Check Point®
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

# VPN-1

## NG with Application Intelligence

**FIPS 140-2 Non-Proprietary
Security Policy**

**Level 2 Validation
Version 0.71**

**March 2004**

# Table of Contents

# Introduction

## Purpose

This is a non-proprietary Cryptographic Module Security Policy for Checkpoint Software Technologies Ltd. (Check Point) VPN-1 version Next Generation (NG) with Application Intelligence.  This security policy describes how the Check Point VPN-1 version NG with Application Intelligence meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode.  This policy was prepared as part of the Level 2 FIPS 140-2 validation 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/.

The Check Point VPN-1 version NG with Application Intelligence is referred to 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 security policy.  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/) contains contact information for answers to technical or sales-related questions for the module.

## Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Check Point. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2

Validation Documentation is proprietary to Check Point and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Check Point.

# CHECK POINT VPN-1

## *Overview*

Check Point's VPN-1 version NG with Application Intelligence 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 FW-1 and the hardened Operating System SecurePlatform.

- Check Point FW-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 FW-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

Check Point VPN-1 version NG with Application Intelligence is considered to be a multi-chip standalone module for FIPS 140-2. VPN-1 is a software module intended to run on any standard personal computer (PC). It includes a hardened operating system that is not general purpose and does not implement physical security mechanisms.

Logically, the cryptographic boundary is composed of the Check Point VPN-1 and FW-1 software running on the Secure Platform Operating System. Physically, the cryptographic boundary of the module is the PC case, which physically encloses the complete set of hardware and software. The physical ports, logical interfaces, and FIPS logical interfaces are described in table Table 2. The module was tested on a Dell Optiplex GX 1 PC.

The module is intended to meet overall FIPS 140-2 level 2 requirements (see table Table 1).

| Section | Section Title | Level |
|---------|---------------|-------|
| 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 | N/A |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key Management | 2 |
| 8 | EMI/EMC | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

**Table 1 – Intended Level Per FIPS 140-2 Section**

### Module Interfaces

As a multi-chip standalone module being evaluated on a standard PC, the physical ports of the module include the network ports, keyboard/mouse ports, USB ports, and serial ports. All of these physical ports are separated into logical interfaces into the 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.

Although the module consists entirely of software, the FIPS 140-2 evaluated platform is a standard PC, which has been tested for and meets applicable FCC EMI and EMC requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

### 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.
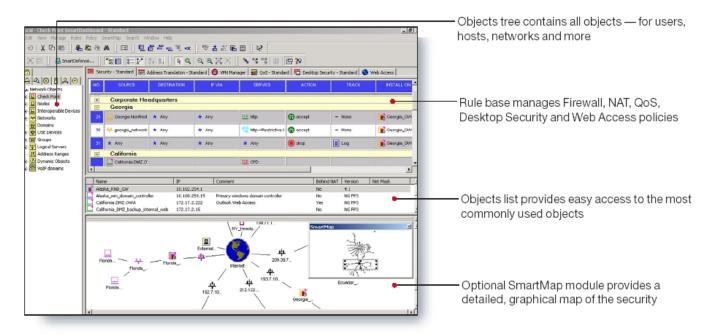


Objects tree contains all objects — for users, hosts, networks and more

Rule base manages Firewall, NAT, QoS, Desktop Security and Web Access policies

Objects list provides easy access to the most commonly used objects

Optional SmartMap module provides a detailed, graphical map of the 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 |
| Define and Implement Security Polices (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) |

| Service | Description | Input | Output | Critical Security Parameter (CSP) 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 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 |

| Service | Description with CLI commands | Input | Output | CSP |
|---|---|---|---|---|
| System management commands | Display or clear audit logs (audit); backup the system configuration (backup); restore the system configuration (restore); reboot the module (reboot); shutdown the module (shutdown); apply an upgrade or hotfix (patch) – not available in FIPS mode | Commands, any options, and configuration parameters | Status of commands and status information (logs) | None |
| System diagnostic commands | Change logging options (log); Display top 15 processes ranked by CPU usage (top); display or send diagnostic information (diag) | Commands and any options | Status of commands and status information (process list or diagnostic information) | None |
| Check Point module commands | 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)<br><br>Start the Check Point applications (cpstart); stop the Check Point applications (cpstop); show Check Point diagnostic information (cpinfo); display the status of Check Point applications (cpstat); manage Check Point licenses (cplic); show the SVN Foundation version (cpshared_ver); enable the high availability feature (cphastart); disable the high availability feature (cphastop); define a critical process (cphaprob) | Command (cpconfig), menu options, and configuration information<br><br><br><br><br><br><br><br>Command, any options, and configuration information | Status of commands/menu options and status information (configuration information)<br><br><br><br><br><br>Status of commands and status information (diagnostic information, version numbers, and license information) | None |
| Network diagnostic commands | Ping network hosts (ping); trace the route of packets to a host (traceroute); show network statistics (netstat) | Commands and any options | Status of commands and status information (diagnostic information) | None |
| Network configuration commands | Show and modify the kernel's ARP cache (arp); show, set, or remove hostname to IP mappings (hosts); show, configure, and store network interface settings (ifconfig); configure virtual LAN interfaces (vconfig); show and configure routing entries (route); get or modify the system's host name (hostname); get or set the system's domain name (domainname); show, add, or remove domain name servers (dns); interactive script for configuring the network and security settings of the system (sysconfig) | Commands, any options, and configuration information | Status of commands and status information (configuration information) | None |
| 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. | Outside of scope | Outside of scope | All CSPs stored on the module's hard drive |

*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 1024 bit key pair, which 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 1024 bit key pair. This mechanism is as strong as the RSA algorithm using a 1024 bit key pair, which 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 only the case sensitive English alphabet and the numerals 0-9 using a 6 digit password with repetition, the number of potential passwords is $62^6$. |
| 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**

*Unauthenticated Services*

The module has unauthenticated services that provide no security relevant functionality, and these services are available to all roles.

The module provides a full suite of firewall services without authentication, including packet filtering and quality of service. Additionally, access to the authentication mechanisms utilized by the different roles is unauthenticated.

### Physical Security

The physical security of this module do not apply to this module. Check Point VPN-1 version NG with Application Intelligence is a software module and does not implement any physical security mechanisms.

### Operational Environment

The operational environment requirements do not apply to this module. Check Point VPN-1 version NG with Application Intelligence does not provide a general-purpose operating system nor does it provide a mechanism to load new software.

The module was tested on the Check Point Secure Platform Operating System version NG with Application Intelligence.

### Cryptographic Key Management

Check Point adheres to 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 implements the following FIPS-approved algorithms:

Data Encryption:

- Advanced Encryption Standard (AES) in CBC mode (128 or 256 bit keys) – as per NIST FIPS PUB 197 (Certificate 88)

- Data Encryption Standard (DES) in CBC mode (56 bit keys) – as per NIST PUB FIPS 46-3 (Certificate 110 and 142) (for legacy use only)

- Triple DES (3DES) in CBC modes (168 bit keys) – as per NIST PUB FIPS 46-3 (Certificate 41 and 80)

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). (Certificate 42 and 69, Vendor affirmed)

Data Hashing:

- Secure Hash Algorithm (SHA-1) – as per NIST PUB FIPS 180-2 (Certificate 42 and 69)

PRNG:

- X9.31-based PRNG with Yarrow controls on entropy gathering

  o Triple DES (3DES) in ECB modes (112 bit keys) – as per NIST PUB FIPS 46-3 (Certificate 41)

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

Digital Signatures:

- RSA – as per PKCS#1 (Vendor affirmed)

Session Security:

- TLS v1.0 – as per RFC 2246

- IPSec

Key Agreement:

- Diffie-Hellman (used by IKE)

In addition, 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

- Secure Socket Layer (SSL) v3 – as per the Transport Layer Security Working Group draft.

| 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 bits) | RSA key generation (outside of crypto-boundary) | Stored "encrypted" on disk in P12 format ($CPDIR/conf/sic_cert.p12)- plaintext | Authentication during TLS handshake |
| RSA key pair for IKE | RSA key pair (1024 bits) | RSA key generation (outside of crypto-boundary) | Stored on disk ($FWDIR$/database/fwauth.NDBX) - plaintext | Authentication during IKE |
| Preshared keys for IKE (SHA-1 HMAC) | IKE preshared key (48 – 512 bits) | Outside of crypto-boundary | Stored on disk ($FWDIR$/database/fwauth.NDB) - plaintext | Authentication during IKE |
| Diffie-Hellman key pairs | Diffie-Hellman key pairs (768, 1024, 1536 bits) | Generated by IKE negotiations | RAM only (public parameters stored on disk ($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) | Random number generator |

| | | | - plaintext | |
|---|---|---|---|---|

<div align="center">**Table 7 – Listing of the Module's CSPs**</div>

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 is generated externally by the management software. This key pair is loaded onto the module over a secure TLS session established between the module and the management software. This key pair is stored on the module's hard drive 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.

## 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, and Triple-DES encryption/decryption, pseudo-random number generation, SHA-1 hashing, and HMAC with SHA-1 calculation.

    o  AES-CBC KAT

    o  DES-CBC KAT

    o  Triple-DES-CBC KAT

    o  PRNG KAT

    o  RSA KAT/pairwise consistency check

    o  SHA-1 KAT

o   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

- 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 configuration management system for the module and its components. CVS is used for configuration management of the source code. This software provides access control, versioning, and logging. Manual configuration management controls are utilized for the documentation. A formal process has been established, whereby a log is kept of all documentation and its updates. Documentation is tied to versions of the module through this log.

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

### Mitigation of Other Attacks

This section is not applicable. The module is designed to meet the overall FIPS 140-2 level 2 requirements and provides the level of security that comes with meeting those requirements. It does not mitigate against other attacks.

# SECURE OPERATION

Check Point VPN-1 version NG with Application Intelligence meets Level 2 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.

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

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 Secure Platform NG with Application Intelligence [Maintenace]" 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. Exit expert mode.

20. Switch the module to FIPS mode by entering the following command.

fips on

21. 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.

Note: In order for the management station to operate correctly with the module running in FIPS mode, the following commands must be run on the management station.

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 Steps*

> Once SIC trust has been established, the Remote Crypto-Officer must configure FireWall-1 implied rules to "Accept VPN-1 & FireWall-1 control connections: First." This is depicted in figure Figure 2.
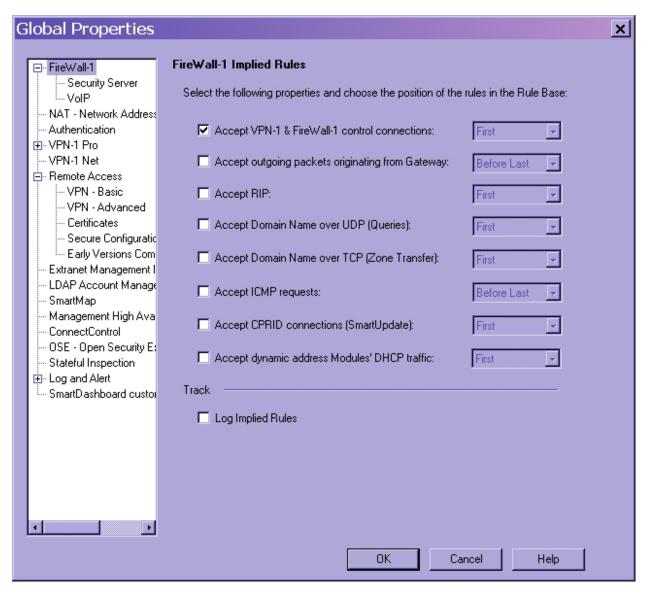


**Figure 2 – Select the Following Implied Rules for FireWall-1**

*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)

- Triple-DES

- AES

Data Packet Integrity

- HMAC with SHA1
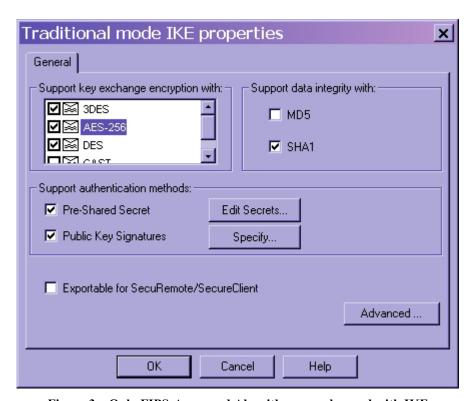
Authentication

- Certificates

- Pre-shared keys



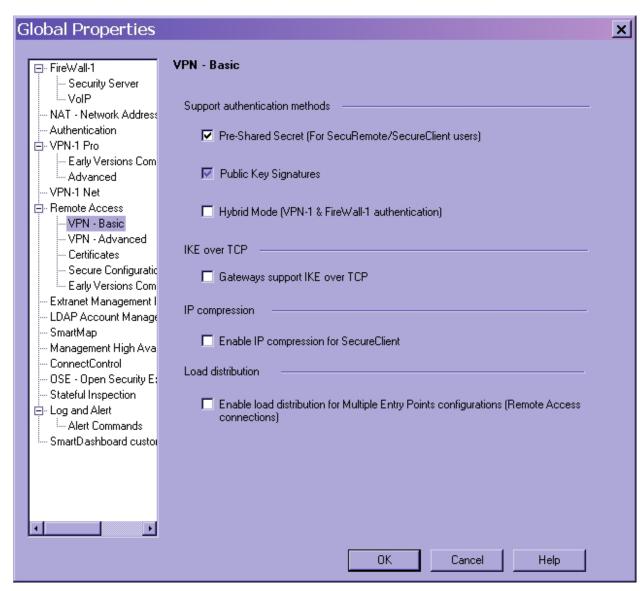**Figure 3 – Only FIPS-Approved Algorithms may be used with IKE**

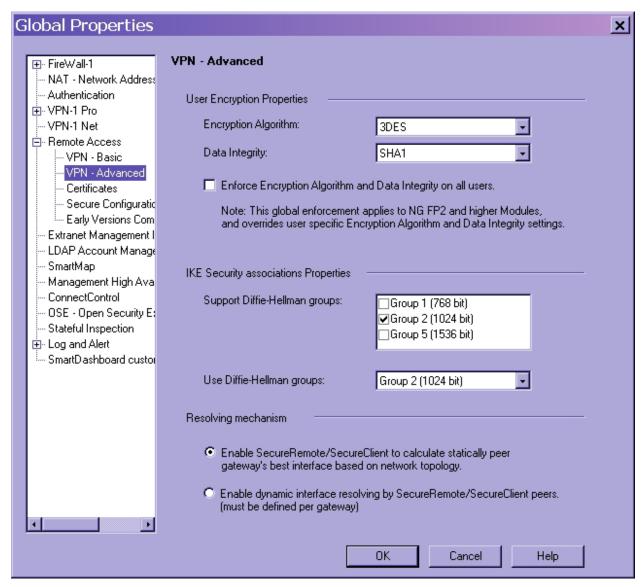**Figure 4 – Only Pre-Shared Keys or Digital Certificates may be used to Authenticate Clients**

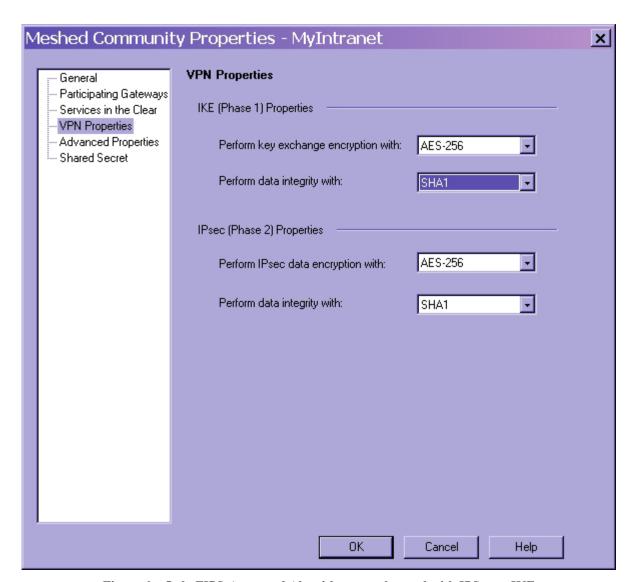**Figure 5 – Only FIPS-Approved Algorithms may be used with IPSec**

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

### *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 |
| 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 |
| 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 |