Check Point
VPN-1 Gateway Next Generation FP1

VPN-1 GATEWAY
Secure Virtual Network Architecture

FIPS 140-1 Non-Proprietary Security Policy

Level 2 Validation

September 2001

Table of Contents

1 INTRODUCTION 3

1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 DOCUMENT ORGANIZATION 3

2 CHECK POINT VPN-1 GATEWAY NEXT GENERATION FP1 4

2.1 PLATFORM SECURITY WITH WELL-DEFINED INTERFACES 5
2.2 ROLES AND SERVICES 6
2.2.1 Remote Crypto-Officer Role 7
2.2.2 Local Crypto-Officer Role 8
2.2.3 Client User Role 8
2.3 SECURE CRYPTOGRAPHIC KEY MANAGEMENT 9
2.4 STRONG CRYPTOGRAPHIC ALGORITHMS 10
2.5 CONTINUOUS SELF-TESTING 11
2.6 SECURE MANAGEMENT SOFTWARE 12

3 FIPS 140-1 LEVEL 2 COMPLIANT MODE 14

1 INTRODUCTION

1.1 Purpose

This is a non-Proprietary FIPS 140-1 Security Policy for the Check Point VPN-1 Gateway Next Generation (NG). It describes how the Check Point VPN-1 Gateway NG meets all FIPS 140-1 Level-2 requirements. The Security Policy was prepared as part of the level 2 FIPS 140-1 validation of the Check Point VPN-1 Gateway NG.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1) is a U.S. government standard entitled "Security Requirements for Cryptographic Modules". This standard mandates a set of strict design and documentation requirements that hardware and software cryptographic module must meet in order to be validated by the U.S. national institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada.

1.2 References

This FIPS 140-1 Security Policy describes features and design of Check Point VPN-1 Gateway NG components using the technical terms of FIPS 140-1.

- For more information on the FIPS 140-1 standard and validation program readers are referred to the NIST website at http://csrc.nist.gov/cryptval/.

- For more information on the Check Point product line, please visit the Check Point web site at http://www.CheckPoint.com.

1.3 Document Organization

This section provides a general introduction to the Security Policy. Section 2 introduces the Check Point software package. Section 3 discusses the Check Point VPN-1 Gateway NG and how it meets FIPS 140-1.

Corsec Security, Inc. under contract to Check Point prepared this document. This document may be freely distributed whole and intact according to the copyright notice above.

2 Check Point VPN-1 Gateway Next Generation FP1

Check Point VPN-1 Gateway Next Generation (NG) is a tightly integrated software solution combining the market-leading FireWall-1® security suite with sophisticated VPN technologies. The cornerstone of Check Point's Secure Virtual Network architecture, VPN-1 Gateway NG meets the demanding requirements of Internet, intranet, and extranet VPNs by providing secure connectivity to corporate networks, remote and mobile users, satellite offices, and key partners. Check Point VPN-1 Gateway NG software may be deployed on a range of platforms for maximum flexibility and scalability.

Check Point VPN-1 Gateway NG provides built-in resiliency for remote access VPNs. Extranets are made possible through support for industry standards as well as all leading PKI products and services. For superior performance, VPN-1 Gateway solutions may also include bandwidth management, compression, and hardware-based VPN acceleration. FireWall-1 offers features that include access control, client and session authentication, network address translation, and logging. Plus, it uses Check Point's patented Stateful Inspection technology and is administered within Check Point's centralized policy management and distributed deployment framework.

Check Point VPN-1/FireWall-1™ is designed to allow secure access to the organization's resources to multiple users over an unsecured TCP/IP network. The Check Point VPN-1/FireWall-1™ is installed on the corporate server and secures connections to other Gateways or Clients. It performs all the required security functions and provides the following high-level functionality:

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

A Virtual Private Network (VPN) protects communications between remote access users to their organizations using the Internet or between two networks through peer gateways. This advanced technology lets the organization extend its network services over the Internet to branch offices, nomadic and remote clients, creating a secured private WAN (Wide Area Network) over the unsecured Internet.

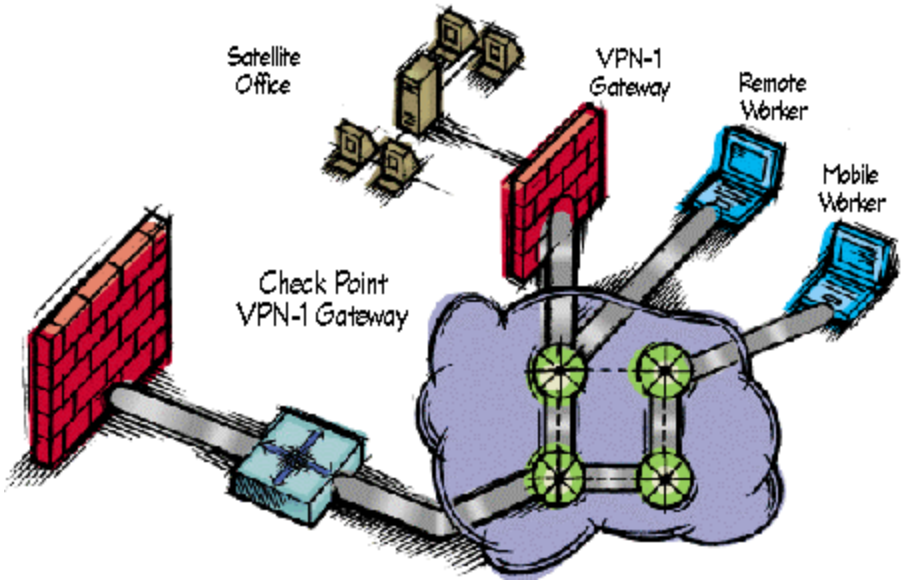

Figure 1 – Check Point VPN-1 Gateway Next Generation in the Real World

2.1 Platform Security with Well-Defined Interfaces

Check Point VPN-1 Gateway NG is considered to be a multi-chip standalone module for FIPS 140-1. The module functions on a variety of operating systems including Microsoft Windows NT 4 and 2000, Sun Solaris 7 and 8, and Red Hat Linux 6.2 and 7.0. For added security, the Check Point VPN-1 Gateway even operates on the ITSEC–evaluated Microsoft Windows NT v4.0 SP6a with the appropriate PC hardware (as defined in the ITSEC evaluation). In addition to the security provided by this certified platform, tamper-evident labels can be affixed to the PC's case, meeting FIPS 140-1 level 2 requirements by giving indication of tamper attempts. This is detailed in section 3 of this document.

The physical interfaces of the module include the computer keyboard, CD-ROM drive, floppy drive, mouse, screen and ports. The Check Point software logically interfaces to the network through the network-level after the information has been accessed through those physical interfaces.

The logical interfaces in the Check Point software (and the physical interfaces they cross) are:

FIPS 140-1 Logical Interface	Logical Interface	Physical Interface
Data input interface	User Interface (UI) for the Check Point VPN-1/FW-1 Gateway utilities and services, Data Link Layer interface, UI for the Operating System	Keyboard, network ports, disk drive, CD-ROM
Data output interface	UI for the Check Point VPN-1/FW-1 Gateway utilities, Data Link Layer interface, UI	Network ports, monitor, disk drive

	for the Operating System	
Control input interface	UI for the Check Point VPN-1/FW-1 Gateway utilities, Data Link Layer interface, UI for the Operating System	Keyboard, mouse, network ports
Status output interface	UI for the Check PointVPN-1/FW-1 Gateway utilities and services, Data Link Layer, UI for the Operating System	Network ports, monitor
Power interface	Power interface	Power connector

Table 1 – Mapping Physical and Logical Interfaces to FIPS 140-1 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 data, control and status traffic over the Network ports by analyzing the packets header information and contents.

The machines used in the ITSEC Level E3 evaluation have been tested and meet applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and electromagnetic Compatibility (EMC) requirements for home use as defined in Subpart B of FCC part 15.

2.2 Roles and Services

The module supports three distinct roles using Digital signatures and passwords for authentication: Client User, Local Crypto-Officer, and remote Crypto-Officer roles.

The Remote and Local Crypto-Officer roles perform primary configuration of the Check Point VPN-1/FireWall-1. After authenticating, the Crypto-Officer uses a powerful set of management tools to configure and monitor the Check Point VPN-1 Gateway. These tools can be installed locally, on the device running Check Point VPN-1 Gateway, or remotely. The remote management session uses TLS to ensure security.

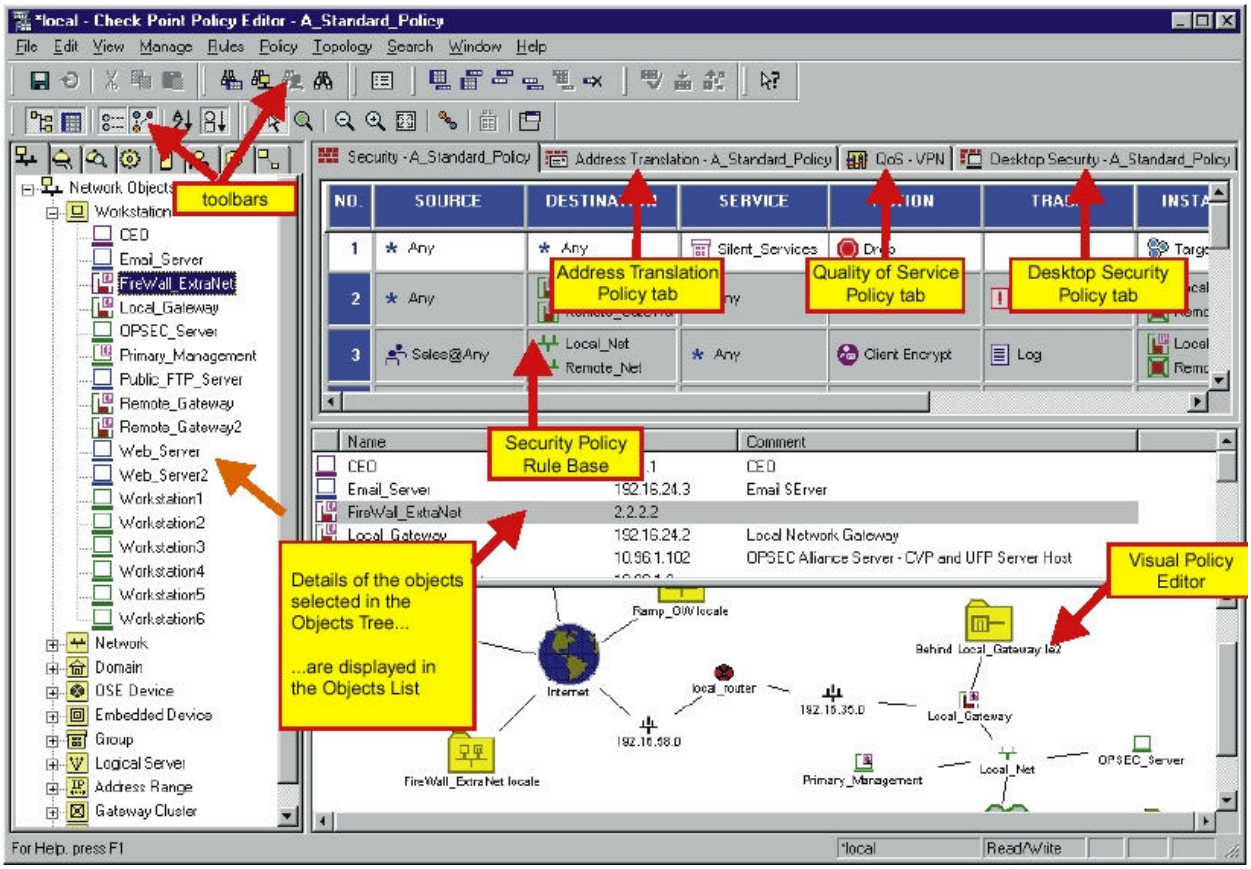

Figure 2 – Easy to Use Management Tools

The User role is for clients that are accessing the Check Point VPN-1 Gateway NG 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 VPN-1 Gateway and the client using IPSec. Of note, the Check Point VPN-1 Gateway NG can itself act as a User when establishing tunnels to other Check Point VPN-1 Gateways.

2.2.1 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 station (i.e., Remote Crypto-Officer) authenticates to the module through TLS using digital certificates. After authenticating, the Remote Crypto-Officers uses Check Point management software to manage the module over the secure TLS session. The following services are available to the Remote Crypto-Officer:

- *Create and Manipulate Network Objects*: Define your network as a series of objects such as workstations, networks, domains, etc. With various properties for each object, the Crypto-Officer has a wide-variety of configuration options. By modifying single objects or groupings of objects, the Crypto-Officer has control with varying granularity.
- *Create and Configure Users/User Groups*: Defining users and user groups allows the Crypto-Officer to create permission for individual users or a whole group of users.

Permissions such as access hours, user priority, authentication mechanisms, protocols allowed, filters applied, and types of encryption allowed are available to the Crypto-Officer. As with network objects, this provides the Crypto-Officer with varying granularity.

- *Define and Implement Security Polices:* Define and implement security policies that are applied to the network and Users. A set of rules is configured and installed to the Check Point VPN-1 Gateway module. These rules 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.
- *Management of keys*: Configure the digital certificates and/or preshared keys for use by IPSec and IKE for authentication. Besides manually managing keys, the Crypto-Officer also uses the key management involved with TLS.
- *Initialization of Secure Internal Communication (SIC)*: Establish trust between management station and the Check Point VPN-1 Gateway module to allow configuration of the module's services
- *Monitoring:* Provides detailed information for both monitoring of connection activities and the system status. This information can be viewed using the Check Point Log Viewer and System Status applications.

2.2.2 Local Crypto-Officer Role

The role of the Local Crypto-Officer is the same as that of the Remote Crypto-Officer. Local operators authenticated to the module through the Operating System, 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. The following services are available to the Local Crypto-Officer:

- *Installation and removal of the VPN-1 Gateway software:* By uninstalling the module and reformatting the partition or hard drive containing the VPN-1 Gateway software, the Local Crypto-Officer can destroy all keys stored on the module.
- *Initialization of the Check Point VPN-1 Gateway software*: Install licenses, configure the SIC one time password, etc.
- *System Administration*: Modify the criteria-based rules, start/stop VPN-1 services, bind/unbind VPN-1 kernel modules, configure the Operating System, etc. The Local Crypto-Officer can use command line utilities and text editors to modify various configurations settings of the module.
- *Access control*: Set up the local Crypto-Officers and partially configure remote Crypto-Officers (i.e., initialization of SIC). The Local Crypto-Officer defines the users and permissions associated with the Operating System.
- *Monitoring:* Viewing logs and system status through local tools and the Operating System

2.2.3 Client User Role

The User role includes accessing IPSec services on the Check Point VPN-1 Gateway. This involves the following abilities:

- *Authentication:* Use IKE with a password (pre-shared key) or a digital certificate to authenticate to the module. Remote access users can also use other methods such a Secure ID.
- *Key management*: Use IPSec to generate (through IKE) keys, destroy keys, and managed keys for connections.
- *Secure Sessions:* Establish, maintain, and terminate secure connections to the VPN-1 module using IPSec.

2.3 Secure Cryptographic Key Management

The following table summaries the module's keys:

Key	Key type	Storage	Use
RSA key pair for management	RSA key pair (1024 bits)	Stored on disk.	Authentication during TLS handshake.
RSA key pair for IKE	RSA key pair (1024 bits)	Stored on disk.	Authentication during IKE.
Preshared keys for IKE	IKE preshared key	Stored on disk.	Authentication during IKE.
Session keys for IPSec	DES/TDES keys (56/128 bits)	RAM only.	Secure IPSec traffic.
Session keys for management	DES/TDES keys (56/128 bits)	Cached to disk.	Secure TLS traffic (SIC).

Table 2 – Summary of the VPN-1 Gateway's Keys

The module implements IPSec key management in compliance with IKE (Internet Key Exchange), negotiating Security Associations (SAs) and agreeing upon session keys. Diffie-Hellman (DH) is used by IKE to perform the key exchange. The implementation supports Main and Aggressive modes using pre-shared secret keys or digital certificates for authentication. RSA capabilities for digital signatures and key exchange are provided.

For IPSec, session keys are negotiated at the beginning of an SA lifetime and can be modified as often as required during a connection's lifetime. Diffie-Hellman as part of IKE is used to generate the initial session keys for an IPSec connection. As session keys expire, IKE negotiates new keys for the connection, exchanging new session keys over the secure IPSec connection or via a DH key exchange. Session keys for IPSec are DES and TripleDES keys.

In addition, TLS is implemented for management sessions or secure internal communication (SIC). The TLS handshake protocol is used for key exchange, along with digital certificates and one time or fixed passwords for authentication. Session keys for TLS are DES and TripleDES keys.

When a module's SIC is first being initialized, a one-time password is used for authentication. After this is completed, the module is issued an RSA key pair along with a digital certificate. From that point on, SIC is conducted over a secure session using TLS.

Initialization of IPSec functionality including IKE is done over a secure management session. All preshared IKE keys are electronically entered over this connection as well as RSA key pairs. The module's VPN and firewall services can all be configured over these TLS-secured sessions as well.

User ID's and passwords for local Crypto-Officers are stored within the module. These are part of the Operating System.

Further, Check Point VPN-1 Gateway NG also supports the FWZ Encryption Scheme (public key schemes). FWZ is a Check Point proprietary key exchange mechanism. It uses Diffie-Hellman for the underlying key exchange protocol, and supports a variety of authentication techniques.

All keys can be zeroized by uninstalling the module and reformatting the partition or hard drive that contained the VPN-1 Gateway software.

2.4 Standards-based Cryptographic Algorithms

Check Point adheres to cryptographic standards and provides the strongest cryptography available. Check PointVPN-1 Gateway'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 Check Point VPN-1 Gateway provides the capability to use TLSv1 to secure management sessions. The module supports IPSEC/ESP for data encryption, IPSEC/ESP for data integrity and IPSEC/AH for data integrity. It implements all IKE modes: main, aggressive and quick, using ISAKMP as per the standard.

The Check Point VPN-1 Gateway implements the following FIPS-approved algorithms:

Data Encryption:

- Data Encryption Standard (DES) in CBC mode (56 bit keys) – as per NIST PUB FIPS 46-2
- Triple DES (3DES) in CBC modes (168 bit keys) – as per NIST PUB FIPS 46-2

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).

Data Hashing:

- Secure Hash Algorithm (SHA-1) – as per NIST PUB FIPS 180-1

Digital Signatures:

- RSA – as per PKCS#1

Session Security:

- TLS v1.0 – as per RFC 2246
- IPSec

Key Exchange:

- Diffie-Hellman (used by IKE)

PRNG:

- X9.17-based PRNG with Yarrow controls on entropy gathering

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

- AES (128 or 256 bits) – as per NIST FIPS PUB 197.
- CAST (128 bits)
- FWZ Encryption Scheme (public key schemes)
- FWZ1 (symmetric encryption algorithm)
- HMAC-MD5 (16 bytes) – as per RFC 2104 (HMAC: Keyed-Hashing for Message Authentication) and RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH).
- MD5
- Secure Socket Layer (SSL) v3 – as per the Transport Layer Security Working Group draft.

2.5 Self-Testing

The VPN-1 Gateway performs a set of self-tests to ensure proper operation in accordance with FIPS 140-1. The module includes the following self-tests:

Hardware Tests: When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.
Software Integrity Tests: The module checks the integrity of its various components using DES-MACs.
Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up for the DES and Triple DES encryption/decryption, RSA digital signature signing/verifying, and Message Authentication Codes.

DES-CBC KAT
Triple-DES-CBC KAT
SHA-1 KAT

Continuous Random Number Generator Test: This test is constantly run to detect failure of the module's random number generator

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

2.6 Secure Management Software

The Check Point VPN-1 Gateway can be managed, both locally and remotely, with a suite of powerful tools. This software provides an intuitive graphical interface to the configurations of the VPN-1 Gateway and it allows for extensive monitoring of the status of the module. With remote capabilities and TLS sessions, an administrator can securely keep track of all Check Point VPN-1 Gateway modules across an enterprise from one location.

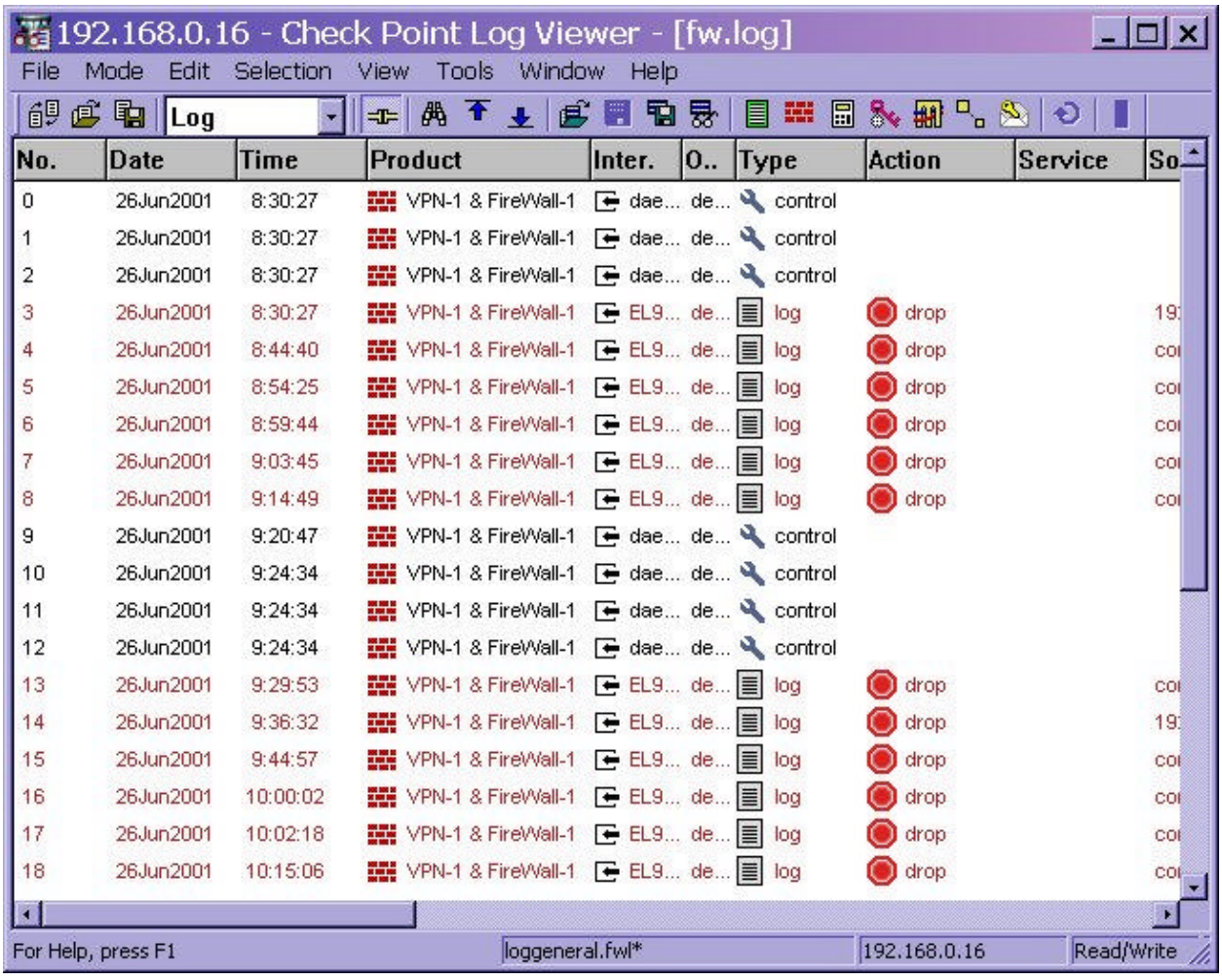

Figure 3 – Quick Access to the Logs

The Policy Editor shown in Figure 1 and the Log Viewer depicted above in Figure 3 are two of the intuitive utilities provided with the VPN-1 Gateway. These are just a few components of the management software suite provided by Check Point, which includes report generating, traffic monitoring, and system status applications.

3 FIPS 140-1 Level 2 Compliant Mode

The Check Point VPN-1 Gateway has a capability of operating in a FIPS 140-1 mode of operation and a non-FIPS 140-1 mode of operation. Hence, it is necessary to properly configure the module for running in FIPS 140-1 mode. The following steps must be taken to configure the module for FIPS mode.

To meet FIPS 140-1 level 2 requirements, the module must be installed on the ITSEC-evaluated C2-rated Microsoft Windows NT4 SP6a. The ITSEC evaluation applies only to particular hardware configurations on which Microsoft Windows NT is installed and setup in a particular manner. The Administrator's and User's Security Guide (for running Microsoft Windows NT 4 SP6a in the C-2 rated manner) can be downloaded here:

http://www.microsoft.com/technet/itsolutions/security/exe/C2SecGuide.exe

More information on using Microsoft Windows NT 4 SP6a in the C2-rated configuration can be found here:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/prodtech/c2deploy.asp

To make sure that the hardware (Compaq ProLiant 7000) containing the module is not tampered, the Check Point FIPS labeling kit must be used. To seal the system, you must apply serialized, tamper-evident labels as follows:

- Turn off and unplug the system before cleaning the chassis and applying labels.
- Clean the chassis of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol-based cleaning pads are recommended for this purpose.
- Apply labels as depicted in figure 4. (Of note, the tamper-evident label must cover the opening of the floppy.)
- Record the serial numbers of the labels applied to the system in a security log.

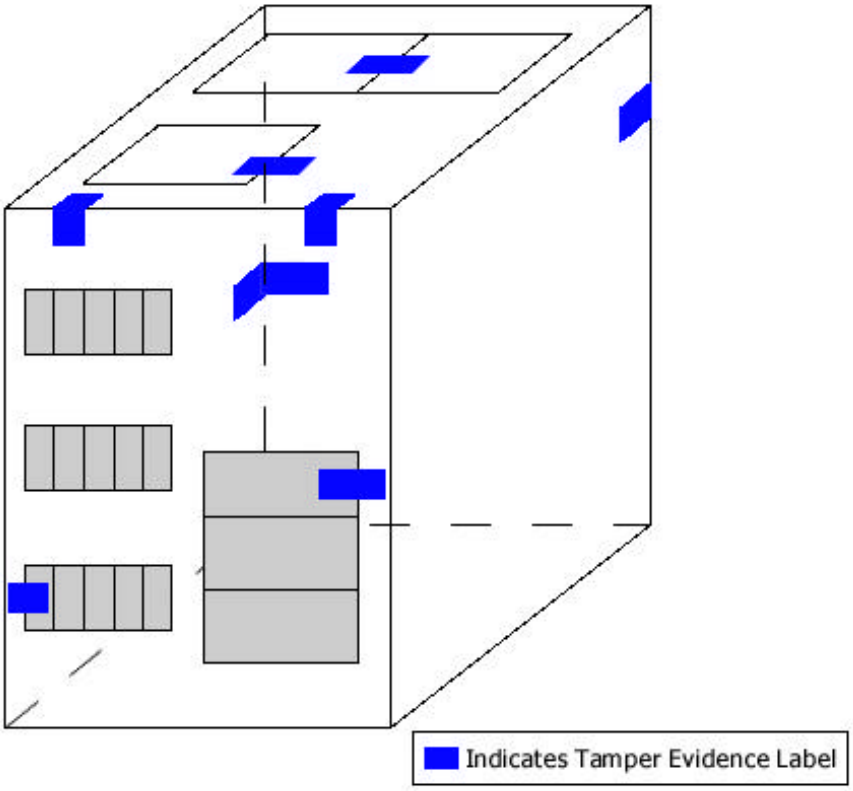

Figure 4 – Tamper-evident labels prevent unauthorized modification

The Check Point software should be installed on a separate partition from that of the underlying OS. This is done to allow for the zeroization of all keys via reformatting the partition without destroying the OS. If desired, the whole hard drive could be reformatted to zeroize all keys.

Once Microsoft Windows NT SP6a is configured in the C2-rated manner and tamper-evident labels have been applied to the hardware, installation of the Check Point VPN-1 Gateway software can begin.

A DES-MAC must be calculated over all system binaries. To enable this functionality for the SVN package, the following should be done (before installing the SVN foundation):

1. Edit the product.ini file found in SVN Foundation package.

2. Change the line “FIPS140=0” to “FIPS140=1”.

3. Install the SVN Foundation package.

During installation of the SVN Foundation, remember to select the partition created for the Check Point software as the installation destination. After installation of the SVN foundation package completes, run the command prompt. Switch to the %CPDIR%\bin (where CPDIR is

the directory in which the SVN foundation package was installed) and run the following command:

```
ckp_regedit -a "Software\Check Point\SIC" FIPS_140 -n 1
```

This command need to be run on the management station as well.

Additionally, the Remote Installation Daemon must be disabled after the SVN Foundation is installed. The following outlines how to disable this service:

1. Goto Start->Setting->Control Panel->Services and select the "Check Point Remote Installation Daemon".

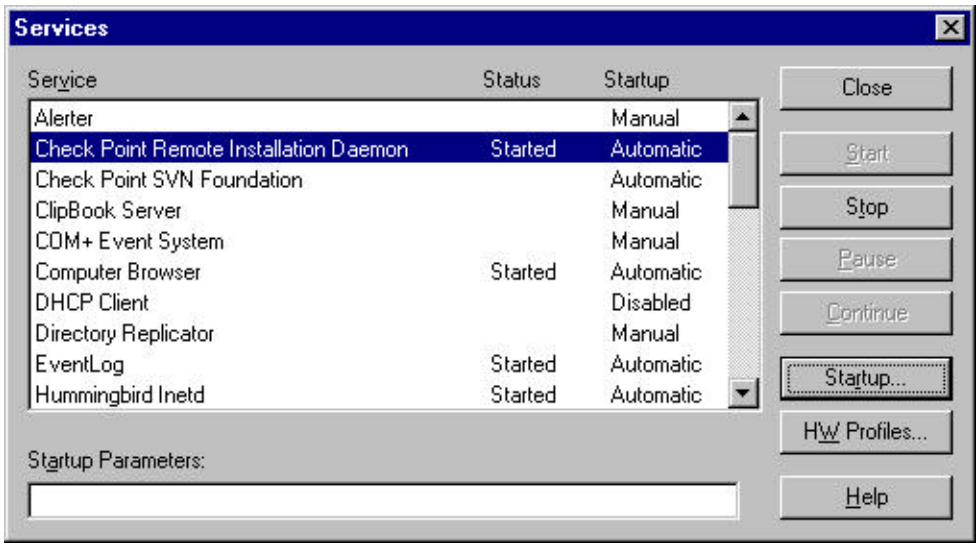

Figure 5 - Stop the Remote Installation Daemon service

2. Press 'Stop' (this will stop the service).

3. Press 'Startup'

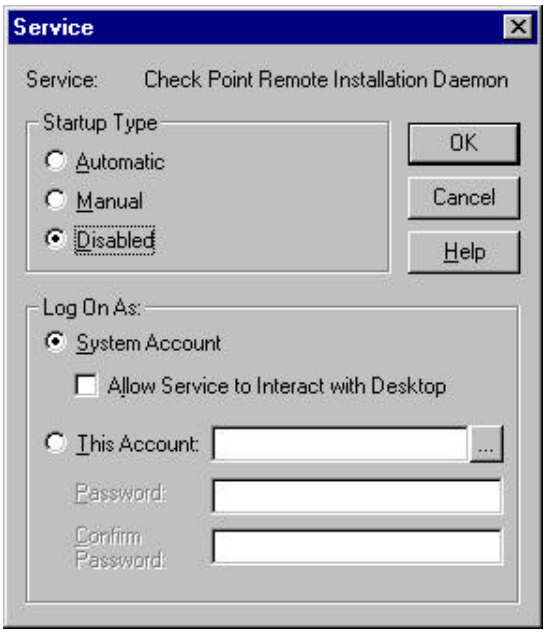

Figure 6 - Disable the Remote Installation Daemon service

4. Change the Start up type from 'Automatic' to 'Disabled'

5. Press OK.

All Remote Crypto-Officer services must be accessed through secure and authenticated channels. The following steps outline how to setup management session security for FIPS compliance:

1. If the SVN foundation is running, stop it by running 'cpstop'

2. Backup sic_policy.conf. The file is found under %CPDIR%/conf where CPDIR is the directory in which the SVN foundation package was installed.

3. Open sic_policy.conf with an editor and remove the following keywords:

   sslca_rc4
   sslca_rc4_comp
   asym_sslca_rc4
   asym_sslca_rc4_comp
   none
   sslca_clear
   ssl
   sslclear
   fwa1
   skey
   fwn1
   skey2
   ssl_opsec
   fwn1_opsec

Note: If removal of these terms results in the column being blank (columns are delimited by a semi-colon (';')) then comment the line out or remove it. If these words are followed by a comma (', ') , then remove it as well.

4. If you stopped the SVN foundation service in step 1, rerun it by issuing cpstart.

This set of four commands needs to be run on the management station as well.

Upon completion of these actions for the SVN Foundation, installation of the VPN-1/FW-1 package can begin.

As previously stated for the SVN Foundation, a DES-MAC must be calculated over all system binaries. To enable this functionality for the Check Point VPN-1/FW-1 package, the following should be done (before installing the VPN-1/FW-1 package):

1. Edit the product.ini file found in the VPN-1/FW-1 package.

2. Change the line “FIPS140=0” to “FIPS140=1”.

3. Install the VPN-1/FW-1 package (follow the steps below detailing how to install only the enforcement module).

The management software must be installed on a different machine from that of the module. During installation of the Check Point VPN-1/FW-1 package, remember to select the partition created for the Check Point software as the installation destination. Additionally, select the option to install only the “Enforcement Module” (see figure 7).

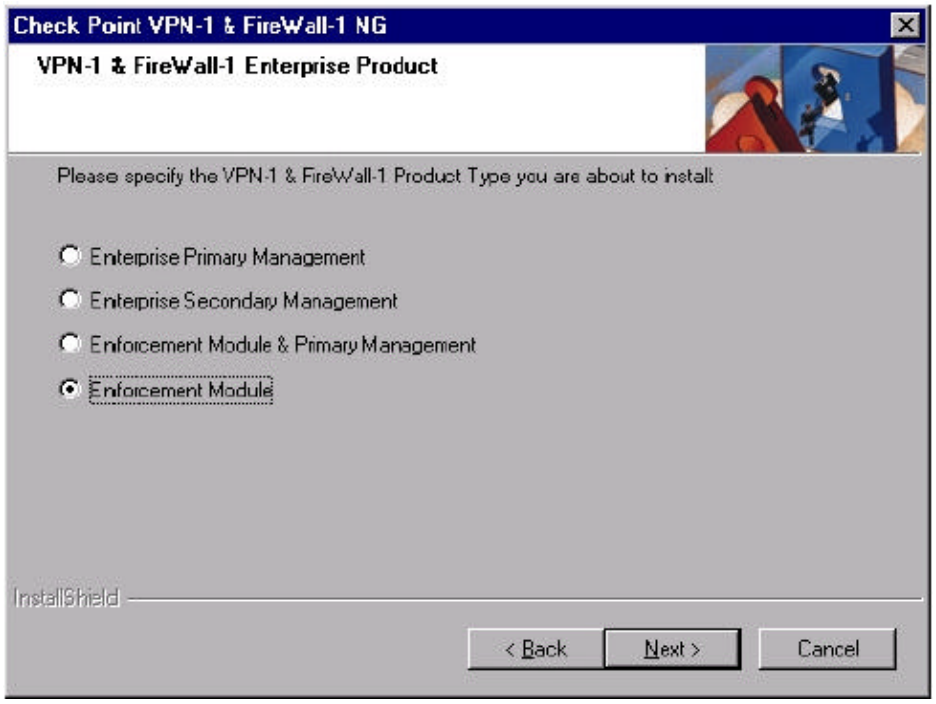

Figure 7 - Do not install the management modules locally

After installation of the VPN-1/FW-1 package is completed, the module is rebooted. Next, the boot and initial policies must be changed from the default to the following:

For the 'boot policy' -
Drop all connections.

For the 'initial policy'
Allow inbound control connections
Drop all other connections

In order to do change these policies, perform the following actions:

1. Backup the file %FWDIR%\conf\defaultfilter.pf (FWDIR is the directory where the FW is installed).
2. copy %FWDIR%\lib\defaultfilter.drop %FWDIR%\conf\defaultfilter.pf
3. Run comp_init_policy
4. Reboot.

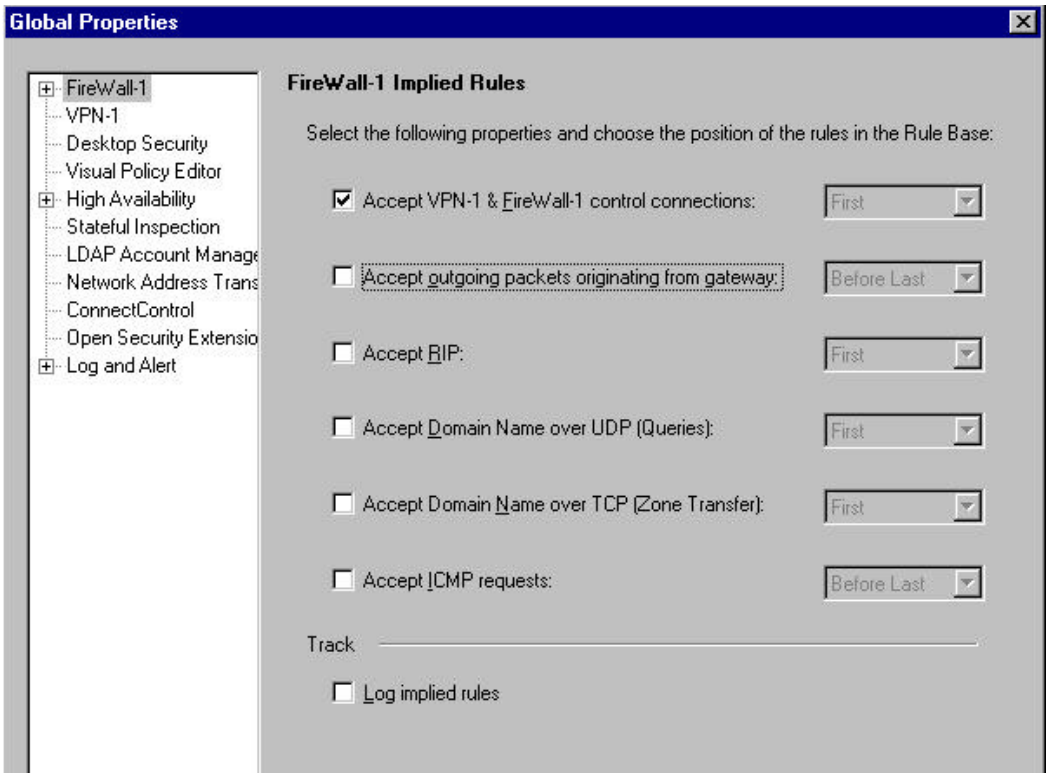

Figure 8 - Configure Check Point VPN-1 Gateway for FIPS mode

The FireWall-1 implied rules must be configured as depicted in figure 8. Only “Accept VPN-1 & FireWall-1 control connections: First” should be selected.

IPSec must be configured to use IKE (with Diffie-Helman key exchange) employing preshared keys or digital certificates for authentication.

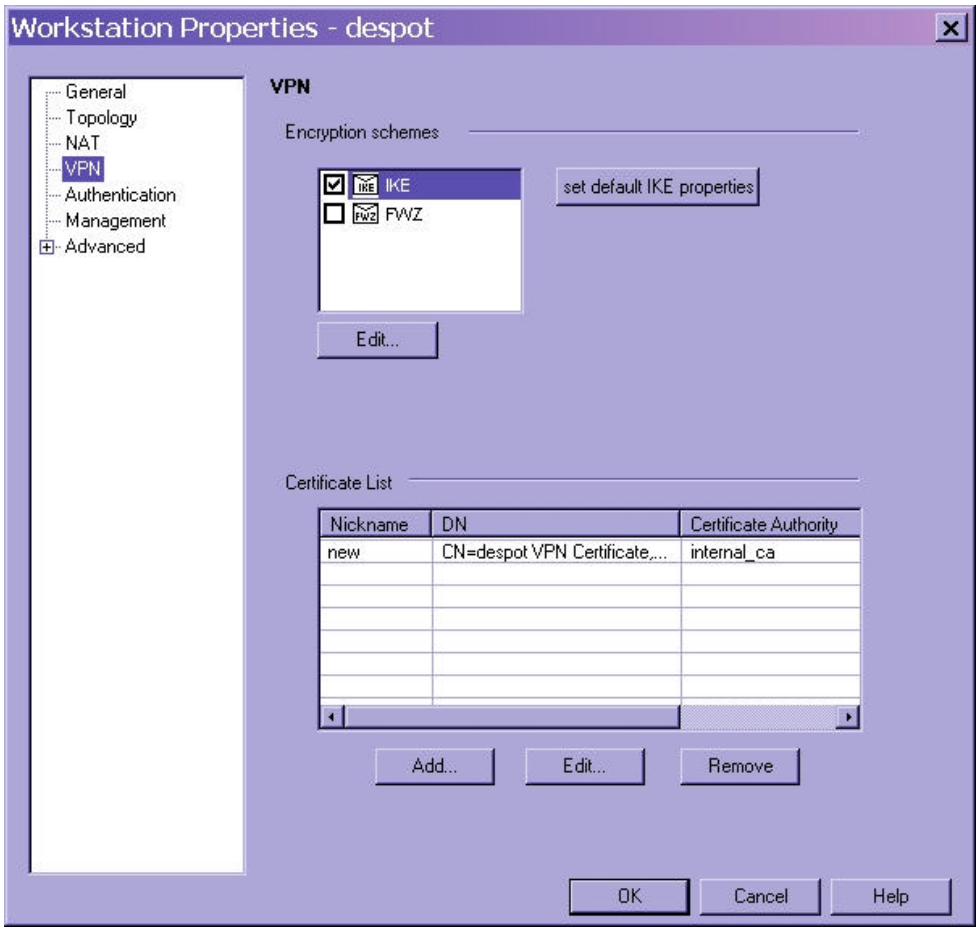

Figure 9 – Only IKE for IPSec

Only the following settings may be used with IPSec:

Data Encryption

- DES
- Triple DES

Data Packet Integrity

- HMAC with SHA1

Authentication

- Certificates
- Pre-shared keys

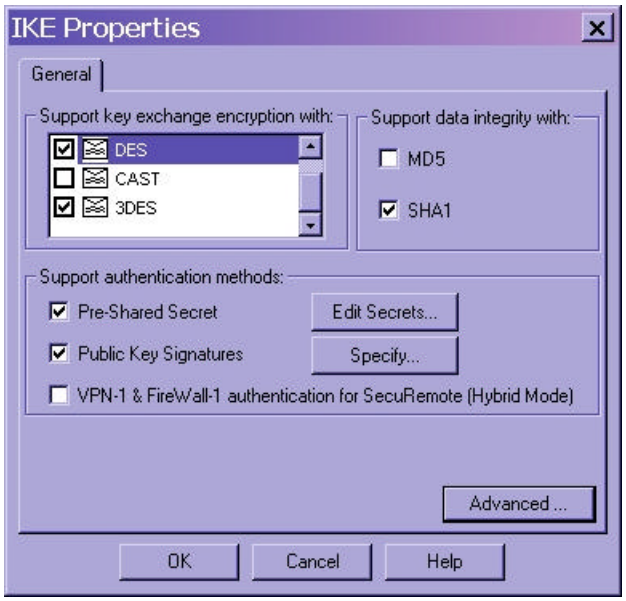

Figure 10 – Only FIPS-approved method employed by IKE/IPSec

After the initial configuration of the module, the VPN-1 Gateway's services should only be started/stopped manually through the "Services" interface under the "Control Panel." Local command-line utilities should not be utilized for FIPS-relevant configuration at this point (i.e., editing FireWall rules, configuring VPN rules, service starting/stopping, etc.). Only the appropriate Check Point and Windows NT GUI tools should be utilized by the Local Crypto-Officer for the management of the module once running in a FIPS-compliant manner.