Cisco Systems, Inc. 871, 876, 877, and 878 Integrated Services Routers

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version: Version 1.13

September 20, 2006

INTRODUCTION

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the 871, 876, 877, and 878 Integrated Services Routers with fixed-configuration from Cisco Systems, Inc., referred to in this document as the modules, routers, or as previously stated. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

This policy was prepared as part of the FIPS 140-2 Level 2 validation of the 871, 876, 877, and 878.

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 website at http://csrc.nist.gov/cryptval/.

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 Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.
- The NIST Cryptographic Module Validation Program website (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 complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

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

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc.

CISCO SYSTEMS, INC. 871, 876, 877, AND 878 INTEGRATED SERVICES ROUTERS

Cisco 800 Series

Building on Cisco's integrated services router portfolio, the new Cisco 800 Series routers extend concurrent data, security, and wireless to enterprise branch offices, teleworkers, and small businesses to help increase productivity and streamline operations. The Cisco 870 series allow small offices to operate secure concurrent services, including firewall, VPNs, and wireless LANs, at broadband speeds. Easy deployment and centralized management features make the Cisco 870 Series ideal for:

- Small offices or teleworker sites as part of an enterprise network
- Small and medium-sized businesses for secure WAN and wireless LAN connectivity
- Service providers to offer business-class broadband and wireless LAN services to their customers

Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area 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	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 1 – Validation Level by Section

The Cryptographic Module

The modules are validated as multiple-chip standalone cryptographic modules, and the cryptographic boundary of each module is the router case. All of the functionality discussed in this document is provided by components within this cryptographic boundary.

Module Interfaces

The physical interfaces are separated into the logical interfaces from FIPS 140-2 as described in the following tables:

Router	Router Physical Interface	FIPS 140-2 Logical Interface
Cisco 871, 876, 877, 878	FastEthernet LAN Ports 0-3 Console/Auxiliary Port	Data Input Interface
Cisco 871	WAN Port	
Cisco 877	ADSL-over-POTS Port	
Cisco 876	ISDN S/T Port ADSL-over-ISDN Port	
Cisco 878	ISDN S/T Port G.SHDSL Port	
Cisco 871, 876, 877, 878	FastEthernet LAN Ports 0-3 Console/Auxiliary Port	Data Output Interface
Cisco 871	WAN Port USB Ports 0-1 (Cisco 871 Only)	
Cisco 877	ADSL-over-POTS Port	
Cisco 876	ISDN S/T Port ADSL-over-ISDN Port	
Cisco 878	ISDN S/T Port G.SHDSL Port	
Cisco 871, 876, 877, 878	FastEthernet LAN Ports 0-3 Console/Auxiliary Port Power Switch	Control Input Interface
Cisco 871	WAN Port	
Cisco 877	ADSL-over-POTS Port	
Cisco 876	ISDN S/T Port ADSL-over-ISDN Port	
Cisco 878	ISDN S/T Port G.SHDSL Port	
Cisco 871, 876, 877, 878	FastEthernet LAN Ports 0-3 Console/Auxiliary Port LEDs	Status Output Interface
Cisco 871	WAN Port	
Cisco 877	ADSL-over-POTS Port	
Cisco 876	ISDN S/T Port ADSL-over-ISDN Port	
Cisco 878	ISDN S/T Port G.SHDSL Port	
Cisco 871, 876, 877, 878	Power Plug	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces 871, 876, 877, 878

Roles and Services

Authentication is role-based. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The module supports RADIUS and TACACS+ for authorization of remote VPN operators, and operators can authenticate as a User or Crypto Officer (defined by their password). A complete description of all the management and configuration capabilities of the modules can be found in the *Performing Basic System Management* manual and in the online help for the modules.

User Services

A User enters the system by accessing the console/auxiliary port with a terminal program or via IPSec protected telnet to a LAN port. The IOS prompts the User for their password. If the password is correct, the User is allowed entry to the IOS executive program. The services available to the User role consist of the following:

- **Status Functions**: view state of interfaces and protocols, version of IOS currently running
- **Network Functions**: connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace)
- **Terminal Functions:** adjust the terminal session (e.g., lock the terminal, adjust flow control)
- **Directory Services**: display directory of files kept in flash memory

Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the "enable" password) is defined. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- **Configure the Router**: define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.
- **Define Rules and Filters**: create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **Status Functions**: view the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.
- **Manage the Router**: log off users, shutdown or reload the outer, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.
- **Set Encryption/Bypass**: set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address. Performs basic encryption and decryption services.

Authentication Mechanisms

The module supports password-based authentication authenticating operators. To log on to the modules for management purposes, an operator must connect to it through one of the management interfaces (Console Port or Telnet) and provide a password.

Authentication Type	Strength
Username Password mechanism	Passwords must be a minimum of 6 characters (see Secure Operation section of this document). The password can consist of alphanumeric values, a-zA-Z0-9, yielding 62 choices per character.

	Since the password is required to have at least one letter and one number, the probability of a successful random attempt is $1/[(62)^6 - (52)^6 - (10)^6]$, which is much less than 1/1,000,000. The probability for a successful random attempt during a one-minute period is $60/[(62)^6 - (52)^6 - (10)^6]$which is much less than 1/100,100.This is also valid for RADIUS or TACACS+ shared secret keys.

Table 3 – Estimated Strength of Authentication Mechanisms

Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection of the Crypto Officer role login, and can be zeroized by the Crypto Officer. All zeroization consists of overwriting the memory that stored the key. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE).

The module supports the following critical security parameters (CSPs):

CSP Number	Name	Description	Storage
CSP 1	PRNG Seed Key	This is the seed key for X9.31 PRNG. This key is stored in DRAM and updated periodically after the generation of 400 bytes; hence, it is zeroized periodically. Also, the operator can turn off the router to zeroize this key.	DRAM (plaintext)
CSP 2	Diffie Hellman private exponent	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
CSP 3	skeyid	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
CSP 4	skeyid_d	Same as above	DRAM (plaintext)
CSP 5	skeyid_a	Same as above	DRAM (plaintext)
CSP 6	skeyid_e	Same as above	DRAM (plaintext)
CSP 7	IKE session encrypt key	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
CSP 8	IKE session authentication key	The IKE session authentication key. The zeroization is the same as above.	DRAM (plaintext)
CSP 9	ISAKMP preshared	The key used to derive IKE skeyid during preshared-key authentication. **`no crypto isakmp key`** command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)
CSP 10	IKE hash key	This key derives keys 3, 4, 5 and 6. This key is zeroized after deriving those keys.	DRAM (plaintext)
CSP 11	IPSec encryption key	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
CSP 12	IPSec authentication key	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
CSP 13	Router authentication key 1	This key is used by the router to authenticate itself to the peer. The router itself gets the password (that is used as this key) from the AAA server and sends it onto the peer. The password retrieved from the AAA server is zeroized upon completion of the	DRAM (plaintext)

		authentication attempt.	
CSP 14	PPP authentication key	The authentication key used in PPP. This key is in the DRAM and not zeroized at runtime. One can turn off the router to zeroize this key because it is stored in DRAM.	DRAM (plaintext)
CSP 15	Router authentication key 2	This key is used by the router to authenticate itself to the peer. The key is identical to #18 except that it is retrieved from the local database (on the router itself). Issuing the "no username password" zeroizes the password (that is used as this key) from the local database.	NVRAM (plaintext)
CSP 16	User password	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
CSP 17	Enable password	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
CSP 18	Enable secret	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered to be stored in plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
CSP 19	RADIUS secret	The RADIUS shared secret. This shared secret is zeroized by executing the "no" form of the RADIUS shared secret set command.	NVRAM (plaintext), DRAM (plaintext)
CSP 20	TACACS+ secret	The TACACS+ shared secret. This shared secret is zeroized by executing the "no" form of the TACACS+ shared secret set command.	NVRAM (plaintext), DRAM (plaintext)
CSP 21	Manual IPSec Authentication Keys	The IPSec authentication keys that are manually entered using **`the set session-key inbound ah spi hex-key-data`** and **`set session-key outbound ah spi hex-key-data`**. Keys are zeroized with the command **`no set session-key inbound | outbound ah`**	NVRAM (plaintext)
CSP 22	Manual IPSec Encryption Key	The IPSec encryption keys that are manually entered using the **`set session-key inbound esp spi cipher hex-key-data [authenticator hex-key-data]`** and **`set session-key outbound esp spi cipher hex-key-data [authenticator hex-key-data].`** Keys are zeroized with the command **`no set session-key inbound | outbound esp`**.	NVRAM (plaintext)
CSP 23	PRNG Seed	Seeds the FIPS-approved PRNG and zeroized when the module is rebooted or power cycled.	DRAM (plaintext)

Table 4 – Critical Security Parameters

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in Table 5:

SRDI/Role/Service Access Policy	Security Relevant Data Item	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16	CSP 17	CSP 18	CSP 19	CSP 20	CSP 21	CSP 22	CSP 23
Role/Service																								
User role																								
Status Functions																								
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r							
Terminal Functions																								
Directory Services																								
Crypto Officer Role																								
Configure the Router																r w d								
Define Rules and Filters																								
Status Functions																								
Manage the Router		d												r w d	d		r w d	r w d	r w d	r w d	r w d			d
Set Encryption/Bypass		r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d	r w d		r w							r w d	r w d	r w d

Table 5 – Role and Service Access to CSPs

The module supports the following key management schemes:

1. Pre-shared key exchange via electronic key entry. TDES/AES key and HMAC-SHA-1 key are exchanged and entered electronically.
2. Internet Key Exchange method with support for pre-shared keys exchanged and entered electronically.
    - The pre-shared keys are used with Diffie-Hellman key agreement technique to derive DES, TDES or AES keys.
    - The pre-shared key is also used to derive HMAC-SHA-1 key.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol. All of the keys and CSPs of the module can be zeroized. Please refer to the Description column of Table 4 for information on methods to zeroize each key and CSP.

Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to insure all components are functioning correctly. The modules implement the following power-on self-tests:

Implementation	Tests Performed
IOS	• Software/firmware integrity test • Bypass test • AES KAT • TDES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT
HW Cryptographic Engine	• AES KAT • TDES KAT • HMAC SHA-1 KAT • DH test

Table 6 - Module Power On Self Tests

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of all input/output interfaces; this prevents the module from passing any data during a power-on self-test failure.

The module also provides the following conditional self-tests:

Implementation	Tests Performed
IOS	• Continuous Random Number Generator test for the FIPS-approved RNG • Continuous Random Number Generator test for the non-approved RNGs • Conditional Bypass test

Table 7 - Module Conditional Self Tests

SECURE OPERATION OF THE 871, 876, 877, AND 878 INTEGRATED SERVICES ROUTERS

Once the configuration steps in this section are completed, these modules meet all the applicable Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation. All configuration activities must be performed via the command line interface via the console (for initial configuration) or IPSec protected telnet sessions – neither the web configuration tools CSRW or SDM may be used.

System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 12.4(4)T2 Advanced Enterprise is the only allowable image; no other image may be loaded.
2. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

   ```
   config-register 0x0102
   ```

3. The Crypto Officer must create the "enable" password for the Crypto Officer role. The password must be at least 6 characters, including at least one letter and at least one number, and is entered when the Crypto Officer first engages the "enable" command. The Crypto Officer enters the following syntax at the "#" prompt:

   ```
   enable secret [PASSWORD]
   ```

4. The Crypto Officer must always assign passwords (of at least 6 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

   ```
   line con 0
   password [PASSWORD]
   login local
   ```

5. The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 6 characters long, including at least one letter and at least one number. Also, the Crypto Officer must secure traffic between the module and the RADIUS/TACACS+ server via IPSec tunnel. As such, authentication parameters are sent encrypted with a FIPS-approved algorithm.
6. The Crypto Officer must apply tamper evidence labels as described later in this document.

The module is in FIPS mode once Steps 1-6 above have been performed.

IPSec Requirements and Cryptographic Algorithms

1. The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE).
2. Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:

- ah-sha-hmac
- esp-sha-hmac
- esp-TDES
- esp-aes

Protocols

1. SNMP v3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*. Since SNMP v2C uses community strings for authentication, only *gets* are allowed under SNMP v2C.
2. The SSL protocol must not be used in FIPS mode.
3. The Crypto Officer must ensure that the PC that is used for the console connection is a stand-alone or a non-networked PC

Remote Access

1. Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.
2. SSH access to the module is not allowed in FIPS mode of operation.

Cryptographic Algorithms

The appliances support many different cryptographic algorithms; however, only FIPS approved algorithms may be used. The following cryptographic algorithms are to be used:

- AES encryption/decryption
- TDES encryption/decryption
- SHA-1 hashing
- HMAC- SHA-1 for hashed message authentication
- X9.31 for RNG

Note: Pursuant to the DES Transition Plan and the approval of the *Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation*, the DES algorithm should not be used in FIPS approved mode of operation. The DES algorithm must not be used when the TDES/AES licenses are installed.

The module can be configured to use cryptographic implementations in software or in hardware residing with the modules' processor. Each cryptographic implementation has achieved the following validations:

Algorithm	IOS	800 Hardware Crypto
AES	325	324
TDES	390	389
SHA-1	399	398

SHA-1 HMAC	134	131
RNG	147	Not Supported in FIPS Mode

Table 8 - Algorithm Certificates

Non-FIPS Approved Algorithms

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

- DES
- RC4
- MD5
- MD5 HMAC
- Diffie-Hellman (allowed for use in FIPS mode) provides 80 or 96 bits of encryption strength.
- RSA (non-compliant)

Tamper Evidence

All CSPs are stored and protected within each appliance's tamper evident enclosure. The administrator is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit. These security labels are very fragile and cannot be removed without clear signs of damage to the labels. Security labels have non-repeated serial numbers which are non-repeating and are visible at all times.

The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

Application of the serialized tamper evident labels is as follows:

Cisco 871, 877, 876, and 878

1. Turn off and unplug the system before cleaning the chassis and applying labels.
2. Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
3. Apply one label to cover the bottom/front as shown in Figure 1. The label should wrap to include the bottom of the router.

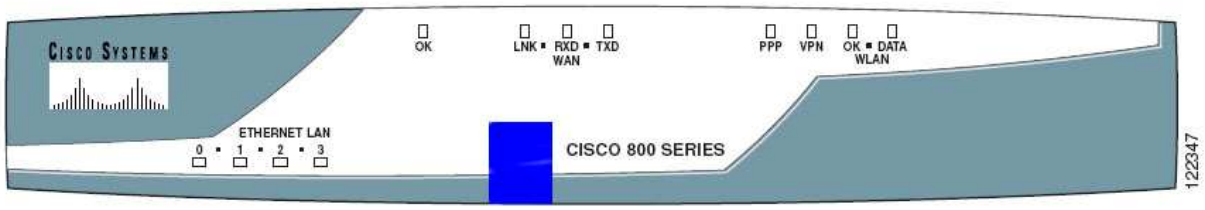

Figure 1 – 800 Series Tamper Evident Label Placement (Front View)

4. Apply one label to cover the top/back of the router as shown in Figure 2. The label should wrap to include the top of the router.

Figure 2 - 800 Series Tamper Evident Label Placement (Back View)

The tamper evidence seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the router will damage the tamper evidence seals or the material of the module cover. Since the tamper evidence seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the module has not been tampered. Tamper evidence seals can also be inspected for signs of tampering, which include the following: curled corners, rips, tears, and slices. The word “OPEN” may appear if the label was peeled back.