Provider-1

Version R71 with R7x hotfix

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Level 1 Validation on SecurePlatform

Document Version 1.08
June 16, 2013

Table of Contents

INTRODUCTION

Purpose

This non-proprietary cryptographic module Security Policy describes the Check Point Software Technologies Ltd. (Check Point) Provider-1 cryptographic module, Version R71 with R7x hotfix. This security policy describes how the Provider-1 module meets the security requirements of FIPS 140-2 and how to configure and operate the module in the FIPS 140-2 Approved mode. This policy was prepared to support the Level 1 FIPS 140-2 validation testing of the module on Check Point SecurePlatform.

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

Check Point's *Provider-1* Version R71 with R7x hotfix is alternatively referenced in this document as Check Point's *Provider-1*, *Provider-1 server*, *the module*, and *the software*.

References

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

- The Check Point website (http://www.checkpoint.com/) contains information on the full line of products from Check Point.
- The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) provides contact information for answers to technical or sales-related questions regarding the module.

Document Set for Submission

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

- Security Policy Document (This document) titled, *Provider-1 Version R71 with R7x hotfix FIPS 140-2 Non-Proprietary Security Policy*
- Finite State Machine Document titled, *Provider-1 Version R71 with R7x hotfix FIPS 140-2 Finite State Machine*

- Vendor Evidence Documentation titled,
  Provider-1 Version R71 with R7x hotfix Vendor Evidence Documentation

- *R71 Installation and Upgrade Guide*

- *Provider-1 R71 Administration Guide*

The FIPS 140-2 Validation Submission Documentation is Check Point – proprietary, with the exception of the Non-Proprietary Security Policy Document.

PROVIDER-1

Overview

Check Point Provider-1 technology provides virtualized security management, segmenting your security management into multiple virtual domains. Businesses of all sizes can easily create virtual domains based on geography, business unit or security function to strengthen security and simplify management.

Check Point products are based on a 3-tier technology architecture where a typical Check Point deployment is composed of gateways or other managed devices such as firewalls, routers, and switches, the Provider-1 server and SmartConsole GUI applications.

Deployment

There are two basic deployment approaches:

- Standalone deployment - where the gateway and the Provider-1 server are installed on the same machine.
- Distributed deployment - where the gateway and the Provider-1 server are installed on different machines.

A typical distributed deployment is shown in Figure 1.

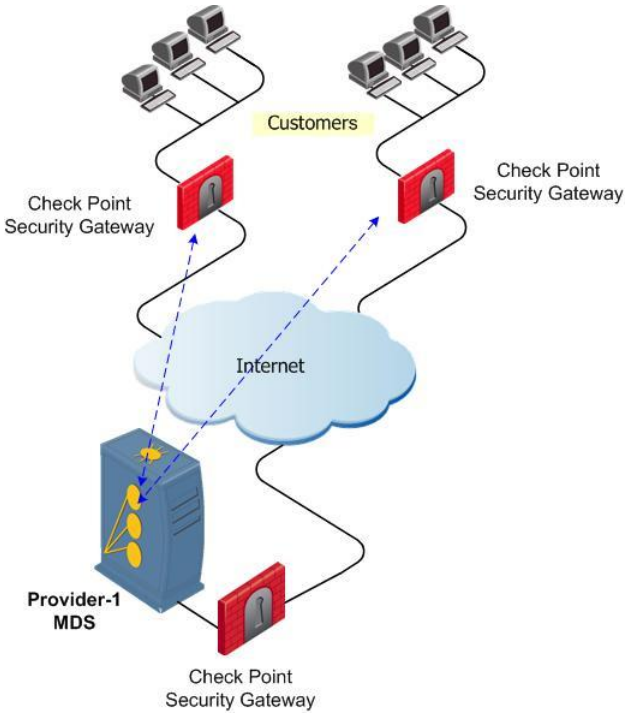

Figure 1. Typical R7x Provider-1 Server Deployment

This typical deployment includes the following components:

- **Gateways** connect to the Internet on one side, and to a LAN on the other.

- A **Virtual Private Network (VPN)** can be created between gateways, to secure all communication between them.

- The **Provider-1 server** is installed in the LAN, so that it is protected by a Security Gateway. The Provider-1 server is the component that manages the gateways and allows remote users to connect securely to the corporate network. The Provider-1 server manages the database and policies, and downloads policies to gateways.

- **SmartDashboard** is a tool used to create, edit, and install policies. It may be installed on the Provider-1 server or on any other machine. SmartDashboard is one of a set of GUI applications called SmartConsole for managing aspects of a corporate network.

  Objects are created in SmartDashboard by the system administrator to represent actual hosts and devices, as well as intangible components such as services (for example, HTTP and TELNET) and resources, (for example, URI and FTP). Each component of an organization has a corresponding object which represents it. Once these objects are created, they can be used in the rules of the Security Policy. Objects are the building blocks of Security Policy rules and are stored in the Objects database on the Provider-1 server.

- In addition to Check Point gateways, other **OPSEC-partner modules** (such as an AntiVirus Server) can be deployed in order to complete the network security in collaboration with the Provider-1 server and gateways.

Software Blades

Software Blades are independent and flexible security modules installed in the Provider-1 server that enable you to select the functions you want to build into your Check Point Security Gateways. Some Provider-1 Software Blades include (but are not limited to):

- Network Policy Management

- Logging & Status

- Monitoring

The Provider-1 server must be able to communicate with all the gateways and partner-OPSEC applications that it manages, even though they may be installed on different machines. And interactions between nodes must take place to ensure that the gateways receive all the necessary information — such as the Security Policy — from the Provider-1 server.

Secure communication channels between nodes can be set up using Secure Internal Communication (SIC). This ensures that these nodes can communicate freely and securely using a simple communication initialization process. The following security measures are taken to ensure the safety of SIC:

- Certificates for authentication are issued by the Provider-1 server's Internal Certificate Authority (ICA).
- Standards-based SSL (TLS v1.0) for the creation of the secure channel.
- 128 bit AES and Triple-DES for encryption.

The ICA management tool is the Secure Platform UI, Check Point's hardened Linux user interface tool, which allows a user to connect and manage the ICA by using a browser. Secure Platform UI is off by default. The Provider-1 server's ICA is used for creating and revoking certificates used in intra-TOE communications. ICA certificates are used for securing management traffic between a Provider-1 server and managed Check Point Software Blades R7x appliances. The ICA publishes CRLs internally to TOE components. The ICA also generates administrator certificates.

All internal communications between the Management GUI and the Provider-1 server, between the Provider-1 server and Check Point Software Blades R7x appliances as well as communications with remote trusted IT entities that interact with the TOE using OPSEC APIs (i.e. CVP or UFP servers) are protected using a Secure Internal Communications mechanism that is based on the TLS protocol. Certificates for SIC are generated and managed by the ICA and are signed using SHA 256-bit hashing.

Cryptographic Module

Provider-1 is a firmware module intended to run on any general purpose computer (GPC).

Note, within this Security Policy GPC denotes a standard computer hardware platform (Intel x86), excluding any operating system. The term GPC excludes other processing platforms such as smart phones, and smart cards.

The module is packaged with a custom built operating system (Check Point Secure Platform) that is installed on the GPC before the module.

When installation is complete, the module is locked in FIPS approved mode.

The Provider-1 cryptographic module is considered to be a multi-chip standalone module for FIPS 140-2. It includes a hardened operating system that is not general purpose and does not implement physical security mechanisms.

FIPS 140-2 validation testing was performed using the following operational environment configuration:

- Check Point Smart-1 50
- Module software and Check Point SecurePlatform™ Operating System Version R7x

FIPS 140-2 validation is maintained so long as the same module is installed onto any GPC with a compatible 32 bit x86 code-compatible CPU, e.g. Intel® Xeon®, AMD Opteron®, etc.

FIPS 140-2 validation is maintained so long as the same module is installed onto any GPC with a compatible 32 bit x86 code-compatible CPU. The following figure shows the GPC model Check Point Smart-1 50 (2 x Xeon E5410 2.33GHz (Harpertown), Quad Core 2x6MB L2, 1333MHz FSB) used for testing.

Logically, the cryptographic boundary is composed of the Secure Platform Operating System integrated with the Provider-1 software. 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 2.

The CMVP allows vendor porting of a validated level 1 firmware cryptographic module from the GPC specified on the validation certificate to a GPC that was not included as part of the validation status, as long as no source code modifications are required. The validation status is maintained on the new GPC without re-testing the cryptographic module on the new GPC. The CMVP makes no statement as to the correct operation of the module when so ported if the specific operational environment is not listed on the validation certificate.

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

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

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

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

Module Interfaces

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

FIPS 140-2 Logical Interface	Logical Interface	Standard PC Physical Port
Data input interface	User Interface (UI) for the Secure Platform, Network Layer IP interface	Network ports
Data output interface	User Interface (UI) for the Provider-1 server, Network Layer IP interface	Network ports
Control input interface	User Interface (UI) for the Provider-1 server, Network Layer IP interface	Keyboard ports, USB ports, serial console, network ports, power switch
Status output interface	User Interface (UI) for the Provider-1 server, Network Layer IP interface, Log files	Network ports, serial console, video port, Console port, LCD Display.
Power interface	N/A	Power connector

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

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

Roles and Services

The module supports three distinct roles:

- Remote Crypto-Officer (on page 11)
- Local Crypto-Officer (on page 13)
- User (on page 15)

The module uses digital signatures and passwords for authentication.

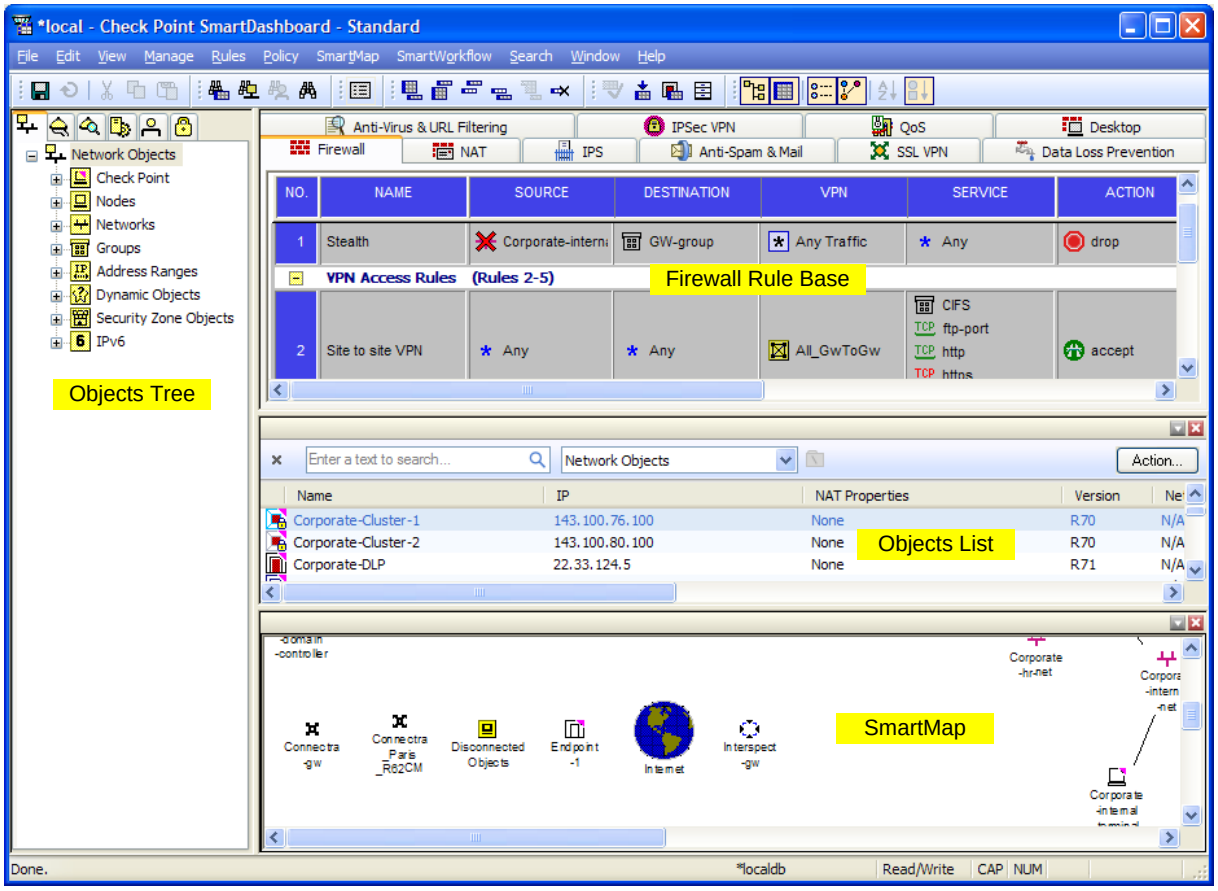

Figure 2. – Easy to Use Management Tools (SmartDashboard)

This section lists system services available to each of the above roles. All of the listed services are available in FIPS mode and in non-FIPS mode except the System Management Command to apply an upgrade or hotfix (patch) is not available in FIPS mode.

Note Do not apply upgrades, hotfixes or patches as any change to the validated module firmware will invalidate the FIPS module.

Remote Crypto Officer Role

The Remote Crypto-Officer role performs primary configuration of Provider-1 server. After authenticating, the Remote Crypto-Officer uses a powerful set of management tools (SmartDashboard) to configure and monitor the module. The remote management session uses TLS to ensure security.

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 3 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); DRBG SP 800-90AA seed keys, V & C values (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	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	Commands and configuration data (policy files)	Status of commands and configuration data (policy files)	RSA key pair for Secure Internal Communication (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 Provider-1 server 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
Password Authentication	Enable remote crypto officers to log in to the web interface.	User ID and Password	Authentication Status	Password
Status Output	The output indicators described for all services.	Service Inputs	Service Outputs	CSPs that are accessed by the services used.

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

Local Crypto Officer Role

The Local Crypto-Officer role is responsible for the installation, minimal configuration, and removal of the Provider-1 server. These operations are performed locally using physical access to the PC the module is installed on.

Local Crypto-Officers 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 CLI utilities and configurations available to that role.

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

Service	Description with CLI commands	Input	Output	CSP
FIPS mode	Switch to FIPS mode and enable integrity check.	Command and any options	Status of commands	None
Power-up self test.		Power up the system or power cycle the system.	Module powers up without error.	AES-CMAC firmware integrity key,

Service	Description with CLI commands	Input	Output	CSP
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)
Manage ICA Settings	Sign and Revoke certificates (cpconfig)	Commands, any options, and password	Status of commands	ICA RSA private key
View local help documentation	List available commands and their respective descriptions.	Commands	Status of commands and status information (help information)	None
Get and set date and time	View/change date (date); view/change time (time); view time zone (timezone)	Commands, any options, and date or time settings	Status of commands and status information (date, time, or time zone information)	None
System management commands	Display or clear audit logs (audit); backup the system configuration (backup); restore the system configuration (restore); reboot the module (reboot); shutdown the module (shutdown); apply an upgrade or hotfix (patch) – not available in FIPS mode	Commands, any options, and configuration parameters	Status of commands and status information (logs)	None
System diagnostic commands	Change logging options (log); Display top 15 processes ranked by CPU usage (top); display or send diagnostic information (diag)	Commands and any options	Status of commands and status information (process list or diagnostic information)	None
Check Point module commands	Install licenses, configure the SNMP daemon, modify the list of Unix groups authorized to register a cryptographic token and configure the one time SIC password (all functionality is provided through text-based menuing system after executing cpconfig)	Command (cpconfig), menu options, and configuration information	Status of commands/menu options and status information (configuration 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

Service	Description with CLI commands	Input	Output	CSP
Network configuration commands	Show and modify the kernel's ARP cache (arp); show, set, or remove hostname to IP mappings (hosts); show, configure, and store network interface settings (ifconfig); configure virtual LAN interfaces (vconfig); show and configure routing entries (route); get or modify the system's host name (hostname); get or set the system's domain name (domainname); show, add, or remove domain name servers (dns); interactive script for configuring the network and security settings of the system (sysconfig)	Commands, any options, and configuration information	Status of commands and status information (configuration information)	None
Key/CSP zeroization	The Local Crypto-Officer can zeroize all of the module's CSPs by reformatting the hard drive the module is installed on.	None	None	All CSPs stored on the module's hard drive
Password Authentication	Enable local crypto officers to log in to the CLI.	User ID and Password	Authentication Status	Password
Status Output	The output indicators described for all services.	Service Inputs	Service Outputs	CSPs that are accessed by the services used.
Non-Approved Service				
Upgrade and Hotfix Service	Enables a local crypto officer to apply software upgrades and hotfixes. **Do not use as any change to the validated module firmware will invalidate the module.**	Commands and any options	N/A	N/A

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

User Role

The User role is for users that are accessing the module from remote locations to perform management operations for managed devices such as VSX, gateway, and Connectra systems. These users can authenticate the module through TLS using digital certificates, and they authenticate themselves to the module using password authentication.

Once authenticated, an encrypted tunnel is established between the Check Point Provider-1 server and the user.

Service	Description	Input	Output	CSP
TLS	Access the module's TLS to create a secure session for remotely managing managed devices.	TLS handshake parameters, TLS inputs, data	TLS outputs and data	RSA key pair for management (read access); Session keys for management (read/write access); DRBG SP 800-90AA seed keys, V & C values (read access)
Manage managed devices	Perform operations affecting managed devices	Clicking on GUI objects, entering values into dialog boxes.	Status of operations	None
View local help documentation	Show help screens for available GUI operations.	Clicking the help pull down menu and choosing help topics.	Help information	None
Password Authentication	Enable users to log in to the web interface.	User ID and Password	Authentication Status	Password
Status Output	The output indicators described for all services.	Service Inputs	Service Outputs	CSPs that are accessed by the services used.

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 (role-based methodology) is used to authenticate to the module during the TLS handshake. This mechanism is as strong as the RSA algorithm using a key pair of either 2048 or 4096 bits. Using a 2048 bit key pair is generally considered equivalent to brute forcing a 112 bit key (i.e., a 1 in 2^112 chance of false positive).
Password-based authentication	Passwords (identity-based methodology) are required to be between 6 and 128 characters long, 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 5 – Estimated Strength of Authentication Mechanisms

Each authentication mechanism shown in Table 5 demonstrates that a single, random authentication attempt has less than a 1:1,000,000 chance at success (i.e., a false positive).

Repeated attempts to randomly guess the authentication data within a 1-minute period would require the following attempt rates:

- RSA-based: ((2^112) / (100,000 *60)) = 8.6538281×10^{26} attempts per second
- Password-based ((62^6) / (100,000 *60)) = 9467 attempts per minute

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

Unauthenticated Services

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

Physical Security

Check Point Provider-1 is a firmware module and runs on a production grade GPC.

Operational Environment

The FIPS 140-2 Operational Environment requirements do not apply to this module. Check Point Provider-1 server does not provide a general-purpose operating system nor does it provide a mechanism to load new software.

The cryptographic module is software and was tested under the Check Point SecurePlatform™ operating system on the processor types provided by General Purpose Computing platforms in the configurations shown in section *Cryptographic Module* on page 7. These processor types are also reflected in the module's cryptographic algorithm validation certificates.

Cryptographic Key Management

Check Point adheres to FIPS-Approved cryptographic standards and provides the strongest cryptography available. Check Point Provider-1 server'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.

The Provider-1 server provides the capability to use TLSv1 to secure management sessions.

The Check Point Provider-1 server cryptographic module implements the following FIPS-Approved algorithms (NIST-assigned algorithm validation certificate numbers shown in boxed items):

Data Encryption:

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

Provider-1 server R7x
Certificate #1836

Triple DES in CBC mode (e/d KO 1,2) – as per NIST FIPS PUB 46-3

Provider-1 server R7x
Certificates #1188 and #1189

Data Integrity:

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

Provider-1 server R7x
Certificates #1089 and #1090

Data Hashing:

Secure Hash Standard (SHS SHA-1, SHA-256, SHA-384, and SHA-512) – as per NIST PUB FIPS
180-2

Provider-1 server R7x
Certificates #1615 and #1616

DRBG:

DRBG SP 800-90A Implementation

Provider-1 server R7x
Certificate #146

HASH-DRBG with SHA-256 and a seed length of 440 bits in accordance with SP 800-90A

Digital Signatures:

RSA – PKCS#1 and ANSI X9.31 key generation.

Provider-1 server R7x
Certificate #925

The RSA implementation is used both for signature generation and verification (per PKCS#1), and also for key transfer when supporting Distributed Key Management (DKM) implemented in managed devices.

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

Session Security:

- TLS v1.0 – as per RFC 2246
  TLS v1.0 is equivalent to Secure Socket Layer (SSL) v3.1.

Key Wrapping (Key Agreement / Key Establishment):

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

- The RSA key wrapping methodology (used by TLS), provides 112 or 150 bits of encryption strength.

- The module supports key entry though TLS using 3-key Triple-DES session keys. Triple-DES (Cert. #1188), key wrapping; key establishment methodology provides 112 bits of encryption strength.

- The module supports key entry though TLS using AES session keys. AES (Cert #1836), key wrapping; key establishment methodology provides 256 bits of encryption strength.

In addition, the Check Point Provider-1 server provides the following algorithms that are *not approved for FIPS*:

- 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
- DES
- AES CMAC

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

Key	Key type	Generation	Storage	Use
Local Crypto-Officer passwords	N/A	Entered by local crypto officer	Stored on disk (/etc/password) - plaintext	Local Crypto-Officer authentication
Remote Crypto Officer Password	N/A	Entered by remote crypto officer	Stored as a SHA256 hash on disk.	Remote Crypto Officer Authentication
User Password	N/A	Entered by user	Stored as a SHA256 hash on disk.	User Authentication
RSA key pair for management	RSA key pair (2048 or 4096 bits)	Internal, ANSI X9.31 compliant	Stored on disk in P12 format ($CPDIR/conf/sic_cert.p12) (considered plaintext)	Authentication during TLS handshake
RSA key pairs for managed devices	RSA key pair (2048 or 4096 bits)	Internal, ANSI X9.31 compliant	Not Stored. Exported to managed devices.	Used by managed devices.
Session keys for management	AES (256 Bits) or TDES	Generated by TLS handshake	Cached to disk ($CPDIR$/database/session.NDBX) - plaintext	Secure TLS traffic (SIC)
HMAC session key for management	HMAC	Generated by TLS handshake	Cached to disk ($CPDIR$/database/session.NDBX) - plaintext	Authenticated TLS traffic
DRBG SP 800-90A HASH_DRBG seed keys	Seed Key of 440 bits according to SP 800-90A.	Generated by gathering entropy	RAM only, but entropy used to generate keys is cached to disk ($CPDIR/registry/HKLM_registry.data and $CPDIR/registry/HKLM_registry.data.old) - plaintext	Random bit generator
DRBG SP 800-90A HASH_DRBG V & C values	Internal state for the Hash_DRBG	Internal state derived from seed value	RAM only	Random bit generator
Integrity Check key	AES-CMAC	Generated outside the module.	Hardcoded into the CPHASH binary.	Module firmware integrity check

Table 6 – Listing of the Module's CSPs

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

When DKM is used, the key pair is generated internally by the module. The Local Crypto Officer configures the module for either internal key generation or to import external keys from the management station. This key pair is stored on the module's hard drive in plaintext and can be zeroized by reformatting the module's hard drive containing the module's software. Additionally, it can be overwritten by generating a new RSA key pair.

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 AES-CMAC 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 firmware integrity check. The keys cached to disk can be zeroized by reformatting the partition (or whole hard drive).

The SP 800-90A random bit generator (DRBG) seed 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 SP 800-90A RNG. The seed length is 440 bits in accordance with SP800-90A. 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 an AES-CMAC.

Cryptographic Algorithm Known Answer Tests (KATs): KATs are run at power-up for the following algorithms:

- AES-CBC KAT
- Triple-DES-CBC KAT
- DRBG KAT
- RSA (encrypt/decrypt) and (sign/verify) KAT tests
- SHA-1 KAT
- SHA-256 KAT
- SHA-384 KAT
- SHA-512 KAT
- SHA-1 HMAC KAT

Conditional Self-tests:

- Continuous DRBG Test: This test is constantly run to detect failure of the module's random number generator.
- RSA pair-wise consistency test: This test is run by the module whenever RSA key pairs are generated internally.

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

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

Design Assurance

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

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

Mitigation of Other Attacks

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

SECURE DELIVERY AND OPERATION

Check Point Provider-1 server meets overall Level 1 requirements for FIPS 140-2. The sections below describe how to securely deliver the module to authorized operators, and includes how to place and keep the module in FIPS-approved mode of operation.

Secure Delivery

The cryptographic module ships from the manufacturer to the customer without any cryptographic keys. The only critical security parameter (CSP) is the default password contained in the ISO image that is configured during installation. All other cryptographic keys and CSPs are generated by the Internal Certificate Authority after the module is installed and initially powered up.

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

Other known answer tests (see Self-Tests on page 21 in this document for a complete description of known answer tests) confirm the correct operation of cryptographic algorithms and security functions. If any of these tests fail, the module will not initialize.

Crypto-Officer Guidance

Installation and Initialization

The Local 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 Provider-1 server user manuals.

The Local Crypto-Officer receives the module in a shrink wrapped package containing a CD-ROM with the Provider-1 server 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 Local Crypto-Officer must maintain control of the installation media.

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

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

The Local Crypto-Officer must establish the SIC configuration and create the Internal CA using cpconfig 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 a SmartConsole GUI.

Management

Once initialization of the module has been completed, the Remote Crypto-Officer must manage the module using SmartDashboard. Through this GUI, the Crypto-Officer is able to configure policies for the module.

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

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

Note Do not apply upgrades, hotfixes or patches as any change to the validated module firmware will invalidate the FIPS module.

Termination

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

FIPS Mode Configuration

Local Crypto-Officer Installation and Configuration Steps

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

Note - The TCP/IP network protocol must be installed, properly configured, and operational before you begin the installation process.

To Install and Configure the SecurePlatform:

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

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

2. Connect to the server's IP address over https (https://<ip_address>), or using the command line.

3. Log in with the user name: `admin` and password: `admin` .

4. When prompted, change the admin password. You can also change the admin user name.

5. Run: `sysconfig`
   The first-time system configuration wizard starts. Press `n` to continue.

6. In the **Network Configuration** menu, configure these options and press `n` to continue:

   - Host Name
   - Domain Name
   - DNS server
   - Network Interfaces
   - Routing Configuration

7. In the **Time and Date Configuration** menu, configure these options and press n to continue:

   - Date
   - Time and time zone

To Install the Software Blades:

8. To continue with choosing the Software Blades, press `n`.

   If you want to import a configuration file of another SecurePlatform installation, press `1` and see the Advanced Upgrade on SecurePlatform in the *Installation and Upgrade Guide*.

9. The installation wizard welcome message appears. Press N.

10. Read the End User License agreement and press Y to accept the terms.

11. Select:

    - **New Installation** - press N to continue the installation process.

    - **Installation Using Imported Configuration** - the installation process looks for an exported configuration file.

12. In the **Software Blades** screen, select the blades you wish to install and press N to continue.

13. If you select **Provider-1 server**, select whether it should be installed as a primary Provider-1 Server secondary Provider-1 server, or a Log server without the security management component and press N.

14. If you selected **SmartEvent** and **SmartReporter**, select one or more of the Software Blades and press N:

    - SmartEvent

    - SmartReporter

    - SmartEvent Correlation unit

15. If you selected **Provider-1 Server** and **Endpoint Security Server**, you should install the Endpoint Security server as a Primary Endpoint Security server in standalone mode and press N. If you only selected **Endpoint Security Server**, select one of the Software Blades and press N:

    - **Primary Endpoint Security Server**. If you selected primary, decide whether it should be installed as a

      Endpoint Security server - standalone installation

      Endpoint Security server - distributed installation

    - **Secondary Endpoint Security Server**.

    - **Connection Point**.

16. A message validates your choice of Software Blades. Press N to continue.

The required installation files are extracted and Software Blades installed.

Post-Install Configuration Steps

The Configuration Tool runs automatically after the installation process is complete. The Configuration Tool can also be run manually by running the `cpconfig` command. The configuration features for a Provider-1 server include:

- Licenses: Generates a license for the Provider-1 server and the gateway.
- Administrators: Creates an administrator with Provider-1 server access permissions. The administrator must have Read/Write permissions in order to create the first security policy.
- GUI Clients: Creates a list of names or IP addresses for machines that can connect to the Provider-1 server using SmartConsole.
- Certificate Authority: Provides definitions that are used to initiate the Internal Certificate Authority, which enables secure communication between the Provider-1 server and its gateways. For some operating systems, such as Windows, you must specify the name of the host where the ICA resides. You may use the default name or provide your own. The ICA name should be in the hostname.domain format, for example, ica.checkpoint.com.
- Fingerprint: Verifies the identity of the Provider-1 server the first time you log in to SmartConsole. Upon SmartConsole login, a Fingerprint is displayed. This Fingerprint must match the Fingerprint shown in the Configuration Tool window in order for authentication to succeed. You may want to export this Fingerprint for verification purposes when you log in to SmartConsole for the first time.

To configure Using the Configuration Tool:

1. Start the Configuration Tool, `cpconfig`, if not already running.
2. Add Licenses. Perform one or both of the following procedures:
   - Fetch one or more licenses from a file.
   - Add a license manually.
3. Add Administrators. Only one administrator can be added that uses SmartConsole to connect to the Provider-1 server. Additional administrators can be added using SmartDashboard.

4. Define GUI Clients.

   Important - If you do not define at least one GUI client, you can only manage the Provider-1 server from a local GUI client that runs on the same machine as the Provider-1 server.

   You can add a GUI client using any of the following formats:

   - **IP address**: For example, `1.2.3.4`.
   - **IP/net mask**: A range of IP addresses, for example, `192.168.10.0/255.255.255.0`.
   - **Machine name**: For example, **Alice**, or **Alice.checkpoint.com**.
   - **Any**: Any IP address.
   - **IP1-IP2**: A range of IP addresses, for example, **192.168.10.8 - 192.168.10.16**.
   - **Wild cards**: For example, **192.168.10**.*

5. Initialize the Internal Certificate Authority.

   This option enables you to initialize an Internal Certificate Authority (ICA) on the Provider-1 server and a Secure Internal Communication (SIC) certificate for the Provider-1 server. SIC certificates authenticate communication between Check Point communicating components, or between Check Point communicating components and OPSEC applications.

   Important - Components can communicate with each other only after the Certificate Authority is initialized and each component has received a SIC certificate.

6. Export the Provider-1 server's fingerprint to a text file.

   The fingerprint, a text string derived from the Provider-1 server certificate, is used to verify the identity of the Provider-1 server that is being accessed through SmartConsole. The first time SmartConsole connects to the Provider-1 server, compare this string to the string displayed in SmartDashboard.

7. Start the installed products.

To Authenticate the Administrator:

During the login process, administrators connect to the Provider-1 server through SmartDashboard using the same process as SmartConsole clients. The administrator and the Provider-1 server are first authenticated (to create a secure channel of communication) and then the selected SmartConsole starts.

After the first login, the administrator can create a certificate for subsequent logins. For additional information on how to create a certificate, refer to the *Provider-1 R71 Administration Guide*.

1. Open SmartDashboard by selecting **Start > Programs > Check Point SmartConsole >SmartDashboard**.

2. Log in using the **User Name** and **Password** defined in the Configuration Tool's **Administrators** page during the Provider-1 server installation on page 25.

   If you are using a locally stored certificate to authenticate your connection, browse to its location and enter the certificate's password. The certificate's password can be changed by expanding the **More Options** link and clicking **Change Password**.

3. Specify the name or IP address of the target Provider-1 server and click OK.

4. Decide whether to connect in **Read Only** mode. This mode enables you to view the current configuration without accidentally changing it. It also gives access to Provider-1 server when another designated administrator is already connected.

5. **More Options**. Clicking the More Options link enables you to fine tune how SmartDashboard connects to Provider-1 server.

   - The **Change Password** button in the **Certificate Management** area of the dialog enables you to change the password that protects the certificate.

   - **Session Description**. Descriptive information entered here populates the **Session ID** field available in **SmartView Tracker's Audit Mode**. The field can be used to explain why a particular administrator is connecting to Provider-1 server.

   - **Use compressed connection**. This option optimizes the connection to Provider-1 server. By default, the connection to Provider-1 server is compressed. For a very large

configuration database, disabling the compression may help reduce load on the Provider-1 server.

- **Do not save recent connections information**. By default, SmartDashboard server remembers the last user ID and Provider-1 server to which a connection was made. Select this option to prevent SmartDashboard from displaying the last administrator and Provider-1 server to which the administrator successfully connected.

- **Plug-in Demo Mode**. This option enables SmartDashboard demo mode to display windows and options specific to a particular Plug-in. Select the Plug-in from the **Versions** drop-down box. 6. Manually authenticate the Provider-1 server using the Fingerprint provided during the configuration process.

Note Do not apply upgrades, hotfixes or patches as any change to the validated module firmware will invalidate the FIPS module.

Remote Crypto-Officer Configuration Guidelines

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

Authentication during TLS must employ digital certificates. Additionally, only the following FIPS-approved algorithms may be used by TLS:

Data Encryption

- AES
- Triple-DES

Data Packet Integrity

- HMAC-SHA1

Authentication

- Certificates

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

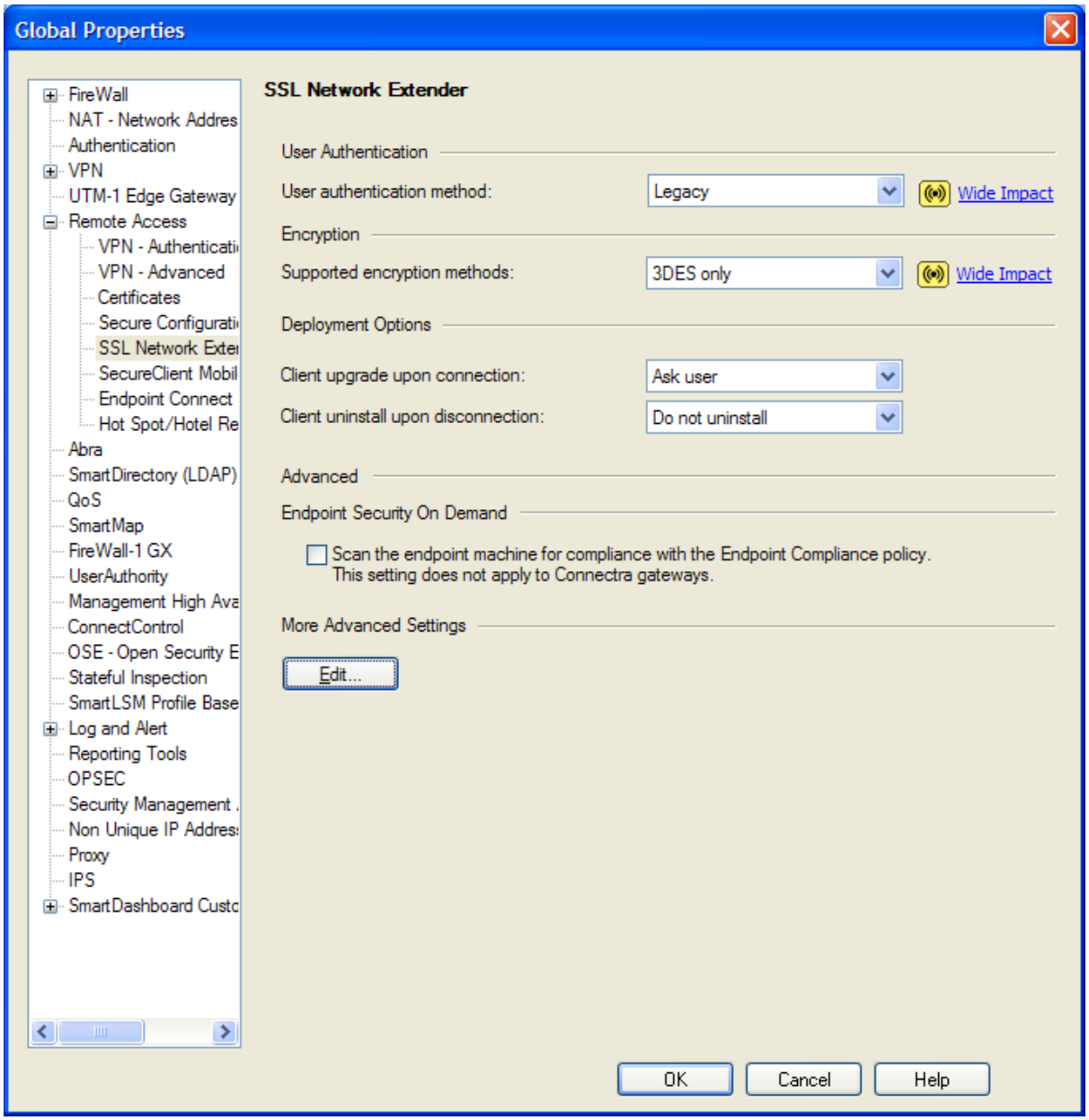

Figure 3 – Only FIPS-Approved Algorithms may be used with TLS

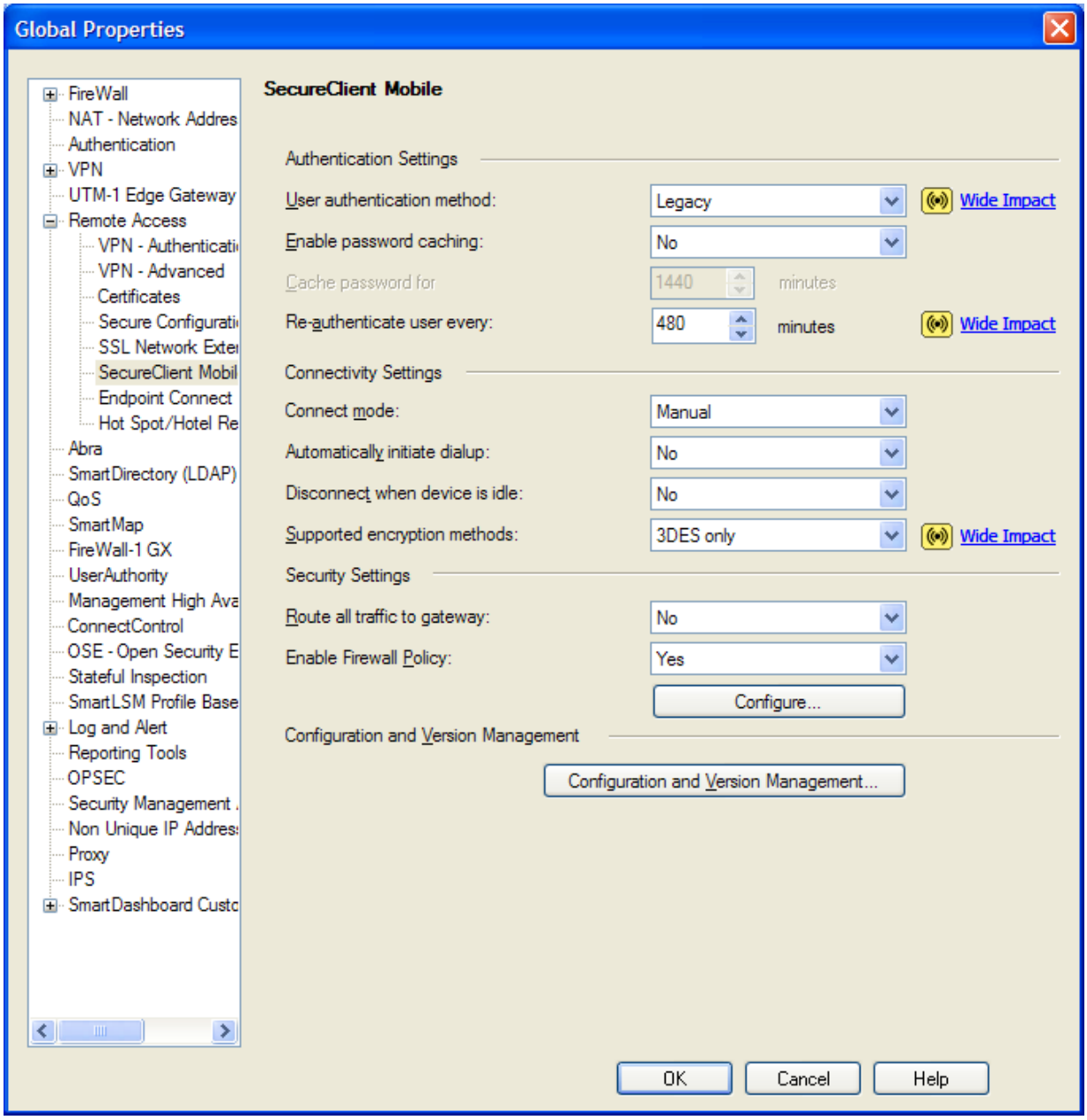

Figure 4 – Only FIPS-Approved Algorithms may be used with TLS

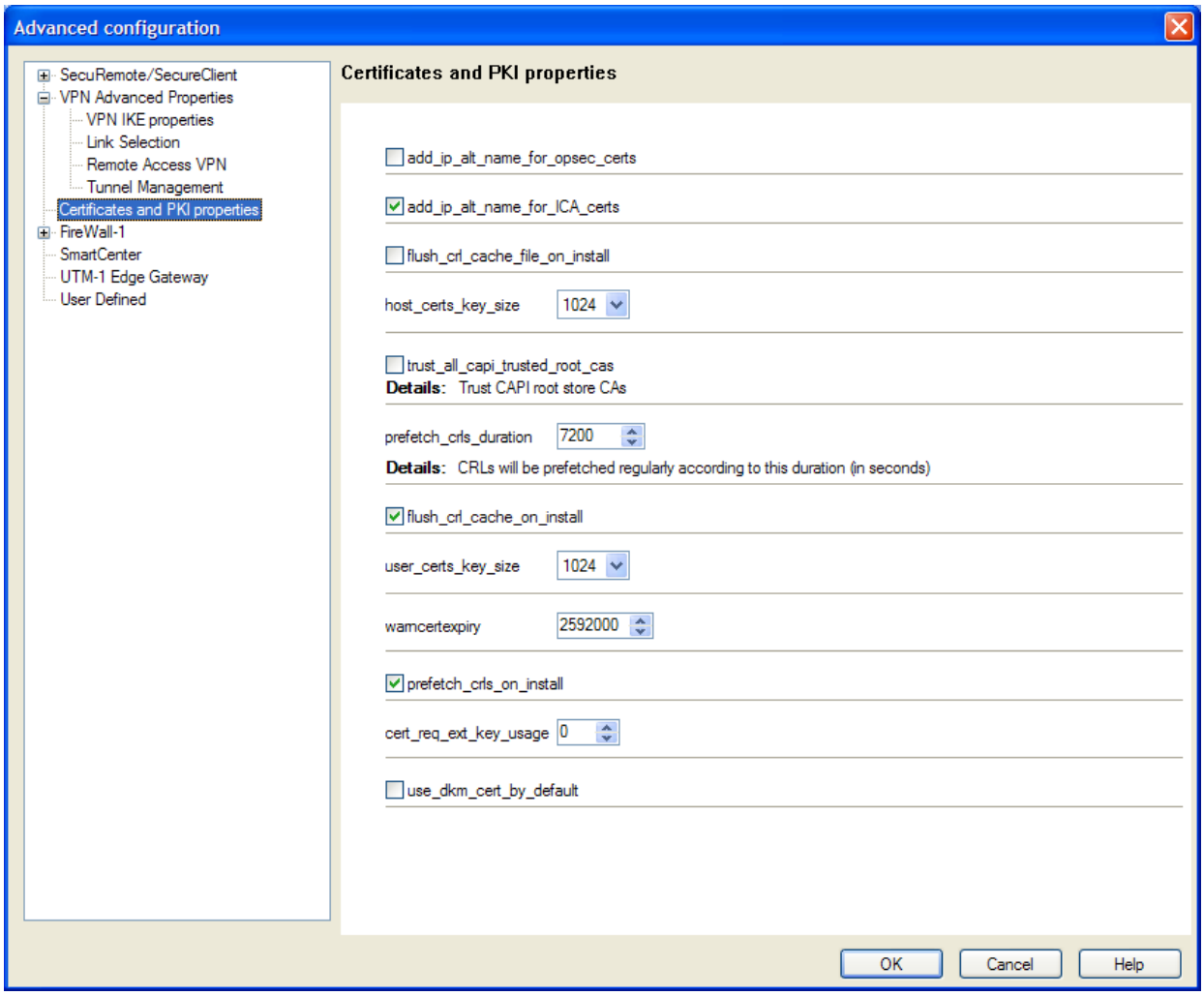

Figure 5 – Configuring the module to enable Distributed Key Management (DKM) globally for managed devices

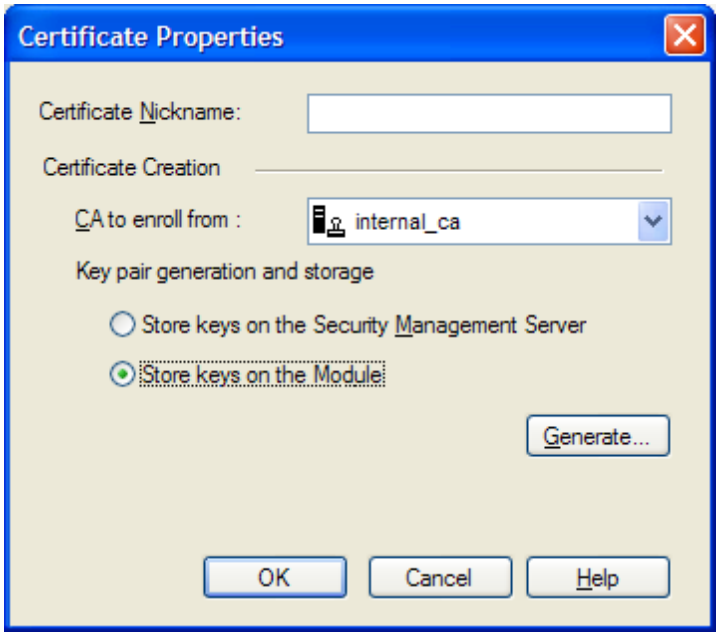

Figure 6 – Configuring the module to generate RSA keys with DKM on a per-certificate basis

ACRONYMS

AH	Authentication Header
ANSI	American National Standards Institute
CA	Certificate Authority
CBC	Cipher Block Chaining
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DKM	Distributed Key Management
DRBG	Deterministic Random Bit Generator. Also known as a pseudorandom number generator (PRNG).
DSA	Digital Signature Standard
ECC	Elliptic Curve Cryptography
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FP	Feature Pack
HF	Hot Fix
ICA	Internal Certificate Authority
IKE	Internet Key Exchange
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

