Future SecuwayPCI

Operator’s Guide

Registered trademarks

※Future SecuwaySuite is a registered trademark of Future System Co., Ltd.

※Future SecuwayCenter is a registered trademark of Future System Co., Ltd.

※Future SecuwayGate is a registered trademark of Future System Co., Ltd.

※Future SecuwayPCI is a registered trademark of Future System Co., Ltd.

※Future SecuwayClient is a registered trademark of Future System Co., Ltd.

Note

This Operator's Guide was last modified in July 18, 2000. This guide is subject to change without prior notice to reflect changes and improvement in product and to correct errata that might take place during the printing.

Head office, R&D Center: 1009-1,7&8Fl. Korea Land Corp. Bldg., Daechi-dong, Gangnam-ku, Seoul, Korea 135-851

Tel: 82-2-578-8925 / Fax: 82-2-578-8929

Factory: Ma-905, Factory complex, Yatap-dong, Bundang-ku, Seongnam-shi, Gyeonggi province, Seoul, Korea 463-070

Tel: 82-342-709-3875/ Fax: 82-342-709-3875

http://www.future.co.kr

Preface

Thank you for purchasing SecuwayPCI—security device that enables you to protect banking and financial transactions from unauthorized access.

The Future Systems Inc. specialized in network security solutions development is delighted to introduce the SecuwayPCI—a system security device that performs user authentication and encrypts TCP/IP communications.

SecuwayPCI is designed to protect the delivering of business-critical data containing confidential financial transactions information. SecuwayPCI works in conjunction with SecuwayCenter and SecuwayGate to ensure safe data transmission, regardless of production location: within the financial institutions, cross-institutional networks, ATMs, high amount transactions systems. etc. SecuwayPCI protects the financial transactions information that is extremely crucial to individuals, organizations, and governments.

Before getting started

1. About SecuwayPCI Operator's Guide

SecuwayPCI supports the standard PCI interface allowing users to operate SecuwayPCI through their personal computers where Window NT is installed.

* Window 98 is to be supported soon.

This guide consists of four chapters.

Chapter 1: "The Introduction to SecuwayPCI" contains the general information about SecuwayPCI its features.

Chapter 2: "Configuring SecuwayPCI" is a complete guide to PCI Security board installation and software configuring.

Chapter 3: "How to use SecuwayPCI" deals with using Secuway PCI.

Chapter 4: "Automatic Upgrade" explains you you how to perform the automatic upgrade.

2. Notations

	References
	Warnings
❑	Terminology definitions
*	For more details, see footnotes or references.
|	"Or" command
[ ]	Optional parameters
Underline	Underlined characters refer to the remote system

Contents

Chapter 1: Introduction To SecuwayPCI

1. Introduction to Secuway PCI

As a key component of the SecuwaySuite, SecuwayPCI operates in conjunction with SecuwayCenter and SecuwayGate and provides the comprehensive solutions related to the security items of data transmission.

SecuwayPCI is a hardware-based security token that encrypts and decrypts network packets through key management based on Internet standard.

SecuwayPCI saves the communication key on PCI security board after receiving it from SecuwayCenter administrator. As the security functions are from the SecuwayPCI security board, they will be activated on installing the SecuwayPCI security board, saving users from making separate preparation to activate them. PCI board provides fast data transmission through many different computing environments, regardless of its being ATM or desktop.

2. Features of Secuway PCI

SecuwayPCI features:

Security token in PCI board type

The PCI board-typed security token is easy to install, fast and provides the straightforward interface.

Compliance with the security standard

SecuwayPCI is in full compliance with the international standards including IPSec (Internet Protocol Security Protocol), IKE (Internet Key Exchange), and Cryptoki (PKCS#11). It is ready to work with other upcoming products.

Providing data communications security

In line with IPSec, SecuwayPCI provides the authentication mechanism (AH: Authentication Header) that authorizes the producers of packets and verifies packets. SecuwayPCI performs Encapsulating Security Payload (ESP) that encrypts the data entailed in packets to meet the communication security requirements. SecuwayPCI uses the standard TCP/IP protocol allowing users to send encrypted data to destination in the network.

Korean-government certified encryption algorithms

SecuwayPCI uses the encryption chips and hardware developed under the Korean government's supervision. As a security device, SecuwayPCI performs reliable encryption and decryption process.

Automatic upgrade

SecuwayPCI automatically reflects the changes made on relevant files.

Records the action history

SecuwayPCI manages and records the users' information and their actions that can be printed out and saved on disks. Administrators can use this function to keep track of users and find a root-cause of errors and security breaches.

Tamper-Proof hardware protection

In order to prevent leakage of information, SecuwayPCI deletes encryption algorithms—key parameters required for encryption and decryption—and other security information, in the cases of an unauthenticated user attempts to operate, disassemble SecuwayPCI hardware, or gain access to memory.

Chapter 2: Configuring of SecuwayPCI

1. Before the Secuway PCI Configuring

1. Operating Environment for SecuwayPCI

System requirements

▶ PCI Revision 2.1 compatible 32-bit, 33MHz, Card slot, PCI slot.

Compatible with IBM-PC AT, 80486CPU or higher, Main memory of 8M or higher

▶ Window NT operating system service pack 4 or higher

Product components

▶ Secuway PCI board (1ea)

▶ CD with installation software (1 ea)

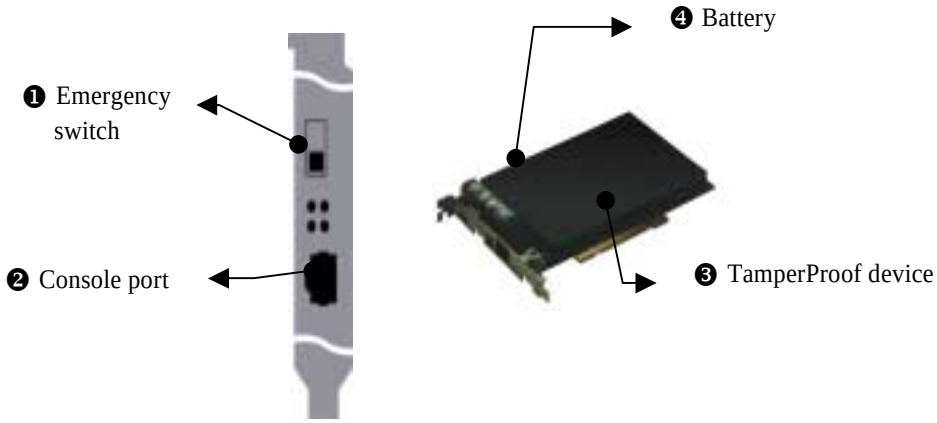
▶ User's Guide (1ea)

2. Hardware Specifications

Size	170mm x 110mm x 13mm
Processor	32-bit RISC
Memory	16Mbytes
Tamper-proof device	The Tamper-proof device deletes key information if an unauthorized person attempts to open the cover on a circuit in order to find out internal key information.
PCI power	PCI Universal Card standard power (+5.0V, +3.3V) Maximum power usage 10W, 2A

3. External Interface

The components of the external interface are:



❶ Emergency switch

The emergency switch deletes the internal information to prevent leakage of key and information in the event of emergency. The switch turns on, when it is pushed up.

PCI security board is a hardware intended to maintain a key safely. To install the board, the emergency switch should be in down position to the console port, as shown in figure ❶.

A system will not boot up even after the installation of PCI board, if the emergency switch doesn't point towards the console port.

❷ Console port

Console port is to be used as a debugger and to upgrade the internal software. The hyper terminal on the Windows system is used to connect to the console part.

❸ Tamper-proof device

Tamper-proof device is a protector of the internal key and user information. The tamper-proof device deletes all the security information, if an unauthorized user attempts to open up the black lid of the board or to damage it. Make sure to handle it with care before and after installation.

❹ Battery

Battery is used to maintain the information inside the PCI security board when power to a personal computer is down. When the battery is removed from the Secuway PCI board, the internal information is deletedbecause of no power supply goes on to the system.

2. Installation & Configuration

1. Installation step by step

Installation goes on through 3 steps:

❶ SecuwayPCI Installation

❷ Configuring the software

❸ Preparation for key insertion

■ Starting Filesetupwiz.exe

- A key insertion requires the initialization of setup files made at SecuwayCenter.

2. Secuway PCI Installation

Switch off the computer and insert the PCI board.

3. Configuring the Software

Insert CD with software in CD-ROM drive and start SETUP.EXE file.

Step 1: Starting SETUP.EXE

Press the **next** button to continue the installation.

Step 2: Selecting a folder

Create a folder or select from the exisiting folders where the program files are to be saved. The default folder is Program Files\Future\SecuwayPCI.

Step 3: Selecting a program folder

Select a SecuwayPCI folder. The default folder is SecuwayPCI that can be changed according to an individual user environment.

The program files are copied to the hard drive after a program folder is chosen.

Step 4: Installing IPSec driver

The steps 4 to 7 are performed automatically according to script files. If a user presses other buttons than "**ok**" the installation process might be interrupted.

SecuwayPCI uses IPSec standard for data encryption and decryption.

Press the "**Yes**"button to install a driver for Window NT. Press the "**No**" button to finish the installation.

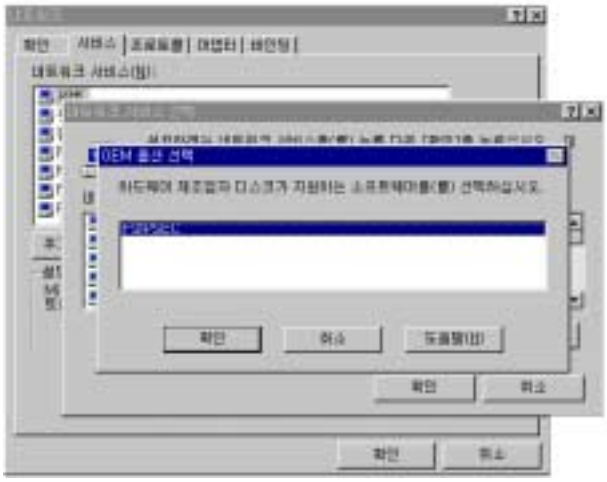
Step 5: Message for drive installation

Press "**OK**" to automatically copy scripted files for drive installation. Please wait until you see the following message.

Step 6: Drive installation

Press "**OK**" button to prompt the program installation script that activates the network, then add service and set up the binding.

Step 7: Adding network service



Press “OK” to reboot the system. When the network environment is modified and files are copied to a hard drive the system must be rebooted to start Secuway PCI administrator’s program.

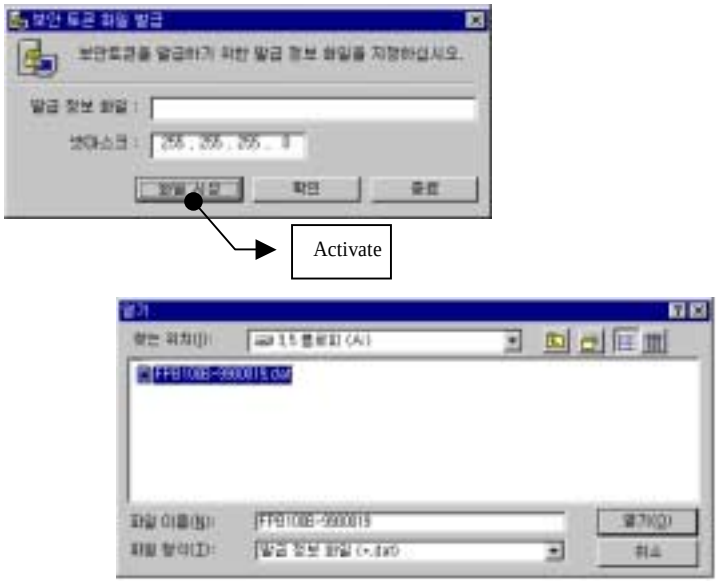
4. Preparation for the key insertion

Initialize Filesetupwiz.exe

The preparation for key insertion starts when the system has been rebooted in order to add the installed PCI board and the program files to the system.

Activate Filesetupwiz.exe file located in installation folder. A dialogue box appears upon activating the files. Insert the key from SecuwayCenter to SecuwayPCI board. Select a file to determine the settings.

Select a file ->press "**OK** " button -> press "**Finish**" button.



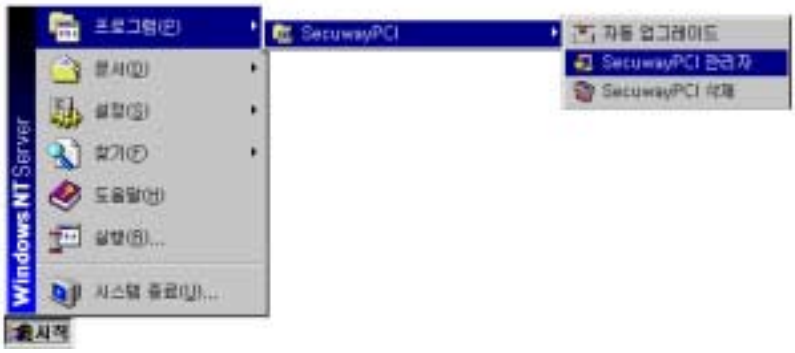
Press the "**Open**" button to select a file, then press "**OK**" button in a dialogue box to create a security token file in order to assign disk information to SecuwayCenter to PCI security board.

Please, make sure that the key disk from SecuwayCenter administrator is available. Otherwise the installation cannot be completed.

3. Getting Started

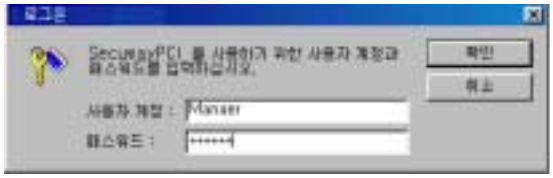
The presence of administrator menu in star\program\SecuwayPCI indicates that the installation is completed successfully.

Run the FileSetupwiz.exe to insert a key and activate SecuwayPCI administrator.



1. Log-on

The log-on box comes up when the system is rebooted. Add SecuwayPCI hardware and software to the system. User ID is 'Manager' and a password is issued from the SecuwayCenter.

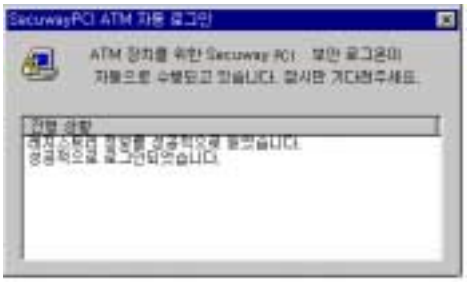


SecuwayPCI must be in the slot when a computer boots up. Otherwise the following messageis displayed: "Security token is missing."

2. SecuwayPCI administrator log-on for ATM operations.

SecuwayPCI for ATM operations doesn't require administrator log-on after the installation. Log-on takes place once during the installation.

The picture below is the log-on dialog box.



Activate FileSetupwiz.exe to get ready for key insertion if the above dialogue box did not appear. Missing the log-on dialogue box means that preparation for key insertion is not completed.

Toolbar Menu Box

SecuwayPCI administrator program automatically runs when Windows NT is rebooted. Click the right mouse button on the right side of toolbar to bring up the menu as shown below.

❍ **SecuwayPCI administrator View (V)**

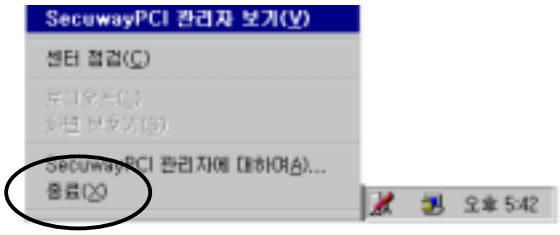
The administrator view displays the settings of SecuwayPCI, communications and log status.

❍ **Center checkup**

Center checkup examines the encryption process that involves SecuwayCenter. When the center checkup is completed SecuwayPCI administrator program creates a log saying, "SecuwayCenter responded."

3. Close

Choose the “Close” command to log-off and exit the SecuwayPCI administrator program.

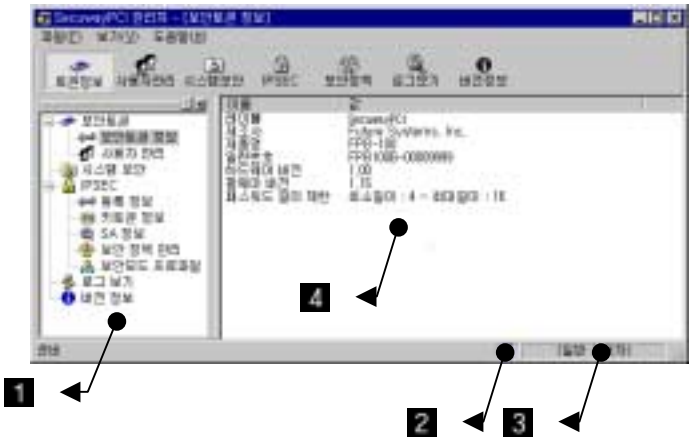


When the program is closed encryption cannot be performed. A server that requires encrypted communication has no access to the network.

To run the program again, go to Start\Programs\SecuwayPCI and run SecuwayPCI administrator.

4. Main Window

The picture below illustrates the main window of SecuwayPCI that comes up after log-on.



1 Control panel that contains the same menus as the icons on the toolbar.

2 Indicates that the key token is in use. Hardware token is marked as a square.

3 User grade. There are two users grades: premium user and regular user.

4 Information window with thedetails about menus on the control panel

Memo

Chapter 3: How to use SecuwayPCI

1. Security Token Information

2. User Information

3. System Security

4. IPSec

5. Viewing Logs

6. Version Information

1. Security Token Information

Security token is software or hardware module (PCI or PCMCIA type) which has been designed to provide security services including log-on, key management, encryption/decryption, measuring and verifying authentication parameters service, management of security information and time.

Security token uses Cryptoki (PKCS#11) standard API by RSA, which is considered as the industry standard.

❑ SecuwayPCI plays the role of security token. Security token information is contained in SecuwayPCI.

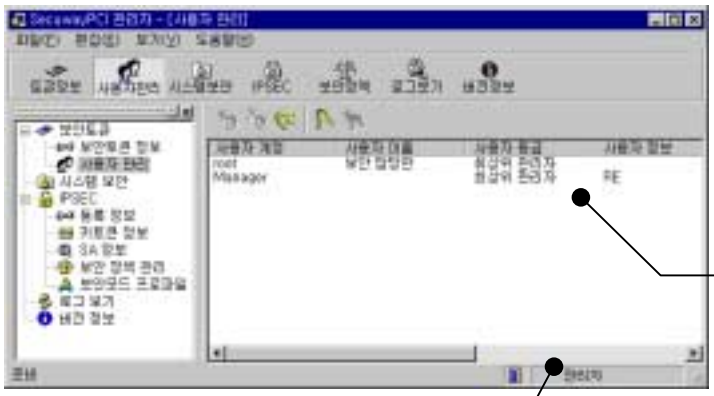
❑ SecuwayPCI entails key token, SA information, security policies, and security mode profiles.

2. User Management

SecuwayPCI administrator can register users to allow multiple users to sign on with different IDs.

*** Users cannot gain access to user management functions.**

1. Adding, Deleting, and Modifying User Information



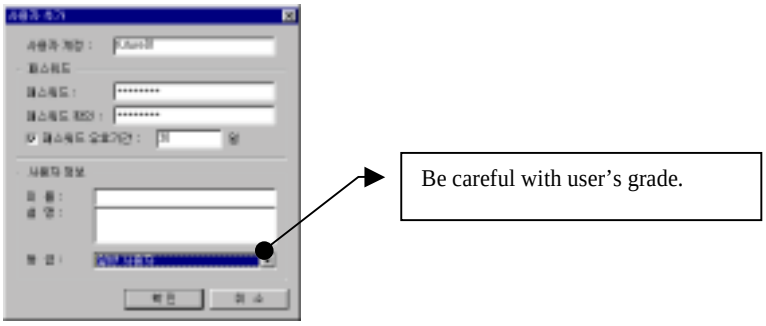
This window displays user information online.

This column displays the users' grade, which can be: root, administrator, premium users, and regular users.

Only administrator has a permission to add, delete users' accounts, and change users' passwords. Neither premium nor regular users have access to this functions.

Adding users

Administrators can register 6 premium and regular users in all. Be careful with user's grade, when adding a new user.



❍ **Validity of password**

When a password expires, a dialogue box comes up to remind users to change the password. Users need to enter a new password to log on to the program.

❍ **User grade**

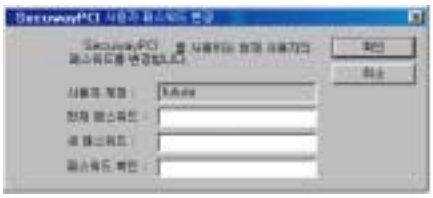
There are two grades for users: premium and regular. The premium users can register the security path in the **"system security"** menu, while the regular users are not allowed to do this.

Deleting a user

When an administrator deletes a user he/she cannot log on to the program. The dialogue box below comes up when the user's account deleting process is activated.

An administrator can delete any users. However, users cannot delete their ID or initialize the password.

Changing password



Administrator can change all the users' passwords. The regular users can change only their own

passwords.

It is recommended to change passwords on a regular basis. Password must be comprised of numbers and ideograms to make it difficult for others to guess.

- If users forget their passwords, administrators can initialize the password to reset it.

- If an administrator forgot his/her password, ask SecuwayCenter about root ID and then log on with the root ID to initialize password and reset it..

SecuwayPCI for ATM operations is registered with the root and manager ID in consideration for its circumstances.

2. Users gradation

All the users can be graded as administrators, premium user, or regular users. Regardless of grades, users are provided with the settings for disk security, screen saving functions, and reliable encrypted communication services.

However, some of the functions are graduated according to user grades:

Administrator

Administrator can add and delete premium and regular users. Administrator can add path for system security options.

Premium users

Premium users can add path for system security options. However, they cannot add users' accounts.

Regular users

This is the basic level given to users, when they are registered with SecuwayPCI administrator program. Regular users can use the existing security path, however, they are neither allowed to add new users nor set a new security path.

Roots and managers are the highest level of administrators in SecuwayPCI for ATM operations, due to the circumstances.

3. System Security

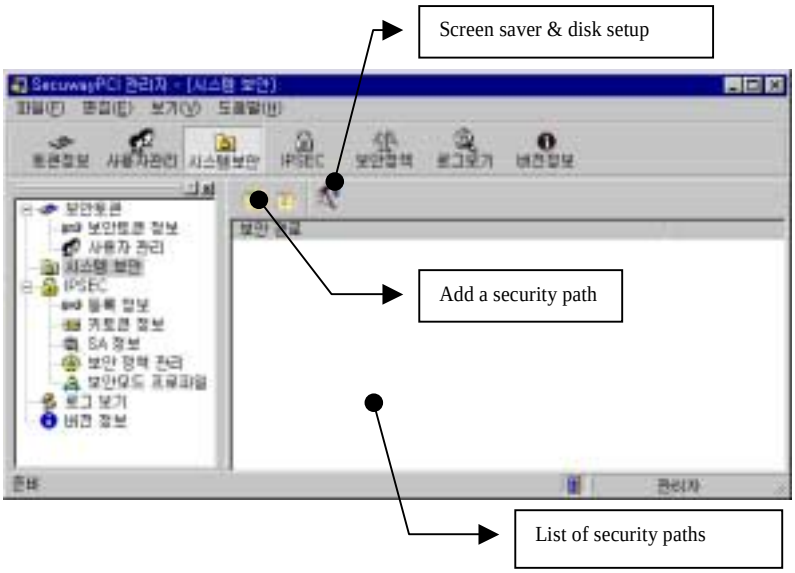
To meet the system security requirements, SecuwayPCI selects or removes a folder related to hard disk encryption/decryption as well as settings of floppy disk security functions.

*** This function is not available with SecuwayPCI for ATM operations.**

*** Regular users cannot use the system security functions.**

System security functions allows you to perform following:

- When a file is copied to a folder on the security path, SecuwayPCI encrypts the file.
- When a file on the security path is copied to a folder out of the path, SecuwayPCI decrypts the file.
- SecuwayPCI allows the access to files on the security path only to those uswrs, which are registered with the SecuwayPCI program.
- If a disk is protected through the SecuwayPCI disk security option, files on the disk cannot be opened in other systems without SecuwayPCI program. If a user copies a file from a SecuwayPCI-protected hard disk to other system without SecuwayPCI program, the content of files cannot be read because it is encrypted.
- Sub folders of a folder on the security path are protected by the same security functions.
- When a folder is put on the security path, the existing files in the folder will be all encrypted.



1. Adding a Security Path

Once a folder is added on the security path, the files and the programs in the folder are automatically encrypted and decrypted when they are copied or activated. This function does not allow unauthorized users to get access to users' system.

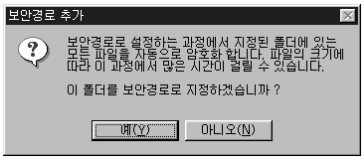
Once a folder is included in a security path, copying files is allowed, however moving files to a directory outside the security path is disabled. Moving a file causes errors.

1.1 Adding a security path

Adding a folder to a security path

Select a folder to be added to the security path. Selected folder you want to be displayed on the window when the **system security menu** is chosen.

Once a folder is added to a security path, all the files and sub-folders in the folder will be encrypted. The existing files in the selected folder will be encrypted as well.



Only SecuwayPCI users can read and write encrypted files. An unauthorized system doesn't recognize an encrypted file as a normal file.

Encrypted program displays the "It is not an appropriate WIN32 program" message to an unauthorized user. Encrypted text files are unreadable for unauthorized users.

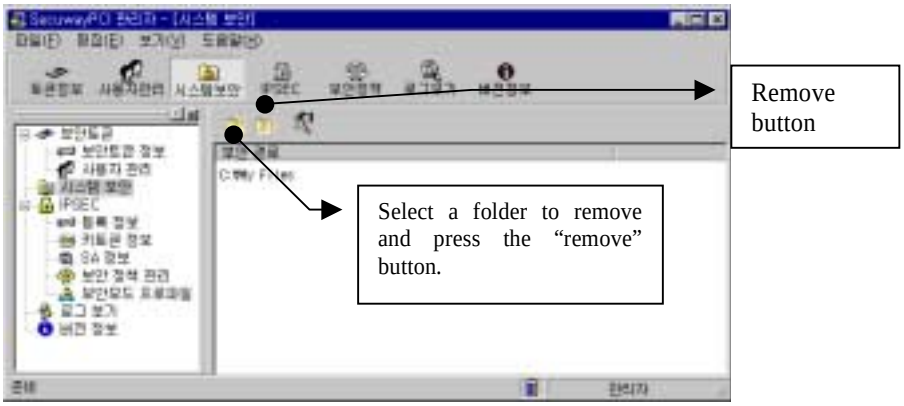
The security path doesn't cover the whole window, window system folders, local C or D drives.

1.2 Removing a Security Path

Removing a folder

Removing a folder from a security path decrypts the files in the folder and makes them accessible to unauthorized users without SecuwayPCI program.

Select a folder to remove and press the **"remove"** button.



When removing a folder, the following dialogue box comes up, asking whether the files in the folder should be deleted for the sake of security.

2. Registration Information

The registration function sets up screen saver and determines whether a floppy disk needs to be protected or not.

2.1. Screen Saver Settings

Sets a waiting time from the last input and until the screen saver is activated. The screen saver with the SecuwayPCI program has no connections with screen saving functions in the Windows system.

* This function is not available with SecuwayPCI for ATM operations.

2.2. Disk security

Disks can be divided into security and regular disks.

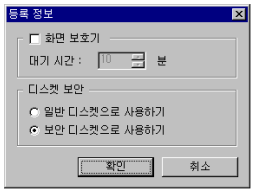
Regular disks

Files on a floppy disk will not be encrypted in regular disk mode. The right side window of the system will have an icon looking like a floppy disk.

This is when a user decides to use a floppy disk without encryption.

Security disks

All the information on a floppy disk is encrypted and saved in security disk mode. Information on the disks goes through decryption, when a user brings up the information.



Security disk mode is indicated by the icon of a disk with a key.

In the security disk mode, an authorized user cannot read information from a floppy disk. To read the information users need to log on to SecuwayPCI program.

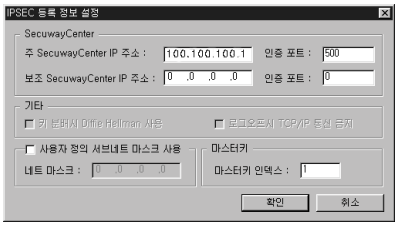
4. IPSec

1. Registration Information

IPSEC displays the information on SecuwayPCI security token issued from a SecuwayCenter.

IPSec registration information

The registration information comprises the settings of SecuwayPCI active in the networks.



❍ **Main SecuwayCenter IP address, Redundant SecuwayCenter IP address**

A main SecuwayCenter IP address, redundant SecuwayCenter IP address, and authentication port are from SecuwayCenter. Enter an altered IP address, should system settings or network environment be modified.

❍ **User definition subnet mask**

User definition subnet mask is a subnet mask according to user IP address. Standard subnet mask in A, B, and C classes doesn't require user definition subnet mask. A Class is 255.0.0.0, B Class is 255.255.0.0, and C Class is 255.255.255.0.

Should subnet mask IP not be in the standard A, B, and C, tick on the user definition subnet mask and enter a subnet mask. For example: if IP address is 100.100.100.1 (A class) and subnet is 255.255.255.0 (C class), click the user definition subnet mask and enter the subnet.

❍ **Master Key**

A master key is used for encryption and keys in use are listed up from the total 100 keys. SecuwayCenter determines the value of keys and sends it to SecuwayPCI. The key values must be the same in different devices in order to ensure the communications take place.

If a user changes the master key value ignoring the instruction of SecuwayCenter administrator, the encryption will be disabled. Thus, it is important to remind users avoid to alter the master key value of their own.

 View the latest information (refresh)

Bring up the changed and saved information.

Host

Hosts are IPSec objects. Hosts include SecuwayGate, dynamic IP address, and static IP address. SecuwayPCI is an object either with dynamic or static IP addresses by light of IPSec.

Host ID

Host ID is the only identifier for each IPSec host registered with SecuwayCenter. Host ID consists of 8 bytes (the first 4 bytes are currently pre-determined) in 이진값 and screen pointer? goes in the order of a-bbb-ccc.

All the SecuwaySuite products follow the same numbering system for all host IDs. The first digit is the type IPSec hosts (devices): 0 is SecuwayCenter, 2 is SecuwayClient, SecuwayPCI and SecuwayGate.

Master Key

Master key is the highest security key of all in the IPSec standard and each IPSec host has the unique value.

2. Key token information

Key token is a shared key among IPSec hosts for security communication.

Key token ID

Key token ID is the only identifier to tell apart key tokens. Key token information is created when an IPSec host starts communicating with other host, as shown above. SecuwayCenter sends key tokens to help encryption process.

There is no communication with SecuwayCenter or an error is caused by network settings, if no key token is created between the hosts attempting to communicate. Check the SecuwayCenter IP address and that of a computer with SecuwayPCI to ensure that they are appropriately entered to the system.

Remote Host ID

A remote host ID is for users who gain access into the system through SecuwayPCI.

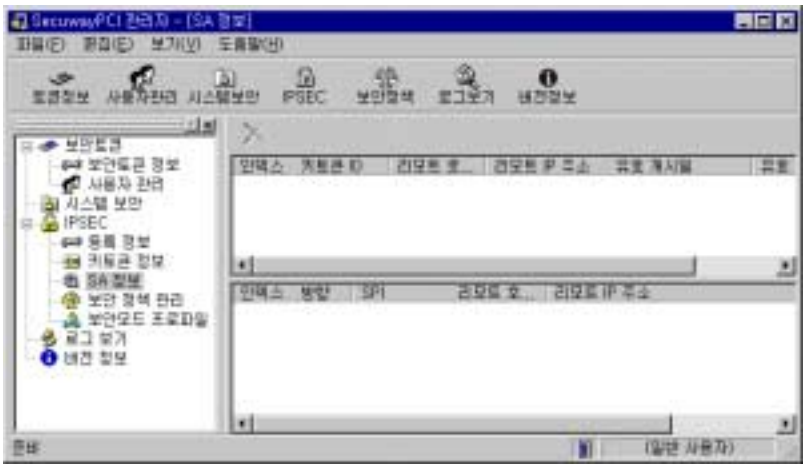
Valid starting date

Valid starting date is used when hosts start communicating with creating a key token.

Key tokens and SA are created when IPSec hosts perform the encrypted communications.

3. SA Information

SA (Security Association) is shared encryption, authentication mechanism, and keys between two hosts necessary to protect the exchanged information. SA information varies depending on the security protocol.



SA window displays both sender's and recipient's SA information, remote host ID, and IP address when communication takes place normally.

See below for an example of SA information displayed during encrypted communication. The upper part displays key token ID of a host being accessed, while the lower part shows remote host ID, its IP address, authentication/encryption algorithms in use.

Sender, receiver, and SA information is created to provide the connection status to a corresponding host.

If two hosts are in different security mode, request from a host trying to have access is not returned with response. Set the same security mode profiles for two hosts.

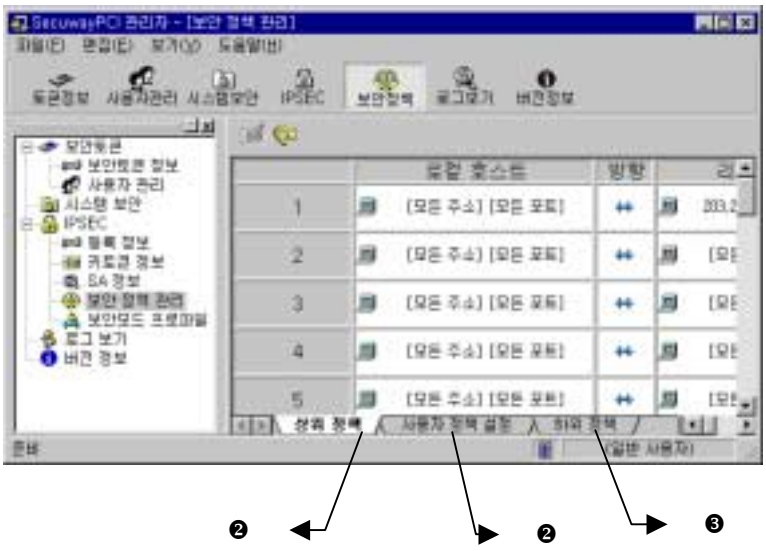
4. Managing Security Policy

Security policy is database of rules of how IPSec standard should process IP packets. Security policy is composed of sub rules that work on packets in ascending order, meaning Number 1 rule is the first rule to be applied.

4.1 Formation of Security Policy

Security policy is divided into higher, lower, and user defined policy. SecuwayPCI administrator creates user-defined policy. SecuwayCenter determines the priority of the policy.

Security policy is presented as ❶ for higher policy ❷for user policy ❸ for lower policy.



Writing a security policy

Make sure to save the changes by pressing the "Write a security policy" button after adding or deleting a rule in user policy setup menu. The security policy takes effect after saving.

The "**write a security policy**" button is located on the user policy setup tab. Only SecuwayCenter can determine the priority of security policy (higher, lower); even the SecuwayPCI administrator cannot do the modification.

Viewing the latest information

Higher policy

Press ❶ to bring out the list of higher policy set by SecuwayCenter. SecuwayCenter administrator determines the priority of policy and SecuwayPCI cannot add or alter the policy. The maximum number of higher rules is 30.

User definition policy

Users can add, modify and delete policy. The maximum number of user definition rules is 30.

Lower policy

Press the lower policy tab menu ❸ to bring up the list of lower policy. Only SecuwayCenter administrator can determine the priority of policy and SecuwayPCI administrator cannot modify or delete it. The lower policy allows the network environment to operate and saves SecuwayPCI administrator from manual setup processing. The maximum number of lower policies is 10.

Security policy works in order of higher, user definition, and lower policy. If two different rules have conflicting details, SecuwayPCI program applies a higher rule over lower rule.

Operating security policy
Once SecuwayCenter sets up a policy that allows all the hosts to communicate, except the servers protected by security function, SecuwayPCI administrator doesn't have to create settings for communications. That is to say, SecuwayCenter writes all the rules to ensure SecuwayPCI works on networks without the necessity to write new rules.

4.2 Writing a security rule

Adding and deleting a rule

Click the right mouse button on the gray screen to bring up the "**Add a rule**" and "**Delete a rule**" menus.

Click the right mouse button to bring up the above dialogue box.

Editing a rule

Double-click the mouse on a column to bring up a dialogue box that enables the editing of security rules. The top security rule has the highest priority and is first to be activated on communications.

Multiple rules can be made to meet specific requirements of individual network environment and security policy.

Local host and remote host

❍ **IP address**

Enter an IP address of local host or host to be accessed. The "**All**" command makes a rule capable to work on all the IP addresses of the hosts.

❍ **Port**

Enter the number of a port to be bound by a rule. Enter 23, if a rule is pointed for a specific port like TELNET.

Communication directions

❍ **Local host → remote host**

This option governs the packets going from a local to a remote host (outgoing packets).

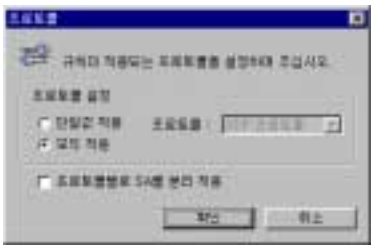
❍ **Local host ← remote host**

This option governs the packets going from a remote to a local host (incoming packets).

❍ **Local host ↔remote host**

This option governs the packets that go back and forth between a remote and a local host.

Protocol



❍ **Setting up a protocol**

Select either TCP or UDP as a protocol after checking with your program. If you choose the "**All**" option, security policy will cover all the protocols.

❍ **Separate SA application by protocol**

This option allows the protocols to have different SA applications.

Date/Time

Users can put restrictions on packets by date and time. For example, if you want to make a policy that disables communications on Saturday and Sunday, enter the days of a week and time in a corresponding field and select "**Communication disabled**" option on the field of security mode.

Security mode

❍ **Communications allowed/communication banned**

This option enables or disables the communications without analyzing the packets. Security mode is not used.

❍ **IPSec application (all the time)**

This option available in security mode is to implement IPSec communications through authentication and encryption protocols on 24 hours a day and 7 days a week basis.

❍ **IPSec application (optional)**

This option allows to perform selective IPSec communications through encryption and authentication protocol. It passes packets that are not eligible for IPSec communications to enable transactions without encryption.

Security mode

Select a security profile from the drop-down list. Security profile is required for IPSec application, but is not needed when security mode is "**Allow the passage (by packets)**" or "**Disable the passage (by packets).**"

5. Security profile

Security profile determines authentication and encryption algorithms on packets. Security profile is only in use for IPSec communications and doesn't go into effect when the "**Passage allowed**" security policy rules are on a packet.

Writing a security policy

Press the "**write a security policy**" button to save changes in the SecuwayPCI program after adding or deleting user defined rules. Otherwise, the rule doesn't take effect while it has been added to the system. The basic profile menu tab is only available to SecuwayCenter administrator and users cannot write a security policy using this menu.

❍ **Basic profile**

The basic profile is security mode that is created at SecuwayCenter and sent to SecuwayPCI. SecuwayPCI users are not allowed to modify the basic profiles, but they can check the security protocols currently in use.

❍ **User defined profile**

Users can determine a profile.

Security protocol

ESP - Only encryption protocol is in use during communications.

❍ **ESP (Encapsulating Security Payload) protocol**

ESP is IPSec security protocol intended to maintain the confidentiality of IP packets and to selectively provide connectionless integrity, data origin authentication, anti-reply services, and traffic low confidentiality on IP packet data.

Application mode

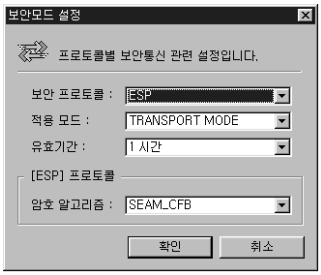
❍ **Transport mode**

Transport mode refers to AH or ESP security protocol header placed between IP and protocol header. In transport mode the AH security protocol provides security for all the IP packets including the header, while the ESP security protocol protects IP packet data excluding the header.

❍ **Tunnel mode**

Tunnel mode is added in the structure of proxy IP address header to host IP address that provides the security functions, AH or ESP header on back of the proxy IP address packets and IP address packets. In tunnel mode, either AH or ESP is in use.

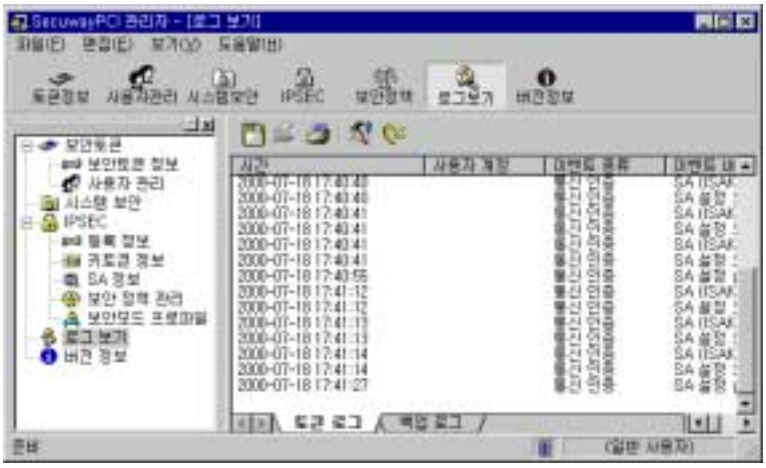
Setting a security mode



The SEAM_CFB encryption algorithm and SecuwayCenter reset the security mode when it was expired.

5. Viewing log

Viewing logs provides the crucial information about the system operation by allowing users to keep track of it. Logs show the status of unauthorized accesses or communications errors as well as the business-as-usual transactions.



The figure above illustrates the arrangement of information related to the time, user ID, description of events, and errors.

Menus are presented in icons.

Saving logs

This option allows you to save token logs. When logs are saved in a file, token log tab menu logs deletes the particular set of logs. Users can decide the name of a log file.

Reading logs

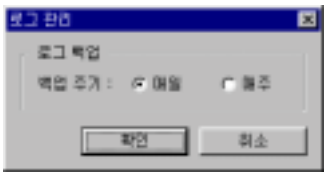
This option brings up the backed up (saved) logs. Go to the back-up log menu tab to view the saved logs.

Printing logs

This option provides the logs to be printed.

Log management

Click the log management icon to bring up the following dialogue box.



Set the period for log backup.

Description of events

As for key management, the descriptions of events are:

- Altered a master key
- Failed to alter a master key

As for security information management, the descriptions of events are:

- Altering a security information
- Altering security policy
- Deleting key token information

- Deleting 1-step authentication information
- Receiving security policy from a security center

As for online registration, the descriptions of events are:

- Requesting online registration
- Completing online registration
- Online registration is failed
- Errors in password registering

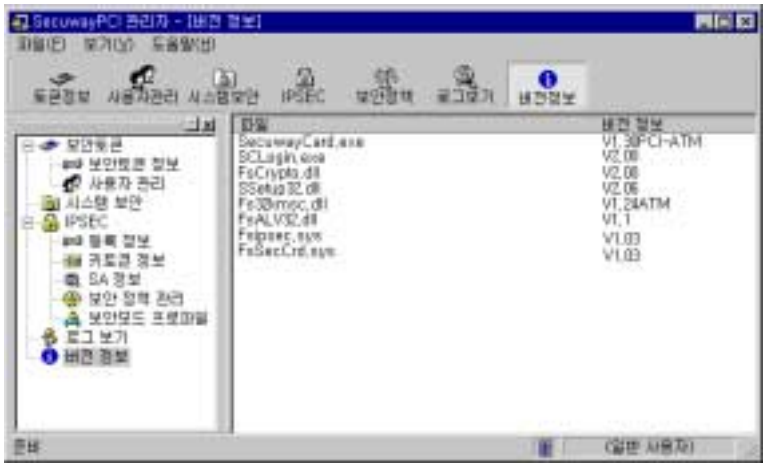
Normal communications between hosts create logs as shown below.

- Requesting time
- Requesting key token
- Receiving key token
- Starting SA setup
- Completing SA setup
- Starting SA (ISAKMP) setup
- Completing SA (ISAKMP) setup
- Starting SA (IPSec transfer) setup

- Completing SA (Outgoing IPSec) setup
- Starting SA (Incoming IPSec) setup
- Completing SA (Incoming IPSec) setup

6. Version Information

The version information displays the version of files used in Secuway PCI program. The figure below shows the current versions of files as opposed to versions needed to be upgraded through the automatic upgrade.



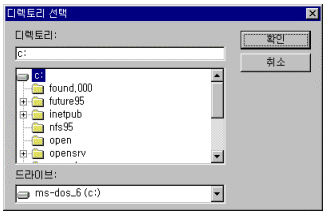
Memo

Data backup: This option allows you to create a backup file ~autoup~.bak for the files existing on a client and save it to a directory.

Directory: This option allows you to receive the data from the server and save it to the directory.

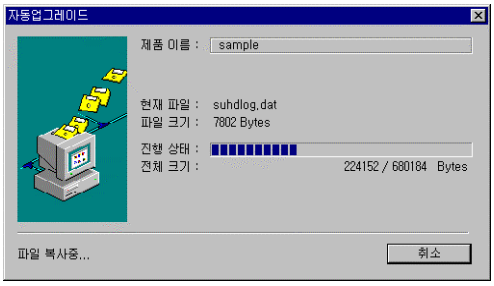
2.1 Changing Directory

Select the "**change directory**" option in the automatic upgrade to bring up a dialogue box that allows you to select and create a directory.



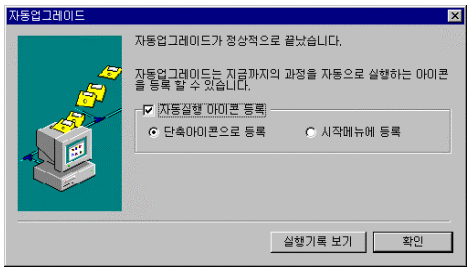
2.2 Automatic Upgrade

Select a directory and press "**OK**" to run the automatic file upgrade.

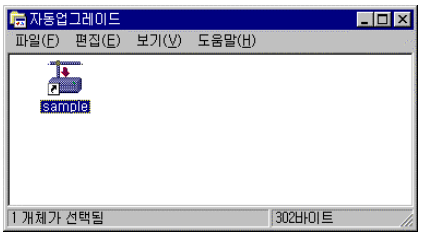


2.3 Automatic Execution Icon

Registering an automatic execution icon saves users from having to try accessing to an upgrade server every time they do upgrade. By registering an upgrade icon on start menu files will be automatically upgraded when a computer is booting or the process cfn be activated by the click on the icon.



Select the "**register an automatic execution icon**" and then the "**register a shortcut icon**" options to create a set of icons that corresponds to all the automatic upgrade progress that we have gone through so far. This will save users from having to register for every automatic upgrade. And upgrade process is activated through the click of the icon.



Place the automatic execution icon to the start menu to prompt the automatic upgrade when the system is booting.

Appendix

1. What is IPSec?

SecuwayPCI is based on the IPSec standard that manages security keys using IKE protocol. The IPSec standard and IKE protocol are:

1.1 IPSec Standard

IPSec (Internet Protocol Security Protocol) is Internet security standard that makes up for downsides of TCP/IP protocols and standardizes the IP protocol-based security services. The IPSec standard is documented in RFC 1828-1829, 2104, 2085, 2401-2412 and 2451 of IETF (Internet Engineering Task Force). SecuwayPCI is fully compliant with the requirements.

1.2 Features of IPSec

IPSec is highly flexible protocol designed to materialize multiple security services required of different Internet environments. IPSec is designed to accommodate the security requirements that arise with the development of Interent. IPSec has the following features :

- IPSec is an effective solution that addresses the shortfalls of TCP/IP communications and sets up the reliable paths for encrypted communications between hosts.

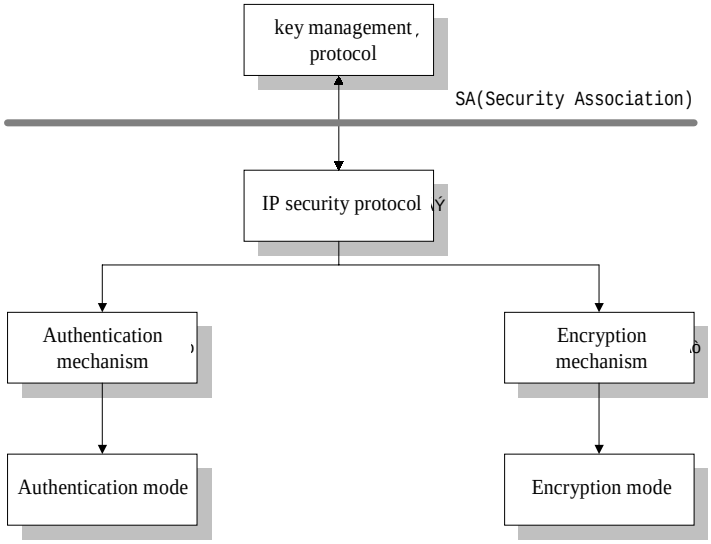
- The autonomous IP security protocol and key management mechanism ensures that IPSec is flexible to adapt to varied Internet environments.

- IP security protocol is divided into authentication (AH) and encryption (ESP), allowing users to select the security service suitable for their computing environment.

- It is easy to add a new security mode to security protocol. Various encryption and authentication algorithms are available.

1.3 Formation of IPSec

IPSec is broken down into IP security protocol and key management protocol. IP security standard and key management protocol work independently, but are still connected through SA (Security Association).



IP security standard consists of:

A) AH: Authentication Header that verifies the origin of IP packets and authenticity of packets and

B) ESP: Encapsulating Security Payload that provides the confidentiality of data transmission. Users can selectively choose from two mechanisms to their system requirements or choose both of them.

1.3.1 SA (Security Association)

SA is the logical settings for security mechanism, security mode, authentication, and encryption algorithms, key values, and other parameters. SA goes only in one direction requiring senders and receivers to set up and maintain their own versions. Set by key management protocol, SA is used to provide the security to IP protocol. SAs can be told apart by IP address and 32-byte SPI (Security

Parameter Index).

SA contains the following information:

- ✓ Types of security mechanism: AH and ESP
- ✓ SPI
- ✓ Security mode
- ✓ Self IP address
- ✓ IP address of a counterpart
- ✓ Authentication key
- ✓ Encryption keys
- ✓ Valid period of SA
- ✓ Packet sequential No.

1.3.2 Authentication mechanism

Authentication mechanism (AH) provides the connectionless integrity, data origin authentication, and anti-replay service.

An authentication mechanism measures MAC value of IP packets of a sending host and transfers the packets. For incoming hosts, AH measures the MAC value of them to see if it is the same as received value. Authentication key reads only two communicating hosts, eliminating the possibility of a third party copying IP packet and authentication information. AH tells apart authentic IP packets of a communicating host from unauthorized copies. Packet sequential number of 32-byte in AH is used to measure MAC (authentication information) preventing replay attacks that take advantage of the transferred IP packets.

With AH in use, the number “51” is placed on the next header field of IP header in front of AH, meaning that next AH comes up.

Next Header	Payload Length	Reserved
SPI		
Sequence Number		
Authentication Data		

When AH is used in transport mode the AH comes next IP header and before higher-level protocol or other IPSec header. IP packet is configured as follows allowing AH in transport mode work on the IP packets of the current standard IPv4.

Regular IP packets without AH

IP Header	TCP Header	Data

IP packets with AH

IP Header*	AH	TCP Header	Data

Authentication

(*) The field value is 51 on the next header of the IP header.

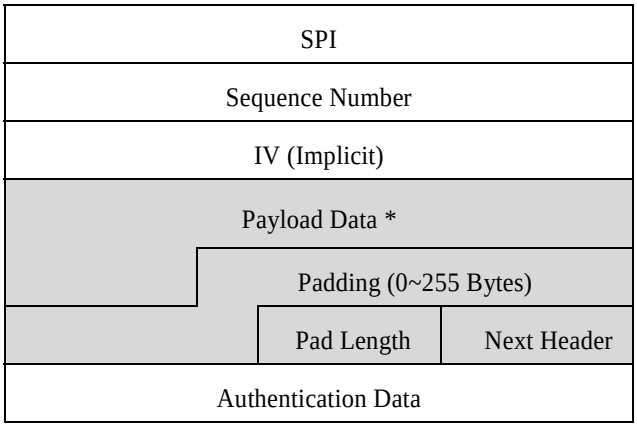
1.3.3 Encryption mechanism

Encryption mechanism (ESP) provides the IP packet data confidentiality and selectively includes the authentication information in order to support connectionless integrity, data origin authentication, and anti-replay service.

The encryption mechanism encrypts IP data (higher-level data) excluding the header to ensure

the confidentiality of communications. It measures the MAC value on ESP header and IP data to provide the encryption services. AH calculates all the authentication information related to IP packets, while the ESP factors in only the ESP components excluding the authentication information field.

When the ESP in place, the next header in the IP header has the number "50" for the field value to indicate that ESP is in use. The general formation of ESP is:



(*) Payload Data is IP packet data (upper-level).

With ESP in transport mode the ESP comes after IP header and before upper-level protocol or other IPSec header. IP packet has the following configuration when the ESP is in transport mode working on IP packets of the current standard IPv4.

Regular IP packets without ESP

IP packets with ESP

IP Header*	ESP Header	TCP Header	Data	ESP Trailer	Auth. Data

(*) The field value of the next header is 50 (inside the IP Header).

1.3.4 IKE Protocol

IKE protocol is a key management protocol that authorizes the hosts for IPSec communications and negotiates with SA to determine the process and formula of setting up, modifying, and deleting security keys.

IKE protocol manages the keys through two steps . In step 1 two hosts that are up for communications authorize each other and set up their own ISAKMP SA. In step 2 the IPSec SA comes into play for IPSec communications like AH and ESP. The ISAKMP SA formed in step1 protects the messages created in step 2. Each step sees negotiation, formation, key exchanges, and mutual authentication going on in preparation for SA information to be used later.

2. Definitions of Terminologies

■ AH (Authentication Header)

AH is an IPSec protocol that provides powerful connectionless integrity and data origin authentication to IP packets. It supports anti-replay service as an option to users.

■ ESP (Encapsulating Security Payload)

ESP is an IPSec protocol that guarantees the confidentiality of IP packets. On top of this, it provides connectionless integrity, data origin authentication, anti-replay service, and limited traffic flow confidentiality services.

■ Ethernet

Ethernet is LAN-based communication developed by private companies, such as: Xerox, Digital Equipment (DEC), and Intel. IEEE802.3 is the second version of Ethernet standard developed on the base of IEEE802.3 designation. Thus, Ethernet version 2 and IEEE802.3 can operate on one cable while Ethernet version 1 and 2 don't co-exist.

■ HOST

Hosts are nodes that are connected to network.

■ IPSec (Internet Protocol Security Protocol)

Developed by IPSEC Working Group, IPSec is standard Internet security protocol that overcomes the shortfalls of TCP/IP protocols in network and standardizes security mechanisms. It is designed to service the current IPv4 version as well as IPv6—the next generation Internet protocol. IPSec standard defines security protocols (AH, ESP) for network communications, SA, and key management protocols (IKE).

■ IPSec security mode

IPSec security mode refers to all security services activated on an IP packet. AH and ESP are applied to a packet: one in transport and the other in tunnel mode or all in transport mode simultaneously.

■ IPSec security profile

IPSec security profile is comprised of multiple security modes listed up in order of priority. The security profiles are used to negotiate with a corresponding IPSec host over IPSec SA in step 2 of IKE protocol.

■ SA

SA (Security Association) is a series of mechanisms and keys shared between hosts to protect communication information. The definition of communication information varies depending on security protocols.

■ SecuwayGate

SecuwayGate is hardware-typed security device that protects TCP/IP communications between network server interface and users or between multi-layered network interface and multiple users.

■ Security Rule

Security rules are the basic components of security policy. Security rules are comprised of the packets, security decision, and security mode for IPSec communication. Should a packet be eligible for security policy, the security rules allow, reject communication or pass for IPSec communications.

■ Making a decision

Decision is made on how to process a packet. The types of decisions are: "Allow the communications", "Disable the communication", and "IPSec communication" that uses key management.

■ Master key

Master key is the highest level of keys in IPSec security function. It has unique value to each IPSec host. SecuwayCenter determines the master keys.

■ Security policy

Security policy is a type of database that contains the rules on how to process IP packets in IPSec communications. Security policy is a list of rules that goes down in order of priority. Rules refer to

the internal information to decide whether to work on a packet or not. This reference check-up process goes on until a packet is matched with a right rule that will examine the packet. When no rule is found for a packet, the packet is discarded and the communications are interrupted. Security policy implemented in IPSec hosts, such as: SecuwayClient, SecuwayPCI, and SecuwayGate is divided into higher-level, lower-level, and user defined policy, according to a creator of the policy (either SecuwayCenter or host users). The security policy takes effect in above-mentioned order. The higher and lower-level policy are made in SecuwayCenter and delivered to IPSec hosts, while IPSec hosts draft user define policy.

■ Security token

Security token is software modules and hardware (SecuwayPCI) that provides log-on, encryption/decryption, measures/confirms authentication information, and manages time services (this is optional by products) for network communication security services. Security token is fully compliant with Cryptoki (PKCS#11) standard API by RSA.

■ User defined policy

This is a security policy made by IPSec hosts. User defined policy comes after higher and before lower-level security policies in order of priority.

■ Higher-level policy

Made by SecuwayCenter, higher-level policy has the highest priority among security policies. Higher-level policy is rules that must be implemented to IPSec hosts.

■ Lower-level policy

The lower-level policy takes the back seat to higher-level and user defined security. Made by SecuwayCenter, the lower-level policy governs on how to process a packet that is out of the scope of definition by IPSec users.

■ Communication allowed

"Communication allowed" is a decision that rules out IPSec security on handing an IP packet. This allows to income the IP packet as it is, without encryption.

3. Index

FCC NOTICE

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

NOTE: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.