Check Point

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Check Point IP Appliances

(formerly Nokia VPN Appliances)

FIPS 140-2 Cryptographic Module Security Policy
Level 2 Validation

Version 1.11
August 2011

IP1280

IP2450

IP2455

Module Hardware Versions:
    IP1280, IP2450 and IP2455

Firmware Version:
    Check Point VPN-1 NGX R65 with hot fix HFA 30 with IPSO v4.2

Table of Contents

1   INTRODUCTION

1.1   Purpose

This document is a nonproprietary Cryptographic Module Security Policy supporting the Check Point IP Appliance family that has been designed to meet the Reduction of Hazardous Material Standard (RoHS). This security policy describes the Check Point IP Appliance and describes how it meets the security requirements of FIPS 140-2. It also describes how to run the module in an Approved FIPS 140-2 mode of operation. This document was prepared as part of the FIPS 140-2 Level 2 validation of the module.

The modules covered in this Security Policy are the IP1280, IP2450 and IP2455. These modules implement the IPSO 4.2 operating system and the Check Point VPN -1 cryptographic module, version *NGX R65* with hot fix HFA 30 firmware.

The Check Point IP Appliance is referenced in this document as *IP security platform*, *security platform*, *platform*, and *the module*.

1.2   References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. The Check Point Web site (http://www.checkpoint.com/) contains information on the full line of products from Check Point.

2 CHECK POINT IP APPLIANCE

2.1 Overview

The Check Point IP Appliance is an IP security platform designed to provide a secure, reliable, and manageable integrated security solution for secure Internet communication and access control for networks. The security platform combines the security-hardened operating system, IPSO, with the market-leading Check Point VPN-1 firmware suite on a purpose-built security hardware platform. As a network device, the Check Point IP Appliance supports a comprehensive suite of IP-routing functions and protocols, including RIPv1/RIPv2, IGRP, OSPF and BGP4 for unicast traffic and DVMRP for multicast traffic.

Some highlighted security features of the Check Point IP Appliance are:

- Read/write and read-only access modes
- Screening of all incoming communications to ensure authorized user access
- SSH-secured remote management of the modules (IPSO)
- SSHv2 supported
- TLS-secured remote management of Check Point applications
- Secure VPN between subsystems
- Multiple layers of authentication required when accessing the remote management interface for IPSO

This Check Point IP Appliance is a rack mounted device that is differentiated from other Check Point IP Appliances through its internal CPU processors and performance level. The module is designed to efficiently support real-world, mixed traffic solutions. As a VPN platform, the module greatly accelerates the embedded Check Point VPN-1/FireWall-1 performance by using the Firewall Flows. VPN performance is enhanced through the use of internal hardware cryptographic acceleration. The following chart illustrates the performance of the module covered by this Security Policy:

Model	CPU Type	Firewall Speed	VPN Speed (AES)
IP1280	Quad Core Xeon	9.0 Gbps	2.0 Gbps
IP2450 and IP2455	(2) Quad Core Xeon	9.0 Gbps	2.0 Gbps

2.2 Cryptographic Module

The Check Point IP Appliance was tested as multi-chip standalone cryptographic module. The module's metal enclosure physically encloses the complete set of hardware and firmware components, including excluded components, and represents the cryptographic boundary of the module. The cryptographic module supports the following hardware versions:

- IP1280 – full width 2U rack mount
- IP2450 – full width 2U rack mount
- IP2455 – full width 2U rack mount

The Check Point IP Appliance runs the proprietary, security-hardened IPSO operating system along with a binary image of the Check Point VPN-1 cryptographic firmware for VPN and firewall functionalities.

The IP1280, IP2450 and IP2455 hardware chassis include support for Field Replaceable Unit (FRU) upgrades to internal network interface cards, hard drives, FLASH memory, and other components (e.g., fans and power supplies replaced with identical components). However, all FRU upgrades are performed by the factory or a reseller prior to delivery of the module to the end user. The end-user has no option to service or install these internal components. All FRU component slots are secured with tamper seals (see Section 3.1.1.1) for FIPS mode. The differences between the modules are that the IP1280 is single CPU, the IP2450 has dual CPUs and the IP2455 is the new chassis and model number for the IP2450.

The following hardware combination was used for the FIPS 140-2 validation testing covered by this Security Policy:

Model	Tested Configuration	Part Number of Cards	Type
IP1280	1 4-port ethernet pcm card; 1 blank pcm-faceplate; 2 hard-disks; 2 pcm carriers (w/ 2 blank faceplates each installed); 2 power-supplies FIPS KIT	CPAP-IP1285-D-GFIP (Nokia NBB1270000) CPIP-A-4-1C CPIP-A-D80G-CA CPIP-A-CA-12-24 N431174001 (12 pc)	system 4port Ethernet HDD FRU PMC Carrier Tamper-evident seal kit
IP2450	1 4-port ethernet pcm card; 1 blank pcm-faceplate; 1 hard-disks; 1 blank hd-faceplate; 2 pcm carriers (w/ 2 blank pcm-faceplates each); 2 power-supplies FIPS KIT	CPAP-IP2455-D-GFIP (Nokia NBB3450000) CPIP-A-4-1C CPIP-A-D80G-CA CPIP-A-CA-12-24 N431174001 (12 pc)	system 4port Ethernet HDD FRU PMC Carrier Tamper-evident seal kit

IP2455	1 4-port ethernet pcm card; 1 blank pcm-faceplate; 1 hard-disks; 1 blank hd-faceplate; 2 pcm carriers (w/ 2 blank pcm- faceplates each); 2 power-supplies FIPS KIT	CPAP-IP2455-D-GFIP CPIP-A-4-1C CPIP-A-D80G-CA CPIP-A-CA-12-24 N431174001 (12 pc)	system 4port Ethernet HDD FRU PMC Carrier Tamper-evident seal kit

Note: Alternative untested configurations were not validated and are not included in this certificate.

The IPSO OS and the module's physical hardware chassis and computing platform provide the operational environment upon which the Check Point VPN-1 application binary executes. The following firmware combination was used for the FIPS 140-2 validation testing covered by this Security Policy:

- **Check Point VPN-1 NGX R65 with hot fix HFA 30 with IPSO v4.2**

The cryptographic module implements a version of Check Point firmware that is certified with certificate number #1219. However, the IPSO operating system and IP Appliance hardware combination constitute different operational environments for the Check Point VPN-1 NGX R65 with hot fix 30 firmware; therefore the Check Point VPN-1 NGX R65 with hot fix HFA 30 module binary image was packaged into the Check Point IP Appliance configuration and was retested as part of the complete Check Point IP Appliance FIPS 140-2 solution.

FIPS Algorithm validation testing was performed and validation certificates obtained for all Approved cryptographic functions implemented by the module covering the hardware and firmware configuration listed in this document. This includes separate algorithm validations for algorithms implemented by IPSO, the Check Point VPN-1 firmware, and hardware accelerator chips. See Section 2.8 for a list of algorithms implemented. See Appendix B for a list of the Approved algorithm validation certificate numbers.

The module operates in both a non-Approved and Approved FIPS 140-2 mode of operation. Only approved cryptographic algorithms and security functions are allowed in the approved mode of operation. The module is intended to meet overall FIPS 140-2 Level 2 requirements. The following table presents the individual FIPS 140-2 compliance areas and the Security Levels to which the module was tested:

FIPS 140-2 DTR Section	Requirements Section Title	Level Tested
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

Table 1 – Intended Level Per FIPS 140-2

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.

2.3 Module Interfaces

The security platforms provide a number of physical ports:

	IP1280	IP2450	IP2455
10/100/1000 BaseTx, Ethernet Ports (standard)	0	0	0
Auxiliary Port (Disabled)	1	1	1
Console Port	1	1	1
I/O Option Slots (for adding Dual-port Gigabit Ethernet MMF, Dual-port SMF 1000Base-LX, Dual-port GigE Copper V2, Four-port 10/100 MBps Ethernet, 1000BaseT or 1000 Mbps fiber Ethernet, V.35, or X.21 protocol options)	4 2 – PMC Carrier slots (can each hold a card w/ 2 PMC Expansion slots) 2 – PMC Expansion slot (validated configuration is: 1 configured with a 4 port Ethernet card standard)	4 2 – PMC Carrier slots (can each hold a card w/ 2 PMC Expansion slots) 2 – PMC Expansion slot (validated configuration is: 1 configured with a 4 port Ethernet card standard)	4 2 – PMC Carrier slots (can each hold a card w/ 2 PMC Expansion slots) 2 – PMC Expansion slot (validated configuration is: 1 configured with a 4 port Ethernet card standard)
PCMCIA Slots	N/A	N/A	N/A
Power Switch	1 per Power Supply	1 per Power Supply	1 per Power Supply
Reset Switch	1	1	1
Power input	1 per Power Supply	1 per Power Supply	1 per Power Supply
Status LEDs			
Rear Power Indicator	Per Power Supply -- 1 power LED built into the removable fan and power supply (The power supply also has 1 power supply fault and 1 power supply overtemp LED).	Per Power Supply -- 1 power LED built into the removable fan and power supply (The power supply also has 1 power supply fault and 1 power supply overtemp LED).	Per Power Supply -- 1 power LED built into the removable fan and power supply (The power supply also has 1 power supply fault and 1 power supply overtemp LED).
Front Power Indicator	NOKIA (Logo illuminates)	NOKIA (Logo illuminates)	Check Point SOFTWARE TECHNOLOGIES LTD. (Logo illuminates)
Front Fault Indicator (see Table 3)	1	1	1
Ethernet Port status (green indicates connection, yellow blinking indicates data being transmitted)	depends on number of I/O option cards installed (1 LED per installed Ethernet port)	depends on number of I/O option cards installed (1 LED per installed Ethernet port)	depends on number of I/O option cards installed (1 LED per installed Ethernet port)

Hard Disk Drive status	2 HDD slots – (Each installed HDD has 1 status, 1 activity, and 1 hot swap LED)	2 HDD slots – (Each installed HDD has 1 status, 1 activity, and 1 hot swap LED)	2 HDD slots – (Each installed HDD has 1 status, 1 activity, and 1 hot swap LED)

Table 2 - FIPS 140-2 Physical Ports

Table 3 - Descriptions of the status LEDs

The physical ports are separated into logical interfaces defined by FIPS 140-2, as described in Table 4.

Module Physical Port	FIPS 140-2 Logical Interface
Network ports	Data input interface
Network ports	Data output interface
Network ports, console port, power switch, reset switch	Control input interface
Network ports, console port, LEDs	Status output interface
Power plug, Power switch	Power interface

Table 4 – FIPS 140-2 Logical Interfaces

Data input and output, control input, and status output are defined as follows:

- Data input and output are the packets that use the firewall, VPN, and routing functionalities of the module.

- Control input consists of manual control inputs for power and reset through the power and reset switch. It also consists of all of the data that is entered into the module while using the management interfaces.

- Status output consists of the status indicators displayed through the LEDs and the status data that is output from the module while using the management interfaces.

The module distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packets header information and contents.

2.4 Roles and Services

The modules support role-based authentication. The two roles in the module (as required by FIPS 140-2) that operators can assume are: a Crypto Officer role and a User role.

2.4.1 Crypto Officer Role

The Crypto Officer role can configure, manage, and monitor the module. Three management interfaces can be used for this purpose:

- CLI – the Crypto Officer can use the CLI to configure and monitor IPSO systems. There are two ways to access the Crypto Officer role through the CLI. Access can be provided for the Crypto Officer locally by using the console port or remotely by using the SSH secured management session.

- SNMP – the Crypto Officer can use SNMPv3 to view MIB values.

- SmartDashBoard – the Check Point TLS-secured management interface. The Crypto Officer can use this interface after the initial configuration of the Check Point module through the CLI. The TLS client RSA public key is used for authentication during TLS session establishment.

- The Crypto Officer can zeroize the module.

- The Crypto Officer can configure alternating bypass.

- Loading non-tested or non-approved code prior to invoking FIPS mode will invalidate the module.
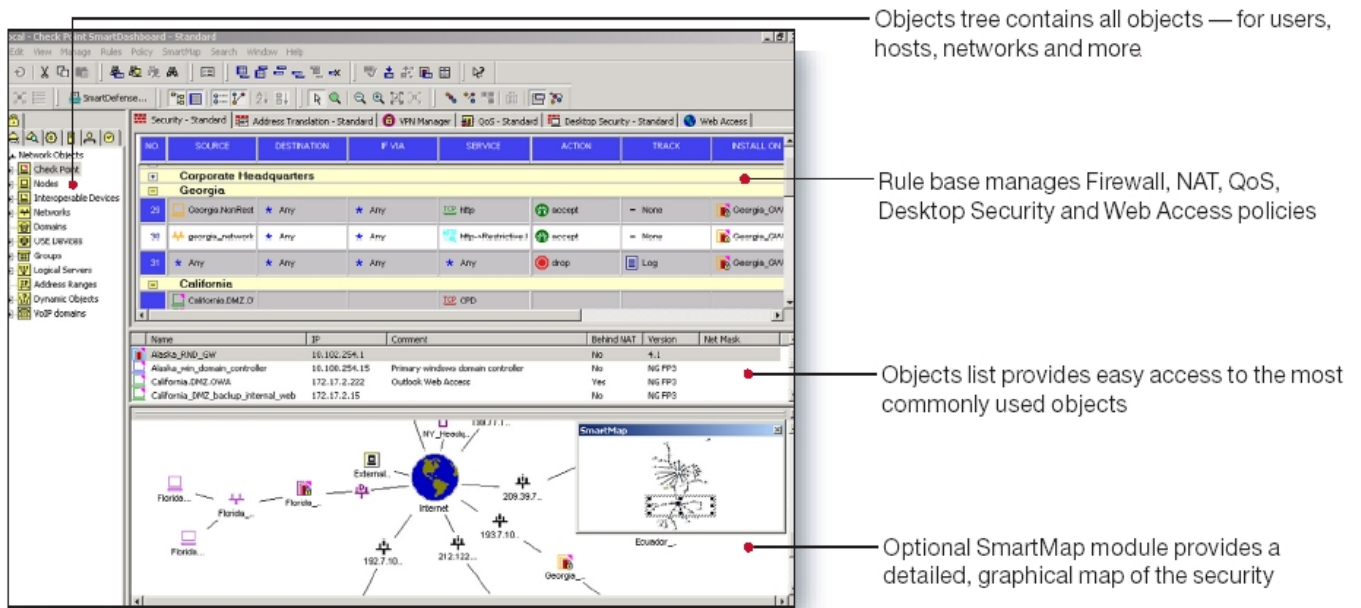
Figure 1 – Easy to Use Check Point Management Tools

Descriptions of the services available to the Crypto Officer role are provided in Table 5.

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
Startup configuration	Provide network connectivity and set a password for the admin account	Commands and configuration data(via local console)	Status of commands and configuration data	Admin password (read/write access)
Firmware loading (Disabled in FIPS mode) (Enabled when not in FIPS mode)	Provide for the loading of firmware	Commands and configuration data(via local console)	Status of commands and configuration data	Admin password (read/write access)
Power-up tests	Ability to run the integrity tests	Reboot of the module	Status of self tests and successful boot	

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
SSH	Provide authenticated and encrypted sessions while using the CLI	SSH key agreement (SSHv2) parameters, SSH inputs, and data	SSH outputs and data	RSA DSA host key pair (read access) ;RSA or DSA authorized key (read access); Diffie-Hellman key pair for SSHv2 key exchange (read/write access); session key for SSH (read/write access); X9.31 PRNG keys (read access)
TLS	Provide authenticated and encrypted sessions while using the Check Point management interface	TLS handshake parameters, TLS inputs, and data	TLS outputs and data	RSA key pair for TLS key transport (read access); session keys for TLS (read/write access); X9.31 PRNG keys (read access)
Boot manager commands	Control the boot-up process and obtain system information	Commands and configuration data	Status of commands and configur-ation data	Password (read/write access)
SNMPv3 Get commands	View MIB values	Commands	Status of commands, configuration data	Password (read access) The password itself is read-write while the v3 service is read access

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
Interface commands	Configure, manage, and view physical and logical interfaces through the CLI: view all interfaces; delete any logical interface; view IPsec VPN tunnels; view status and statistics; configure ARP behavior, physical and logical ATM interfaces, physical and logical Ethernet interfaces, physical and logical FDDI interfaces, physical and logical ISDN interfaces, physical or logical loopback interfaces, and physical and logical serial interfaces	Commands and configuration data	Status of commands and configuration data	None
Routing commands	Configure, manage, and view the routing protocols through the CLI: configure, manage, and view BGB BGP, OSPF, RIP, IGRP, IGMP, PIM, route aggregation, BOOTP, DVMRP, static routes,, ICMP router discovery, IP broadcast helper, Network Time Protocol, and dial on demand routing; configure a variety of miscellaneous options that affect routing; configure trace routing settings; view summary information about routes on the system; view general information that the IPSO routing daemon records; view information about multicast forwarding cache	Commands and configuration data	Status of commands and configuration data	None

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
Network Security and Access commands	Configure, manage, and view the security and access features through the CLI: configure and view network access; add firmware licenses to the platform; configure Authentication, Authorization, and Accounting (AAA); enable and disable and configure SSH services; add and delete new system users; create and delete groups, and add and remove members; enable and disable a VPN accelerator card; display VPN accelerator status or statistics	Commands and configuration data	Status of commands and configuration data	Admin, monitor, user passwords; shared secret for RADIUS; shared secret for TACPLUS; SSH host keys; SSH authorized keys; Read/write access for all CSPs
Traffic management commands	Configure, manage, and view traffic management functionality through the CLI: configure an access list to control the traffic from one or more interfaces; create or delete existing aggregation classes and modify the mean rate or burst size; configure depth of queues, assign logical names to some of the queues, and set up a queue specifier; add, delete, or show ATM QoS descriptors; add, delete, or show association of ATM QoS descriptors with ATM VCs; show available or reserved bandwidth on an ATM interface; enable and disable DSCP to VLAN mapping	Commands and configuration data	Status of commands and configuration data	None

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
System configuration commands	Configure, manage, and view system configuration settings through the CLI: view the platform configuration; configure the system to perform regularly scheduled backups (manual backups not allowed in FIPS mode); schedule regular jobs; configure system failure; configure domain name and domain name servers; configure static host names for particular IP addresses; configure host name of platform; manage IPSO images; manage configuration sets; manage relay configuration; configure network system logging; configure the date and time; view date and time settings; view the disks that IPSO detects on local system; specify other systems as network time protocol servers or peers; display information about packages installed on the local system	Commands and configuration data	Status of commands and configuration data	None
SNMP commands	Configure, manage, and view SNMP settings through the CLI: configure SNMP parameters; enable and disable SNMP; add users who are authorized to use SNMPv3; show SNMP implementation commands; show SNMPv3 user commands	Commands and configuration data	Status of commands and configuration data	Password (read/write access)

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
IPv6 commands	Configure, manage, and view IPv6 settings through the CLI: show a summary of IPv6 configuration; associate and disassociate an IPv6 address with a logical interface, anycast address, or IPv6 address family; map an IPv6 address to a physical machine address recognized in the local network; create IPsec VPN tunnels by using specific encapsulation schemes; configure and delete an IPv6 interface to IPv4 interface; create, enable, or disable an IPv6 interface attached to an IPv4 network that does not have IPv6 native support; configure IPv6 routing; add and delete logical IPv6 hosts; enable and disable network access and view current status of network access	Commands and configuration data	Status of commands and configuration data	None (the use of IPv6 tunneling* is independent of encryption. The IKE service handles any encryption for a route) *encapsulating IPv6 packets into IPv4 packets for transmission across networks that are not IPv6 aware
Monitoring commands	Configure, manage, and view monitoring settings through the CLI: configure CPU utilization reports, memory utilization reports, interface linkstate reports, rate shaping bandwidth reports, interface throughput reports by turning data collection on or off and setting the data collection time interval; display interface settings, system logs, system statistics, interface monitor, resource statistics, forwarding table, system status information	Commands and configuration data	Status of commands, configuration data, and status information	None

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
Check Point's CLI commands	Initial configuration of the Check Point firmware: install licenses, configure the SNMP daemon, modify the list of UNIX groups authorized to run VPN-1 services, register a cryptographic token, configure the one-time SIC password, and specify whether the VPN-1 services should automatically start at boot time	Command (cpconfig), menu options, and configuration information	Status of commands and menu options and status information (configuration information)	One-time SIC password (read/write access)
Check Point SmartDashBoard services	Create and configure users and user groups: define users and user groups; 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
	Define and implement security policies: 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.	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 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)

Service	Description	Input	Output	Critical Security Parameter (CSP) Access
	Zeroization of keys: overwrite or delete the secret and private keys used by the module	Commands and configuration data (SIC policy files)	Status of commands and configuration data (policy files)	All CSPs (write access)
	Initialization of Secure Internal Communication (SIC): establish trust between management server and the module to allow configuration of the module's services	Commands and configuration data (SIC policy)	Status of commands	RSA key pair for TLS (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 5 – Crypto Officer Services, Descriptions, Inputs, and Outputs

2.4.2 User Role

The User role accesses the module IPSec and IKE services. Service descriptions, inputs, and outputs are listed in Table 6.

Service	Description	Input	Output	CSP
IKE	Access the module IKE functionality 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 6 – User Services, Descriptions, Inputs and Outputs

2.4.3   Authentication Mechanisms

The modules implement password-based authentication (console and SSH), RSA-based authentication (TLS, IKE and SSH), DSA-based authentication (SSH). HMAC SHA-1 is used for data packet integrity during authentication functions (IKE with pre-shared keys).

2.4.3.1   Crypto Officer Authentication

The Crypto Officer must successfully authenticate before a management interface can be accessed. The authentication methods are described below.

- CLI (local) – the Crypto Officer must authenticate by using user ID and password. The password must be at least six characters long. Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used. The local interface is also used to establish the keys necessary for authentication when using the two alternate methods of communication to perform. Before the alternate methods can be used key pairs are generated outside the module and then the public key is loaded by the Crypto Officer after local authentication. The SSH session requires that the client Diffie-Hellman public key is loaded into the module. For TLS the client RSA public key is loaded.

- CLI (remote) – for this authentication method, an RSA or DSA key pair is first generated at the client. The Authorized RSA or DSA public key associated with the key pair is then output from the client to be entered into the module. Before starting an SSH session, the Crypto Officer must login to the module locally at initialization through the console CLI and enter the Authorized RSA or DSA public key generated at the client. The Crypto Officer can now successfully authenticate during the SSH session establishment using the private key. Once a session is established, the Crypto Officer can also be asked to authenticate again by using the user ID and password before the management interface can finally be accessed.

- SNMP – the Crypto Officer must authenticate by using the user ID and password. It is the same password used to access the CLI. The only restriction is that the password must be at least eight characters long.

- SmartDashBoard (Check Point Management Station) – A the TLS session is established between the Check Point management station and the VPN Appliance, the Crypto Officer must authenticate with his private key against his pre-loaded digital

certificate issued by a trusted Certification Authority (CA). A TLS RSA key pair is used for authentication during TLS session establishment.

2.4.3.2 User Authentication

User authentication to the module is performed during IKE using digital certificates or pre-shared secret keys. The pre-shared keys must be at least six characters long and use at least four different characters.

2.4.3.3 Estimated Strength of the Authentication Mechanisms

The estimated strength of each authentication mechanism implemented by the module is described in Table 7.

Authentication Type	One-Time Strength	Multiple Attempts Strength
DSA-based authentication (SSHv2)	DSA signing and verification is used to authenticate the module during SSHv2. This mechanism is as strong as the DSA algorithm using a 1024 bit key pair and provides 80 bits of equivalent security.	1500 attempts per minute possible, resulting in a less than 1 in $8.05*10^{20}$ chance per minute
RSA-based authentication (SSHv2 and TLS handshake)	RSA encryption and decryption is used to authenticate the module during SSHv2, and the TLS handshake. TLS supports using a key pair of either 1024, 2048 and 4096 bits, SSHv2 supports a key pair of 1024 bits. Using a 1024 bit key pair provides 80 bits of equivalent security.	1500 attempts per minute possible, resulting in a less than 1 in $8.05*10^{20}$ chance per minute
RSA-based authentication (IKE)	RSA signing and verification is used to authenticate to the module during IKE. This mechanism is as strong as the RSA algorithm using a key pair of 1024, 2048 and 4096 bits. Using a 1024 bit key pair provides 80 bits of equivalent security.	Less than 2 attempts per minute possible, resulting in a less than 1 in $6.04*10^{23}$ chance per minute
Pre-shared key-based authentication (IKE)	Pre-shared keys must be at least six characters long and use at least four different characters. Even if only uppercase letters were used without repetition for a six character pre-shared key, the probability of randomly guessing the correct sequence is one in 165,765,600. HMAC SHA-1 verification is used for additional data packet integrity during IKE negotiations with pre-shared keys.	Less than 2 attempts per minute possible, resulting in a less than 1 in 82,882,800 chance per minute
Password-based authentication	Passwords are required to be between 6 and 128 characters long (SNMPv3 requires at least eight characters). Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used, which gives a total of 95 characters to choose from. Considering only the minimum password length with a case-insensitive alphabet using a password with repetition, the number of potential passwords is 26^6.	Less than 36 attempts per minute possible, resulting in a less than 1 in 8,580,993 chance per minute

Table 7 – Estimated Strength of Authentication Mechanisms

2.5 Electromechanical Interference/Compatibility (FCC Compliance)

The module hardware configuration was tested and found compliant with requirements for a Class A digital device, pursuant to Part 15 of the FCC rules and thus the FIPS 140-2 Level 2 EMI/EMC requirements.

2.6 Physical Security

The Check Point IP Appliance is multi-chip, standalone cryptographic module. The module is entirely contained within its respective hard metal enclosure. The enclosure is resistant to probing and is opaque within the visible spectrum. The FIPS hardware configuration of the module includes factory-installed lance baffle inserts to protect the front and side vent holes of the enclosure from direct viewing or probing of the module's interior components. Rear vent holes are likewise obscured by internal fan or power supply components.

Serially numbered tamper-evident seals provide additional protection to those parts of the module chassis that can be opened or disassembled. The seals provide indications of attempts to tamper with the module. The tamper-evident seals are affixed to the module by the Crypto Officer in numbers and locations that vary depending on the module hardware version. Specific quantities and locations are described in Section 3.1 "Crypto Officer Guidance" of this document.

After applying the tamper-evident seals the customer must maintain physical security by inspecting labels & enclosure for signs of tampering according to a predefined inspection schedule. It is recommended that this inspection be performed at least once per month.
The FIPS approved state is only maintained as long as the Tamper Evident seals are maintained.

2.7 Operational Environment

The FIPS 140-2 operational environment requirements do not apply to this module. The Check Point IP Appliance does not provide a general-purpose operating system nor does it provide a mechanism to load software. The module operator interacts with the module through customized interfaces that provide only specific command options.

2.8 Cryptographic Key Management

Cryptographic algorithms are implemented in firmware by IPSO and Check Point VPN-1 and in hardware by the encryption accelerators.

The IPSO operating system provides the capability to use SSHv2 to secure the remote CLI management sessions. The implemented FIPS-approved algorithms include RSA and DSA (SSHv2) for authentication, Triple-DES for data encryption, SHA-1 for data hashing, and HMAC SHA-1 for data packet integrity. Key establishment is performed by using the Diffie-Hellman key agreement for SSHv2.

Check Point provides the capability to use TLSv1 to secure management sessions. The implemented FIPS-approved algorithms include RSA for authentication; Triple-DES[1], and AES for data encryption; SHA-1 for data hashing; and HMAC SHA-1 for data packet integrity. Key establishment is performed by using RSA key wrapping. The embedded Check Point application supports IPSec/ESP for data encryption and IPSec/AH for data integrity. The Check Point module implements all IKE modes: main, aggressive, and quick, using ISAKMP according to the standard. IKE uses RSA signatures or pre-shared keys for authentication. Key establishment in IKE is performed by using the Diffie-Hellman key agreement technique.

Enhanced VPN performance is achieved by accelerating DES, AES, Triple-DES, and Diffie-Hellman modular exponentiation processing implemented by the Check Point firmware. Hardware acceleration is accomplished either by hard-wired accelerator chips or by optional version-specific internal accelerator cards that are installed by the factory or reseller prior to delivery to the end-user. The IP1280, IP2450 and IP2455 use an accelerator card. Accelerated DES and Triple DES Keying Option 3 is non-compliant (Keying Option 3 uses one key 3 times). Only the FIPS approved Triple-DES and AES encryption algorithms shall be used.

Accelerator chips differ only in performance. The module operating system automatically senses the accelerator chip at power on and performs power on self tests on all the functions provided by the appropriate accelerator chip as well as self-tests for all firmware-based cryptographic functions.

To summarize, the modules implement the following FIPS-approved and non FIPS-approved algorithms (see Appendix B – *Algorithm Validation Certificate* Numbers for the algorithm certificate numbers of the validated FIPS-approved algorithms):

---

[1] DES and Keying Option 3 (K3 mode) `are non-compliant. Only the FIPS approved Triple-DES and AES encryption algorithms should be used to remain in the FIPS Approved mode.

Non FIPS-Approved

Data encryption:

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

- Triple DES (TDES), Keying Option 3 (K3 mode): Triple- DES Keying Option 3 is non-compliant (Keying Option 3 uses one key 3 times) – according NIST FIPS PUB 46-3 (withdrawn) and NIST Special Publication 800-67.

- CAST - Disabled

- DES (40 bits) - Disabled

- Arcfour - Disabled

- Twofish - Disabled

- Blowfish - Disabled

Data packet integrity:

- HMAC MD5 - Disabled

Data hashing:

- MD5 - Disabled

Digital signatures:

- DSA (Public key sizes under 1024-bits, private key sizes under 160-bits)

Digital signatures and Key transport:

- RSA (Key sizes under 1024-bits)

Key agreement / Key establishment:

- Diffie-Hellman (Public key sizes under 1024-bits, private key sizes under 160-bits)

Pseudo-Random Number Generation:

This module implements the following non-Approved PRNGs, which are not used for cryptographic purposes. These two PRNGs are used by the underlying operating system and have been excluded from the testing requirements as they are non-security relevant:

- ARC4-based PRNG (used to create "unpredictable" sequence numbers)

- Simple Linear Congruential PRNG (used for random head/tail packet discard and salt generation)

FIPS-Approved

Data encryption:

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

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

Only the FIPS-approved Triple DES and AES encryption algorithms are to be used in FIPS mode. DES and Triple DES keying option 3 are not FIPS-approved algorithms and should not be used in FIPS mode.

Data packet integrity:

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

Data hashing:

- Secure Hash Algorithm (SHA-1) – according to NIST FIPS PUB 180-1

Digital signature:

- Digital Signature Algorithm (DSA) – according to NIST FIPS PUB 186-2 with Change Notice 1

Digital signatures and Key transport:

- RSA – all digital signature implementations are according to PKCS #1

The RSA key wrapping methodologies provide the following encryption strengths during key transport:

- TLS: provides 80 – 150 bits of encryption strength.

Only methodologies providing a minimum of 80 bits of encryption strength are allowed in FIPS mode. Encryption strength is determined in accordance with FIPS 140-2 Implementation Guidance 7.5 and NIST Special Publication 800-57 (Part 1).

Key agreement / Key establishment:

- The Diffie-Hellman key agreement key establishment methodology used by the different firmware implementations present in the module (used for IKE and SSHv2) provides the following encryption strengths:

  IPSO: Only DH Groups 2 through 14 shall be used be used to provide between 80 and 112 bits of encryption strength..

  o **Check Point VPN-1 NGX R65 with hot fix HFA 30**: In FIPS mode the Diffie-Hellman key agreement methodology implemented by the module (used by IKE) provides between 80 and 128 bits of encryption strength (DH Groups 2 through 18 shall be used). Check Point recommends only DH Groups 14 to 18 should be used, providing between 112 and 128 bits of encryption strength.

- Only methodologies providing a minimum of 80 bits of encryption strength are allowed in FIPS mode. Encryption strength is determined in accordance with FIPS 140-2 Implementation Guidance 7.5 and NIST Special Publication 800-57 (Part 1).

Pseudo-Random Number Generation:

- ANSI X9.31 PRNG

The module implements the following protocols permitted for use in a FIPS-approved mode of operation:

Session security:

- SSHv2 (configured to use FIPS-approved algorithms)

- TLS v1.0 (configured to use FIPS-approved algorithms) according to RFC 2246

- IPSec (configured to use FIPS-approved algorithms)

The module supports the following critical security parameters (Table 8):

CSPs	CSPs type	Generation	Storage	Use
Host RSA v2 key pair (via IPSO) [**See footnote 1 below table.**]	512-, 640-, 768- (default), 864-, 1024-bit private and public key pair	Internal – using X9.31 PRNG	Stored in plaintext on disk	SSH server authentication (SSHv2)
Host DSA key pair (via IPSO)	160-bit DSA private key and 1024-bit DSA public key	Internal – using X9.31 PRNG	Stored in plaintext on disk	SSH server authentication to client (SSHv2)
Authorized RSA v2 key (via IPSO)	1024-bit RSA public key	External	Stored in plaintext on disk	Client authentication to SSH server (SSH v2)
Authorized DSA key (via IPSO)	1024-bit DSA public key	External	Stored in plaintext on disk	Client authentication to SSH server (SSHv2)
TLS RSA key pair (via Check Point VPN-1)	1024, 2048, or 4096-bit RSA private and public key pair	External	Stored in plaintext on disk	TLS server authentication and key transport during TLS handshake
TLS client RSA public key (via Check Point VPN-1)	1024, 2048, or 4096-bit RSA public key	External	Stored in plaintext on disk	Client authentication during TLS handshake
IKE RSA key pair (via Check Point VPN-1)	1024, 2048, or 4096-bit RSA private and public key pair	External	Stored in plaintext on disk	Server authentication during IKE
IKE client RSA public key (via Check Point VPN-1)	1024, 2048, or 4096-bit RSA public key	External	Stored in plaintext on disk	Client authentication during IKE
Pre-shared keys (passwords) (via Check Point VPN-1)	6-character pre-shared key	External	Stored in plaintext on disk	Client and server authentication during IKE

CSPs	CSPs type	Generation	Storage	Use
IKE Diffie-Hellman key pair (via Check Point VPN-1) [**See footnote 2 below table.**]	Diffie-Hellman (**160** to **256**-bit) private/(**1024** to **8192** bit) public key pair Less than 1024-bit public is non-Approved	External	Stored in plaintext in memory	Key agreement during IKE
IKE client Diffie-Hellman public key (via Check Point VPN-1) [**See footnote 2 below table.**]	Diffie-Hellman **1024** to **8192**-bit public key Less than 1024-bit public is non-Approved	External	Stored in plaintext in memory	Key agreement during IKE
SSHv2 Diffie-Hellman key pair (via IPSO) [**See footnote 2 below table.**]	Diffie-Hellman (**320** to **384**-bit) private/(**1024** to **2048**-bit) public key pair Less than 1024-bit public is non-Approved	Internal – using X9.31 PRNG	Stored in plaintext in memory	Key agreement during SSHv2
SSHv2 client Diffie-Hellman public key (via IPSO) [**See footnote 2 below table.**]	Diffie-Hellman **1024** to **2048**-bit public key Less than 1024-bit is non-Approved	External	Stored in plaintext in memory	Key agreement during SSHv2
SSH session keys (via IPSO)	168-bit Triple-DES keys; HMAC SHA-1 keys	Established during the SSH key exchange using Diffie-Hellman key agreement (SSHv2)	Stored in plaintext in memory	Secure SSH traffic
TLS session keys (via Check Point VPN-1)	56-bit DES or 168-bit Triple-DES keys; HMAC SHA-1 key	Established during the TLS handshake using RSA key transport	Cached to disk	Secure TLS traffic
IPSec session keys (via Check Point VPN-1) [**See footnote 3 below table.**]	56-bit DES, 128-bit Triple-DES, or 128-, 256-bit AES keys; HMAC SHA-1 key	Established during the Diffie-Hellman key agreement	Stored in plaintext in memory	Secure IPSec traffic

CSPs	CSPs type	Generation	Storage	Use
IPSO X9.31 PRNG keys (via IPSO)	128-bit Triple-DES keys	Internal from random entropy pool	Stored in plaintext in memory	IPSO pseudo-random number generator for RSA, DSA, and Diffie-Hellman keys
IPSO X9.31 PRNG seed values (via IPSO)	64-bit seed values	Internal – by gathering entropy	Stored in plaintext in memory	IPSO pseudo-random number generator input
Check Point X9.31 PRNG keys (via Check Point VPN-1)	128-bit Triple-DES keys	Internal – by gathering entropy	Stored in plaintext in memory, but entropy used to generate keys is cached to disk	Check Point pseudo-random number generator for Diffie-Hellman keys
Check Point X9.31 PRNG seed values (via Check Point VPN-1)	64-bit seed values	Internal from random entropy pool	Stored in plaintext in memory	Check Point pseudo-random number generator input
Passwords (via IPSO)	Six-character password (SNMPv3 requires at least eight characters)	External	Stored in plaintext on disk	Authentication for accessing the management interfaces (CLI and SNMPv3); boot manager authentication; RADIUS authentication; TACPLUS authentication

Table 8 – Listing CSPs for the Module

Note:
1. Only 1024-bit keys, or higher, should be used for RSA in FIPS mode. 1024-bit RSA keys provide 80-bit equivalent security as calculated by IG7.5.
2. When in FIPS mode only Diffie-Hellman Group 2 through 18 shall be used. This provides between of 80 and 128 bits of encryption strength as calculated by IG7.5. Check Point recommends only DH Groups 14 to 18 should be used, providing between 112 and 128 bits of encryption strength.
3. TLS is used for SIC
4. DES must not be used in FIPS mode.

2.8.1 Key Generation

The only keys that can be generated by the modules are RSA public and private keys and DSA public and private keys for SSHv2. The FIPS-approved X9.31 PRNG is used to generate these keys.

2.8.2 Key Establishment

The modules implement IKE, SSH, and the TLS handshake for automatic key establishment. Two types of key establishment techniques are employed by the modules: the Diffie-Hellman key agreement and the RSA key wrapping. The Diffie-Hellman key agreement establishes shared secrets during SSHv2 and IKE. The RSA key wrapping/key transport generates shared secrets during TLS.

2.8.3 Key Entry and Output

All private and secret keys entered into the module are electronically entered and encrypted during RSA key transport or during a Diffie-Hellman key agreement using derived TDES session keys. No private or secret keys are output from the module.

2.8.4 Key Storage

All RSA and DSA keys, pre-shared keys, and passwords are stored in plaintext on disk. The TLS session keys and the gathered entropy for the Check Point PRNG keys are cached to disk. All other keys are ephemeral keys and are stored in plaintext in memory.

2.8.5 Key Zeroization

Ephemeral keys can be zeroized by rebooting. All other keys can be zeroized by the Crypto Officer by overwriting or deleting them.

2.9 Self-Tests

The module performs a set of self-tests 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). Self tests are performed by both IPSO and the Check Point VPN-1 firmware components as appropriate. IPSO also implements self tests on the algorithms provided by the hardware encryption accelerator chips. All module versions were functionally tested during FIPS 140-2 conformance testing.

Power-up Self-tests:

- Integrity tests: the module uses a CRC-32 to check the integrity of its various firmware components, including verifying the integrity of the Check Point VPN-1 binary code.

- Cryptographic algorithm tests:

    o AES-CBC KAT

    o DES-CBC KAT

    o Triple-DES-CBC KAT

    o ANSI X9.31 PRNG KAT

    o RSA sign/verify and encrypt/decrypt KAT

    o DSA sign/verify pair-wise consistency test

    o SHA-1 KAT

    o HMAC SHA-1 KAT

- Policy file integrity test (bypass mode test): the module performs a SHA-1 check value verification to ensure that the policy files are not modified.

Conditional Self-tests:

- RSA pair-wise consistency test: this test is performed when RSA keys are generated for SSHv2.

- DSA pair-wise consistency test: this test is performed when DSA keys are generated for SSHv2.

- Continuous random number generator tests: these tests are constantly run to detect failure of the random number generators of the module.

- Policy file integrity test (bypass mode test): the module performs a SHA-1 check value verification to ensure that the policy files are not modified.

Self Test Error Handling

- If the integrity tests fail, the module enters the bootloader error state and reboots. If the IPSO kernel modules cryptographic algorithm tests fail, the module enters the kernel panic error state and reboots. If the Check Point kernel module cryptographic algorithm tests fail, the module enters the kernel panic error state and must be rebooted by the Crypto Officer to clear the error.

- If the IPSO conditional self-tests fail, the module enters the error state and reboots. If the Check Point continuous RNG test fails, the module enters the error state and reboots. All other self-test errors cause the module to enter the error state, where 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.

All errors are logged and produce error indicators.

2.10 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.

The Check Point IP module hardware data, which includes descriptions, parts data, part types, bills of materials, manufacturers, changes, history, and hardware documentation are managed and recorded using Agile Workplace.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 and Microsoft SharePoint was used to provide configuration management for the module's FIPS documentation. These document management utilities provide access control, versioning, and logging.

The Crypto module is implemented in a high level language.

2.11 Mitigation of Other Attacks

The module does not employ security mechanisms to mitigate specific attacks.

3   SECURE OPERATION (APPROVED MODE)

The Check Point IP Appliance meets Level 2 requirements for FIPS 140-2. The following subsections describe how to place and keep the module in FIPS-approved mode of operation. The Crypto Officer must ensure that the module is kept in a FIPS-approved mode of operation. The procedures are described in "Crypto Officer Guidance". The tamper evident seals shall be installed, as specified in 3.1.1.1, for the module to operate in a FIPS Approved mode of operation.

The User can use the module after the Crypto Officer changes the mode of operation to FIPS-Approved. The secure operation for the User is described in Section 3.2, "User Guidance".

3.1   Crypto Officer Guidance

The secure operation procedures include the initial setup, configuring the Check Point module in a FIPS compliant manner, and keeping the module in a FIPS-approved mode of operation. These procedures are described in the following sections.

To determine if the module is in the alternating bypass state, the crypto officer can examine the VPN rule table. If at least one connection is configured without encryption then the module is in the alternating bypass state. If all connections are configured with encryption the module is not in the alternating bypass state.

3.1.1   Hardware Setup

The Crypto Officer receives the module in a carton. Within the carton the module is placed inside a sealed ESD bag to show tamper evidence during delivery; two foam end caps are placed on both sides of the chassis, protecting the module during shipping. The Crypto Officer should examine the carton and the ESD bag for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

Since the module does not enforce an access control mechanism before it is initialized, the Crypto Officer must maintain control of the module at all times until the initial setup is complete.

Before turning on the module, the Crypto Officer must ensure that the module meets Level 2 physical security requirements. To satisfy these requirements, the Crypto Officer must install one or more tamper-evident seals (also called "FIPS Tape") provided in the module's FIPS kit. Eight (8) seals should be applied to the IP1280, IP2450 and IP2455 modules.

- N431174001 (12 pc) – Tamper-evident seal kit

After the seal(s) are in place, the Crypto Officer must initialize the module and set the module to FIPS mode.

3.1.1.1 Applying the Tamper-Evident Seal(s)

Tamper seals are required to provide tamper evidence for the module chassis. Eight (8) seals should be applied to the IP1280, IP2450 and IP2455 modules. The tamper-evident seals each contain a unique serial number which aids the Crypto Officer in determining whether the original labels have been replaced. Refer to Section 2.2 for the module hardware version and its respective chassis type.

To apply the serialized seal

1. Assure surface where tamper-evident seal is to be applied is clean by wiping with a dry cloth

2. Apply one tamper seal to the module chassis at the front, top; four on the front of the module; and three to the rear of the module as indicated in the figures below.

3. Record the serial number of the applied seal(s) in a security log.

4. Allow 24 hours for the adhesive in the tamper-evident seal(s) to completely cure.

5. The Crypto Office is responsible for control at all times for any unused seals, and the direct control and observation of any changes to the module.
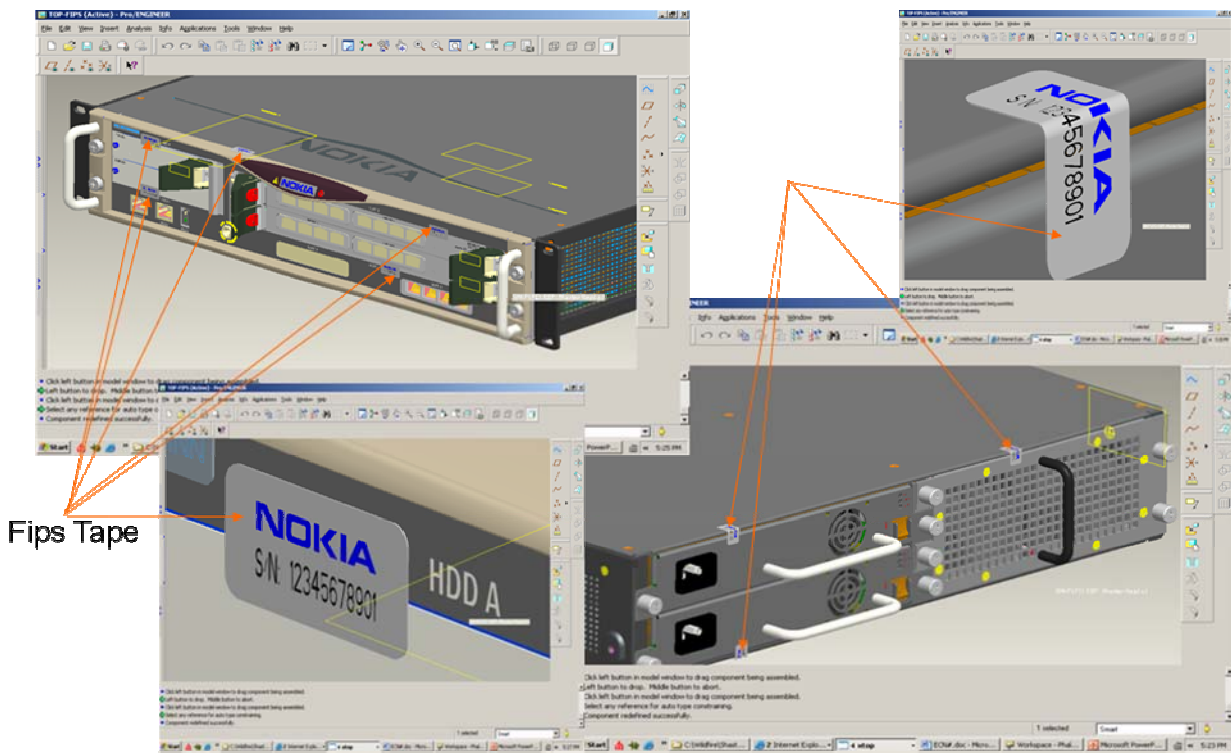
Figure 2 –Tamper Seal Placement on IP1280, IP2450 and IP2455 Chassis (8 Seals)

3.1.1.2 Module Initialization

Before performing the initial configuration, the Crypto Officer must set the boot manager password to prevent unauthorized access to the module hard disk. To be compliance with FIPS 140-2 requirements the Crypto Officer shall use a non-networked general purpose computer to initialize the appliance.

To initialize the appliance

1. Connect the supplied console cable to the local console port on the front panel of the appliance.

2. Connect the other end of the cable to a non-networked GPC running a terminal emulation program or a standalone VT100 console.

3. Press Return.

4. At the boot manager prompt, enter:
    BOOTMGR [0] > passwd

5. At the prompt, enter the new password.

6. At the prompt, re-enter the new password for verification.

7. IPSO can now be started by entering the boot command.

8. Follow the initial configuration procedures described in the appropriate *Appliance Installation Guide*.

3.1.2   Installing the Module Firmware

New modules come preinstalled with the Check Point IPSO operating system and a version of the Check Point VPN-1 application. The FIPS 140-2 conformant configuration consists of IPSO 4.2 with Check Point VPN-1 version NGX R65 with hot fix HFA 30.

3.1.3   Initializing Check Point Modules

Before the User can use the Check Point VPN-1 functionalities (also before he can enable FIPS mode), the Check Point VPN-1 version NGX R65 with hot fix HFA 30 must be enabled and initialized using the CLI.

The initialization process requires that the Crypto Officer establishes the SIC configuration. This is done via the *cpconfig* command. Once you have rebooted the device after installing the correct IPSO and VPN-1 versions, run 'cpconfig' and follow the instructions. Be sure to choose the following options during cpconfig: Distributed Installation (option 2) and Enforcement Module (option 1). You will also be prompted to initialize the SIC (Secure Internal Communication). This is used to initialize secure communication with the Check Point SmartCenter Management Station. Also enter a valid Check Point license.

Module version NGX R65 with hot fix HFA 30 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) must be configured during the initialization process by the Local Crypto-Officer before beginning the initialization of the module. The procedure for enabling the additional groups is obtainable from Check Point support SK27054 on the Check Point website.

Using the SmartDashboard application, the Check Point module should be configured for FIPS mode by selecting the screens and options shown in the screen shots included in Section 3.1.6 of this document. Only the screens shown should be configured.

Once this is completed, the module is adequately initialized and can be managed from the management server. FIPS mode can be enabled only after the Check Point initialization is complete

3.1.4   Setting the Module to FIPS Mode

After installing or upgrading to the appropriate Check Point module and initializing the Check Point module, the Crypto Officer must set the mode of operation to FIPS mode.

To set the mode of operation to FIPS mode

1. Use the CLI from the console port to enter the *set fips on restart* command. This will reboot the device and bring it up in FIPS mode

2. If desired, enter the *show fips* command to verify that the device is in FIPS mode. For the list of disabled access and feature mechanisms, see Appendix A on page 47.

3.1.5   Initializing the Remote Management of the Module

Before the Crypto Officer can manage the module remotely, SSH must be enabled, the Crypto Officer's authorized SSH public key must be entered; only SSHv2 shall be used and only FIPS-approved algorithms can be selected.

To initialize the remote management of the module

1. Using the CLI through the console port, enter the following commands:

   a. *set ssh server protocol **2***
   b. *set ssh server enable **1***

2. To ensure that the Crypto Officer can log in (with a password) using SSH, enter the following command:
   *set ssh server permit-root-login **yes***

3. Configure the type of authentication that the server will use to authenticate the Crypto Officer by entering the following commands:
   set ssh server
   *dsa-authentication **1***

> password-authentication *1*
> rhosts-authentication *0*
> rhosts-authentication *0*
> rsa-authentication *1*

4. Allow only FIPS-approved algorithms for encryption and configure the SSH protocol by entering the following commands:
set ssh server
> ciphers **3des-cbc**
> ` *keepalives <0 │ 1>*
> *listen-addr* IPv4/IPv6 address
> *listen-addr2* IPv4/IPv6 address
> *port <1 │ 2 │ 1,2>*
> *server-key-bits* **1024**

5. Generate host keys for SSHv2 by entering the following commands:
set ssh hostkey
> **v2 rsa size 1024**
> ` **v2 dsa size 1024**

6. Enter the Crypto Officer's authorized public key for SSHv2 with the following commands:
add ssh authkeys
> *v2 rsa user* name *<openssh-format* name *│ ssh-format file* name*> comment* name
> *v2 dsa user* name *<openssh-format* name *│ ssh-format file* name*> comment* name

7. For optional configuration settings, see the *CLI Reference Guide* for *IPSO 4.2.*

The module can now be managed remotely with SSH-secured management sessions.

When changing the configuration, the preceding settings denoted by bold letters and numbers must not be changed.

3.1.6 Management and Monitoring

After the initial setup, the Crypto Officer can locally or remotely manage, configure, and monitor the IPSO module with the CLI, or monitor with SNMPv3. The Crypto Officer can manage the Check Point module with the remote management server via the Check Point SmartDashboard application. Through this server, the Crypto Officer can configure policies for the module. These policies determine how the firewall and VPN services of the module function. Screen shots from the Check Point

SmartDashboard application are included to aid in illustration of the steps described below.

During the management of the module, the Crypto Officer must satisfy the following:

- The SSH configuration settings specified in Section 3.1.5 must be satisfied.

- Authorized public keys must be entered into the module with the SSH-secured management session.

- The AUX port must not be enabled.

- The module logs must be monitored. If a strange activity is found, the Crypto Officer should take the module off line and investigate.

- The tamper-evident seal must be regularly examined for signs of tampering.

- No keys or CSPs should be shared between the non-Approved mode and the Approved mode of operation when switching between modes of operation. To ensure that no sharing occurs, all keys must be zeroized while in one mode of operation before switching to another mode of operation.

The VPN functionality must be configured to use only FIPS-approved algorithms. The following pages denote sample screen shots of the various Check Point configuration screens. Authentication during IKE must employ pre-shared keys or digital certificates. IPSec and IKE can use only the following FIPS-approved algorithms:

Data encryption

- Triple DES
- AES

Data packet integrity

- HMAC with SHA1

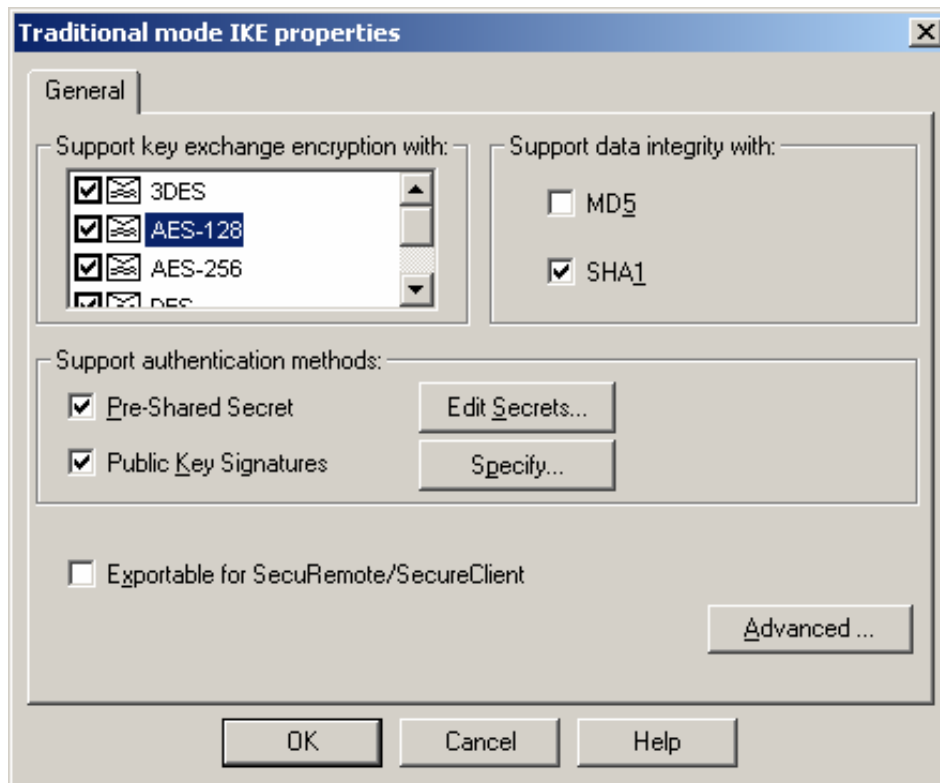**Authentication**

- Certificates
- Pre-shared keys

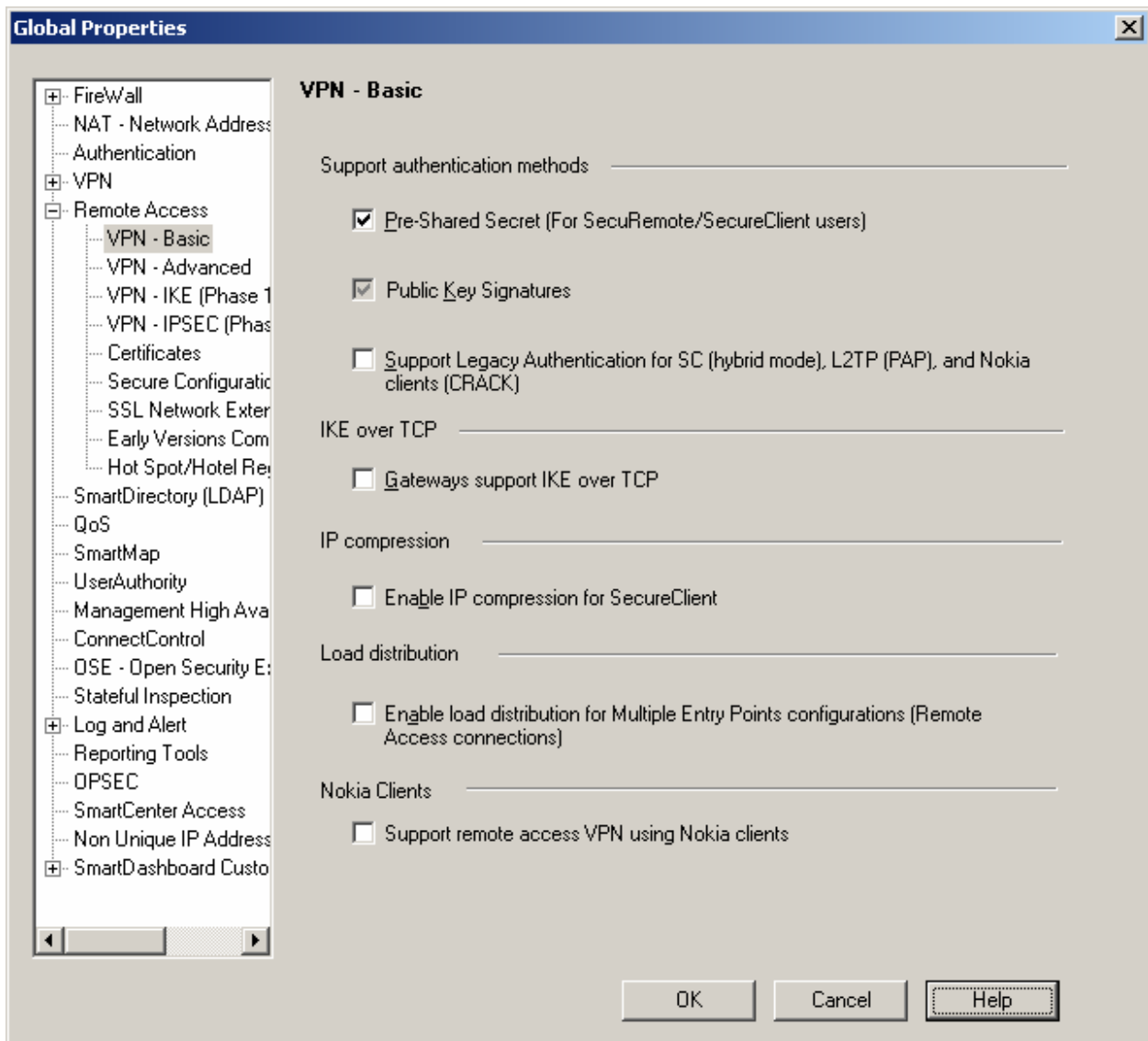**Figure 3 – Only FIPS-Approved Algorithms Can Be Used with IKE**

Figure 4 – Only Pre-shared Keys or Digital Certificates Can Be Used to Authenticate Clients

Notes:

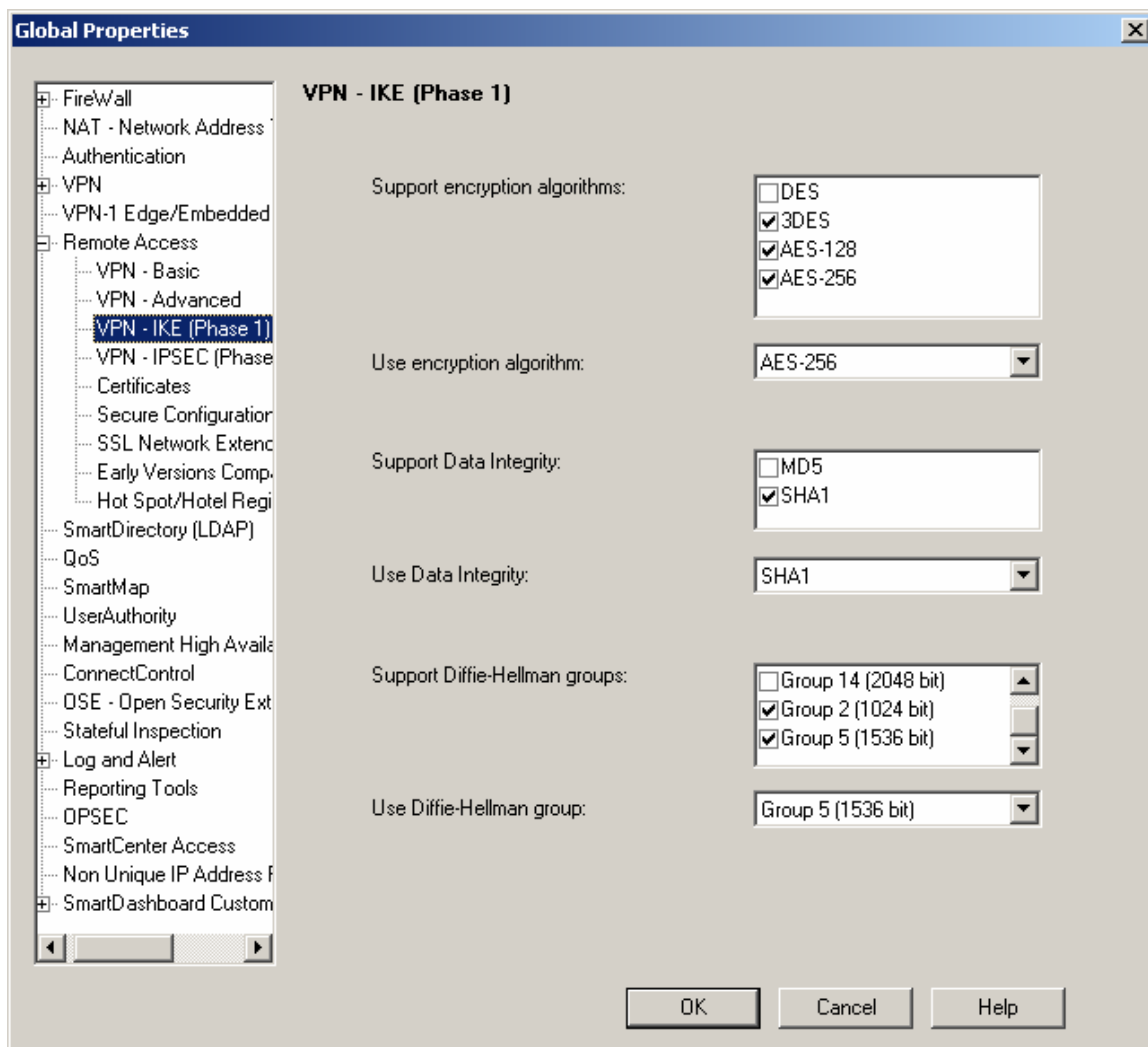Only 1024-bit or higher DSA and RSA key sizes should be used in FIPS mode.

Figure 5 – Only FIPS-Approved Algorithms Can Be Used with IKE

Notes:

1. Only Diffie-Hellman Groups 2 or higher (1024 bit modulus), providing 80 or more bits of encryption strength should be used in the FIPS approved mode of operation. Check Point recommends only DH Groups 14 (2048 bit modulus), to 18 should be used, providing between 112 and 128 bits of encryption strength.

2. After applying Check Point VPN-1 NGX R65 with hot fix HFA 30 and SK27054 (from Check Point support), additional Diffie-Hellman groups 15-18 (2048 bits to 8192 bits) are selectable as options.
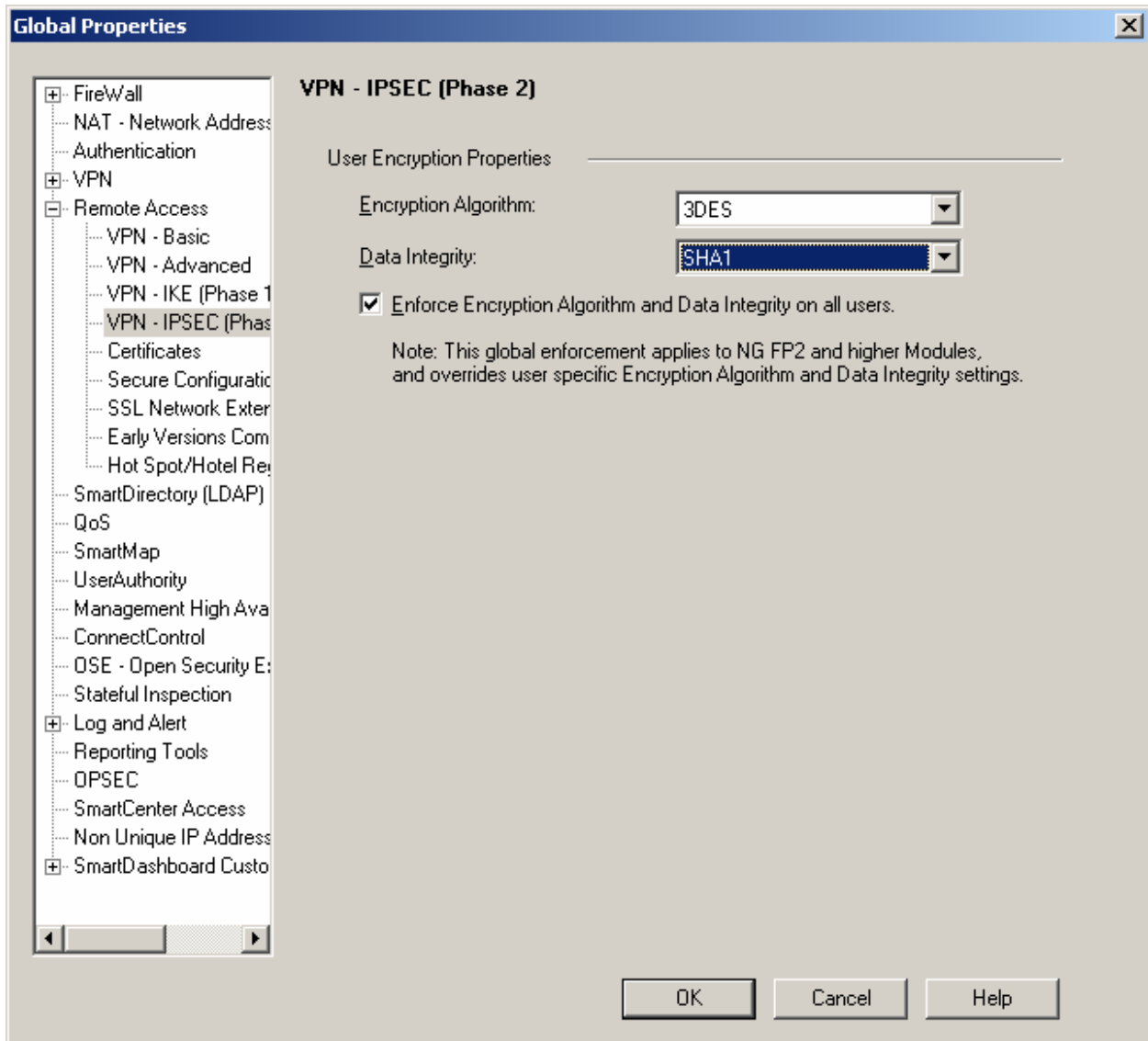
Figure 6 – Only FIPS-Approved Algorithms Can Be Used with IPSec

Notes:

The Crypto Officer should also make certain that no keys or CSPs are shared between the non-Approved mode and the Approved mode of operation when switching between modes of operation. To ensure that no sharing occurs, a Crypto Officer must zeroize all keys while in one mode of operation before switching to another mode of operation. The Crypto Officer User should only use 1024-bit keys or higher for RSA and Diffie-Hellman in FIPS mode. The DES algorithm, Triple-DES keying option 3, and public key sizes less than 1024-bits are not allowed in FIPS mode.
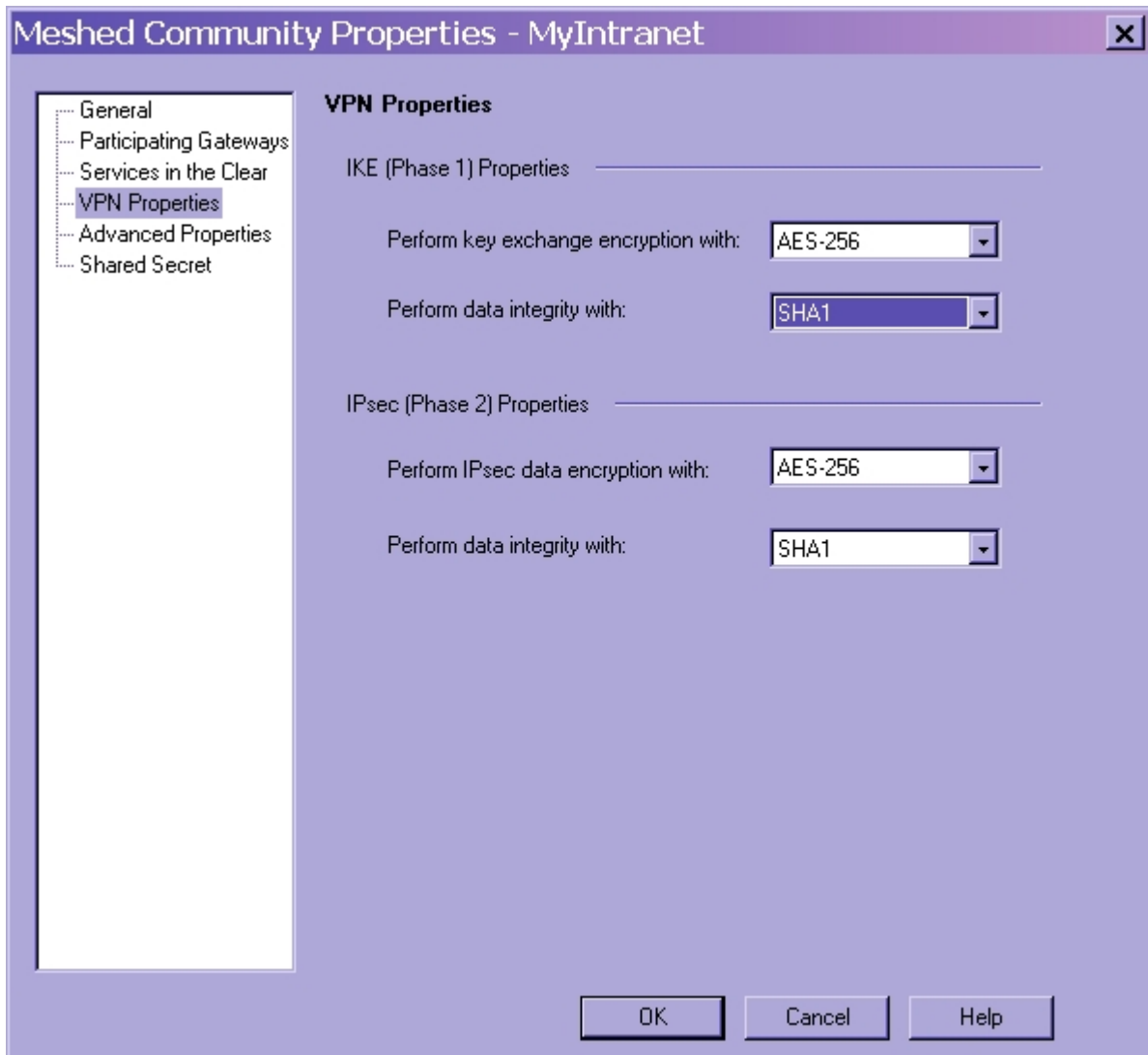
Figure 7 – Only FIPS-Approved Algorithms Can Be Used with IPSec or IKE

Note: This applies equally for either star or meshed VPN community properties

3.2 User Guidance

The User accesses the module 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.

APPENDIX A – DISABLED MECHANISMS

Warning: When running in a FIPS mode of operation, many of the existing and new features of Check Point IPSO are disabled as required for FIPS compliance.

The following list shows all the access and feature mechanisms that are disabled when the module is in FIPS mode:

- HTTP access

- FTP access

- Telnet access

- TFTP access

- Load Sharing (IPSO Clustering) and High Availability (VRRP)

- NTP

- Check Point remote installation daemon

- Firmware loading

- SSLv3

- SSHv1

- Disabled algorithms:

    o CAST

    o DES (40 bits)

    o MD5

    o HMAC MD5

    o Arcfour

    o Twofish

    o Blowfish

APPENDIX B – ALGORITHM VALIDATION CERTIFICATE NUMBERS

The module supports several independent implementations of the same FIPS-Approved algorithms. The following table lists the certificate numbers for the validated FIPS-approved algorithms implemented in IPSO, the Check Point VPN-1 firmware, and the cryptographic accelerator chips. Accelerator cards (when used) accelerate the Check Point firmware DES, Triple-DES, or AES VPN functions as indicated. Accelerated DES and Triple DES Keying Option 3 is non-compliant (Keying Option 3 uses one key 3 times). To remain in the FIPS Approved mode, only the FIPS approved Triple-DES and AES encryption algorithms should be used.

	Check Point Firmware	Check Point Firmware	Cryptographic Accelerator Chips
	IPSO 4.2	**NGX R65** w/HFA 30	**IP1280/IP2450/IP2455**
AES	N/A	**#709**	**#91**
DES[2]	N/A	N/A	N/A
Triple-DES[3]	**#637**	**#638, #729**	**#204**
HMAC	**#384**	**#385, #499**	**#203**
SHS	**#734**	**#735, #883**	**#500**
DSA	**#271**	N/A	N/A
RSA	**#332**	**#333**	N/A
RNG	**#417**	**#418**	N/A

Key Establishment Methodologies:

The following key establishment (Key Agreement or Key Wrapping) methodologies are implemented by the module. The relative encryption strengths provided by the mechanisms described are calculated in accordance with FIPS 140-2 Implementation Guidance 7.5 and NIST Special Publication 800-57.

Diffie-Hellman Key Agreement:
- **IKE - NGX R65:** provides between 96 and 128 bits of encryption strength; less than 80 bits non-compliant

- **SSHv2 - IPSO (4.2):** provides between 80 and 112 bits of encryption strength; less than 80 bits non-compliant

---

[2] DES is a non-FIPS Approved algorithm (not to be used in FIPS mode) and should not be selected for use. See Section 3.1.6 for configuration instructions.

[3] TDES keying option 3 is non-compliant (not to be used in FIPS mode) and should not be selected for use. See Section 3.1.6 for configuration instructions.

<u>RSA Key Wrapping:</u>

- **TLS:** Provides 80 - 150 bits of encryption strength

Note that only methodologies providing 80 or more bits of encryption strength are FIPS Approved. Sections 3.1.5 and 3.1.6 include instructions for configuring the module into approved mode.

APPENDIX C – ACRONYM DEFINITIONS

AH	Authentication Header
AI	Application Intelligence
ANSI	American National Standards Institute
BGP	Border Gateway Protocol
CBC	Cipher Block Chaining
CLI	Command-Line Interface
CMVP	Cryptographic Module Validation Program
CRC	Cyclical Redundancy Check
CSP	Critical Security Parameter
DSA	Digital Signature Standard
DVMRP	Distance Vector Multicast Routing Protocol
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FP	Feature Pack
IGRP	Inter-Gateway Routing Protocol
IKE	Internet Key Exchange
IPSec	IP Security
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OSPF	Open Shortest Path First
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
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
VPN	Virtual Private Network