Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

# VSX

Version R67.10 with R7x hotfix

# FIPS 140-2 Non-Proprietary Security Policy

## FIPS 140-2 Level 1 Validation

**Document Version 1.8**
**May 31, 2013**

Documentation produced by Rosenberry Associates, Inc. under contract to Check Point.

# Table of Contents

# Introduction

## *Purpose*

This non-proprietary cryptographic module Security Policy describes the Check Point Software Technologies Ltd. (Check Point) VSX cryptographic module, Version R67.10 with R7x hotfix. This security policy describes how the Check Point VSX module meets the security requirements of FIPS 140-2 and how to configure and operate the module in the FIPS 140-2 Approved mode. This policy was prepared to support the Level 1 FIPS 140-2 validation testing of the module.

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

Check Point's VSX Version R67.10 with R7x hotfix is alternatively referenced in this document as Check Point *VSX*, *VSX*, *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,
  *VSX* Version R67.10 with R7x hotfix *FIPS 140-2 Non-Proprietary Security Policy*

- Finite State Machine Document titled,
  *VSX* Version R67.10 with R7x hotfix *FIPS 140-2 Finite State Machine*

- Vendor Evidence Documentation titled,
  *VSX* Version R67.10 with R7x hotfix *Vendor Evidence Documentation*

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

# VSX

## *Overview*

Check Point's VSX (Virtual System Extension) is a security and VPN solution, designed to meet the demands of large-scale environments. Based on the proven security of Check Point Security Gateway, VSX provides comprehensive protection for multiple networks or VLANs within complex infrastructures. It securely connects them to shared resources such as the Internet and/or a DMZ, and allows them to safely interact with each other. VSX is supported by *IPS™ Services*, which provide up-to-date preemptive security.

VSX incorporates the same patented Stateful Inspection and Application Intelligence technologies used in the Check Point Security Gateway product line. It runs on high speed platforms (known as VSX gateways) to deliver superior performance in high-bandwidth environments.

Administrators manage VSX via Check Point's Security Management server or Provider-1 Multi-Domain Server (MDS), delivering a unified management architecture that supports enterprises and service providers.

A VSX gateway contains a complete set of virtual devices that function as physical network components, such as Security Gateway, routers, switches, interfaces, and even network cables. Centrally managed, and incorporating key network resources internally, VSX allows businesses to deploy comprehensive firewall and VPN functionality, while reducing hardware investment and improving efficiency.

Figure 1 shows a typical configuration where VSX is deployed on a LAN. Each "virtual" Security Gateway is known as a Virtual System in VSX terminology, and functions as an independent firewall, protecting a specific network and providing the same security and networking functionality as a physical gateway.

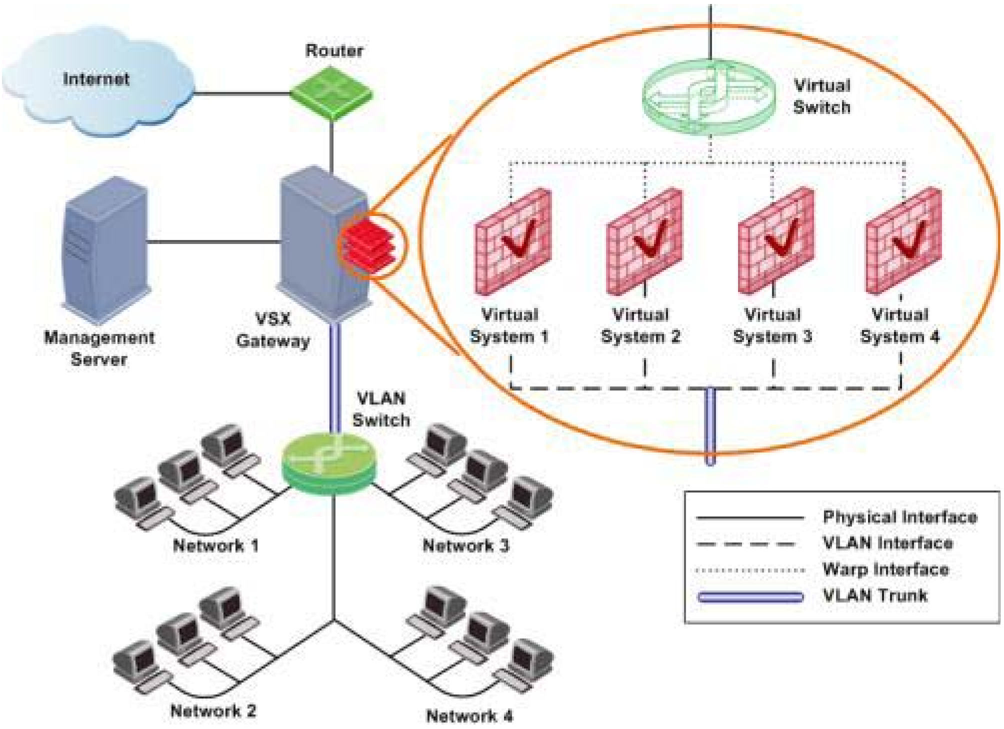


**Figure 1. Typical VSX Deployment – One VSX Gateway for Multiple Networks**

This deployment example shows:

- A VSX Gateway, which directs traffic to the Virtual System protecting the destination network. VSX virtual networks reside on a single configurable VSX gateway or cluster that defines and protects multiple independent networks, together with their virtual components.
- Four Virtual Systems, each handling packet traffic to and from discrete networks. Virtual Systems connect to internal protected networks using VLAN interfaces. The Virtual System inspects all traffic and passes or rejects it according to rules contained in its Rule Base.
- One Virtual Switch providing connectivity for all the Virtual Systems to the Internet router.
- "Virtual" interfaces and network cables (known as Warp Links) providing point-to-point connections between the Virtual Systems and the Virtual Switch.
- A VLAN switch, which is connected to the VSX gateway via an 802.1q VLAN trunk.

Figure 1 above illustrates how a single VSX gateway, in this case containing four Virtual Systems, protects all four networks. The use of VLANs provides scalability as well as granularity, allowing administrators to provision additional Virtual Systems and protected networks quickly and without impacting the existing IP address structure.

In contrast, physical networks consist of many hardware components. Figure 2 shows a deployment with four physical Security Gateways, each protecting a separate network. Each Security Gateway is a separate, physical machine that is hard-wired to the perimeter router and its corresponding network.

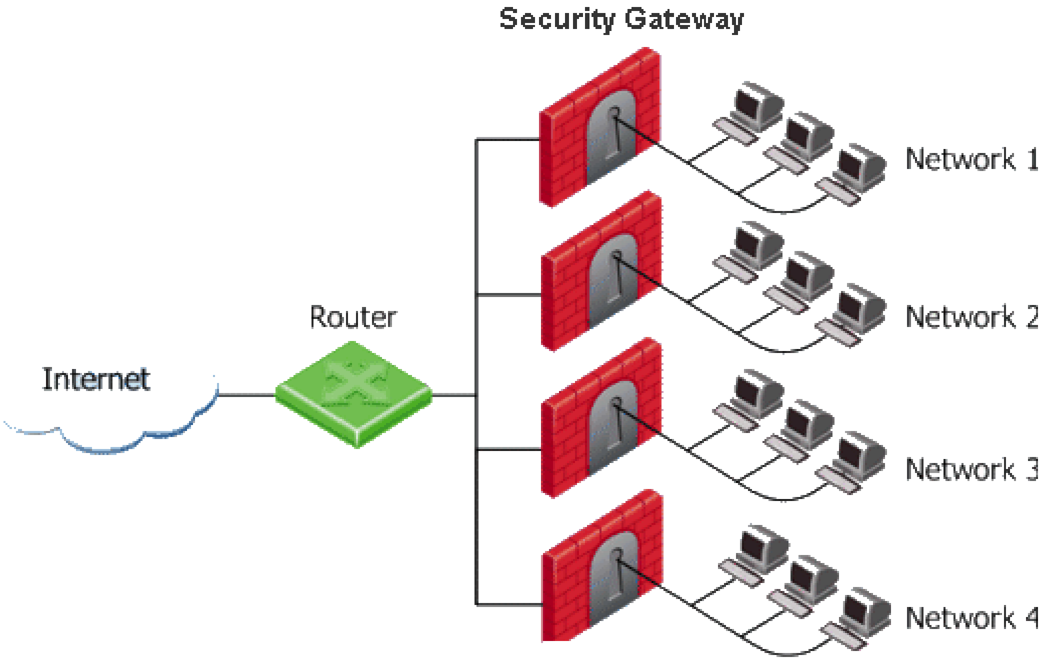


**Figure 2. Separate Physical Gateways Protecting Each Network**

### *Cryptographic Module*

Check Point VSX is a firmware module intended to run on any standard 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 Check Point VSX 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:

- Module firmware and Check Point SecurePlatform™ Operating System Version NGX R67
- General Purpose Computer (GPC) with dual Intel Xeon processors 2.33GHz

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.  The following figure shows the GPC model Check Point Power-1 9070 (2 x Intel Xeon 5410 "Harpertown" 2.33GHz 1333MHz FSB) used for testing.

Logically, the cryptographic boundary is composed of the Secure Platform Operating System integrated with the Check Point VSX 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 VSX, Network Layer IP interface | Network ports |
| Data output interface | User Interface (UI) for the VSX, Network Layer IP interface | Network ports |
| Control input interface | User Interface (UI) for the VSX, Network Layer IP interface | Keyboard ports, USB ports, serial ports, network ports, power switch |
| Status output interface | User Interface (UI) for the VSX, Network Layer IP interface, Log files | Network ports, serial ports, video 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
- Local Crypto-Officer
- Client User

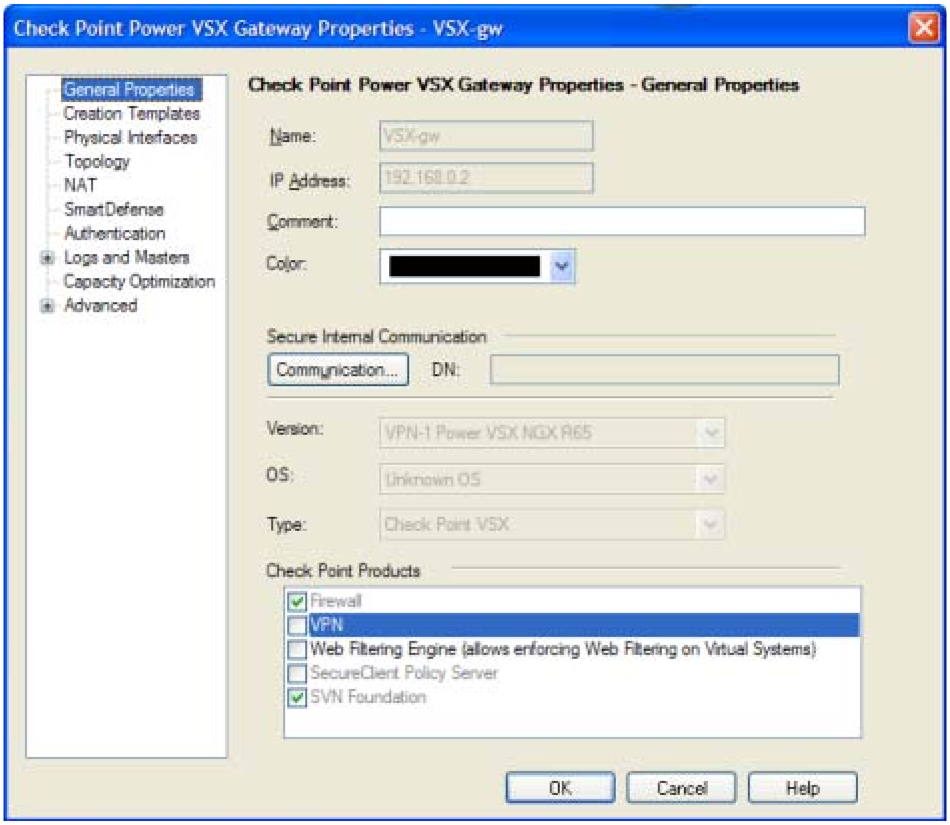
It uses digital signatures, pre-shared keys, and passwords for authentication.

The Local Crypto-Officer role is responsible for the installation, minimal configuration, and removal of the VSX. 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 VSX. 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.

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 VSX and the client using IPSec.

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.



Check Point Power VSX Gateway Properties - General Properties

Name: VSX-gw

IP Address: 192.168.0.2

Comment:

Color: ■

Secure Internal Communication

DN:

Version: VPN-1 Power VSX NGX R65

OS: Unknown OS

Type: Check Point VSX

Check Point Products

- ☑ Firewall
- ☐ VPN
- ☐ Web Filtering Engine (allows enforcing Web Filtering on Virtual Systems)
- ☐ SecureClient Policy Server
- ☑ SVN Foundation

**Figure 3. – Easy to Use Management Tools**

**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 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 Remote 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 800-90A seed key, 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 |
| Create and configure internal virtual TLS or IPsec and IKE devices. | Define external and internal network parameters such as IP addresses, VLAN tags, Net Mask, Default Gateway, | Virtual System Wizard inputs | Policy file defining the Virtual Device | Same parameters as for TLS and for IPsec and IKE (See Table 5) |
| 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 |

| Service | Description | Input | Output | Critical Security Parameter (CSP) Access |
|---|---|---|---|---|
| Management of keys | Configure the digital certificates and/or pre-shared keys for use by IPSec and IKE | Commands and configuration data (policy files) | Status of commands and configuration data (policy files) | RSA key pair for IKE (read/write access); pre-shared keys for IKE (read/write access) |
| Initialization of Secure Internal Communication (SIC) | Establish trust between management server and the VSX 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 |
| 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*

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

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

| Service | Description with CLI commands | Input | Output | CSP |
|---|---|---|---|---|
| FIPS mode | Switch to FIPS mode and enable integrity check. | Command and any options | Status of commands | None |
| Power-up self test. | | Power up the system or power cycle the system. | Module powers up without error. | AES-CMAC firmware integrity key, |
| Manage CLI settings | Switch between standard and expert CLI modes (expert);<br>Logout of the CLI (exit);<br>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) |

| Service | Description with CLI commands | Input | Output | CSP |
|---|---|---|---|---|
| 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);<br>view/change time (time);<br>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);<br>backup the system configuration (backup);<br>restore the system configuration (restore);<br>reboot the module (reboot);<br>shutdown the module (shutdown);<br>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);<br>Display top 15 processes ranked by CPU usage (top);<br>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);<br>trace the route of packets to a host (traceroute);<br>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);<br>show, set, or remove hostname to IP mappings (hosts);<br>show, configure, and store network interface settings (ifconfig);<br>configure virtual LAN interfaces (vconfig);<br>show and configure routing entries (route);<br>get or modify the system's host name (hostname);<br>get or set the system's domain name (domainname);<br>show, add, or remove domain name servers (dns);<br>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.<br>**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 access the module's IPSec and IKE services, Status Output services, and authenticates to the module using digital certificates or pre-shared keys (available for IKE).

Service descriptions and inputs/outputs are listed in Table 5:

| 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);<br>Diffie-Hellman key pair for IKE (read/write access);<br>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) |
| Status Output | The output indicators described for all services. | Service Inputs | Service Outputs | CSPs that are accessed by the services used. |

**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 (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). |
| RSA-based authentication (IKE) | RSA signing/verifying (role-based methodology) is used to authenticate to the module during IKE. This mechanism is as strong as the RSA algorithm using a key pair of either, 2048 and 4096 bits.<br>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 be 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. |
| Pre-shared key-based authentication (IKE) | SHA-1 HMAC generation/verification (role-based methodology) is used to authenticate to the module during IKE with pre-shared keys (at least 6 characters in length). |

**Table 6 – Estimated Strength of Authentication Mechanisms**

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

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

- IKE / HMAC: ( (94^6) / (100,000 *60) ) = 114,978 attempts per second
- RSA-based: ( (2^112) / (100,000 *60) ) = 8.6538281 × $10^{26}$ attempts per second

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

#### *Unauthenticated Services*

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

### *Physical Security*

The physical security of this module will not be tested. Check Point VSX 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 VSX does not provide a general-purpose operating system nor does it provide a mechanism to load new software.

The cryptographic module is firmware and was tested under the Check Point SecurePlatform™ operating system on the processor types provided by General Purpose Computing platforms in the configurations shown in section *Cryptographic Module* on page 6. 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 VSX’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.

VSX 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 VSX 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

| VSX Version R67.10 with R7x hotfix |
|---|
| Certificate #1837 |

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

| VSX Version R67.10 with R7x hotfix |
|---|
| Certificate #1190, #1191 |

**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).

| VSX Version R67.10 with R7x hotfix |
|---|
| Certificate #1091, #1092 |

**Data Hashing:**

Secure Hash Standard supporting SHA-1, SHA-256, SHA-384, and SHA-512, as per NIST PUB FIPS 180-3

| VSX Version R67.10 with R7x hotfix |
|---|
| Certificate #1617, #1618 |

### DRBG:

DRBG SP 800-90A Implementation

| VSX Version R67.10 with R7x hotfix |
|---|
| Certificate #147 |

HASH-DRBG with SHA-256 and a seed length of 440 bits in accordance with SP800-90A.

### Digital Signatures:

RSA – PKCS#1 and X9.31 key generation

| VSX Version R67.10 with R7x hotfix |
|---|
| Certificate #926 |

The RSA implementation is used both for signature generation and verification (per PKCS#1).

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.
- IPSec

### 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 module supports IKEv2 by default and IKEv1 for compatibility.

- In FIPS mode the Diffie-Hellman key agreement methodology implemented by the module (used by IKE) provides between 80 and 128 bits of encryption strength. Less than 80 bits is non-compliant with FIPS. Check Point recommends that only Diffie-

Hellman Groups 14 to 18 be used, to provide between 112 and 128 bits of encryption strength.

- The RSA key wrapping methodology (used by TLS), provides 112 bits or 150 bits of encryption strength.
- The module supports key entry though TLS using 3-key Triple-DES session keys. Triple-DES (Cert. #1191), key wrapping; key establishment methodology provides 112 bits of encryption strength)

In addition, the Check Point VSX 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 |
| RSA key pair for management | RSA key pair (2048 or 4096 bits) | Outside of crypto-boundary) | Stored on disk in P12 format ($CPDIR/conf/sic_cert.p12) (considered plaintext) | Authentication during TLS handshake |
| RSA key pair for IKE | RSA key pair (2048 or 4096 bits) | Outside of Crypto boundary | Stored on disk ($FWDIR$/database/fwauth.NDBX) – plaintext | Authentication during IKE |
| Pre-shared keys for IKE (SHA-1 HMAC) | IKE pre-shared key (48 – 512 bits) | Outside of crypto-boundary | Stored on disk ($FWDIR$/database/fwauth.NDB) - plaintext | Authentication during IKE |
| Diffie-Hellman key pairs | Diffie-Hellman key pairs (2048, 3072, 4096, 6144, 8192 bits) | Generated by IKE negotiations | RAM only (public parameters stored on disk ($FWDIR/database/objects.C and $FWDIR/state/local/FW1/local.objects) - plaintext | Key exchange during IKE |
| Session keys for IPSec | Triple-DES keys (168 bits), AES (128, 256 | Generated by IKE negotiations | RAM only - plaintext | Secure IPSec traffic |

| Key | Key type | Generation | Storage | Use |
|---|---|---|---|---|
| | Bits) | | | |
| Session keys for management | Triple-DES keys (168 bits) | 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 |
| Integrity check key | AES CMAC | Outside of crypto-boundary | Hard-coded into the cphash binary | Power-up integrity test |
| SP 800-90A Hash_DRGB 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 |
| 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 |

**Table 7 – Listing of the Module's CSPs**

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

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

The RSA key pair used by IKE is generated external to the module 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. The Local Crypto Officer configures the module 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.

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. Diffie-Hellman Groups 14 to 18 are used, to provide between 112 and 128 bits of encryption strength. The public parameters are exchanged over a secure TLS session established between the module and the management software. These parameters are deleted from the system after IKE key exchange is complete.

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

Session keys for 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 deterministic random bit generator (DRBG) 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 SHA-256 DRBG. 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**:

- Firmware Integrity Tests: The module checks the integrity of its various components using a 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
- Policy file integrity test (bypass mode test): the module performs a SHA-1 check value verification to ensure that the policy files are not modified.

**Conditional Self-tests**:

- Continuous DRBG Test: This test is constantly run to detect failure of the module’s random bit generator.
- Policy file integrity test (bypass mode test): the module performs a SHA-1 check value verification to ensure that the policy files are not modified.

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 firmware integrity check fails, the system enters the integrity check failure state, halts, and has to be restarted. If the firmware integrity check passes, the event is logged to the Check Point log. If the continuous DRBG 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 VSX 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 contauined in the ISO image that is configured during installation. All other cryptographic keys and CSPs are generated after the module is installed and initially powered up.

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

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

## *FIPS Mode Configuration*

### *Local Crypto-Officer Configuration Steps*

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

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

Module version VSX Version R67.10 with R7x hotfix includes support for Diffie-Hellman Groups up to Group 14 (2048 bit modulus) key sizes. Additional Diffie-Hellman Groups 15-18 (3072 bits to 8192 bits) must be configured during the initialization process by the Local Crypto-Officer before beginning the initialization of the module. Check Point recommends that Diffie-Hellman Groups 14 to 18 be used, The procedure for enabling the additional groups is obtainable from Check Point support SK27054 on the Check Point website.

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

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

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

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

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

   ```
   sysconfig
   ```

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

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

b. When prompted to select Check Point software to install on top of the operating system, select only “VPN-1 Power VSX”..

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

4. Reboot the module.

5. Login to the console.

6. Switch to expert mode.

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

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

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.disabled to /etc/cpshell/fips.cfg

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. Copy $CPDIR/conf/fips_sic_policy.conf to $CPDIR/conf/sic_policy.conf

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

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 firmware integrity check.

*Management Station Configuration Steps*

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

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

   ```
   cpstop
   ```

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

3. Copy $CPDIR/conf/fips_sic_policy.conf to $CPDIR/conf/sic_policy.conf

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

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

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

   ```
   cpstart
   ```

### *Remote Crypto-Officer Configuration Guidelines*

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

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

**Data Encryption**

- Triple-DES
- AES

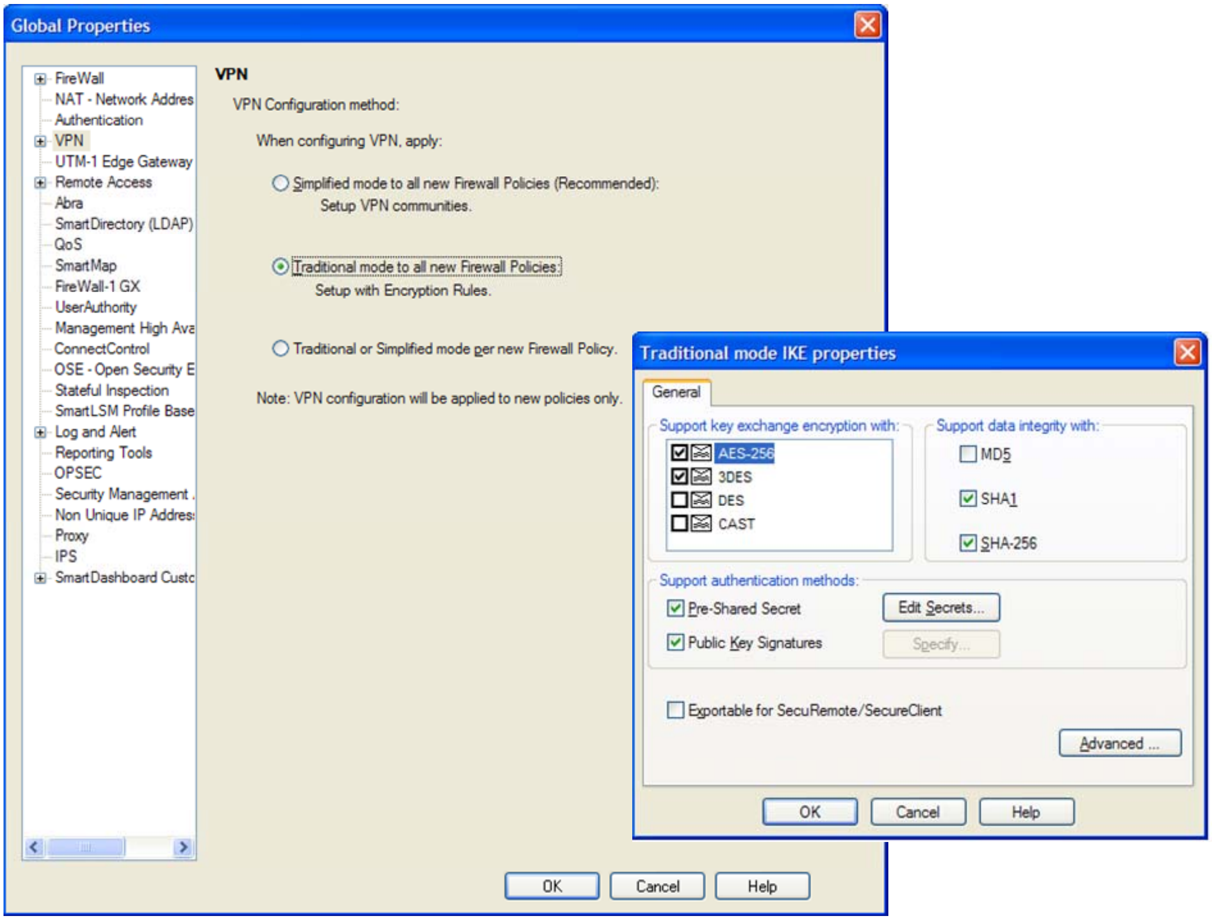
**Data Packet Integrity**

- HMAC with SHA1

**Authentication**

- Certificates
- Pre-shared keys

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



VPN

VPN Configuration method:

When configuring VPN, apply:

○ Simplified mode to all new Firewall Policies (Recommended):
Setup VPN communities.

● Traditional mode to all new Firewall Policies:
Setup with Encryption Rules.

○ Traditional or Simplified mode per new Firewall Policy.

Note: VPN configuration will be applied to new policies only.

Traditional mode IKE properties

Support key exchange encryption with:

☑ AES-256
☑ 3DES
□ DES
□ CAST

Support data integrity with:

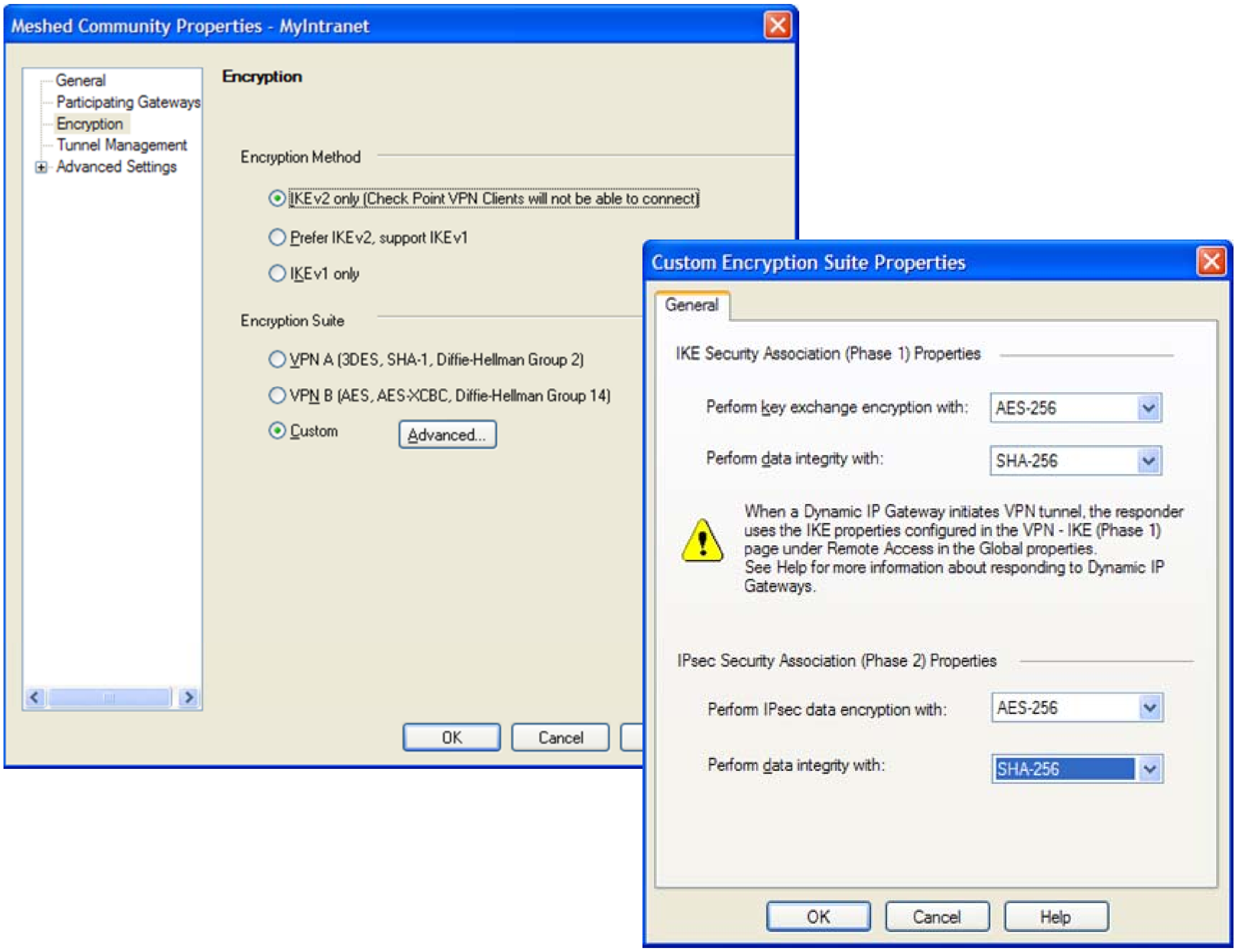
□ MD5
☑ SHA1
☑ SHA-256

Support authentication methods:

☑ Pre-Shared Secret
☑ Public Key Signatures

□ Exportable for SecuRemote/SecureClient

Figure 4 – In Traditional Mode, Select Only FIPS-Approved Algorithms for use with IKE



Meshed Community Properties - MyIntranet

Encryption

Encryption Method

- ● IKEv2 only (Check Point VPN Clients will not be able to connect)
- ○ Prefer IKEv2, support IKEv1
- ○ IKEv1 only

Encryption Suite

- ○ VPN A (3DES, SHA-1, Diffie-Hellman Group 2)
- ○ VPN B (AES, AES-XCBC, Diffie-Hellman Group 14)
- ● Custom

Custom Encryption Suite Properties

IKE Security Association (Phase 1) Properties

Perform key exchange encryption with: AES-256

Perform data integrity with: SHA-256

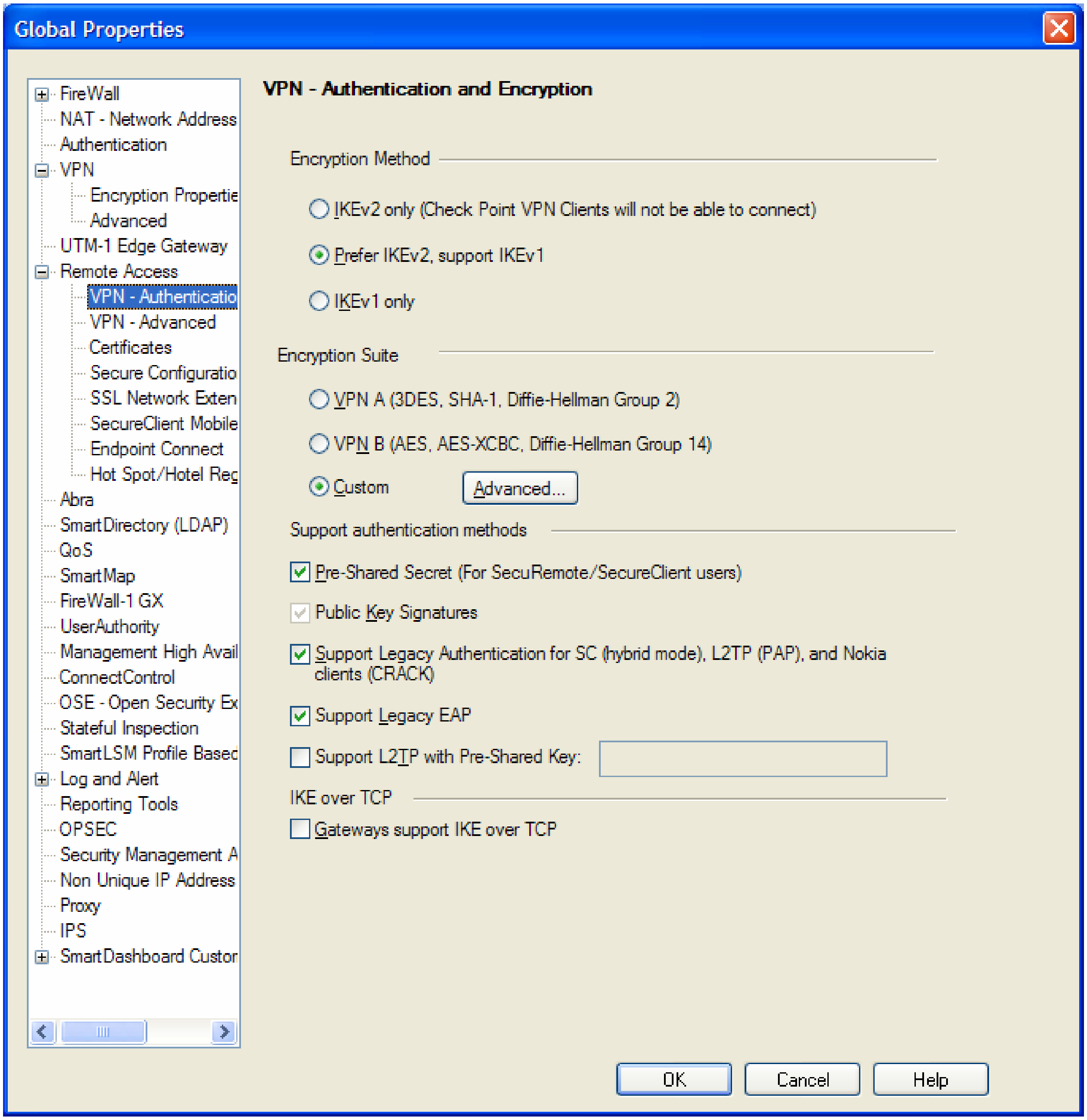
When a Dynamic IP Gateway initiates VPN tunnel, the responder uses the IKE properties configured in the VPN - IKE (Phase 1) page under Remote Access in the Global properties.
See Help for more information about responding to Dynamic IP Gateways.

IPsec Security Association (Phase 2) Properties

Perform IPsec data encryption with: AES-256

Perform data integrity with: SHA-256

**Figure 5 – In Meshed Communities Select Only FIPS-Approved Algorithms for use with IKE**



VPN - Authentication and Encryption

Encryption Method

○ IKEv2 only (Check Point VPN Clients will not be able to connect)

● Prefer IKEv2, support IKEv1

○ IKEv1 only

Encryption Suite

○ VPN A (3DES, SHA-1, Diffie-Hellman Group 2)

○ VPN B (AES, AES-XCBC, Diffie-Hellman Group 14)

● Custom  Advanced...

Support authentication methods

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

☑ Public Key Signatures

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

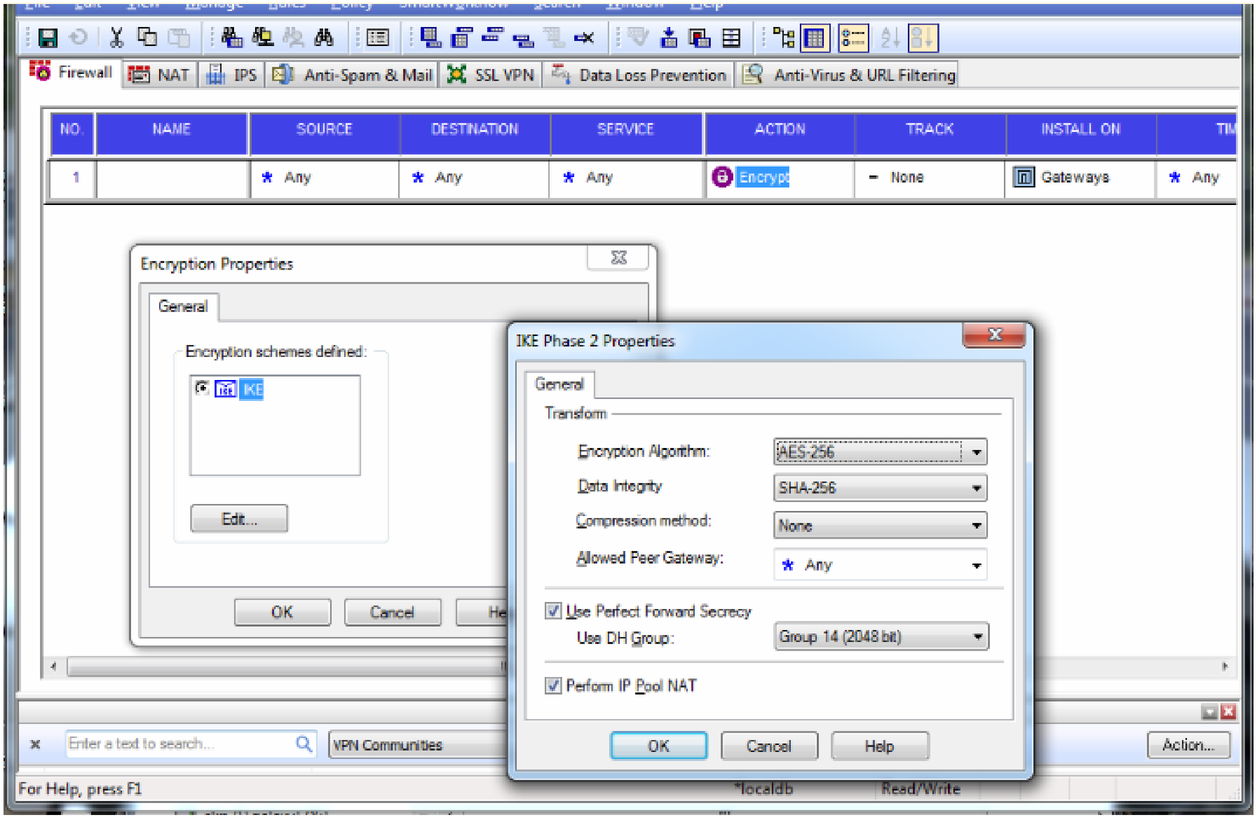
☑ Support Legacy EAP

□ Support L2TP with Pre-Shared Key:

IKE over TCP

□ Gateways support IKE over TCP

**Figure 6 – Only Pre-Shared Keys or Digital Certificates may be used to Authenticate Clients**



| NO. | NAME | SOURCE | DESTINATION | SERVICE | ACTION | TRACK | INSTALL ON | TI |
|---|---|---|---|---|---|---|---|---|
| 1 |  | * Any | * Any | * Any | Encrypt | − None | Gateways | * Any |

Encryption Properties

General

Encryption schemes defined:

● IKE

IKE Phase 2 Properties

General

Transform

Encryption Algorithm: AES-256

Data Integrity: SHA-256

Compression method: None

Allowed Peer Gateway: * Any

☑ Use Perfect Forward Secrecy

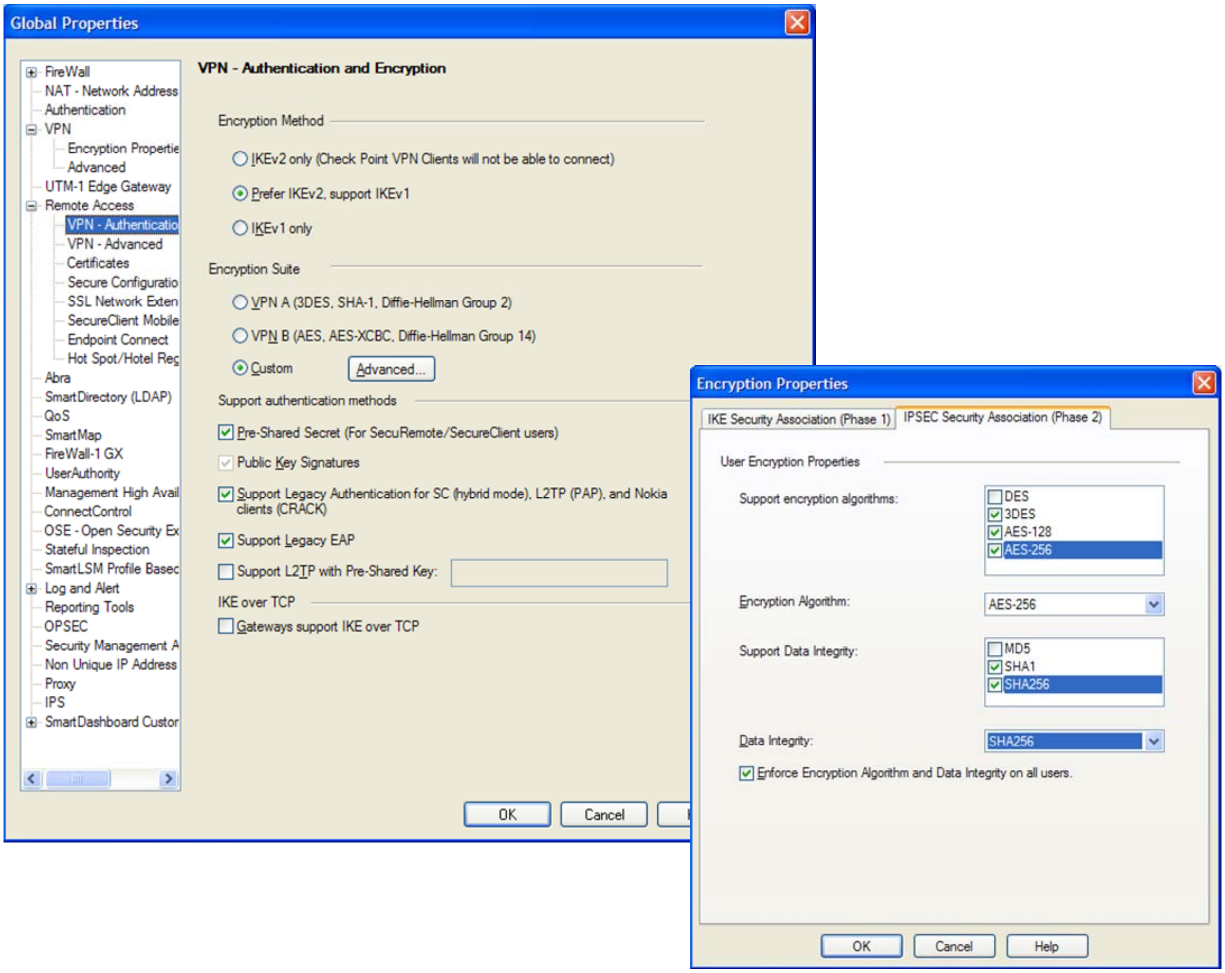
Use DH Group: Group 14 (2048 bit)

☑ Perform IP Pool NAT

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

Notes:

1. Diffie-Hellman Group 14 (2048-bits) provides 112 bits of encryption strength. Check Point recommends the use of Diffie-Hellman groups 14 or higher, to provide 112 or more bits of encryption strength.



VPN - Authentication and Encryption

Encryption Method

○ IKEv2 only (Check Point VPN Clients will not be able to connect)

● Prefer IKEv2, support IKEv1

○ IKEv1 only

Encryption Suite

○ VPN A (3DES, SHA-1, Diffie-Hellman Group 2)

○ VPN B (AES, AES-XCBC, Diffie-Hellman Group 14)

● Custom   Advanced...

Support authentication methods

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

☑ Public Key Signatures

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

☑ Support Legacy EAP

□ Support L2TP with Pre-Shared Key:

IKE over TCP

□ Gateways support IKE over TCP

User Encryption Properties

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

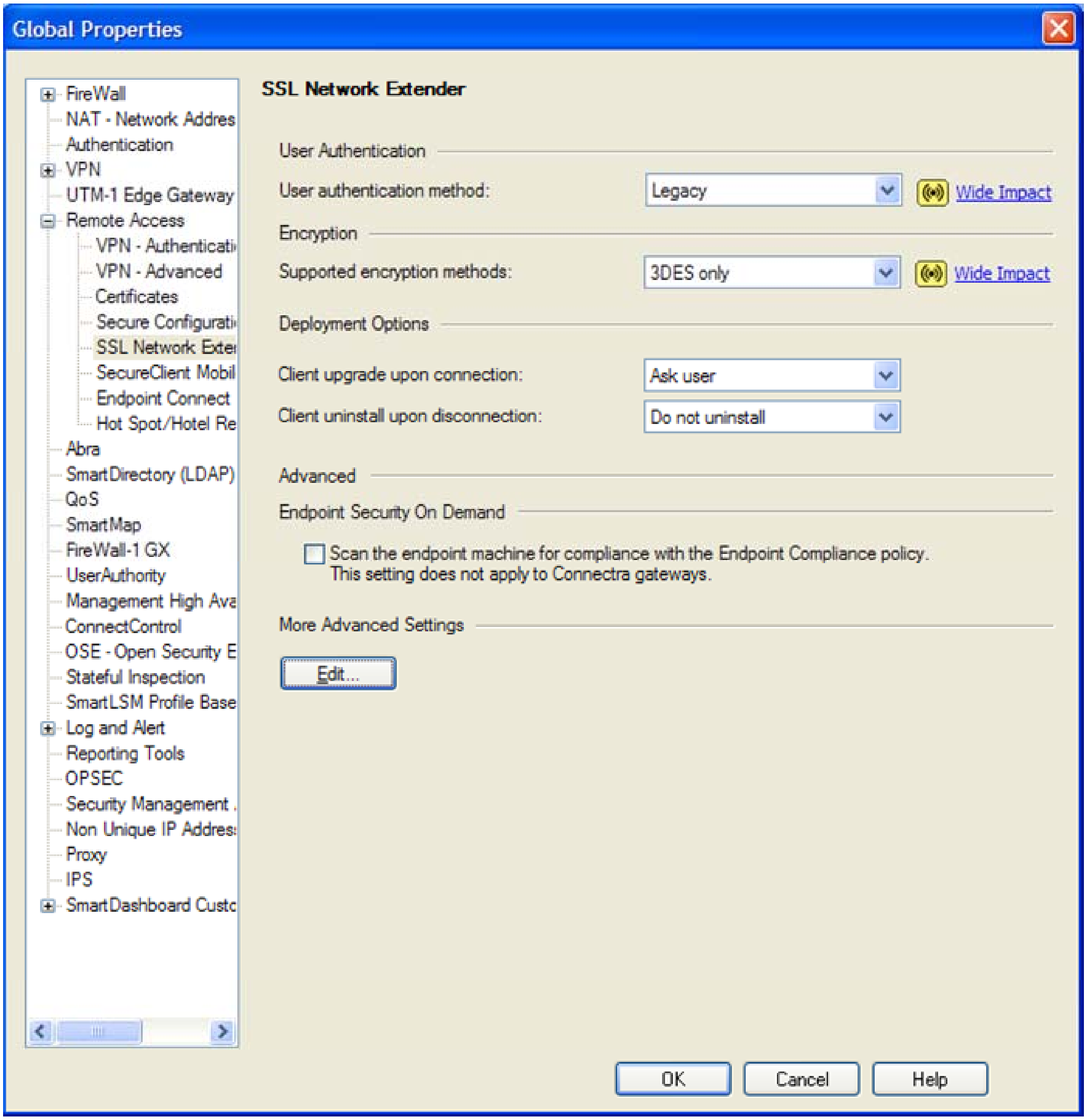
Encryption Algorithm: AES-256

Support Data Integrity:
□ MD5
☑ SHA1
☑ SHA256

Data Integrity: SHA256

☑ Enforce Encryption Algorithm and Data Integrity on all users.

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



SSL Network Extender

User Authentication

User authentication method: Legacy

Encryption

Supported encryption methods: 3DES only

Deployment Options

Client upgrade upon connection: Ask user

Client uninstall upon disconnection: Do not uninstall

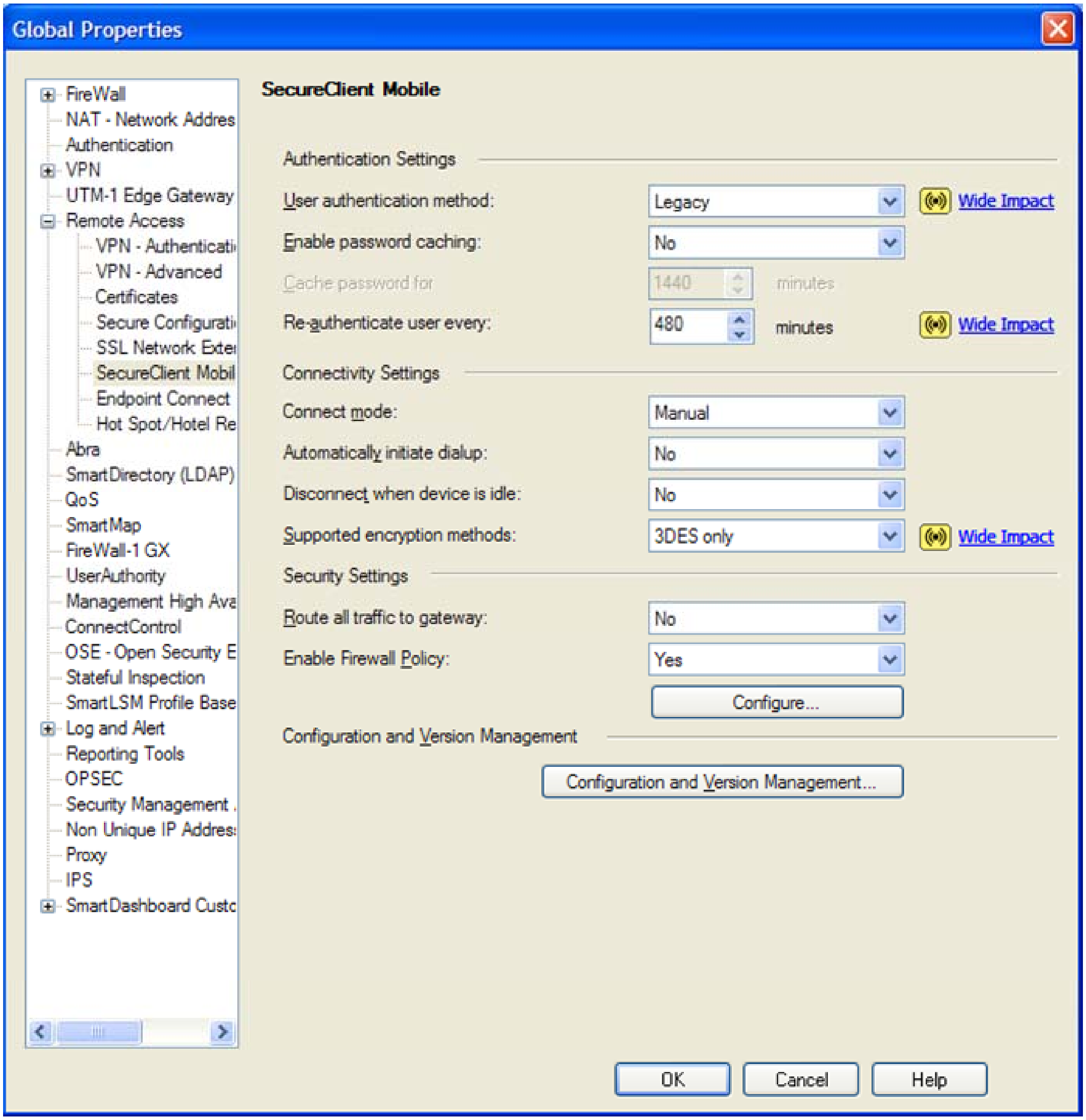
Advanced

Endpoint Security On Demand

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

More Advanced Settings

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



Global Properties

SecureClient Mobile

Authentication Settings

User authentication method: Legacy (Wide Impact)

Enable password caching: No

Cache password for 1440 minutes

Re-authenticate user every: 480 minutes (Wide Impact)

Connectivity Settings

Connect mode: Manual

Automatically initiate dialup: No

Disconnect when device is idle: No

Supported encryption methods: 3DES only (Wide Impact)

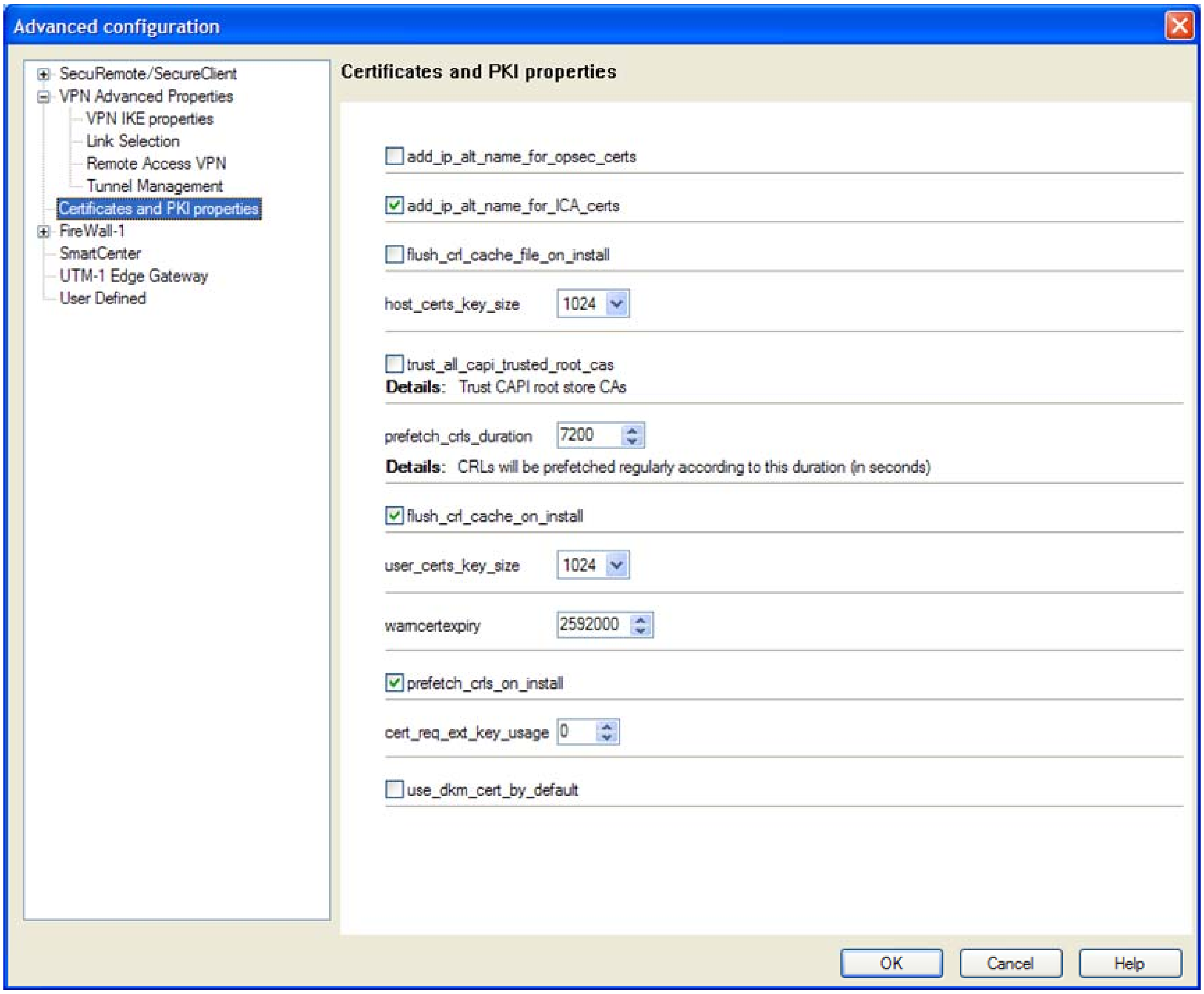
Security Settings

Route all traffic to gateway: No

Enable Firewall Policy: Yes

Configuration and Version Management

**Figure 10 – Only FIPS-Approved Algorithms may be used with TLS**



Certificates and PKI properties

□ add_ip_alt_name_for_opsec_certs

☑ add_ip_alt_name_for_ICA_certs

□ flush_crl_cache_file_on_install

host_certs_key_size 1024

□ trust_all_capi_trusted_root_cas
**Details:** Trust CAPI root store CAs

prefetch_crls_duration 7200
**Details:** CRLs will be prefetched regularly according to this duration (in seconds)

☑ flush_crl_cache_on_install

user_certs_key_size 1024

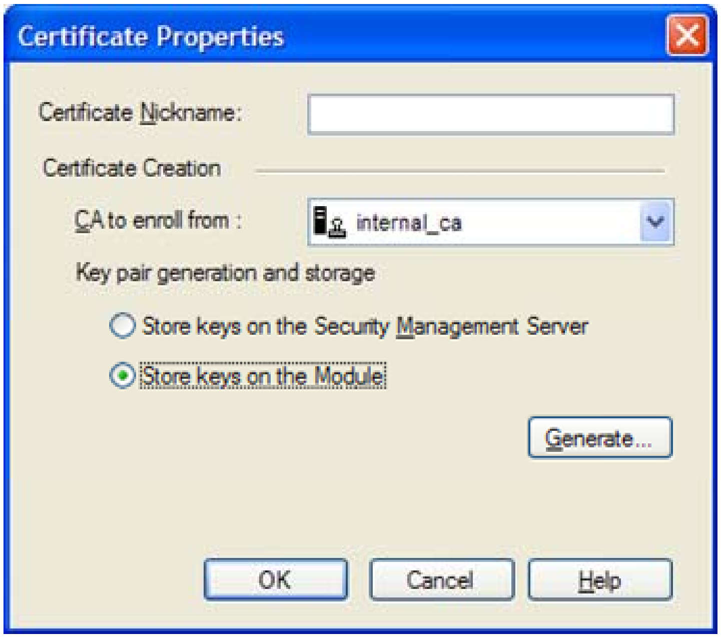
warncertexpiry 2592000

☑ prefetch_crls_on_install

cert_req_ext_key_usage 0

□ use_dkm_cert_by_default

**Figure 11 – Configuring the module to enable Distributed Key Management (DKM) globally**



Certificate Properties

Certificate Nickname:

Certificate Creation

CA to enroll from : internal_ca

Key pair generation and storage

○ Store keys on the Security Management Server

● Store keys on the Module

**Figure 12 – Configuring the module to generate RSA keys with DKM on a per-certificate basis**

### *Crypto-Officer Guidance*

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 VSX user manuals.

The Local Crypto-Officer receives the module in a shrink wrapped package containing a CD-ROM with the VSX 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 password must be changed immediately upon logging into the module after installation.

The Local 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.

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

#### *Management*

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

The 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 Remote or Local 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.

### *User Guidance*

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

## ACRONYMS

| | |
|---|---|
| AH | Authentication Header |
| ANSI | American National Standards Institute |
| CBC | Cipher Block Chaining |
| CLI | Command Line Interface |
| CRC | Cyclic Redundancy Check |
| CSP | Critical Security Parameter |
| DRBG | Deterministic Random Bit Generator. Also known as a pseudorandom number generator (PRNG). |
| DSA | Digital Signature Standard |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| ESP | Encapsulating Security Payload |
| FCC | Federal Communication Commission |
| FIPS | Federal Information Processing Standard |
| FP | Feature Pack |
| HF | Hot Fix |
| IKE | Internet Key Exchange |
| IPSec | IP Security |
| KAT | Known Answer Test |
| LED | Light Emitting Diode |
| MAC | Message Authentication Code |
| NG | Next Generation |
| NIST | National Institute of Standards and Technology |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| PC | Personal Computer |
| 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 |

## APPENDIX: DEFINING ADVANCED DIFFIE-HELLMAN GROUPS FOR IKE

Based on the following Check Point support article:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk27054

Solution ID: sk27054
Product: VSX, Security Gateway
Version: NGX R61, NGX R67, NGX R65, NGX R62, NGX R60, R70, R71, R75
OS: All
Last Modified:22-May-2011

### *Cause*

By default, VPN-1 Pro supports Diffie-Hellman groups 1, 2 and 5. RFC 3526 defines new DH groups, numbered 14 to 18. These groups use longer modulus, and are expected to become widely used in the next few years. While VPN-1 Pro is able to use these groups starting with VPN-1 NG with Application Intelligence R55 HFA 10, these new groups are not yet defined in the database. This document describes how to define these objects in the database.

### *Solution*

The Diffie-Hellman prime numbers are presented as complete strings. The excessive horizontal formatting of this article is due to the length of these strings. Follow the below instructions to define groups 14 through 18. Group 24 is added and supported in R7x Use cut-and-paste to copy the DH prime number.

*To define Diffie-Hellman group 14:*

1. Close SmartDashboard.
2. Open 'GuiDBedit'.
3. In the top left corner, go to 'VPN -> encryption'.
4. Right-click the top right window and choose "New..."
5. Under "Class" choose "IKE_Diffie_Hellman_parameters_object".
6. Under Object, type "Group 14 (2048 bit)".
7. Click 'OK'.
8. Set "DH_group_number" to 14.
9. Set "mod"->"value" to the MODP string below.
   NOTE: cut and paste into 'GuiDBedit'.
10. Set "modsize" to 2048.
11. Set "private_key_length" to 256.
12. Set "root"->"value" to "02" (zero-two).
13. Set "rootsize" to 2.
14. "type" should be set to "IKE_DH_parameters".
15. Save and exit.

Group 14's MODP:

```
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139
B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B57662
5E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE64928665
1ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62
F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE
39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956A
E515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF
```

*To define Diffie-Hellman group 15:*

1. Close SmartDashBoard.
2. Open GuiDBEdit.
3. In the top left corner, go to VPN->encryption.
4. Right-click the top right window and choose "New..."
5. Under "Class" choose "IKE_Diffie_Hellman_parameters_object".
6. Under "Object", type "Group 15 (3072 bit)".
7. Click 'OK'.
8. Set "DH_group_number" to 15.
9. Set "mod"->"value" to the MODP string below.
   NOTE: cut and paste into 'GuiDBEdit'.
10. Set "modsize" to 3072.
11. Set "private_key_length" to 256.
12. Set "root"->"value" to "02" (zero-two).
13. Set "rootsize" to 2.
14. "type" should be set to "IKE_DH_parameters".
15. Save and exit.

Group 15's MODP:

```
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139
B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B57662
5E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE64928665
1ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62
F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE
39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956A
E515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458D
BEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D226
1AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C77098
8C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
```

*To define Diffie-Hellman group 16:*

1. Close SmartDashBoard.
2. Open 'GuiDBEdit'.
3. In the top left corner, go to VPN->encryption.
4. Right-click the top right window and choose "New..."
5. Under "Class" choose "IKE_Diffie_Hellman_parameters_object".
6. Under Object, type "Group 16 (4096 bit)".

7. Click 'OK'.
8. Set "DH_group_number" to 16.
9. Set "mod"->"value" to the MODP string below.
   NOTE: cut and paste into 'GuiDBEdit'.
10. Set "modsize" to 4096.
11. Set "private_key_length" to 256.
12. Set "root"->"value" to "02" (zero-two).
13. Set "rootsize" to 2.
14. "type" should be set to "IKE_DH_parameters".
15. Save and exit.

Group 16's MODP:

```
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139
B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B57662
5E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE64928665
1ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62
F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE
39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956A
E515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458D
BEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D226
1AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C77098
8C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788
719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF
92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2
D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93
4063199FFFFFFFFFFFFFFFF
```

*To define Diffie-Hellman group 17:*

1. Close SmartDashBoard.
2. Open 'GuiDBEdit'.
3. In the top left corner, go to VPN->encryption.
4. Right-click the top right window and choose "New..."
5. Under "Class" choose "IKE_Diffie_Hellman_parameters_object".
6. Under Object, type "Group 17 (6144 bit)".
7. Click 'OK'.
8. Set "DH_group_number" to 17.
9. Set "mod"->"value" to the MODP string below.
   NOTE: cut and paste into 'GuiDBEdit'.
10. Set "modsize" to 6144.
11. Set "private_key_length" to 256.
12. Set "root"->"value" to "02" (zero-two).
13. Set "rootsize" to 2.
14. "type" should be set to "IKE_DH_parameters".
15. Save and exit.

Group 17's MODP:

```
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139
B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B57662
5E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE64928665
1ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62
F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE
39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956A
E515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458D
BEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D226
1AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C77098
8C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788
719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF
92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2
D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93
402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB38
2F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7
F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03
F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC8
8BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF2
9BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D
76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
```

*To define Diffie-Hellman group 18:*

1. Close SmartDashBoard.
2. Open 'GuiDBEdit'.
3. In the top left corner, go to VPN->encryption.
4. Right-click the top right window and choose "New..."
5. Under "Class" choose "IKE_Diffie_Hellman_parameters_object".
6. Under Object, type "Group 18 (8192 bit)".
7. Click 'OK'.
8. Set "DH_group_number" to 18.
9. Set "mod"->"value" to the MODP string below.
   NOTE: cut and paste into 'GuiDBEdit'.
10. Set "modsize" to 8192.
11. Set "private_key_length" to 256.
12. Set "root"->"value" to "02" (zero-two).
13. Set "rootsize" to 2.
14. "type" should be set to "IKE_DH_parameters".
15. Save and exit.

Group 18's MODP:

```
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139
B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B57662
5E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE64928665
1ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62
F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE
39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956A
E515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458D
BEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D226
1AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C77098
```

```
8C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788
719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF
92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2
D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93
402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB38
2F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7
F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03
F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC8
8BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF2
9BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D
76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E43877
7CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663
AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C
0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5
BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC5
0846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F9240094
38B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC8
1F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFFF
```