Non-Proprietary Security Policy for the NetFortress™ Cryptographic Kernel Version 4.0 with Standard and Segmented Modes of Operation

October 8, 2003

Security Policy v4.3

This security policy of Fortress Technologies, Inc., for the NetFortress™ Cryptographic Kernel Version 4.0 defines general rules, regulations, and practices for NIST validated FIPS 140-1 security level 1 NetFortress™ NF Crypto Kernel products in the "Standard"/encrypted and "Segmented"/bypass operation modes. The rules and regulations defined by this Security Policy have been and must be followed in all phases of the security projects, including the design, development, manufacture, service, delivery and distribution, and operation of products.

Contents

Figures and Tables

1.0 Introduction

This security policy includes all security rules under which the NetFortress™ Cryptographic Kernel (NF Crypto Kernel) must operate (and enforce), particularly rules derived from FIPS security requirements and those derived from additional security requirements imposed by the manufacturer.

The NF Crypto Kernel is a software system. According to FIPS 140-1 terminology, the NF Crypto Kernel is a multi-chip standalone cryptographic module, whose cryptographic boundary is the self-contained compiled code that is installed by the Vendor at the Vendor's laboratory or at the customer's site into production-quality compliant computer hardware, which constitutes the module physical boundary.

The NF Crypto Kernel software, installed on production-quality computer hardware, is an *electronic encryption device* designed to prevent a hacker from "sniffing" and reading data transferred across the Internet or other network. Authorized personnel only, such as the crypto officer, can log into the module. It applies secure authentication, coupled with encryption techniques, (3DES and DES, as well as IDEA for commercial, non-FIPS validated application), and advanced security protocols. Most of the security protocols are implemented without human intervention to reduce the opportunity for human error.

The NF Crypto Kernel operates at the network layer (IP) of the OSI model as shown in Figure 1.1. The network (IP) layer in the OSI model is "below" the layer utilized by most firewalls.

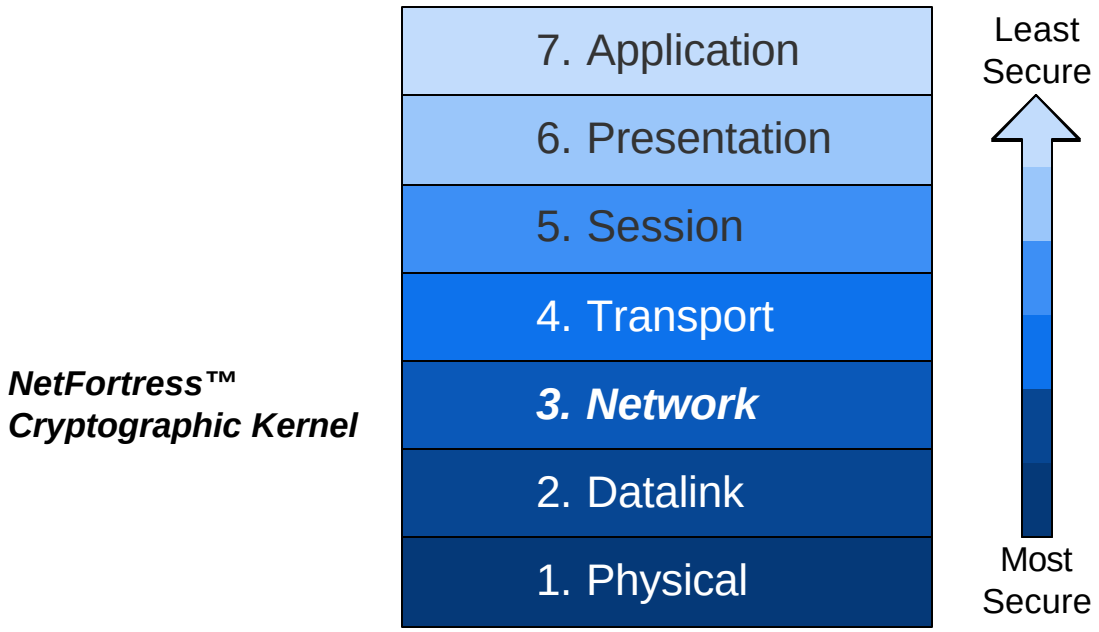

Figure 1.1: The Seven Layers of the OSI Reference Model

The NF Crypto Kernel requires no special configuration for different network applications. Its security protocols are implemented without human intervention to prevent any chance of human error. It provides an inexpensive, effective tool for building Virtual Private Networks over the Internet. It is also useful for securing communication within enterprise-wide intranets. A n example application of the NF Crypto Kernel is shown in Figure 1.2.

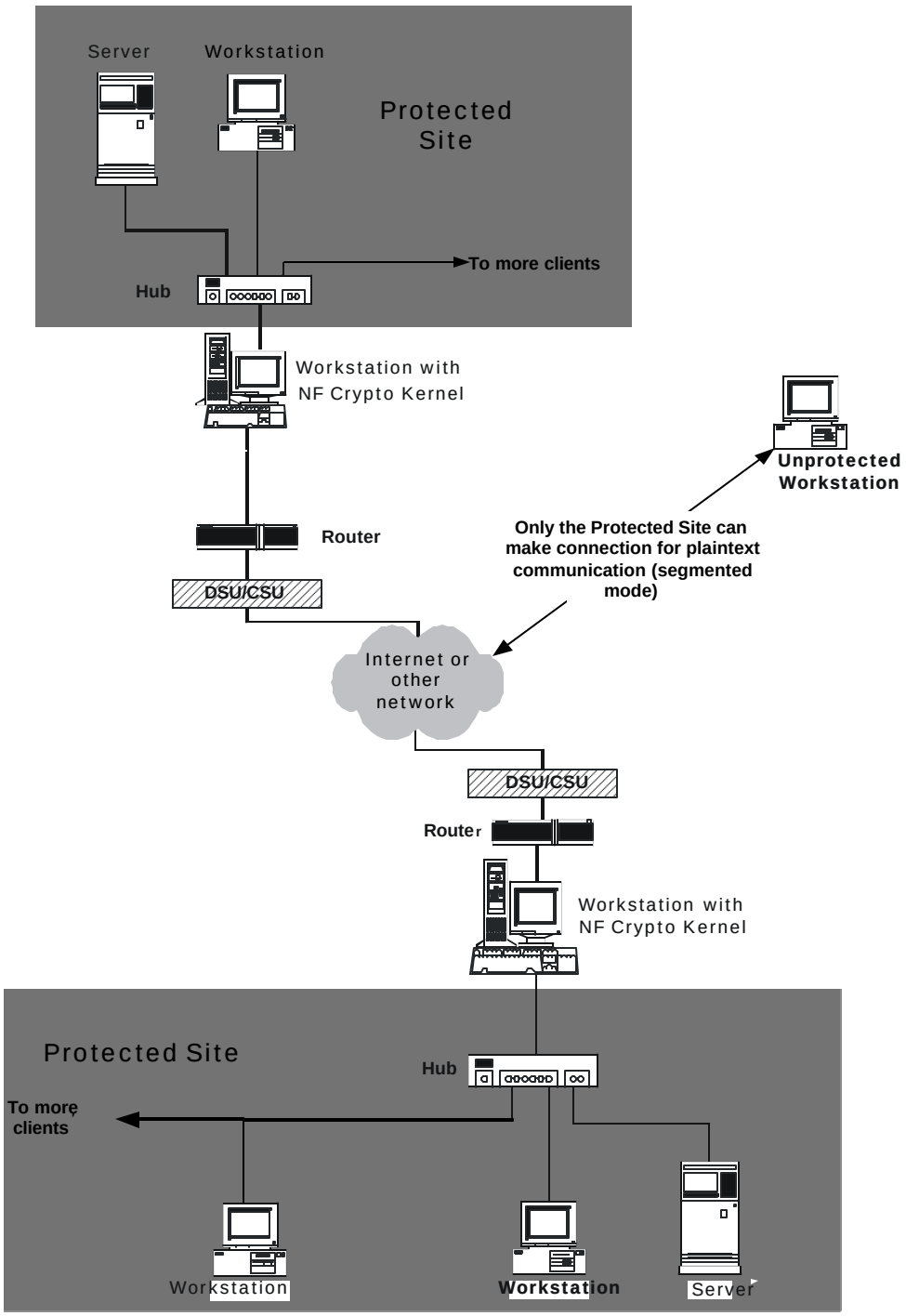

Figure 1.2: Example application of the NF Crypto Kernel

2.0 Overview of the NF Crypto Kernel Security Level Specification

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 approved at overall Security Level 1.* The document specifically covers the Fortress Technologies, Inc., security policy for the following features defined in the FIPS PUB 140-1 document and listed in Table 2.1.

Table 2.1: The NF Crypto Kernel Security Level Specification

FIPS 140-1 Categories	Security Level
Cryptographic Module	1
Module Interfaces	1
Roles and Services	2
Finite State Machine	1
Physical Security	1
Software Security	3
Operating System Security	N/A
Cryptographic Key Management	1
Cryptographic Algorithms	1
EMI/EMC	1
Self-Tests	1

2.1 The Cryptographic Module

FTI has implemented the following principal security rules in the NetFortress™ Cryptographic Kernel design, development, and application:

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

The following five security design concepts were developed to fulfill these objectives and the security requirements listed in the Table 2.1:

1. Minimize the human intervention to the module operation by supporting a high degree of automation. The automation is important, because the module as a commercial product is intended to be used in a variety of security environments (targeted at a moderate level, or Security Level 1 (L1) per the FIPS PUB 140-1 security level definitions) by a variety of customers.
2. 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.

3. Create and assign a unique *Company Proprietary Signature (CPS)* to each customer organization and a unique *Company Security Identifier, (CSI)* within a company, a group or division thereof, defined by the customer. During installation, the *CPS* is placed into the software of every cryptographic module that is used to establish the customer's VPN. All key exchanges between the modules of a particular VPN are encrypted by the *Module's Secret Key* and thus protected from unauthorized modification and substitution. Using a unique *CSI* ensures that only modules with the same *CSI* can exchange keys and establish a secure VPN; all other modules are excluded.
4. Prevent the module from being used fraudulently, if stolen after installation at a customer's site. The following two consecutive steps enforce this concept:
    - Activating the module at the factory.
    - Installing and deploying the kernel, including the initial startup and the first outgoing message procedures, performed at the customer's site. Performing these steps permanently attaches the module to a customer's site.
5. The NF Crypto Kernel can be installed only in security level 1 (production grade, as defined by FIPS PUB 140-1) computer hardware at the customer's site or at Fortress Technologies, Inc.

The NF Crypto Kernel can be purchased and subsequently used in one of two modes of operation:

- *Standard*: The NF Crypto Kernel standard module provides secure (ciphertext) communication with other NF Crypto Kernel protected sites (nodes) in a network.
- *Segmented*: The segmented mode of operation provides secured communication (equivalent to *Standard mode*) in a network with other NF Crypto Kernel protected sites, but it also provides (bypass service) unsecured (plaintext) communication. If a secured site (with NF Crypto Kernel) initiates the communication by sending a plaintext message (See Figure 1.2) the module will recognize and process the plaintext response. The module indicates when an encrypted or unencrypted (bypass) packet leaves using standard indicators available on the hardware (LEDs, audible alerts, and so forth).

The mode of operation is set at the manufacturer's site. Once set, the mode of operation can only be changed through a reinstallation of the module. A crypto-officer, or any other operator, does not have the capability to modify the mode of operation.

2.2 Module Interfaces

The NF Crypto Kernel interfaces (APIs) include:

- Client side interface (designated as *eth0* or *unencrypted*): a port for plain-text data input/output streams.
- Network side interface (designated as *eth1* or *encrypted*): a port for ciphertext data input/output streams through the standard mode, and for cipher- or plaintext data input/output streams through the segmented mode of operations.
- Control interface physically shared with the client and network side interfaces.
- Status output interface, which may include the computer hardware LEDs, speaker, the GUI on the service monitor, which also indicates the modes of operation (that is, standard or segmented/bypass.

In the case of NF Crypto Kernel, the data interfaces should not be thought of as separate data entry and exit ports. Each interface serves, as both a data entry and an exit port, since the data streams through both interfaces are *bi-directional* and conforming to the real-time, two-way

information exchange over the network. Data includes Ethernet packets of IP, ICMP, and IGMP protocols.

Neither cryptographic key management nor data authentication use separate ports. Cryptographic key exchanges between communicating modules proceed by using IP (key) packets.

2.3 Roles and Services

The module performs role-based authentication. Crypto-Officers are authenticated with the use of a password. Users are authentication by knowledge of the module's secret key.

2.3.1 Roles

One of the basic security design concepts of the module was to automate the device's functions, as much as possible, to *minimize human intervention* in its operation. Another basic security concept was to prevent the module's illegal use if it were stolen after installation at a customer's site. These security concepts were successfully implemented in the NF Crypto Kernel. The implementation results in a *reduced set of authorized tasks* supported by the module.

Most of the authorized tasks usually performed by a crypto officer in earlier cryptographic devices—cryptographic key management, key and parameter entry or zeroization, key cataloging, and so forth—are automated in the NF Crypto Kernel. The crypto officer role is, consequently greatly simplified.

The automated security functions cannot be accessed or monitored. The parameters are contained in the inaccessible storage medium and the results of the security functions (common secret keys, encryption subkeys, and so forth) are automatically checked and stored for future use in the volatile memory of the module. Some security parameters (dynamic secret keys, encryption subkeys) change periodically, and regenerate after a reboot. Because they are stored in volatile memory, these parameters are not retained when the module is powered off or when a power loss occurs.

As previously noted, most of the standard crypto officer tasks associated with the module's operation are now automated. However, the crypto officer must still perform certain tasks. These are:

- Installing the module and connecting it to the customer's systems.
- Providing Discretionary Access Control (DAC) to operate the module only with the crypto officer's ID and password.
- Initiating the first outgoing message, thus preventing the unit's illegal use if stolen. After installation, the first message passing through the module writes the IP and MAC addresses of its client(s) into the module's storage memory, which implies the rule: "Access is restricted to only authorized personnel of the legitimate customer." The write-in process results in an additional advantage for the legitimate user: Once a NF Crypto Kernel is installed at a site (i.e., with a client computer or at a Class C LAN), it cannot be used at another site. This protection also means that if the customer wants to relocate the device to a new site belonging to the same customer, the module must be returned to Fortress Technologies for reprogramming.
- Performing administrative functions of the system through the terminal attached to the module's control interface. This action automatically applies zeroization of critical security parameters in the NF Crypto Kernel.
- Accessing and initiating the zeroization action that erases all security and data contents of the module's file storage medium, thus making the unit inoperable.

Those crypto-officer tasks associated with the customer's systems should be included in the customer's own security policy, which either remains valid or very likely will be revised to include the features and services of the NF Crypto Kernel (a potentially significant change). How the crypto officer role is redefined depends on the security mode of operation, the type of information processed, and the degree of the security risk to the customer's site.

The user tasks are even more simplified than those of the crypto officer by the module's automated operation. User tasks are as follows (functions related to a segmented/bypass mode of operation only are indicated with an asterisk *):

- Monitoring the module's operation (check status).
- Monitoring the physical integrity, connectivity, and security of the module.
- Performing power resets and power-up self-tests of the computer (rebooting is the only way a user can initiate the module's self tests).
- *Initiating the bypass mode operation (for the segmented configuration only as described in the NF Crypto Kernel User Manual)

The module does not support multiple concurrent authorized operators.

The NF Crypto Kernel Roles are summarized in Table 2.2.

Table 2.2: Summary of Roles of NF Crypto Kernel

Roles	Crypto Officer	User
Installing and connecting the module to the client systems	X	
Establishing DAC to operate the module	X	
Performing diagnostics and troubleshooting	X	
Initiating zeroization	X	
Performing module administration.	X	
Monitoring the status of the module's operation mode	X	X
Monitoring physical integrity, connectivity, and security	X	X
Performing power resets and power-up self-tests of the computer	X	
Initiating bypass operation in the "Segmented" mode	X	X
Encryption/Decryption		X
Implementing a customer's security policy		X

Table 2.3: Access Table

Cryptographic Service/CSP	Role	Access
Symmetric Keys	Automatic	N/A
Asymmetric Keys	Automatic	N/A
Hashing	Automatic	N/A
Password	C-O	Write
Zeroization	C-O/ or Automatic	Execute
Self-test	C-O/ or Automatic	Execute
Set Segmented Mode	C-O, User	Read/Write

2.3.2 Services

The design concepts of the NF Crypto Kernel clearly define the basic services that the module is expected to perform to protect a single client or a particular network from potential security threats and serve as an automated tool to build Virtual Private Networks over the Internet.

After installation, the module serves as a cryptographic co-processor for the client systems and performs the following *automated services* (services related to a segmented/bypass unit only are indicated with an asterisk *):

1. *Key Management Operations*: *performed automatically during the module operation:*
    - Restricting key exchange to within the company using the *Company Security Identifier (CSI)* (*Crypto-Officer*).
    - Generating the module's own key pairs (*User*).
    - Generating crypto keys by encrypted Diffie-Hellman key exchanges (*User*).
    - Initiating dynamic cryptographic key exchange once every 24 hours after the connection and key exchange are established (*User*).
    - Maintaining data tables (the *Host table,* containing information on all contacted sites both secured and unsecured; the *MAC table,* for LAN type modules containing the IP and MAC addresses of all its clients) (*Crypto-Officer*).
    - Module power-off, power-on, reset, zeroization (*Crypto-Officer*).
2. *Cryptographic operations and management: performed automatically during the module operation (all User services):*
    - Classifying/filtering packets and protocols.
    - Encryption/decryption on network layer (all sensitive packet header information is hidden).
    - Strong authentication of sender; encrypted checksum in dynamic key packets assures that the communicating parties *share the same static common secret key.*
    - Strong authentication of the origin of a message packet; the encrypted checksum assures that the communicating parties *share the same dynamic common secret key.*
    - Integrity tests of encryption/decryption and the data integrity in transit by using checksums.
    - *Bi-directional cipher communication with secured sites and user (client) originated

plaintext communication with unsecured sites.

3. *Self-Tests: performed automatically each time at the system power-up and/or by demand of the Crypto-Officer.*

2.4 Finite State Machine

The NF Crypto Kernel is built to conform to a Finite State Machine (FSM).

2.5 Physical Security

The module's physical security is provided by the computer hardware housing the module and the customer's security policy. The NF Crypto Kernel is installed by the Fortress Technologies, Inc., in a security level 1 (i.e., production grade), FCC-approved hardware, which also defines the crypto module physical boundary. The NF Crypto Kernel can be installed in a computer with the following features:

- Any x86 processor
- 32 MB file storage media (for example, a hard drive or a flash drive)
- At least 124 MB available DRAM
- At least one free serial port
- Two network connections

2.6 Software Security

The NF Crypto Kernel software is written in C and C++ and operates on the Linux operating system. The software is installed in the host hardware storage medium in executable format. All maintenance must be performed by qualified and authorized Fortress Technology, Inc., Security Officers. No cryptographic keys are stored in the module's permanent memory except the Company Proprietary Identifier and its SHA-1 function, the Module's Secret Key. With the exception of the Module's Secret Key, they are all automatically zeroized at the system shutdown.

2.7 Operating System Security

The NF Crypto Kernel operates automatically after power-up. The module provides no means whereby an operator could load and execute software or firmware that was not included as part of the module's validation. Thus FIPS PUB 140-1 requirements associated with operation system security, as required are not applicable to the NF Crypto Kernel.

2.8 Cryptographic Key Management

The FIPS 140-1 required Cryptographic Key Management are performed automatically by the NF Crypto Kernel itself, except the *Module's Secret Key,* which is permanently written in the host hardware flash memory in executable format.

2.8.1 Key Generation

The NF Crypto Kernel applies five cryptographic keys:

- Module's Secret Key.
- Static Private Key.
- Static Public Key.
- Static Secret Key

- Dynamic Private Key.
- Dynamic Public Key.
- Dynamic Secret (session) key

2.8.2 Protocol Support

The NF Crypto Kernel supports the Diffie-Hellman, SHA-1, (NIST Certification Number 34) and automatic key re-generation of the Dynamic Common Secret Key between two modules in every 24 hours or at the system power up**.**

2.8.3 Key Storage

No encryption keys are stored permanently in the module's hardware, except the *Module's Secret Key* in executable format in the storage memory.

2.8.4 Zeroization of Keys

The Static and Dynamic keys of the NF Crypto Kernel are automatically zeroized when the system is turned off, and are regenerated at every boot-up of the host hardware. All keys, including the *Module's Secret Key*, can be zeroized only by the crypto officer though the module's terminal. (See the user manual.)

2.9 Cryptographic Algorithms

The AF Gateway applies FIPS-validated 3DES, DES and SHA-1 algorithms. Diffie-Hellman is, provided for FIPS validated operation. The IDEA algorithm is available for non-FIPS validated operation.

2.10 EMI/EMC

All EMI/EMC issues are hardware related, thus the responsibility of the customer. Fortress Technologies installs the NF Crypto Kernel only on FCC-compliant computer hardware.

2.11 Self-Tests

This section provides information for the self-tests performed of the standard and the segmented modes of operations. It addresses the test categories such as the power-up tests and the conditional tests, when a module performs a particular function or operation.

The following list of all self-tests includes both power-up tests and conditional tests. These tests are almost identical for the standard and segmented modes. (Items marked with an asterisk (*) are additional test(s) performed in the segmented/bypass mode).

A. Power-Up Tests

- Standard Power-On Self Test (POST)
- Basic Input-Output System (BIOS) Test
- Linux Operating System Boot Test
- Known Answer Test, (with DES, TDES and SHA-1)
- Authenticity Check of the FTI Executable Programs
- Flash Checksum Test
- *Bypass Test (for Segmented Mode only)

B. Conditional Test

- Continuous Random Number Generation Test
- Double Integrity (Pair-wise Key Consistency Integrity and Message Transit Integrity) Test

Power-up tests involve self-tests, six of which are common to both modes, (i.e., the standard and the segmented ones)**.** These are executed when the module is first powered on.

The conditional critical function tests include two tests, which are also common to the standard and segmented modes: A mandatory self-test for Continuous Random Number Generation and a double integrity test.

The Continuous Random Number Generation Test is performed whenever a pseudorandom number is generated by the ANSI X9.31 (A.2.4) Pseudo-Random Number Generator, as the module is initializing and prior to cryptographic processing. The double integrity test is performed while the module is in the user service substate of the operational state.

3.0 Customer Security Policy

FTI expects that after the module's installation, any potential *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the module(s) and the customer's network(s) must operate. This security policy is expected to include multilevel DAC. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

4.0 Maintenance

Only the Fortress Technologies security officer can perform maintenance and upgrade procedures, on the NF Crypto Kernel either at the customer's site or at Fortress Technologies. This requirement includes the software reinstallation of the NF Crypto Kernel. The host computer hardware maintenance is the customer's responsibility.

- * - * -

End of the "Non-Proprietary Security Policy for the NetFortress™ Cryptographic Kernel, V-4.0 with Standard and Segmented Modes of Operation" document.