

Check Point[®]
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

VPN-1

FIPS 140-2 Non-Proprietary Security Policy

**FIPS 140-2 Level 1
Firmware**

**Version 1.0
October 2006**

Table of Contents

INTRODUCTION.....	3
PURPOSE.....	3
REFERENCES	3
CHECK POINT VPN-1	4
OVERVIEW	4
CRYPTOGRAPHIC MODULE	5
MODULE INTERFACES	7
ROLES AND SERVICES.....	8
<i>Remote Crypto Officer Role</i>	<i>9</i>
<i>Local Crypto Officer Role</i>	<i>11</i>
<i>User Role</i>	<i>13</i>
<i>Authentication Mechanisms</i>	<i>14</i>
<i>Unauthenticated Services</i>	<i>15</i>
PHYSICAL SECURITY	15
OPERATIONAL ENVIRONMENT	15
CRYPTOGRAPHIC KEY MANAGEMENT	15
<i>Management Workstation</i>	<i>20</i>
SELF-TESTS.....	20
DESIGN ASSURANCE	21
MITIGATION OF OTHER ATTACKS.....	22
SECURE OPERATION	22
FIPS MODE CONFIGURATION	22
<i>Local Crypto-Officer Configuration Steps</i>	<i>22</i>
<i>Management Station Configuration Steps.....</i>	<i>25</i>
<i>Remote Crypto-Officer Configuration Guidelines</i>	<i>27</i>
CRYPTO-OFFICER GUIDANCE	32
<i>Management</i>	<i>32</i>
<i>Termination</i>	<i>33</i>
USER GUIDANCE	33
ACRONYMS	34

Introduction

Purpose

This is non-proprietary cryptographic module Security Policy describes the Check Point Software Technologies Ltd. (Check Point) VPN-1 cryptographic module, version *NGX (R60)* with hot fix HFA-03. This security policy describes how the Check Point VPN-1 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/cryptval/>.

Check Point VPN-1 version NGX (R60) with HFA-03 is alternatively referenced in this document as *Check Point VPN-1*, *VPN-1*, *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.ncsl.nist.gov/cryptval/>) provides contact information for answers to technical or sales-related questions regarding the module.

CHECK POINT VPN-1

Overview

Check Point's VPN-1 is a tightly integrated software solution combining the FireWall-1 (FW-1) security suite with sophisticated Virtual Private Network (VPN) technologies and a hardened Operating System (OS). The cornerstone of Check Point's Secure Virtual Network (SVN) architecture, VPN-1 meets the demanding requirements of Internet, intranet, and extranet VPNs by providing secure connectivity to corporate networks, remote and mobile users, branch offices, and business partners. VPN-1 solutions are available on the industry's broadest range of open platforms and security appliances — meeting the price/performance requirements of any size organization.

Check Point VPN-1 is integrated with the industry-standard, market-leading FireWall-1 and the hardened Operating System SecurePlatform.

- Check Point VPN-1/FireWall-1, the industry's leading Internet security solution, provides the highest level of security, with access control, content security, authentication, and integrated Network Address Translation. Only FireWall-1 delivers true Stateful Inspection across the broadest set of applications in the industry, including Voice over IP and multimedia applications.
- Check Point SecurePlatform is 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.

VPN-1 is designed to allow secure access to an organization's resources to multiple users over an unsecured TCP/IP network. Relying on a hardened, optimized operating system coupled with FireWall-1, it performs all the required security functions and provides the following high-level functionality:

- Screening of all incoming communications to ensure authorized user access.
- Secure, authenticated and encrypted sessions with Clients and subsystems.
- Secure VPN between subsystems.
- Central security administration.

Cryptographic Module

The Check Point VPN-1 cryptographic module is a FIPS 140-2 firmware module. The physical embodiment is multi-chip standalone. VPN-1 is intended to run on any general purpose PC-class computing platform. Because the module is a firmware module, the Cryptographic Algorithm Validation Program (CAVP) requires the specific processors upon which the firmware algorithms execute to be included in the implementation specification. This information is included in Chart 1 below. 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 VPN-1 and FireWall-1 firmware running on the Secure Platform Operating System. Physically, the cryptographic boundary of the module is the GPC case, which physically encloses the module. The physical ports, logical interfaces, and FIPS logical interfaces are described in Table 2.

In order to install the FIPS 140-2 compliant module, version NGX (R60) with hotfix HFA-03 or later must be used. See the section of this document titled *Secure Operation* for more details.

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

Operational Environment	Module firmware and Check Point SecurePlatform™ Operating System Version NGX (R60) with HFA-03 or later
	<u>Test Platforms</u> <ul style="list-style-type: none"> ▪ General Purpose Computer (GPC) with single and dual AMD Opteron® processor configurations ▪ General Purpose Computer (GPC) with single and dual Intel XEON® processor configurations

Chart 1 – Module Operational Environments Tested

The following representative GPC platforms were used in testing:

- **AMD Opteron®:** Sun Fire x64/x86 server family, single and dual processors
- **Intel XEON®:** SmartGig platform, single and dual processors



FIPS 140-2 validation is maintained so long as the module is installed onto any GPC that implements one of the tested processor configurations specified above.

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	3
9	Self-tests	1
10	Design Assurance	2
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.

This version of the module is identical to the FIPS 140-2 validated version Next Generation (NG) with Application Intelligence (AI) (R54) [FIPS 140-2 Certificate #634] with the exception that version NGX (R60) HFA-03 adds additional support for Internet Key Exchange (IKE) functions by including

the following Diffie-Hellman Modular Exponential (MODP) Groups per RFC 3526 in addition to the modulus sizes already supported in version NG with Application Intelligence (R54):

<u>Diffie-Hellman Group</u>	<u>Modulus Size</u>
14	2048
15	3072
16	4096
17	6144
18	8192

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	Keyboard ports, USB ports, serial ports, network ports
Data output interface	User Interface (UI) for the VPN-1, Network Layer IP interface	Network ports, serial ports, monitor port
Control input interface	User Interface (UI) for the VPN-1, Network Layer IP interface	Keyboard ports, USB ports, serial ports, network ports
Status output interface	User Interface (UI) for the VPN-1, Network Layer IP interface, Log files	Network ports, serial ports, monitor port
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 VPN-1. 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 VPN-1. 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.

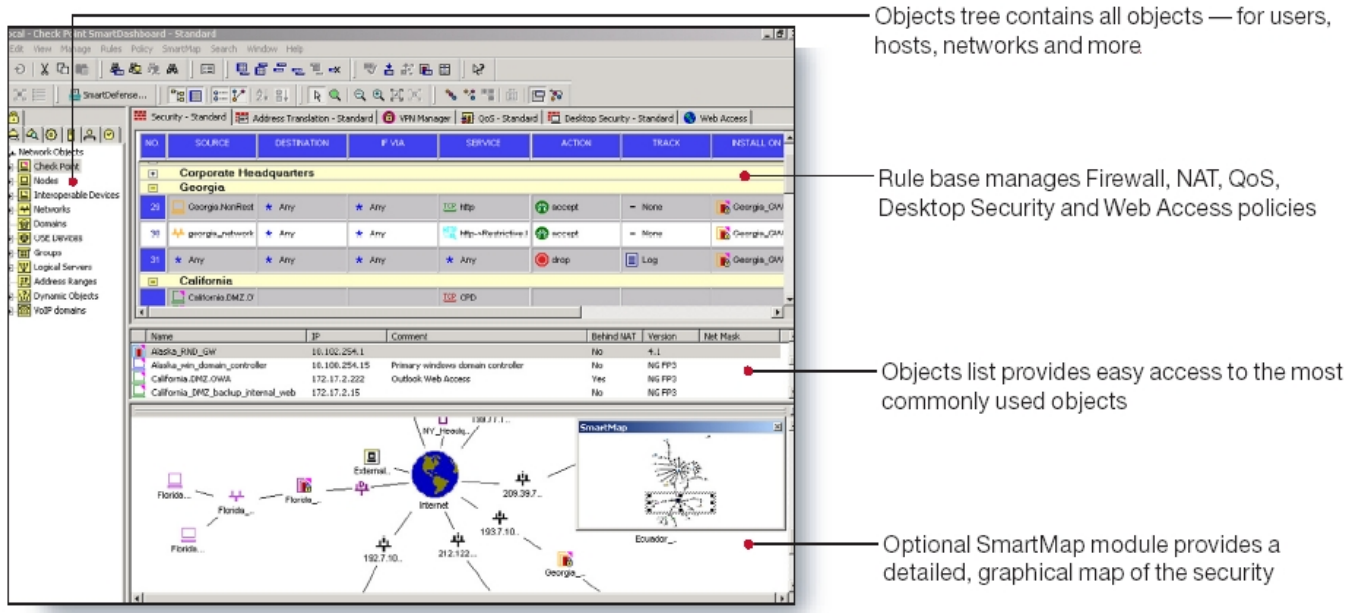


Figure 1– Easy to Use Management Tools

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 VPN-1 and the client using IPsec. Of note, module can itself act as a User when establishing tunnels to other modules.

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

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
Define and Implement Security Policies (including the rule sets governing the automatic, alternating bypass)	Configure and install security policies that are applied to the network and users. These policies contain a set of rules that govern the communications flowing into and out of the module, and provide the Crypto-Officer with a means to control the types of traffic permitted to flow through the module. These policies include the rules that govern the automatic, alternating bypass state of the module.	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 for authentication	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	RSA key pair for IKE (read/write access); pre-shared keys for IKE (read/write access)
Initialization of Secure Internal Communication (SIC)	Establish trust between management server and the VPN-1 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	DES-MAC integrity key (read access)
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

Service	Description with CLI commands	Input	Output	CSP
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
Check Point module commands	<p>Install licenses, configure the SNMP daemon, modify the list of Unix groups authorized to run VPN-1/FW-1 services, register a cryptographic token, enter random data to help seed the PRNG, configure the one time SIC password, and specify whether the VPN-1/FW-1 services should automatically start at boot time (all functionality is provided through text-based menuing system after executing cpconfig)</p> <p>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)</p>	<p>Command (cpconfig), menu options, and configuration information</p> <p>Command, any options, and configuration information</p>	<p>Status of commands/menu options and status information (configuration information)</p> <p>Status of commands and status information (diagnostic information, version numbers, and license information)</p>	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

Service	Description with CLI commands	Input	Output	CSP
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
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.	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 authenticates to the module using digital certificates or pre-shared keys.

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)

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 1024, 2048 and 4096 bits. Using 1024 bit key pair (the default), is generally considered equivalent to brute forcing an 80 bit key (i.e., a 1 in 2^{80} 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 1024, 2048 and 4096 bits. Using a 1024 bit key pair (the default), this is generally considered equivalent to brute forcing an 80 bit key (i.e., a 1 in 2^{80} chance of false positive).
Pre-shared key-based authentication (IKE)	SHA-1 HMAC generation/verification is used to authenticate to the module during IKE with pre-shared keys (at least 6 characters in length). Considering the possible field of ASCII characters, the number of potential passwords is 94^6 .
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: $(2^{80}) / (100,000 * 60) = 2 * 10^{17}$ 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 VPN-1'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.

VPN-1 provides the capability to use TLSv1 to secure management sessions. 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 VPN-1 cryptographic module implements the following FIPS-Approved algorithms (NIST-assigned algorithm validation certificate numbers shown in boxed items):

Data Encryption:

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

NGX (R60)
Certificate #257

- Data Encryption Standard (DES) in CBC mode (56 bit keys) – as per NIST PUB FIPS 46-3 (withdrawn)

NGX (R60)
Certificate #314 (transitional phase only - valid until May 19, 2007)

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

NGX (R60)
Certificate #338

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).

NGX (R60)
Certificate #67

Data Hashing:

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

NGX (R60)
Certificate #332

PRNG:

- ANSI X9.31 Implementation

NGX (R60)
Certificate #90

Digital Signatures:

- RSA – PKCS#1 and X9.31

NGX (R60)
Certificate #66 (SigGen/SigVer) Certificate #132 (KeyGen)

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 70 and 202 bits of encryption strength.
- The RSA key wrapping methodology (used by TLS), provides between 80 bits and 150 bits of encryption strength.

In addition to the FIPS-Approved algorithms, the Check Point VPN-1 provides the following non FIPS-approved algorithms:

- CAST (40 or 128 bit keys)
- HMAC-MD5 (16 bytes) – as per RFC 2104 (HMAC: Keyed-Hashing for Message Authentication) and RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH).
- MD5

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 (1024 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	RSA key pair (1024, 2048 or 4096 bits)	Outside of Crypto boundary	Stored on disk (\$FWDIR\$/database/fwauth.NDBX) – plaintext	Authentication during IKE
		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 (768, 1024, 1536, 2048, 3072, 4096, 6144, 8192 bits)	Generated by IKE negotiations	RAM only (public parameters stored on disk (\$FWDIR/database/objects.C and \$FWDIR/state/local/FW1/local.objects) - plaintext	Key exchange during IKE
Session keys for IPSec	DES/TDES keys (56/168 bits), AES (128, 256 Bits)	Generated by IKE negotiations	RAM only - plaintext	Secure IPSec traffic
Session keys for management	DES/TDES keys (56/168 bits)	Generated by TLS handshake	Cached to disk (\$CPDIR\$/database/session.NDBX) - plaintext	Secure TLS traffic (SIC)
DES-MAC integrity check key	DES keys (56 bits)	Outside of crypto-boundary	Stored on disk (\$CPDIR/bin/cphash) - plaintext	Perform integrity check of module's software
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 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 RSA key pair used by IKE 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.

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.

Diffie-Hellman (DH) key pairs are generated during IKE for use for key exchange during IKE. These are ephemeral key pairs. The Diffie-Hellman public parameters are generated externally by the management software. These parameters are loaded onto the module over a secure TLS session established between the module and the management software. These parameters are stored on the module's hard drive, and can be zeroized by reformatting the hard drive containing the module's software or by generating a new set of DH public parameters.

Session keys for IPSec are ephemeral keys established for IPSec connections. These keys are negotiated during IKE as part of the DH key exchange. 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 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 DES-MAC integrity check key is generated externally from the module and is hard-coded into the cphash binary. This key is stored on the module's hard drive in plaintext and is used to perform the software integrity check. The keys cached to disk can be zeroized by reformatting the partition (or whole hard drive).

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.

Management Workstation

The Check Point management workstation, which is external to this module, generates RSA keys using ANSI X9.31. Those keys are used to digitally sign messages that are verified by the module when the management workstation (the Remote Crypto Officer) sends it commands. The management workstation's implementation of RSA has been issued NIST RSA algorithm certificate #67.

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:

- Software Integrity Tests: The module checks the integrity of its various components using a DES-MAC.
- Cryptographic Algorithm Known Answer Tests (KATs): KATs are run at power-up for AES, DES, RSA, and Triple-DES encryption/decryption, pseudo-random number generation, SHA-1 hashing, and HMAC with SHA-1 calculation.
 - AES-CBC KAT
 - DES-CBC KAT
 - Triple-DES-CBC KAT
 - PRNG KAT
 - RSA (encrypt/decrypt) and (sign/verify) KAT tests

- SHA-1 KAT
- SHA-1 HMAC KAT
- Bypass Mode Test: The module performs SHA-1 check value verification to ensure the policy files have not been modified.

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.
- Bypass Mode Test: The module performs SHA-1 check value verification to ensure the policy files have not been modified.

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.

Microsoft SharePoint® 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 OPERATION

Check Point VPN-1 version NGX meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

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 NGX (R60) HFA-03 or higher. The Local Crypto-Officer must reinstall and reinitialize the module as per these instructions.

Module version NGX (R60) includes support for Diffie-Hellman Groups up to Group 14 (2048 bit modulus) key sizes. 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 SmartGig 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. At point, the enterprise suite options menu is entered. Select “New Installation” and continue.
 - c. The next configuration menu determines which Check Point software to install on top of the operating system. Select only “VPN-1 & FireWall-1” and continue.
 - d. The setup type menu is now displayed. Select a distributed installation and continue.
 - e. The installation type menu is entered at this point. Select only “enforcement module” and continue.
 - f. 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 \$CPDIR/conf/sic_policy.conf to \$CPDIR/conf/sic_policy.conf.bak.
 17. 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.

18. Save \$CPDIR/conf/sic_policy.conf.
19. 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.

20. Exit expert mode.

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

```
fips on
```

22. Run the following command to rebuild the software integrity values.

```
fips integrity on
```

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

Data Encryption

- DES (for legacy use only; see notes following Figure 4)
- 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:

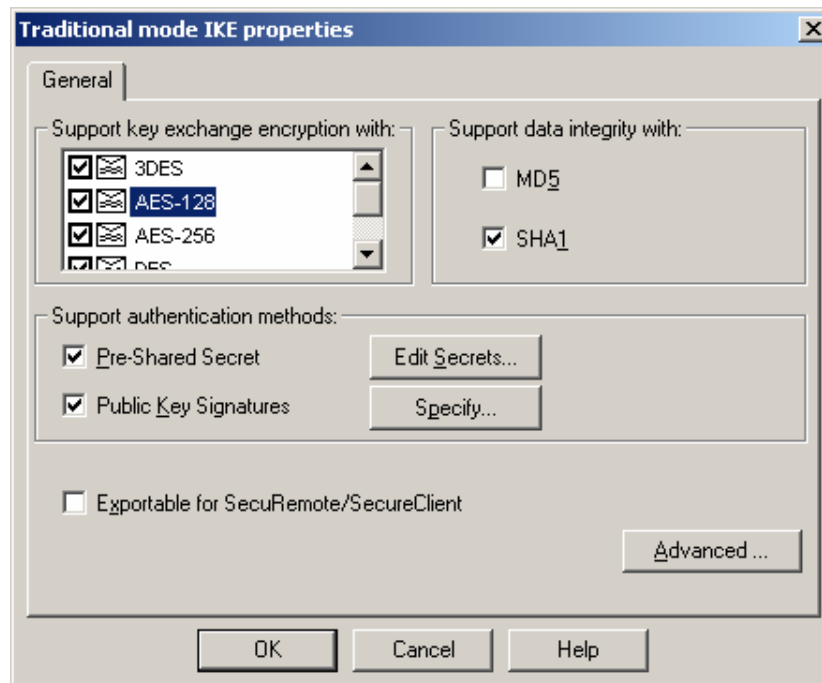


Figure 2 – Only FIPS-Approved Algorithms may be used with IKE

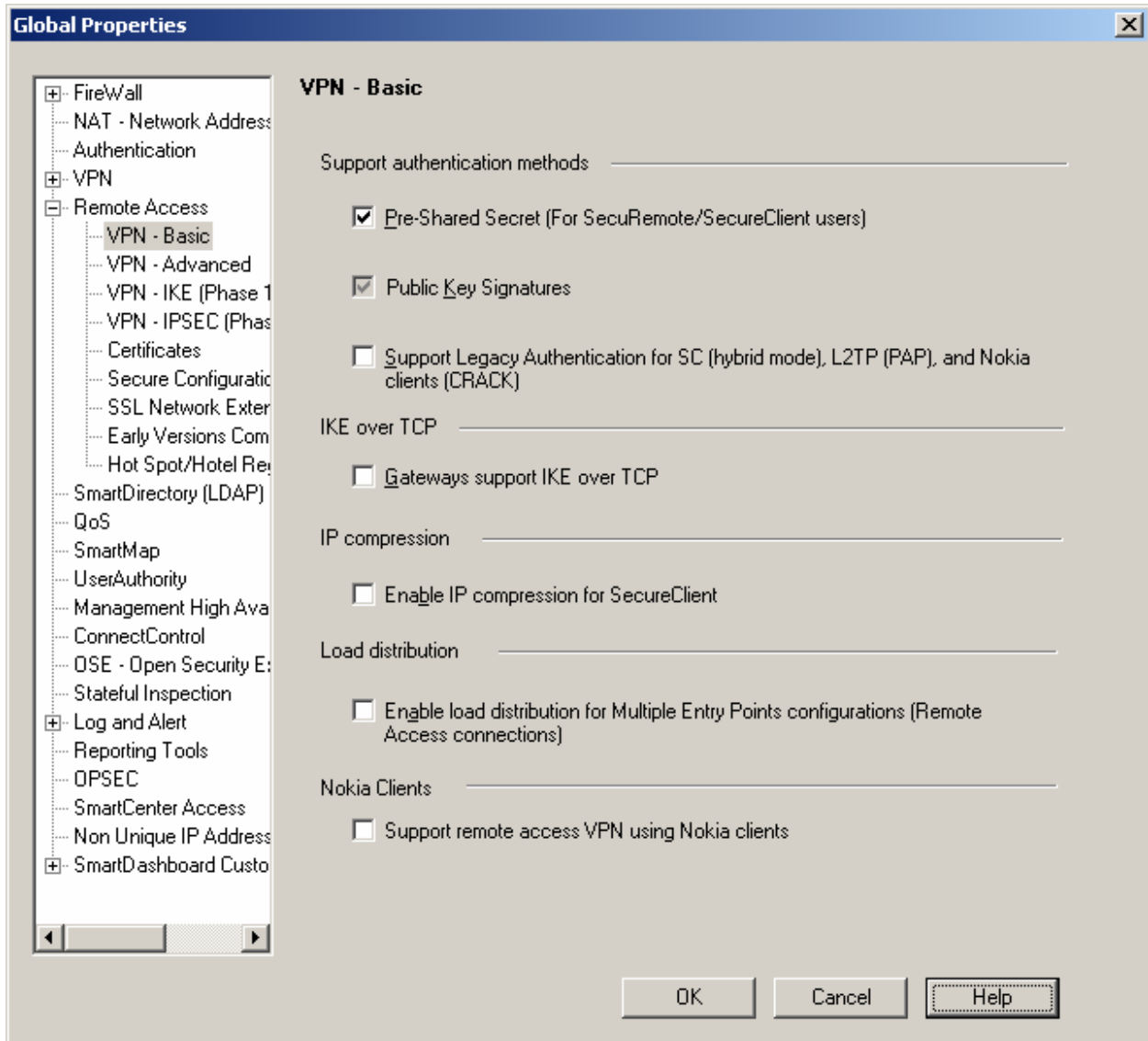


Figure 3 – Only Pre-Shared Keys or Digital Certificates may be used to Authenticate Clients

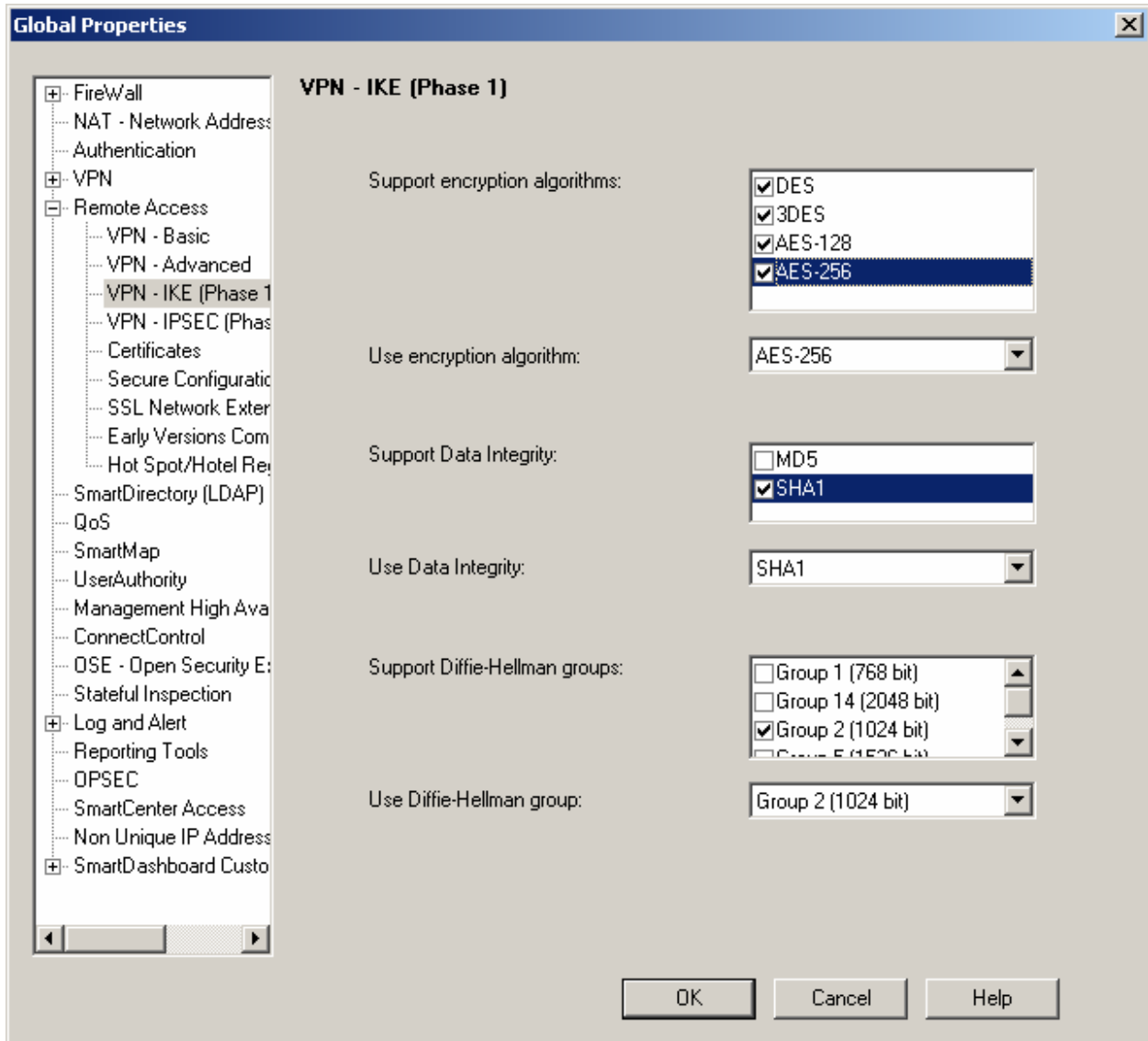


Figure 4 – Only FIPS-Approved Algorithms may be used with IKE

Notes:

1. DES (56 bit) will no longer be allowed in FIPS mode after May 19, 2007.
2. Diffie-Hellman Group 1 (768-bits) provides only 57 bits of encryption strength. After May 19, 2007, only Diffie-Hellman groups 2 or higher, providing 80 or more bits of encryption strength should be used.

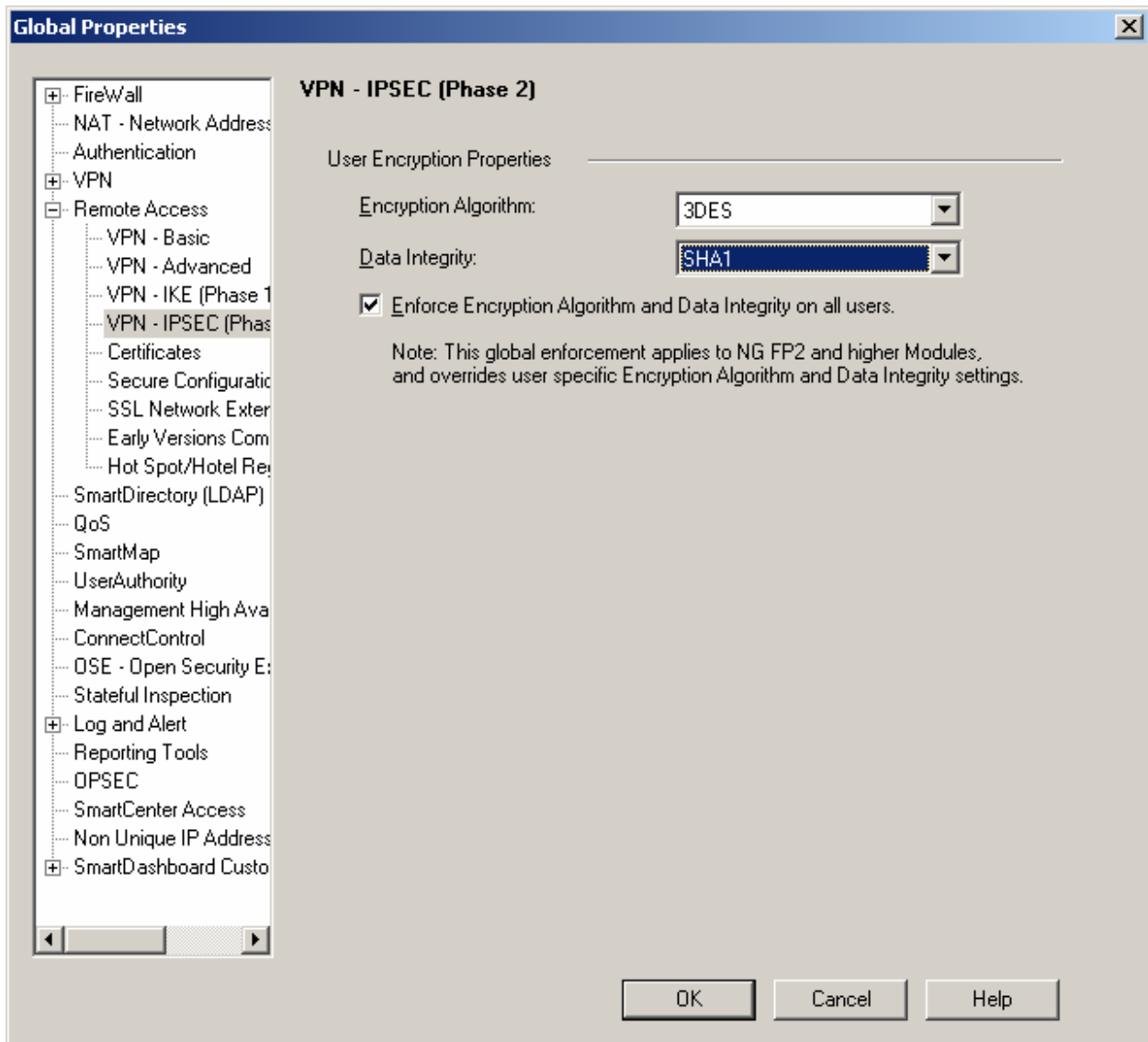


Figure 5 – Only FIPS-Approved Algorithms may be used with IPsec

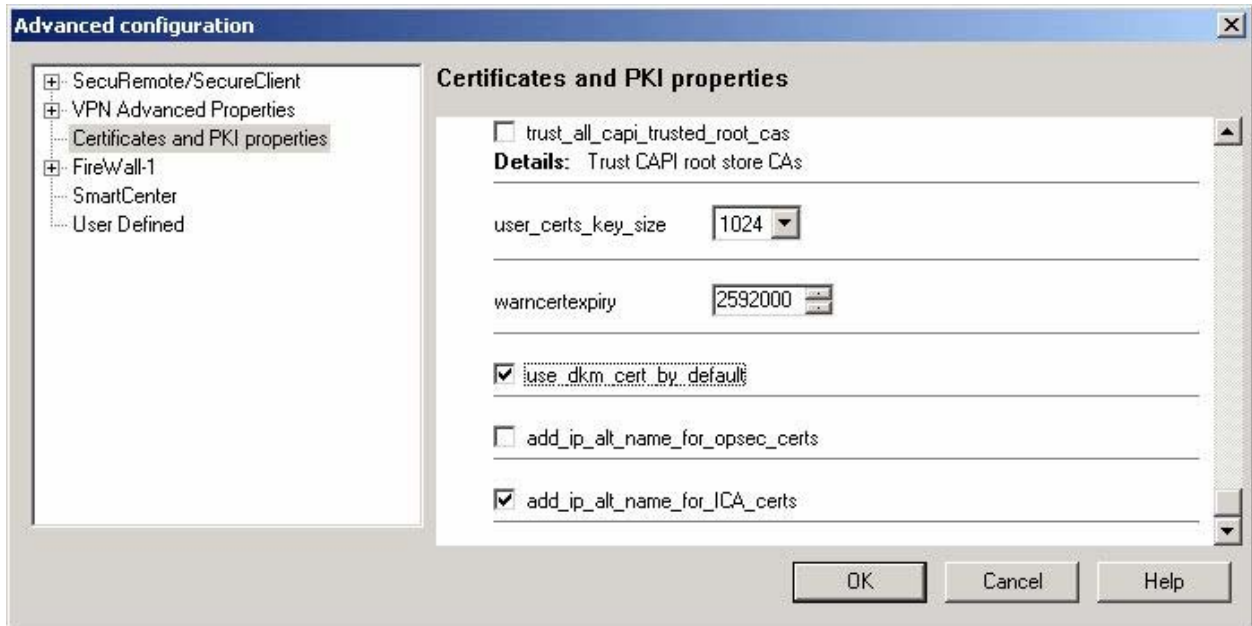


Figure 6 – Configuring the module to enable Distributed Key Management (DKM) globally

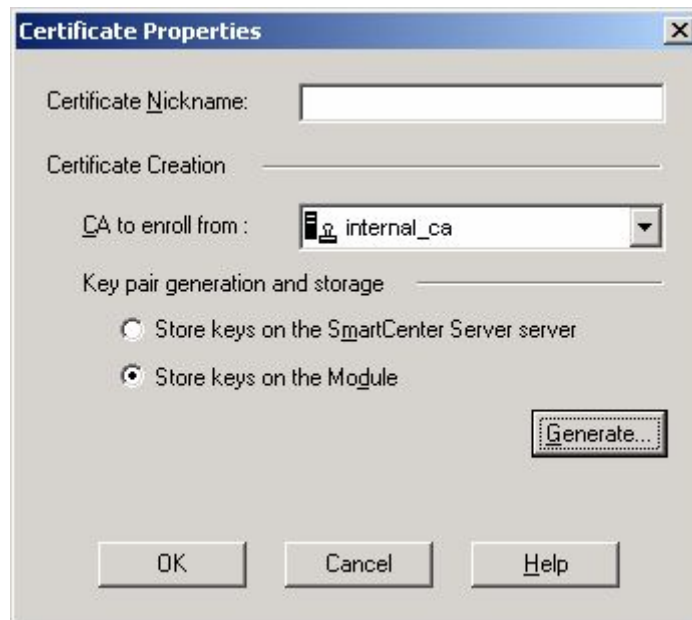


Figure 7 – Configuring the module to generate RSA keys with DKM on a per-certificate basis

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 NG user manuals.

The Crypto-Officer receives the module in a shrink wrapped package containing a CD-ROM with the VPN-1 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 should 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 should 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 firewall and 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 strange activity is found, the Crypto-Officer should take the module offline and investigate.

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

Termination

At the end of the life cycle of the module, the Crypto-Officer should reformat the hard drive containing the module's software. This will zeroize all keys and other CSPs.

User Guidance

The User access the module's VPN functionality as an IPSec client. Although outside the boundary of the module, the User should 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