FIPS 140-2 Security Policy

3Com Embedded Firewall PCI Cards

3Com Corporation
5403 Betsy Ross Drive
Santa Clara, CA 95054
USA

February 24, 2006

Revision Version 0.4

1. Introduction

The following describes the security policy for 3Com Corporation's 3Com Embedded Firewall PCI Cards. The card is available as a copper NIC (3CRFW200B) and a fiber NIC (3CRFW220B). The hardware version number for 3CRFW200B PCI Copper NIC is 03-0229-501 while that for 3CRFW220B PCI Fiber NIC is 03-0347-501. The 3CRFW200B family of NICs provides FIPS 140-2 validated IPSec (TDES/SHA-1) offloading and Embedded Firewall functionalities. The firmware version of the sleep image and reflash image running on the card is 03.101.015. The runtime and diagnostic images have firmware version number 03.101.015. The module is referred to as the 3CRFW200B throughout this document.

The 3CRFW200B is a PCI 2.2 based Ethernet Network Interface Card. It has an embedded ASIC that consists of among others ARM9 processor and an IPSec offload engine. The PCI interface allows the NIC to communicate with the host computer. The associated device driver, agent and the firmware for 3CRFW200B allow the Operating System to offload IPSec functionality to the NIC adapter, and afford the embedded firewall function.

The embedded firewall provides a centrally managed and distributed firewall capability, in which the distributed policy enforcement takes place on the NIC. The embedded firewall functionality involves secure exchange of cryptographic sessions keys that are then used to communicate firewall policy and new keys between the NIC and the remote policy server. Additionally, the flash firmware present on the NIC performs image authentication for all firmware modules downloaded to the NIC by the host system. And EFW session keys, IPSec SA keys and random seed keys entered into 3Com NIC cross PCI bus from the host, are encrypted. Overall 3CRFW200B meets FIPS 140-2 compliance of security Level 1. The 3Com NIC is considered a multi-chip embedded module for FIPS 140-2 purposes.

1.1. Purpose

This document covers the secure operation of 3CRFW200B, including the initialization and the responsibilities for operating the product in a secure, FIPS-compliant manner.

1.2. Glossary

Term/Acronym	Description
NIC	Network Interface Card
OS	Operating System
PC	Personal Computer
MMC	Microsoft Management Console
SA	Security Association
CO	Crypto Officer

EDC	Error Detection Code
PS	Policy Server
EFW	Embedded Fire Wall
RNG	Random Number Generator
PRNG	Pseudo Random Number Generator

2. Roles, Services, and Authentication

2.1. Roles

The module supports the following two roles:

User Role

The User role is assumed by any entity requesting the services of the card, both cryptographic and non-cryptographic. The User can send and receive both encrypted and unencrypted data using the NIC. The User can also configure the NIC settings using the NIC Doctor diagnostic utility and gather and view NIC statistics. In the User Role, i.e. when a non-administrative user is logged on the OS, the user cannot enable or disable 3CRFW200B. They also cannot alter the IPSec policy or EFW policy setup on the PC. They can only transmit and receive packets as per the IPSec or EFW policy active on the PC. Only one User role is supported.

Crypto-officer Role

The Crypto-Officer (CO) is responsible for installing the NIC and corresponding drivers, diagnostic software and EFW Agent Software on the PC. Typically a user needs administrative privileges for the OS to be able to install a NIC. 3CRFW200B is first installed on the PC system using the conventional installation procedures as pertains to the underlying OS. The Crypto-officer Role (i.e. the Administrator in OS context) has privilege to install/uninstall, enable/disable and configure the NIC. The CO must configure the Windows Operating System for IPSec and ensure that encryption and data-authentication offloads are done on the NIC. They can setup policies (i.e. IPSec offload, TDES, SHA-1) for the PC. Setting up the IPSec policies also requires Administrative privileges on the PC. Such policies are then enforced on any user that uses the PC. Only one Crypto Officer role is supported. The CO must also update and configure the FLASH for EFW operations.

2.2. Services

At any given time 3CRFW200B can execute only one firmware image. The following images provide services to the User and Crypto Officer.

1. Runtime image: This firmware image is the operational image of the module and is responsible for providing the IPSec offload functionality to the host OS and EFW functionality to the remote Policy Server. This image must be loaded on the card memory by the device driver

2. Diagnostic image: In addition to the services provided the runtime image the diagnostic image also provides additional diagnostic capabilities. This image must be loaded on the card memory by the device driver

3. Sleep image: This image is stored in the FLASH memory on the card and is automatically loaded when the module powers-up.

4. Reflash image: This image allows the flash memory to be upgraded to a new digitally signed flash image. The device driver must load this image on the card memory when the FLASH image needs to be updated.

The services provided by the respective images are defined below. Common Services are services that are provided by all images.

Service	Description	Role
COMMON SERVICES		
Transmit enable	Enable packet transmission onto Ethernet interface	User/Crypto-Officer
Transmit disable	Disable packet transmission onto Ethernet interface	User/Crypto-Officer
Receive enable	Enable packet reception from Ethernet interface	User/Crypto-Officer
Receive disable	Disable packet reception from Ethernet interface	User/Crypto-Officer
Read receive filter	Read current receive filters	User/Crypto-Officer
Set receive filter	Set receive filter to given value	User/Crypto-Officer
Read Statistics	Return the Statistics table to host	User/Crypto-Officer
Cycle Statistics	Initiate or disable a periodic transfer of statistics	User/Crypto-Officer
Clear Statistics	Clear Statistics Counter	User/Crypto-Officer
Read Var Section	Read VAR section of flash	Crypto-Officer
Write Var Section	Write VAR section of flash	Crypto-Officer
Read Static Section	Read Static section of flash	Crypto-Officer
Read flash page	Read the specified flash page	Crypto-Officer
Write flash page	Write to the “data only” flash pages	Crypto-Officer
Select Tranceiver	Setup PHY to advertise configuration	User/Crypto-Officer
Test Mux	Test MII pin	Crypto-Officer
Enable PHY loopback	Enables loopback of packets at the PHY interface	User/Crypto-Officer
Disable PHY loopback	Disables loopback of packets at the PHY interface	User/Crypto-Officer
Read Mac Control	Return MAC Control Register Value	User/Crypto-Officer
Write Mac Control	Set MAC Control Register	User/Crypto-Officer

Read Max Packet Size	Read Max Packet Size	User/Crypto-Officer
Write Max Packet Size	Write Max Packet Size	User/Crypto-Officer
Read Media Status	Read Link Status	User/Crypto-Officer
Write Media Status	Set Media Status Register	User/Crypto-Officer
Read Network Diag	Read Network Diag Register	User/Crypto-Officer
Write Network Diag	Set Network Diag Register	User/Crypto-Officer
Read Physical MGMT	Read MII Register	User/Crypto-Officer
Write Physical MGMT	Write MII Register	User/Crypto-Officer
Write Multicast Hash Mask	Enable/disable hash bit in the mcast hash register	User/Crypto-Officer
Add multicast address	Adds a new multicast address to receive packets	User/Crypto-Officer
Set MAC address	Sets the station MAC address to that specified	User/Crypto-Officer
Read MAC address	Reads the current MAC address	User/Crypto-Officer
Read VLAN type	Reads the current VLAN type	User/Crypto-Officer
Write VLAN type	Sets the VLAN type to that specified	User/Crypto-Officer
Write Broadcast Throttle	Set Broadcast Limit	User/Crypto-Officer
Read Broadcast Throttle	Read Broadcast Limit	User/Crypto-Officer
Issue software reset	Performs software reinitialization	User/Crypto-Officer
Issue software halt	Stops the current firmware image from executing	User/Crypto-Officer
Read version information	Reads the current image's version information	User/Crypto-Officer
Set interrupt coalescing	Enables/Disables interrupt coalescing	User/Crypto-Officer
Read PCI config register	Reads the specified PCI Configuration register	User/Crypto-Officer
Write PCI config register	Sets the specified PCI Configuration register	User/Crypto-Officer
Read/Write Offload Capability	Read or write Offload Capability option	User/Crypto-Officer
Read SOS	Read SOS pin status	User/Crypto-Officer
Get link status	Returns the link status (connected/disconnected)	User/Crypto-Officer

Read IPSEC Info	Read IPSec Statistics	User/Crypto-Officer
Get IPSEC Enable	Return current Ipsec enable state of the card	User/Crypto-Officer
Test Get/Set Power	Get or Set current power mode	User/Crypto-Officer

SLEEP SERVICE		
Goto Sleep	Set adapter to sleep power state	Crypto-officer
Add wakeup packet	Allows host to add wakeup patterns to 3CRFW200B	Crypto-officer
Enable sleep events	Allows host to perform events like Respond to Ping	Crypto-officer
Enable wakeup events	Allows host set wakeup events like Wake-On-Ping	Crypto-officer
Firmware Image Download	Allows download of firmware images to 3CRFW200B	User/Crypto-Officer

RUNTIME SERVICE		
Add Security Association	Adds a new security association provided by host	User/Crypto-officer
Delete Security Association	Deletes an offloaded security association	User/Crypto-officer
Transmit IPSec packets	Encrypts and transmits IPSec packets	User/Crypto-officer
Receive IPSec packets	Decrypts and receives IPSec packets	User/Crypto-officer
Transmit EFW packets	Encrypts, authenticates and transmits EFW packets to Policy Server. Also enforces EFW filtering rules to allow or deny the packet transmission.	User/Crypto-officer
Receive EFW packets	Decrypts, authenticates and receives EFW packets from Policy Server. Also enforces EFW filtering rules to allow or deny the received packets	User/Crypto-officer

DIAGNOSTIC SERVICE		
Test ARM2HOST registers	Tests the ARM to HOST registers	Crypto-officer
Test HOST2ARM registers	Tests the HOST to ARM registers	Crypto-officer
Test PCI DMA	Tests the PCI DMA interface	Crypto-officer

Test PCI interrupt	Tests the PCI interrupts	Crypto-officer
Test receive interrupt	Tests receive MAC interrupts	Crypto-officer
Test transmit interrupt	Tests transmit completion interrupts	Crypto-officer
Test oneshot timer	Tests the one shot timer on 3CRFW200B	Crypto-officer
Test Crypto Algorithm	Tests PRNG, T-DES, HMAC SHA1 algorithm	Crypto-officer
Transmit Waveform	Transmit Waveform setup by TestMux	Crypto-Officer
Test Rings	Diagnostic Ring Buffer problem	Crypto-Officer

REFLASH SERVICE		
Flash Image Update	Allows flash image to be updated	Crypto-officer
Zeroize EFW Keys	Sets the TDES & HMAC SHA-1 EFW session keys, Policy Server Public key, and Random Seed key to zeros	Crypto-officer
Zeroize HMAC SHA-1 and Encryption Secret Keys	Sets the HMAC SHA-1 and Encryption Secret keys to zeros	Crypto-officer

2.3. Authentication Mechanisms and Strength

The module does not provide authentication for any role. A role can be assumed implicitly by requesting services which have been assigned to that role.

Firmware Authentication

The module does authenticate firmware uploads by using an Approved authentication technique in the form of HMAC-SHA1. 3CRFW200B requires the host to download a digitally signed firmware image from 3Com. The NIC authenticates the firmware module by re-computing and comparing the HMAC SHA-1 digest, using 3Com's HMAC-SHA1 Secret Key stored in FLASH. If the firmware module fails authentication, 3CRFW200B enters a failure mode and becomes non-functional. Crypto offloads and packet transmission or reception are blocked. To recover such 3CRFW200B NIC the PC has to be reset. Any new firmware that is uploaded on the card must be FIPS 140-2 validated.

3. Secure Operation and Security Rules

In order to operate 3CRFW200B and to utilize the IPSec offload function the Crypto Officer must know how to configure Microsoft Management Console (MMC) for Windows Operating System. Once the policies are setup to offload IPSec session, the OS will automatically initiate and setup IPSec session with a remote client and then offload the crypto functions for that session to the NIC.

In order for 3CRFW200B to communicate with a remote Policy Server, the NIC must be setup to operate in EFW mode. And the NIC must communicate with the Policy Server securely.

3.1. Security Rules

The security rules enforced by 3CRFW200B include both the security rules that 3Com Corporation has imposed and the security rules that result from the security requirements of FIPS 140-2.

3Com Security Rules

The following are 3Com security rules:

1. 3CRFW200B shall store the HMAC SHA-1 Secret Key.
2. 3CRFW200B shall store the TDES encryption secret key.
3. 3CRFW200B shall never output the TDES encryption secret key.
4. 3CRFW200B shall never output the HMAC SHA-1 Secret Key or the IPSec Session Key.
5. 3CRFW200B will not store any IPSec session keys in its non-volatile memory.
6. 3CRFW200B shall encrypt EFW data sent to Policy Server using TDES.
7. 3CRWW200B shall authenticate EFW messages sent to Policy Server using HMAC SHA-1.
8. All EFW packets received from Policy Server shall be encrypted using TDES and authenticated suing HMAC SHA-1.

FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2. The module enforces these requirements when initialized into FIPS Level 1.

1. When initialized to operate in Level 1 mode, 3CRFW200B shall only use FIPS-approved cryptographic algorithms.
2. 3CRFW200B shall provide the Crypto Officer the capability to zeroize the HMAC SHA-1 secret and encryption secret keys stored in the flash. It will also zeroize the IPSec session key when the OS deletes the Security Association (SA).
3. 3CRFW200B will only allow to load and run digitally signed firmware module from 3Com Corporation.

4. 3CRFW200B will also perform firmware integrity self-test, know answer tests of all crypto components and PRNG Know Answer Test during power-up. On any failure the unit will become non-functional.

5. 3CRFW200B will validate the on-board firmware using 16bit EDC checksum.
6. Flash firmware on 3CRFW200B shall be upgraded only with a digitally signed flash image from 3Com.
7. The Crypto-Officer shall not configure IPSec policies that use MD5, HMAC-MD5, DES for IPSec.
8. The module must be run on a Windows 2000 OS and the associated device driver provided by 3Com.

9. The module is always in an alternating bypass mode providing cryptographic and bypass services depending on the packet IP header.
10. The Pseudo Random Number Generator (PRNG) in the firmware shall confirm to ANSI X9.31 using 3-Key TDES; a FIPS 140-2 approved algorithm.
11. The Random Seed Key shall be encrypted when entering the NIC across PCI bus during network installation process.
12. The EFW session and authentication keys shall be encrypted when entering the NIC across PCI bus during diskette installation process.
13. The IPSec SA key shall be encrypted across PCI bus when written to NIC memory.
14. The EFW session and authentication keys shall be zeroed out when re-keyed, session shutdown, system reboot, or re-initialized.

3.2. Secure Operation Initialization Rules

3CRFW200B provides many different cryptographic algorithms to ensure compatibility with today's marketplace. Specifically, the 3CRFW200B provides the following algorithms:

Algorithm Type	Key Sizes/ Modes	FIPS-approved
Symmetric Algorithms		
TDES (Cert. #212)	168-bit, CBC & ECB	Yes
DES (Cert. #234)	56-bit, CBC & ECB	No
Hashing Algorithms		
SHA-1 (Certs. #188 and #189)	Byte-oriented	Yes
MD5		No
Authentication Algorithms		
HMAC-SHA1 (Certs. #120 and #130)		Yes
HMAC-MD5		No
Random number generation algorithms		
ANSI X9.31 RNG (Cert. #139)	3Key TDES	Yes

Key transport algorithm		
RSA (PKCS#1)	Provides 80-bits of security	No[1]

Because FIPS 140-2 prohibits the use of non-FIPS approved algorithms while operating in a FIPS compliant manner, the Crypto Officer should follow the following rules to initialize a new 3CRFW200B to invoke the Approved mode of operation.

1. Power-up the PC with 3CRFW200B.
2. After the OS loads, install the device driver for 3CRFW200B using the installation CD.
3. After the NIC is installed, setup the system IPSec policy using MMC. Refer to Microsoft System Administrator's Guide for more details on MMC. The Crypto Officer must create such IPSec policies on the Windows Operating System that only use FIPS Approved algorithms (SHA-1 for AH and TDES, SHA1 for ESP). DES, MD5 and HMAC-MD5 should not be used in an Approved mode. Furthermore, the IP Security rules and IP Filter actions must be configured to only allow IPSec traffic to flow on all network connections. The configuration must disallow communication with computers that do not support IPSec.
4. Once the IPSec policies are defined, all sessions initiated or received by the PC will be encrypted.
5. The OS will then offload the IPSec session and its SA's to 3CRFW200B.
6. Once IPSec sessions are offloaded to 3CRFW200B, it will encrypt/decrypt any IPSec traffic that matches the SA.

3.3. EFW Operation Initialization Rules and Cryptographic Activities

To ensure the integrity of the EFW system, cryptography is used not only during normal EFW operation but also during the installation of the system components. An EFW system is assembled using the following sequence of events:

- *The NIC hardware is deployed.* NICs to host an embedded firewall must be deployed and operate properly on the network using the standard 3Com drivers provided with 3CRFW200B.

- *Policy Servers and Consoles are installed.* One or more policy servers and management consoles are installed and configured.

- *Installation package construction.* Using the management console, the administrator creates installation packages that are distributed to hosts intended to become part of the domain. Two mechanisms for creating and distributing these packages are afforded by the EFW: diskette keyed and network based.

[1] RSA is allowed for key transport in FIPS mode

1. Diskette based Installation- the administrator creates a keying diskette for an individual NIC to be added to the EFW system. This diskette is a DOS bootable floppy that contains the policy server public RSA key and an initial shared private TDES session key for the NIC. The diskette itself is encrypted with an administrator-chosen password. The host for the NIC for which this keying diskette was created, is then booted from the floppy disk to accomplish the portion of the embedded firewall installation that modifies NIC non-volatile memory. The EFW session keys, the policy server public key and the hashes are subsequently stored in the NIC's non-volatile memory using programs running under DOS. At this point the NIC and the Policy Server share a DES/TDES encryption key and an authentication key.

2. Network Installation- The administrator constructs a custom InstallShield installation package and writes it to a Windows folder. This package is custom to the domain because it contains the policy server public key. When this package is executed on any target host, all three aspects of embedded firewall installation take place in one step. This includes writing the policy server public key and the hashes as well as the random seed key to the NIC's non-volatile memory. The random seed key is encrypted using a secret TDES key stored in NIC's FLASH before written to the non-volatile memory cross PCI bus. The first time the NIC boots up after this installation, it creates an initial TDES encryption key and an authentication key when it sees there are no EFW session keys present in its non-volatile memory. Random seed key is used in a FIPS compliant pseudo random number generator to generate this key. Upon receiving the wakeup from the NIC, the policy server can use its RSA private key to decrypt the initial EFW session keys and then use them to authenticate and decrypt the wakeup packet. If the packet authenticates and decrypts properly, the keys contained in the packet are saved in the database as the NIC's keys. The NIC and the server now have a shared encryption and authentication key.

The Policy Server immediately changes the encryption key on the NIC after the NIC is initially established, and at every wake-up of the NIC after that point during the life of the system. "Rekey" is a command to the NIC from the policy server, and is accomplished by encrypting the new key with the old key.

4. Definition of SRDIs Modes of Access

This section specifies 3CRFW200B's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by it.

4.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a level 1 FIPS-compliant manner, the 3CRFW200B NIC contains the following security relevant data items:

Security Relevant Data Item	SRDI Description
HMAC SHA-1 Secret Key	A 512-bit HMAC SHA-1 secret key embedded within the 3CRFW200B's Flash memory. This key is used to verify the signature attached to a downloaded firmware image.
IPSec Session Keys	The OS offloads the IPSec session keys (TDES keys for encryption and HMAC-SHA1 keys for data authentication) to 3CRFW200B and they are stored in the volatile RAM memory on 3CRFW200B. These keys are zeroized when the OS deletes the SA or when 3CRFW200B is powered off.
Encryption Secret Key	A 168-bit TDES key embedded within the 3CRFW200B's Flash memory. This key is used to encrypt the IPSec session key, Random Seed key and EFW session keys transferred from the Host to NIC across PCI bus.
Policy Server Public Key	A 1024-bit RSA public key. The public key is used for initial session key exchange for NIC/PS communication under network installation method. A network installed NIC generates and sends an initial key to policy server encrypted with this policy server public key. There is one RSA key pair for an EFW domain.
EFW Session Keys	A 168-bit TDES key and a 160-bits HMAC SHA1 key. The keys are used for communications between Policy Server and NIC. Under the diskette-keyed installation method, the keying diskettes contain initial EFW session keys for individual EFW NICs. Under the network installation method, the keys are generated by firmware in the NIC. These keys are often rekeyed.
Random Seed Key	Random seed key is used as a seed to a PRNG in the firmware that is used to create EFW session keys.

4.2. Access Control Policy

3CRFW200B allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the NIC in a given role. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read (R), write (W) and use (U). If no permission is listed, then an operator has no access to the SRDI. Only those services that provide any access to the SRDIs are listed below. All other services from the Services table in Section 3 above do not provide any access to the SRDIs of the module.

3CRFW200B SRDI/Role/Service Access Policy	Security Relevant Data Item	HMAC SHA-1 Secret Key	IPSec Session Keys	Encryption Secret Key	Policy Server Public Key	EFW Session Keys	Random Seed Key
Role/Service							
User role							
Transmit IPSec packets (encrypt)			U				
Receive IPSec packets (decrypt)			U				
Add Security Association			W				
Delete Security Association			W				
Firmware Image Download		R/U					
Transmit EFW packets					U	U	
Receive EFW packets						U/W	
Crypto-Officer Role							
Transmit IPSec packets (encrypt)			U				
Receive IPSec packets (decrypt)			U				
Add Security Association			W				
Delete Security Association			W				
Firmware Image Download		R/U					
Flash Image Update		R/U		R/U	W	W	W
Zeroize HMAC SHA-1 & Encryption Secret Keys		W		W			
Transmit EFW packets					U	U	
Receive EFW packets					U	U/W	
Zeroize EFW Keys					W	W	W

5. Self-tests

The module provides the following power-up and conditional self-tests

5.1. Power-Up Tests

These are performed when the module boots up.

- TDES CBC Known Answer Test for the hardware implementation
- HMAC-SHA-1 Known Answer Test for the hardware implementation
- SHA-1 Known Answer Test for the hardware implementation
- HMAC-SHA-1 Known Answer Test for the firmware implementation
- A 16-bit Firmware Integrity Check on all firmware
- HMAC-SHA-1 Known Answer Test for the firmware implementation in the flash upgrade utility.
- PRNG Know Answer Test.

5.2. Conditional Tests

The following load test is performed when a firmware image download is requested.

- Firmware Load test: The module performs an HMAC-SHA-1 keyed hash verification of each image that is downloaded on the card. The module enters an error state in case of self-test failures and does not provide any functionality. It must be reset to recover from the error state.
- Bypass self-test: The module performs a bypass self-test on each packet which is sent out in plaintext. If the test fails, the packet is dropped.
- PRNG Continuous RNG Test.

6. Mitigation of Other Attacks

This section is not applicable as the module does not provide mitigation against any commonly known attacks.