MOTOROLA

Motorola Network Router (MNR)
S2500
Security Policy

Document Version 2.4

Revision Date: 5/6/2011

TABLE OF CONTENTS

1. Module Overview

The MNR S2500 router, also referred to as the S2500, is a multi-chip standalone cryptographic module encased in a commercial grade metal case made of cold rolled steel. The module cryptographic boundary is the routers enclosure which includes all components, including the encryption module which is a separate part. Figure 1 illustrates the cryptographic boundary of the MNR S2500 router. In the photo, blank plates cover slots that can hold optional network interface cards that are external to the boundary of the module. The FIPS validated firmware version is XS-16.0.1.44

Configurations	S2500 Base Unit		S2500 Encryption Module		FW Version
	HW P/N	Revision	HW P/N	Revision	
	CLN1713F	Rev D	CLN8262C	Rev F	XS-16.0.1.44

Table 1. MNR S2500 Router Version Numbers

Previously Validated Versions – FIPS 140-2 Cert. #1014

S2500 Base Unit			S2500 Encryption Module			FW Versions
HW P/N	Tanapa Number	Revision	HW P/N	Tanapa Number	Revision	
ST2500B	CLN1713E	Rev B	ST2516A	CLN8262C	Rev C	XS-15.1.0.75, XS-15.1.0.76, XS-15.2.0.20, XS-15.4.0.60, XS-15.6.0.27 or XS-15.7.0.60

Table 2. MNR S2500 Versions from FIPS 140-2 Cert. #1014

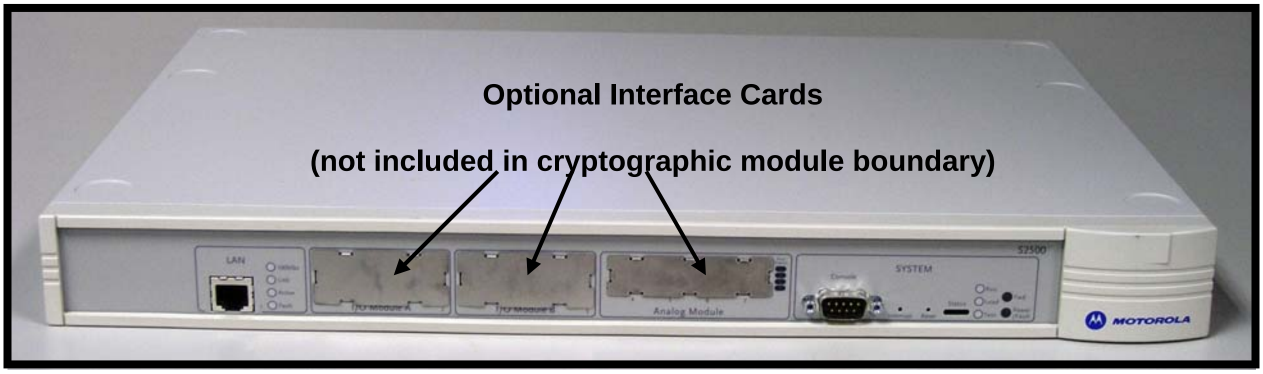

Figure 1 – MNR S2500 Router Cryptographic Module Boundary

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 3 – Module Security Level Specification

3. Modes of Operation

Approved mode of operation

In FIPS mode, the cryptographic module supports the following FIPS-Approved algorithms as follows:

Hardware Implementations

a. Triple-DES– CBC mode (112 or 168 bit) for IPsec and FRF.17 encryption (Cert. #588)

b. AES - CBC mode(128, 192, 256 bit) for IPsec and FRF.17 encryption (Cert. #625)

c. HMAC-SHA-1 for IPsec and FRF.17 authentication (Cert. #342)

d. SHA-1 for message hash (Cert. #693)

Firmware Implementations

a. Triple-DES– CBC mode (112 and 168 bit) for IKE and SSHv2 encryption (Cert. #581)

b. AES - CBC (128, 192, 256 bit), ECB (128), and CFB (128) modes for IKE and SSHv2 encryption (Cert. #611)

c. HMAC-SHA-1 for IKE and SSHv2 authentication (Cert. # 322)

d. SHA-1 for message hash (Cert. # 659)

e. RSA PKCS1 v1.5 1024 bit – for digital signatures (Cert. #283)

f. DSA 1024 bit – for public/private key pair generation and digital signatures (Cert. #237)

g. ANSI X9.31 Deterministic Random Number Generator (RNG) (Cert .#349)

The MNR S2500 router supports the commercially available IKE and Diffie-Hellman protocols for key establishment, IPsec (ESP) and FRF.17 protocols to provide data confidentiality using FIPS-approved encryption and authentication algorithms and SSHv2 for secure remote access.

Allowed Algorithms

- Diffie-Hellman: Groups 2, 5, and 14 (allowed for key agreement per Annex D, key agreement methodology provides 80 to 112 bits of encryption strength)
- Hardware non-deterministic RNG: Provides seed for approved deterministic RNG

Non-FIPS approved algorithms

In a Non FIPS mode of operation, the cryptographic module provides non-FIPS Approved algorithms as follows:

- DES for encryption/decryption
- Non approved SW RNG
- Diffie-Hellman (Group 1 - 768 bit)
- MD5: for hashing (Provides interoperability within supported protocols)
- HMAC-MD5

Entering FIPS Mode

To enter FIPS mode, the Crypto Officer must follow the procedure outlined in Table 3 below. For details on individual router commands, use the online help facility or review the *Enterprise OS Software User Guide* and the *Enterprise OS Software Reference Guide*.

Step	Description
1.	Configure the parameters for the IKE negotiations using the **IKEProfile** command. For FIPS mode, only the following values are allowed: Diffie-Hellman Group (Group 2 or Group 5), Encryption Algorithm (AES or 3DES), Hash Algorithm (SHA), and Authentication Method (PreSharedKey).
2.	Manually establish via the local console port the pre-shared key (PSK) to be used for the IKE protocol using: **ADD –CRYPTO FipsPreSharedKey <peer_ID> <pre-shared_key> <pre-shared_key>** The PSK must be at least 80 bits in length with at least 80 bits of entropy.
3.	Configure IPsec and FRF.17 selector lists using the command **ADD –CRYPTO SelectorLIst**
4.	If IPsec is used, configure IPsec transform lists using the **ADD –CRYPTO TransformLIst** command. For FIPS mode, only the following values are allowed: Encryption Transform (ESP-3DES, or ESP-AES) and Authentication Transform (ESP-SHA).
5.	If FRF.17 is used, configure FRF.17 transform lists using the **ADD –CRYPTO TransformLIst** command. For FIPS mode, only the following values are allowed: Encryption Transform (FRF-3DES, or FRF-AES) and Authentication Transform (FRF-SHA).
6.	For each port for which encryption is required, bind a dynamic policy to the ports using **ADD [!<portlist>] –CRYPTO DynamicPOLicy <policy_name> <priority> <mode> <selctrlist_name> <xfrmlist_name> [<pfs>] [<lifetime>] [<preconnect>]** To be in FIPS mode, the selector list and transform list names must be defined as in previous steps.
7.	For each port for which encryption is required, enable encryption on that port using **SETDefault [!<portlist>] –CRYPTO CONTrol = Enabled**
8.	DSA-2048 sized keys must not be used in FIPS mode. This implementation has not been tested.
9.	FIPS-140-2 mode achieved

Table 4 – FIPS Approved mode configuration

To review the cryptographic configuration of the router, use the following command:

SHOW –CRYPTO CONFiguration

This command shows a detailed summary of the cryptographic configuration and allows a user to verify that encryption is enabled on user-determined ports and that only FIPS-Approved algorithms are used for encryption and authentication.

Step 1: Look at the IKEProfile section of the cryptographic configuration summary output to verify that FIPS-approved algorithms have been selected for IKE negotiations (AES or DES for encryption, and SHA as the hash algorithm), Diffie-Hellman groups 2, 5 or 14 have been selected and that pre-shared key has been selected as the authentication method. Summary output should look similar to the following:

```
CRYPTO IKEProfile:
Priority  Authentication Method  Encrypt Alg  Hash Alg  DH Group  Lifetime

   1   PreSharedKey         AES/256     SHA      Group2   1 dy
   2   PreSharedKey         AES/256     SHA      Group2   1 dy
```

Step 2: For each port for which encryption is required, verify that the dynamic policy points to a transform list that uses FIPS-approved algorithms (AES or DES for encryption, and SHA as the hash algorithm), as shown in the following example:

```
CRYPTO DynamicPOLicy: dp1

 Priority:      1
 PortList:      !V1
 DpolCont:      Enabled
 Mode:          Tunnel
 Lifetime:      GlobalLifeTime (8 hr)
 PFS:           GlobalPFS (NoPFS)
 SelectorLIst:  s1
 TransformLIst: t1
 Preconnect:    Yes, Peer IP: 10.1.233.165

CRYPTO TransformLIst: t1            In use by 1 policy

   1  ESP-AES/256  ESP-SHA
```

In this example, the dynamic policy named dp1 points to a transform list t1. The transform list t1 uses FIPS-approved algorithms AES/256 and SHA.

Step 3. For each port for which encryption is required, look at the summary output to verify that encryption has been enabled on the required ports, as shown in the following example:

```
CRYPTO CONFiguration:
```

```
Port !V1    CONTrol = Enabled
Port !V102  CONTrol = Enabled
```

Upon successful completion of these three steps, the Crypto Officer has been shown the FIPS Mode Indicator and verified that the gateway is in FIPS mode.

4. Ports and Interfaces

Table 5 below provides a listing of the physical ports and logical interfaces for the MNR S2500 router.

The MNR S2500 base unit provides a single 10/100 Mbps Ethernet interface and a console port. The MNR S2500 router incorporates two I/O slots for WAN and LAN connectivity and one slot for analog connectivity. The optional LAN/WAN interface cards are not part of the validated module boundary.

Physical Port	Qty	Logical interface definition	Interface Card	Comments
Ethernet	1	Data input, data output, status output, control input	Part of the 2500 Base system	LAN port that provides connection to Ethernet LANs using either 10BASE-T or 100BASE-TX Ethernet
Console	1	Status output, control input	Part of the S2500 Base system	RS-232 interface
LAN/WAN	0, 1 or 2	Data input, data output, status output, control input, power output	Optional Ethernet and WAN interface cards	The interface to the cryptographic boundary is the interface card connector on the base module.
Analog	0, 1	Data input, data output, status output, control input, power output	Optional conventional-to-IP (E&M)	The interface to the cryptographic boundary is the interface card connector on the base module.
Power Plug	1	Power input	N/A	External Power input port
LEDs	7	Status Output	N.A	Provides LED status output on network traffic, power, and errors

Table 5 – S2500 physical ports and logical interfaces

5. Identification and Authentication Policy

Assumption of roles

The MNR S2500 router supports five distinct operator roles: Crypto Officer (SuperUser), Admin, Network Manager, User and Maintenance. The first four roles require user authentication via user name and password when accessing the router via any interface. The unauthenticated maintenance role is entered only via the router console port.

The MNR S2500 router enforces the separation of roles by providing specific services only to operators who have been authenticated to a role with the required privilege to access those services. The role-based authentication capabilities will be described here, although the role based-authentication is not required to comply with Level 1 requirements.

An operator must enter a username and his password to log in. Passwords are alphanumeric strings consisting of 7 to 15 characters chosen from the 94 standard keyboard characters. Upon correct authentication, the role is selected based on the username of the operator. At the end of a session, the operator must log-out.

When a router power cycles, sessions are terminated. A user must reauthenticate to access the router.

Multiple concurrent operators. Each operator has an independent session with the router, either though Telnet, SSH, or via the console. Once authenticated to a role, each operator can access only those services for that role. In this way, separation is maintained between the role and services allowed for each operator.

The definition of all supported roles is shown in Table 6 below.

Role	**Type of Authentication**	**Authentication Data**	**Description**
Crypto Officer (Super User)	Role-based operator authentication.	Username and Password. The module stores operator identity information internally,	The owner of the cryptographic module with full access to services of the module.
Network Manager	Role-based operator authentication.	Username and Password. The module stores user identity information internally.	A user of the cryptographic module with almost full access to services of the module.
Admin	Role-based operator authentication	Username and Password. The module stores user identity information internally.	An assistant to the Crypto Officer that has read only access to a subset of module configuration and status indications.
User	Role-based operator authentication	Username and Password. The module stores user identity information internally.	A user of the cryptographic module that has read only access to a subset of module configuration and status indications.
Maintenance	None (see comment)	N/A	Maintenance role can be entered via the external console port (unauthenticated) or via EOS software command (requires Network Manager authentication)

Table 6 – Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/94^7 which is less than 1/1,000,000. After three consecutive unsuccessful login attempts, a user is locked out for two minutes, ensuring that that the probability is less than one in 100,000 that random multiple attempts will succeed or a false acceptance will occur within any one minute period.

Table 7 – Strengths of Authentication Mechanisms

6. Access Control Policy

Authenticated Services

- Firmware Update: load firmware images digitally signed by RSA (1024 bit) algorithm.
- Key Entry: Enter Pre-Shared Keys (PSK)
- User Management: Add/Delete and manage operator passwords
- Reboot: force the module to power cycle via a command
- Zeroization: actively destroy all plaintext CSPs and keys
- Crypto Configuration: Configure IPsec and FRF.17 services
- IKE: Key establishment utilizing the IKE protocol
- IPsec tunnel establishment: IPsec protocol
- FRF.17 tunnel establishment: Frame Relay Privacy Protocol
- Alternating bypass: Provide some services *with* cryptographic processing and some services *without* cryptographic processing
- SSHv2 for remote access to the router
- Network configuration: Configure networking capabilities
- Enable Ports: Apply a security policy to a port
- File System: Access file system

- Authenticated Show status: Provide status to an authenticated operator
- Access Control: Provide access control for all operators

Unauthenticated Services:

- Unauthenticated Show status: provide the status of the cryptographic module – the status is shown using the LEDs on the front panel.
- Power-up Self-tests: execute the suite of self-tests required by FIPS 140-2 during power-up not requiring operator intervention.
- Conditional Self-tests: Execute the self-tests required by FIPS 140-2 when specified operational conditions occur
- Monitor: Perform various hardware support services.

Roles and Services

Service	**Crypto Officer (SuperUser)**	**Network Manager**	**User**	**Admin**	**Maintenance**
Firmware Update	X	X			
Key Entry	X	X			
User Management	X	X			
IKE	X	X			
IPsec Tunnel Establishment	X	X			
FRF.17 Tunnel Establishment	X	X			
SSHv2	X	X			
Reboot	X	X			
Zeroization	X	X			
Crypto Configuration	X	X			
Network Configuration	X	X			
Alternating Bypass	X	X			
Enable Ports	X	X			
File System	X	X			
Authenticated Show Status	X	X	X	X	
Unauthenticated Show Status	X	X	X	X	X
Power-up Self-Tests	X	X	X	X	X
Conditional Self-Tests	X	X	X	X	
Monitor	X				X
Access Control	X	X			

Table 8 – Services to Roles mapping

Definition of Critical Security Parameters (CSPs)

The following CSPs are contained within the module:

Key	Description/Usage
KEK	This is the master key that encrypts persistent CSPs stored within the module. KEK-protected keys include PSK and passwords. Encryption of keys uses AES128ECB
IKE Preshared Keys	Used to authenticate peer to peer during IKE session
SKEYID	Generated for IKE Phase 1 by hashing preshared keys with responder/receiver nonce
SKEYID_d	Phase 1 key used to derive keying material for IKE SAs
SKEYID_a	Key used for integrity and authentication of the phase 1 exchange
SKEYID_e	Key used for TDES or AES data encryption of phase 1 exchange
Ephemeral DH Phase-1 private key (a)	Generated for IKE Phase 1 key establishment
Ephemeral DH Phase-2 private key (a)	Phase 2 Diffie Hellman private keys used in PFS for key renewal
IPSEC Session keys	128/192/256-bit AES-CBC and 168-bit TDES keys are used to encrypt and authenticate IPSEC ESP packets
FRF.17 Session Keys	168-bit TDES-CBC and 128/192/256-bit AES-CBC keys are used to encrypt and authenticate FRF.17 Mode 2
SSH-RSA Private Key	Key used to authenticate oneself to peer
SSH-DSA Private Key	Key used to authenticate oneself to peer
SSH Session Keys	168-bit TDES-CBC and 128/192/256-bit AES-CBC keys are used to encrypt and authenticate SSH packets
SSH DH Private Key	Generated for SSH key establishment
RNG Seed	Initial seed for FIPS-approved deterministic RNG
RNG Seed Key	Initial seed key for FIPS-approved deterministic RNG
Network Manager Password (Root)	7 (to 15) character password used to authenticate to the CO Role (Crypto Officer)
Admin	7 (to 15) character password used to authenticate to the User Role
User Accounts	7 (to 15) character password used to authenticate accounts created on the module

Table 9 – Critical Security Parameters (CSPs)

Definition of Public Keys:

The following public keys are contained within the module:

Key	**Description/Usage**
RSA Firmware Load Key	Distributed to module, for firmware authentication
SSH-RSA Key	Distributed to peer, used for SSH authentication
SSH-DSA Key	Distributed to peer, used for SSH authentication
SSH Known Host Keys	Distributed to module, used to authenticate peer
IKE DH public key (g^a)	Generated for IKE Phase 1 key establishment
IKE DH phase-2 public (g^a) key	Phase 2 Diffie Hellman public keys used in PFS for key renewal (if configured)
SSH DH Key	Generated for SSH key establishment

Table 10 – Public Keys

Definition of CSPs Modes of Access

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read: the data item is read from memory.
- Write: the data item is written into memory.
- Zeroize: the data item is actively overwritten.

CSP	Firmware Update	Key entry	User Management	IKE	Ipsec tunnel establishment	FRF.17 tunnel establishment	SSH	Reboot	Zeroization	Crypto Configuration	Network Configuration	Enable Ports	File System	Authenticated Show Status	Monitor	Access Control
KEK			R					R	Z	R						
IKE Pre-shared Key		W		R					Z	W			RW	R		
SKEYID				RW				Z	Z							
SKEYID_d				RW					Z							
SKEYID_a				RW					Z							
SKEYID_e				RW					Z							
Ephemeral DH Phase-1 private key				RW					Z							
Ephemeral Phase-2 DH private key				RW					Z							
IPSEC Session Keys				RW	R				Z							
FRF.17 Session Keys				RW		R			Z							
SSH-RSA Private Key							RW		Z	RW						
SSH-DSA Private Key							RW		Z	RW						
SSH Session Keys							RW		Z							
SSH DH Private Key							RW		Z							
Root Password			RW						Z						RW	R
User(Admin)			RW						Z						RW	R
User Accounts			RW						Z							R
RNG Seed				RW					Z							
RNG Seed Key				RW					Z							

Table 11 – Services to CSP Access mapping

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the MNR S2500 router does not contain a modifiable operational environment.

8. Security Rules

The cryptographic module's design corresponds to the example cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The MNR S2500 router provides five distinct operator roles: Crypto Officer (SuperUser), Admin, Network Manager, User, and Maintenance. The Crypto Officer role uses the root account.
2. The MNR S2500 router encrypts message traffic using the AES or TDES algorithm, except in bypass mode.
3. The MNR S2500 router performs the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:

      Hardware Implementation:

      a. AES-CBC Known Answer Test

      b. TDES-CBC Known Answer Test

      c. HMAC-SHA-1 Known Answer Test (Includes SHA-1 KAT)

      Firmware Implementation

      a. AES-CBC Known Answer Test

      b. TDES-CBC Known Answer Test

      c. HMAC -SHA-1 Known Answer Test (Includes SHA-1 KAT)

      d. ANSI X9.31 RNG Known Answer Test

      e. RSA Known Answer Test

      f. DSA Known Answer Test

   2. Firmware Integrity Test (16 bit CRC)

B. Conditional Self-Tests:

a. Continuous Random Number Generator (RNG) test on FIPS-approved deterministic RNG and Hardware NDRNG.

b. Firmware load test – RSA signature verification of externally loaded code.

c. Alternating bypass tests – when enabling FRF.17 and IPsec encryption or configuring Selector Lists.

d. Pair-wise consistency test for public and private key establishment (RSA)

e. Manual key entry test

4. At any time the MNR S2500 router is in an idle state, the operator can command the router to perform the power-up self-test by power-cycling or rebooting the router.
5. Data output is inhibited during key generation, self-tests, zeroization, and error states.

6. To enter the alternating bypass state, the two required independent internal actions that are required are first, to configure the module for alternating bypass, and second, to verify the integrity of the configuration by running the alternating bypass test.

The operator can determine if bypass is activated by executing the following command:

“sh -cry conf”

Then verify that there are selector lists excluding specific traffic as follows:

```
SelectorLIst: s1            In use by 1 policy

   1  Action:       Exclude
      Filters:      UDP
      UDP Ports:      (49402,49402)
      Source IP:      0.0.0.0/0
      Destination IP: 0.0.0.0/0
```

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

9. Crypto Officer Guidance

The module is distributed to authorized operators wrapped in plastic with instructions on how to securely install the module. On initial installation, perform the following steps:

1. Power on the module and verify successful completion of power-up self tests from console port or inspection of log file. The following message will appear on the console interface: “power-on self-tests passed”.

2. Authenticate to the module using the default user acting as the Crypto Officer with the default password and username.
3. Verify that the Hardware and Firmware P/Ns and version numbers of the module are the FIPS approved versions.
4. Change the Network Manager (Crypto Officer) and User passwords using the **SysPassWord** command.
5. Initialize the Key Encryption Key (KEK) with the **KEKGenerate** command. Account passwords and certain keys are persistent across reboots and are encrypted with the Key Encryption Key (KEK). This key can be reinitialized at any time.
6. DSA-2048 sized keys must not be used in FIPS mode. This implementation has not been tested.

The module supports a minimum password length of 7 characters and a maximum length of 15 characters. The Crypto Officer controls the minimum password length through the **PwMinLength** parameter:
SETDefault -SYS PwMinLength = <length>, where **<length>** specifies the minimum length.

Before entering or exiting the Maintenance Role or non-FIPS mode, the operator shall use the Zeroization Service to zeroize all CSPs. The Zeroization Service should also be invoked prior to removing a router from service for repair.

10. Physical Security Policy

Physical Security Mechanisms

The MNR S2500 router is composed of industry standard production-grade components.

11. Mitigation of Other Attacks Policy

The module has not been designed to mitigate against other attacks outside the scope of FIPS 140-2.

12. Definitions and Acronyms

AES – Advanced Encryption Standard

CBC – Cipher Block Chaining

CLI – Command Line Interface

CSP – Critical Security Parameter

DH – Diffie-Hellman

FRF – Frame Relay Forum

FRF.17 – Frame Relay Privacy Implementation Agreement

FRPP – Frame Relay Privacy Protocol

HMAC – Hash Message Authentication Code

IKE – Internet Key Exchange

IP – Internet Protocol

IPsec – Internet Protocol Security

KAT – Known Answer Test

KDF – Key Derivation Function

KEK – Key Encrypting Key

MNR – Motorola Network Router

OSPF – Open Shortest Path First

PFS – Perfect Forward Secrecy

RNG – Random Number Generator

SHA – Secure Hash Algorithm

SSH – Secure Shell

SNMP – Simple Network Management Protocol

Tanapa - The part number that is built and stocked for customer orders.