Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Connectra

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Level 1
Firmware

Firmware version NGX R66.1 with hotfix 1

Version 1.08
December 14, 2010

Table of Contents

INTRODUCTION 3

PURPOSE 3
REFERENCES 3

CHECK POINT CONNECTRA 4

OVERVIEW 4
CRYPTOGRAPHIC MODULE 6
MODULE INTERFACES 7
ROLES AND SERVICES 8
Local Crypto Officer Role 11
User Role 13
Authentication Mechanisms 14
Unauthenticated Services 15
PHYSICAL SECURITY 15
OPERATIONAL ENVIRONMENT 15
CRYPTOGRAPHIC KEY MANAGEMENT 15
SELF-TESTS 19
DESIGN ASSURANCE 21
MITIGATION OF OTHER ATTACKS 21

SECURE DELIVERY AND OPERATION 21

SECURE DELIVERY 22
FIPS MODE CONFIGURATION 22
Local Crypto-Officer Configuration Steps 22
Management Station Configuration Steps 25
Remote Crypto-Officer Configuration Guidelines 26
CRYPTO-OFFICER GUIDANCE 34
Management 35
Termination 35
USER GUIDANCE 35

ACRONYMS 36

Introduction

Purpose

This non-proprietary cryptographic module Security Policy describes the Check Point Software Technologies Ltd. (Check Point) Connectra cryptographic module, version *NGX R66.1* with hot fix HFA 1. This security policy describes how the Check Point Connectra module meets the security requirements of FIPS 140-2 and how to configure and operate the module in the FIPS 140-2 Approved mode. This policy was prepared to support the Level 1 FIPS 140-2 validation testing of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM.

Check Point Connectra version NGX R66.1 with HFA 1 is alternatively referenced in this document as *Check Point Connectra*, *Connectra*, *the module*, and *the software*.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module. More information is available on the module from the following sources:

- The Check Point website (http://www.checkpoint.com/) contains information on the full line of products from Check Point.

- The NIST Validated Modules website http://csrc.nist.gov/groups/STM) provides contact information for answers to technical or sales-related questions regarding the module.

CHECK POINT CONNECTRA

Overview

Check Point's Connectra is a tightly integrated firmware solution combining sophisticated IPsec and SSLv3 Virtual Private Network (VPN) technologies with a hardened Operating System (OS). Connectra allows mobile and remote workers to connect easily and securely to critical resources while protecting enterprise networks and endpoints from external threats. A broad range of connectivity scenarios coupled with integrated intrusion prevention and unified with powerful central management offer unprecedented control over remote access configurations and security policy administration. As a first line of defense, Connectra offers comprehensive endpoint security to protect networks and endpoints from debilitating viruses, malware and malicious attacks.

Connectra is integrated with Check Point's SecurePlatform, a customized and hardened Operating System, with no unnecessary components that could pose security risks. SecurePlatform is pre-configured and optimized to perform its task as a network security device. An embedded apache server daemon (httpd) supports centralized administration over TLS using a SmartCenter administration server.

Connectra is designed to allow secure access to an organization's resources to multiple users over an unsecured TCP/IP network. Execuring in a DMZ behind a firewall, the Connectra system performs all the required security functions and provides the following high-level functionality:

- Secure, authenticated and encrypted sessions with Clients and subsystems.
- Secure IPsec and TLS VPN between subsystems.
- Central security administration.

Figure 1 shows a configuration where Connectra™ is deployed on a LAN. Figure 2 shows a configuration where Connectra™ is deployed in a DMZ.

When deployed in a LAN, the remote user opens a browser and initiates an HTTPS request to the Connectra™ gateway. Sessions initiated using HTTP will be redirected automatically to HTTPS. The SSL connection is terminated within the LAN, and the clear text requests forwarded to the internal servers. The internal servers reply "in the clear" to Connectra™, which encrypts the back connection to the remote user. In the scenario shown in Figure 2, the perimeter firewall must be configured to allow encrypted SSL traffic to Connectra™.

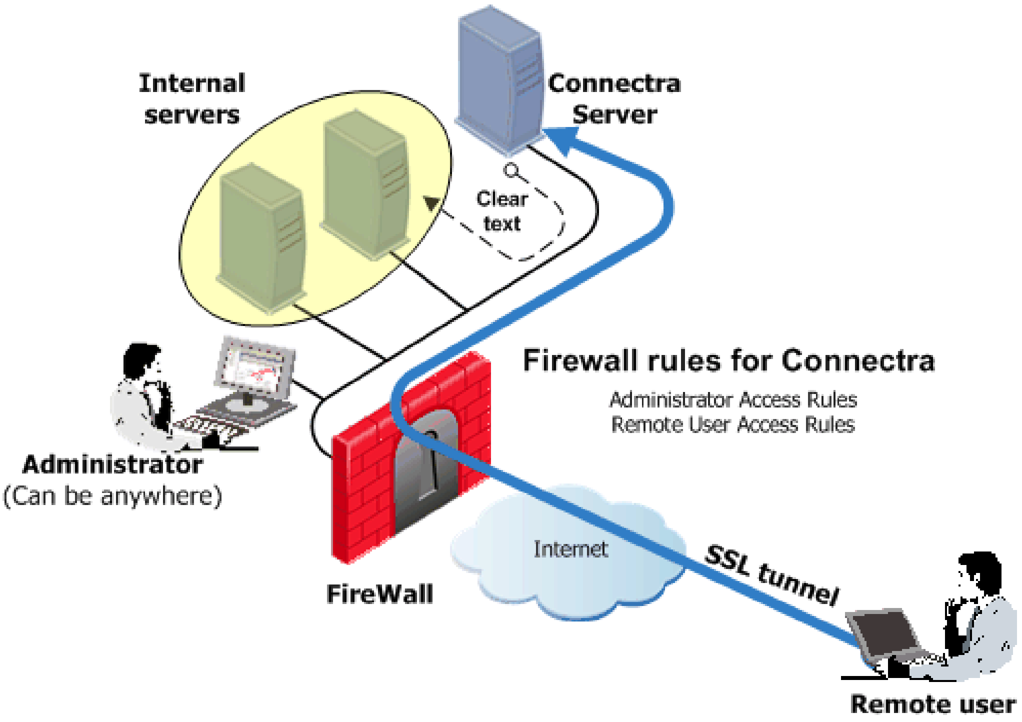


Figure 1. Connectra™ Deployed on a LAN

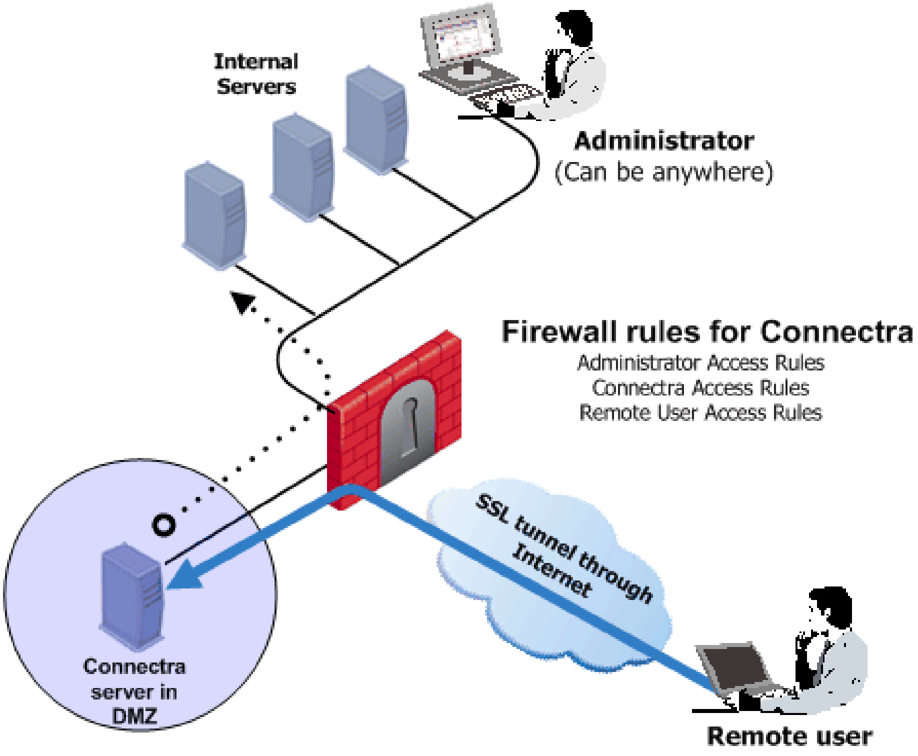


Figure 2. Connectra™ Deployed in a DMZ.

When Connectra is placed in the DMZ, traffic initiated both from the Internet and from the LAN to Connectra is subject to firewall restrictions. By deploying Connectra in the DMZ, the need to enable direct access from the Internet to the LAN is avoided. Remote users initiate an SSL connection to the Connectra Gateway. The firewall must be configured to allow traffic from the user to the Connectra server, where SSL termination, Web and Application Intelligence inspection, authentication, and authorization take place. Requests are then forwarded to the internal servers via the firewall. Administration traffic is always SSL encrypted.

Cryptographic Module

The Check Point Connectra cryptographic module is a FIPS 140-2 firmware module. The physical embodiment is multi-chip standalone. Connectra is intended to run on any general purpose PC-class computing platform. Check Point supplies a proprietary, hardened operating system (SecurePlatform) that along with the General Purpose Computer (GPC) containing the required processor(s) provides the cryptographic module's operational environment. The operational environment is not modifiable, as it does not allow the module operator to load code or applications that are not part of the FIPS 140-2 validation. Physical security mechanisms are provided by the industry standard computer components and passivation coatings.

Logically, the cryptographic module boundary is composed of the Check Point Connectra firmware running on the Secure Platform Operating System. Physically, the cryptographic boundary of the module is the GPC case, which physically encloses the module. Table 2 describes the physical ports, logical interfaces, and FIPS logical interfaces

FIPS 140-2 validation testing was performed using the operational environment configuration shown in Chart 1.

Operational Environment	Module firmware and Check Point SecurePlatform™ Operating System Version NGX R66.1 with hot fix HFA 1
	Test Platform **Connectra-1 3070 –** General Purpose Computer (GPC) with Intel® Core™2 Duo processor.

Chart 1 – Module Operational Environments Tested

FIPS 140-2 validation is maintained so long as the same module is installed onto any GPC with a compatible 32 bit x86 code-compatible CPU, e.g. Intel Celeron®, AMD Opteron®, etc. The CMVP allows vendor porting of a validated firmware cryptographic module from the GPC specified on the validation certificate to a GPC which was not included as part of the validation status, as long as no source code modifications are required. The validation status is maintained on the new GPC without re-testing the cryptographic module on the new GPC.

The module meets the FIPS 140-2 requirements for an overall Level 1 validation. The following table summarizes the individual FIPS 140-2 requirements sections as outlined in the FIPS 140-2 Derived Test Requirements (DTR) document, as well as the level implemented by the module for each section.

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Table 1 –Security Level Implemented Per FIPS 140-2 Test Section

Although the module consists entirely of software, the FIPS 140-2 evaluated platforms are standard Personal Computer enclosures, which each meet the applicable FCC EMI and EMC requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

In addition to the IKE/IPSec-based VPN the evaluated module allows users to establish TLS-based VPN tunnels (via the SSL Network Extender and SecureClient Mobile features). The same CSPs and cryptographic module implementation is used for both VPN protocol sets.

Module Interfaces

As a multi-chip standalone module implemented on a General Purpose Computer (GPC), the physical ports of the module include the computer’s network ports, keyboard/mouse ports, USB ports, and serial ports. All of these physical ports are separated into logical interfaces by the module software, and these software logical interfaces are then mapped into FIPS 140-2 logical interfaces, as described in the following table.

FIPS 140-2 Logical Interface	Logical Interface	Standard PC Physical Port
Data input interface	User Interface (UI) for the Secure Platform, Network Layer IP interface	Network ports
Data output interface	User Interface (UI) for the Connectra, Network Layer IP interface	Network ports
Control input interface	User Interface (UI) for the Connectra, Network Layer IP interface	Connectra 3070 Platform: Console port, keypad, network ports General Purpose Platform: network ports, keyboard, mouse
Status output interface	User Interface (UI) for the Connectra, Network Layer IP interface, Log files	Connectra 3070 Platform: Network ports, Console port, LCD Display, General Purpose Platform: Monitor, network ports
Power interface	Power interface	Power connector

Table 2 – Mapping Standard PC Physical Ports and Logical Interfaces to FIPS 140-2 Interfaces

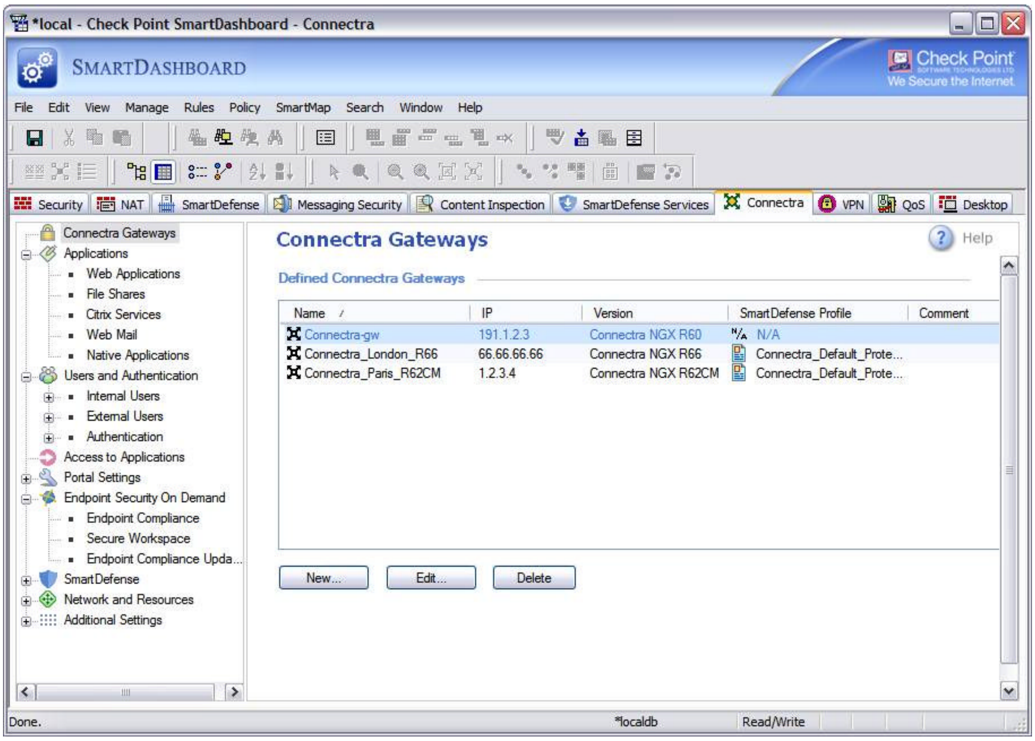
The logical interfaces are separated by the UIs that distinguish between data input, data output, control input and status output through the dialogues. Similarly, the module distinguishes between different forms of data, control and status traffic over the Network ports by analyzing the packets header information and contents. Log files are only utilized for status output.

Roles and Services

The module supports three distinct roles: Client User, Local Crypto-Officer, and remote Crypto-Officer roles. It uses digital signatures, pre-shared keys, and passwords for authentication.

The Local Crypto-Officer role is responsible for the installation, minimal configuration, and removal of the Connectra. These operations are performed locally using physical access to the PC the module is installed on.

The Remote Crypto-Officer role performs primary configuration of Connectra. After authenticating, the Remote Crypto-Officer uses a powerful set of management tools to configure and monitor the module. The remote management session uses TLS to ensure security.



Connectra Gateways

Defined Connectra Gateways

Name	IP	Version	SmartDefense Profile	Comment
Connectra-gw	191.1.2.3	Connectra NGX R60	N/A	
Connectra_London_R66	66.66.66.66	Connectra NGX R66	Connectra_Default_Prote...	
Connectra_Paris_R62CM	1.2.3.4	Connectra NGX R62CM	Connectra_Default_Prote...	

Figure 3– Easy to Use Management Tools

The User role is for clients that are accessing the module from remote locations. These operators can authenticate through IKE using either pre-shared keys or digital certificates. Once authenticated, an encrypted tunnel is established between the Check Point Connectra and the client using IPSec.

Remote Crypto Officer Role

The role of the Remote Crypto-Officer includes refinement of administrative permissions, generation and destruction of keys, user access control and creation of the information database. Each management server (i.e., Remote Crypto-Officer) authenticates to the module through TLS using digital certificates. After authenticating, the Remote Crypto-Officers use Check Point management software to manage the module over the secure TLS session.

Descriptions of the services available to the Crypto Officer role are provided in the table below.

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
TLS	Access the module's TLS to create a secure session for remotely managing the module.	TLS handshake parameters, TLS inputs, data	TLS outputs and data	RSA key pair for management (read access); Session keys for management (read/write access); X9.31 PRNG keys (read access)
Create and Configure Users/User Groups	Define users and user groups allows the Crypto-Officer to create permission for individual users or a whole group of users; set permissions such as access hours, user priority, authentication mechanisms, protocols allowed, filters applied, and types of encryption	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	None
Management of keys	Configure the digital certificates and/or pre-shared keys for use by IPSec and IKE or by TLS for VPN authentication	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	RSA key pair for IKE / TLS (read/write access); pre-shared keys for IKE (read/write access)
Initialization of Secure Internal Communication (SIC)	Establish trust between management server and the Connectra module to allow configuration of the module's services	Commands and configuration data (SIC policy)	Status of commands	RSA key pair for management (read/write access)
Monitoring	Provides detailed information for both monitoring of connection activities and the system status	Commands	Status of commands and status information (logs)	None

Table 3 – Crypto Officer Services, Descriptions, Inputs and Outputs

Local Crypto Officer Role

Local operators authenticate to the module using a user name and password. Once authenticated, the operator implicitly assumes the role of Local Crypto-Officer and can access the various utilities and configurations available to that role.

Table 4 contains a list of all of the services available to the Local Crypto-Officer, a description of those services along with the relevant CLI commands, the inputs to the services, and the outputs of the services.

Service	Description with CLI commands	Input	Output	CSP
FIPS mode	Switch to FIPS mode and enable integrity check.	Command and any options	Status of commands	None
Manage CLI settings	Switch between standard and expert CLI modes (expert); Logout of the CLI (exit); Change the logged in Local Crypto-Officer's password (passwd)	Commands, any options, and password (for switching between CLI modes)	Status of commands	Local Crypto-Officer password (read/write access)
View local help documentation	List available commands and their respective descriptions (help or ?)	Commands	Status of commands and status information (help information)	None
Get and set date and time	View/change date (date); view/change time (time); view time zone (timezone)	Commands, any options, and date or time settings	Status of commands and status information (date, time, or time zone information)	None
System management commands	Display or clear audit logs (audit); backup the system configuration (backup); restore the system configuration (restore); reboot the module (reboot); shutdown the module (shutdown); apply an upgrade or hotfix (patch) – not available in FIPS mode	Commands, any options, and configuration parameters	Status of commands and status information (logs)	None
System diagnostic commands	Change logging options (log); Display top 15 processes ranked by CPU usage (top); display or send diagnostic information (diag)	Commands and any options	Status of commands and status information (process list or diagnostic information)	None

Service	Description with CLI commands	Input	Output	CSP
Check Point module commands	Install licenses, configure the SNMP daemon, modify the list of Unix groups authorized to register a cryptographic token and configure the one time SIC password (all functionality is provided through text-based menuing system after executing cpconfig) Start the Check Point applications (cpstart); stop the Check Point applications (cpstop); show Check Point diagnostic information (cpinfo); display the status of Check Point applications (cpstat); manage Check Point licenses (cplic); show the SVN Foundation version (cpshared_ver); enable the high availability feature (cphastart); disable the high availability feature (cphastop); define a critical process (cphaprob)	Command (cpconfig), menu options, and configuration information Command, any options, and configuration information	Status of commands/menu options and status information (configuration information) Status of commands and status information (diagnostic information, version numbers, and license information)	None
Network diagnostic commands	Ping network hosts (ping); trace the route of packets to a host (traceroute); show network statistics (netstat)	Commands and any options	Status of commands and status information (diagnostic information)	None
Network configuration commands	Show and modify the kernel's ARP cache (arp); show, set, or remove hostname to IP mappings (hosts); show, configure, and store network interface settings (ifconfig); configure virtual LAN interfaces (vconfig); show and configure routing entries (route); get or modify the system's host name (hostname); get or set the system's domain name (domainname); show, add, or remove domain name servers (dns); interactive script for configuring the network and security settings of the system (sysconfig)	Commands, any options, and configuration information	Status of commands and status information (configuration information)	None

Service	Description with CLI commands	Input	Output	CSP
Key/CSP zeroization	The Local Crypto-Officer can zeroize all of the module's CSPs by reformatting the hard drive the module is installed on. The module must be under control of the operator during reformatting.	None	None	All CSPs stored on the module's hard drive

Table 4 – Local Crypto-Officer Services, Descriptions, Inputs and Outputs

User Role

The User role access the module's IPSec and IKE services and the TLS VPN services and authenticates to the module using digital certificates or pre-shared keys (available for IKE).

Service descriptions and inputs/outputs are listed in the following table:

Service	Description	Input	Output	CSP
IKE	Access the module's IKE functionality in order to authenticate to the module and negotiate IKE and IPSec session keys	IKE inputs and data	IKE outputs, status, and data	RSA key pair for IKE (read access); Diffie-Hellman key pair for IKE (read/write access); pre-shared keys for IKE (read access)
IPSec	Access the module's IPSec services in order to secure network traffic	IPSec inputs, commands, and data	IPSec outputs, status, and data	Session keys for IPSec (read/write access)
TLS	Access the module's TLS functionality in order to authenticate to the module and negotiate TLS session keys in order to secure network traffic	TLS inputs and data	TLS outputs, status, and data	RSA key pair for TLS (read access); session keys for TLS (read/write access)

Table 5 – User Services, Descriptions, Inputs and Outputs

Authentication Mechanisms

The module implements password-based authentication, RSA-based authentication, and HMAC-based authentication mechanisms.

Authentication Type	Strength
RSA-based authentication (TLS handshake)	RSA encryption/decryption is used to authenticate to the module during the TLS handshake. This mechanism is as strong as the RSA algorithm using a key pair of either 2048 or 4096 bits. Using a 2048 bit key pair is generally considered equivalent to brute forcing a 112 bit key (i.e., a 1 in 2^112 chance of false positive).
RSA-based authentication (IKE)	RSA signing/verifying is used to authenticate to the module during IKE. This mechanism is as strong as the RSA algorithm using a key pair of either, 2048 and 4096 bits. Using a 2048 bit key pair is generally considered equivalent to brute forcing a 112 bit key (i.e., a 1 in 2^112 chance of false positive).
Password-based authentication	Passwords are required to be at least 6 characters in length, a mixture of alphabetic and numeric characters, at least four different characters, and not to use simple dictionary words or common strings such as “qwerty.” Considering only the case sensitive English alphabet and the numerals 0-9 using a 6 digit password with repetition, the number of potential passwords is 62^6.

Table 6 – Estimated Strength of Authentication Mechanisms

Each of the authentication mechanisms shown in Table 6 demonstrates that a single, random authentication attempt has less than a 1:1,000,000 chance at success (i.e., a false positive).

Repeated attempts to defeat the authentication mechanisms over a 1-minute period such that there would be a chance for a false positive would require the following attempt rates:

- IKE / HMAC: ((94^6) / (100,000 *60)) = 114,000 attempts per second
- RSA-based: ((2^112) / (100,000 *60)) = 8.6538281×10^26 attempts per second

The cryptographic module cannot process repeated authentication attempts at these frequencies. Additionally, when operating in Approved Mode, the module only allows a maximum of three unsuccessful password-based attempts before imposing a 60 minute lockout period. The module successfully meets the FIPS 140-2 requirements for strength of authentication for all of its authentication mechanisms.

Unauthenticated Services

The cryptographic module does not provide any unauthenticated services. All module services are available only to authenticated operators assuming either a Crypto Officer or a User role.

Physical Security

The module meets the physical security requirements for a FIPS 140-2 level 1 firmware module.

Operational Environment

The FIPS 140-2 Operational Environment requirements do not apply to this module. The module does not provide a general-purpose operating system nor does it provide a mechanism to load new software.

The cryptographic module is firmware and was tested under the Check Point SecurePlatform™ operating system on the processor types provided by General Purpose Computing platforms in the configurations shown in Chart 1 on Page 5. These processor types are also reflected in the module's cryptographic algorithm validation certificates.

Cryptographic Key Management

Check Point adheres to FIPS-Approved cryptographic standards and provides the strongest cryptography available. Check Point Connectra's efficient implementation of standard cryptographic algorithms ensures the highest level of interoperability. In addition, the module's implementations provide some of the fastest system performance available in software.

Connectra provides the capability to use TLSv1 to secure management sessions and remote access TLS-based VPN. The module supports IPSEC/ESP for data encryption and IPSEC/ESP for data integrity. It implements all IKE modes: main, aggressive, and quick, using ISAKMP as per the standard.

The Check Point Connectra cryptographic module implements the following FIPS-Approved algorithms (NIST-assigned algorithm validation certificate numbers shown in boxed items):

<u>Data Encryption:</u>

- Advanced Encryption Standard (AES) in CBC mode (128 or 256 bit keys) – as per NIST FIPS PUB 197

Connectra R66
Certificates #1369, #1458

- Triple DES (3DES) in CBC modes (168 bit keys) – as per NIST PUB FIPS 46-3 (withdrawn) and NIST Special Publication 800-67

Connectra R66
Certificates #944, #984

Data Packet Integrity:

- HMAC-SHA-1 (20 byte) – as per NIST PUB FIPS 198, RFC 2104 (HMAC: Keyed-Hashing for Message Authentication), and RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH).

Connectra R66
Certificates #802, #855

Data Hashing:

- Secure Hash Standard (SHS/SHA-1) – as per NIST PUB FIPS 180-2

Connectra R66
Certificates #1251, #1319

PRNG:

- ANSI X9.31 Implementation

Connectra R66
Certificate #756

Digital Signatures:

- RSA – PKCS#1 and X9.31

Connectra R66
Certificates #670, #713

The RSA implementation is used both for signature generation and verification (per PKCS#1), and also for key generation (per ANSI X9.31) when supporting Distributed Key Management (DKM).

The module implements the following protocols permitted for use in a FIPS-Approved mode of operation (per FIPS 140-2 Implementation Guidance 7.1):

Session Security:

- TLS v1.0 – as per RFC 2246
- IPSec
- Secure Socket Layer (SSL) v3.1 – as per the Transport Layer Security Working Group draft

Key Agreement / Key Establishment:

Encryption strength is determined by using the equation provided in FIPS 140-2 Implementation Guidance 7.5 and NIST Special Publication 800-57, Part 1. Encryption strength is a function of the key size implemented.

- The Diffie-Hellman key agreement methodology implemented by the module (used by IKE) provides between 112 and 202 bits of encryption strength.
- The RSA key wrapping methodology (used by TLS), provides between 112 bits and 150 bits of encryption strength.

The following is a list of the Critical Security Parameters (CSPs) implemented by the module:

Key	Key type	Generation	Storage	Use
Local Crypto-Officer passwords	-	-	Stored on disk (/etc/password) - plaintext	Local Crypto-Officer authentication
RSA key pair for management	RSA key pair (2048 or 4096 bits)	Outside of crypto-boundary)	Stored on disk in P12 format ($CPDIR/conf/sic_cert.p12) (considered plaintext)	Authentication during TLS handshake
RSA key pair for IKE and TLS based VPNs	RSA key pair (2048 or 4096 bits)	Outside of Crypto boundary	Stored on disk ($FWDIR$/database/fwauth.NDBX) – plaintext	Authentication during IKE and TLS
		Internal using DKM	Stored on disk in P12 format ($FWDIR/conf/dkmKeys.p12) – plaintext	
Preshared keys for IKE (SHA-1 HMAC)	IKE preshared key (48 – 512 bits)	Outside of crypto-boundary	Stored on disk ($FWDIR$/database/fwauth.NDB) - plaintext	Authentication during IKE
Diffie-Hellman key pairs	Diffie-Hellman key pairs (2048, 3072, 4096,	Generated by IKE negotiations	RAM only (public parameters stored on disk ($FWDIR/database/objects.C and	Key exchange during IKE

Key	Key type	Generation	Storage	Use
	6144, 8192 bits)		$FWDIR/state/local/FW1/local.objects) - plaintext	
Session keys for IPSec	TDES keys (168 bits), AES (128, 256 Bits)	Generated by IKE negotiations	RAM only - plaintext	Secure IPSec traffic
Session keys for TLS	TDES keys (168 bits)	Generated by TLS negotiations	RAM only – plaintext	Secure TLS traffic (VPN)
Session keys for management	TDES keys (168 bits)	Generated by TLS handshake	Cached to disk ($CPDIR$/database/session.NDBX) - plaintext	Secure TLS traffic (SIC)
X9.31 PRNG seed keys	Triple-DES (112 bit)	Generated by gathering entropy	RAM only, but entropy used to generate keys is cached to disk ($CPDIR/registry/HKLM_registry.data and $CPDIR/registry/HKLM_registry.data.old) - plaintext	Random number generator

Table 7 – Listing of the Module's CSPs

The Local Crypto-Officer passwords are used to authenticate the Local Crypto-Officer to the CLI. Additionally, these passwords are used to switch CLI modes and to access the bootloader. These passwords are configured by the local Crypto-Officer over the CLI or by the Remote Crypto-Officer over an authenticated, encrypted management session. These passwords are stored on the module's hard drive, and can be zeroized by changing the password or reformatting the hard drive. The module must be under control of the operator during reformatting.

The RSA key pair for remote management sessions is generated externally by the management software. This key pair is loaded onto the module during the setup of secure communications with a management station over a secure TLS session. This key pair is stored on the module's hard drive and can be zeroized by reformatting the hard drive containing the module's software or re-initializing SIC. The module must be under control of the operator during reformatting.

The RSA key pair used by IKE and remote access TLS-based VPN can be generated either external to the module by the management software or internally by the module through Distributed Key Management (DKM). When generated externally, this key pair is loaded onto the module over a secure TLS session established between the module and the management software. When DKM is used, this key pair is generated internally by the module. The Local Crypto Officer configures the module for either internal key generation or to import external keys from the management station. This key pair is stored on the module's hard drive in plaintext and can be zeroized by reformatting the module's hard drive containing the module's software. Additionally, it can be overwritten by generating a new RSA key pair. The module must be under control of the operator during reformatting.

Pre-shared keys are input into the module over an encrypted management session. These keys are used during IKE for authentication. The pre-shared key configuration information is stored on the module's hard drive and can be zeroized by reformatting the hard drive containing the module's software. Additionally, it can be overwritten by changing the pre-shared key. The module must be under control of the operator during reformatting.

Diffie-Hellman (DH) key pairs are generated during IKE for use for key exchange during IKE. These are ephemeral key pairs

Session keys for IPSec are ephemeral keys established for IPSec connections. These keys are negotiated during IKE as part of the DH key agreement. They are generated as needed by an SA and are only stored in volatile memory. These keys can be zeroized by powering down the module.

Session keys for TLS-based VPNs are ephemeral keys established as part of the TLS handshake protocol. They are generated as needed and are only stored in volatile memory. These keys can be zeroized by powering down the module.

Session keys for management session are established by the TLS handshake protocol. These keys are used to encrypt management session and are generated as needed by the TLS handshake. These keys are stored in volatile memory as well as cached to disk for possible reuse. The keys in volatile memory can be zeroized by powering down the module. The keys cached to disk can be zeroized by reformatting the hard drive containing the module's software. The module must be under control of the operator during reformatting.

The X9.31 pseudo-random number generator (PRNG) keys are generated by the module using entropy gathered from various sources. The entropy used to generate these keys is cached to the module's hard drive and are used by the X9.31 PRNG. This entropy can be zeroized by reformatting the hard drive containing the module's software. The module must be under control of the operator during reformatting.

Non-Approved Algorithms

The cryptographic module includes the following non-approved algorithms:

- RSA (Key Transport)
- Diffie-Hellman (Key agreement)

- CAST (40 bits)
- CAST (128 bits)
- HMAC MD5
- MD5
- DES-CBC

Self-Tests

The module performs a set of self-tests in order to ensure proper operation in compliance with FIPS 140-2. These self-tests are run during power-up (power-up self-tests) or when certain conditions are met (conditional self-tests).

Power-up Self-tests:

- Firmware Integrity Tests: The module checks the integrity of its various components using a 56-bit error detection code (EDC) calculated by the cphash binary when FIPS mode is enabled.
- Cryptographic Algorithm Known Answer Tests (KATs): KATs are run at power-up for AES, RSA, and Triple-DES encryption/decryption, pseudo-random number generation, SHA-1 hashing, and HMAC with SHA-1 calculation.
    - AES-CBC KAT
    - Triple-DES-CBC KAT
    - PRNG KAT
    - RSA (encrypt/decrypt) and (sign/verify) KAT tests
    - SHA-1 KAT
    - SHA-1 HMAC KAT

Conditional Self-tests:

- Continuous Random Number Generator Test: This test is constantly run to detect failure of the module’s random number generator
- RSA pair-wise consistency test: This test is run by the module whenever RSA key pairs are generated internally to support

Distributed Key Management to verify that a valid key pair was created.

If any of the kernel module KATs fail, the system enters the kernel panic state. If any one of the service KATs fails, that service halts and the system enters the error state. If the KATs are passed (by both the kernel modules and the services), the success is logged to the Check Point log. If the power-up software integrity check fails, the system enters the integrity check failure state, halts, and has to be restarted. If the software integrity check passes, the event is logged to the Check Point log. If the continuous RNG test fails, the system reboots. All errors are logged to the Check Point logs.

When the module enters the error state, all cryptographic services and data output for the problem service is halted until the error state is cleared. Restarting the module or the failed service can clear the error state.

Design Assurance

Check Point uses a hybrid configuration management system for its products and documentation management needs. Both CVS and Rational® ClearCase® are used for configuration management of product source code releases. These software applications provide access control, versioning, and logging capabilities for tracking the components included in the various Check Point products. Manual configuration management controls are utilized for the associated product documentation. A formal process has been implemented whereby a log is kept of all product documentation and updates. Product documentation releases are tied to versions of the cryptographic module and source code build releases through this log.

Subversion is used to provide configuration management and archival for the module's FIPS 140-2 documentation. This document database application provides access control, versioning, and logging for documents created in support of FIPS 140-2 validation testing efforts.

Mitigation of Other Attacks

The module is designed to meet the overall FIPS 140-2 level 1 requirements and provides the standard level of security that comes with meeting those requirements. It does not provide mitigation against other attacks.

SECURE DELIVERY AND OPERATION

Check Point Connectra version NGX meets overall Level 1 requirements for FIPS 140-2 and level 3 for design assurance. The sections below describe how to securely deliver the module to authorized operators,and place and keep the module in FIPS-approved mode of operation.

Secure Delivery

The cryptographic module ships from the manufacturer to the customer without any cryptographic keys. The only critical security parameter (CSP) is the default password contauined in the ISO image that is configured during installation. All other cryptographic keys and CSPs are generated after the containing module installation.

When the module powers up, firmware integrity tests check the integrity of its various components using a 56-bit error detection code (EDC) calculated by the cphash binary when FIPS mode is enabled.

Other known answer tests (see Self Tests in this document for a complete description of known answer tests) confirm the correct operation of cryptographic algorithms and security functions. If any of these tests fail, the module will not initialize.

FIPS Mode Configuration

Local Crypto-Officer Configuration Steps

The Local Crypto-Officer must perform the following operations during installation and initialization of the module in order to enable the FIPS mode of operation.

Note: These instructions also apply if the Local Crypto-Officer is migrating from previous module versions to the evaluated cryptographic module version. The Local Crypto-Officer must reinstall and reinitialize the module as per these instructions.

Module version NGX R66.1 with hot fix HFA 1 includes support for Diffie-Hellman Group 14 (2048 bit modulus) key size. Additional Diffie-Hellman Groups 15-18 (3072 bits to 8192 bits) can be optionally configured. To support Groups 15-18, the Local Crypto-Officer must obtain SK27054 from Check Point support before beginning the initialization of the module. The SK contains a procedure for enabling the additional groups and will be run during the initialization process.

The system time clocks of the module platform, the management station, and any other trusted systems must all be synchronized.

1. Install the Secure Platform operating system. The module automatically reboots the system once this is completed.

   Note: when installing onto some computing platforms, it will be necessary to load the software from a temporarily-connected USB CD-ROM or via the network interface by using FTP.

2. Login to the console using the default Local Crypto-Officer password. The module will immediately request that this password be changed.

3. At the command prompt, run the following command to begin configuration of the module.

   ```
   sysconfig
   ```

   The following will be performed via the menus displayed when “sysconfig” is run.

   a. Perform the network configuration, date and time configuration, and the licensing configuration.

   b. When prompted to select Check Point software to install on top of the operating system, select only “Connectra Power”, and select a distributed (not standalone) installation.

   c. Continue through the rest of the configuration until the sysconfig command finishes.

4. Reboot the module.

5. Login to the console.

6. Switch to expert mode.

7. Copy /boot/grub/grub.conf to /boot/grub/grub.conf.bak.

8. Edit /boot/grub/grub.conf and remove all of the lines below and including the “title Start in maintenance mode” line.

9. Save /boot/grub/grub.conf.

10. Copy /etc/cpshell/cpshell.cfg to /etc/cpshell/cpshell.cfg.bak.

11. Edit /etc/cpshell/cpshell.cfg and remove the line beginning with “patch”.

12. Save /etc/cpshell/cpshell.cfg.

13. Copy /etc/cpshell/fips.cfg to /etc/cpshell/fips.cfg.bak.

14. Edit /etc/cpshell/fips.cfg and add the following line.

    ```
    expert 0 1 “expert” “Switch to expert mode”
    ```

15. Save /etc/cpshell/fips.cfg.

16. Copy /bin/fips to /bin/fips.bak.

17. Edit /bin/fips and remove -f from the following line.

```
file -f  `cat exe_files | grep ^/boot/` | grep -v dir | grep -v sym
```

18. Save /bin/fips.

19. Copy $CPDIR/conf/sic_policy.conf to $CPDIR/conf/sic_policy.conf.bak.

20. Edit $CPDIR/conf/sic_policy.conf and remove all of the following keywords:

    sslca_rc4

    sslca_rc4_comp

    asym_sslca_rc4

    asym_sslca_rc4_comp

    none

    sslca_clear

    ssl

    sslclear

    fwa1

    skey

    fwn1

    skey2

    ssl_opsec

    fwn1_opsec

    Note: If removal of these terms results in the column being blank (columns are delimited by a semi-colon (';')) then comment the line out or remove it. If these words are followed by a comma (', '), then remove it as well.

21. Save $CPDIR/conf/sic_policy.conf.

22. This step is optional. If configuring support for additional Diffie-Hellman Groups 15-18, follow the instructions found in SK27054 for defining the moduli for these Diffie-Hellman Groups in the product database. See also note under Step #1.

23. Exit expert mode.

24. Switch the module to FIPS mode by entering the following command:

```
fips on
```

25. Reboot.

Running the “fips on” command disables SSH, disables the Web UI, removes support for SSLv3 from SIC (i.e. only TLS is supported), enables Local Crypto-Officer account lockout of 60 minutes after 3 failed authentication attempts, disables remote installation daemon, and removes access to the fw, fwm, and vpn command line utilities.

The Local Crypto-Officer must not switch out of FIPS mode or disable the software integrity check.

Management Station Configuration Steps

In order for the external management station to operate correctly with the module running in FIPS mode, the following commands must be run on the management station. Also, the time clock on the management station should be synchronized with the module platform as well as any other trusted systems.

1. If the Check Point services are running, execute the following command to stop all Check Point services.

```
cpstop
```

2. Copy $CPDIR/conf/sic_policy.conf to $CPDIR/conf/sic_policy.conf.bak.

3. Edit $CPDIR/conf/sic_policy.conf and remove all of the following keywords:

```
sslca_rc4
sslca_rc4_comp
asym_sslca_rc4
asym_sslca_rc4_comp
none
sslca_clear
ssl
sslclear
fwa1
```

```
skey
fwn1
skey2
ssl_opsec
fwn1_opsec
```

Note: If removal of these terms results in the column being blank (columns are delimited by a semi-colon (';')) then comment the line out or remove it. If these words are followed by a comma (', '), then remove it as well.

4. Run the following command to enable only TLSv1 for management sessions.

```
ckp_regedit -a "Software\CheckPoint\SIC" FIPS_140 -n 1
```

5. If the Check Point services were stopped in step 1, restart them by entering the following command.

```
cpstart
```

Remote Crypto-Officer Configuration Guidelines

The Remote Crypto-Officer must follow the following guidelines for configuring the modules services.

Authentication during IKE and TLS must employ pre-shared keys or digital certificates. Additionally, only the following FIPS-approved algorithms may be used by IPSec, IKE and TLS:

Data Encryption

- Triple-DES
- AES

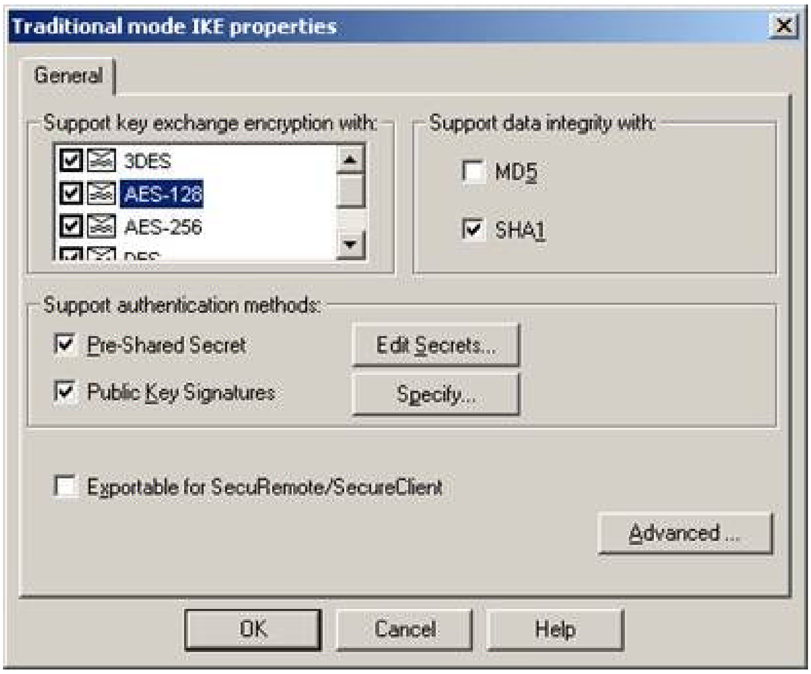
Data Packet Integrity

- HMAC with SHA1

Authentication

- Certificates
- Pre-shared keys

The following figures contain screen-shots that illustrate the module’s FIPS mode settings:



Support key exchange encryption with:

- ☑ 3DES
- ☑ AES-128
- ☑ AES-256
- DES

Support data integrity with:

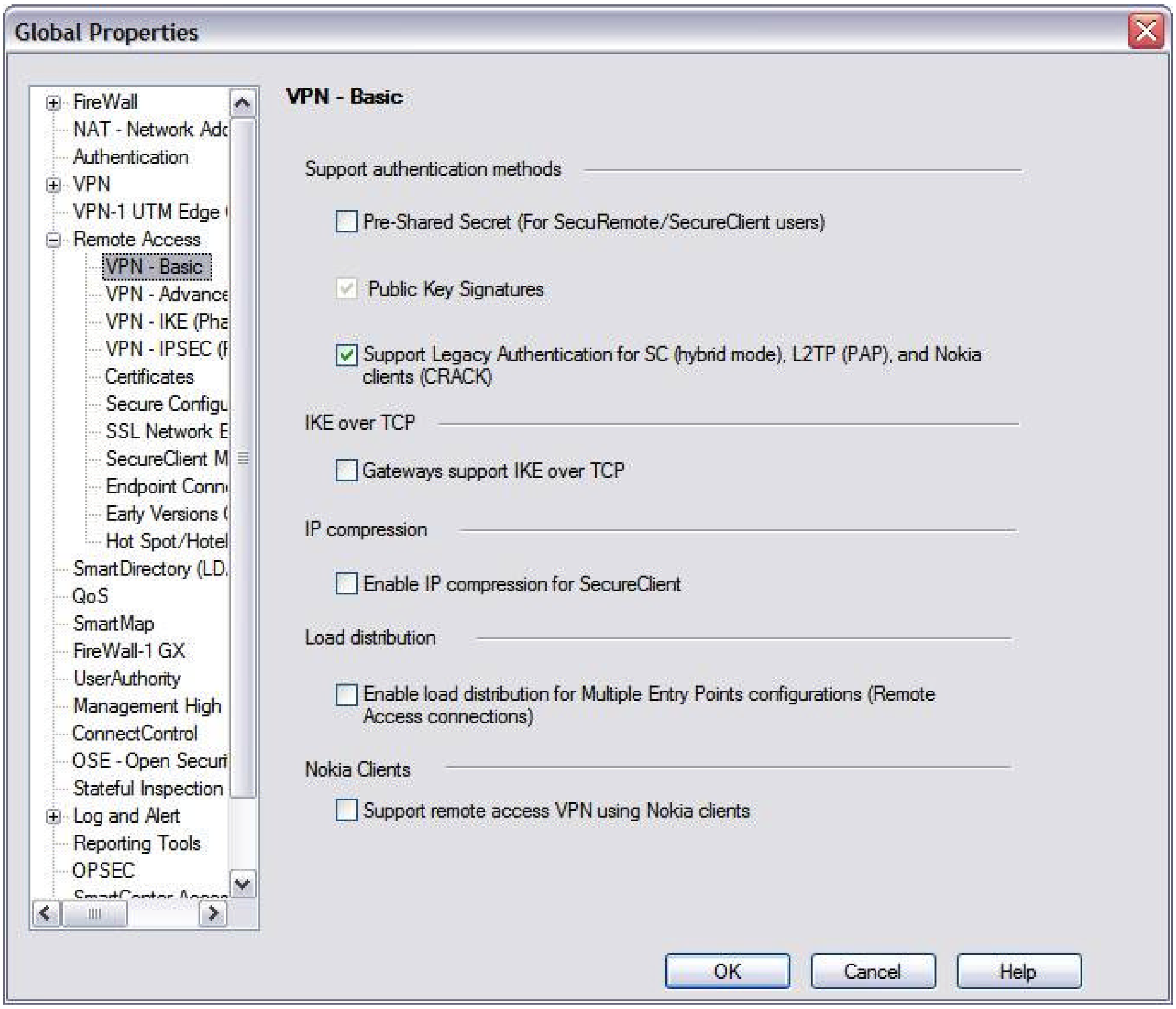
- □ MD5
- ☑ SHA1

Support authentication methods:

- ☑ Pre-Shared Secret
- ☑ Public Key Signatures

□ Exportable for SecuRemote/SecureClient

Figure 4 – Only FIPS-Approved Algorithms may be used with IKE



VPN - Basic

Support authentication methods

□ Pre-Shared Secret (For SecuRemote/SecureClient users)

☑ Public Key Signatures

☑ Support Legacy Authentication for SC (hybrid mode), L2TP (PAP), and Nokia clients (CRACK)

IKE over TCP

□ Gateways support IKE over TCP

IP compression

□ Enable IP compression for SecureClient

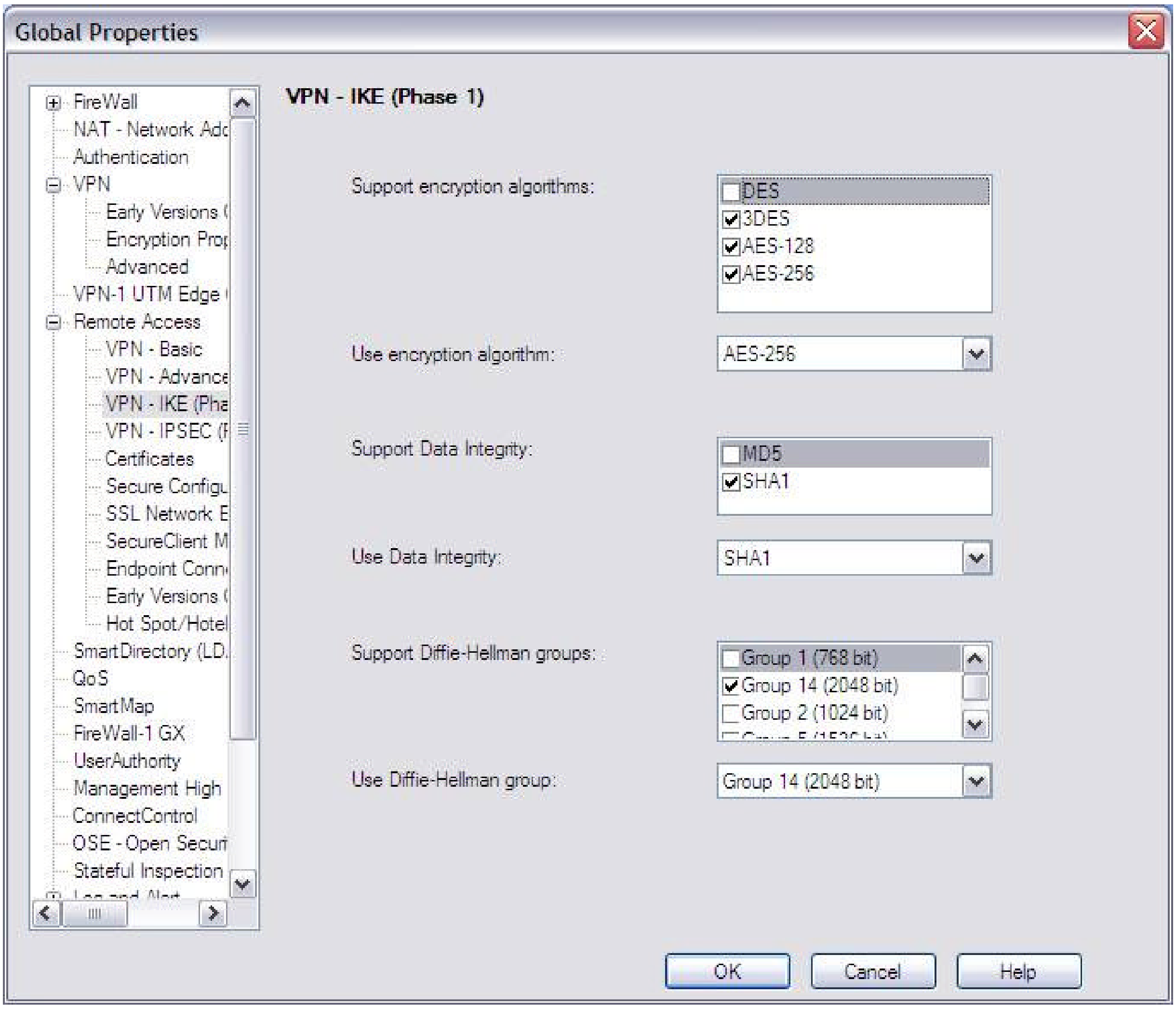
Load distribution

□ Enable load distribution for Multiple Entry Points configurations (Remote Access connections)

Nokia Clients

□ Support remote access VPN using Nokia clients

Figure 5 – Only Pre-Shared Keys or Digital Certificates may be used to Authenticate Clients



VPN - IKE (Phase 1)

Support encryption algorithms: □ DES ☑ 3DES ☑ AES-128 ☑ AES-256

Use encryption algorithm: AES-256

Support Data Integrity: □ MD5 ☑ SHA1

Use Data Integrity: SHA1

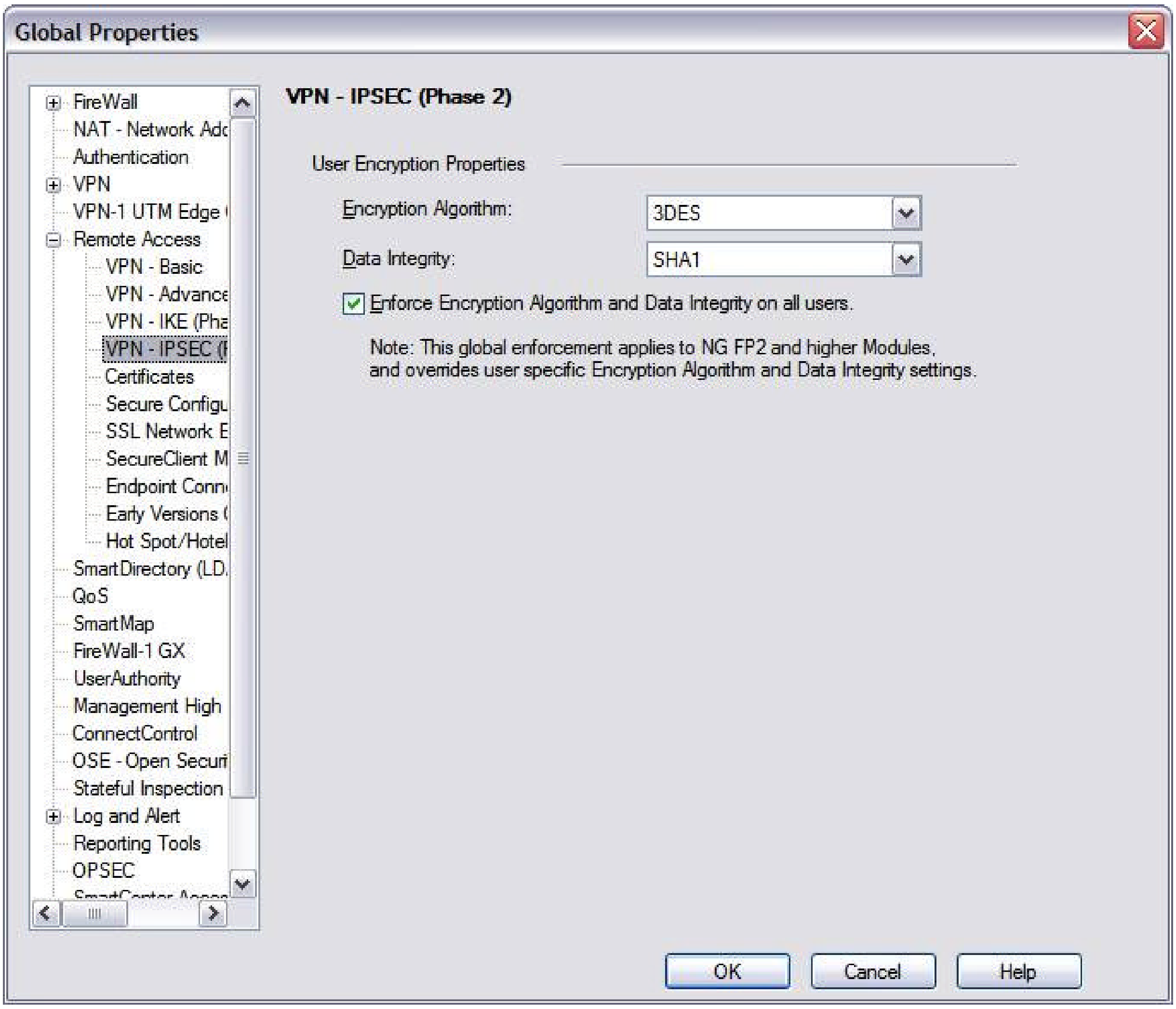
Support Diffie-Hellman groups: □ Group 1 (768 bit) ☑ Group 14 (2048 bit) □ Group 2 (1024 bit)

Use Diffie-Hellman group: Group 14 (2048 bit)

Figure 6 – Only FIPS-Approved Algorithms may be used with IKE

Notes:

1. Diffie-Hellman Group 14 (2048-bits) provides 112 bits of encryption strength. Only Diffie-Hellman groups 14 or higher, providing 112 or more bits of encryption strength may be used.



VPN - IPSEC (Phase 2)

User Encryption Properties

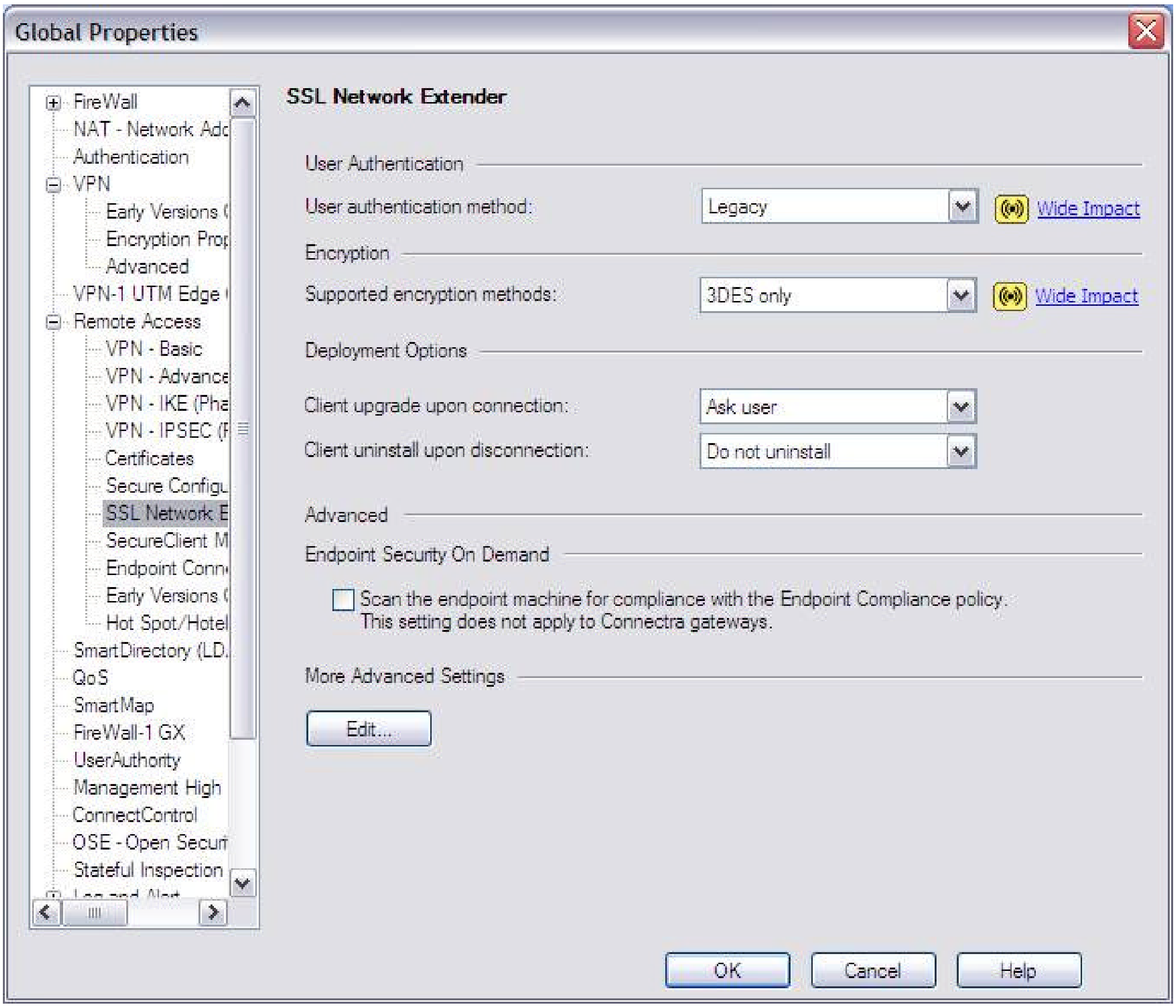
Encryption Algorithm: 3DES

Data Integrity: SHA1

☑ Enforce Encryption Algorithm and Data Integrity on all users.

Note: This global enforcement applies to NG FP2 and higher Modules, and overrides user specific Encryption Algorithm and Data Integrity settings.

Figure 7 – Only FIPS-Approved Algorithms may be used with IPSec



SSL Network Extender

User Authentication

User authentication method: Legacy

Encryption

Supported encryption methods: 3DES only

Deployment Options

Client upgrade upon connection: Ask user

Client uninstall upon disconnection: Do not uninstall

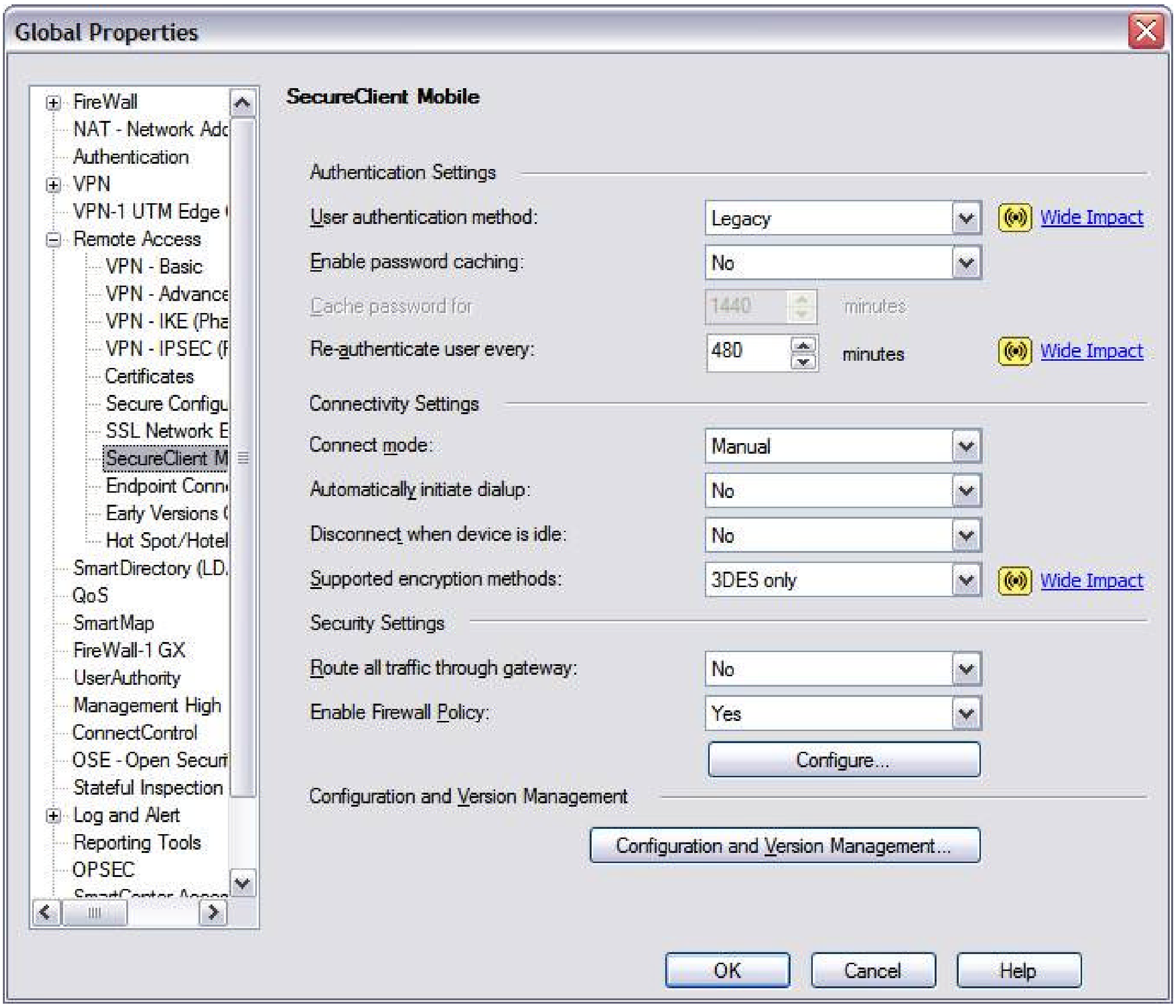
Advanced

Endpoint Security On Demand

□ Scan the endpoint machine for compliance with the Endpoint Compliance policy.
This setting does not apply to Connectra gateways.

More Advanced Settings

Figure 8 – Only FIPS-Approved Algorithms may be used with TLS



SecureClient Mobile

Authentication Settings

User authentication method: Legacy

Enable password caching: No

Cache password for 1440 minutes

Re-authenticate user every: 480 minutes

Connectivity Settings

Connect mode: Manual

Automatically initiate dialup: No

Disconnect when device is idle: No

Supported encryption methods: 3DES only

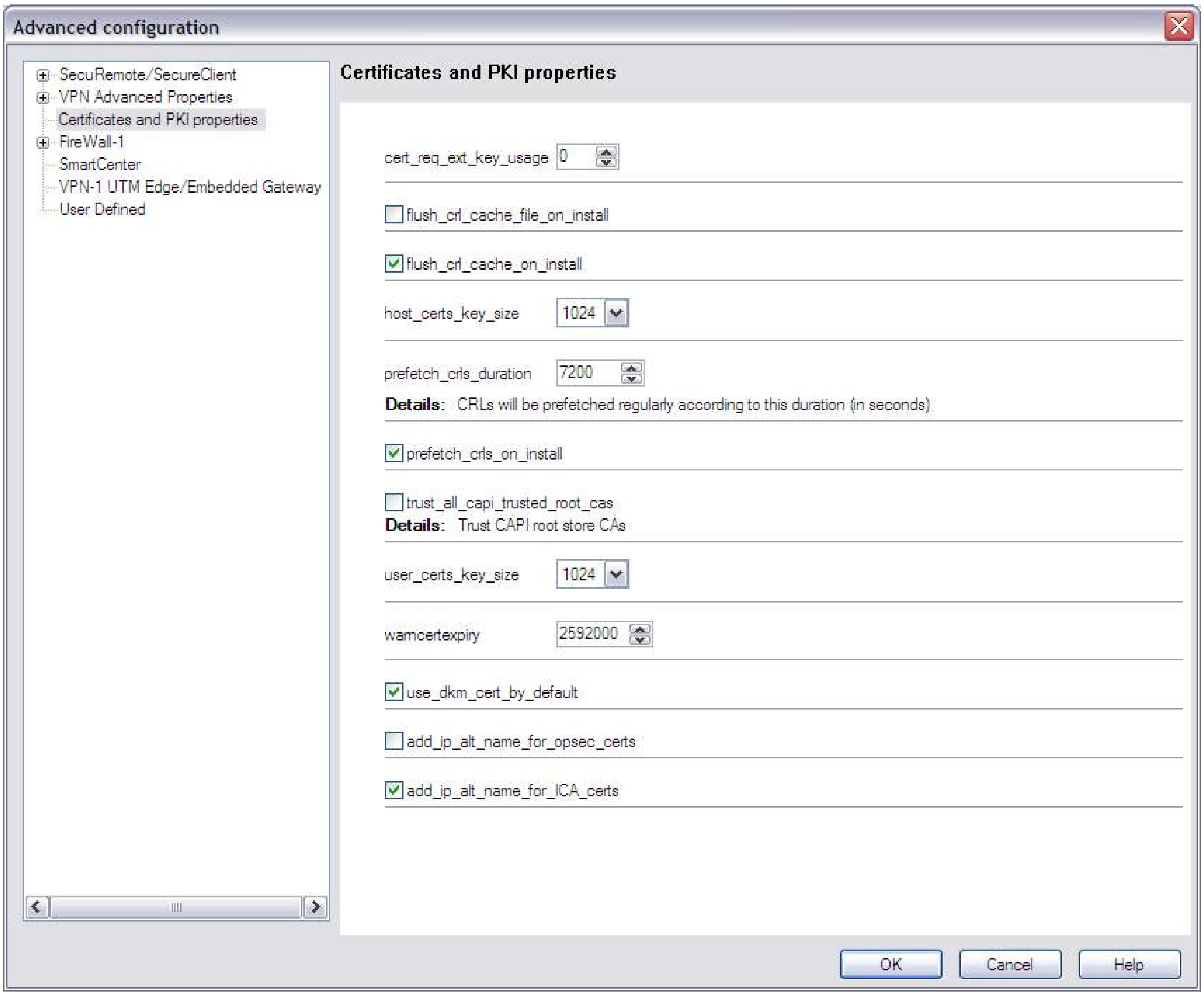
Security Settings

Route all traffic through gateway: No

Enable Firewall Policy: Yes

Configuration and Version Management

Figure 9 – Only FIPS-Approved Algorithms may be used with TLS



Advanced configuration

Certificates and PKI properties

cert_req_ext_key_usage 0

□ flush_crl_cache_file_on_install

☑ flush_crl_cache_on_install

host_certs_key_size 1024

prefetch_crls_duration 7200

Details: CRLs will be prefetched regularly according to this duration (in seconds)

☑ prefetch_crls_on_install

□ trust_all_capi_trusted_root_cas

Details: Trust CAPI root store CAs

user_certs_key_size 1024

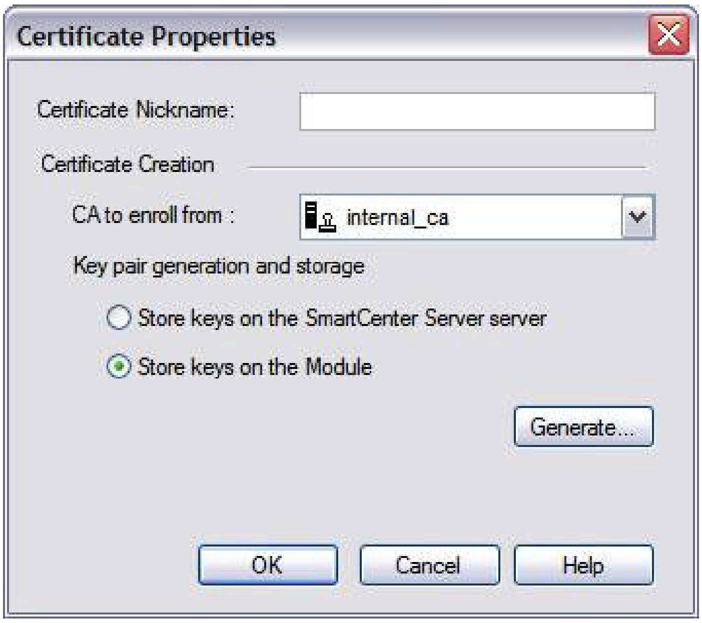
warncertexpiry 2592000

☑ use_dkm_cert_by_default

□ add_ip_alt_name_for_opsec_certs

☑ add_ip_alt_name_for_ICA_certs

Figure 10 – Configuring the module to enable Distributed Key Management (DKM) globally



Certificate Properties

Certificate Nickname:

Certificate Creation

CA to enroll from : internal_ca

Key pair generation and storage

○ Store keys on the SmartCenter Server server

● Store keys on the Module

Figure 11 – Configuring the module to generate RSA keys with DKM on a per-certificate basis

Crypto-Officer Guidance

The Crypto-Officer is responsible for installation and initialization of the module, configuration and management of the module, and removal of the module. More details on how to use the module can be found in the Check Point Connectra user manuals.

The Crypto-Officer receives the module in a shrink wrapped package containing a CD-ROM with the Connectra installation media and user documentation. The Crypto-Officer should examine the package and shrink wrap for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

Before the installation of the module, there is no access control provided by the module. Therefore, the Crypto-Officer must maintain control of the installation media.

During installation, the Crypto-Officer boots a standard PC from the CD-ROM containing the module's software. The Crypto-Officer will walk through a series of steps, and must follow the directions above to properly configure the module for FIPS 140-2 compliance.

The Local Crypto-Officer password for the module is a default after installation. Before this is changed, the Crypto-Officer must maintain control of the module. This must be changed immediately upon logging into the module after installation.

The Crypto-Officer must establish the SIC configuration after logging into the module for the first time. Once this has been completed, the module has been adequately initialized and can be managed from the management server.

Management

Once initialization of the module has been completed, the Crypto-Officer must manage the module using the remote management server. Through this server, the Crypto-Officer is able to configure policies for the module. These policies determine how the VPN services of the module will function.

The Crypto-Officer is responsible for maintaining the module. Besides management of the module, this involves monitoring the module's logs. If unusual or suspicious activity is found, the Crypto-Officer must take the module offline and investigate.

If the module consistently malfunctions or otherwise repeatedly enters an error state, the Crypto-Officer must contact the manufacturer.

Termination

At the end of the life cycle of the module, the Crypto-Officer must reformat the hard drive containing the module's software. This will zeroize all keys and other CSPs. Note the module must be under control of the operator during reformatting.

User Guidance

The User accesses the module's VPN functionality as an IPSec client or as a remote access TLS-based VPN client. Although outside the boundary of the module, the User must be careful not to provide authentication information and session keys to other parties.

ACRONYMS

AH	Authentication Header
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DKM	Distributed Key Management
DSA	Digital Signature Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FP	Feature Pack
HF	Hot Fix
IKE	Internet Key Exchange
IPSec	IP Security
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NG	Next Generation
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PC	Personal Computer
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RIP	Routing Information Protocol
RSA	Rivest Shamir and Adleman
SA	Security Association
SHA	Secure Hash Algorithm
SIC	Secure Internal Communications
SNMP	Simple Network Management Protocol
SP	Secure Platform
SSH	Secure Shell
SVN	Secure Virtual Network
TLS	Transport Layer Security
VPN	Virtual Private Network