IP Technology Labs
Network Communications Simplified™

WELBECK SECURE

Deploying Welbeck/IpTL Secure Appliances for FIPS 140-2 Operation

Technical Resource Guide

Highlights

- Model numbers and features
- Firmware Versioning and operational environment
- Physical Security Attributes
- Crypto Officer/Access Security
- Crypto Module Certification
- Key material management and zeroization
- Manual zeroization procedures
- Managing the WSS FIPS Mode Appliance
- Firmware update and authentication

Inquiries and orders:

Welbeck Secure Solutions
7910 Woodmont Ave., Ste 1250
Bethesda, MD 20814
sales@welbecksecure.com
855-WELBECK (855-935-2325)

Introduction

Welbeck Secure Solutions (WSS) offers a specific product line of its appliances which encompasses the stringent security requirements for crypto conformance, physical security, and authorized device access. This guide details the actions, operations, and features to enable and ensure a FIPS140-2 compliant deployment of WSS appliances within your network.

WSS appliances are ordered and shipped as 140-2 FIPS Compliant Appliances (FCA.) These appliances have the necessary FIPS140-2 and other security best-practices incorporated into the firmware, hardware, and operational aspects of the appliance. FCA specific appliances eliminate confusion between COTS equipment including all the compliant elements out-of-the-box. FCA operation cannot be disabled by the user and elements to maintain compliance cannot be circumvented.

WSS FIPS Operational Highlights

- No user access to key material or certificates
- Web/UI Management via HTTPS only
- Management control and SNMP/Syslog over secure facilities only
- No Telnet, SSH, Console, or Modem access
- No "Shell" daemon running or root access
- Encryption cipher locked at AES256
- No DES/3DES/MD5 available
- Local and remote Zeroization
- High-Availability/Redundant operation (STP) is over secure tunnel
- Diffie-Hellman Key Exchange locked to ____ group
- SNMP RW is disabled for LAN access

Physical security elements of FIPS compliance are pre-installed at the factory prior to shipment including non-penetrating vent holes and Level 2 tamper stickers.

Over all, WSS FIPS Solutions eliminates confusion between COTS appliances, reducing audit/compliance activities; and provides quick and deterministic deployment.

FIPS 140-2 Compliant Operational Environment

The operational environment for the standalone appliances is IpTL's own BroadLane™ firmware and is a closed system. As this is not a general purpose computing device, there are no user applications which can be loaded/installed and run. Additionally, there is no user access to operating firmware. All device administrative access is via the web UI, SNMP, or SYSLOG and only via secured access methods.

The IpTL Virtual Appliances also run IpTL's BroadLane™ and do not allow any user installed applications or user access to the underlying BroadLane™ OS. Thus, the instance of the virtual appliance provides the same FIPS compliant operational environment as the physical appliances. Note however that one must separately address the Virtual Machine Host/system instance and its compliance with FIPS 140-2 requirements. It is the responsibility of the crypto officer to ensure that the complete system is in compliance (for example, using a Virtual Machine with a FIPS140-2 validated cryptographic module if necessary).

FIPS 140-2 Level 2 requires tamper evident physical security or pick resistant locks. WSS provides tamper evidence via tamper resistance labels or labeling methods.

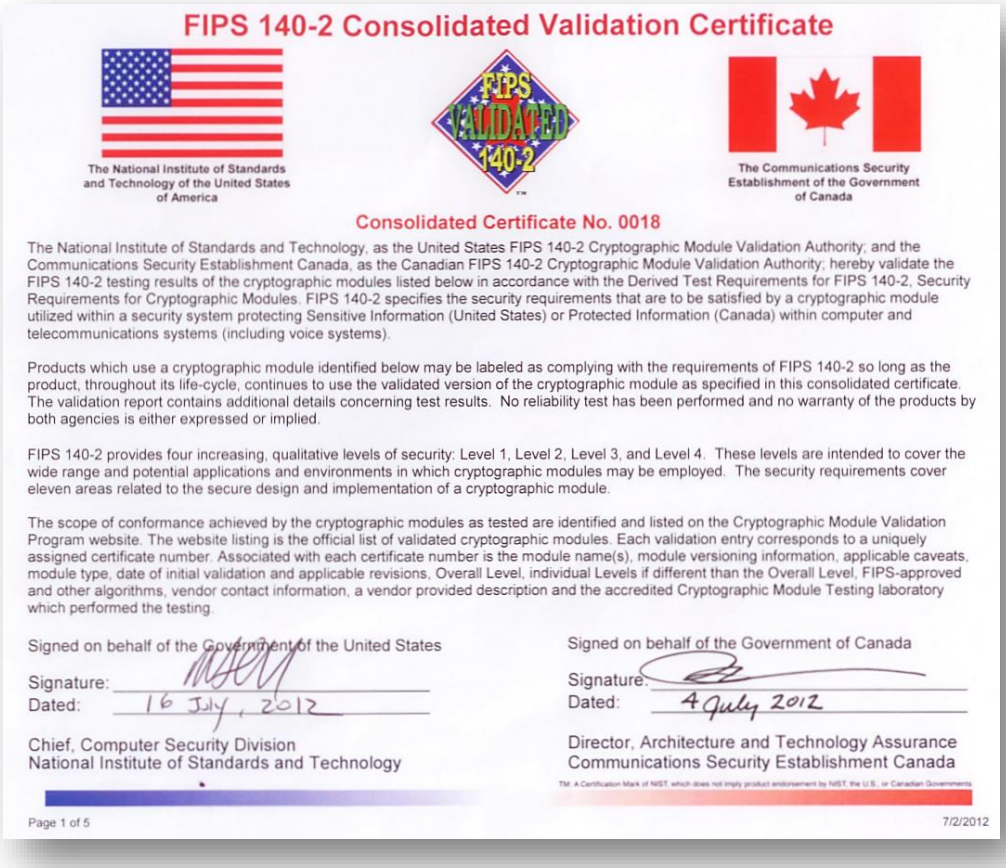
For system access, FIPS 140-2 Level 2 provides for role-based authentication. WSS provides for multi-level administrative access to control, configure or maintain the appliance. Additionally, WSS allows software cryptography in multi-user timeshared systems when used in conjunction with a C2 or equivalent trusted operating system.

Initial Review

Before carrying out any step to secure a WSS appliance it is important to verify that the product has not been tampered with. You should also confirm that the product received matches the version that is certified as FIPS 104-2 compliant.
Verify product security by observing the tamper-evident stickers (pictured above).

Crypto Module Validation

WSS employs the OpenSSL Source toolkit library for implementing Transport Layer Security protocols as well as a full-strength general purpose cryptography. This library is FIPS140-2 certified with the validation awarded on June 27, 2012, under certification number #1747. The CMVP list(s) of Validated Cryptographic Modules provide the official validation information for each module and combines certifications under a consolidated certification list. The CMVP no longer issues individual module validation certificates. As such, certification number #1747 is listed under Consolidated Certificate No.0018.



FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0018

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature:

Dated: 16 July, 2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 4 July 2012

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Page 1 of 5

7/2/2012

Details can be found at:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0018.pdf

Model Numbers/SKU listing for FIPS Compliant Appliances

The following model numbers are for WSS FIPS140-2 FIPS Mode Compliant Appliances (FCA.) These appliances have the necessary FIPS140-2 and other security best-practices incorporated into the firmware. All FCA SKU's are prefixed with the number 110 and follow the format of 110xx-xx-xx where the x equals specific models within the product line.

SKU/Part Number	Description
11070-7-xx	IpTL NetBlazer Model 7 Secure Remote Access Adapter Series with integrated 802.11 WiFi; WiFi Access Point and Station-Uplink; internal antennal, single 10/100 TX Ethernet Port; USB Port powered.
11070-71LW-xx	FastLane IpTL 71LW LAN Virtualization Secure Tunneling Bridge Series with integrated 802.11 or 3G/UMTS/GPRS access; dual antenna; dual 10/100 Ethernet Ports; local or remote operation; Single Unit
11070-7x-xx	FastLane IpTL 70 Series Secure Tunneling Bridge and Ethernet VPN Security Gateway, Single or MultiTunnel; quad 10/100/1000 Ethernet, Single unit;
11070-770-xx	FastLane IpTL 770 Series Multipath Ethernet Secure Remote Gateway, Dual Tunnel; quad 10/100/1000 Ethernet, Single unit; Configured for zero (0) tunnels; Support from 1 to 25 tunnels
11070-79-xx	FastLane IpTL 79R Multipath Ethernet Access Server, Licensed as server for 25 clients, 6 ports of copper 10/100/1000 Ethernet with bypass, 19" Rack mount Chassis, Single UI Power Input 100-240VAC 50/60Hz
11070-70v-xx	FastLane IpTL 70v eGate Access Virtual Appliance (AVA) Series with 1 Connection License for server or client tunnel connection. Add one or more 10070-77-95xx Series licenses to activate additional simultaneous connections.

FIPS Compliant Firmware Versioning and Firmware Authentication

Standalone appliances as well as the virtual appliance application all have firmware version numbers to explicitly indicate that the firmware includes the FIPS140-2 compliant elements. Appliances listed in the SKU list will not be able load or run non-compliant versions of firmware. Compliant Firmware Versions are denoted with a preceding **F** in the firmware version number. An example would be version F3.2.5a. Firmware version numbers can be found on the home page of the individual appliance's UI.

Firmware Upgrade and Authentication

The firmware is AES256 encrypted and SHA-256 authenticated. All firmware updates are validated prior to loading and all non-compliant firmware is rejected.

Running Configuration Export/Import

The device configuration files for export or import are AES256 encrypted and SHA-256 authenticated to the specific appliance.

Zeroization of an Appliance

Zeroization of a WSS appliance permits the positive destruction of key material and passwords/passphrases in a fielded appliance. During the zeroization event, all keys, certifications, passwords, and passphrases are securely overwritten in both the file system and in memory with a random pattern. Then the system is put into a "factory" default mode erasing all other information including tunnel host information, ACL's, and WiFi/Connectivity details.

Physical Zeroization

Depress and hold the appliance's reset switch for 60 seconds. All appliance indicators will flash simultaneously approximately once per second to indicate that the process is completed. Release the reset button and the unit will attempt to reboot but will not find any operational configuration or code. The front panel status LED will flash approximately once every 5 seconds to indicate this state.

After secure zeroization the unit will need to be returned to the factory under a return-material-authorization (RMA) to be reprogrammed.

WEB/UI Zeroization

Log into the web UI with the cryto officer credentials. On the left side of the screen will be a Zeroize button. After accepting action, the zeroization will immediately occur. After this action all appliance indicators will flash simultaneously approximately once per second to indicate that the process is completed.

After secure zeroization the unit will need to be returned to the factory under a return-material-authorization (RMA) to be reprogrammed.