831 Secure Broadband Routers

FIPS 140-2 Non Proprietary Security Policy
Level 2 Validation

Version 1.6

November 15, 2004

Table of Contents

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Cisco 831 Secure Broadband Router. This security policy describes how the Cisco 831 Secure Broadband Router (Hardware Version: 831; Firmware Version: IOS 12.3(8)T5) meets the security requirements of FIPS 140-2, and how to operate the Cisco 831 Secure Broadband Router in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the Cisco 831 Secure Broadband Router.

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/.

1.2 References

This document deals only with operations and capabilities of the 831 router in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the 831 router and the entire 800 Series from the following sources:

- The Cisco Systems website contains information on the full line of products at www.cisco.com. The 800 Series product descriptions can be found at: http://www.cisco.com/en/US/products/hw/routers/ps380/index.html

- For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

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

1.3 Terminology

In this document, the Cisco 831 Secure Broadband Router is referred to as the router, the module, or the system.

1.4 Document Organization

The Security Policy document is part of the 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 document provides an overview of the 831 router and explains the secure configuration and operation of the modules. This introduction section is followed by Section 2, which details the

general features and functionality of the 831 router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

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

2 The 831 Router

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Cisco 831 provides a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements. This section describes the general features and functionality provided by the Cisco 831 router.

2.1 The 831 Cryptographic Module

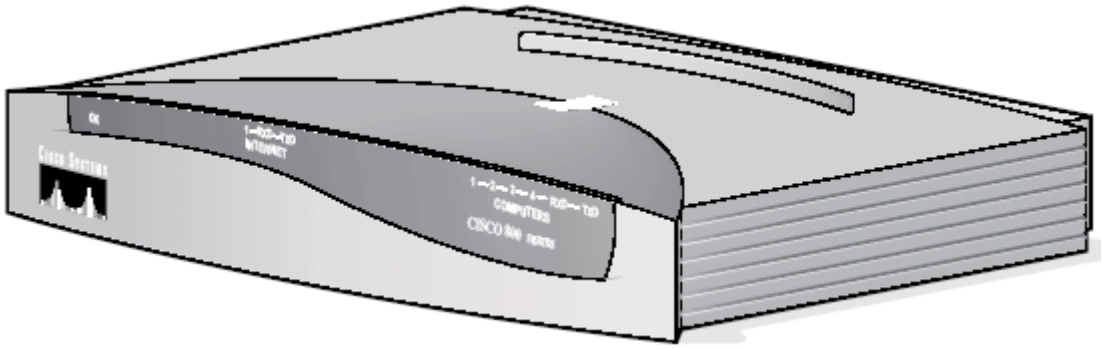

Figure 1 – The 831 Router

The 831 router is a multiple-chip standalone cryptographic module. The cryptographic boundary of the module is the device's case. All of the functionality discussed in this document is provided by components within this cryptographic boundary. Symmetric and asymmetric encryption, decryption and authentication functionality is performed by the Hifn 7902 cryptographic coprocessor located on the router's main board.

2.2 Module Interfaces

The interfaces for the router are located on the rear panel as shown in Figure 2.

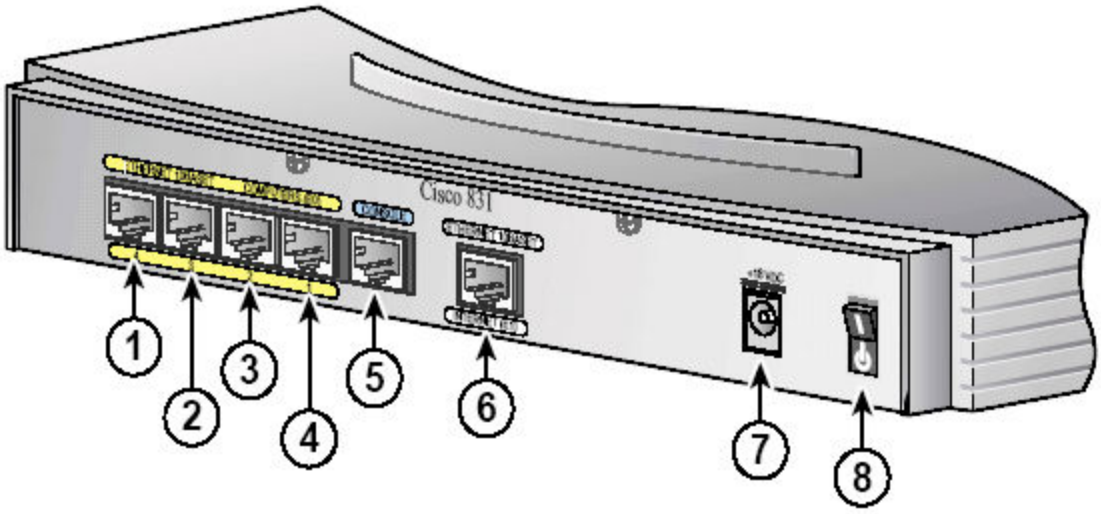

Figure 2 – Physical Interfaces

The Cisco 831 router features a console/auxiliary port, four fixed LAN interfaces and a WAN interface. Figure 1 shows the front panel and Figure 2 shows the back panel. The front panel contains 10 LEDs that output status data about the device's power, the WAN and the LAN ports. The back panel contains four (4) RJ45 ports that access the 10Base-T/100Base-T Ethernet switching capability (these are identified as 1, 2, 3, and 4 in Figure 2. Item 5 is a RJ45 port that provides console or terminal access to the router's control functionality. Item 6 is a RJ45 port to connect the router to the WAN using the 10Base-T Ethernet protocol. Item 7 is the power input jack, and item 8 is the power on/off switch.

The following table provides more detailed information conveyed by the LEDs on the front panel of the router:

Table 1 – Front Panel Indicators

LED	Description
LED_PWR_OK	Steady: successfully booted Blinks if an error occurred during boot, driven by 857DSL
LAN_LED_RXD	LAN Ethernet receive data, driven by 857DSL
LAN_LED_TXD	LAN Ethernet transmit data, driven by 857DSL
LAN_LED_OK1	LAN Ethernet Port 1 line OK status, Driven by Ethernet
LAN_LED_OK2	LAN Ethernet Port 2 line OK status, Driven by Ethernet
LAN_LED_OK3	LAN Ethernet Port 3 line OK status, Driven by Ethernet
LAN_LED_OK4	LAN Ethernet Port 4 line OK status, Driven by Ethernet
WAN_LED_OK	WAN Ethernet line OK status, Driven by Ethernet
WAN_LED_RXD	WAN Ethernet receive data, driven by 857DSL
WAN_LED_TXD	WAN Ethernet transmit data, driven by 857DSL

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

Router Physical Interface	FIPS 140-2 Logical Interface
10/100BASE-TX LAN Port Console/Auxiliary Port WAN Port	Data Input Interface
10/100BASE-TX LAN Port Console/Auxiliary Port WAN Port	Data Output Interface
10/100BASE-TX LAN Port WAN Port Power Switch Console/Auxiliary Port	Control Input Interface
10/100BASE-TX LAN Port WAN Port LAN Port LEDs WAN Port LEDs Power LED Activity LEDs Console/Auxiliary Port	Status Output Interface
Power Plug	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

2.3 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 authentication. A complete description of all the management and configuration capabilities of the Cisco 831 router can be found in the *Performing Basic System Management* manual and in the online help for the router.

2.3.1 User Services

A User enters the system by accessing the console/auxiliary port with a terminal program or via IPSec protected telnet or ssh session 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

2.3.2 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.

2.4 Physical Security

The router is entirely encased by a plastic case. The rear of the unit provides a WAN connector, four LAN connectors, the Console/Auxiliary connectors, the power cable connection and a power switch. The top portion of the chassis may be removed to allow access to the motherboard, memory, and expansion slots.

Once the router has been configured in to meet FIPS 140-2 Level 2 requirements, the router cannot be accessed without signs of tampering. To seal the system, apply serialized tamper-evidence labels as follows:

1. Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10°C.
2. Place the first label on the router as shown in Figure 3. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the router. Any attempt to remove the enclosure will leave tamper evidence.
3. Place the second label on the router as shown in Figure 3. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the router. Any attempt to remove the enclosure will leave tamper evidence.

4. Place the third label on the router as shown in Figure 3. This label covers the console port of the router. This step should be performed after any initial configuration requiring the console port is complete.
5. The labels completely cure within five minutes.

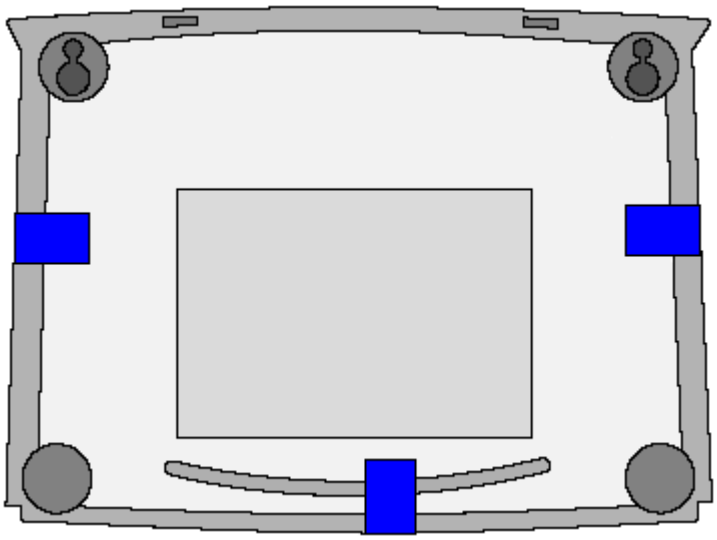

Figure 3 - Tamper Evident Label Placement (Bottom View)

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, bubbling, crinkling, rips, tears, and slices. The word "OPEN" may appear if the label was peeled back.

2.5 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 on 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 modules contain a Hifn 7902 cryptographic accelerator chip, which provides DES (56-bit), and 3DES (168-bit) IPSec encryption, MD5 and SHA-1 hashing, and has hardware support for DH and RSA key generation. However, RSA operations are prohibited in policy.

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

#	CSP Name	Description	Storage
1	CSP 1	This is the seed key for X9.31 PRNG. This key is	DRAM

		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.	(plaintext)
2	CSP 2	The private exponent used in Diffie-Hellman (DH) exchange. Zeroized after DH shared secret has been generated.	DRAM (plaintext)
3	CSP 3	The shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)
4	CSP 4	The IKE session encrypt key. The zeroization is the same as above.	DRAM (plaintext)
5	CSP 5	The IKE session authentication key. The zeroization is the same as above.	DRAM (plaintext)
6	CSP 6	The key used to generate 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)
7	CSP 7	This key generates key 3. This key is zeroized after generating the key.	DRAM (plaintext)
8	CSP 8	The fixed key used in Cisco vendor ID generation. This key is embedded in the module binary image and can be deleted by erasing the Flash. The command “erase flash” should be used to erase the flash.	NVRAM (plaintext)
9	CSP 9	The IPSec encryption key. Zeroized when IPSec session is terminated.	DRAM (plaintext)
10	CSP 10	The IPSec authentication key. The zeroization is the same as above.	DRAM (plaintext)
11	CSP 11	The key used to encrypt values of the configuration file. This key is zeroized when the “no key config-key” is issued.	NVRAM (plaintext)
12	CSP 12	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 authentication attempt.	DRAM (plaintext)
13	CSP 13	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)
14	CSP 14	This key is used by the router to authenticate itself to the peer. The key is identical to #22 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	NVRAM (plaintext)

		database.	
15	CSP 15	This is the SSH session key. It is zeroized when the SSH session is terminated.	DRAM (plaintext)
16	CSP 16	The password of the User role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
17	CSP 17	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
18	CSP 18	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext)
19	CSP 19	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)
20	CSP 20	The TACACS+ shared secret. This shared secret is zeroized by executing the "no" form of the RADIUS shared secret set command.	NVRAM (plaintext), DRAM (plaintext)

Table 3 – Critical Security Parameters

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed in the Table 4.

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
Role/Service																					
User role																					
Status Functions																					
Network Functions		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			r w d			r w d						
Define Rules and Filters																					
Status Functions																					
Manage the Router		d										r w d	r w d	d			r w d	r w d	r w d	r w d	r w 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		r w d					
Change WAN Interface Cards																					

Table 4 – Role and Service Access to CSPs

The module supports DES (for legacy use only), 3DES, DES-MAC, TDES-MAC, AES, SHA-1, HMAC SHA-1, MD5, HMAC MD5, Diffie-Hellman, cryptographic algorithms. The MD5, HMAC MD5, and RSA algorithms shall not be used when operating in FIPS mode.

The module supports three types of key management schemes:

1. Pre-shared key exchange via electronic key entry. DES/3DES/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, 3DES 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.

Key Zeroization:
All of the keys and CSPs of the module can be zeroized. Please refer to the Description column of Table 3 for information on methods to zeroize each key and CSP.

2.6 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. If any of the self-tests fail, the router transitions into an error state. Within the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

Self-tests performed by the IOS image

Power-up tests
- Firmware integrity test
- DES KAT
- TDES KAT
- AES KAT
- SHA-1 KAT
- PRNG KAT
- Power-up bypass test
- Diffie-Hellman self-test

HMAC SHA-1 KAT

Conditional tests

Conditional bypass test

Continuous random number generator tests

3 Secure Operation of the Cisco 831 Router

The Cisco 831 router meets all the 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 ssh or telnet sessions – neither the web configuration tools CSRW or SDM may be used.

3.1 System Initialization and Configuration

1. The Crypto Officer must perform the initial configuration. IOS version 12.3(8)T5 is the only allowable image; no other image may be loaded. The allowable CCO image filename is "C831-k9o3sy6-mz.123-8.T5".
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 8 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 8 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 8 characters long, including at least one letter and at least one number.
6. The Crypto Officer must configure the router to use the hardware accelerator by executing the following commands:

   ```
   configure terminal
   crypto engine accelerator
   end
   ```

7. The Crypto Officer must apply tamper evidence labels as described in Section 2.4 of this document. This step should be performed after console access is no longer needed, since the console port is covered.

3.2 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-des
    - esp-sha-hmac
    - esp-3des
    - esp-aes
3. The following algorithms are not FIPS approved and should not be used:
    - MD-5 for signing
    - MD-5 HMAC
    - RSA

3.3 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.

3.4 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 only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.