Security Policy for the Standard and Segmented NetFortress® VPN Level 2 Multi-Chip Standalone Module

This policy was developed for FIPS 140-1 certification of the FIPS 140-1 certified version ("GVPN") of our NetFortress® VPN-1, version 1. The project began when Fortress Technologies was DSN Technology, and only one version of the product was developed, called the NetFortress.

To maintain consistency throughout the life of the certification project, all documentation has kept the original product name.

DocumentRevision History:

5/20/98	Original document
7/14/98	Corporate name updated
7/22/98	Document title revised to match FIPS Conformance Testing Results report
10/21/98	Inclusion of zeroization switch, update trademark, correct from tamper resistant to tamper evident

Table of Contents

Security Policy for the Standard and Segmented NetFortress® VPN Level 2 Multi-Chip Standalone Module

1.0 Introduction

Federal Information Processing Standard Publication (FIPS PUB) 140-1, *Security Requirement for Cryptographic Modules*, [Ref.1], requires *a stand-alone document* that specifies the Security Policy for a cryptographic module intended for use as security equipment protecting sensitive but unclassified information within government computer and telecommunication (including voice) systems. The Security Policy is a supporting document to the main Submittal [Ref. 2], that contains the other required information about the cryptographic module.

The Security Policy includes all the security rules under which the module must operate (and enforce), particularly rules derived from the security requirements of the standard (see **Vendor Requirement VE01.07.01** [Ref. 3])**,** and the security rules derived from additional security requirements imposed by the manufacturer. Thus, a proper security policy describes all roles, services, and security-relevant data items pertaining to the cryptographic module. The policy specifies what access, if any, a user performing a service within the context of a given role is permitted to each of the security-relevant data items. The specification is required to be complete and detailed enough to answer the question, "What access does operator X, performing service Y, while in role Z, have to security-relevant data item K?" This question must be asked and answered for every role, service, and security-relevant data item contained in the cryptographic module.

This document describes the Security Policy for the multi-chip stand-alone cryptographic module, called "NetFortress®", a security product of Fortress Technologies, Inc. (FTI). The Security Policy in its present form was developed as a result of a continuing series of discussions with CygnaCom's Cryptographic Equipment Assessment Laboratory (CEAL). This laboratory, contracted by FTI, is testing and evaluating the module's compliance with FIPS Security Level 2 requirements.

The security rules and directives described in this document *serve as a reference, guide, and obligation in any federal government-related transaction concerning this product which is expected to be approved at Security Level 2.* The document specifically covers the:

- Rules and directives related to the module's security during manufacturing
- Module's "trusted distribution procedure" (including factory-set activation and installation)
- Module's "maintenance and service" at the vendor's premises

While this is an "internal" FTI document, and its scope is intended to be "informative", it is a non-proprietary document. The rules it contains are of great benefit when conducting business transactions with federal agencies. Therefore, the company's management, specifically those involved in Manufacturing, Marketing, Sales, and post-sale Customer Service (delivery, installation, and maintenance of this module) must become familiar with the contents of this document.

2.0 Security Design Concepts

The NetFortress®' security policy, the security rules under which the module must be used and is constructed to enforce, is strongly related to the module's original *design objectives* to*:*

- Implement a simple computational device to protect a single host or a particular network from potential security threats (hence the name "NetFortress®"), and
- Serve as an inexpensive, automatic tool to build Virtual Private Networks (VPNs) over the Internet.

The following four security design concepts were developed to fulfill these objectives:

1. Contain the device's hardware in a sealed, *tamper-evident* metal box, in a secure cryptographic module, and *minimize the human intervention* to its operation with a high degree of automation. The automation is rather important, because the module as a commercial product, is intended to be used in a variety of security environments (targeted at a medium level, or Security Level 2, per the FIPS security level categories ranging from Security Levels 1 to 4) by a variety of customers. Allowing any of its sensitive operational tasks, including maintenance, to be performed under these conditions by operators would represent a liability, rather than an aid, to security.
2. Create and assign *a unique Company Proprietary Signature (CPS)* to each customer organization (or a group or division thereof). During manufacturing, the CPS is placed into the software of every cryptographic module that is used to establish the customer's VPN. Using a unique CPS ensures that only modules with the same CPS can exchange keys and establish a secure VPN; all other modules are excluded. ***All*** key exchanges between the modules of a particular VPN are encrypted and protected from unauthorized modification and substitution.
3. Prevent the module from being used fraudulently, if stolen after installation at a customer's site. The following two consecutive steps enforce this concept: (a) *activating the module at the factory*, followed by (b) the *installation* process, including the *initial startup* and the *first outgoing message* procedures, performed at the customert's site. Performing these steps permanently attaches the module to a customer's site.

4.* Besides providing encrypted communication between secured sites, should provide restricted bypass operation with an unsecured site.

After installation, the module serves not only to *guard* against threats from outside the network, but also acts as a *cryptographic co-processor* for client systems requiring cryptographic services.

With regard to these services the high degree of automation has the following advantages: a.) the module can provide cryptographic services with only minimal human intervention and at low level security risk, b.) simple role based access control is considered to be satisfactory for its usage, c.) to enforce this access control, the module can apply the least complex access-control mechanism, d.)* for the segmented configuration the module enforces encrypted communication between secured sites and it enforces the rule that allows unencrypted (bypass) communication with an unsecured site only if that communication was initiated by the secured client, e.) the burden to cope with the eventual high security tasks is shifted to the local security policy of the customer.

- The automation reduces the role of an operator (user) essentially to survey only the power/status/connectivity of the module. This type of operator activity generally poses a relatively low-level security risk
- Consequently, it is expected that the security of the module from inside attacks does not require a stricter security policy than a minimal role-based Discretionary Access Control (DAC), that conforms to the concept of "access, restricted only to operators who are authorized by the legitimate customer."
- Thus it seems unnecessary that the module would employ more complex DAC-enforcing mechanism (e.g., password or PIN reader, token or biometrics processor, smart card, etc.), rather than using *a simple, role-based authentication device* such as a *key-operated security power lock*. Applying more advanced mechanisms would only decrease the cost-effectiveness of the NetFortress®, and would inhibit its operational efficiency.
- The NetFortress® reduces the security risk associated with its operation, and *per se*, does not require strict access control. This does not mean that presence of the module would not affect the local security policy of a customer. It is expected, that after installing a NetFortress®, the security rules for the personnel who is servicing the client systems, particularly for those who are performing sensitive tasks such as cryptographic traffic handling, would be modified. It is also expected, that the access control mechanisms or tools of the client systems, particularly where the plaintext messages become visible, would be upgraded.

Effective implemention of the above described security design concepts and considerations is outlined below.

3.0 Implementing the Security Design Concepts

3.1 Minimizing Human Intervention to the Module's Operation

The NetFortress® is a multi-chip, standalone cryptographic module. It is housed in a steel case having "non removable" boundaries. Its ports (serial, parallel, floppy disk, video, keyboard and mouse) are covered by a sealed security barrier rear plate, therefore no keyboard or monitor can be connected to the module. Not only does the module block hacker attacks, it also blocks local access to its firmware and its operating and file systems. Its factory-set type or configuration (see 3.4 below), as well as the CPS, cannot be altered without leaving evidence.

A factory-set and activated module automatically adapts itself to any Ethernet platform using TCP/IP. The NetFortress® needs no special modification for most network applications. The module assumes *many operational functions usually performed by human operators at earlier types of cryptographic modules. The NetFortress® automatically* uses protocols, performs key management (on an installed module there is no manual key or cryptographic parameter entry) to establish VPNs, and *provides cryptographic services, such as encryption and decryption.* The module changes dynamic keys automatically every 24 hours of operation, and *verifies the encryption/decryption process,* as well as checking data integrity after transmission. All of these functions greatly reduce the possibility for human error.

3.2 The Roles of the Crypto-Officer and the User

The physical security lock, mounted on the front panel, enables AC line power to the unit to be under the control of individuals authorized by the legitimate customer to install and operate (to power) the unit. These individuals, defined as crypto-officers, who have the keys that operate the lock, and the user. In several cases the same individual can perform the tasks of both the crypto-officer and the user.

FTI supplies two sets of two (2) unique keys with each module. They operate the security lock and the lock for the zeroization switch. The security keys are given to the crypto-officer by an authorized FTI employee who participates in the *Trusted Distribution* of the modules (description given in Section 3.5), and provides assistance to the crypto-officer during the *module's initial start up. After the initial startup, the crypto-officer either operates the module himself, or designates and authorizes a user to operate the module. At any later time, when the crypto-officer deems it necessary, he/she can perform zeroization using the second pair of security keys. Both the FTI and the customer inventory the identification number on all four keys.*

Thus, each module enforces a crypto-officer's and a user's *role. It satisfies* **Vendor Requirement VE03.02.01** which specifies that any cryptographic module, as a minimum, must support two roles: a crypto-officer role and a user role.

The crypto-officer's role is to install (or reinstall) the NetFortress® at the customer's site, perform its initial startup, send the first outgoing message, and render the unit inoperable – if needed.

The user's role is limited to operating the module, by

- using the power switch or connector *when the lock is in the "on" position* [1],
- attaching the connecting cables to the client system's data port and to the outside network,

---

[1] *The lock must be "on" for the unit to operate. This permission mode is non-symmetric in the sense that to change the state of the NetFortress® to be "powered up", both the lock and the push button switch on the module's face plate must be operated. However, someone without access to the key lock can shut off the power to the unit and disable the communication link by pushing the push button switch. This lock-based security approach facilitates the ability to shut down a communications link that may be considered untrustworthy, rather than passing data through that link if trust is questioned*

- observing the module’s status, and to rebooting the module, given a power loss or apparent malfunction (resulting in an “error” state). (*Powering off the module zeroizes all the sensitive cryptographic data in the module’s dynamic memory*.)
- *initiating bypass operation (for segmented modules only) by initiating communication with an unsecured site.

The module’s physical connection to a client system is under continuous surveillance according to the customer’s local security policy, so that it cannot be subject to a communication interception attack with a “sniffing” device from a remote location.

3.3 Tamper Evident Seals, No Scheduled Maintenance

The sealed, tamper-resistant metal box housing the NetFortress® hardware is neither intended to be, nor allowed to be opened by the user. *The module neither requires nor permits scheduled maintenance*. The seal consists of a minimum of two, numbered, *tamper-evident labels that leave detectable traces on the surfaces of the affected module. Removing the traces takes a minimum of two hours*. Both FTI and the customer inventory the number on each label.

The most important goals of a customer’s own security policy are prevention and quick detection of the module’s tampering. FTI is not responsible for malfunction of the module after installation due to tampering or breach of security by successful tampering attacks. FTI provides, however, full technical support and cooperation in any investigation associated with detected tampering attempts, or security breach and security damage control due to tampering attacks, and will test/perform necessary maintenance of the tampered module for reasonable compensation.

Maintenance or tests (particularly after “hard” failures) requiring human access to the module’s interior cannot be performed at the customer’s site. They must be performed *exclusively at FTI premises* (for detailed information, see Appendix A, *Maintenance at FTI Premises*).

3.4 Factory-Set Configuration, Company Proprietary Signature and Activation

NetFortress® modules are available in two types (host and LAN). The host module provides protection for a single node (a “client” computer). The LAN module provides security for up to 254 nodes on the same Class C LAN. The modules of these types provide secure communication with other NetFortress®-protected nodes only.

Based on the customer’s interest and needs, *the type*, as well as the unique *CPS*, are set at the factory and cannot be altered by the user. Arrangements must be made with FTI to change the type or the assigned CPS.

These two security provisions ensure that no one can compromise the integrity of a network by substituting the proper modules with other (inappropriate) ones.

- The CPS (the module’s secret key, or “hard key” to be used to encrypt [with DES] the static Diffie-Hellman key exchange) is generated and tested when the module is manufactured for a given customer. The CPS is a hexadecimal number whose length is 56 bits. It is generated and assigned externally for each customer by an authorized FTI employee.

The FTI employee's tests the CPS for uniqueness and for "guessability" (i.e., whether the CPS contains any potentially useful information concerning the customer's real name, logo, well-known product, or any characteristics from which a seasoned "guesser" would be able to determine the generated number). After this test, the selected CPS, *in DES sub-key expanded form* is written into the module's software, which is then loaded into the flash. (Note that since the CPS is written into the software it cannot be zeroized.) The flash is automatically subjected to the *Flash Checksum Test* at each start-up of the module.

At FTI the list of CPSs, the customer's identity, and the associated software hard copies *are kept under secure conditions* (with encrypted files in secured computers and redundant encrypted diskettes in a bank vault).

- Factory-set *activation* is the first *security step* against fraudulent use of the module before a module is put into service. An authorized FTI employee performs the activation during the manufacturing process. The activation *allows or disallows* burning a client's IP and MAC addresses (in a LAN module, the MAC address used is from the first node to send a message) into the flash by the first message from the client. Activation also provides an important security element for FTI's *"Trusted Distribution"* system for the modules. *Trusted distribution* assures detection of any tampering with a module's firmware from the time it leaves the vendor site to the time it arrives and is installed at a customer's site. Consequently, it protects the security of the information to be processed on the module(s) (see section 3.5).

  The activation procedure, performed under laboratory conditions, is as follows:

  1. From a dedicated, standalone computer program, *"activate"* sends an activation packet (an IP packet with a "FTI Activation" string in the payload) through the module.
  2. The module writes its *serial no*. and *the time of activation, after* receiving this packet and after checking for potential previous activation, into a specific location of the flash memory.
  3. A UDP (User Datagram Protocol) packet is sent to the computer that previously sent the activation packet, as an acknowledgment.
  4. The activation program then verifies that the module was successfully activated and displays the message: "Box has been activated."

3.5 Trusted Distribution, Initial Startup, and the Role of the First Outgoing Message

According to the *FTI's Trusted Distribution* system, each NetFortress® is shipped to a customert's site in an activated condition and under appropriate security procedures, such as in a sealed case, with no power-on possibility. FTI personnel, traveling separately from the module's shipment, brings the keys for the security lock and for the zeroization switch to the customer's site to provide assistance installing the module by the crypto-officer.

During installation, the intact (sealed) module is strategically placed between the protected LAN segment (a single machine, a specific area of a network, or the entire network) and the external communication link. During the initial start-up of the module by the crypto-officer (and/or FTI personnel), as part of the power-up self test process (see Table 14.1, Part A, of the Submittal) the module *validates* (by comparing the content of a predefined location of the flash memory with a known hex constant, called the FTI *authentication string*) that the executable used in the flash memory is the authentic FTI version, checks that the integrity of the software is intact, and *that the module is activated.*

- Breach of the module's seals or failure of the FTI software authenticity or integrity represents a "fatal" *hard error*, resulting in maintenance/repair at FTI premises. Failure of the activation check prompts the FTI code to set the *box_active* flag to 0. If successful, the flag is set to 1.
- The flag is tested when the client system's first message (e.g., PING, ARP request, or IP packet) transits the module. If the module is not activated, the IP and MAC addresses of the client systems are *not allowed to be burned into the flash*. Consequently, *reproducible static key cannot be generated* for the module.
- If the module is activated, the IP address and MAC address (for a single client system, or the Class-C part of the IP address and MAC-address of the first client system (for a LAN module), are **burned into the flash** (*representing the second security step against fraudulent use of the module*). The module is permanently tied to the client computer or to the Class-C LAN due to the burn-in process. Therefore, *any attempt to breach security by moving a module to a site with a different IP address (i. e., stealing and using it fraudulently) would be a waste of effort, since the unit won't work.*
- Another result of the burn-in is that the code now can generate *reproducible static key*. From this point, the reproducible static key will be an attribute (a property) of the module, allowing proper operation to resume after each reboot.
- *Nobody can spoof the client's IP to another module* after the first (static) key exchange with another party, when the IP addresses of the communicating modules, together with the common static keys, are stored in each of the modules. An intruder with a purchased NetFortress® would be unable to successfully masquerade as a legitimate user.
- *The Lan-type* NetFortress® *prevents spoofing the IP address of any of its client system(s)*. For a LAN module to deliver packets to its clients, it builds a table containing its client systems' IP and MAC addresses. Whenever a packet arrives from the outside network, the source's IP in each packet is matched against the IP addresses listed in this table, and the packet is rejected if the source's IP address matches an entry in the table.

4.0 Customer Security Policy Issues

It is to be emphasized that regardless of the features to avert security attacks built into the module, FTI expects that after the module's installation, any potential *customer* (government or commercial entity or division thereof*) employs its own internal security policy* covering all the rules under which the module(s) and the customer's network(s) must operate [Ref. 4]. The customer's security policy would ensure that those responsible for security are kept current on hacker techniques and programs, regulate all access to/from the Intranet, and protect against insiders. This security policy is expected to include multilevel DACs. Also, if needed, the customer systems are expected to be upgraded to contain appropriate security tools to enforce the internal security policy.

DACs can be implemented in a variety of ways, including:

- Using passwords, tokens or other security tools
- Configuring servers to selectively restrict services (e.g., ftp, telnet, etc.) to specified terminals, IP addresses or users
- Proxy servers to shield sensitive node
- *Privileges to handle cryptographic material*
- *Carefully granted super-user privileges*

5.0 Summary

The security rules, directives, and obligations imposed by the NetFortress®' Security Policy alone (disregarding the module's operational requirements) can be summarized as follows:

- During manufacture, a unique *Company Proprietary Signature (CPS)* will be determined and assigned by an authorized FTI employee to each module that will be a member of a particular Virtual Private Network. FTI is obligated to provide the uniqueness and secure handling of the CPS.
- The modules are delivered to the customer according to the procedures of FTI's *Trusted Distribution System*. Thus, an authorized FTI employee *activates* each sealed module before shipping. There is no possibility of power-on during shipment because the keys of the security lock and of the zeroization switch will be with FTI personnel traveling separately from the shipment. The keys will be given to the *crypto-officer authorized by the customer*.

  The crypto-officer, assisted by the FTI employee, will *install* the delivered module(s) (i.e., perform the initial start up and send the first outgoing message). After the installation the crypto-officer will either assume the role of the user or he will designate and authorize the user to operate the module. The module enforces that only the crypto- officer, the bearer(s) of the security lock's key, and the user can operate the module. *Similarly, the module enforces that only the crypto-officer, the bearer(s) of the key for the zeroization switch, can perform zeroization of the module. Both FTI and the customer will inventory the number on the keys.* After installation, the module's security will be subjected to the customer's own security policy.
- The module *does not require scheduled maintenance*. The *steel security plate,* as well as the *tamper evident seals (labels)* over the screws and plate edge, *do not permit* any type of maintenance. B*oth FTI and the customert will inventory the label number. FTI will not take any responsibility for malfunction of a tampered module or security breach due to tampering attacks.*

- *To change the type or configuration of the module, or to change the unique Company Proprietary Signature,* arrangements must be made with FTI. Any remanufacture after zeroization, repair, maintenance, or test, etc., that requires human access to the module's interior can be performed only at FTI premises, under the controlled conditions described in Appendix A, *Maintenance at FTI Premises,* of this document.

APPENDIX A. MAINTENANCE AT FTI PREMISES

Due to the module's design, the *maintenance of the interior components is a rather complex task, and not a field-expedient process.* Maintenance is considered to be a process that can be correctly and securely performed at a dedicated maintenance depot operated and controlled by the manufacturer. Thus, **Vendor Requirement VE02.06.01**, requiring detailing the field maintenance process, *is not applicable*.

Maintenance actions or physical modifications (including *changing the CPS)* are done by opening the module case and testing or replacing the several hardware components contained within. Opening the module case breaches the tamper evident seals (labels) on the case exterior and provides evidence of the case opening. Only the vendor can replace this seal (label) with another one, which number will be again *inventoried*, after completion of the internal procedures to the module.

Zeroization Before Maintenance. The critical data and security parameters contained inside the module, when powered on and in an operational state, are effectively zeroized when the "maintenance interface" is accessed, in the sense that to perform maintenance in the context just described, the module is powered off so that the hardware components may be removed and examined (**Vendor Requirement VE02.07.01**).

When this is done, the Host and MAC tables (see Section 9.1.2 of the submittal), cryptographic keys and other data that have been computed and stored in the volatile memory are lost (only "hardwired" parameters, like CPS, certain seed values for random number generation survive, and the module's own battery operated clock remains operable). This is the same scenario that exists in any personal computer, when software writes to certain memory locations, and power to the computer is switched off. The information being stored is permanently lost. Any effort to open the case and remove the flash ROM card for possible de-compilation would yield the same result.

In addition, if it is deemed necessary, the zeroization switch can be used by the crypto-officer at the client's site before sending the unit for maintenance, thus erasing everything from the flash. In this case, testing of the components is not possible; the flash has to be rewritten.

Procedure for Authorized Maintenance (Change of the Company Proprietary Signature). Maintenance actions, as stated, requires returning the module to the vendor so that it may be opened and the internal components tested for proper operation. These tests (**Vendor Requirement VE02.08.01**) include the following items:

1) Visual inspection of the module on receipt, testing for case integrity, evidence of loose parts inside, ability of data interfaces to accept and retain standard network cables (RJ-45 type).

2) Module powered off and opened. Visual inspection of the physical integrity of all interior components, checking for loose connectors, hardware, fan, etc.

3) Module powered on, and the components are tested.

- Power Supply — Proper voltage output.
  Proper ventilation/cooling with operating fan access unblocked.

- System Board — Passes Power-On Self-Test (test with hardware diagnostic card).
  Boots to BIOS setting screen, parameters OK (test with video).
  Proper ventilation/cooling with operating fan properly mounted.
  Tests system board with hardware diagnostic card, if necessary.
  Tests memory SIMMS for non-faulty operation, if necessary (can be part of above step, test done in-place or externally).

- Ethernet Cards — Tests in diagnostic station, proper operation; proper configuration.

- Flash Card — Tests in diagnostic station, tests for proper boot-up, examines known memory location for valid activation string. Changes the CPS, if required.

- General — Mechanical integrity of all option cards, jumpers, header pin connectors, riser card, and option cards fully seated in slot.

Repair items are generally limited to replacing the faulty component. In the case of any of the option cards (Ethernet or flash), reprogramming and return to service is a possibility. In the case of the system board, replacing the board is considered due to cost and availability of component-level repair of main boards.

4) Module assembled.

   - Insert in test network and pass network traffic through the module, testing for connectivity using TCP/IP diagnostic (ICMP) packets or application type packets (typically FTP, file transfer protocol) between two end-point stations communicating through the module.

5) Log information relative to the module, all part numbers, check that the *activation string is present,* attach the security labels and log the numbers on them, and return the module to the customer by the FTI Trusted Distribution (Section 3.5).

6) Replace the old module with a new one. *Perform activation sequence on the replacement module,* log all part numbers, attach the security labels and log the numbers on them, and return the new module to the customer by the FTI Trusted Distribution.

BIBLIOGRAPHY OF REFERENCES

[1] FIPS140-1, “Security Requirements for Cryptographic Modules”, Federal Information Processing Standards Publication 140-1, U.S. Department of Commerce/NIST, National Technical Information Service, Springfield, VA (1994).

[2] “Information for FIPS 140-1 Certification of the NetFortress”, Fortress Technology, Inc., Tampa, FL (September, 1997).

[3] Havener, W.N.; Medlock, J.; Mitchel, L.D; Walcott, R.J; “Derived Test Requirements for FIPS PVP 140-1, Security Requirements of Cryptographic Modules”, NIST/MITRE, (March, 1995).

[4] NIST Special Publication 800-14, “Generally Accepted Principles and Practices for Securing Information Technology Systems”, Swanson, M. and Guttman, B.; U.S. Department of Commerce, Technology Administration/NIST, (September, 1996).