

ViRobot GatewayWall for Unix Ver 3.0

Manual

■ **Copyright © 1998-2003 by HAURI Inc.**

First Edition/Second Published, February 2003

This software and documentation is sole property of HAURI and protected by copyright laws.

This documentation and software cannot, in whole or partially, be copied, duplicated, translated, or converted into electronic media or any machine readable form without prior

written consent of HAURI Inc.

■ Technical Support/Customer Support

USA : Global HAURI Inc.

Address : 3003 North First Street, Suite 234 San Jose, CA 95134
Homepage : <http://www.globalhuri.com>
Email : support@globalhuri.com, sales@globalhuri.com
Tel : +1 408 232 5463
Fax : +1 408 232 5464

Singapore : HAURI ASIA Pte. Ltd

Address : Block 750C, Chai Chee Road, #02-12 Technopark @ Chai Chee, Singapore
469003
Homepage : <http://www.huriasia.com>
Email : support@huriasia.com, sales@huriasia.com
Tel : +65 6243 7913/24 (Sales), +65 6243 7914/7915 (Technical support)
Fax : +65 6442 0223

Japan : HAURI JAPAN Inc.

Address : 4th Fl., MS Bldg., #11-5, Shiba 4-Chome, Minato-ku, Tokyo 108-0014, Japan
Homepage : <http://www.haurijapan.com>
Email : Japan@huri.net
Tel : +81 3 5444 7916
Fax : +81 3 5444 7980

China : China Blue Star Hauri Technology

Address : 15th Fl., Blue Star Bldg., No.17 Bei San Huan East Street, Chao Yang District,
Beijing 100029, P.R.C.
Email : support@cbht.com.cn
Tel : +86 10 6444 5900(Rep.), +86 10 6444 5911(Technical support)
Fax : +86 10 6444 5922

Korea : HAURI Inc.

Postal Code : 156-754
Address : 8th Fl., Yuhan Yanghang Bldg., 49-6, Daebang-dong, Dongjak-gu, Seoul,
Korea
Homepage : <http://www.huri.co.kr/>
Email : support@huri.net, sales@huri.net
Tel : +82 2 828 0820 (Rep.)
Fax : +82 2 828 0840

For the Reader

This Manual is for our registered users of ViRobot GatewayWall for Unix. The ViRobot GatewayWall for Unix Manual may be slightly different from your program due to ongoing functional improvements. ViRobot GatewayWall for Unix and HAURI are the registered trademarks of HAURI Inc.

Introduction

Your Manual consists of 5 chapters and an appendix.

Chapter 1 explains how to contact our customer support center and access useful information.

Chapter 2 describes features and installation requirements for ViRobot GatewayWall for Unix, as well as how to install or remove it.

Chapter 3 shows user how to execute and configure ViRobot GatewayWall for Unix in the web environment.

Chapter 4 explains how to execute and configure your ViRobot GatewayWall for Unix in the console environment.

Chapter 5 provides a guide for ViRobot GatewayWall for Unix administrator. Also, the appendix consist of some useful information, including virus definitions.

Table of Contents

Before You Begin

1. Registering Your Copy of ViRobot GatewayWall for Unix
2. How to Contact Us

I. Installation Planning

1. System Requirements
2. More information before installation
3. How to install

II. Getting Started with ViRobot GatewayWall for Unix

1. Features
2. Shipping package
3. Installation
4. Uninstalling your ViRobot GatewayWall for Unix

III. Running ViRobot GatewayWall for Unix in the Web Environment

1. Getting Started
2. Menus
3. GatewayWall
4. File scan
5. Update
6. Log

7. Statistical Data Management

8. Administrator

9. Help

IV. Running ViRobot GatewayWall for Unix in the Console Environment

1. Scan

2. Update

V. Administrator Guide of ViRobot GatewayWall for Unix

1. Installation Information

2. Configuring ViRobot GatewayWall for Unix Manually on the Console

3. Administrator Tips

Appendix

1. Symbols and Terminology

2. How to change the mail server's port

3. DNS Server Configuration

4. FAQ

Before You Begin

1. Registering Your Copy of ViRobot
2. How to Contact Us

1. Registering Your Copy of ViRobot

All registered customers will receive HAURI email newsletters and benefit from its various technical support, customer support, and product updates, as well as virus definitions and security information.

1) Information collection and use for customers

We may require you to fill in and submit a customer registration form of ViRobot GatewayWall for Unix Server. We will retain your information for one year (or the term specified on the optional 'HAURI Software License'), and you may modify your information at anytime.

2) Registered customers will enjoy the following benefits for one year (or the term specified on the optional 'Software License') at no extra cost.

- Regular engine updates on every Wednesday, and spontaneous update of our repair engine when a new virus is found.
- Newsletters on viruses and how to deal with them sent via "Security Alerts" mailing service once a week
- Consultations and enquiries regarding product usage are available over the phone, via email or through our Web site's bulletin board
- Free software upgrade for the same product within the registered period.
- Discounted price is given for some products (specified by HAURI) when you purchase a new product.
- Other complementary services provided by HAURI.
- After the customer support period expires, you can extend it by paying a minimal fee in order to continue to enjoy the benefits and services.

3) Customer Support

We aim to provide our registered customers with technical support for any problems that may occur during the use of our product, installed in a properly configured system and environment.

4) How to Register

You may register your ViRobot GatewayWall for Unix Server via the Internet. Visit our homepage (<http://www.hauri.net>) and use the on-line registration form. One time registration is sufficient. **Please note that Telephone and/or email registrations are not accepted.**

- Fill in the Customer Registration card included in the ViRobot product package and send it by mail or fax.
- Or use Online Customer Registration on HAURI Web site (<http://www.hauri.net>).

5) We highly recommend that you renew your registration when your customer support period expires.

Due to the characteristics of anti-virus program, you need to update the engine regularly to detect and remove new viruses. When you renew your registration, you will be entitled to an upgrade of your ViRobot for only a small percentage of the purchase price.

For more information, visit our homepage or contact our sales representative.

2. How to Contact Us

Most of the information you will need for the operation of ViRobot GatewayWall for Unix can be found here. However, if you require further assistance, please contact us at:

1) Internet

- HAURI Homepage at <http://www.hauri.net>
- E-mail
Technical/Customer Support at support@hauri.net
Purchase Inquiry at sales@hauri.net

2) Mailing Address and Telephone Number

USA : Global HAURI Inc.

Address : 3003 North First Street #234 San Jose, CA 95134

Homepage : <http://www.globalhauri.com>

Email : support@globalhauri.com, sales@globalhauri.com

Tel : +1 408 232 5463

Fax : +1 408 232 5464

Singapore : HAURI ASIA Pte. Ltd

Address : Block 750C, Chai Chee Road, #02-12 Technopark @ Chai Chee, Singapore 469003

Homepage : <http://www.hauriasia.com>

Email : support@hauriasia.com, sales@hauriasia.com

Tel : +65 6243 7913/24 (Sales), +65 6243 7914/7915 (Technical support)

Fax : +65 6442 0223

Japan : HAURI JAPAN Inc.

Address : 4th Fl., MS Bldg., #11-5, Shiba 4-Chome, Minato-ku, Tokyo 108-0014, Japan

Homepage : <http://www.haurijapan.com>

Email : Japan@hauri.net

Tel : +81 3 5444 7916

Fax : +81 3 5444 7980

China : China Blue Star Hauri Technology

Address : 15th Fl., Blue Star Bldg., No.17 Bei San Huan East Street, Chao Yang District, Beijing 100029, P.R.C.

Email : support@cbht.com.cn

Tel : +86 10 6444 5900(Rep.), +86 10 6444 5911(Technical support)

Fax : +86 10 6444 5922

Korea : HAURI Inc.

Postal Code : 156-754

Address : 8th Fl., Yuhan Yanghang Bldg., 49-6, Daebang-dong, Dongjak-gu, Seoul, Korea

Homepage : <http://www.hauri.co.kr>

Email : support@hauri.net, sales@hauri.net

Tel : +82 2 828 0820 (Rep.)

Fax : +82 2 828 0840

I. Installation Planning

1. System Requirements
2. More information before installation
3. How to install

1. System Requirements

Installing and Operating Environment

① Operating Systems

- Solaris Version
 - Solaris 2.6 (sparc 32), 2.7 (sparc32, sparc64), 2.8 (sparc64)
- HP-UX Version
 - HP-UX 11.x
- AIX Version
 - AIX 4.3

② System Resources

- Memory: 128MB (512MB recommended)
- HDD: storage space of about 30MB necessary for installing ViRobot G/W and a minimum storage space of 1G for log and backup

③ Executable environment (mail server)

- Functions on Sendmail, Qmail or other mail servers
- Any mail server with a modifiable receiving port can be used

The above system requirements are only a summary of the minimum requirements. Detailed H/W requirements will be discussed.

2. More Information Before Installation

Before you make a decision regarding the installation of ViRobot GatewayWall onto the existing mail server or onto a separate server, you need to take note of the following issues:

- **Ability to modify the service port number of your mail server**
- **H/W environments of your mail server**
- **Decisions of your team and/or management**

First, you should determine whether you are able to change the service port number of the existing mail server.

In order to distinguish different Internet services based on TCP/IP, each service is assigned with its own Port Number. For instance, TCP/25 belongs to the Mail while TCP/80 belongs to the Web. Due to its mail service functions, ViRobot GatewayWall uses TCP/25 port number. Therefore, to install ViRobot GatewayWall onto the existing mail server, you will need to change the mail server's port. If the mail server's port is not modifiable, you will need to install ViRobot GatewayWall onto a new server that is placed before the mail server.

Secondly, you should check the H/W status of you current mail server.

You should ensure that the existing mail server has enough memory to operate efficiently when ViRobot GatewayWall is installed in it. In other words, a mail server administrator's accurate assessment is required in this case, based on the statistics of CPU and the memory usage rates (with regards to the maximum number of mails processed per day, or the number of mails processed per hour) in the mail server. If your mail server does not fulfill the requirements, you will need to upgrade it. However, if the mail server cannot be upgraded, but is port-modifiable, we recommend the installation of ViRobot on another server in order to avoid any problems that may arise in the future. Please note that if you are installing ViRobot on a separate server without any statistical data of the existing mail server, a mail server level (or higher) H/W is recommended.

Thirdly, you need to discuss ViRobot GatewayWall installation issue with your team and/or management.

You should decide between installing ViRobot on the existing mail server or on another server that is placed before the mail server.

2.1 Key features of installation options

- Installing ViRobot on the existing mail server
 - Easy installation of ViRobot.
 - No additional H/W required – no extra costs.
 - Virus disinfection is available for both incoming and outgoing mail.

- Installing ViRobot on another server that is placed before the mail server
 - Additional H/W and modification of DNS configurations required.
 - Although virus disinfection for incoming mail is available, you will need to change the SMTP address of mail clients for disinfection of outgoing mail.
 - Improvement on mail server system as ViRobot blocks malicious mails prior to the mail server.

Detailed information about both installation options of ViRobot GatewayWall is available in the next page.

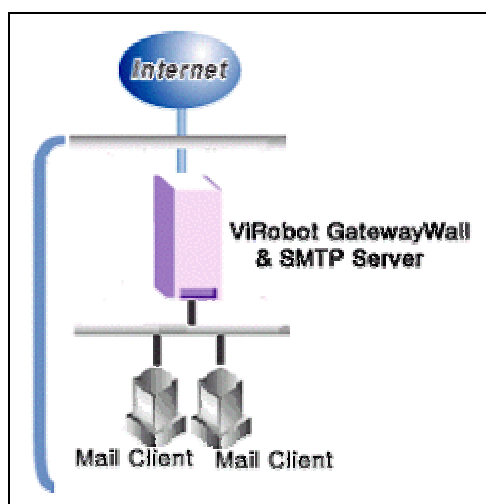
3. How to Install

3.1 Single Server

Install ViRobot on the mail server

In order to install ViRobot GatewayWall for Unix on the current mail server, you will need to change the port assigned to the mail server. In other words, you should set ViRobot GatewayWall for Unix to use the basic service port 25, and set the existing mail server to use another port so that both virus disinfection and mail service are available on the same mail server. If the mail server is neither Sendmail nor Qmail but is port-modifiable, you can install, execute ViRobot GatewayWall for Unix on it.

(Please refer to the Appendix 2. How to change mail server's port.)

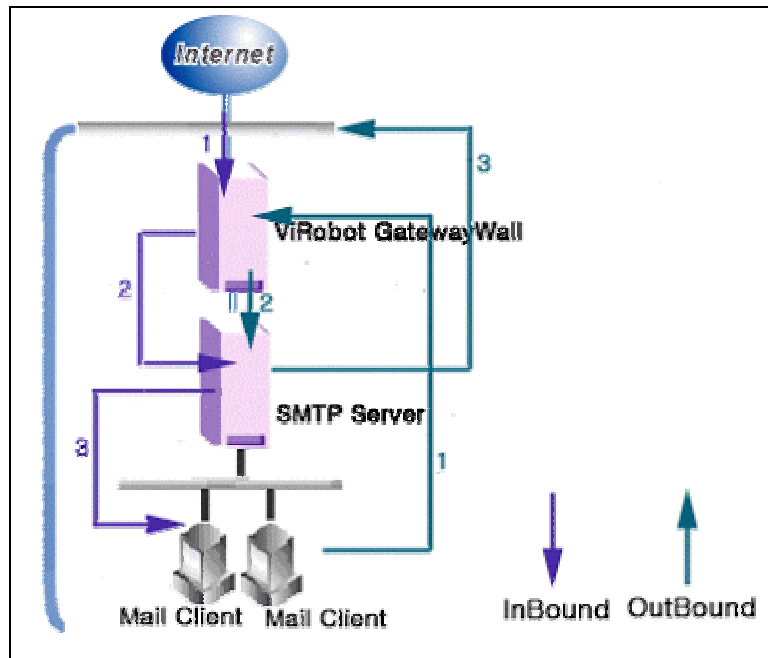


1. Install ViRobot GatewayWall for Unix onto SMTP Server.
2. Stop the SMTP service and change the port from 25 to another port. (E.g. port 5555)
3. Start the SMTP service, and set mail server address or port in Set G/W server. Next, access the Server that ViRobot GatewayWall for Unix is installed in. ([http://\[URL or IP of Server that has ViRobot installed\]:8080/](http://[URL or IP of Server that has ViRobot installed]:8080/))

Installing ViRobot on another server (placed before the mail server)

You do not have to change the existing mail server's port number when you install ViRobot GatewayWall for Unix separately. After its installation, you need to change the MX value set in DNS in order to forward incoming mails to ViRobot GatewayWall for Unix system. (For more information on MX value modifications, please refer to **Appendix 3. Set DNS server.**) You can improve your system performance and completely prevent malicious mails by installing

ViRobot GatewayWall for Unix on another server that is placed before the mail server.



1. Install ViRobot GatewayWall for Unix onto Server.
2. Set mail server address (host domain or IP) in Set G/W server via Web Browser after you have connect to the server, which ViRobot GatewayWall for Unix is installed in.
([http://\[URL or IP of Server that has ViRobot installed\]:8080/](http://[URL or IP of Server that has ViRobot installed]:8080/))

- **Inbound**

Virus disinfection against incoming mail is available.

1. ViRobot GatewayWall receives incoming mails through port 25.
2. After ViRobot GatewayWall blocks virus, spam, and other malicious mails, it forwards normal mails to SMTP Server.
3. SMTP Server forwards normal mails to each mail client.

- **Outbound**

For disinfection of outgoing mail, you will need to change SMTP address of mail client.

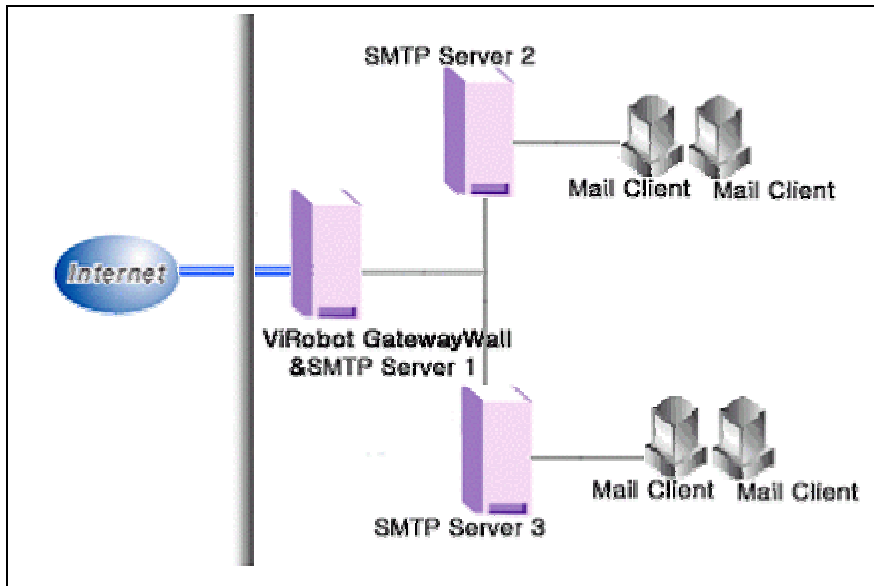
1. ViRobot GatewayWall checks outgoing mail for virus infections.
2. ViRobot GatewayWall forwards the mail to SMTP Server.
3. SMTP Server forwards the mail to the external mail server.

3.2 Multiple Servers

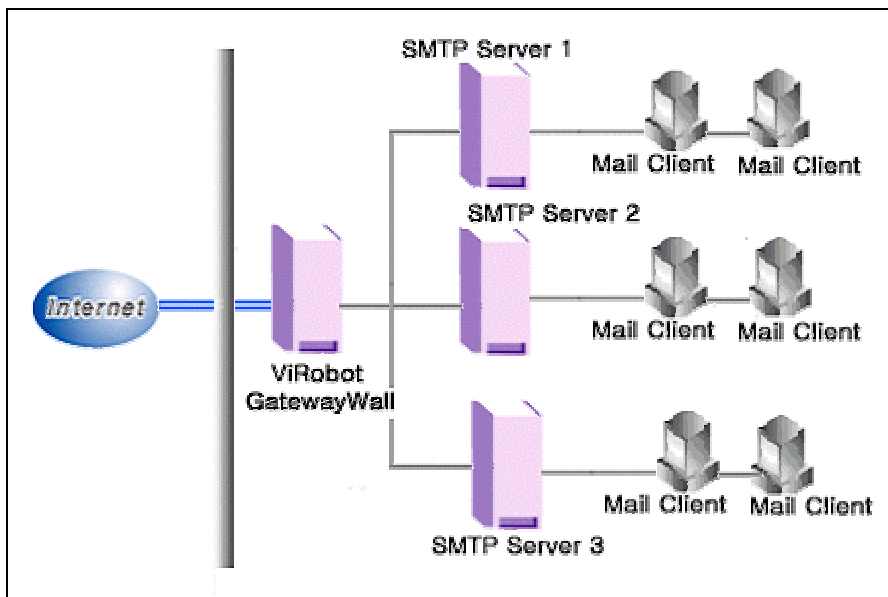
ViRobot GatewayWall supports multiple servers even if each mail server's domain is different.

Diagram of Multiple servers

- Install ViRobot GatewayWall on the existing mail server



- Install ViRobot GatewayWall on a server that is placed before the mail server



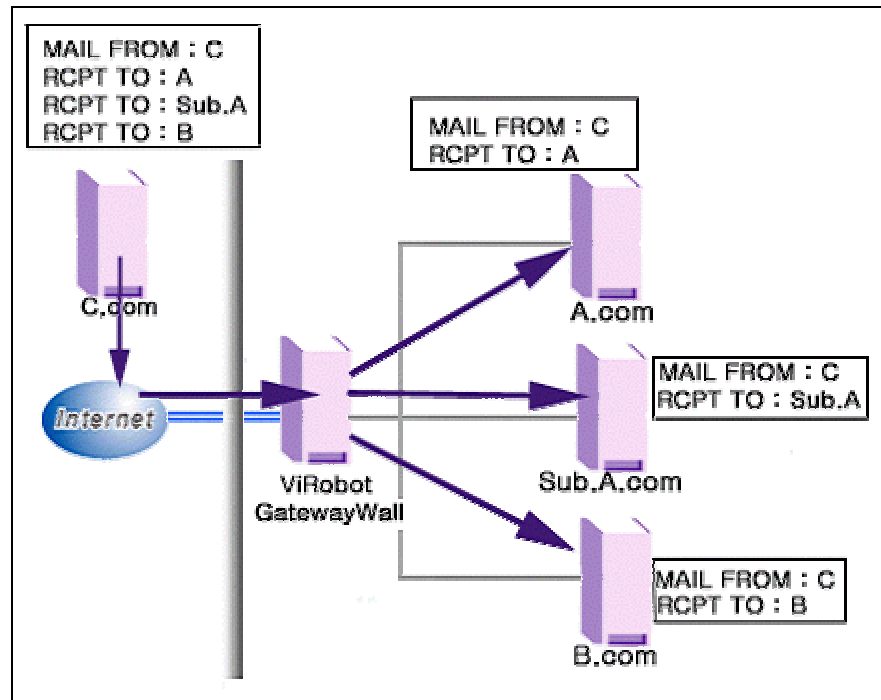
Example of Multiple Servers Support

- Example of multiple servers support (Install ViRobot GatewayWall separately)

Domain	Mail Server	Port Number
A.com	123.124.125.126	25
Sub.A.com	127.128.129.130	25
B.com	131.132.133.134	25
C.com	134.135.136.137	25

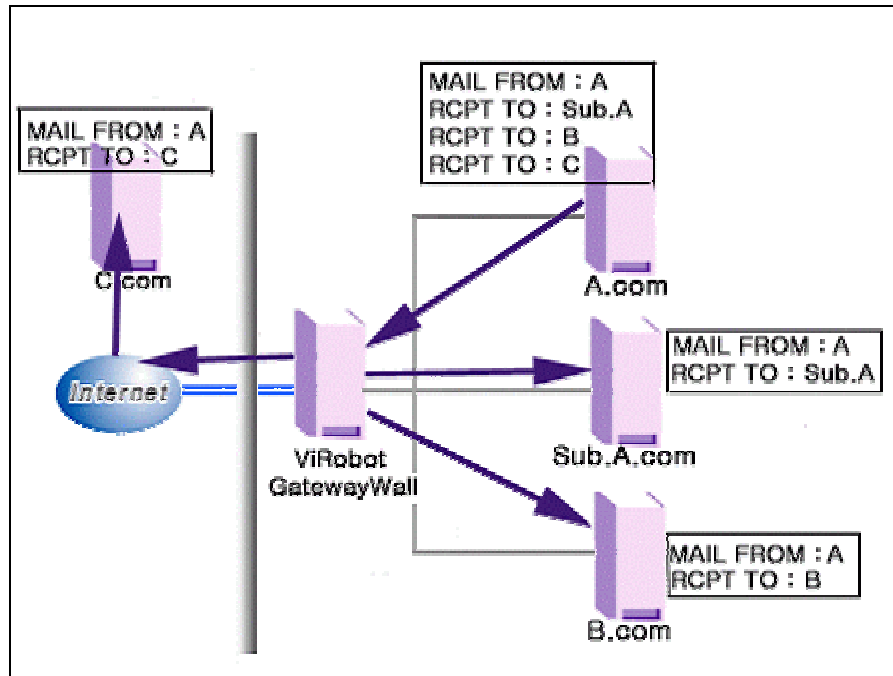
※ C.com : External Mail

- 1) Install ViRobot GatewayWall separately and place it before the mail server



- When external mail server (C.com) sends a mail to Domain A.com, Sub.A.com, and B.com :
 1. ViRobot GatewayWall receives the mail forwarded from the external mail server. (Port 25)

2. After blocking virus mail, spam, or other malicious mails, ViRobot GatewayWall forwards a normal mail to each mail server at the domain registered.



- When internal mail server (A.com) sends a mail to B.com, Sub.A.com, and C.com :
 1. ViRobot GatewayWall receives the mail and checks for virus infections.
 2. The normal mail is forwarded to each mail server at the domain registered.

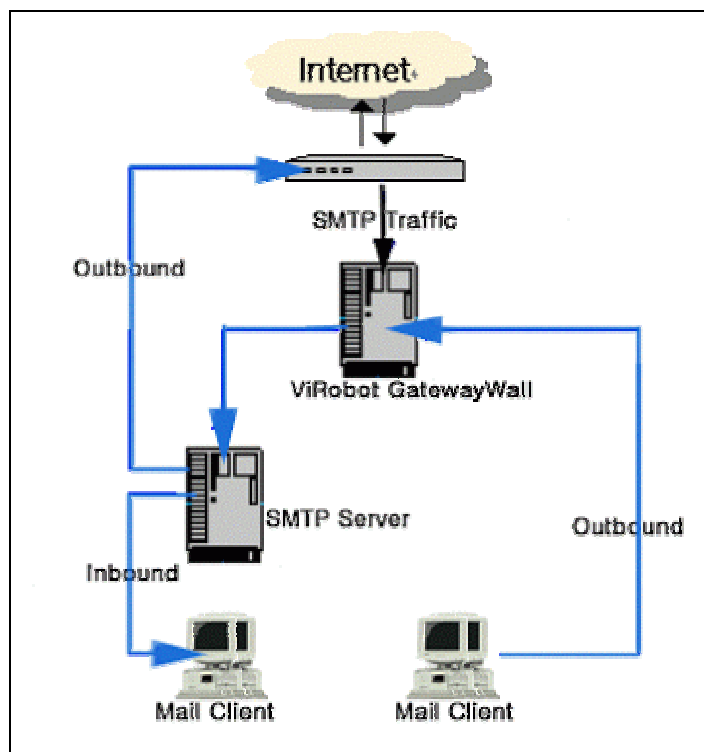
II. Getting Started with ViRobot GatewayWall for Unix

1. Features
2. Shipping Package
3. Installation
4. Uninstalling your ViRobot GatewayWall for Unix

1. Features

Product name: **ViRobot GatewayWall for Unix Version 3.0** (henceforth refer as “ViRobot G/W”)

ViRobot GatewayWall for Unix is a mail server antivirus program developed by HUARI Inc. with its unique technologies. ViRobot is capable of intercepting spam mails, detecting virus mails, and removing viruses. It allows the administrator to administrate the mail server anywhere, anytime, thanks to the Web user interface. This superb antivirus software’s powerful logging function also helps to increase the work efficiency of the administrator.



■ Powerful ViRobot Engine

Your ViRobot G/W is equipped with powerful ViRobot engine to offer reliable detections and repairs. With ViRobot’s advance functions that detect unknown viruses in all platforms (DOS, Windows, Macro, Java Applets, etc.), your system is always updated and protected against any new virus.

ViRobot engines are already loaded on many other information security products.

■ **Blocking Virus Received through Mail**

In order to protect users from infections and/or inconveniences, all messages that are sent and received via mail server equipped with ViRobot G/W are simultaneously scanned for spam mail and viruses. When an infected message is detected, an alert mail is sent to the administrator via email as well as to the recipient and sender.

■ **Support for System Self-disinfection**

ViRobot G/W includes a ViRobot G/W module that supports file system disinfection. It provides email disinfection and disinfection of the server on which it is installed.

■ **Support for Various Operating Systems**

Since email disinfection modules are operated at the server level, ViRobot G/W provides diverse support for Solaris, HP-UX, AIX operating systems.

■ **Enhanced Update**

Due to the characteristics of antivirus software, it is essential for you to update your engine periodically. You can update your engine through HTTP and use the scheduled update function for your convenience.

■ **Filtering**

ViRobot G/W offers integrated filtering that is indispensable for blocking email viruses that are widespread. It includes filtering that blocks attached files before they are able to infect any PC, content filtering for blocking spam mail, email size filtering that blocks messages which can cause network overload, sender filtering that blocks messages from specific sender and IP filtering that blocks messages from specific IP address.

■ Mail Resending

You may set up your ViRobot G/W to backup the original messages of blocked mail. If a very important message has been blocked or lost, the administrator may resend the original message to you.

■ Convenient Log and Backup Management

You can log and view the result of file scan, virus detection during system self-test or email transactions, inbound and outbound mails, virus mails, spam mails, and other emails. The infected file can be backuped for resending. You may set the period of logging and the size of log and backup files for system management.

■ Scanning Compressed Files

Your ViRobot G/W supports various compressed file formats including ZIP, ARJ(JAR), LZH(LHA), RAR, and ACE. It will detect and remove any virus in a multi-compressed file by its compression level.

■ Administrating ViRobot through Web Browser

ViRobot G/W allows easy remote configurations, detection and removal of viruses through its web interface. In addition, operations such as update of module, patches, new functions, or execution files, can be performed remotely via Web interface or console mode.

■ Administrating ViRobot through Web Browser

ViRobot GatewayWall for Unix provides statistical data that enables user to view the ratio of spam mail, virus mail and normal mail, incoming rates, and filtering status, sorted according to day/week/month. In addition, it is able to display these data in graphical format, thus helping in the creation of statistical reports concerning the mail server.

2. Shipping Package

Enclosed with the ViRobot G/W package are :

- 1 CD-ROM
- Manual
- Customer registration card, Software license

3. Installation

3.1 Files for ViRobot G/W

[Folder Description]

- ① **Install.sh** – To install ViRobot GatewayWall
- ② **setup** – To set up the product
- ③ **virobot.tar** - ViRobot tar module
- ④ **VRUninstall** – To remove your ViRobot GatewayWall

3.2 Loading the CD-ROM

- ① Insert your ViRobot G/W CD in the CD-ROM drive.
- ② The setup program will start automatically. If not, follow the instruction below:

- Solaris

```
# mount /dev/dsk/##t6d0s2(CD-ROM Device Name) /cdrom(Directory to start installation)
```

- HP-UX

```
# mount /dev/dsk/##t2d0(CD-ROM Device Name) /cdrom(Directory to start installation)
```

- AIX

```
# mount /dev/cd0(CD-ROM Device Name) /cdrom(Directory to start installation)
```

[Warning] CD-ROM device name may be different on different system.

3.3 Installing ViRobot

Connect to the server console to install ViRobot Gatewaywall for Unix with root-level privileges.

- ① Move to the directory that you have mounted the CD-ROM.

```
[root@localhost ]# cd /cdrom (Mount Directory)
[root@localhost cdrom]#
```

- ② Check the list of the directory.

- ③ Move to the directory for your operating system.

```
[root@localhost cdrom]# cd solaris6_sparc32
[root@localhost solaris6_sparc32]#
```

- ④ Run **./Install.sh** or **sh Install.sh** command to start installation.

```
[root@localhost solaris6_sparc32]# ./Install.sh
```

- ⑤ When the installation process starts, you will see a message prompting you to enter the product serial number. Enter the **serial number** provided on the CD and press Enter.

ViRobot GatewayWall for Unix

10 Sep 2002 Korea

Copyright (c) 1998-2003 HAURI Inc.

All rights reserved

E-mail : support@huri.net

Version 3.0

Type your Serial Number :

- ⑥ The following message will appear upon entering the correct serial number.

```
-----  
ViRobot GatewayWall for Unix                               10 Sep 2002 Korea  
Copyright (c) 1998-2003 HAURI Inc.                         All rights reserved  
E-mail : support@hauri.net                                 Version 3.0  
-----  
  
Type your Serial Number : vrtm-xxxx-xxxx-xxxx-xxxx  
  
ViRobot GatewayWall for Unix configuration -----  
[1] Temporary Path      : /tmp  
[2] Install Path       : /usr/local  
[3] Port                : 8080  
[4] Server IP          : xxx.xxx.xxx.xxx  
[5] Set Defaults  
[6] Exit  
[0] Save and proceed to install  
  
-----  
Choose Number :
```

You can change the installation environment of your ViRobot G/W here.

- [1] Temporary Path : Specify the temporary folder to be created during installation.
- [2] Install Path : Directory to install your ViRobot G/W.
(Requires more than 30Mb of free hard disk space)
- [3] **Port** : HTTP port number to connect.
- [4] **Server IP** : IP address of the server. Please **change** this field if you are using different IP address.
- [5] **Set Defaults** : Revert any changes back to default value.
- [6] **Exit** : Exit from the screen.
- [0] **Save and proceed to install** : **Start Installation** after storing the current setting.

[Warning]

1. You cannot use port 80 if you are operating your site on the Apache Web Server. The usage of port 80 in this case will cause collision with the existing port, resulting in the malfunction of Apache Web Server. **(Port 8080 is recommended by default.)**
2. Please enter the server IP that is provided to your computer. Remote administration will not be available through 127.0.0.1 (local IP).
3. If you need to change the specified port or server IP, you can do so by modifying the Apache configuration file. After modifying the Apache configuration file, you should restart the Apache Web Server.

```
# cd [ViRobot Installation Directory]/ViRobot/etc/apache
# vi httpd.conf
# cd ../../sbin
# ./apachectl restart
```

- ⑦ Once the configuration is completed, enter **0** to start installation.
- ⑧ You will see a message stating “Press Enter key to start install...” during installation.

```
Press Enter key to start install.
```

Press Enter key to continue with the installation.

- ⑨ When the installation is successfully completed, you will see a message “Install complete ViRobot G/W” on the screen.

```
Install complete ViRobot GatewayWall for Unix.
[root@localhost unix_i386]#
```

3.4. Starting the Service

After completing the program installation, you may set up the environment and run the program to start the proxy service.

[Warning] Please complete environment setup before running the program. Otherwise, you may encounter errors or failure in the operation of the program. Refer to '**III. Running GatewayWall for Unix in the Web environment**' to run the program right after completing environment setup on the Web.

1) Running ViRobot in the Web Environment

You may run the program by using "Service" in the [GatewayWall] > [Set G/W server] menu. Please refer to '3. GatewayWall' in 'III. Running ViRobot GatewayWall for Unix in the Web Environment'.

2) Running ViRobot in the console

To run the program in the console, use the following method.

```
[root@localhost] cd [ViRobot Installation Directory]/ViRobot/proxy/sbin
[root@localhost sbin]# ./start.sh (or # sh start.sh)

*** ViRobot GatewayWall for vrproxyd Restarting ***

*** ViRobot GatewayWall for vrspold Restarting ***

*** ViRobot GatewayWall for vrchecker Restarting ***
[root@localhost sbin]#
```

For more details on the usage of vrstart, see '3. Tips for Administrator' in 'V. Administrator Guide of ViRobot GatewayWall for Unix.

4. Uninstalling your ViRobot GatewayWall for Unix

When you install your ViRobot G/W, the utility to **remove** the product automatically will be stored in “**/sbin/VRUninstall**” directory. Use this utility to remove your ViRobot easily.

- ① Move to **/sbin** directory.

```
[root@localhost ]# cd /sbin  
[root@localhost sbin]#
```

- ② Check if **VRUninstall** file is there in the directory.

```
[root@localhost sbin]# ls VRUninstall  
  
VRUninstall
```

- ③ Run **VRUninstall**.

```
[root@localhost sbin]# ./VRUninstall
```

- ④ Enter 'y' and press Enter to remove your ViRobot G/W.

```
[root@localhost sbin]# ./VRUninstall  
  
Do you uninstall ViRobot GatewayWall for Unix? (y/n) y
```

- ⑤ You will see the message shown in the figure below when the uninstallation is successfully completed.

```
[root@localhost sbin]# ./VRUninstall  
  
Do you uninstall ViRobot GatewayWall for Unix? (y/n) y  
  
ViRobot GatewayWall for Unix files removed.  
  
ViRobot GatewayWall for Unix information removed.  
  
ViRobot GatewayWall for Unix removed.  
  
[root@localhost sbin]#
```

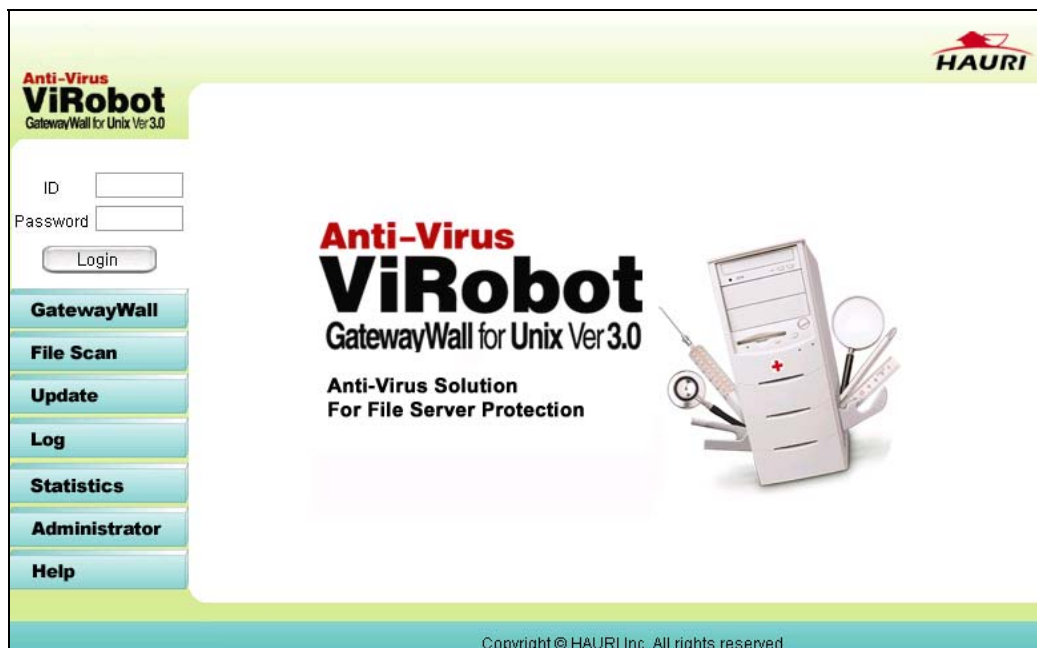
III. Running ViRobot GatewayWall for Unix in the Web Environment

1. Getting Started
2. Menus
3. GatewayWall
4. File Scan
5. Update
6. Log
7. Statistical Data Management
8. Administrator
9. Help

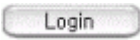
1. Getting Started

- ① Open your web browser. (Microsoft Internet Explorer 5.0 or higher version is recommended.)
- ② Enter the **address** (IP or URL) of the server, in which ViRobot G/W is installed, in the address box of browser.
- ③ Enter ':' and **port number** to the address that you have entered. The screen shown below will appear upon successful connection to the server.

How to Connect - [http://\[URL or IP address of the server\]: Http Port/](http://[URL or IP address of the server]: Http Port/)
(E.g. <http://222.222.222.222: Http Port/>)



[Fig. 3 – 1, Sign-in to access ViRobot G/W on the Web]

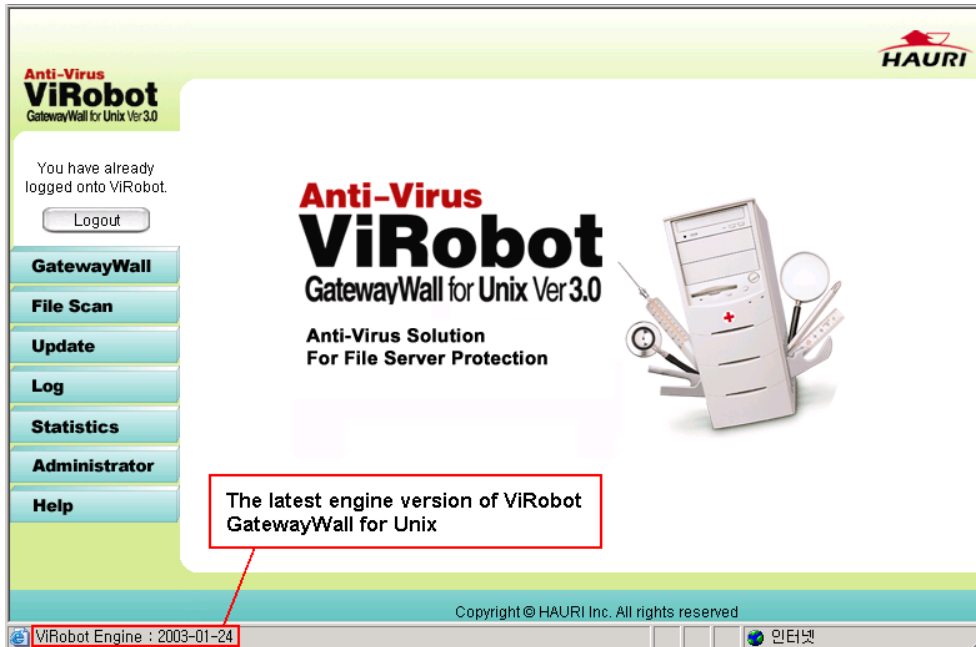
- ④ You will need to use the default user ID and password for the initial logon.
The default user ID and password are 'virobot' and 'admin', respectively.
(Case sensitive)
- ⑤ Click  at the bottom of the screen to proceed.

[Warning] If the http service on the server is restarting or unavailable, the web interface for ViRobot G/W may not work. Try the following on the server before you connect from the client.

```
[root@localhost /root]# cd [ViRobot Installation Directory]/ViRobot/sbin
[root@localhost sbin]# ./apachectl restart
./apachectl restart: httpd not running, trying to start
./apachectl restart: httpd started
[root@localhost sbin]#
```

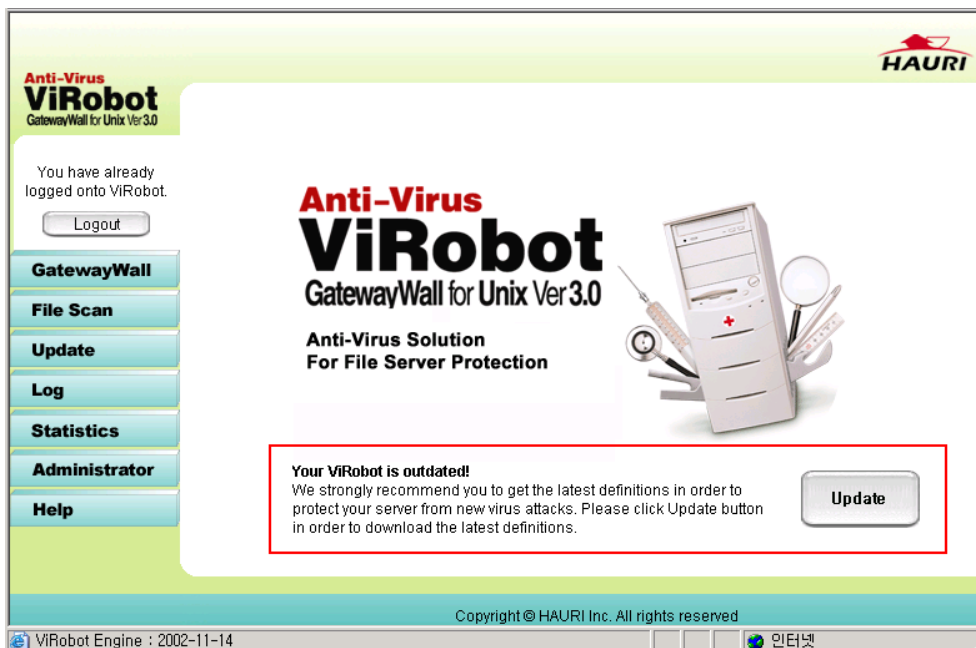
2. Menus

Once the correct user ID and password are entered, the screen shown in the figure below will appear.




[Fig. 3 – 2, Sign-in to access ViRobot G/W on the web]

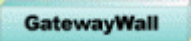

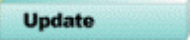

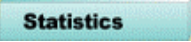
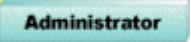

The windows shown below will be displayed if ViRobot is outdated for more than 15 days.



[Fig. 3 – 3, ViRobot has been outdated for more than 15 days.]


Click  to access Update menu. (Please refer to '5. Update')

2.1. Menubar

- ①  - For configuring the ViRobot G/W server and scanning/blocking of mail.
- ②  - For scanning of the ViRobot G/W server's file.
- ③  - For update of the engine and module.
- ④  - For viewing the Email log, file scan log, and update log.
- ⑤  - For viewing the statistical data of the mail server over different period of time.
- ⑥  - For modification of the administrator information and to set the IP addresses that are permit to access the server through the web interface.
- ⑦  - Product information and help.

3. GatewayWall

This menu contains the basic settings for ViRobot G/W, virus blocking and mail filtering.

Click  and the following menu will be shown.

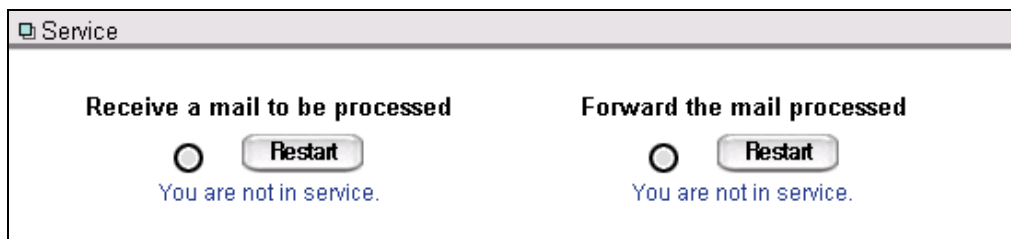
GatewayWall

- Set G/W Server
- Set Virus Protection
- Set Mail Filter
- Set Spam Blocking

3.1. Set G/W Server

This is used to manage data and functions that are essential for the operation of ViRobot G/W.


- ① Click [Set G/W server] from the sub-menus in the [GatewayWall].

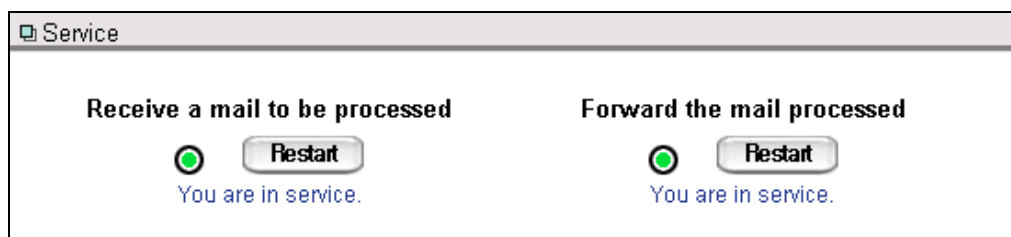


[Fig. 3 – 4, Suspend mail service]


Receive a mail to be processed : To receive a mail to be processed by the server.

Forward the mail processed : To forward the mail processed by the server.

Click  to restart any service. If the server is in service, the LEDs will light up in green. (shown below)



[Fig. 3 – 5, Start mail service]

[Warning] For initial execution of the program (after installation), please click  after completing the configuration.

Set Mail Server Domain

- Server configurations status : **Single server support**
- Change server configurations : **Change to multiple server**

Use it as a relay server
 [Notice] If you click "Use it as a relay server", some external users may use it illegally.

Mail domain **Add**

Delete



Mail Server Domain or IP Port

[Fig. 3 – 6, Set Mail Server Domain - **Single server support**]

Set Mail Server Domain

- Server configurations status : **Multiple servers support**
- Change server configurations : **Change to a single server**

Use it as a relay server
 [Notice] If you click "Use it as a relay server", some external users may use it illegally.
 For multiple servers, the domain listed on the top is available to be used as a relay server.

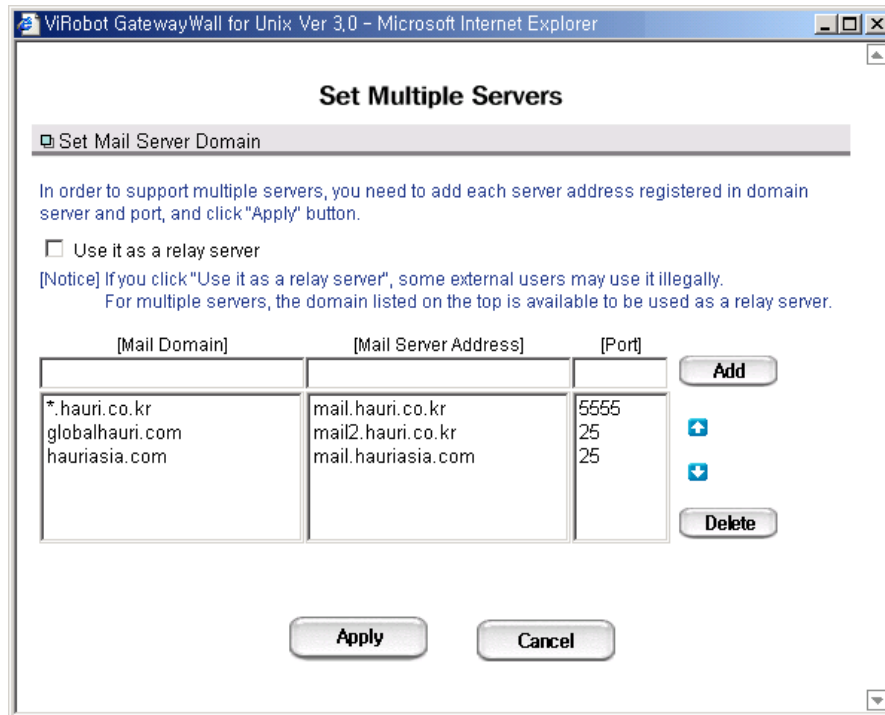
[Mail Domain]	[Mail Server Domain or IP]	[Port]	
*.hauri.co.kr	mail.hauri.co.kr	5555	Add   Delete
globalhauri.com	mail2.hauri.co.kr	25	
hauriasia.com	mail.hauriasia.com	25	

[Fig. 3 – 7, Set Mail Server Domain - **Multiple servers support**]

[Notice] As shown above, the interface of mail server domain configurations for single server support is different from the multiple server support.

- **Server configuration status** : It indicates your server status (single or multiple) supported by G/W
- **Change server configuration** : You can change to single mail server support or multiple mail servers support.

- ❖ When you click on **Change to multiple server** button, the following window is displayed.



[Fig. 3 – 8, Change to Multiple Servers]

- **Use it as a relay server** : To use the server as a relay server. For multiple servers, the domain listed on the top is available to be used as a relay server.
- **[Mail Domain]/[Mail Server Address]/[Port]** : Add a mail domain name registered in DNS into [Mail Domain], and add a mail server address (host domain or IP) and port number into [Mail Server Address]/[Port]. GatewayWall will process any mails sent to the registered domain first before sending them to the mail server.

✂ You can set mail domain as follow.

E.g. huri.co.kr - Register "huri.co.kr" domain.

***huri.co.kr** - Register all the sub-domains of "huri.co.kr".

(mail.huri.co.kr or unix.huri.co.kr is included, but huri.co.kr is not)

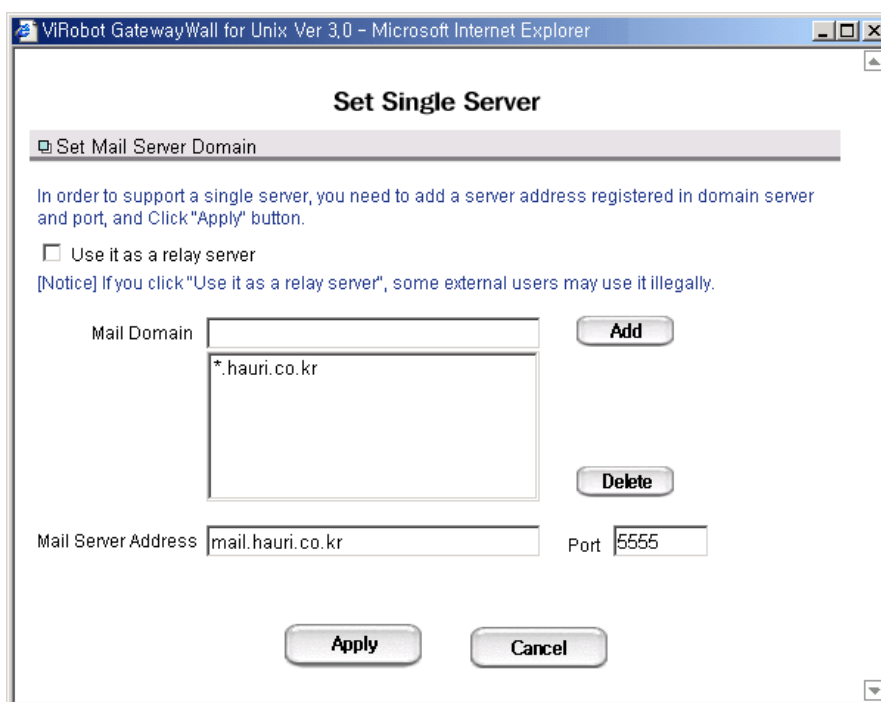
huri.* - huri.co.kr, huri.net, or huri.com is included.

huri.co.* - huri.co.kr, or huri.co.jp is included.

[Notice] When you click on the "Apply" button after configurations for multiple mail servers, Multiple Servers Support/[GatewayWall] > [Set G/W Server] > [Set Mail Server Domain] is automatically modified (shown above).

[Warning] If you enable "Use it as a relay server", some external users may use the server illegally.

- ❖ When you click on the **Change to a single server** button, the following page is displayed.



[Fig. 3 – 9, Change to Single Server]

- **Use it as a relay server** : To use the server as a relay server.
- **Mail Domain** : Add a domain name registered in DNS.

⊗ You can set mail domain as follow.

E.g. hauri.co.kr - Register "huri.co.kr" domain.

***huri.co.kr** - Register all the sub-domains of "huri.co.kr".

(mail.huri.co.kr or unix.huri.co.kr is included, but huri.co.kr is not)

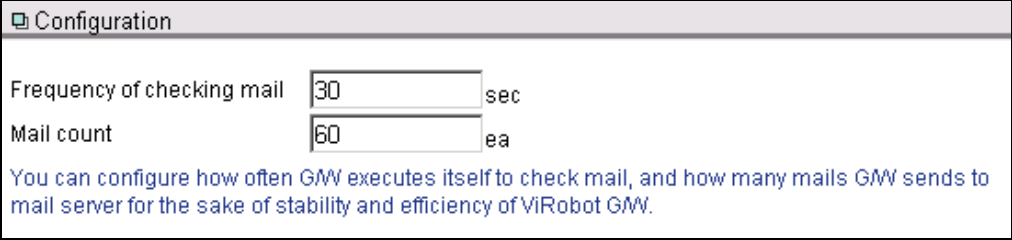
huri.* - huri.co.kr, huri.net, or huri.com is included.

huri.co.* - huri.co.kr, or huri.co.jp is included.

- **Mail Server Address/ Port** : Add a mail server address and port that the processed mail is sent to.

[Notice] If you click on the "Apply" button after configurations for a single mail server, Single Servers Support/[GatewayWall] > [Set G/W Server] > [Set Mail Server Domain] is automatically modified (shown above).

[Warning] If you enable "Use it as a relay server", some external users may use the server illegally.



The screenshot shows a window titled "Configuration". It contains two input fields: "Frequency of checking mail" with the value "30" and "sec", and "Mail count" with the value "60" and "ea". Below the fields is a blue text note: "You can configure how often GW executes itself to check mail, and how many mails GW sends to mail server for the sake of stability and efficiency of ViRobot GW."

[Fig 3 – 10, configuration]

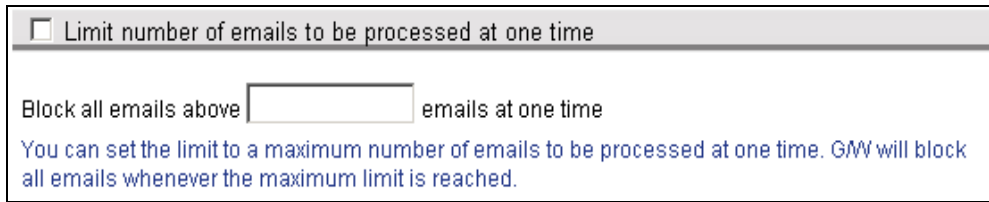
- **Frequency of checking mail** : You can configure how often G/W executes itself to check for mail. The default is 30 seconds; the allowed range is 1~3600 seconds.
- **Mail count** : Set how many mails G/W sends to mail server. Defaulted at 60, the number may vary from 1 to 200.
- **The administrator may change these values according to the system performance.**



The screenshot shows a window titled "Limit Mail Size" with an unchecked checkbox. Below the title is an input field containing the number "3" followed by the text "MB or higher size mail blocking". A blue text note below reads: "You can limit the mail size from 3MB."

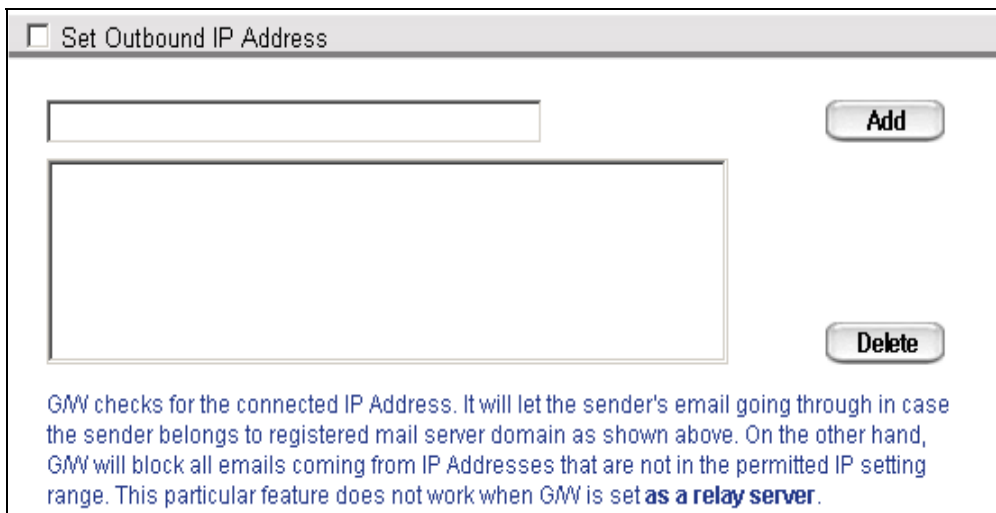
[Fig 3 – 11, Limit Mail Size]

Limit mail size : You can limit the mail size from 3MB onwards. Enter the size limit that is suitable for your environment.



[Fig 3-12, Limit number of emails to be processed at one time]

Limit number of emails to be processed at one time : You can set the limit to a maximum number of emails to be processed at one time. G/W will block all emails whenever the maximum limit is reached. The feature is useful to block any spam message, which are randomly sent at one time. (You can set the limit to a number that is greater than 1)

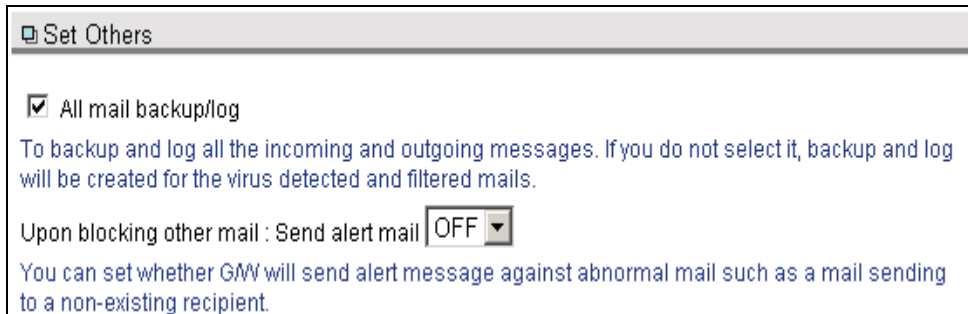


[Fig 3-13, Set Outbound IP Address]

Set Outbound IP Address : You can configure G/W to check sending emails for valid IP Address before sent out from the SMTP server. The sender must be in the registered mail server domain to have a valid IP Address. A domain is registered under [Set G/W server] > [Set Mail Server Domain]. G/W checks for valid connected IP Address, and blocks all other emails that do not belong to registered mail server domain. This particular feature does not work when G/W is set as a relay server.

E.g : Set a specific IP Address – 222.222.222.222

Set a IP Address Range – 172.1.1.*



[Fig 3 – 14, Set Others]

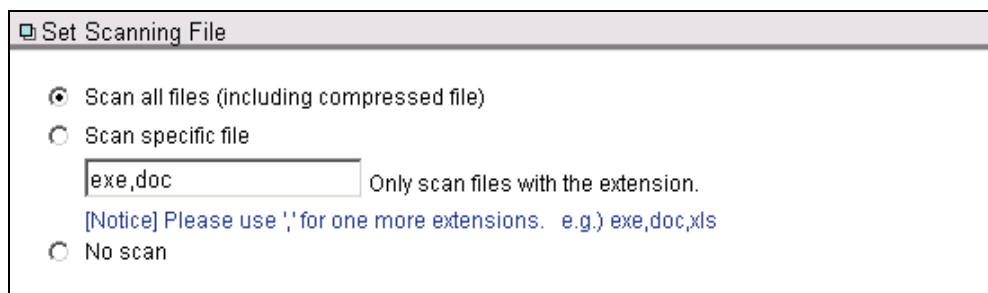
All mail backup/log : To backup and log all the incoming and outgoing mails. If this is not enabled, backup and log will be created for virus and filtered mails only.

Upon blocking other mail : G/W sends an alert message against irregular mails such as mail sending to non-existing mail recipient. An options, which you can choose to receive an alert mail, is newly updated. If you set off, alert mail will not be sent out.

3.2. Set Virus Protection

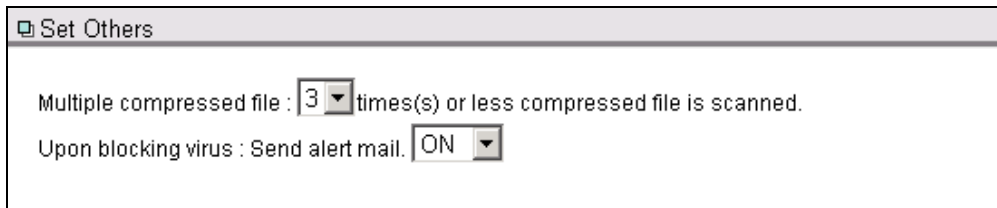
Using this menu, you can configure the virus scan for all mail attachment files and enable the function of sending alert mails whenever a virus is detected.

- ① Click [Set Virus Protection] from the sub-menus in the [GatewayWall].



[Fig. 3 –15, Set scanning file]


- **Scan all files** : Scans all files attached to the mails.
- **Scan specific files** : Scans files with specified extensions.
- **No scan** : Disables virus scanning of the attached files.



[Fig. 3 – 16, Set others (compression and alert mails)]

- **Multiple compressed file** : Scans multiple compressed files in 3 stages.
- **Send alert mail** : To send alert mails upon detection of virus mail attachments, set this option to ON. You may change the alert mail recipient using [Administrator] > [Set alert mail] menu (please refer to '7. Administrator').

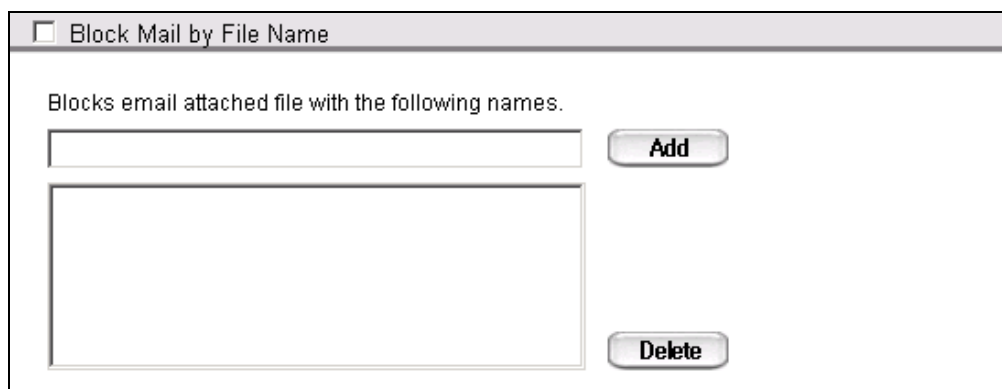
② Select the options to be defined.

③ Click  to save the configuration.

3.3. Set Mail Filter

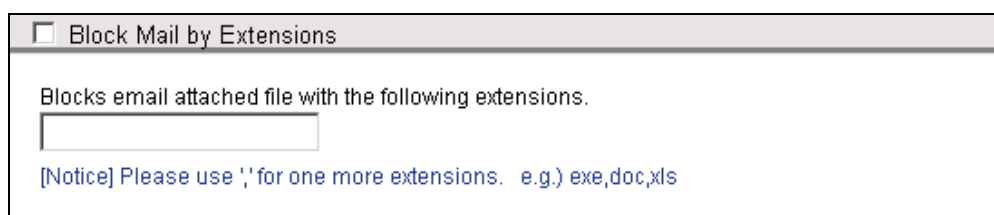
This menu allows you to configure the settings for filtering of mails and to enable the sending of alert mail whenever a mail is blocked.

① Click [Set Mail Filter] from the sub-menus in the [GatewayWall].



[Fig. 3 – 17, Block mail by file name]

- **Block Mail by File Name** : Select this option if you want to block messages by specifying the file names (not case sensitive).
- ※ You may prevent viruses from spreading rapidly via email by registering the specific names of attached files.



[Fig. 3 – 18, Block Mail by extensions]


- **Block Mail by Extensions** : Select this option if you want to block messages by specifying the file extensions (not case sensitive).



[Fig. 3 – 19, Send alert mail upon blocking mail]

- **Alert mails** : To send alert mails when any email is blocked, set this option to ON. You may change the alert mail recipient using [Administrator] > [Set alert mail] menu (please refer to '7. Administrator').

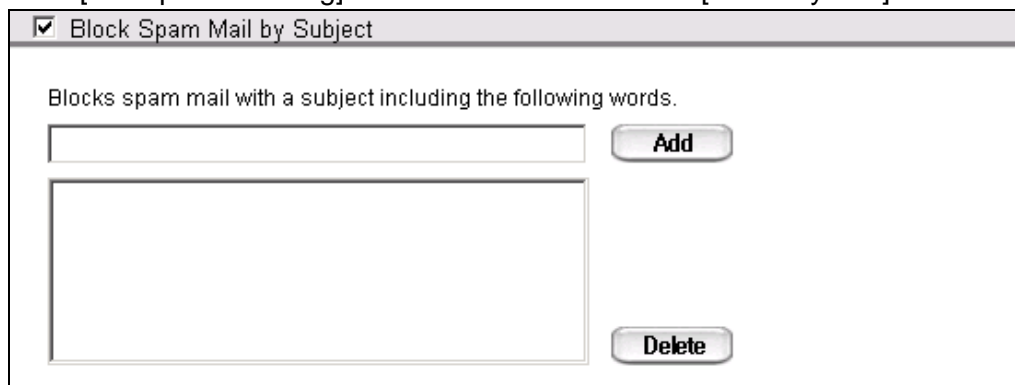
② Select the options to be defined.

③ Click  to save the configuration.

3.4. Set Spam Blocking

This menu allows you to block any mails that contain a specified string in their subject lines or mails that are from specified email addresses and IP addresses. Alert mail notification function is also available here.

① Click [Set Spam Blocking] from the sub-menus in the [GatewayWall].



[Fig. 3 – 20, Block spam mail by subject]

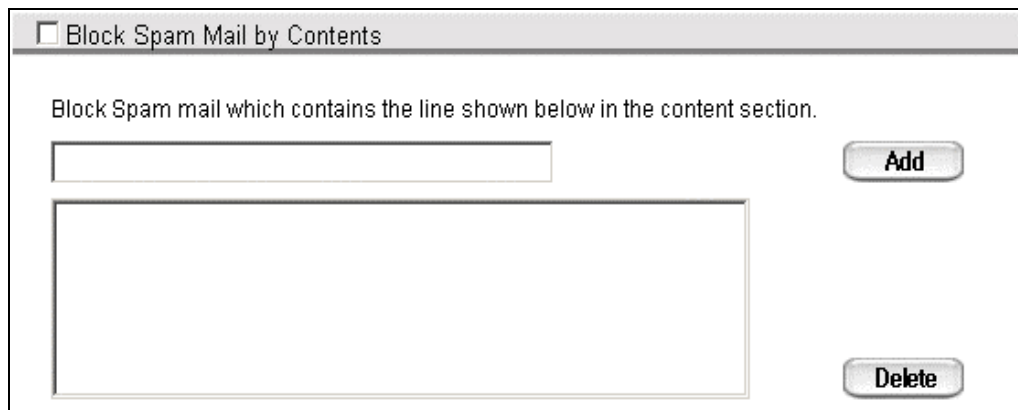
- **Block spam mail by subject** : Add in any text string and any mail with a subject line that contains this string will be blocked.
(Not case sensitive)

E.g. Register the string 'Advertisement'

[Advertisement] -> Block

[Adver.....*****..... tisement] -> Block ('*****' has no meaning, therefore it is blocked.)

[Adver.....abc.....tisement] -> Accept ('abc' has some meaning, therefore it is accepted.)



[Fig. 3 – 21, Block spam mail by contents]

- **Block spam mail by contents** : You can register the line in the content to be block. Note that it is not case sensitive, but space in the line text is sensitive.

E.g. 'sex' is registered to be blocked, then

[sex] -> G/W blocks this email from reaching to the recipient

[s ex] ->G/W permits the email to go through



[Fig. 3 – 22, Block spam mail by address]

- **Block spam mail by address** : Add in email addresses of any sender that you want to block. All spam mails with the specified address will be blocked. (Not case sensitive)



[Fig. 3 – 23, Block spam mail by IP]

- **Block spam mail by IP** : Add in the IP addresses and IP ranges that you want to block. All spam mails from these IP addresses will be blocked.

E.g. 123.123.123.*
123.123.123.1*
111.111.111.11



[Fig. 3 – 24, Send alert mail upon blocking of spam mail]

- **Alert mails** : To send alert mails when any spam mail is blocked, set this option to ON. You may change the alert mail recipient using [Administrator] > [Set alert mail] menu (please refer to '7. Administrator).


[Warning] Alert mails for spam mail will not be sent to the sender.

② Select the options to be defined.

③ Click  to save the configuration.

4. File Scan

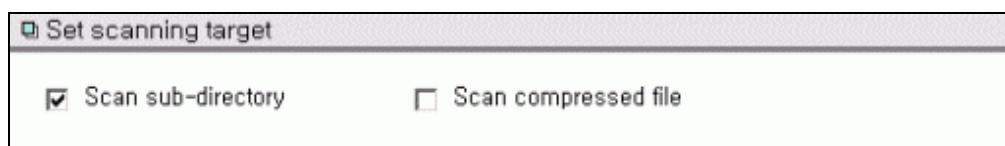
You can configure file scanning for the server in which ViRobot G/W is installed.

Click  and the following sub menu will be displayed.



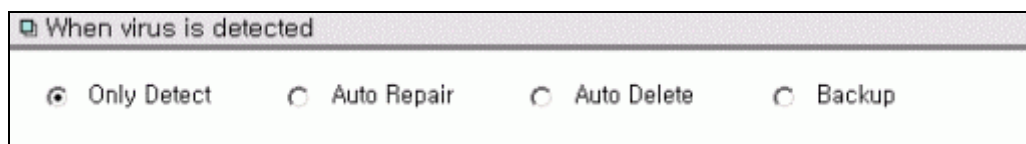
4.1. Set Scan/Repair

① Click **[Set Scan/Repair]** from the sub-menus in the **[File Scan]**



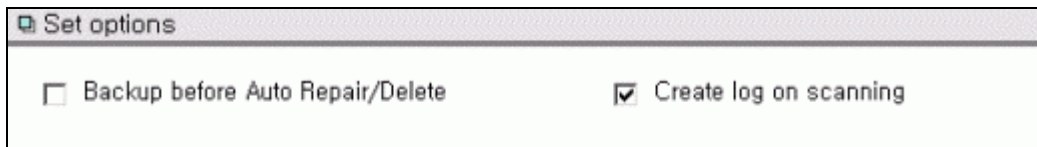
[Fig. 4 – 1, Set scanning target]

- **Scan sub-directory** : Scan all files in the target directory and its sub-directories.
- **Scan compressed file** : Scan compressed files in the target directory. For these compressed files, you can only check if they are infected. Thus, you will need to decompress them first to repair the infected file.
(ZIP, ARJ(JAR), LZH, RAR, and ACE formats are supported)



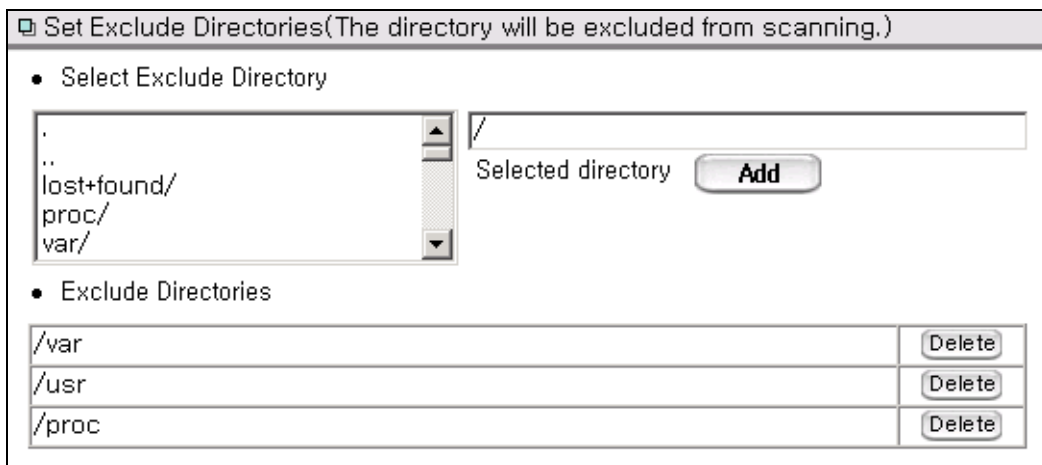
[Fig. 4 – 2, When virus is detected]

- **Only Detect** - Detect files without repairing.
- **Auto Repair** - Repair viruses detected without prompting you.
- **Auto Delete** - Delete infected file automatically when detected .
- **Backup** - Backup the infected files automatically to the specified directory.



[Fig. 4 – 3, Set options to backup before auto repair/delete and to create log]


- **Backup before auto repair/delete** – Backup the infected files before repairing or deleting them automatically.
- **Create log on scanning** - Create the corresponding log.

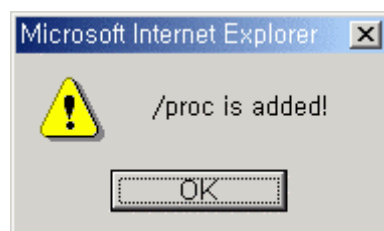


[Fig. 4 – 4, Set Exclude Directories]

Set Exclude Directories


- You can choose the directory that you want to exclude from scanning.
- You can search for the directory by using the scroll bar, or by typing the name.

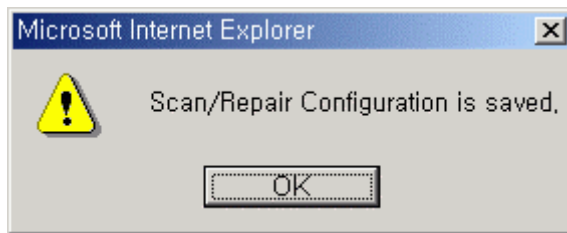
- 1) You can choose the exclude directory by typing it.
- 2) Click  to add the directory chosen.
 - If the directory exists, the following message is displayed.



- If the directory does not exist, the following message is displayed.

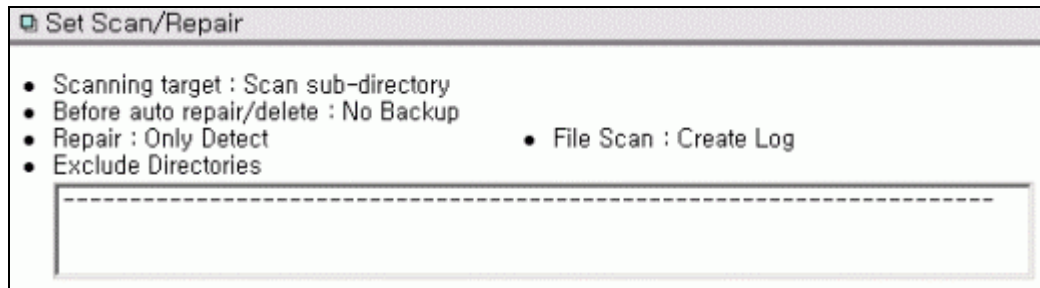


- ② Select the options to be defined.
- ③ Click  to save the configuration.
- ④ You will see a confirmation message box. Click 'OK'.



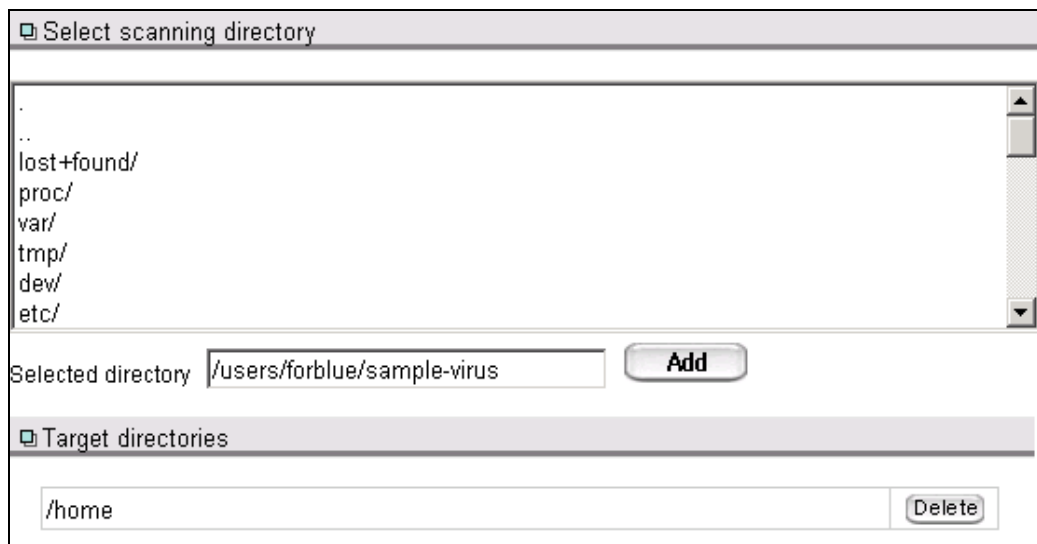
4.2 Scan

- ① Click '**Scan**' from the sub-menus in the **File Scan**



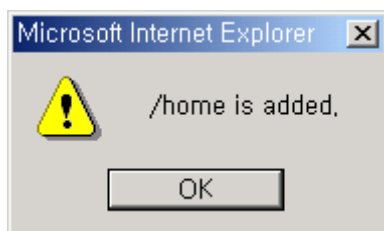
You can see the scanning configuration.

- ② You can select the target directory to scan by clicking it.

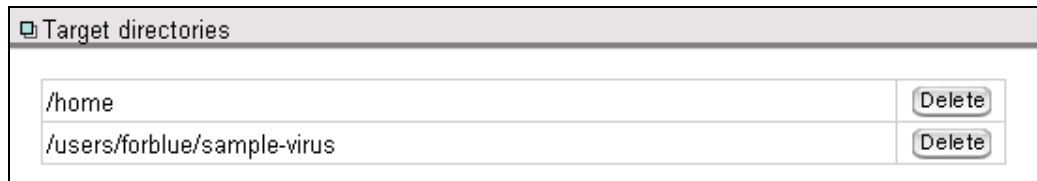


[Fig. 4 – 5, Select file scanning directory]

- ③ Click to add the directory selected.
- ④ You will see a confirmation message box. Click "OK".




- ⑤ The selected directory will be added in the target directories.



[Fig. 4 – 6, Add target directory]

[Warning] Scanning may take longer for a long list or a large-sized directory.


- ⑥ If you want to remove any directory from the list, click  button to the left of the directory.

- ⑦ Click  button to start scanning.

[Warning] You may encounter a 'time out' message during scanning if the directories are large in size. Although the web page of the virus scan may show incorrect result due to 'time out' error, the scanning process is still running.

You can check the scanning result through 'View Log' at a later time.




1) Scan and Repair

 is used to check the scanning result on the browser. You can remove detected virus through your web browser in real time and the result will be displayed on the browser.

- ① Specify the target directory and click  to start scanning. As following, scanning file name is displayed.




Scanning Files	/usr/lib/perl5/5.8.0/i386-linux-thread-multi/SAFE.pm
-----------------------	------------------------------------------------------

- ② After scanning for virus in the target directory:
- The following list will be shown if any infected file is detected. If scan is completed, following message is displayed.

Scanning Files	Complete		
		Select file(s)	
<input type="checkbox"/>	File Name	Virus Name	Status
<input type="checkbox"/>	/home/cs9752/virus/Macro/X97M.Laroux.HW	X97M.Laroux.HW	Repairable
<input type="checkbox"/>	/home/cs9752/virus/Script/VBS.Lowjo.C	VBS.Lowjo.C	Repairable
Total file(s)	Infected file(s)	Repaired file(s)	Deleted file(s)
3	2	0	0

[Fig. 4 – 7, View the list of infected files]

- The following screen will be shown when there is no infected file detected.

Scanning Files	Complete		
		Select file(s)	
<input type="checkbox"/>	File Name	Virus Name	Status
Total file(s)	Infected file(s)	Repaired file(s)	Deleted file(s)
5	0	0	0

- ③ Check the box next to the file from which you want to remove the virus.

Or, click **Select All** to select all files in the list.

Select All		Clear All		Select file(s)		Repair	
	File Name	Virus Name	Status				
<input checked="" type="checkbox"/>	/users/forblue/sample-virus/FIND.EXE	HLLP.5602.B	Repairable				
<input checked="" type="checkbox"/>	/users/forblue/sample-virus/_503.cvs	Proto-T.507	Unrepairable				
<input checked="" type="checkbox"/>	/users/forblue/sample-virus/_516.cvs	Leapfrog.516	Repairable				
<input checked="" type="checkbox"/>	/users/forblue/sample-virus/DEBUG.EXE	HLLP.5602.B	Repairable				
<input checked="" type="checkbox"/>	/users/forblue/sample-virus/FDISK.EXE	HLLP.5602.B	Repairable				
<input checked="" type="checkbox"/>	/users/forblue/sample-virus/_383.cvs	Unidentified_004	Suspected				
Total file(s)		Infected file(s)	Repaired file(s)	Deleted file(s)			
13		6	0	0			

[Fig. 4 – 8, Select the list of infected files]

- ④ Select the file and click **Repair**.
- ⑤ The repair results will be shown on the screen.

Select All		Clear All		Select file(s)		Repair	
	File Name	Virus Name	Status				
<input type="checkbox"/>	/users/forblue/sample-virus/FIND.EXE	HLLP.5602.B	Repaired				
<input type="checkbox"/>	/users/forblue/sample-virus/_503.cvs	Proto-T.507	Deleted				
<input type="checkbox"/>	/users/forblue/sample-virus/_516.cvs	Leapfrog.516	Repaired				
<input type="checkbox"/>	/users/forblue/sample-virus/DEBUG.EXE	HLLP.5602.B	Repaired				
<input type="checkbox"/>	/users/forblue/sample-virus/FDISK.EXE	HLLP.5602.B	Repaired				
<input type="checkbox"/>	/users/forblue/sample-virus/_383.cvs	Unidentified_004	Suspected				
Total file(s)		Infected file(s)	Repaired file(s)	Deleted file(s)			
13		1	4	1			

[Fig. 4 – 9, Repair files]

[Status after repair]

Repaired: Infected files are repaired

Fail to Repair: Repair has failed. Please send the file(s) to HAURI Customer Support Center.

Deleted: Files infected with overwriting or backdoor type of virus were deleted. These files were created by viruses and have nothing to do with your system.

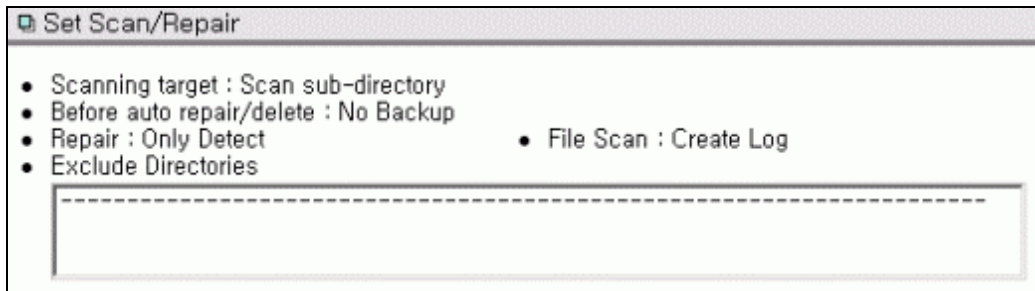
Repair after decompression: This message will appear when a virus is detected in a compressed file but is not repaired. Decompress the file in a temporary folder and run ViRobot again to detect and repair the folder.

Repair after decryption: Sometimes the macro virus document is locked with a password and ViRobot GatewayWall for Unix cannot repair these files. Therefore, you will need to unlock the file before using ViRobot again.

Suspected: This message will appear when ViRobot GatewayWall for Unix detects a virus through an unknown virus detection function. Please send the file to HAURI Customer Support Center. We will send you the results after analysis.

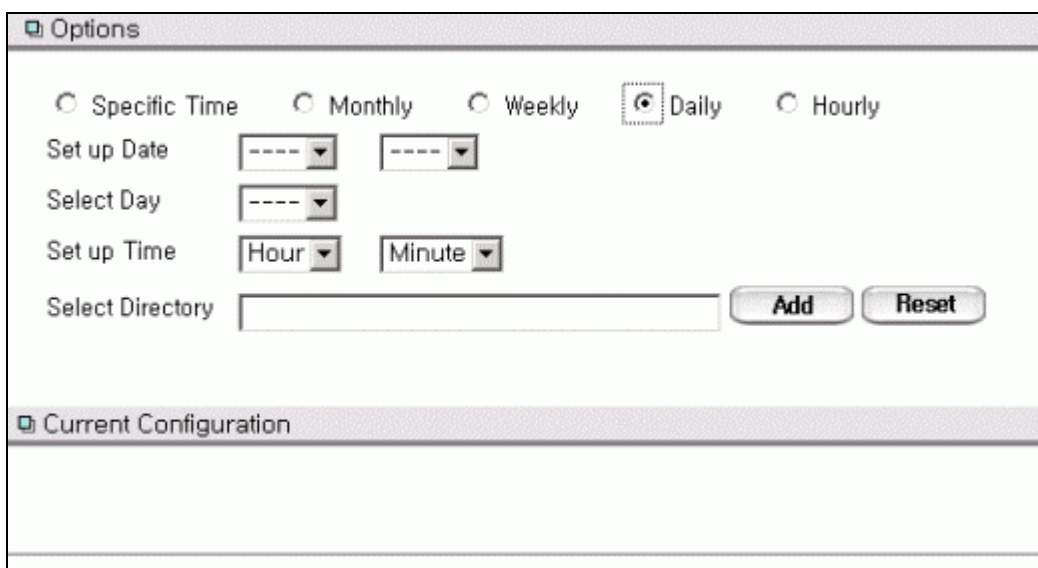
4.3 Scheduled Scan

- ① Click '**Scheduled Scan**' from the sub-menus in the **File Scan**



You can see the scanning configuration.

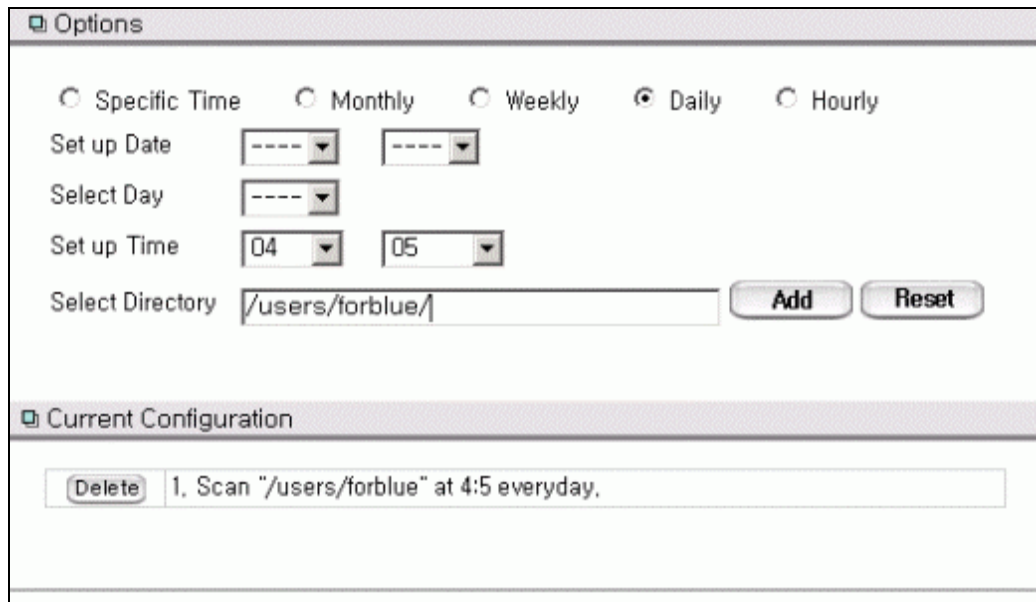
- ② The most commonly used type of scheduled scan will be shown as an example. Select **Daily**.



[Fig. 4 – 10, Add scheduled file scan]

- **Specified Time** – To scan for viruses only once at the designated time.
- **Monthly** - To scan for viruses on a specific day of the month.
- **Weekly** - To scan for viruses on a specific day of the week.
- **Daily** - To scan for viruses on a specific time of the day.
- **Hourly** – To scan for viruses once per hour.

- ③ Set Hour and Minute in **Setup time**.
- ④ Enter the directory in **Select Directory** field. (E.g. /users/forblue/)
- ⑤ Click **Add** to add the schedule in the list.



- ⑥ Click **Delete** (next to the list) to delete the schedule.
- ⑦ This function will scan the selected directories at the scheduled time.
- ⑧ After scanning, you may check the results using [Log] > [View Log] > [Logs for File Scan].

View Log


Selected Log

	Scan time	Event	progress state	Detect state	
<input type="checkbox"/>	2003/02/04/10:49:50	Scan via Web	Completed	Not detected	<input type="button" value="View"/>
<input type="checkbox"/>	2003/02/04/11:01:32	Scan via Web	Completed	Detected	<input type="button" value="View"/>
<input type="checkbox"/>	2003/02/04/11:03:27	Scan via Logs	Completed	Detected	<input type="button" value="View"/>
<input type="checkbox"/>	2003/02/04/11:05:27	Scan via Logs	Completed	Detected	<input type="button" value="View"/>
<input type="checkbox"/>	2003/02/04/11:05:41	Scan via Web	Completed	Detected	<input type="button" value="View"/>

[Fig. 4 – 11, View logs for scheduled file scan]

5. Update

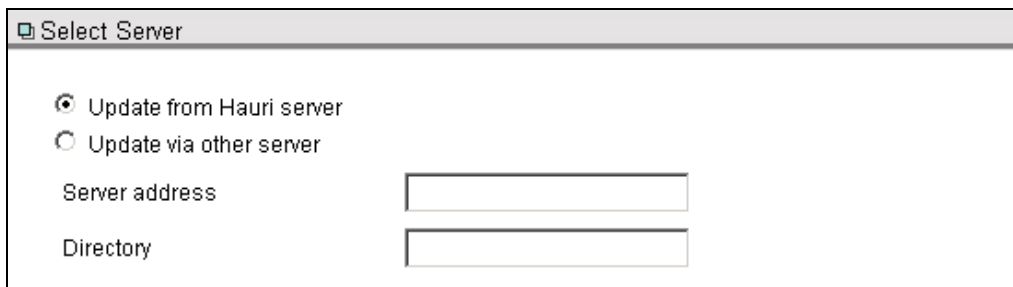
You can update your ViRobot G/W.

When you click  button, the following sub menu will be displayed.




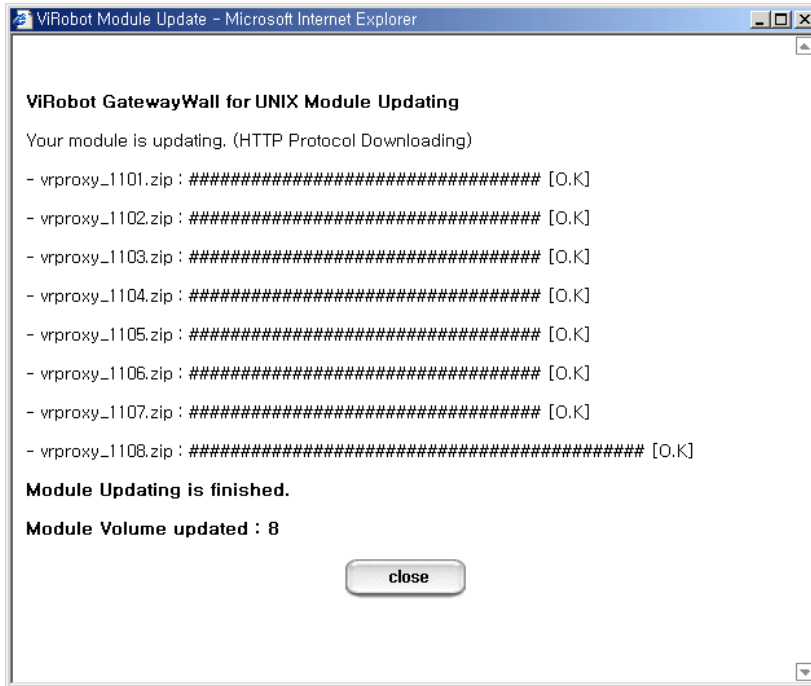
5.1. Update

- ① Click [Update] from the sub-menus in the [Update].
- ② Select the server for update. Default setting will be Update from HAURI server.

A dialog box titled 'Select Server'. It contains two radio button options: 'Update from Hauri server' (which is selected) and 'Update via other server'. Below these options are two text input fields: 'Server address' and 'Directory'.

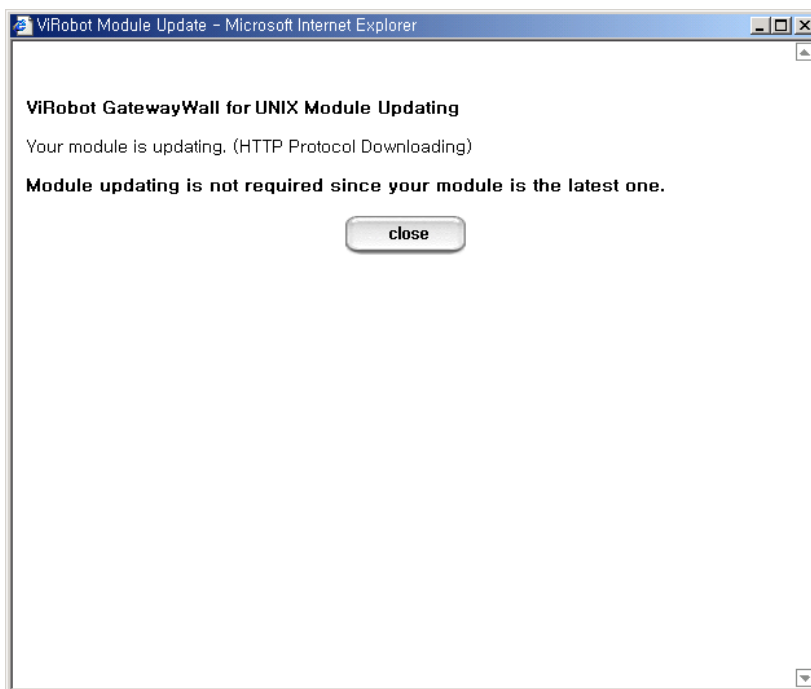
[Fig. 5 – 1, Select the server for update]

- **Update from Hauri server** – You can update from Hauri ViRobot engine update server.
 - **Update via other server** – You can enter the update server address.
- ③ Click  to update your engine.
 - ④ When the update has completed, the new window shown below will be displayed.
(You can select other server if you fail to update using the current server.)



[Fig. 5 – 2, Update completed 1]

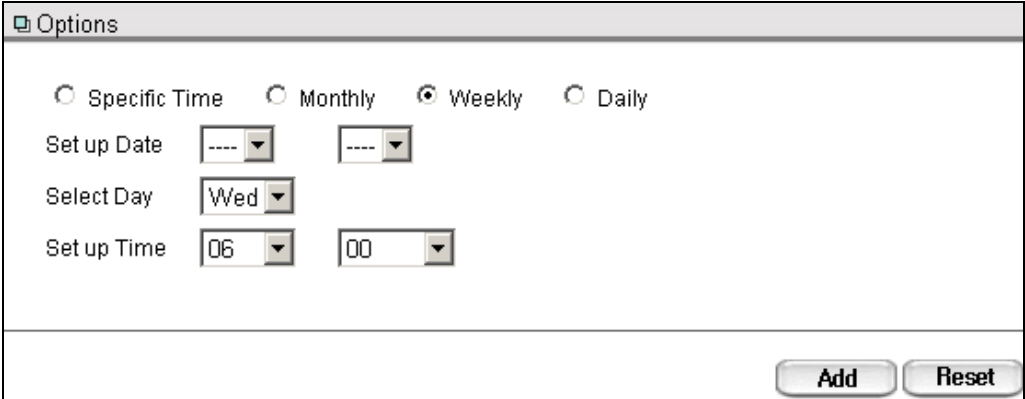
[Warning] If your ViRobot engine is the latest version, there will be no update and the following message will be displayed.



[Fig. 5 – 3, Update completed 2]

5.2. Scheduled Update

- ① Click [Scheduled Update] from the sub-menus in the [Update].

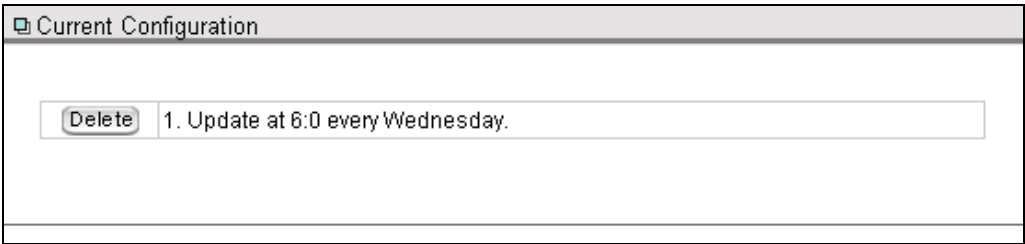


The screenshot shows a window titled "Options" with the following controls:

- Radio buttons: Specific Time, Monthly, Weekly, Daily
- Set up Date: Two dropdown menus, both showing "----".
- Select Day: A dropdown menu showing "Wed".
- Set up Time: Two dropdown menus, showing "06" and "00".
- Buttons: "Add" and "Reset" at the bottom right.

[Fig. 5 – 4, Add update schedule]

- **Specified Time** – To update only once at the designated time.
 - **Monthly** - To update on a specific day of the month.
 - **Weekly** - To update on a specific day of the week.
 - **Daily** - To update on a specific time of the day.
- ② Set the time and period to update the engine.
 - ③ Click **Add** to add the schedule in the list.



The screenshot shows a window titled "Current Configuration" with a list containing one item:

- 1. Update at 6:0 every Wednesday.

A "Delete" button is located to the left of the list item.


[Fig. 5 – 5, Delete update schedule]

- ④ Click **Delete** (next to the list) to delete the schedule.
- ⑤ The engine will be updated according to the schedule. After updating, you may

check the results using [Log] > [View Log] > [Logs for Update].

6. Log

This menu allows you to manage the log information of ViRobot G/W.

When you click  button, the following sub menu will be displayed.



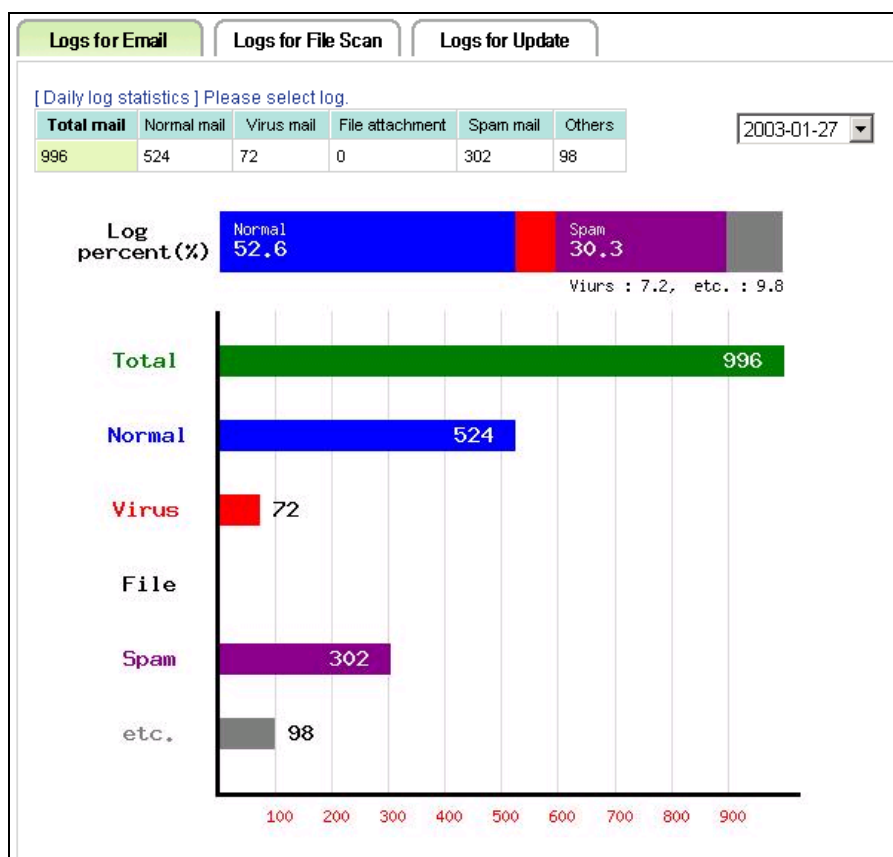
6.1. View Log

Click this button to view Email Log, Logs for File Scan, and Logs for Update.

1) Email Log

① Click [View Log] from the sub-menus in the [Log].

For any email log, the latest log statistics and graphs will be shown.



[Fig. 6 – 1, View statistics and graphs of email log 1]

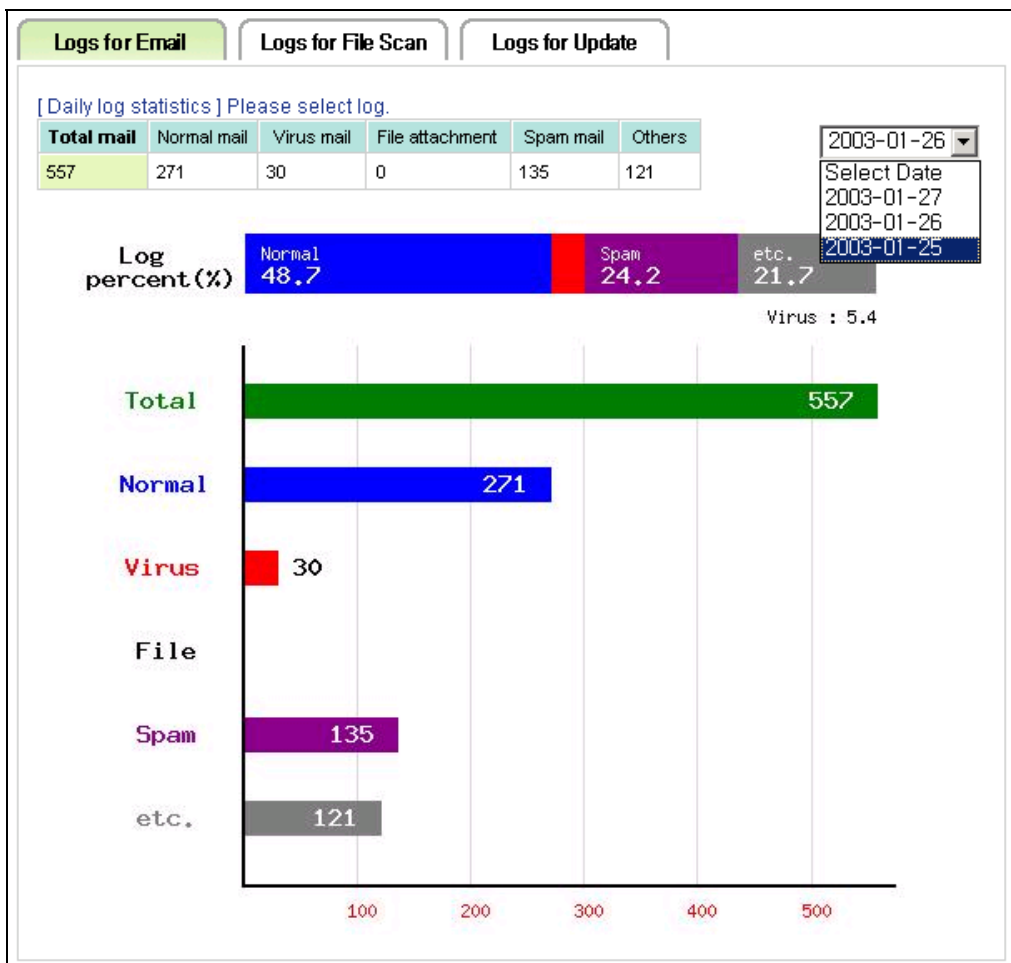
The statistical data of messages received during the day is available in tables and graphs for easy viewing.

You will see the screen shown below if there is no previously created log.



[Fig. 6 – 2, View statistics and graphs of email log 2]

- ② You may select the log for a specific date through Select Date option (top right hand corner). Logs that were deleted, through [Set Backup/Log], cannot be viewed.



[Fig. 6 – 3, View statistics and graphs of email log 3]

③ [Daily Mail Statistics] Select the category of log that you want to view.

- Total mail** - Log for all the mails.
- Normal mail** - Log for normal mails (not blocked).
- Virus mail** - Log for virus mails and blocked mails.
- File attachment** - Log for mails blocked by mail filtering.
- Spam mail** - Log for mails that were blocked by spam mail setting.
- Others** - Log for mails that were blocked due to an error in the mail server.

The screenshot shows a web interface for email logs. At the top, there are three tabs: 'Logs for Email' (selected), 'Logs for File Scan', and 'Logs for Update'. Below the tabs, there is a link for '[Daily log statistics] Please select log.' and a date selector set to '2003-01-26'. A summary table shows the following counts: Total mail (557), Normal mail (271), Virus mail (30), File attachment (0), Spam mail (135), and Others (121). Below this are several action buttons: 'Select All', 'Clear All', 'Reload', 'View Excel', 'Search', 'Selected mail', 'Delete', and 'Resend'. The main part of the interface is a table with the following columns: 'Detected Time', 'IP', 'Sender', 'Recipient', 'Subject', 'Original mail', and 'Alert'. The table contains 9 rows of data, each with a checkbox in the first column. The first row shows a 'Virus Report' detected at 2003-01-26 23:45:1 from IP 64.4.22.204. The last row shows a 'Re: Movies' detected at 2003-01-26 19:03:1 from IP 211.194.249.21. A page number '1' is centered at the bottom of the table area.

Detected Time	IP	Sender	Recipient	Subject	Original mail	Alert
<input type="checkbox"/> 2003-01-26 23:45:1	64.4.22.204	ghktn255@hotm	hauri98@hauri.c	Virus Report	View	View
<input type="checkbox"/> 2003-01-26 22:00:1	211.39.138.70	jabaek@hanmir.	webmaster@he	A very nice game	View	View
<input type="checkbox"/> 2003-01-26 21:32:1	61.43.160.139	big@boss.com	webmaster@he	Re: Sample	View	View
<input type="checkbox"/> 2003-01-26 21:32:1	61.75.146.34	big@boss.com	webmaster@he	Re: Document	View	View
<input type="checkbox"/> 2003-01-26 21:19:1	206.46.170.108	cyberman@veri	hauri98@hauri.c	A new game	View	View
<input type="checkbox"/> 2003-01-26 21:06:1	211.213.161.64	big@boss.com	webmaster@he	Re: Movies	View	View
<input type="checkbox"/> 2003-01-26 21:01:1	211.243.238.19	big@boss.com	hinnie@hauri.cc	Re: Document	View	View
<input type="checkbox"/> 2003-01-26 20:07:1	61.248.37.202	big@boss.com	webmaster@he	Re: Sample	View	View
<input type="checkbox"/> 2003-01-26 19:03:1	211.194.249.21	big@boss.com	hauri98@hauri.c	Re: Movies	View	View

[Fig. 6 – 4, View email log list]

A log consists of the following items:

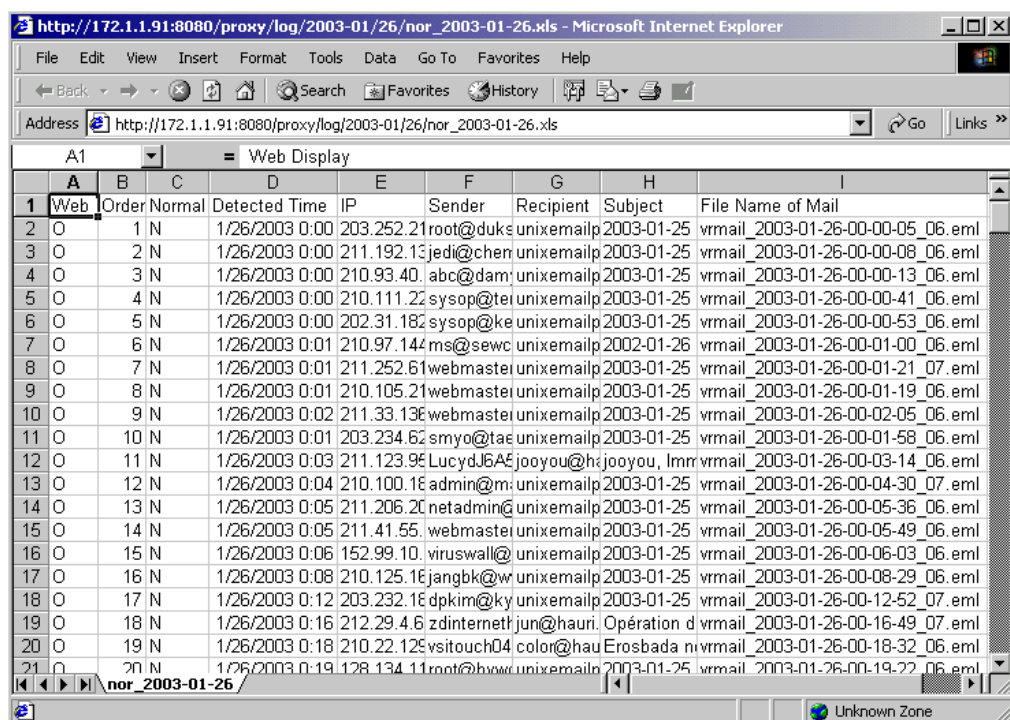
- **Detected Time** : Time of receiving mail.
- **IP** : IP address of the computer from which the message was sent.
- **Sender** : Sender's address.
- **Recipient** : Recipient's address.
- **Original mail** : The original content of the mail.
- **Subject** : Subject line of the mail.
- **Alert** : Alert mails for blocked mail.

- ④ Click **View** from Alert column on the right to view alert mails generated.



[Fig. 6 – 5, View alert mails for email log]

- ⑤ To refresh the log, click **Reload**.
- ⑥ To open the log in Excel file, click **View Excel**. The log file will be opened as



[Fig. 6 – 6, View the log in Excel sheet]

- ⑦ To store the log in Excel sheet, save the document by selecting [File]>[Save As].

[Warning] Due to the cache function in Internet Explorer, changes made in the Excel sheet in [View Log] will not be applied when you open it again next time. You will have to delete the cache (follow the instructions shown below) and select **View Excel** one more time.

Internet Explorer

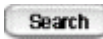
Click **Internet Options** in **Tools Menu** for version 5.x and 6.x, or **View Menu** for version 4.x. Click **Delete File** in the dialog box of **Internet Options**.

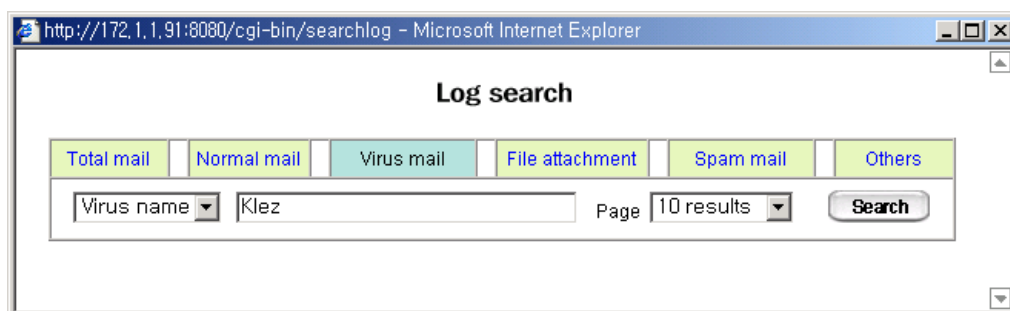
Netscape Navigator 6.x

Click **Default** in the **Edit** menu. Extend the **Advanced** category.

Click **Cache** and then **Clear Memory Cache**.

Click **Delete Disk Cache**.

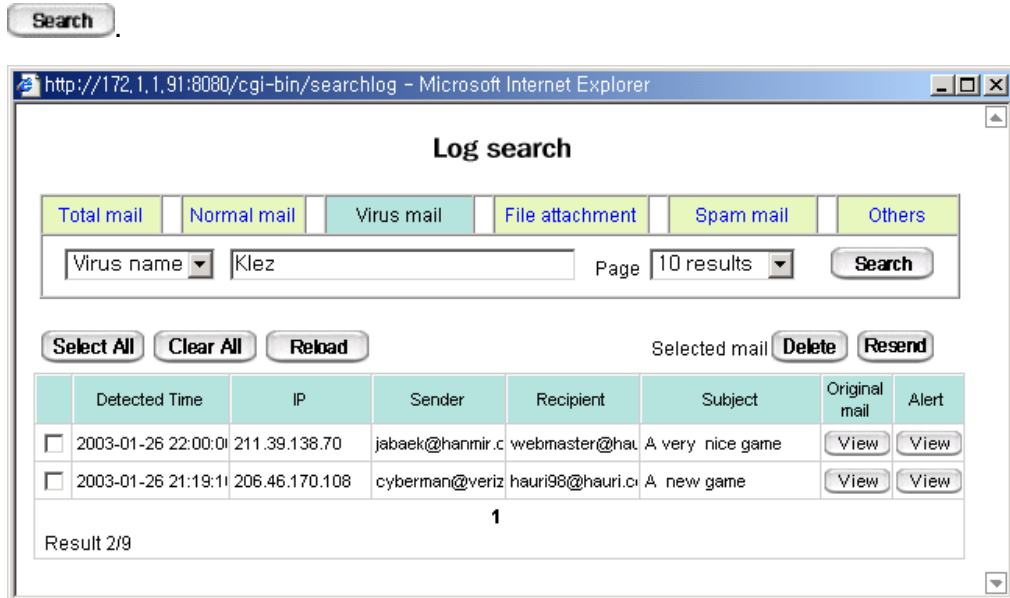
- ⑧ G/W provides a convenient mail search function in every log. Click  to view the Search window.



[Fig. 6 – 7, Search email log]

- ⑨ Select the category of log and use the option on the left side to select the search criteria. Search criteria that you may choose (according to log category):
- **Normal Mail** : Subject, sender, recipient, sender's IP
 - **Virus Mail** : Subject, virus name, sender, recipient, sender's IP
 - **File Filtering Mail** : Subject, file filter name, sender, recipient, sender's IP
 - **Spam Filtering Mail** : Subject, spam filter name, sender, recipient, sender's IP
 - **Others** : Subject, sender, recipient, sender's IP

- ⑩ After selecting the search criteria, enter the correct name accordingly. For the Page option, enter the number of results to be shown on one page and click



[Fig. 6 – 8, Search result of email log]

- ⑪ To delete the log on the screen or from search results, select it and click **Delete**. Click **Select All** to select all the logs at once.

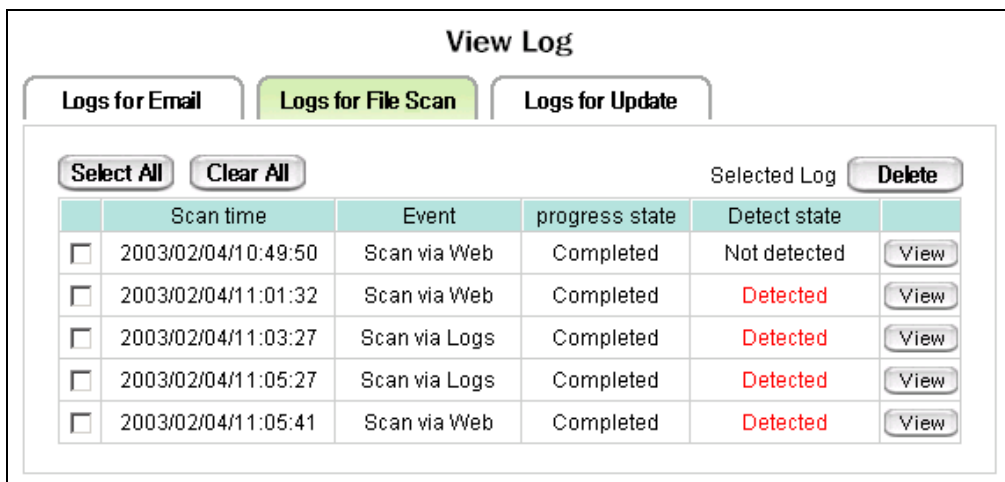
[Warning] Backup and logs exceeding the defined days and size limit will be automatically deleted to comply with the storage period and capacity configured in [View Log] > [Set Backup/Log]. Since manually deleting each log may take some time, we recommend that you use this automatic deletion function.

- ⑫ To resend mails that are blocked by virus protection or by other filtering functions, click **Resend**.

[Warning] Resending detected virus mail may cause the recipient to be infected with the virus. Please be careful in resending blocked virus mails.

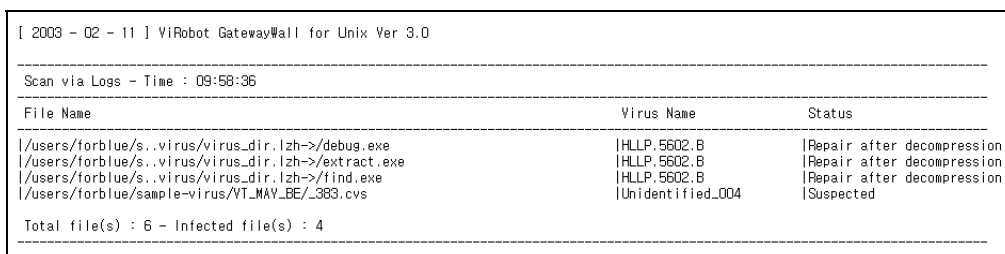
2) Logs for File Scan

- ① Click [Logs for File Scan] from the sub-menus in the [View Log].



[Fig. 6 – 9, View logs for file scan]

- ② If a virus is detected, the status will be displayed as <Detected>.
- ③ To view the details of the log, click **View** next to it.

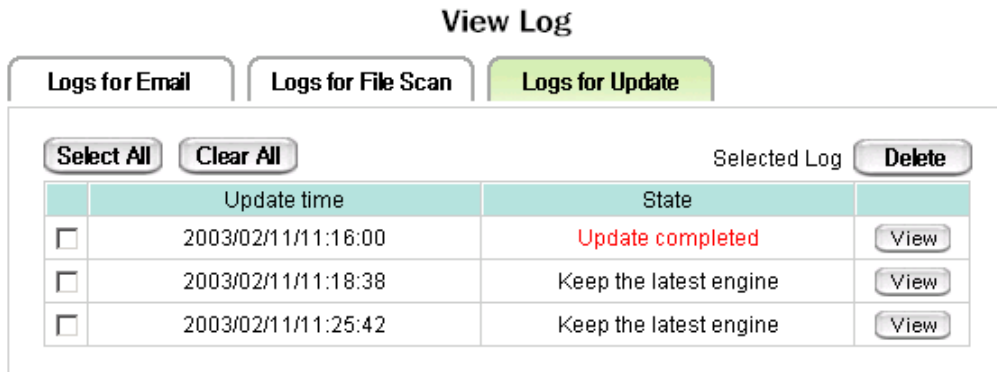


[Fig. 6 – 10, View the details of the log for file scan]

- ④ Click **Delete** to remove any selected log file.
- ⑤ To refresh the log, click **Reload**.

3) Logs for Update

- ① Click [Logs for Update] from the sub-menus in the [View Log].

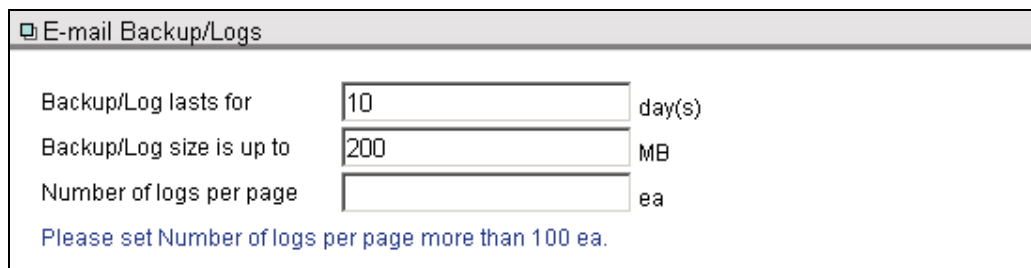


[Fig. 6 – 11, View log for update]

- ② To view the details of the log, click next to it.
- ③ Click to remove any selected log file.
- ④ To refresh the log, click .

6.2. Set Backup/Log

- ① Click [Set Backup/Log] from the sub-menus in the [Log]



E-mail Backup/Logs

Backup/Log lasts for day(s)

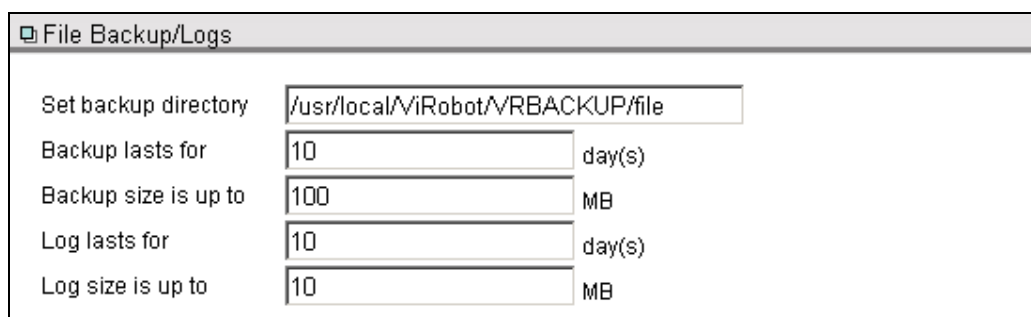
Backup/Log size is up to MB

Number of logs per page ea

Please set Number of logs per page more than 100 ea.

[Fig. 6 – 12, Set backup/log for email]

- **Backup/Log lasts for** : Period of storing mail backup/log. Upon expiration, email backup/log will be automatically deleted.
- **Backup/Log size is up to** : Limits the size of mail backup/log directory. When the size is exceeded, the previous backup/log will be automatically deleted from the directory.
- **Number of logs per page** : Defines the number of logs displayed on one page on [View Log]>[Email Log] screen.



File Backup/Logs

Set backup directory

Backup lasts for day(s)


Backup size is up to MB

Log lasts for day(s)

Log size is up to MB

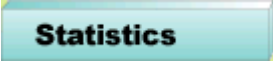
[Fig. 6 – 13, Set file backup/log]

- **Set backup directory** : A backup directory for detected virus files. By default, this is VRBACKUP/file, a sub directory of the install directory for ViRobot G/W. You may change this by entering your desired directory path.
- **Backup lasts for** : Specifies the period to keep the backup of the infected files.
- **Backup size is up to** : Sets the capacity of the backup directory.
- **Log lasts for** : Specifies the period to keep the log.
- **Log size is up to** : Sets the capacity of the log directory..

- ② Select the options to be defined.
- ③ Click  to save the configuration.

7. Statistics

This menu shows the statistical data of logs by period using your ViRobot G/W.

Click  and the following submenu will be displayed.



7.1 Total Mail

You can view comprehensive statistical data of normal, virus, spam, file attachment, and other mails.

- ① Click [Total Mail] from the sub-menus in the [Statistics].

For any log of the current date, the initial window will provide daily statistical data as shown:

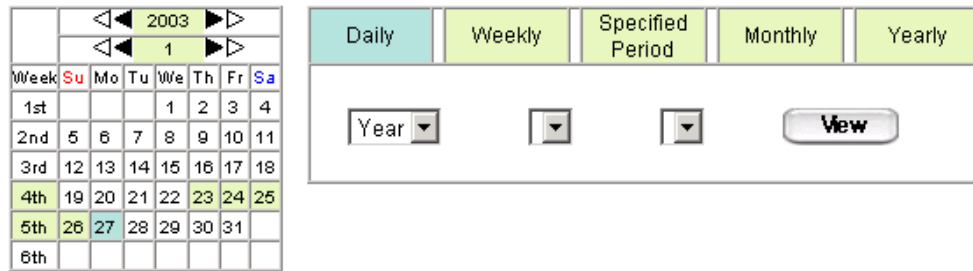


You can view the statistical data of the target mail by period you define

Volume of the target mail by period is shown in graphs and tables.

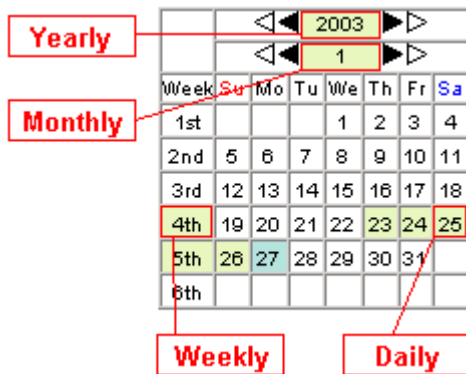
[Fig. 7 – 1, Daily log statistics of total mail]

1) Select the period to view [Total Log].



There are two options for you to view the statistical data by period:

- By calendar



※ Each color represents:

- The log exists within the period and you can view it by clicking on the link.
- The period of current statistics on the screen. Not linked.
- No log within the period. Not linked.

- Daily – Click on the date to view the log that day.
(E.g. Click 25 for the date of 25.)
- Weekly – Click on the week to view the log for that week.
(E.g. Click 4th for the fourth week.)
- Monthly – Click on the month to view the log for that month.
(E.g. Click 1 for January)
- Yearly – Click the year to view the log for that year.
(E.g. Click 2003 for the year 2003.)

[Note] Using ◀ ▶ button next to Year and Month on the calendar, you can select the year and the month that you want.

[Warning] The viewing of these statistics will **not be available from your calendar.**

- By period check box

Daily	Weekly	Specified Period	Monthly	Yearly
2003	01	23	~	
	2003	01	27	View

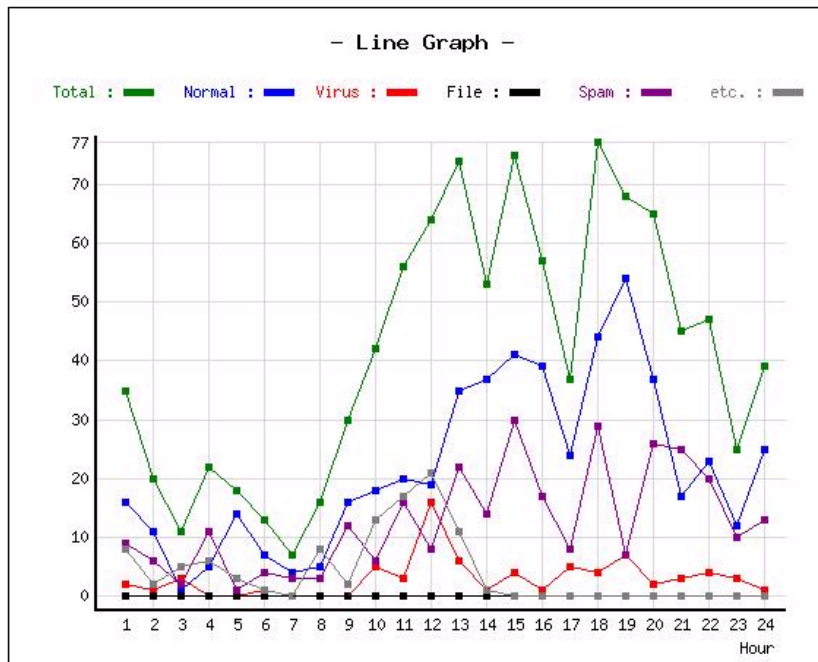
To view the statistics, select the period by using the Select Option list.

- Daily – Select year, month and date, and then click View button.
- Specified period – Select a specific period and click View button.
You can set the period ranging up to 30 days.
(*E.g.* Dec 15, 2002 – Jan 13, 2003)
- Monthly – Select year and month, and then click View button.
- Yearly – Select year and then click View button.

[Warning] The weekly statistics will not be available from your period check box for viewing.

2) Volume of the total mail by period is shown in graphs and tables.

- Line graph and figure table

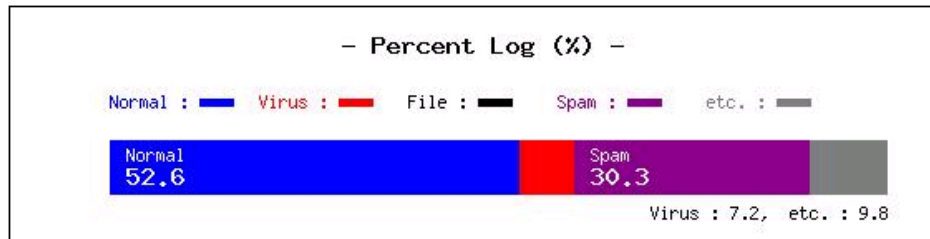


Time	Total mail	Normal mail	Virus mail	File attachment	Spam mail	Others
01:00	35	16	2	0	9	8
02:00	20	11	1	0	6	2
03:00	11	1	3	0	2	5
04:00	22	5	0	0	11	6
05:00	18	14	0	0	1	3
06:00	13	7	1	0	4	1
07:00	7	4	0	0	3	0
08:00	16	5	0	0	3	8
09:00	30	16	0	0	12	2
10:00	42	18	5	0	6	13
11:00	56	20	3	0	16	17
12:00	64	19	16	0	8	21
13:00	74	35	6	0	22	11
14:00	53	37	1	0	14	1
15:00	75	41	4	0	30	0
16:00	57	39	1	0	17	0
17:00	37	24	5	0	8	0
18:00	77	44	4	0	29	0
19:00	68	54	7	0	7	0
20:00	65	37	2	0	26	0
21:00	45	17	3	0	25	0
22:00	47	23	4	0	20	0
23:00	25	12	3	0	10	0
24:00	39	25	1	0	13	0

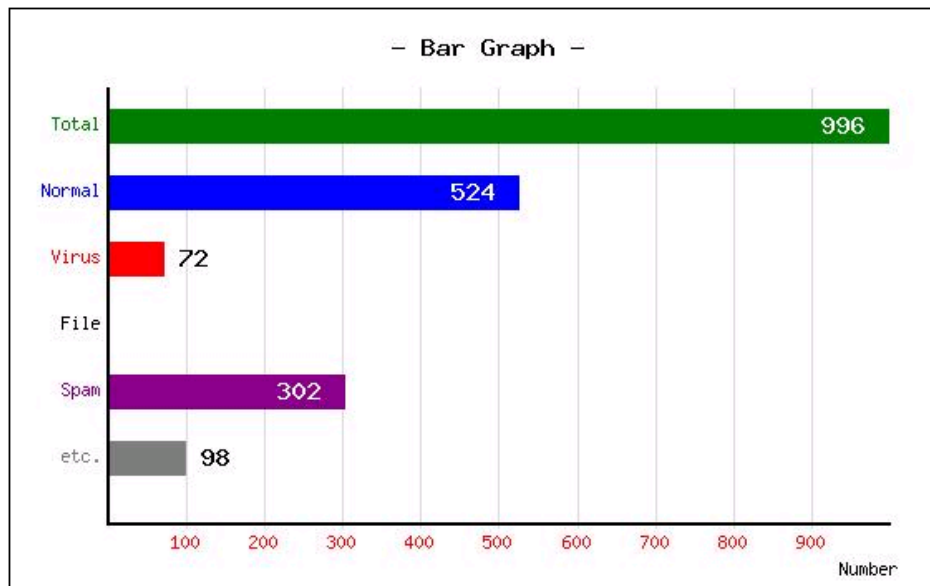
[Fig. 7 – 2, Daily log statistics for total mail in line graph]

[Warning] Line graphs and numeric data may not be available when you try to view daily statistics from the log statistics of **total, normal, virus, file attachment, spam and other** mails. This occurs when the log of the specific date was deleted due to size and period limit.

- Percent log, bar graph and figure table



	Total mail	Normal mail	Virus mail	File attachment	Spam mail	Others
Volume of mail	996	524	72	0	302	98
Percent	100.00 %	52.61 %	7.23 %	0.00 %	30.32 %	9.84 %



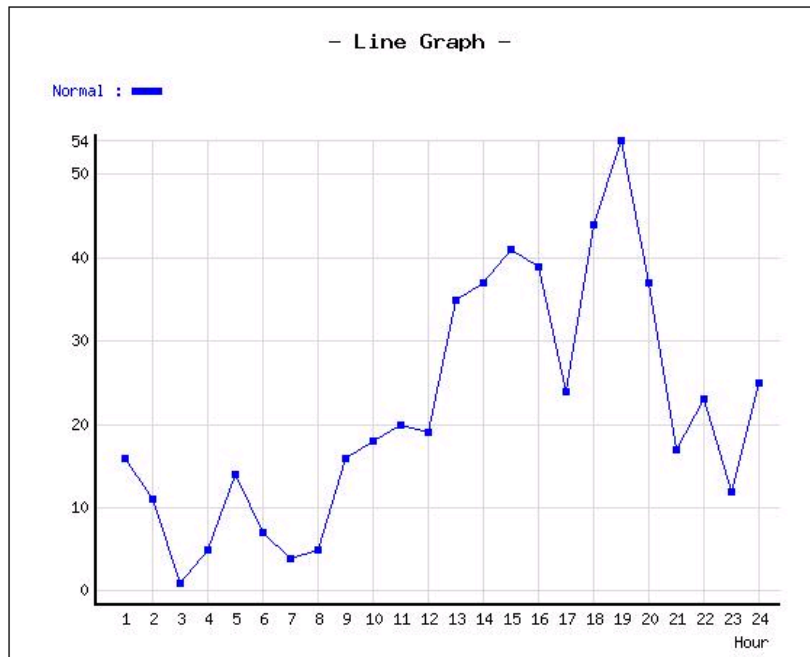
[Fig. 7 – 3, Daily log statistics for total mail in percent log and bar graph]

[Warning] You may not have percent logs, bar graphs and numeric data from the log statistics of **normal, virus, file attachment, spam and other mails.**

7.2 Normal, Virus, File Attachment, Spam and Other Mails

To view the statistics data of normal, virus, file attachment, spam and other mails, **set the period in the same way that you did for total mail**. However, only **line graphs and numeric data** is available.

- ① Click [Normal Mail] / [Virus Mail] / [Filtered Attachment Mail] / [Spam Mail] / [Others] from the sub-menus in the [Statistics].



Time	Normal mail	Percent
01:00	16	3.05
02:00	11	2.10
03:00	1	0.19
04:00	5	0.95
05:00	14	2.67
06:00	7	1.34
07:00	4	0.76
08:00	5	0.95
09:00	16	3.05
10:00	18	3.44
11:00	20	3.82
12:00	19	3.63
13:00	35	6.68
14:00	37	7.06
15:00	41	7.82
16:00	39	7.44
17:00	24	4.58
18:00	44	8.40
19:00	54	10.31
20:00	37	7.06
21:00	17	3.24
22:00	23	4.39
23:00	12	2.29
24:00	25	4.77

[Fig. 7 – 4, Statistics for normal mails, over the specified period in line graph]

- ② Available **only in the daily statistics for virus mails**, the most common virus types on a specific date will be shown in the **Top 10 virus infection list**.

Virus Infections TOP 10			
Rank	Virus Name	Infection Count	Rate
1	I-Worm.Win32.Sobig.A	30	41.67
2	I-Worm.Win32.Klez.H	25	34.72
3	Win32.Nimda.D	8	11.11
4	Trojan.Win32.IRCAttack.48448	3	4.17
5	Win95.Dupator.1503	2	2.78
6	Spyware.Win32.Tsad.204800	2	2.78
7	EICAR-test	1	1.39
8	VBS.Redlof	1	1.39

[Fig. 7 – 5, Daily statistics for virus mails in the infection list]

[Note] Graphs used for indicating statistics of mail type and period


Line graph : **L** , Percent log : **P** , Bar graph : **B**

Mail Type Period	Total	Normal	Virus	File attachment	Spam	Other
Daily	L P B	L	L	L	L	L
Weekly	L P B	L	L	L	L	L
Specified period	L P B	L	L	L	L	L
Monthly	L P B	L	L	L	L	L
Yearly	L P B	L	L	L	L	L

- ※ For any mail type, **line graphs (L)** will not be displayed if there is no log for the date you select.
- ※ **The Top 10 virus infection list** will be shown when you view **daily statistics for virus mail**.

8. Administrator

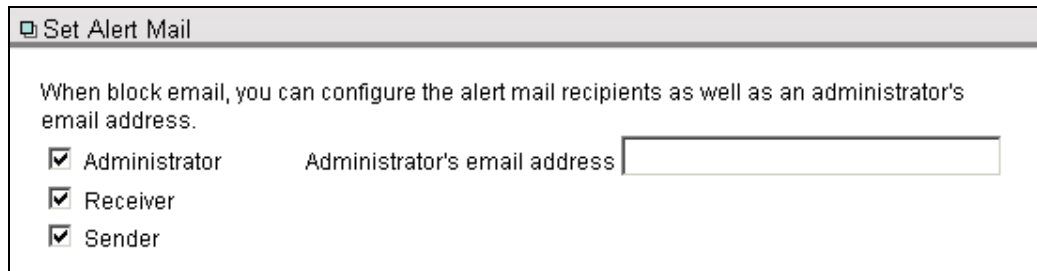
This is for administrator of ViRobot G/W.

Click  and the following sub menu will be shown.



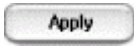
8.1. Set Alert Mail

- ① Click [Set Alert Mail] from the sub-menus in the [Administrator].



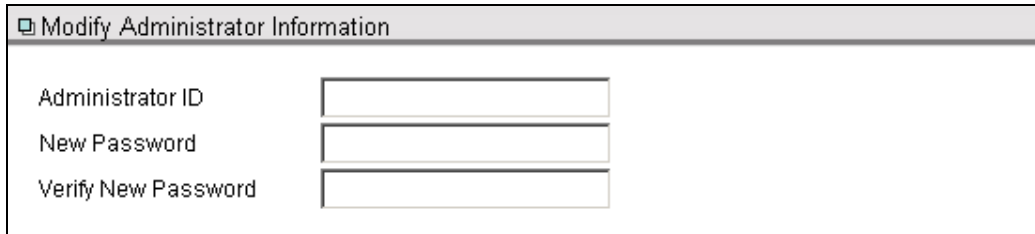
The image shows a window titled "Set Alert Mail". The window contains the following text: "When block email, you can configure the alert mail recipients as well as an administrator's email address." Below this text, there are three checked checkboxes: "Administrator", "Receiver", and "Sender". To the right of the "Administrator" checkbox, there is a text label "Administrator's email address" followed by an empty text input field.

[Fig. 8 – 1, Configure alert mail recipient and administrator's address]

- ② You can configure the alert mail recipients for blocked mails. The alert mails will only be sent to the selected recipients.
- ③ In the Administrator's Email Address portion, enter the email address of the administrator who will receive the alert mails.
- ④ Click  to save the configuration.

8.2. Modify Administrator Information

- ① Click [Modify Admin. Info] from the sub-menus in the [Administrator].



The screenshot shows a web form titled "Modify Administrator Information". It contains three input fields: "Administrator ID", "New Password", and "Verify New Password". Each field is represented by a text label followed by a rectangular input box.

[Fig. 8 – 2, Modify administrator information]

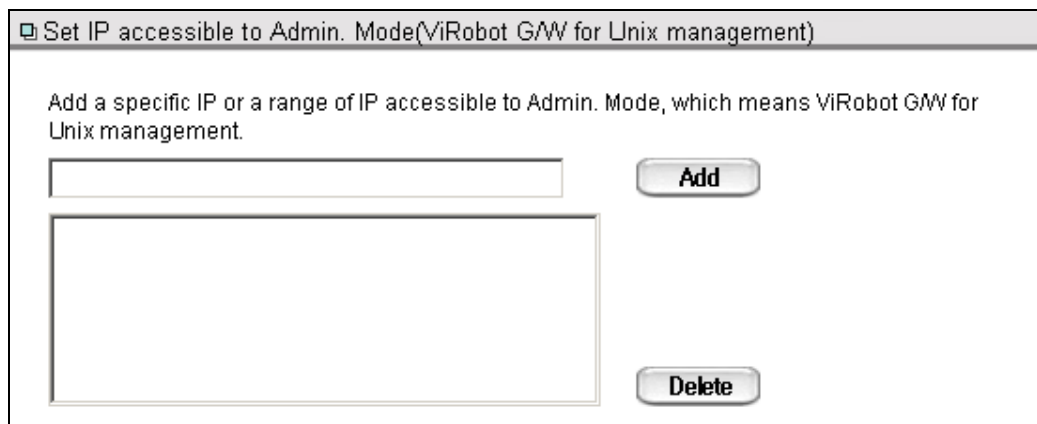
- **Administrator ID** : Enter the user ID for login.
- **New Password** : Enter the password for login.
- **Verify New Password** : Enter the password again to confirm it.

[Warning] Be sure to change the default user ID and the password given. If you forget your new ID or password, you can modify the information on the console. Please refer to the administrator guide.

- ② You can configure specific IP address or IP address range for accession to ViRobot G/W management console. More than one IP address can be added. If no IP address is added, all IP addresses will be able to access.

E.g. To set one IP : 100.100.100.3


To set one whole IP range : 100.100.100



The screenshot shows a web form titled "Set IP accessible to Admin. Mode(ViRobot G/W for Unix management)". Below the title is a text instruction: "Add a specific IP or a range of IP accessible to Admin. Mode, which means ViRobot G/W for Unix management." There are two input fields: a single-line text box and a larger multi-line text box. To the right of the single-line box is an "Add" button, and to the right of the multi-line box is a "Delete" button.


[Fig. 8 – 3, Add IP addresses for accession to Admin. Mode]

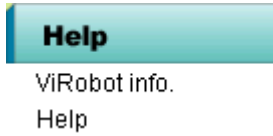
[Warning] You will not be able to connect from the client if you specify incorrect host address via the web. In this case, correct the host address on the console. Please refer to the administrator guide..

- ③ Click  to change Administrator information.

9. Help

This menu contains ViRobot Information and Help page of How to use ViRobot GatewayWall for Unix. You can refer to Help for more details.

Click  and the following submenu will be displayed.



IV. Running ViRobot GatewayWall for Unix in the Console Environment

1. Scan

2. Update

1. Scan

1.1. Scan

- ① Open the console and go to /ViRobot Installation Directory/. Then Run ./virobot.

```
[root@localhost ViRobot]# ./virobot
-----
ViRobot GatewayWall for Unix                               10 Sep 2002 Korea
Copyright (c) 1998-2003 HAURI Inc.                         All rights reserved
E-mail : support@huri.net                                 Version 3.0
-----
Usage : virobot [<option list>] -d [directory]
<option list> :
    --recursive      : Subdirectory Scanning
    --archive        : Archive File Scanning
    --recovery       : Repair Infected File
    --delete         : Delete Infected File
    --backup         : Backup Infected File
    --version        : Display ViRobot Engine Version
    --help           : DisPlay The Command Line Options

[root@localhost ViRobot]#
```

- ② Take a look at the Option List to configure your scanning accordingly.
- ③ “virobot -d Scanning directory name“ will perform directory scan.

```
[root@localhost ViRobot]# virobot -d /home
-----
ViRobot GatewayWall for Unix                               10 Sep 2002 Korea
Copyright (c) 1998-2003 HAURI Inc.                         All rights reserved
E-mail : support@huri.net                                 Version 3.0
-----
----- Scan Result -----
All File           : 0
Scan File          : 0
Infected File      : 0
Maybe Infected File : 0
Repaired File      : 0
Deleted File       : 0
Backupid File      : 0
ViRobot Engine Version : 2003-02-12
-----

[root@localhost ViRobot]#
```

1.2. Additional Functions for Scanning

① Scan Compressed Files

Add **--archive** option to check for virus in the compressed files.

```
[root@localhost ViRobot]# ./virobot —archive -d (directory)
```

② Scan Sub-directories

Add **--recursive** option to include **the sub-directories** in the scanning.

```
[root@localhost ViRobot]# ./virobot —recursive -d (directory)
```

③ Automatic Repair

Add **--recovery** option to automatically repair infected files found during scanning.

```
[root@localhost ViRobot]# ./virobot —recovery -d (directory)
```

[Warning] Any files that are infected by unrecoverable type of viruses will be deleted automatically.

④ Automatic Delete

Add **--delete** option to automatically delete infected files found during scanning.

```
[root@localhost ViRobot]# ./virobot —delete -d (directory)
```

⑤ Automatic Backup

Add **--backup** option to backup (in the backup directory) infected files found during scanning.

```
[root@localhost ViRobot]# ./virobot —backup -d (directory)
```

[Note] The default backup directory is as follows:

[ViRobot Installation Directory]/ViRobot/VRBACKUP/file

- ⑥ *E.g.* Target directory: /home/user/, include all sub-directories, include all compressed files.

```
[root@localhost ViRobot]# virobot --recursive --archive -d /home/user/
```

2. Update

By using **vrproxyupdate** program which is installed with your ViRobot G/W, you can update your virus engine.

2.1. Via HAURI update server:

```
vrproxyupdate -s
```

```
[root@localhost ViRobot]# ./vrproxyupdate -s
```

2.2. Via other update server:

```
vrproxyupdate -h [access server address or URL] -d [access directory]
```

```
[root@localhost ViRobot]# ./vrproxyupdate --h access server address or URL -d access directory
```

V. Administrator Guide of Virobot GatewayWall for Unix

1. Installation Information
2. Configuring ViRobot G/W Manually on the Console
3. Tips for Administrator

1. Installation Information

1.1. Installation Directory

- Installation Directory: `/usr/local/ViRobot/`
Unless you change **[2] Install path**, your ViRobot G/W will be installed in the default directory: `/usr/local/ViRobot/`
If you have changed this option, the installation directory will be **Specified Directory/ ViRobot/**.
In this Manual, we assume that your ViRobot is installed in the default directory : `/usr/local/ ViRobot/`.
- Configuration File Directory : `/usr/local/ViRobot/data/`
- Temporary Directory for Update Files: `/usr/local/ViRobot/update/`
- Engine Directory : `/usr/local/ViRobot/engine/`
- Temporary Directory : `/usr/local/ViRobot/tmp/`
- CGI File Installation Directory : `/usr/local/ViRobot/cgi-bin/`
- HTML File Installation Directory : `/usr/local/ViRobot/`
- Logs for File Scan Directory : `/usr/local/ViRobot/log/file/`
- Logs for Update Directory : `/usr/local/ViRobot/log/update/`
- File Backup Directory : `/usr/local/ViRobot/VRBACKUP/file/`
- Executables Directory : `/usr/local/ViRobot/sbin/`

1.2. Proxy Directory Information

- Proxy Directory : `/usr/local/ViRobot/proxy/`
- Configuration File Directory : `/usr/local/ViRobot/proxy/config/`
- Executables and Daemon Directory : `/usr/local/ViRobot/proxy/sbin/`
- Work Directory : `/usr/local/ViRobot/proxy/work/`
- Temporary Mail Directory : `/usr/local/ViRobot/proxy/temp/`
- Email Backup/Log Directory : `/usr/local/ViRobot/proxy/log/`
- Spooling Mail Directory : `/usr/local/ViRobot/proxy/spool/`
- Error Mail Directory : `/usr/local/ViRobot/proxy/error/`

1.3. Installation File Information

- ① Executables (/usr/local/ViRobot/)
 - Executables for Console : **virobot**
 - Update File : **vrproxyupdate**

- ② Engine (/usr/local/ViRobot/engine/engine version/)
 - Library File : **virobot.so**
 - Data File : **virobot.vib**

- ③ Configuration File (/usr/local/ViRobot/data/)
 - User Information File : **.htaccess**
 - Target Directory Information File : **dir.dat**
 - Configuration File : **ViRobot.cfg**
 - Installation Directory Information File : **ViRobot.key**

[Note] If you forget the user ID and the password, you can use vi editor to open this file and delete the information. After deleting the information, you will be able to login with the default user ID and password.

1.4. Proxy Installation File Information

- ① Executables (/usr/local/ViRobot/proxy/sbin/)
 - Daemon administration process : **vrstart**

- ② Configuration File (/usr/local/ViRobot/proxy/config/)
 - Proxy configuration file : **proxy.conf**
 - Virus protection configuration file : **virus.conf**
 - Mail filter configuration file : **filter.conf**
 - Spam mail blocking configuration file : **spam.conf**
 - Outgoing mail processing frequency configuration file : **spool.conf**
 - Alert mail configuration file : **warning.conf**
 - Domain setting file : **relay.txt**
 - Blocked string setting file : **subject.txt**
 - Blocked address setting file : **sender_reject.txt**
 - Blocked IP setting file : **ip.txt**

- Original messages of alert mail : **error_warning.dat**
- Original messages of mail filtering alert mail : **filter_warning.dat**
- Original messages of daily statistics mail : **stat_notify.dat**
- Original messages of spam alert mail : **subject_warning.dat**
- Original messages of virus alert mail : **virus_warning.dat**

2. Configuring ViRobot Manually on the Console

2.1. ViRobot G/W Configuration

The file named `/usr/local/ViRobot/data/virobot.cfg` contains the following configurations:

```
[root@localhost data]# vi /usr/local/ViRobot/data/virobot.cfg

[Target]
recursive=yes
archive=no

[Repair]
scanning=yes
recovery=no
delete=no
backup=no

[Others]
filelog=yes
filelogsize=10
filebackupsizesize=100
filebackupdue=10
filelogdue=10

[Setup Host]
hosts=
```

[Set Target]

- **recursive** : Enter yes following "recursive=" if you want to scan all files in the sub-directory of the target directory. Otherwise, enter no.
- **archive** : Enter yes following "archive=" if you want to include compressed files for scanning. Otherwise, enter no.

[Repair]

- **scanning** : Always enter yes for "scanning=" so that your ViRobot is able to scan for viruses.
- **recovery** : Enter yes following "recovery=" if you want to repair the infected file automatically after detection. Otherwise, enter no.
- **delete** : Enter yes following "delete=" if you want to repair the infected file automatically after detection. Otherwise, enter no.
- **backup** : Enter yes following "backup=" if you want to backup the infected file automatically to the backup directory after detection. Otherwise, enter no.

[Others]

- **filelog** : Enter yes following "filelog=" if you want to create log during file scan. Otherwise, enter no.
- **filelogsize** : The default size of the log file directory (for logs created during file scan) is 10M bytes. You can change the size of the log file directory:
- **filebackupsizesize** : Specify the size of the directory to backup the infected files that are detected during file scan. The default size is 10Mbytes. To change the size of the directory, enter the size in numeric value after "filebackupsizesize=".
- **filebackupdue** : Specify the period to keep the infected files that are detected during file scan. The default value is 10 days. To change the period, enter the period in numeric value after "filebackupdue=".
- **filelogdue** : Specify the period to keep the log for file scanning. The default value is 10 days. To change the period, enter the period in numeric value.

[Setup Host]

- **hosts** : Setup network IP address for remote management via web browser. You may use only one (1) network IP address for remote management. Enter IP xxx.xxx.xxx.xxx of the target computer after "hosts=".

2.2. Configuration of ViRobot G/W

- ① The file named `/usr/local/ViRobot/proxy/config/proxy.conf` contains the following configurations:

```
[Set mail server]
mail_server=unix.hauri.co.kr
port=5555
smtp_proxy_port=25

[Backup all mails]
allbackup=yes

[Target]
virus=yes
filter_object=yes
filter_name=yes
spam=yes

[Relay]
relay=no

[Size limit]
size=no
MB=10

[Alert mails]
virus_warning=yes
spam_warning=yes
filter_warning=yes

[Set backup/log]
backuplogdue=10
backuplogsize=200
logviewsize=1000
```

[Set Mail Server]

- **mail_server** : Specify the server address that will receive processed mail following "mail_server=".
- **port** : Enter the port of the server that will receive processed mail following "port=".

- **smtp_proxy_port**: For mail receiving service, port No. 25 is the default port. If this port is unavailable, you may change it by entering another port number following "smtp_proxy_port=".

[Backup all mails]

- **allbackup** : Enter yes following "allbackup=" to back up all mails. Otherwise, enter no.

[Target]

- **virus** : Enter yes following "virus=" to scan all mails for virus. Otherwise, enter no.
- **filter_object** : Enter yes following "filter_object=" to block mails attachment files which have the specified extensions. Otherwise, enter no.
- **filter_name** : Enter yes following "filter_name=" to block mails attachment files which have the specified names. Otherwise, enter no.
- **spam** : Enter yes following "spam=" to block spam mail. Otherwise, enter no.

[Relay]

- **relay** : Enter yes following "relay=" to use as Relay Server. Otherwise, enter no.

[Size Limit]

- **size** : Enter yes following "size=" to limit mail size. Otherwise, enter no.
- **MB** : Specify the limit capacity (at least 3MB) following "MB=".

[Alert mails]

- **virus_warning** : Enter yes following "virus_warning=" to send alert mails when blocking virus. Otherwise, enter no.
- **filter_warning** : Enter yes following "filter_warning=" to send alert mails when blocking by mail filtering. Otherwise, enter no.
- **spam_warning** : Enter yes following "spam_warning=" to send alert mails when blocking spam mail. Otherwise, enter no.

[Set backup/log]

- **backuplogdue** : Specify the time limit of storing mail backup/log. The default value is 10. To change it, enter the new number following “backuplogdue=”.
- **backuplogsize** : Specify the size of mail backup/log. The default value is 100MB. To change it, enter the new number following “backuplogsize=”.
- **logviewsize** : Set up the number of logs to be shown on one page in the [View Log]. The default value is 1000; To change it, enter the new number after “logviewsize=”.

- ② The file named `/usr/local/ViRobot/proxy/config/virus.conf` contains the following configurations:

```
[Virus Scanning]
all_scan=yes
scan_object=exe
compress=3
```

[Virus Scanning]

- **all_scan** : Enter yes following “all_scan=” to scan for virus in all mails. If you want to scan for virus in specific files only, enter no.
- **scan_object** : Enter extensions following “scan_object=” to scan mail attachment files which have the specified extensions only. For more than two extensions, separating them with comma.
- **compress** : Scan multiple compressed files. Select the required value from stages 1~3 and enter it after “compress=”.

- ③ The file named `/usr/local/ViRobot/proxy/config/filter.conf` contains the following configurations:

```
[Filter]
filter_object=dll
filter_name=readme.exe|readme.txt
```

[Filter]

- **filter_object** : To block messages by file extension, enter the extensions (separating them with comma) following “filter_object=”.
- **filter_name** : To block messages by file name, enter the files names (separating them with comma) following “filter_name=”.

- ④ The file `/usr/local/ViRobot/proxy/config/spam.conf` contains the following configurations:

```
[Spam Mail]
subject=yes
sender_reject=yes
ip_reject=no
```

[Spam Mail]

- **subject** : Enter yes following “subject=” to block spam mail by subject. Otherwise, enter no.
- **sender_reject** : Enter yes following “sender_reject=” to block spam mail by sender. Otherwise, enter no.
- **ip_reject** : Enter yes following “ip_reject=” to block spam mail by IP address. Otherwise, enter no.

- ⑤ The file named `/usr/local/ViRobot/proxy/config/spool.conf` contains the following configurations:

```
[Advanced Setting]
time=60
process=30
```

[Advanced Setting]

- **time** : Specify the frequency of mail sending (in seconds). The default value is 30. To modify the period, enter the number ranging from 1 to 3600 seconds after “time=”.

- **process** : Specify the number of mails to be sent at once. The default value is 60; To modify it, enter the number ranging from 1 to 200 after “process=”.
- ⑥ The file named `/usr/local/ViRobot/proxy/config/warning.conf` contains the following configurations:

```
[Set alert mail]
admin=yes
sender=no
recipient=yes
admin_address=root@hauri.co.kr
```

[Set Alert Mail]

- **admin** : Enter yes following “admin=” to send a alert mail to the administrator. Otherwise, enter no.
 - **sender** : Enter yes following “sender=” to sent alert mail to the sender. Otherwise, enter no.
 - **recipient** : Enter yes following “recipient=” to sent alert mail to the recipient . Otherwise, enter no.
 - **admin_address** : Enter email of the administrator to send alert mail after “admin_address=”.
- ⑦ You may enter the mail server domain in file `/usr/local/ViRobot/proxy/config/relay.txt`.
- ⑧ Enter the string for blocking mails by subject in: `/usr/local/ViRobot/proxy/config/subject.txt`.
- ⑨ Enter the address for blocking mails by sender address in: `/usr/local/ViRobot/proxy/config/sender_reject.txt`.
- ⑩ Enter the IP if you for blocking mails by IP address in: `/usr/local/ViRobot/proxy/config/ip.txt`.

3. Tips for Administrator

These guidelines will help you in the troubleshooting of ViRobot G/W.

3.1. Mail Server Configuration Checkup

If ViRobot is loaded in the mail server, check if the mail server's port has been changed properly. (Refer to Appendix > How to change the mail server's port)

3.2. Configuration Checkup

Before you run your ViRobot G/W, check whether you have set up the environment properly. If you run G/W with wrong configurations, it will not function properly. In this case, completed the configuration and restart G/W.

3.3. Service Restart

Restart the service using `/usr/local/ViRobot/proxy/sbin/vrstart`.

```
# cd /usr/local/ViRobot/proxy/sbin
# pwd
/usr/local/ViRobot/proxy/sbin
# ./vrstart
```

- Usage : **vrstart [start | stop | restart]**

- # vrstart start : Starts mail receiving and sending services

- # vrstart stop : Suspends mail receiving and sending services

- # vrstart restart : Restarts mail receiving and sending services

- Usage : **vrstart proxy [start | stop | restart]**

- # vrstart proxy start : Starts service for receiving mail

- # vrstart proxy stop : Suspends service for receiving mail

- # vrstart proxy restart : Restarts service for receiving mail

- Usage : **vrstart spool [start | stop | restart]**

- # vrstart spool start : Starts service for sending mail

vrstart spool stop : Suspends service for sending mail

vrstart spool restart : Restarts service for sending mail

⊗ The command for starting the service will not work if you are in service.

Appendix

1. Symbols and Terminology
2. How to change the mail server's port
3. DNS Server Configuration
4. FAQ

1. Symbols and Terminology

❖ **Click**

To press and release a button on a mouse once.

❖ **Double Click**

To click the left button of a mouse twice in rapid succession.

❖ **Intranet**

A data communications network, which is geographically limited, allowing easy interconnection of computers. Typically, it refers to the LAN (Local Area Network).

❖ **Extranet**

A communications network that offers nationwide as well as worldwide interconnection. Typically, it refers to the WAN (Wide Area Network).

❖ **Mailing Service**

An electronic mail service (email). It delivers required information on a regular basis.

❖ **Backup**

To copy all the files on computer disks and keep in safe storage against data loss and damage.

❖ **Compressed Files**

A data-coded file that can save storage space or transmission time. The compression ratio may vary depending on the file type as well as the compression utility.

❖ **Update**

Act of developing or installing a new software version. For an anti-virus program, it refers to replacing the virus pattern with new virus removal functions.

❖ **Interface**

Generally, it means the operating environment or familiarity of use.
(E.g. The User Interface means the interface that users interact with the system.)

❖ **Definition File**

The type of a file that defines the type that users want to check. It defines the executable files and document files that are often infected by computer viruses.

❖ **Repair**

An operation to remove the virus information in a file and recover it to the original condition.

2. How to Change the Mail Server's Port

- 1) When you install ViRobot G/W on the existing SMTP Server

When you install ViRobot G/W on the existing mail server, you should change the current service port of mail server, and set ViRobot GatewayWall for Unix to use the original port instead so as to support both virus-disinfection and mail service on one server. If the mail server's port (regardless of Sendmail or Qmail) is modifiable, you can load and execute ViRobot GatewayWall for Unix on the existing SMTP Server. The following is instructions on how to change the Sendmail, Qmail's port.

● Sendmail

- ① Access Server's console mode with root-level privileges.
- ② Shut down Sendmail service.

```
# /etc/init.d/sendmail stop
Shutting down sendmail : [OK]
```

Modify "SMTP daemon options" part in the sendmail.cf file. (sendmail.cf file's path :/etc/mail/or/etc)

```
# cd /etc/mail (or /etc/)
# vi sendmail.cf
```

Check the following options in sendmail.cf.

Before :

```
# SMTP daemon options
O DaemonPortOptions=Name=MTA
O DaemonPortOptions=Port=587, Name=MSA, M=E
```

After :

```
# SMTP daemon options
#O DaemonPortOptions=Name=MTA
#O DaemonPortOptions=Port=587, Name=MSA, M=E
O DaemonPortOptions=Port=5555
```

③ Restart /etc/init.d/sendmail.

```
[root@localhost] cd /etc/init.d/
[root@localhost init.d]# ./sendmail start
Starting sendmail: [ OK ]
[root@localhost init.d]#
```

● Qmail

- ① Access Server's console mode with root-level privileges.
- ② Revise the following section in /var/qmail/supervise/qmail-smtpd/run.

Check the following section in /var/qmail/supervise/qmail-smtpd/run.

Before :

```
#!/bin/sh
QMAILDUID=`id -u qmail`
NOFILESGID=`id -g qmail`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 2000000 \
/usr/local/bin/tcpserver -v -R -l 0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp /var/qmail/bin/qmail-smtpd 2>&1
```

After :

```
#!/bin/sh
QMAILDUID=`id -u qmail`
NOFILESGID=`id -g qmail`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 2000000 \
/usr/local/bin/tcpserver -v -R -l 0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
#-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp /var/qmail/bin/qmail-smtpd 2>&1
-u "$QMAILDUID" -g "$NOFILESGID" 0 5555 /var/qmail/bin/qmail-smtpd 2>&1
```

③ Restart /var/qmail/bin/qmailctl.

```
[root@localhost] cd /var/qmail/bin/
[root@localhost bin]# ./qmailctl restart
Restarting qmail:
Stopping qmail-smtpd
Sending qmail-send SIGTERM and restarting
Restarting qmail-smtpd
[root@localhost bin]#
```

3. DNS Server Configuration

DNS is referred to in sending mails from external server and its MX (Mail Exchange) value is used to control mail routing. If G/W is installed in your system and you want to do routing to G/W system for the incoming mails from outside, you should change the DNS configuration first.

A. How to configure UNIX/LINUX-operated DNS server

The following shows the procedure for DNS configuration:

- 1) To run DNS service, `/etc/host.conf` file should be configured.

```
# Lookup names via /etc/hosts first then by DNS query
order hosts, bind
# We don't have machines with multiple address
multi on
```

- 2) Set `/etc/hosts` file as needed.
- 3) Check the data about the zone file that you want to change in named server configuration file (`/etc/named.conf`). Set it to indicate DNS table.
- 4) Correct the required zone file.
 - Add GatewayWall for Unix server address.
 - Set the lowest value of MX for GatewayWall for Unix so that it will be recognized as the first mail exchanger of the required domain.
 - If the MX value set up in the actual mail server is "0", modify it to a number that is higher than the MX value of the newly added mail exchanger (GatewayWall for Unix).
 - Increase the serial number in SOA section.

E.g.

DNS before modification				DNS after modification			
@	IN	SOA	xxx.hauri.co.kr. master.hauri.co.kr. (2001082713 ;Serial	@	IN	SOA	xxx.hauri.co.kr. master.hauri.co.kr. (2001082720 ;Serial
			21600 ;Refresh (6 hours)				21600 ;Refresh (6 hours)
			1800 ;Retry (30 minutes)				1800 ;Retry (30 minutes)
			1209600 ;Expire (14 days)				1209600 ;Expire (14 days)
			86400) ;Minimum (1 day)				86400) ;Minimum (1 day)
	IN	NS	xxx.hauri.co.kr.		IN	NS	xxx.hauri.co.kr.
	IN	MX 10	mail		IN	MX 1	proxy
				IN	MX 10	mail
mail		IN	A 111.111.111.111	proxy	IN	A	111.111.111.112
				mail		IN	A 111.111.111.111

[Fig. A4 – 1, DNS configuration in Unix]

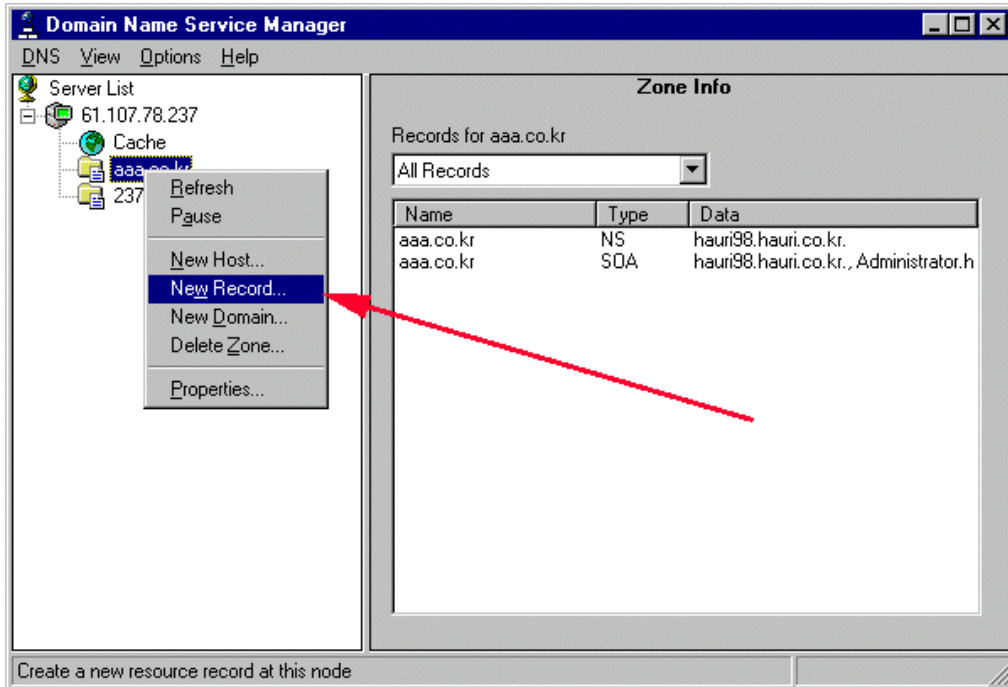
5) Restart name server daemon.

E.g. Restarting name daemon

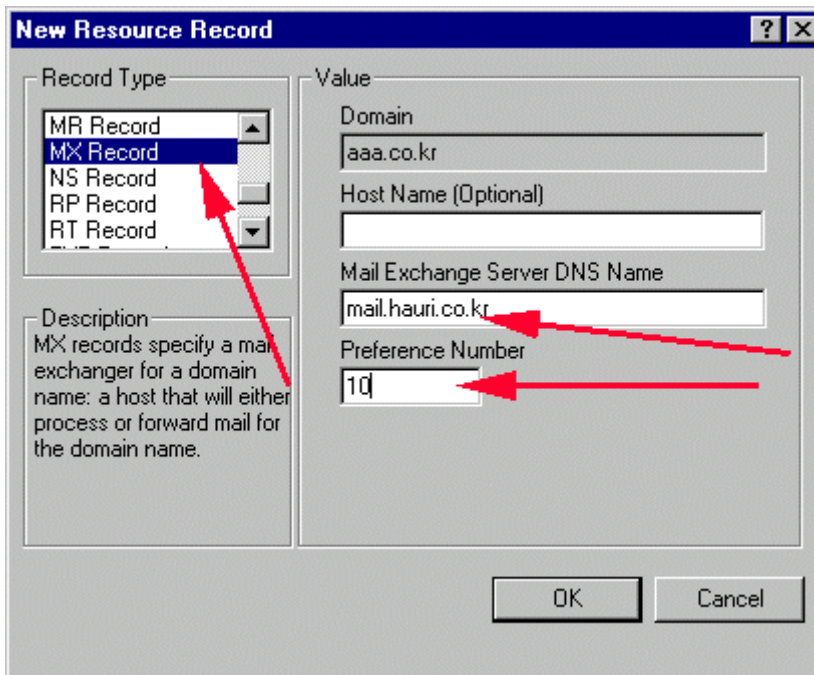
```
# ps -ef | grep named
root 169 1 0 July, 17 ? 24:45 /usr/sbin/in.named
# kill -HUP 169
```

B. How to configure Windows-operated DNS server

❖ Set DNS MX in Windows NT

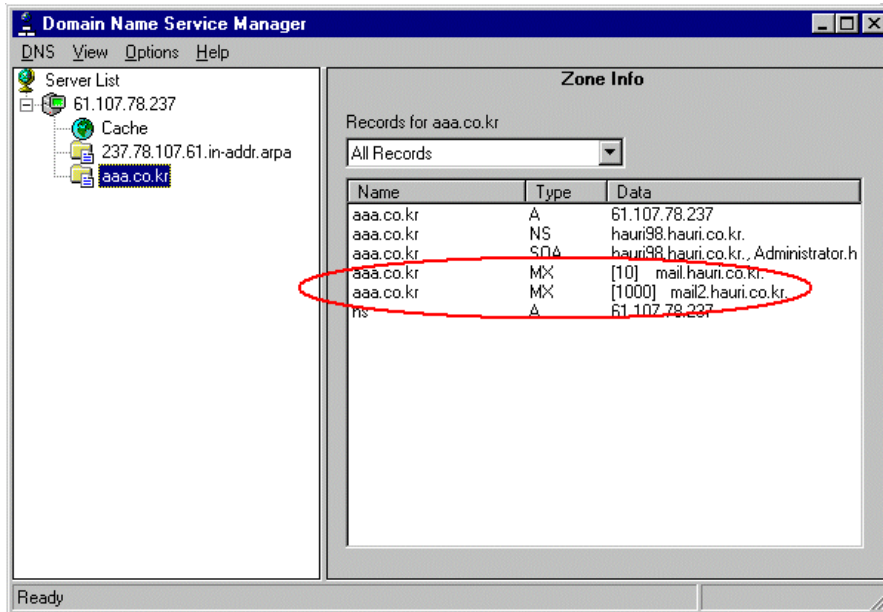


[Fig. A4 – 2,]



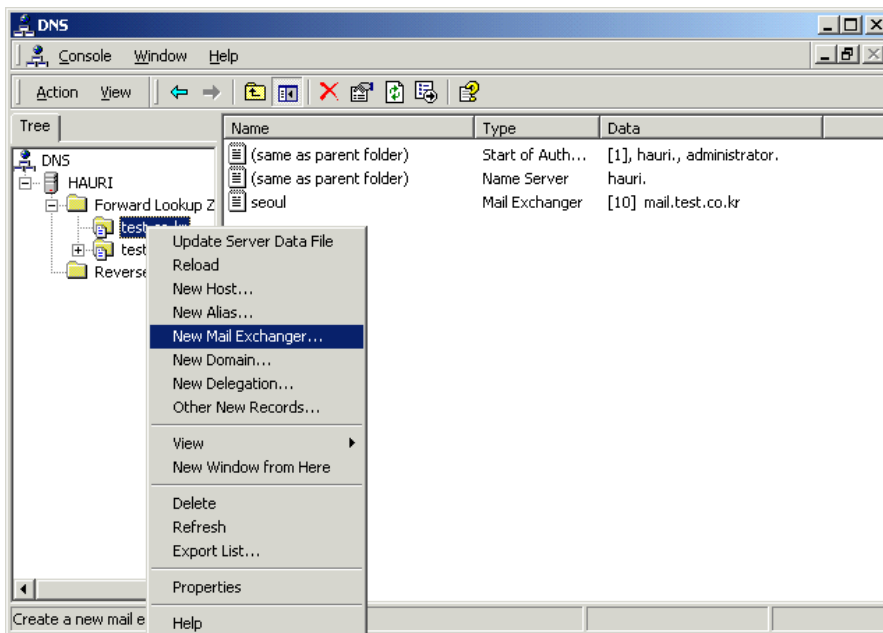
[Fig. A4 – 3, DNS configuration in Windows 2]

The lower the default number is, the higher the priority will be. Set MX value in the Server, which mail server or ViRobot GatewayWall for Unix is loaded in.



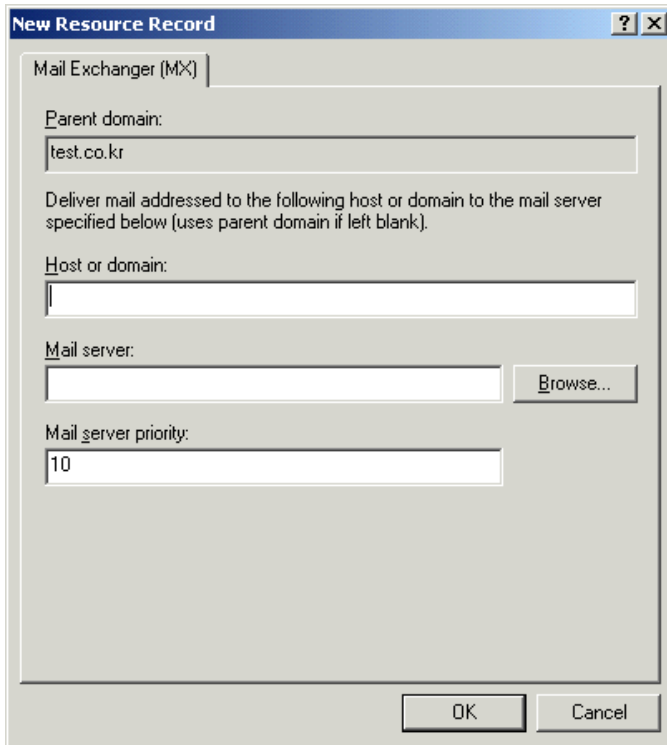
[Fig. A4 – 4,]

❖ Set DNS MX in Windows 2000 Server



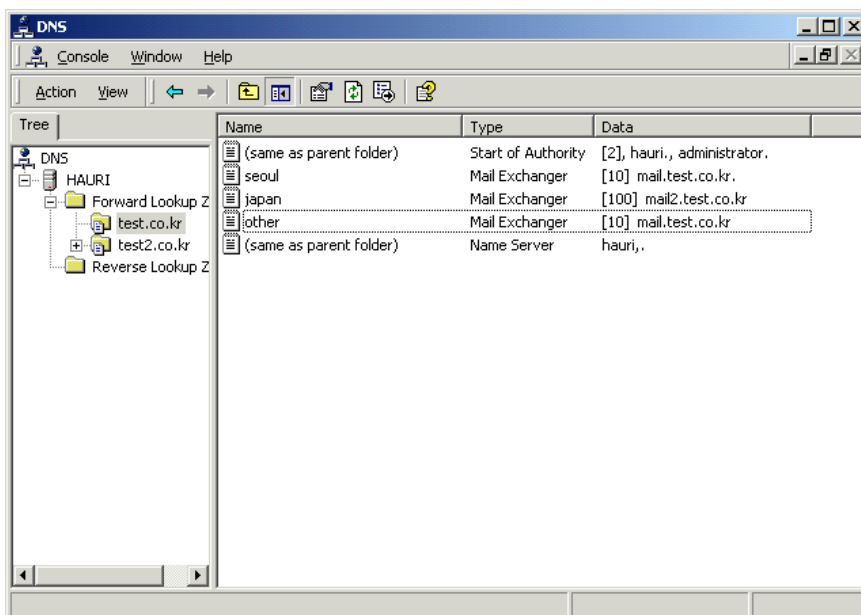
[Fig. A4 – 5,]

Click the right button, and select New Mail Exchanger.



[Fig. A4 – 6,]

Mail Server priority's default value is 10. The value is used to decide the priority when there are more than 2 MX records. The lower the number is, the higher the priority will be.



[Fig. A4 – 7,]

C. Check MX record after set DNS

Use nslookup tool to check if the DNS configuration works properly.

```
# nslookup
Default Server : ns1.hauri.co.kr
Address : 111.111.111.111

> set type=MX
> hauri.co.kr
Server : ns1.hauri.co.kr
Address : 111.111.111.111

hauri.co.kr      MX preference = 1, mail exchanger = proxy.hauri.co.kr
hauri.co.kr      MX preference = 10, mail exchanger = mail.hauri.co.kr
hauri.co.kr      nameserver = ns1.hauri.co.kr
```

4. FAQ

Q 1

ViRobot G/W does not automatically load in the CD-ROM drive.

A 1

If the CD-ROM is not loaded automatically, do the following :

[Solaris]

```
#mount /dev/dsk/c#t6d0s2(CD-ROM Device Name) /cdrom(Mount Directory)
```

[HP-UX]

```
#mount /dev/dsk/c#t2d0(CD-ROM Device Name) /SD_CDROM(Mount Directory)
```

[AIX]

```
#mount /dev/cd0(CD-ROM Device Name) /cdrom(Mount Directory)
```

Said CD-ROM device names may be different by the machine. Therefore, be sure to check your CD-ROM device name before you mount the CD-ROM.

Q 2

I want to stop the service of ViRobot GatewayWall for Unix due to some reason.

A 2

❖ If Sendmail is installed on the existing mail server

1. Stop the service of ViRobot GatewayWall for Unix.

```
# cd [ViRobot Installation Directory]/ViRobot/proxy/sbin/  
# ./vrstart stop
```

2. Set the mail server to use the port 25.

```
# cd /etc/mail (or # cd /etc/)
# vi sendmail.cf

# SMTP daemon options
O DaemonPortOptions=Name=MTA
O DaemonPortOptions=Port=587,Name=MSA,M=E
```

3. Restart `/etc/init.d/sendmail`.

```
# cd /etc/init.d
# ./sendmail restart
Shutting down sendmail : [OK]
Starting sendmail : [OK]
```

❖ If Qmail is installed on the existing mail server

1. Stop the service of ViRobot GatewayWall for Unix.

```
# cd [ViRobot Installation Directory]/ViRobot/proxy/sbin/
# ./vrstart stop
```

2. Modify the following in `/var/qmail/supervise/qmail-smtpd/run` as below.

```
# vi /var/qmail/supervise/qmail-smtpd/run

#!/bin/sh
QMAILDUID=`id -u qmail`
NOFILESGID=`id -g gmail`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 2000000\
/usr/local/bin/tcpserver -v -R -l -x /etc/tcp.smtp.cdb -c "$MAXSMTPD"\
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp /var/qmail/bin/qmail-smtpd 2>&1
```

3. Restart `/var/qmail/bin/qmailctl`.

```
# cd /var/qmail/bin
# ./qmailctl restart
Restarting qmail.
Stopping qmail-smtpd
Sending qmail-send SIGTERM and restarting.
Restarting qmail-smtpd
```

❖ If ViRobot is installed on the existing mail server – Other mail system

1. Change the SMTP server's port, which was changed to install ViRobot GatewayWall for Unix, to the port 25
2. Restart your mail system.

❖ If ViRobot is installed on another server

1. Change or delete MX value, which was added to install ViRobot GatewayWall for Unix in DNS server setting.
2. Change mail server's MX value to give mail server the higher priority.
3. Use `nslookup` to check if DNS modification is applied.

Q 3

After I install ViRobot GatewayWall for Unix, its index page (main page) on the Web Browser is not displayed.

A 3

The reason its index page (main page) is not displayed is because apache web server is not working properly. Please restart apache web server as follow.

```
# cd [ViRobot Installation Directory]/ViRobot/sbin/
# ./apachectl restart
```

Q 4

My ViRobot G/W cannot scan compressed files and sub-directories via web.

A 4

You should enable the scanning of compressed files in the configuration if you want to run ViRobot G/W via web. The same rule applies for sub-directories scanning.

Q 5

When ViRobot G/W is scanning viruses via web, although a new window appears, there is no further action.

A 5

This may happen when you try to scan too many files using ViRobot G/W via web. We recommend that you to scan specific directory when you scan virus via web. For large directory or file, please use Scan(confirm via log) or Scheduled Scan.

Q 6

Scheduled Scan and Scheduled Update do not work from my ViRobot G/W .

A 6

Scheduled scan and update of ViRobot G/W will be activated using daemon called "cron". If these functions are not available, activate "cron" on the console.

Q 7

ViRobot G/W update has failed.

A 7

If you cannot update ViRobot G/W, check the network status first and see if a firewall is installed. If the network is unstable or malfunctioning, the update will not be supported. If the firewall blocks HTTP service, you will encounter the same problem.

Q 8

Even if I install ViRobot GatewayWall for Unix on another mail server, and change DNS server setting, virus mail is still coming through.

A 8

After changing the DNS server setting, it may take some time for the new MX record to be applied.

Q 9

I want to know "Error details" in warning message for other mails in View Log of ViRobot GatewayWall for Unix.

A 9

Other mail is a mail that is blocked due to mail server's error such as a wrong recipient. Meanwhile, You can see the detail of error code, contained in the blocked mail, in View alert message > Error details.

For SMTP response code, if client sends a command to server, server sends back response code to client so that client can decide by this code to go to the next steps or sends back a command of error to server. 200 category of response code informs that the request had been done successfully, whereas 400, 500

categories inform that the response code contains an error.

Server response code	What it means
500	Syntax error, command unrecognized
501	Syntax error in parameters or arguments
502	Command not implemented
504	Command parameter not implemented
553	Requested action not taken, mailbox name not allowed
554	Transaction failed.

For more information, please refer to <ftp://ftp.rfc-editor.org/in-notes/rfc821.txt>.