenticate operators (8 to 40 characters)
- Generation: N/A
- Establishment: N/A
- Storage: MD5, SHA-256 or SHA-512 digest in Compact Flash (Plaintext)
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

19. RADIUS Secret
- Description: Used to authenticate the RADIUS Server (8 to 40 characters)
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: Encrypted/Authenticated over SSHv2 session
- Key-To-Entity: Process
- Destruction: "fipscfg -zeroize" command

20. DH Private Key (256 bits) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: IKEv2 KDF completion or session termination

21. DH Shared Secret (2048 bits) (Used in IKEv2)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H) used in in IKEv2.
- Generation: N/A
- Establishment: IKEv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: Session termination

22. IKEv2 AES-256 Encrypt/Decrypt Keys
- Description: Symmetric keys used for AES-256-CBC or AES-256-GCM encrypt/decrypt
- Generation: N/A
- Establishment: DH Key Agreement and IKEv2 KDF (SP800-135 Section 4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in Cavium key memory
- Entry: N/A
- Output: N/A

- Key-To-Entity: IKEv2 SA Number
- Destruction: Session termination

23. ESP AES-256-GCM Encrypt/Decrypt Keys
- Description: Symmetric keys used for AES-256-GCM encrypt/decrypt
- Generation: N/A
- Establishment: DH Key Agreement and IKEv2 KDF (SP800-135 Section 4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in Blitzer FPGA key memory
- Entry: N/A
- Output: N/A
- Key-To-Entity: ESP SA Number
- Destruction: Session termination

24. IKEv2 KDF State
- Description: Values of the IKEv2 KDF (HMAC-SHA-384 or HMAC-SHA-512) internal state
- Generation: N/A
- Establishment: IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: N/A
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SA control memory
- Destruction: Session termination

25. IKEv2 Authentication Key (PSK)
- Description: Pre-shared secret key used for IKEv2 session authentication (512 bits)
- Generation: N/A
- Establishment: Encrypted/authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9.
- Storage: Plaintext in RAM
- Entry: Encrypted/authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9.
- Output: N/A
- Key-To-Entity: IKEv2 SA control memory
- Destruction: Session termination

26. IKEv2 ECDH P-384 Private Key
- Description: Used in IKEv2 EC Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for elliptic curve is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: IKEv2 KDF completion or session termination

27. IKEv2 ECDSA P-384 Private Key
- Description: Used to authenticate IKEv2 Peer
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command or certificate/CSR deletion

28. IKEv2 Integrity Key (HMAC-SHA-384)
- Description: HMAC-SHA-384 key used to provide data integrity for IKEv2
- Generation: N/A
- Establishment: IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SA Number
- Destruction: Session termination

29. DRBG Internal State (V and Key) (On Cavium)
- Description: SP800-90A DRBG (AES-256-CTR DRBG) Internal State
- Generation: SP800-90A DRBG seeded by raw random data from NDRNG
- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: OpenSSL context per core
- Destruction: Session termination

30. Entropy Data (on Cavium)
- Description: Seed material for SP800-90A DRBG (AES-256-CTR DRBG)
- Generation: internally generated; raw random data from NDRNG
- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: Cavium Random Number Memory
- Destruction: DRBG Instantiation

31. SNMPv3 Auth and Priv password
- Description: Auth and Priv Password (8-32 bytes)
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM; Plaintext in Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

32. SNMPv3 KDF Internal State
- Description: SHA-1 Key Localization Function
- Generation: N/A
- Establishment: SNMPv3 KDF (SP800-135 Section 5.4); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

33. SNMPv3 Auth and Priv Secrets
- Description: Auth Secret 20-bytes (input to HMAC-SHA-1-96 function); Priv secret AES-128-CFB 128-bit key
- Generation: N/A
- Establishment: SNMPv3 KDF (SP800-135 Section 5.4); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM and Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

- - - - - - - - - - - - PUBLIC KEYS - - - - - - - - - - - -

34. DH Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2)

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User

35. DH Peer Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2)
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

36. TLS Public Key (RSA 2048)
- Description: Used by client to encrypt TLS Pre-Master Secret
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: User

37. TLS Peer Public Key (RSA 2048)
- Description: Used to authenticate the client
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

38. FW Download Public Key (RSA 2048)
- Description: Used to update the FW of the module.
- Generation: N/A; Generated outside the module
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: User

39. SSHv2 ECDSA Public Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: User

40. SSHv2 ECDSA Peer Public Key (P-256)
- Description: Used to authenticate SSHv2 client to server
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash

- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

41. LDAP ROOT CA certificate (RSA 2048)
- Description: Used to authenticate LDAP server
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: Process

42. RADIUS ROOT CA certificate (RSA 2048)
- Description: Used to authenticate RADIUS server
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: Process

43. DH Public Key (2048-bit) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: IKEv2 SPI

44. DH Peer Public Key (2048-bit) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: IKEv2 SPI

45. IKEv2 ECDH P-384 Public Key
- Description: Used in IKEv2 EC Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for elliptic curve is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: Plaintext
- Key-To-Entity: IKEv2 SPI

46. IKEv2 ECDH P-384 Peer Public Key
- Description: Used in IKEv2 EC Diffie-Hellman to establish a shared secret
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: IKEv2 SPI

47. IKEv2 ECDSA P-384 Public Key
- Description: Used for IKEv2 Authentication
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: User

48. IKEv2 ECDSA P-384 Peer Public Key
- Description: Used for IKEv2 Authentication
- Generation: N/A
- Establishment: N/A
- Storage: Plaintext in RAM and Plaintext in Compact Flash
- Entry: Plaintext
- Output: Plaintext
- Key-To-Entity: User

49. SSHv2 ECDH Public Key (P-256)
- Description: ECDH public key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM
- Key-To-Entity: Process

50. SSHv2 ECDH Peer Public Key (P-256)
- Description: ECDH public key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: Plaintext
- Output: N/A
- Storage: Plaintext in RAM
- Key-To-Entity: Process

15 Appendix D: CKG as per SP800-133

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated seed, for asymmetric key generation, is the unmodified output from SP800-90A DRBG. Please see section 14 - Appendix C: Critical Security Parameters and Public Keys for further details.