ENTERASYS
NETWORKS™

XSR-1805, XSR-1850, and XSR-3250
(Hardware Version: REV 0A-G, Software Version: REL 6.3, Firmware Version: REL 6.3)

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation
Version 1.00

September 2003

Table of Contents

Introduction

Purpose

This document is a nonproprietary Cryptographic Module Security Policy for the Enterasys Networks XSR-1805, XSR-1850, and XSR-3250 appliances. This security policy describes how the XSR-1805, XSR-1850, and XSR-3250 meet the security requirements of FIPS 140-2 and how to run the modules in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST Web site at http://csrc.nist.gov/cryptval/.

The Enterasys Networks XSR-1805, XSR-1850, and XSR-3250 appliances are referenced in this document as X-Pedition Security Routers, XSR modules, and the modules. The XSR-1805 and XSR-1850 modules are also referenced as the XSR-18xx modules. The differences between the three modules are cited where appropriate.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

The Enterasys Networks Web site (http://www.enterasys.com/) contains information on all Enterasys Networks products.

The NIST Validated Modules Web site (http://csrc.ncsl.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

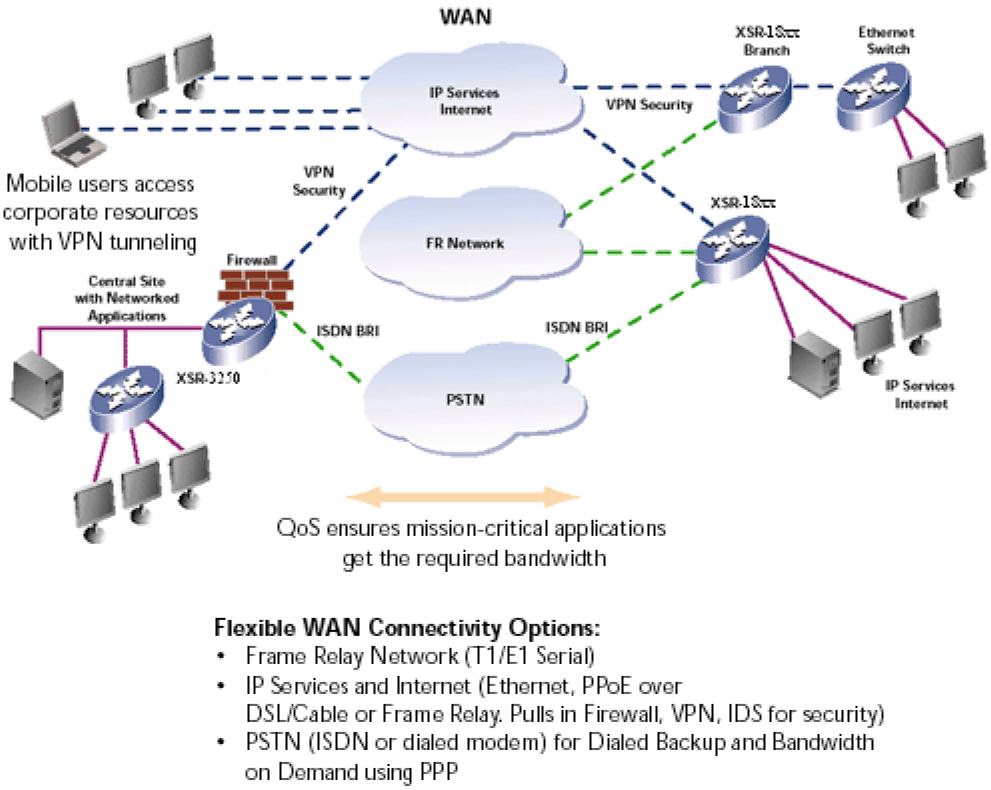
This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Enterasys Networks. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Enterasys Networks and can be released only under appropriate non-disclosure agreements. For access to these documents, please contact Enterasys Networks.

ENTERASYS NETWORKS XSR-1805, XSR-1850, AND XSR-3250

Overview

Part of the Enterasys Networks X-Pedition Security Router (XSR) series, the XSR-1805, XSR-1850, and XSR-3250 modules are networking devices that combine a broad range of IP routing features, a broad range of WAN interfaces and a rich suite of network security functions, including site-to-site and remote access VPN connectivity and policy managed, stateful-inspection firewall functionality.

The XSR-18xx modules were designed to meet the requirements of the branch office, while the XSR-3250 was specifically designed for the regional office. A typical deployment of the modules is shown in Figure 1 below.


WAN
XSR-18xx Branch
Ethernet Switch
IP Services Internet
VPN Security
Mobile users access corporate resources with VPN tunneling
VPN Security
FR Network
XSR-18xx
Firewall
Central Site with Networked Applications
ISDN BRI
ISDN BRI
XSR-3250
PSTN
IP Services Internet
QoS ensures mission-critical applications get the required bandwidth

Flexible WAN Connectivity Options:

- Frame Relay Network (T1/E1 Serial)
- IP Services and Internet (Ethernet, PPoE over DSL/Cable or Frame Relay. Pulls in Firewall, VPN, IDS for security)
- PSTN (ISDN or dialed modem) for Dialed Backup and Bandwidth on Demand using PPP

Figure 1 – Typical Deployment of the XSR Modules

The XSR-1805 is an entry-level, modular router in a desktop form factor delivering powerful performance and features to address the WAN, VPN, and firewall needs of remote offices.

The XSR-1850 varies mainly in its performance and type of enclosure, when compared to the XSR-1805. Delivering faster performance; a rack-mount form factor; and the option for redundant power, the XSR-1850 is ideal to support mission- critical applications extending to the branch office.

The XSR-3250 offers nearly ten times the performance speed of the XSR-1850 and approximately 15 times more VPN tunnels. Coupling these features with the six network interface module (NIM) slots makes the XSR-3250 ideally suited to a regional office required to terminate up to six T3/E3 or 24 T1/E1 connections. A redundant power supply is included.

The features of each XSR module are summarized in **Table 1**.

XSR Model	**XSR-1805**	**XSR-1850**	**XSR-3250**
NIM Slots	2	2	6
Fixed 10/100/1000 LAN Ports	2 10/100	2 10/100	3
Optional Gigabit Ethernet	N/A	N/A	Mini-GBIC
Redundant Power Supplies	No	Option	Standard
VPN Accelerator	Embedded	Embedded	Embedded
Flash Memory	8 MB (upgradeable)	8 MB (upgradeable)	8 MB
DRAM	32 MB (upgradeable)	64 MB (upgradeable)	256 MB (upgradeable)
External Compact Flash	Yes	Yes	Yes

Table 1 - Features At-a-Glance

Some highlighted security features of the XSR modules are:

- Telnet over IPSec or SSHv2-secured remote management of the modules
- Site-to-Site application VPN using IPSec
- Remote access VPN using L2TP over IPSec
- Access control through assigned privilege level
- User, certificate, and host key database files encrypted with a master encryption key

Cryptographic Module

The XSR modules were evaluated as multi-chip standalone cryptographic modules. The metal enclosure physically encloses the complete set of hardware and software components, and represents the cryptographic boundary of each module.

The hardware components for the XSR-18xx modules vary slightly to meet the performance level for each module. The XSR-1850 is an enhancement of the XSR-1805 consisting of the following additional features:

- Two fans
- External power source connector
- One PMC slot for PPMC card
- 19” 1.5 U rack-mount chassis
- 64 MB of DRAM

Due to the large difference in performance levels, the XSR-3250 hardware components vary quite significantly, when compared to the XSR-18xx modules. The main differences include the following:

- Different processor with two CPU cores
- Different hardware encryption accelerator
- Two extra NIM Carrier Cards (NCC) slots with two NIM slots on each card
- One extra Ethernet port connected to both a miniGBIC module and a RJ45 connector
- Dual load-sharing power supplies
- Redundant fans
- 256 MB of DRAM

XSR NIMs will operate on all three XSR modules.

All three modules use the software version XSR Release 6.3. The modules software components consists of three separate executables linked individually:

- Bootrom
- Power-up Diagnostics
- Software image

The software image is contained in a single file with the power-up diagnostics. It is based on the Nortel Open IP design model and runs on top of the VxWorks operating system.

The modules are intended to meet overall FIPS 140-2 Level 2 requirements (see Table 2).

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

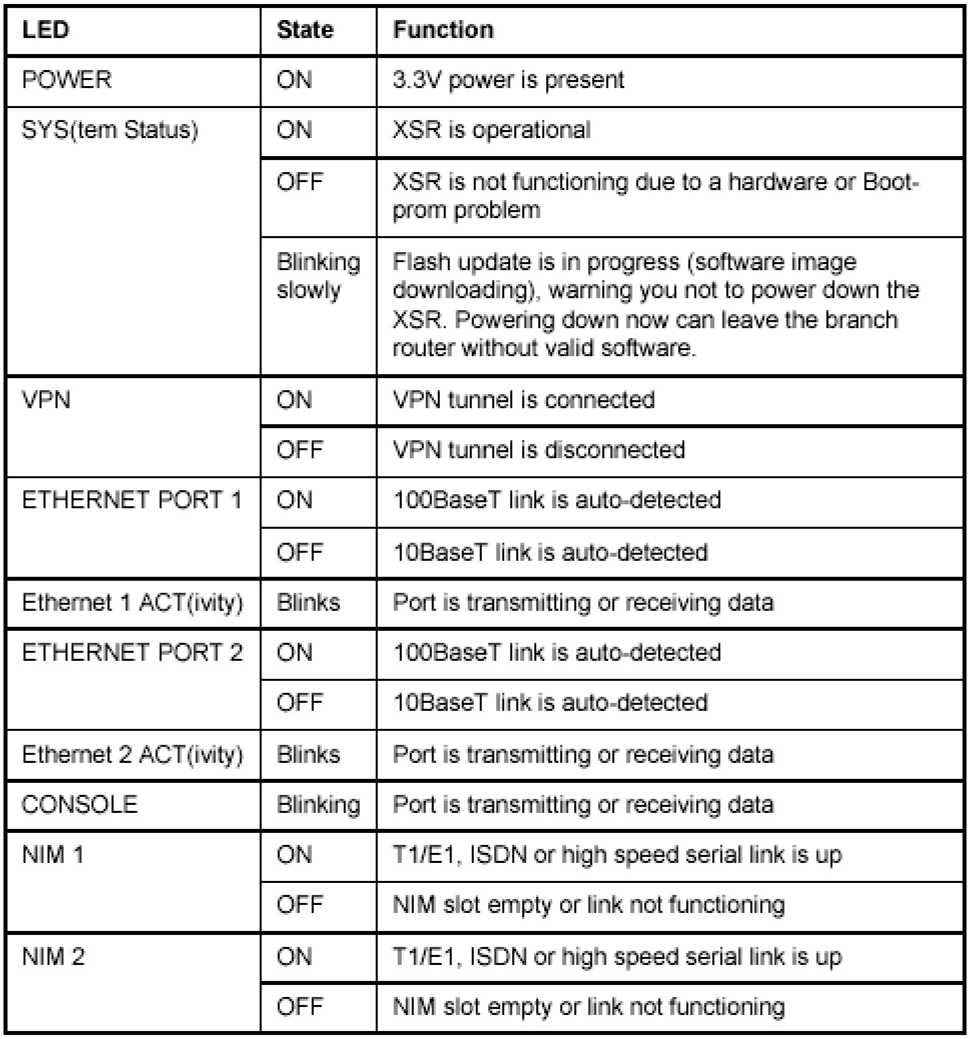
Table 2 – Intended Level Per FIPS 140-2 Section

Module Interfaces

The XSR-1805 provides a number of physical ports:

- Two 10/100BaseT FastEthernet LAN ports
- One console port
- Two PCM slots
- One PCMCIA slot for the optional CompactFlash card

- Ten status LEDs



LED	State	Function
POWER	ON	3.3V power is present
SYS(tem Status)	ON	XSR is operational
	OFF	XSR is not functioning due to a hardware or Boot-prom problem
	Blinking slowly	Flash update is in progress (software image downloading), warning you not to power down the XSR. Powering down now can leave the branch router without valid software.
VPN	ON	VPN tunnel is connected
	OFF	VPN tunnel is disconnected
ETHERNET PORT 1	ON	100BaseT link is auto-detected
	OFF	10BaseT link is auto-detected
Ethernet 1 ACT(ivity)	Blinks	Port is transmitting or receiving data
ETHERNET PORT 2	ON	100BaseT link is auto-detected
	OFF	10BaseT link is auto-detected
Ethernet 2 ACT(ivity)	Blinks	Port is transmitting or receiving data
CONSOLE	Blinking	Port is transmitting or receiving data
NIM 1	ON	T1/E1, ISDN or high speed serial link is up
	OFF	NIM slot empty or link not functioning
NIM 2	ON	T1/E1, ISDN or high speed serial link is up
	OFF	NIM slot empty or link not functioning

- One power connector
- One power switch
- One default configuration button

The XSR-1850 implements the same physical ports as the XSR-1805 and the following additional ones:

- External power source connector
- PPMC slot for Processor

The XSR-3250 varies to the XSR-1805 modules as follows:

- One additional power source connector

- Three 10/100/1000BaseT GigabitEthernet LAN ports with two LEDs on each port, instead of the two 10/100BaseT FastEthernet LAN ports

- Mini-Gigabit Interface Converter (MGBIC) fiberoptic port plus two LEDs

- Two NCC slots with two NIM slots on each card

- No power switch

- No default configuration button

All of these physical ports are separated into logical interfaces defined by FIPS 140-2, as described in Table 3:

Module Physical Ports	FIPS 140-2 Logical Interface
Network ports	Data input interface
Network ports	Data output interface
Network ports, console port, power switch (XSR-18xx only), default button (XSR-18xx only)	Control input interface
Network ports, console port, LEDs	Status output interface
Power connector(s)	Power interface

Table 3 – FIPS 140-2 Logical Interfaces

Data input and output, control input, and status output are defined as follows:

- Data input and output are the packets that use the firewall, VPN, and routing functionalities of the modules.

- Control input consists of manual control inputs for power and reset through the power and reset switch. It also consists of all of the data that is entered into the module while using the management interfaces.

- Status output consists of the status indicators displayed through the LEDs and the status data that is output from the modules while using the management interfaces.

The modules distinguish between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

Roles and Services

The module supports role-based and identity-based authentication[1]. There are two main roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and User role.

Crypto Officer Role

The Crypto Officer role has the ability to configure, manage, and monitor the module. Three management interfaces can be used for this purpose:

- CLI – The Crypto Officer can use the CLI to perform non-security-sensitive and security-sensitive monitoring and configuration. The CLI can be accessed locally by using the console port or remotely by using Telnet over IPSec or the SSHv2 secured management session.

- SNMP – The Crypto Officer can use SNMPv3 to remotely perform non-security-sensitive monitoring and configuration.

- Bootrom Monitor Mode – In Bootrom monitor mode, the Crypto Officer can reboot, update the Bootrom, issue file system-related commands, modify network parameters, and issue various *show* commands. The Crypto Officer can only enter this mode by pressing the key combination CTRL-C during the first five seconds of initialization. It can also be entered if Bootrom cannot find a valid software file.

Due to the different privilege levels (0-15) that can be assigned to each user, the Crypto Officer role can be split into different types of management users:

- Super Crypto Officer – Management users with a privilege level of 15 assume the Super Crypto Officer role. Since 15 is the highest privilege level available, the Super Crypto Officer can issue all the configuration and monitoring commands available through the CLI and SNMP. Only the Super Crypto Officer can enter Bootrom monitor mode.

- Junior Crypto Officer – Management users with a privilege level of 10 assume the Junior Crypto Officer role. The Junior Crypto Officer can issue all monitoring commands with higher security level and some configuration commands. Examples of commands are: *show running-config* and *show interfaces*, and all SNMP *show* commands.

[1] Please note that overall the modules meet the level 2 requirements for Roles and Services.

- Read-only Crypto Officer – Management users with privilege level zero assume the Read-only Crypto Officer role. The Read-only Crypto Officer can only issue monitoring commands with low security level. Examples of commands are: *show version* and *show clock*.

Descriptions of the services available to the Crypto Officer role are provided in the table below.

Service	**Description**	**Input**	**Output**	**Critical Security Parameter (CSP) Access**
SSH	Provide authenticated and encrypted remote management sessions while using the CLI	SSH key agreement parameters, SSH inputs, and data	SSH outputs and data	DSA (SSHv2) host key pair (read access), Diffie-Hellman key pair (read/write access), session key for SSH (read/write access), PRNG keys (read access); Crypto Officer's password (read access)
IKE/IPSec	Provide authenticated and encrypted remote management sessions while using Telnet to access the CLI functionality	IKE inputs and data; IPSec inputs, commands, and data	IKE outputs, status, and data; IPSec outputs, status, and data	RSA key pair for IKE (read access), Diffie-Hellman key pair for IKE (read/write access), pre-shared keys for IKE (read access); Session keys for IPSec (read/write access)
SNMP	Non-security-sensitive monitoring and configuration using SNMPv3 (with standard MIB-II and proprietary MIB support)	Commands and configuration data	Status of commands, configuration data	Crypto Officer's SNMP password (read/write access)
Bootrom Monitor Mode	Reboot, update the Bootrom, issue file system-related commands, modify network parameters, and issue various show commands	Commands and configuration data	Status of commands, configuration data	Crypto Officer's Bootrom password (read/write access)
Configuring Network	Create or specify master encryption	Commands and configuration data	Status of commands and	Master encryption key (read/write

Management	key; create DSA host key for SSHv2; create management users and set their password and privilege level; configure the SNMP agent		configuration data	access), DSA host key pair (read/write access), Crypto Officer's password for CLI and SNMP (read/write access)
Configuring the T1/E1 Subsystem Interfaces	Define the T1/E1 subsystem functionality	Commands and configuration data	Status of commands and configuration data	None
Configuring the XSR Platform	Define the platform subsystem software of the module by entering Bootrom Monitor Mode, File System, fault report, message logging, and other platform related commands	Commands and configuration data	Status of commands and configuration data	None
Configuring Hardware Controllers	Define synchronization features for module	Commands and configuration data	Status of commands and configuration data	None
Configuring the Internet Protocol	Set IP functionality	Commands and configuration data	Status of commands and configuration data	None
Configuring Frame Relay	Define Frame Relay interface features	Commands and configuration data	Status of commands and configuration data	None
Configuring ISDN	Configure BRI/PRI functionality on module	Commands and configuration data	Status of commands and configuration data	None
Configuring Quality of Service (QOS)	Configure QOS values for module	Commands and configuration data	Status of commands and configuration data	None
Configuring the VPN	Configure Public Key Infrastructure (PKI); configure the Internet Key Exchange (IKE) Security Protocol; configure the IPSec protocol	Commands and configuration data	Status of commands and configuration data	RSA keys pair (read/write access), Preshared key (read/write access)
Configuring DHCP	Configure DHCP on module	Commands and configuration data	Status of commands and configuration data	None
Configuring Security	Define security features for module, including Access List, AAA, and firewall functionality	Commands and configuration data	Status of commands and configuration data	AAA user password (read/write access), RADIUS password (read/write access)
Configuring	Define the	Commands and	Status of	None.

Firewall	authorization information for network traffic that flows through the box.	configuration data.	commands and configuration data.	

Table 4 – Crypto Officer Services, Descriptions, Inputs and Outputs, and CSPs

User Role

The User role accesses the module's IPSec and IKE services. Service descriptions, inputs and outputs, and CSPs are listed in the following table:

Service	Description	Input	Output	CSP
IKE	Access the module IKE functionality to authenticate to the module and negotiate IKE and IPSec session keys	IKE inputs and data	IKE outputs, status, and data	RSA key pair for IKE (read access); Diffie-Hellman key pair for IKE (read and write access); pre-shared keys for IKE (read access)
IPSec	Access the module's IPSec services in order to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	Session keys for IPSec (read and write access)

Table 5 – User Services, Descriptions, Inputs and Outputs

Authentication Mechanisms

The module supports role-based and identity-based authentication. Role-based authentication is performed before the Super Crypto Officer enters Bootrom monitor mode and authenticates with just a password (and no user ID). Identity-based authentication is performed for all other types of Crypto Officer and User authentication. These include password-based authentication, RSA-based authentication, and HMAC-based authentication mechanisms.

The estimated strength of each authentication mechanism is described below.

Authentication Type	Role	Strength
Password-based authentication (CLI, SNMP, and Bootrom monitor mode)	Crypto Officer	Passwords are required to be at least six characters long. Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used, which gives a total of 95 characters to choose from. Considering only the case-insensitive alphabet using a password with repetition, the number of potential passwords is 26^6.
RSA-based authentication (IKE)	User	RSA signing and verification is used to authenticate to the module during IKE. This

		mechanism is as strong as the RSA algorithm using a 1024 bit key pair.
Pre-shared key-based authentication (IKE)	User	HMAC SHA-1 generation and verification is used to authenticate to the module during IKE with preshared keys. This mechanism is as strong as the HMAC with SHA-1 algorithm. Additionally, preshared keys must be at least six characters long. Even if only uppercase letters were used without repetition for a six character preshared key, the probability of randomly guessing the correct sequence is one in 165,765,600.

Table 6 – Estimated Strength of Authentication Mechanisms

The firewall mechanism can only be configured by the Crypto-Officer who authorizes the traffic that flows through the module.

Physical Security

The XSR modules are multi-chip standalone cryptographic modules, which were tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules.

The modules are entirely contained within hard metal enclosures. The enclosure is resistant to probing and is opaque within the visible spectrum. The enclosures have been designed to satisfy level 2 physical security requirements. The ventilation holes on all three modules have been designed with baffling and less than 1/16th an inch diameter. Additionally, for the XSR-1850 and the XSR-3250, as soon as a cover (top or bottom) is removed, the nonvolatile RAM of the Real Time Clock chip is cleared, causing the master encryption key, which is used to encrypt user, certificate, and host key database files, to be zeroized.

All three modules require tamper-evident labels to be applied to protect and to notify of any tampering with the modules. Depending on whether the NIM slots are used, the XSR-1805 requires a minimum of seven and a maximum of nine labels to be applied, the XSR-1850 requires a minimum of five and a maximum of seven labels, and the XSR-3250 requires a minimum of four and a maximum of six labels. The labels are employed by the Crypto Officer as described in the *Installation Guide: Attaching XSR Security Labels*.

Operational Environment

The operational environment requirements do not apply to these modules. The XSR modules do not provide a general-purpose operating system, but rather a non-modifiable and embedded operating system.

Cryptographic Key Management

The modules implement the following FIPS-approved algorithms:

Type	Algorithm	Standard	Certificate Number
Symmetric	AES (CBC)	FIPS 197	Cert. #48, #106, #107
	Triple-DES (CBC and ECB)	FIPS 46-3	Cert. #158, #218, #219, #220
	DES (CBC)	FIPS 46-3	Cert. #204, #238, #239, #240
Asymmetric	DSA	FIPS 186-2 Change Notice 1	Cert. #97
	RSA Digital Signature	PKCS #1	Vendor affirmed
Hash function	SHA-1	FIPS 180-1	Cert. #143, #197, #198, #199
MAC	HMAC SHA-1	FIPS 198	Cert. #143, #197, #198, #199; vendor affirmed
PRNG	Appendix 3.1 (Algorithm 1) for computing DSA keys Appendix 3.1 for general purpose	FIPS 186-2 Change Notice 1	N/A

Table 7 – FIPS-Approved Algorithm supported by the Module

Note: DES should be used for legacy purposes only.

The modules implement the following non-FIPS-approved algorithms:

- HMAC MD5
- MD5
- MD4
- 40-bit and 128-bit RC4
- CAST
- Blowfish
- Twofish
- ARCfour
- Diffie-Hellman (permitted for use in a FIPS-approved mode of operation)

Cryptographic algorithms are implemented in software and in hardware by the encryption accelerators. The encryption accelerators implement the following FIPS-approved algorithms:

- XSR-18xx – Triple-DES, DES, and HMAC SHA-1
- XSR-3250 – AES, Triple-DES, DES, and HMAC SHA-1

Cryptographic processing is performed during SSHv2, SNMPv3, IKE, IPSec, and when accessing and storing database files.

The module supports the following critical and non-critical security parameters:

CSPs and non-critical SPs	CSPs and non-critical SPs type	Generation	Storage	Use
Key encryption key	168-bit TDES key	External	Hard-coded in plaintext	Encrypts master encryption key
Master encryption key	168-bit TDES key	Internal – using FIPS 186-2 PRNG Or External	Stored encrypted in NVRAM of the Dallas DS1687 real time clock chip	Encrypts user data, certificates, and DSA host key, and the load test HMAC SHA-1 key
DSA host key pair	160-bit DSA private key and 1024-bit DSA public key	Internal – using FIPS 186-2 PRNG	Stored encrypted in Flash	Module authentication during SSHv2
IKE RSA key pair	1024-bit RSA private/public key pair	Internal – using FIPS 186-2 PRNG	Stored encrypted in Flash	Module authentication during IKE
IKE User RSA public keys	1024-bit RSA public key	External	Stored encrypted in Flash	User authentication during IKE
Pre-shared keys	≥ 6-character pre-shared key	External	Stored encrypted in Flash	User and module authentication during IKE
IKE Diffie-Hellman key pair	768/1024/1536-bit Diffie-Hellman private/public key pair	Internal – using FIPS 186-2 PRNG	Stored in plaintext in memory	Key agreement during IKE
IKE User Diffie-Hellman public key	768/1024/1536-bit Diffie-Hellman public key	External	Stored in plaintext in memory	Key agreement during IKE
SSHv2 Diffie-Hellman key pair	768/1024/1536-bit Diffie-Hellman private/public key pair	Internal – using FIPS 186-2 PRNG	Stored in plaintext in memory	Key agreement during SSHv2
SSHv2 User Diffie-Hellman public key	768/1024/1536-bit Diffie-Hellman public key	External	Stored in plaintext in memory	Key agreement during SSHv2
SSHv2 session keys	168-bit TDES or 128/192/256-bit AES keys; HMAC SHA-1 keys	Established during the SSH key exchange using the Diffie-Hellman key agreement	Stored in plaintext in memory	Secure SSH traffic

IPSec session keys	56-bit DES, 168-bit TDES, or 128/192/256-bit AES keys; HMAC SHA-1 key	Established during the Diffie-Hellman key agreement	Stored in plaintext in memory	Secure IPSec traffic
Load test HMAC SHA-1 key	≥ 80-bit HMAC SHA-1 key	External	Stored encrypted in NVRAM of the real time clock chip	Compute and verify the HMAC SHA-1 value for the software load test
Passwords	≥ 6-character password (SNMPv3 requires at least 8 characters)	External	If stored in configuration file, passwords are stored in plaintext in Flash; if stored in user.dat, passwords are stored encrypted in Flash; Bootrom passwords are stored in plaintext in NVRAM of the real time clock	Crypto Officer authentication for accessing the management interfaces (CLI, SNMPv3, and Bootrom Moniot Mode), RADIUS authentication

Table 8 – Listing CSPs for the Module

Key Generation

The RSA key pair used during IKE, the DSA host key pair used during SSHv2, and the Diffie-Hellman key pairs used during IPSec and SSHv2 are all generated within the module. Additionally, each module gives the option to generate the 3-key Triple-DES master encryption key within the module. All keys that are generated within a module are generated using a FIPS-approved PRNG.

Key Establishment

The modules implement SSHv2 and IKE for automatic key establishment. These protocols implement the Diffie-Hellman key agreement to establish shared secrets.

Key Entry and Output

Three types of secret keys can be entered in plaintext form into the modules: the master encryption key, pre-shared keys, and the load test HMAC SHA-1 key. The master encryption key can either be specified or generated within the module. Pre-shared keys, if chosen as the authentication method for IKE, must always be entered into the module by the Crypto Officer. The HMAC SHA-1 key must be entered into the module before a valid software file is loaded into the module.
The three keys are entered electronically if the SSH or the Telnet over IPSec secured remote session is used or manually if the module is accessed locally through the console port. When these keys are manually entered, a manual key entry test is performed.

If the master encryption key is generated within the module, the module outputs the key to the console as soon as the key is generated in order for the Crypto Officer to note down and store the key securely outside of the module. This is required, since the Crypto Officer must enter the current key before changing or removing it. The master secret key can only be configured through the serial console or over an SSH tunnel.

Key Storage

The three-key Triple-DES key encryption key used to encrypt the master encryption key is hard-coded in plaintext form. The master encryption key is stored encrypted in the extended NVRAM of the Real Time Clock chip. This 3-key Triple-DES key is used to encrypt the user data, certificates, and host key database files (user.dat, cert.dat and hostkey.dat) stored in Flash. Hostkey.dat contains the DSA host key pair, cert.dat contains the certificates (including the module's RSA key pair), and user.dat contains all other CSPs set for the users (pre-shared keys and passwords).
The master encryption key is also used to encrypt the load test HMAC SHA-1 key, which is also stored in the NVRAM of the Real Time Clock chip.

The CLI passwords are stored in plaintext form in the startup-config file in Flash. The SNMP passwords are stored in plaintext form in the private-config file in Flash. The Bootrom password is stored in NVRAM of the Real Time Clock.

Session keys are stored in plaintext form in RAM.

Key Zeroization

The CSPs contained within the database files and the load test HMAC SHA-1 key do not need to be zeroized, since they are encrypted with the master encryption key. The master encryption key can be zeroized by either overwriting the key with a new one, removing it through the CLI, or by pressing the default configuration button (XSR-18xx only) or entering the bootrom password incorrectly five times (XSR-3250). Pressing this button reboots the module and enforces default configuration. The hard-coded key encryption key used to encrypt the master encryption key can be zeroized by formatting the Flash file system or CompactFlash card.

Passwords can be zeroized by overwriting them with new ones or by pressing the default configuration button (XSR-18xx only).

Session keys can be zeroized by rebooting the module.

Self-Tests

The module performs a set of self-tests in order to ensure proper operation in compliance with FIPS 140-2. These self-tests are run during power-up (power-up self-tests) or when certain conditions are met (conditional self-tests).

Power-up Self-tests:

- Software integrity tests: the modules use an EDC, in the form of an MD5 checksum, to check the integrity of its various components
- Cryptographic algorithm tests:
    - AES-CBC KAT
    - DES-CBC KAT
    - Triple-DES-CBC KAT
    - PRNG KAT
    - RSA pair-wise consistency test (signing and verification)
    - DSA pair-wise consistency test
    - SHA-1 KAT
    - HMAC SHA-1 KAT
- Bypass mode test: the module performs SHA-1 check value verification to ensure that the IPSec policies are not modified.
- Software load test: the module uses HMAC SHA-1 to check the validity of the software. Only validated software can be loaded into the modules.
- Critical function test: during cold boot, the module performs power-up diagnostics to verify the functionality of installed hardware (memory and interfaces).

Conditional Self-tests:

- RSA pair-wise consistency test: this test is performed when RSA keys are generated for IKE.
- DSA pair-wise consistency test: this test is performed when DSA keys are generated for SSHv2.

- Continuous random number generator test: this test is constantly run to detect failure of the random number generator of the module.

- Manual key entry test: when entering a pre-shared key, master encryption key, or load test HMAC SHA-1 key, the module performs the manual key entry test by requesting the Crypto Officer to enter the key in twice.

- Software load test: the module uses HMAC SHA-1 to check the validity of the software. Only validated software can be loaded into the modules.

- Bypass mode test: the module performs SHA-1 check value verification to ensure that the policy files are not modified.

If any of the power-up self-tests fail (excluding the interface diagnostic tests), the module enters the Critical Error state and reboots. When the power-up software load test fails, the module enters the Critical Error state, rather than rebooting the module deletes the invalid software file and enters the Bootrom Monitor Mode state.
If any of the conditional self-tests fail (except for the continuous RNG test and the bypass mode test), the module enters the Non-Critical Error state. All cryptographic processing and data output for the problem service is halted until the error state is cleared by the Crypto Officer. If the continuous RNG test or the conditional bypass mode test fails, the module will enter the Critical Error state and reboot.

When the module fails a power-up or conditional self-test, it will output an error indicator via the console port.

Design Assurance

Source code and associated documentation files are managed and recorded by using the configuration management tool ClearCase.

The Enterasys hardware data, which includes Description, Part Data, Part Type, BOM, Manufacturers, Changes, History, and hardware documents are managed and recorded using Agile Workplace.

The FIPS documentation were managed and recorded by using Microsoft Visual Source Safe version 6.0.

Mitigation of Other Attacks

The modules do not employ security mechanisms to mitigate specific attacks.

SECURE OPERATION

The XSR modules meet level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-approved mode of operation. The Crypto Officer must ensure that the module is kept in a FIPS-approved mode of operation. The procedures are described in “Crypto Officer Guidance”.
The User can use the module after the Crypto Officer changes the mode of operation to FIPS mode. The secure operation for the User is described in “User Guidance” on page 24.

Crypto Officer Guidance

The secure operation procedures for the Crypto Officer are covered in the initial setup and Management section. Following these procedures ensure that the module runs in a FIPS-compliant manner.

Initial Setup

The Crypto Officer receives the module in a carton. Within the carton the module is placed inside an ESD bag. The Crypto Officer should examine the carton and the ESD bag for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

Since the module does not enforce an access control mechanism before it is initialized, the Crypto Officer must maintain control of the module at all times until the initial setup is complete.

Before turning on the module, the Crypto Officer must ensure that the module meets level 2 physical security requirements. To satisfy these requirements, the Crypto Officer must apply the tamper-evident labels provided in the FIPS kit. The *Installation Guide: Attaching XSR Security Labels* detail how the labels must be applied to each module.

After all the labels are in place, the Crypto Officer can open a Console session to the XSR using Microsoft’s HyperTerminal, Procomm or other program. The session properties must be set as follows: BPS – 9600, Data bits – 8, Parity – none, Stop bits – 1, Flow control – none.

Setting Passwords

During the first five seconds of initialization, the Crypto Officer must press the key combination CTRL-C to enter Bootrom monitor mode. After the Crypto Officer accesses the mode, the Crypto Officer must set the at least six character long Bootrom password.

To set the Bootrom password

1. Enter **bp**

2. At the prompt <Enter current password: >, press Enter.

3. At the prompt <Enter new password: >, enter the password.

4. At the prompt <Re-enter new password: >, re-enter the password.

5. At the prompt, enter **bc** for cold boot.

The Crypto Officer must now set the at least six character long CLI password.

To set the CLI password

1. When the XSR login appears, enter **admin** and enter no (blank) password.

2. At the CLI prompt, enter **enable** to acquire Privileged EXEC mode.

3. Enter **configure** to acquire Global mode.

4. Enter **username** <*Super Crypto Officer name*> **privilege 15 password secret 0** <password>.

5. Enter **exit**.

6. Enter **copy running-config startup-config**.

7. At the prompt, enter **y**.

If the Super Crypto Officer name is not *admin*, the Super Crypto Officer must log into the newly created account and delete the *admin* user.

After setting the Bootrom and CLI passwords, the Crypto Officer can configure the LAN ports and activate SSH to enable the remote management of the module. For directions, refer to the *XSR Quick Start Guide, XSR Getting Started Guide, XSR User's Guide,* and the *CLI Reference Guide*.

Management

The Crypto Officer must ensure that the module is always operating in a FIPS-approved mode of operation. This can be achieved by ensuring the following:

- Passwords must be at least six characters long.

- Telnet access must be disabled unless used over IPSec.

- Dial backup access must be disabled.
- Syslog remote logging must be disabled.
- VPN services can only be provided by IPSec or L2TP over IPSec.
- Only SNMPv3 can be enabled.
- If cryptographic algorithms can be set for services (such as IKE/IPSec and SNMP), only FIPS-approved algorithms can be specified. These include the following:
    - AES
    - Triple-DES
    - DES
    - SHA-1
    - HMAC SHA-1
    - DSA
    - RSA signature and verification
- FTP and TFTP can only be used to load valid software files. (FTP and TFTP over IPSec can be used to transfer configuration files.)
- The module logs must be monitored. If a strange activity is found, the Crypto Officer should take the module off line and investigate.
- The tamper-evident labels must be regularly examined for signs of tampering.

User Guidance

The User accesses the module VPN functionality as an IPSec client. Although outside the boundary of the module, the User should be careful not to provide authentication information and session keys to other parties.

ACRONYMS

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BOM	Bill of Materials
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DSA	Digital Signature Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electro Static Dissipative
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
IKE	Internet Key Exchange
IPSec	IP Security
KAT	Known Answer Test
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MIB	Management Information Base
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
NVRAM	Nonvolatile Random Access Memory
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RADIUS	Remote Authentication Dial-in User Service
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Security Parameters
SSH	Secure Shell
TFTP	Trivial File Transfer Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
XSR	X-Pedition Security Router