# Cylink's
# NetHawk

# FIPS 140-1 Non-Proprietary
# Security Policy

**Level 2 Validation**
**April 2002**

# Table of Contents

# 1 INTRODUCTION

## *1.1 Purpose*

This is a non-Proprietary FIPS 140-1 Security Policy for the Cylink NetHawk. The Security Policy describes how the NetHawk meets all FIPS 140-1 Level 2 requirements, and was prepared as part of the NetHawk's FIPS 140-1 certification submission package.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1) is a U.S. Government standard entitled "*Security Requirements for Cryptographic Modules*." This standard mandates a set of strict design and documentation requirements that hardware and software cryptographic module must meet in order to be certified by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre de la Sécurité des Télécommunications (CST).

This document is intended for use by FIPS 140-1 evaluators, NIST and CST reviewers, and others interested in how the NetHawk meets all FIPS 140-1 Level 2 requirements.

## *1.2 References*

This FIPS 140-1 Security Policy describes features and designs of the NetHawk using the technical terms of FIPS 140-1.

- For more information on the FIPS 140-1 standard and validation program readers are referred to the NIST web site at http://csrc.nist.gov/cryptval/.

- For more information on the NetHawk product, please visit the Cylink web site at http://www.cylink.com.

## *1.3 Terminology*

In this document the Cylink NetHawk is referred to as the module, the NetHawk device, the device, and the NetHawk.

## *1.4 Document Organization*

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

♦ Vendor Evidence document
♦ Finite State Machine
♦ Module Software Listing
♦ Other supporting documentation as additional references

This document provides an overview of the NetHawk and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the NetHawk. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Cylink-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cylink.

# 2 NetHawk

The Cylink NetHawk is a high-performance, standards-based hardware Virtual Private Network (VPN) and firewall. Providing a high speed, low cost solution, it features the strongest cryptography available and complete manageability. Cylink custom designed a state-of-the-art Application Specific Integrated Circuits (ASIC) for the NetHawk that allow line-speed encryption with Data Encryption Standard (DES) *and* triple-DES.

The NetHawk supports the internationally standardized Internet Protocol Security (IPSec) protocol and Internet Key Exchange (IKE) protocol. Whether securing an enterprise perimeter, a corporate sub-network, or a single host, the NetHawk controls network access and gives administrators a complete toolbox of functionality. The NetHawk includes the following features:

? An embedded firewall secures against network-level attacks
? IPSec support including IKE (using all modes – main, aggressive, and quick)
? X.509 v3 Digital Certificates, Public Key Infrastructure Certificate Management Protocol (PKIX CMP), and pre-shared keys
? Strong cryptography using DES, Triple-DES, SHA-1, and Digital Signature Algorithm (DSA).
? Tamper-resistant/evident case
? Encryption to enforce policy and provide data privacy
? Centralized, remote management using SNMPv2 and TFTP.
? Secure automated software upgrades and security policy updates

The NetHawk acts both as a proxy and a perimeter guard. The module allows you to create enterprise-wide Virtual Private Networks and to securely link distributed networks by adding a single device in front of the network.

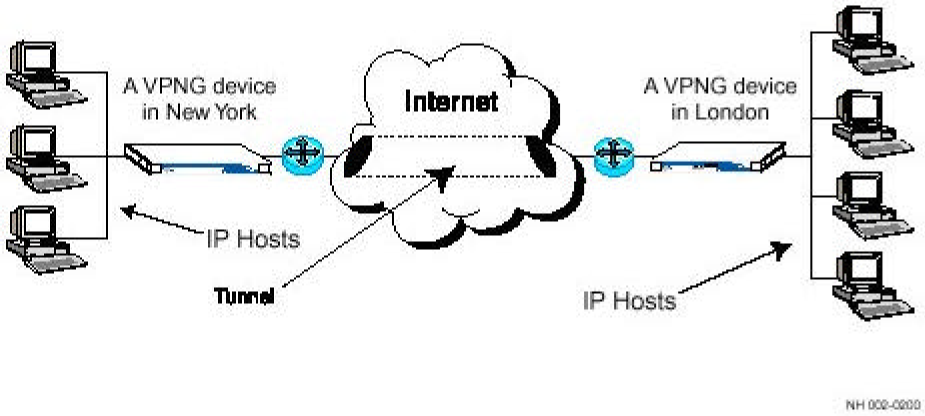


**Figure 1 – NetHawk Securely Links Remote Networks**

## *2.1 Strong Security Inside and Out*

In FIPS terms, the NetHawk is a multi-chip standalone module. It has been evaluated as meeting all FIPS 140-1 requirements at level 2 or higher security. The NetHawk features strong physical security with its tamper-evident case, extruded sheet metal construction, and a Cylink iridescent sticker. The entire module is encapsulated by the steel case that forms the cryptographic boundary, and only specified physical interfaces provide access to the module.

**Figure 2 – The Steel-Cased NetHawk Features Tamper Response Circuitry**

The NetHawk responds to attempts to access its secure internal key storage by power cycling the device, which destroys sensitive cryptographic materials rather than let them be exposed. Two screws, which must be removed in order to gain access to the internals of the module, are connected to micro-switches. While the NetHawk is turned on, if a certain one of these screws is even partially removed, the NetHawk activates tamper-response. While powered off, if the other of these screws is even partially removed, the module will detect the tamper upon the next boot cycle and will not support any cryptographic processes. Tamper evidence for the NetHawk includes dents and scratches in the metallic case, damage to the sticker, alarm and/or error indicators lit, and severe deformation of the front and rear panels.

The module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (Class B), and is labeled in accordance with FCC requirements.

## *2.2 Standards-based Interfaces*

The NetHawk has status indicators on the front panel that allow quick and easy assessment of the working condition of the module. These indicators show whether the module has been tampered with, if an error has occurred, whether the power is connected, and if cryptographic operations are taking place. Figure 3 depicts the front panel of the module.

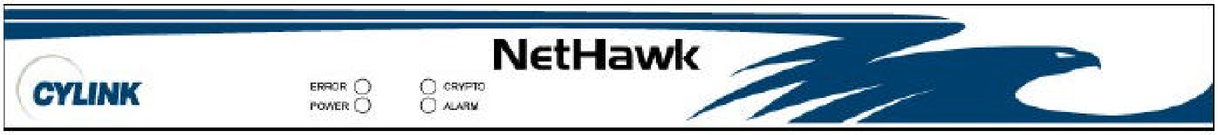


**Figure 3 – Indicators Show The Status Of The Device**

The NetHawk provides Dual 10/100BaseT Ethernet Ports that allow it to plug directly into an existing network.

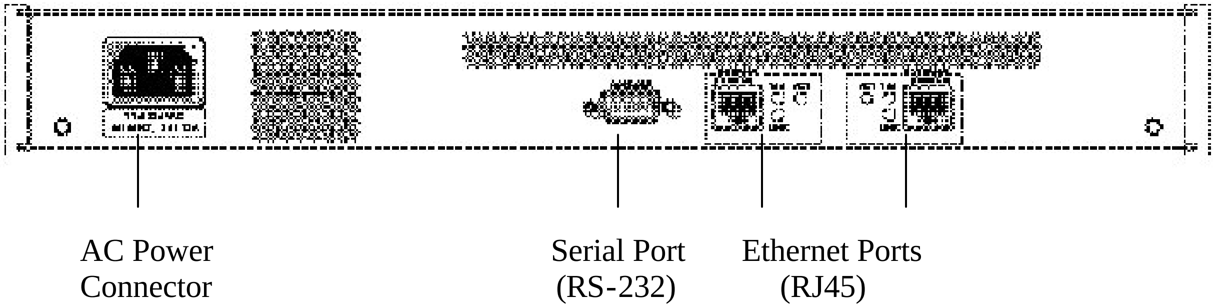


**Figure 4 – Standard Interfaces Plug Directly Into Your Network**

As shown in Figure 4 above, the internal (straight jack) and external (crossover jack) Ethernet ports (10/100baseT) are on the rear panel of the NetHawk. There is also a standard serial port for local configuration. Some local management and monitoring services are available through the Serial port. However, using the secure PrivaCy Manager for NetHawk, an administrator can conveniently and remotely access and modify all configurations of the NetHawk through the Ethernet ports. Secured IPSec connections allow administrators to securely monitor and administer the NetHawk from almost anywhere.

| FIPS 140-1 Logical Interfaces | Adapter physical interfaces |
|---|---|
| Data Input Interface | Internal/external Ethernet ports |
| Data Output Interface | Internal/external Ethernet ports |
| Control Input Interface | Internal/external Ethernet ports, Serial port, AC power connector |
| Status Output Interface | Internal/external Ethernet ports, Serial port, LEDs |
| Power Interface | AC power connector |

**Table 1 – Interfaces**

Table 1 shows the mapping of the FIPS140-1 logical interfaces to the module’s physical interfaces.

## *2.3 Roles and Services*

The NetHawk employs role-based authentication of its operators and supports four roles: Local and Remote Crypto-Officer and Local and Remote User.

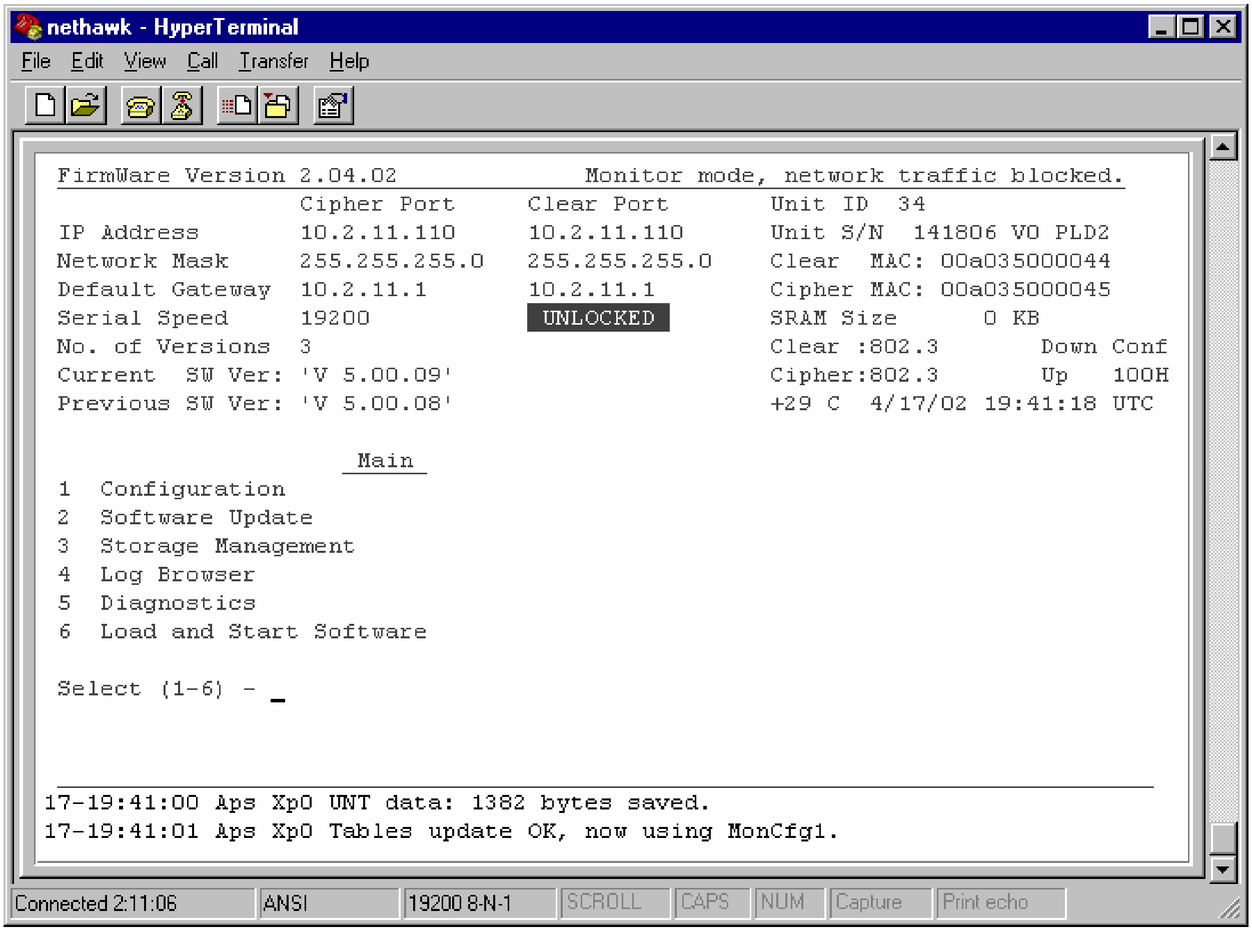
> The Remote Crypto-Officer role is responsible for the initial configuration and activation of the NetHawk. The Remote Crypto-Officer interfaces with the NetHawk using the PrivaCy Manager for NetHawk over an IPSEC secured Ethernet port. This role has access to all remote services provided by the module and is able to modify all sensitive settings.

The Local Crypto-Officer role is responsible for limited configuration of the module. The Local Crypto-Officer interfaces with the NetHawk using the Command Line Interface (CLI – shown in Figure 5a below) through the serial port. This role has access to all local services provided by the module. This menu is activated only during power up.

An additional runtime menu is available for device monitoring and minimal network parameter configuration. (CLI – shown in Figure 5B below)

The Remote User role is able to remotely view detailed status information and change specific non-security related settings. The User interfaces with the module using the PrivaCy Manager for NetHawk over an IPSEC secured Ethernet port. This role is permitted to change certain configuration parameters, and view detailed logs and the status of the module.

The Local User role is able to view status information and change certain non-critical settings. The User interfaces with the module using the CLI/RM (CLI/RM – shown in Figure 5a/5b below) through the serial port in order to change certain configuration parameters, and view logs and the status of the module. The User can also look at the status indicators located on the front and back of NetHawk.



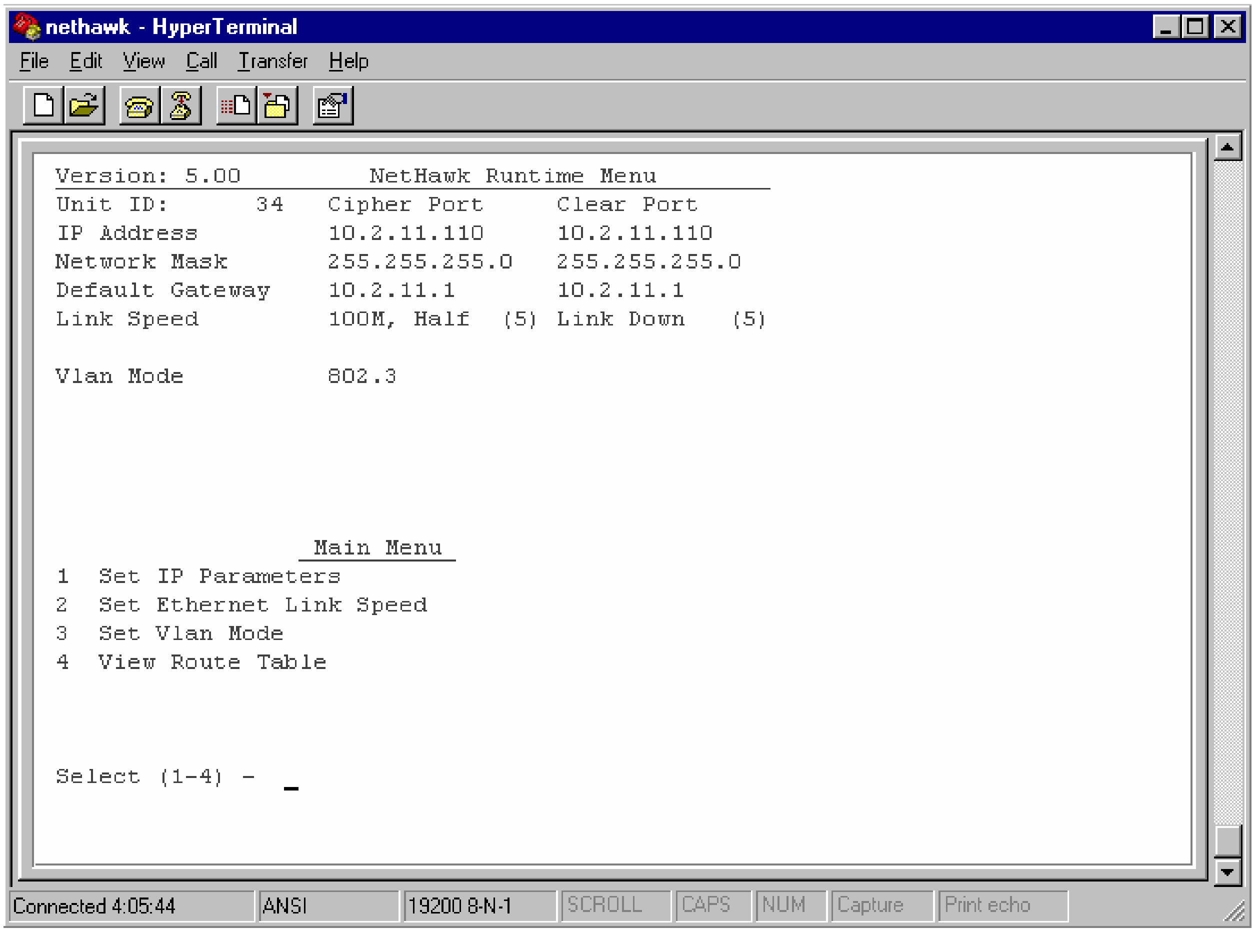
```
FirmWare Version 2.04.02             Monitor mode, network traffic blocked.
                 Cipher Port     Clear Port       Unit ID  34
IP Address       10.2.11.110     10.2.11.110      Unit S/N  141806 V0 PLD2
Network Mask     255.255.255.0   255.255.255.0    Clear  MAC: 00a035000044
Default Gateway  10.2.11.1       10.2.11.1        Cipher MAC: 00a035000045
Serial Speed     19200            UNLOCKED        SRAM Size      0 KB
No. of Versions  3                                Clear :802.3       Down Conf
Current  SW Ver: 'V 5.00.09'                      Cipher:802.3       Up   100H
Previous SW Ver: 'V 5.00.08'                      +29 C  4/17/02 19:41:18 UTC

                     Main
1  Configuration
2  Software Update
3  Storage Management
4  Log Browser
5  Diagnostics
6  Load and Start Software

Select (1-6) - _

17-19:41:00 Aps Xp0 UNT data: 1382 bytes saved.
17-19:41:01 Aps Xp0 Tables update OK, now using MonCfg1.
```

**Figure 5a – Command Line Interface (CLI)**



```
Version: 5.00          NetHawk Runtime Menu
Unit ID:       34   Cipher Port      Clear Port
IP Address          10.2.11.110      10.2.11.110
Network Mask        255.255.255.0    255.255.255.0
Default Gateway     10.2.11.1        10.2.11.1
Link Speed          100M, Half   (5) Link Down   (5)

Vlan Mode           802.3




                   Main Menu
1  Set IP Parameters
2  Set Ethernet Link Speed
3  Set Vlan Mode
4  View Route Table



Select (1-4) -  _
```

**Figure 5b – Runtime Menu (RM)**

A remote operator using the PrivaCy Manager for NetHawk software initially authenticates to the module using DSS within the IKE protocol. The communication between remote operators and the module is secured: packets are encrypted, protected for data integrity, and both sides are authenticated. Authentication is performed as part of the IPSec SA negotiation, and all module configurations are performed securely (encrypted and authenticated). The device supports DSS and RSA authentication methods. However, when the device is operating in FIPS mode, only DSS can be used.

An operator using the CLI must input a password to access certain sensitive settings. This password is set when changing the CLI from an unlocked to locked mode.

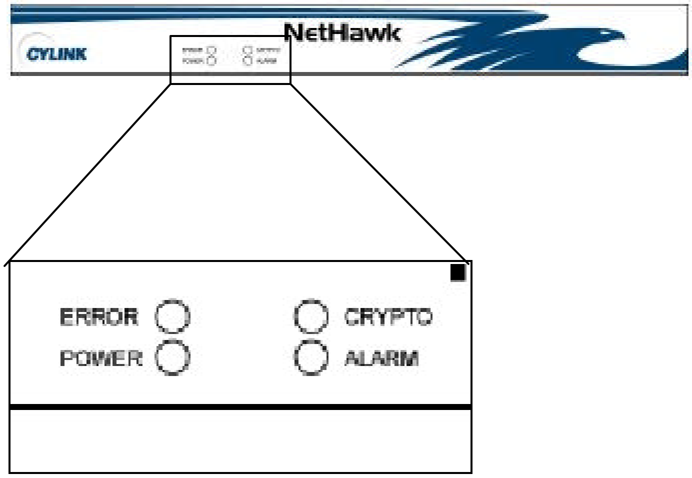


**Figure 6 – Front Panel Indicators**

### 2.3.1 *Remote Crypto-Officer Services*

- Access to all of the module's remote services including the Remote User Services (Section 2.3.3)
- Remotely configure and monitor the module through the Ethernet ports using PrivaCy Manager for NetHawk - using the Privacy Manager for NetHawk software, the Crypto-Officer is able to access all configuration settings of the module, including:
  - All actions possible through the CLI
  - Creating/modifying security policies
  - Creating/modifying security types
  - Creating/modifying protocol profiles
  - Creating/modifying network objects
  - Creating/modifying VPNs and maintaining them
  - Performing key management
  - Resetting the module
  - Certifying the module
  - Activating the module's cryptographic services
  - Configuring the module
  - Maintaining the module
  - Upgrading the firmware
  - Create user and set privileges.
- Cryptographic services are provided as the device encrypts the specified tunnels.

### 2.3.2 *Local Crypto-Officer Services*

- Access to all of the module's local services including the Local User Services (Section 2.3.4)
- Configure and monitor the module through the serial port using the Command Line Interface (CLI) – using the CLI, the Local Crypto-Officer is able to:
  - Upgrading the firmware
  - Re-initializing the module's firmware
  - Clearing tampers
  - Locking/unlocking the CLI
  - Setting the time
  - Viewing limited logs
  - Changing temperature settings
  - Run diagnostics

### 2.3.3 *Remote User Service*

- Access to a variety of status information and limited configuration ability
- Remotely configure and monitor the module through the Ethernet ports using PrivaCy Manager for NetHawk - using the Privacy Manager for NetHawk software, the Remote User is able to access non-critical configuration settings of the module, including:
  - Viewing detailed status and log information
  - Setting the time and time

### 2.3.4 *Local User Services*

- Access to a variety of status information and limited configuration ability
- Front Panel LED Status – the front panel LEDs (see Figure 6 above) provides four basic status indications: Power, Error, Crytpo and Alarm.
- Rear Panel LED Status – the rear panel provides 6 LEDs for status indications of the network ports (3 per port): Act, 100, and Link.
- Monitor the module through the serial port using the Command Line Interface (CLI) – using the CLI, the User is able to:
  - Starting the module
  - Modify VLAN parameters
  - Modify link speed parameters
  - Initialize network parameters prior to certification from Privacy Manager

- Configure and monitor the module through the serial port using the runtime menu (RM) - using the RM, the Local User is able to:
  - Modify VLAN parameters
  - Modify link speed parameters
  - Initialize network parameters prior to certification from Privacy Manager

### *2.4 Standards-based Cryptography and Key Management*

Always adhering to the cryptographic standards, NetHawk provides the strongest cryptography available. NetHawk supports IPSEC/ESP data encryption, IPSEC/ESP data integrity (with the prescribed NULL encryption algorithm), and IPSEC/AH for data integrity in Tunnel mode. NetHawk implements all IKE modes: main, aggressive, and quick, using ISAKMP per RFC. The NetHawk, with the following algorithms, supports these features:

**Data Encryption**

- DES-CBC (56 bits) – as per NIST FIPS PUB 46-3
- Triple DES-CBC (168 bits) – as per NIST FIPS PUB 46-3

**Data Packet Integrity**

- DES-MAC (64 bits) – as per NIST FIPS PUB 113 and ANSI X9.9
- HMAC-MD5 (16 bytes) – per RFC 2104 (HMAC: Keyed-Hashing for Message Authentication).
- HMAC-SHA1 (20 byte) – per draft-ietf-ipsec-auth-hmac-sha1-96-03.txt.

**Authentication**

? DSA – as per NIST FIPS PUB 186-2
? RSA – vendor affirmed to PKCS#1
? All IKE modes – main, aggressive, and quick per RFC
? Pre-shared key

The NetHawk implements key management in compliance with IKE (Internet Key Exchange), negotiating Security Associations (SA) and agreeing upon session keys. The implementation supports Main, Quick and Aggressive modes using pre-shared secret keys, DSA signatures, or RSA signatures for authentication. Full DSA and RSA capabilities for digital signatures are provided.

Session keys are negotiated at the beginning of an SA lifetime, and can be set to automatically rekeyed after a given time limit, a specific amount of data has been transferred, authenticated request from Peer Gateway, or station manager request.

Each NetHawk ships with a Manufacturer Certificate (MC) and private key that gives the device a unique ID. The MC is signed using a DSA signature. The PrivaCy Manager for NetHawk uses the MC to initially authenticate the module. Before a NetHawk can be used, it must be certified. The PrivaCy Manager for NetHawk certifies the device by issuing it a Network Certificate (NC) and a new private key. The NC is used to authenticate sessions between the modules. The NC can be signed using DSA or RSA signature. Therefore, the possible authentication interactions are:

1. NetHawk to NetHawk
2. PrivaCy Manager for NetHawk to NetHawk

When the first secure connection is established between two devices, the NC exchange and SA exchange use the IKE protocol. The Network Certificate (NC) is used to authenticate secure connections and a session key is used to encrypt the packets. New session keys are negotiated for new connections or when a connection/session key is timed out. Each session uses a different session key.

## *2.5 Constant Self-monitoring*

The NetHawk monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-1. The module includes the following self-tests:

**Hardware Tests:** When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.
**Firmware Integrity Test:** After the hardware tests, the module performs signature verification to ensure firmware has not been modified.
**Cryptographic Algorithm KATs:** Known Answer Tests (KATs) are run at power-up for the DES and Triple DES encryption/decryption, and Message Authentication Codes.

**DES-CBC KAT**
**Triple-DES-CBC KAT**
**DES-MAC KAT**
**SHA-1 KAT**
**DSS KAT**
**RSA KAT**

**DSA Pair-wise Consistency Test:** All DSA operations are tested to ensure the correct operation of the DSA key generation, signatures, and SHA-1 hashing algorithms.
**RSA Pair-wise Consistency Test:** All RSA operations are tested to ensure the correct operation of the RSA key generation, signatures, and SHA-1 hashing algorithms.
**Continuous Random Number Generator Test:** This test is constantly run to detect failure of the random number generators in the NetHawk
**Management Configuration Files Integrity Test:** The module performs SHA-1 check value verification to ensure the configuration files have not been modified.
**Firmware Upgrade Test:** Module firmware can only be remotely upgraded from the management system with proper authentication to the module. However, in order to strictly control the loading of new firmware to the NetHawk, the new firmware must be digitally signed by Cylink using a DSA signature.

## *2.6 Secure Remote Management Software*

The NetHawk comes with powerful remote management software, PrivaCy Manager for NetHawk, that can be installed on an NT workstation. This software provides a simple, easy-to-use graphical interface to the configurations of the NetHawk. It also allows for extensive monitoring of the NetHawk, allowing an Administrator to remotely keep track of the module's status. All communications between PrivaCy Manager for NetHawk and the module are through the Ethernet ports over secure, authenticated IPSec tunnels. The SNMPv2 protocol and TFTP protocol are used to carry out the management services.

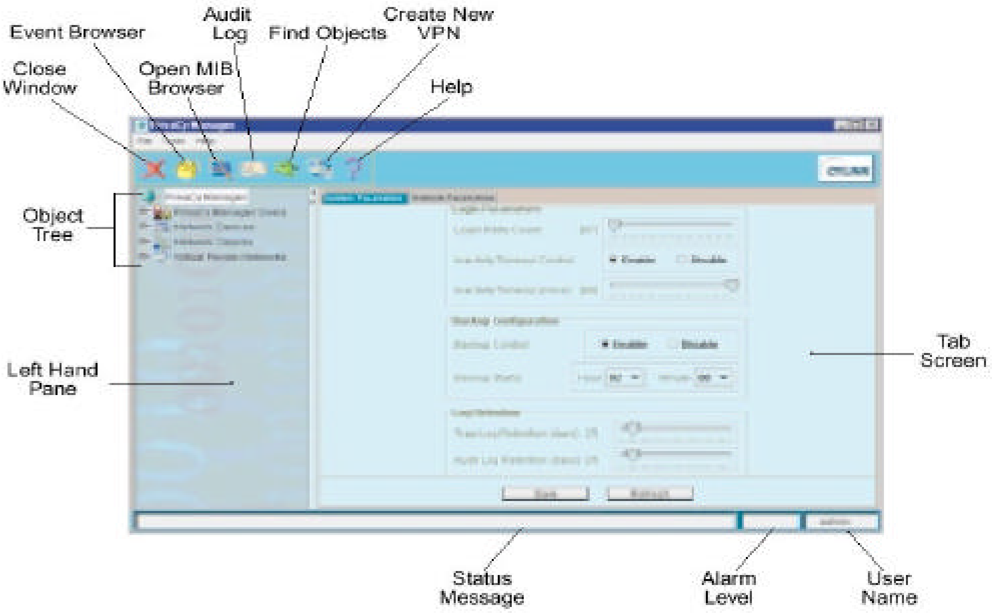


**Figure 7 – PrivaCy Manager for NetHawk**

Figure 7 is a screenshot of the PrivaCy Manager for NetHawk software. All of the management functions are conveniently and logically located in the GUI (Graphical User Interface). The status of the module is clearly shown, and all configurations of the module can be reached from the PrivaCy Manager for NetHawk's menus. An administrator can monitor and control the NetHawk, either on-site or off-site.

# 3 FIPS 140-1 Level 2 Compliant Mode

The NetHawk has the capability of operating in a FIPS 140-1 compliant manner and a non-FIPS 140-1 compliant manner. Therefore, it is necessary to ensure the module's proper configuration for running in a FIPS 140-1 compliant manner.

When operating in a FIPS 140-1 compliant manner, the CLI must be locked and a password set. Before the device is certified, the Remote Crypto-Officer must use proper methods to authenticate the module. The IP address of the device must be set through the Ethernet ports using the PrivaCy Manager for NetHawk software. All Crypto-Officer services must be accessed through secure, authenticated channels. Only the following FIPS-approved cryptographic algorithms may be used:

**Data Encryption**

- DES-CBC (56 bits) – as per NIST FIPS PUB 46-3
- Triple DES-CBC (168 bits) – as per NIST FIPS PUB 46-3

**Data Packet Integrity**

- DES-MAC (64 bits) – as per NIST FIPS PUB 113 and ANSI X9.9
- HMAC-SHA1 (20 byte) – per draft-ietf-ipsec-auth-hmac-sha1-96-03.txt.

**Authentication**

? DSA – as per NIST FIPS PUB 186-2
? RSA – vendor affirmed to PKCS#1

All traffic employing encryption and/or authentication must be encrypted using DES or Triple-DES and/or authenticated using DSA or RSA.

Message Authentication Codes (MACs) must be generated using HMAC-SHA1 or DES-MAC. HMAC-MD5 cannot be used.

The Cylink tamper-evident stickers should be affixed to the NetHawk under normal operating temperatures, and the surface for application of the stickers should be clean and dry.

Note: RSA is implemented as a "FIPS approved" algorithm that is vendor affirmed as it conforms to PKCS#1.

# 4 FIPS 140-1 Level 2 Non-Compliant Mode

The Remote Crypto-Officer will continue to use FIPS approved algorithms to initially authenticate the module. The user must decide to place the device into a non-FIPS 140-1 compliant mode by allowing policy to be set on the device that uses the non-compliant algorithms listed below. All Crypto-Officer services are accessed through secure, authenticated channels. The following are all cryptographic algorithms available in FIPS non-compliant mode:

**Data Packet Integrity**

- HMAC-MD5 (20 byte) – per RFC 2104 (HMAC: Keyed-Hashing for Message Authentication).

Message Authentication Codes (MACs) can be generated using HMAC-MD5.