

F-Secure Internet Gatekeeper for Linux

— A Comprehensive Internet and Anti-Virus Solution —

Version 4

Rev. 20111222

Administrator's Guide






About this Guide

This guide describes the installation and uninstallation, usage, and settings for F-Secure Internet Gatekeeper for Linux.

Please note that "F-Secure Internet Gatekeeper for Linux" is also referred to as "the product" and "Internet Gatekeeper" in this guide.

Symbols

Symbol	Description
 Caution	Provides important information that you need to consider.
 Note	Provides additional information that you should consider.
	Indicates that related information on the topic is available in a different chapter or another document.

Fonts

Font	Description
Arial bold (blue)	Used to refer to menu names and commands, to buttons and other items in a dialog box.
<i>Arial italics (blue)</i>	Used to refer to chapters in the manual, and to book titles of other manuals.
<i>Arial italics (black)</i>	Used for file and folder names, for figure and table captions, and for directory names.
Courier New	Used for messages on your computer screen.
Courier New bold	Used for information that you must type.
SMALL CAPS (BLACK)	Used for a key or key combination on your keyboard.
<u>Arial underlined (blue)</u>	Used for user interface links.
<i>Arial italics</i>	Used for windows and dialog names.

Contents

1. Introduction	6
2. Features.....	8
2.1 Overview	8
2.2 List of Features.....	8
3. System Requirements.....	11
3.1 Hardware Requirements	11
3.2 Software Requirements.....	12
4. Installing F-Secure Internet Gatekeeper for Linux	13
4.1 Installing an rpm Package.....	13
4.2 Installing a deb Package.....	14
4.3 Installing a tar.gz Package	15
4.4 Using the Installation Command	15
4.5 Uninstalling F-Secure Internet Gatekeeper for Linux.....	16
4.6 Backup and Restore.....	16
5. Typical Configurations.....	17
5.1 Configuration Overview.....	17
5.1.1 HTTP Connection	17
5.1.2 SMTP Connection.....	18
5.1.3 POP Connection	19
5.1.4 FTP Connection	20
5.2 Network Configuration Examples.....	21
5.3 Internet Gatekeeper Server Settings	22
5.3.1 Web Console	22
5.3.1.1 Accessing the Web Console	22
5.3.1.2 Web Console Layout	23
5.3.2 Typical Settings.....	24
5.4 Client Settings	25
6. Checking the Proxy Setup.....	26
6.1 Checking the HTTP Proxy.....	26
6.2 Checking the SMTP Proxy	26
6.3 Checking the POP Proxy	27
6.4 Checking the FTP Proxy	27
7. Advanced Settings	28

7.1 Web Console Settings.....	28
7.1.1 Proxy Settings.....	28
7.1.1.1 HTTP Proxy	28
7.1.1.2 SMTP Proxy	35
7.1.1.3 POP Proxy.....	45
7.1.1.4 FTP Proxy.....	52
7.1.1.5 Common Settings	56
7.1.2 Virus Definition Database	62
7.1.3 Logs	63
7.1.4 Top Menu.....	64
7.2 Access Control	65
7.3 Detection Notification Templates	67
7.4 Expert Options.....	69
8. Command-line Tools	70
8.1 Auto-Start	70
8.2 Proxy Execution	71
8.3 Virus Definition Updates.....	72
8.4 Restarting All Services	73
8.5 Creating Diagnostic Information.....	74
9. Logs	75
9.1 Log Files.....	75
9.1.1 Access Logs.....	75
9.1.2 Virus and Spam Detection Logs	78
9.1.3 Error Logs	79
9.1.4 Information Logs	88
9.2 Splitting/Rotating Log Files	94
9.3 Time Display Conversion Tool	95
9.4 Log Analysis Tools	96
9.5 External Output of Logs	97
10. Other Settings	98
10.1 Access Authentication.....	98
10.1.1 Host Authentication.....	98
10.1.2 Authentication using Virtual Networks	100
10.1.3 Proxy Authentication using Internet Gatekeeper	102
10.1.4 Authentication by Mail Servers	104
10.1.5 Authentication using POP-before-SMTP	105
10.2 Transparent Proxy.....	107
10.2.1 Transparent Proxy Details	108
10.2.2 Transparent Proxy – Router Mode	109
10.2.3 Transparent Proxy – Bridge Mode.....	113
10.3 Coexisting with mail servers.....	117
10.3.1 Changing the Port Number of Internet Gatekeeper	117
10.3.2 Changing the Port Number of the Mail Server.....	118

10.3.3 Changing the IP Address	121
10.3.4 Changing IP Addresses with iptables	123
10.4 Scanning Viruses Before Saving Mail to the Mail Server	125
10.5 Reverse Proxy Settings.....	128
10.5.1 Reverse Proxy – Typical Settings.....	128
10.5.2 Coexisting with Web Servers.....	129
10.5.3 Implementing a HTTPS (SSL) Server	130
11. Product Specifications.....	132
11.1 Product Specifications.....	132
11.2 HTTP Proxy Process.....	134
11.3 SMTP Proxy Process	136
11.4 POP Proxy Process	138
11.5 FTP Proxy Process	140
11.6 HTTP Error Responses.....	144
11.7 HTTP Request and Response Headers	146
11.8 SMTP Command Responses.....	148
11.9 SMTP Commands – Operations	151
11.10 POP Commands – Operations.....	155
11.11 FTP Commands – Operations	157
11.12 Connection Error Messages.....	160
11.13 Service Process List.....	162
11.14 Detection Names.....	164
11.15 Riskware.....	166
12. Copyright Information.....	168

1. Introduction

F-Secure Internet Gatekeeper for Linux is an Internet Gatekeeper solution designed to protect corporate networks, Internet Service Provider networks, and home networks against malware.

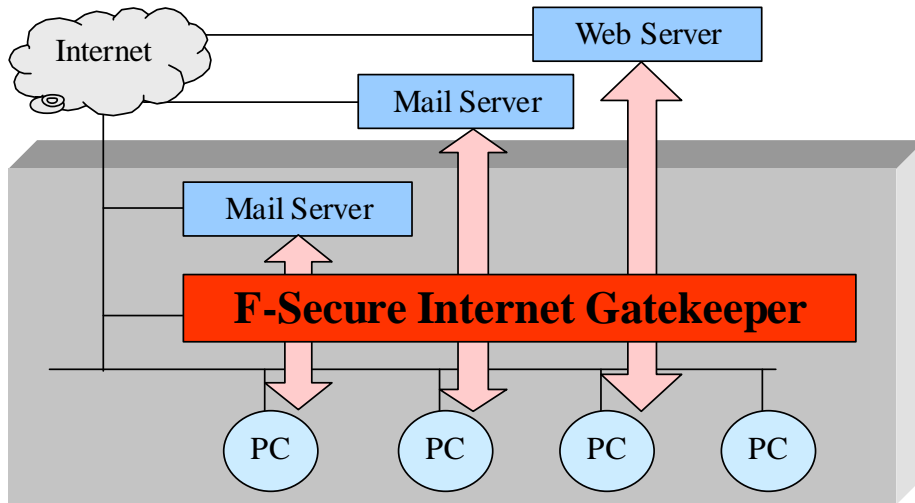
Computer viruses are one of the most harmful threats to the security of data on computers. Viruses have become even more widespread due to the trend in standardizing platforms and the continuous spread of the Internet. In addition to corrupting or falsifying data, viruses can also cause damage by using the Internet to leak confidential company data or personal information. Even if the leaked information is not important in itself, viruses can use the computer to spread their infection more, resulting in harm to others.

With F-Secure Internet Gatekeeper for Linux, you can scan for viruses centrally. You can monitor web site connections, and the sending and receiving of e-mails from all computers in a LAN (Local Area Network).

The product can scan communication that is based on HTTP, FTP, SMTP, and POP. The ability to use the POP protocol means that you do not need to make any changes to the mail server to check e-mail for viruses. You can simply pass all inbound and outbound e-mail through F-Secure Internet Gatekeeper for Linux.

The product is very fast, being optimized for performance. This makes it suitable for large-scale networks, and for networks that support high-speed broadband. It also means that performance is adequate even when the product is run on less powerful computers.

The product also supports a transparent proxy, various authentication functions, and spam blocking. The product is available also in Japanese.



2. Features

2.1 Overview

F-Secure Internet Gatekeeper for Linux:

- Protects a range of different networks against viruses:
 - Internal company networks
 - ISP networks
 - Home networks
- Uses a single computer to monitor the network access by all computers on the company, ISP, or home network.
- Does not use any resources from other computers on the network.
- Is easy to install and administer on an existing network.
- Can be used both on large and small networks. Adequate performance can be obtained also on less powerful computers.

2.2 List of Features

Monitor Web Browsing and E-mail Traffic

- HTTP
- FTP
- SMTP
- POP

High-Speed Virus Scanning Proxy

- Best performance when compared to any Internet Gatekeeper product (based on research by F-Secure)
 - * Pentium III 1GHz Dual, MEM: 1GB, NETWORK: Performance measured on a 1000BaseTX network
 - HTTP : 120Mbps, 640 sessions/sec (Average 23 KB/session)
 - SMTP: 110Mbps, 130 sessions/sec (Average 80 KB/session)
 - 1000 or more simultaneous connections
 - Adequate performance can be obtained on less powerful computers
 - Operation on a single computer is practical even on large networks

Simple Installation

- Runs in almost all Linux environments
- Combines all functions in a single computer
- Can be installed as an rpm or deb package. The rpm package complies with Linux Standard Base, which is used in Red Hat Linux and some other distributions.
- Can be installed as a .tar.gz package (for any Linux distribution)

Simple Configuration

- No configuration changes are required on your mail server
- No changes are required to your network configuration
- Minimal configuration changes for individual users
- All settings can be configured in the web console
- The language of the web console can be changed while using it

Authentication Functions

- Supports POP-before-SMTP authentication
- Supports proxy authentication for various protocols (HTTP proxy authentication, SMTP authentication, POP/FTP user restrictions)
→ Proxy authentication operates via PAMs (Pluggable Authentication Modules) and can integrate with other authentication methods such as UNIX accounts, LDAP, NIS, and Radius.
- Access restrictions can be set for all protocols based on the IP address, host name, or domain name
- The SMTP receive domain can be restricted to prevent relaying through a third party
- Existing SMTP authentication function on a mail server can be used
- Existing APOP function on a mail server can be used

Virus Detection Notifications

- The notification text can be edited and customized freely
- UTF-8 characters (for example, Japanese) can be used in messages
- An e-mail can be sent to the administrator when a virus is detected
- The header and body of the notification e-mail are customizable

Flexible Configuration

- Can use a transparent proxy (HTTP, SMTP, POP, and FTP)
- Individual users can select POP servers independently
- Scans files that are sent by using the HTTP protocol for viruses. Supports POST and PUT methods.
- Supports sending and receiving from dedicated FTP clients
- Supports multi-level connections using parent proxy settings
- Can monitor all connections to designated web servers by using parent proxy settings (reverse proxy)
- Can connect to any mail server
- Can use any mail server running on the same computer
- SMTP reception and SMTP transmission can be configured independently

Anti-Virus

- Uses the award-winning and proven F-Secure engine
- Can handle practically all existing viruses
- Can handle viruses for Windows, DOS, Microsoft Office, VBS, Linux, and other environments
- Combined use of multiple engines (FS-Engine (Hydra) and Aquarius) allows for a quick response to new types of virus
- Low level of misdetection and false alarms
- Supports various file archive formats (ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2 up to six levels of nesting)
- Virus definition files can be updated automatically

Spam Blocking

- Supports spam detection for both SMTP and POP
- Uses a prioritized black list and white list to scan designated headers and the e-mail body to detect spam by using customized conditions
- Uses the Spam detection engine
- Can use a RBL (Realtime Black List) to detect spam from the sender's e-mail address
- Can use a SURBL (SPAM URL Realtime Black List) to detect spam that contains spam domain URLs in the e-mail body
- Adds a spam identification header ("X-Spam-Status: Yes") to spam e-mail to allow easy sorting
- Adds predefined text (such as "[[SPAM]]") to the e-mail subject to allow easy sorting

Other Features

- Can specify whether to block or allow files based on conditions such as the file extension, User-Agent, and file size
- Can block ActiveX and script (JavaScript or VBScript) content
- Can generate access statistics in a Squid compatible log
- Can output to external logs such as syslog
- Includes an HTTPS (encrypted HTTP) proxy function. However, because communication is encrypted, HTTPS (SSL) is not scanned for viruses.
- A virus identification header (X-Virus-Status: infected) can be added to virus detection notification e-mails to allow easy sorting

3. System Requirements

F-Secure Internet Gatekeeper for Linux has the following system requirements.

3.1 Hardware Requirements

Minimum Hardware Requirements

CPU	Intel Pentium compatible CPU
MEMORY	512 MB RAM or more
DISK	5 GB or more free space (Installed files need at least 1GB of free disk space and running system needs significantly more for temporary files, logs etc.)
NETWORK	TCP/IP connection

Recommended Hardware

CPU	Intel Pentium compatible CPU 2GHz or faster
MEMORY	1 GB or more
DISK	20 GB or more free space
NETWORK	100BaseT or better

3.2 Software Requirements

Required Components

- Linux kernel 2.4/2.6
- glibc 2.3.2 or later
- perl 5.8 or later

Supported Distributions

32-bit:

- Asianux Server 3
- Asianux 2.0 (MIRACLE LINUX 4.0)
- Asianux 1.0 (MIRACLE LINUX 3.0)
- CentOS 4/5
- Debian GNU/Linux 5.0
- Red Hat Enterprise Linux 3/4/5
- SuSE Linux Enterprise Server 9/10/11
- Turbolinux 10 Server/11 Server
- Ubuntu 8.04

64-bit(x86_64):

- Asianux Server 3
- Asianux 2.0 (MIRACLE LINUX 4.0)
- CentOS 5
- Debian GNU/Linux 5.0
- Red Hat Enterprise Linux 4/5
- SuSE Linux Enterprise Server 9/10/11
- Turbolinux 10 Server/11 Server
- Ubuntu 8.04

* On x86_64 platforms, the product requires 32-bit libraries to be installed, and it runs in 32-bit mode.

4. Installing F-Secure Internet Gatekeeper for Linux

Use either the rpm package, deb package or tar.gz package to install F-Secure Internet Gatekeeper for Linux.



Note

- Use the rpm package for installation if possible.
- You can install updates by following the same steps. The existing configuration settings are not changed.

4.1 Installing an rpm Package

This section explains how to install F-Secure Internet Gatekeeper for Linux on a server, which runs one of the Red Hat family of Linux distributions.



Note

In a Red Hat distribution, you can easily install the software by using the rpm package. The Red Hat family of distributions include the following:

- Red Hat
- Turbolinux
- SUSE Linux
- MIRACLE LINUX / Asianux

* Please refer to the related installation guides for instructions on how to install each distribution.

You can install the package by double clicking the rpm package, or executing the following command with root privileges:

```
# rpm -Uvh fsigk-XXX.i386.rpm
```

This installs the whole product and makes the web console available for use.

➡ Next, see “[Typical Configurations](#)”, 15.

4.2 Installing a deb Package

This section explains how to install F-Secure Internet Gatekeeper for Linux on a server, which runs one of the Debian or Ubuntu based Linux distributions.



Note

In a Debian or Ubuntu distribution, you can easily install the software by using the deb package.

You can install the package by double clicking the deb package, or executing the following command with root privileges:

```
# dpkg -i fsigk-xxx_all.deb
```

This installs the whole product and makes the web console available for use.

➡ Next, see “*Typical Configurations*”, 15.

4.3 Installing a tar.gz Package

If you cannot use the rpm or deb package to install F-Secure Internet Gatekeeper for Linux, you can install it by using a tar.gz package.

Execute the following command with root privileges:

```
# tar -zxvf fsigk-XXX.tar.gz
# cd fsigk-XXX/
# make install
```

This installs the whole product and makes the web console available for use. To specify the installation options, see “[Using the Installation Command](#)”, 13.

➡ Next, see “[Typical Configurations](#)”, 15.

4.4 Using the Installation Command

When you use the tar.gz package to install the software, you can specify installation options during the installation. Run the installation command as described below. You can omit the options if needed.

```
make [options]... target
```



Although you can specify the installation options, we recommend that you use the "make install" command for installation.

Target

install Install. We recommend that you specify this target. In addition to installing the files, this also installs the startup script and PAM setup files and starts the web console service.

Options

prefix=[dir] Specifies the installation directory. We recommend that you install the product in the default installation directory (/opt/f-secure/fsigk).

suffix=[name] Specifies a suffix. Use this option if you install multiple copies of the software on the same server. Adds a suffix to the executable file and other command names (fsigk) to distinguish between each copy. The suffix must be less than two characters.

adminport=[num] Specifies a port number other than the default port (9012) for the F-Secure Internet Gatekeeper for Linux web console. Use this option when you install multiple copies of the software on the same server.

lang=[ja|en] Specifies the language of the product. The available languages are "ja" (Japanese) and "en" (English). If no language is specified, the language is selected automatically. Automatic selection selects Japanese if the time zone is JST or the LANG environment variable starts with "ja". Otherwise, English is selected. This setting determines the default language for the web console and the default templates for virus detection messages.

Command examples

To install the whole product, use this command:

```
# make install
```

To install multiple copies of the software, use this command:

```
# make prefix=/opt/f-secure/fsigk2 suffix=2 adminport=10012 install
```

4.5 Uninstalling F-Secure Internet Gatekeeper for Linux

Follow the steps below to uninstall the software. This removes the files installed on the system, deletes the configuration settings, and shuts down the service.

Execute the following command with root privileges:

```
# cd /opt/f-secure/fsigk
# make uninstall
# rm -rf /opt/f-secure/fsigk
```

If you use the rpm package, execute the following command:

```
# rpm -e fsigk
```

If you use the deb package, execute the following command:

```
# dpkg -r fsigk
```

4.6 Backup and Restore

Follow these steps to back up and restore F-Secure Internet Gatekeeper for Linux.

To back up the product, save the contents of the following directories as needed:

/opt/f-secure/fsigk : Entire system state

/opt/f-secure/fsigk/conf : Configuration files

/opt/f-secure/fsigk/log : Log files

(Note that the settings for definition file updates are saved separately by using crontab.)

To restore the software to its previous state, restore the files and then (forcibly) reinstall the package.

For rpm package:

```
# rpm -Uvh --force fsigk-xxx-0.i386.rpm
```

For deb package:

```
# dpkg -r fsigk
```

```
# dpkg -i fsigk-xxx_all.deb
```

5. Typical Configurations

Once the installation has completed, locate the appropriate Internet Gatekeeper server and modify the settings as required. The next step is to configure client computers.

5.1 Configuration Overview

The following section describes how HTTP, SMTP, POP, and FTP connections operate in these cases:

- virus scanning is not used
- Internet Gatekeeper performs virus scanning

5.1.1 HTTP Connection

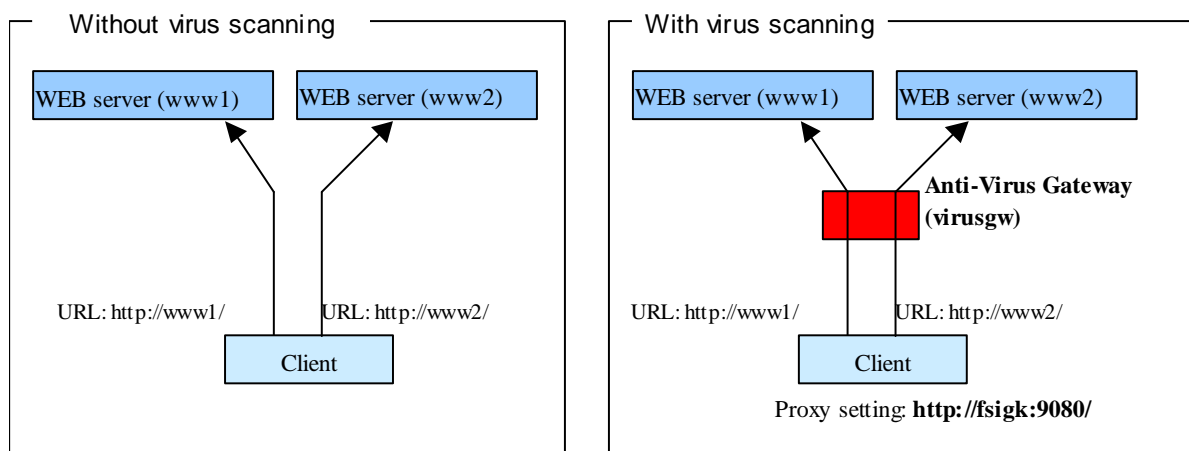
- **Without virus scanning**

The web browser connects to the web server directly and fetches the page.

- **With virus scanning**

When virus scanning is used, Internet Gatekeeper stands between the web server and client and operates as a proxy server for the web browser. The web browser connects to the web server through Internet Gatekeeper. The web browser retrieves pages after they have been scanned for viruses. Internet Gatekeeper connects to the appropriate web server based on the URL that has been requested from the web browser.

HTTP Connection example



5.1.2 SMTP Connection

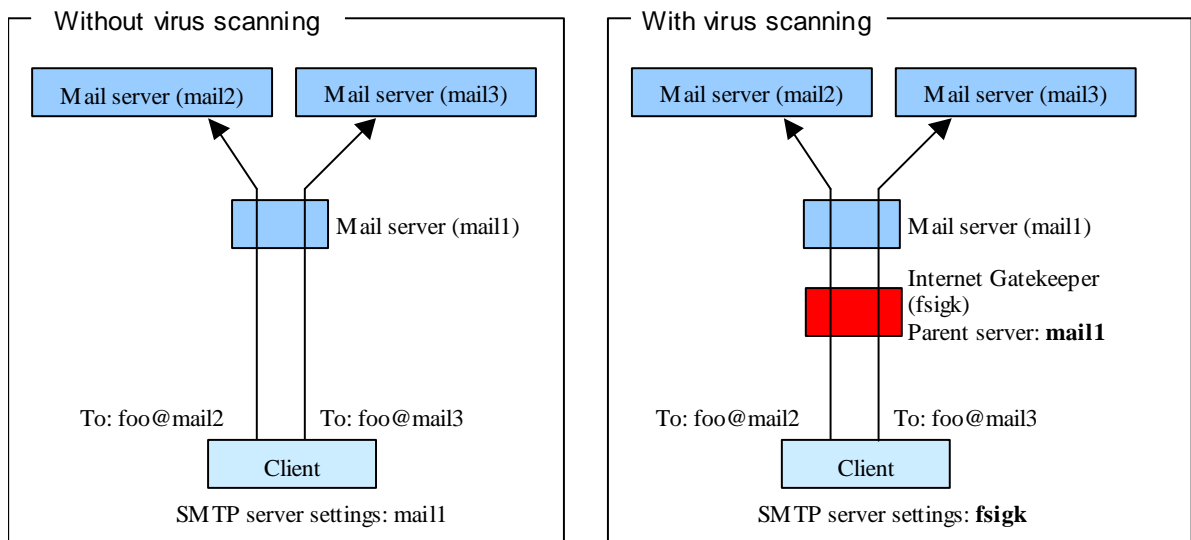
- **Without virus scanning**

The e-mail client sends e-mail to mail servers on the Internet through an SMTP server for outbound e-mail.

- **With virus scanning**

When virus scanning is used, Internet Gatekeeper stands between the client and mail server and operates as the SMTP server for the e-mail client. The client connects to the SMTP server through Internet Gatekeeper. The client sends outbound e-mail to mail servers on the Internet. Internet Gatekeeper forwards the mail through the outbound mail server.

SMTP Connection example



5.1.3 POP Connection

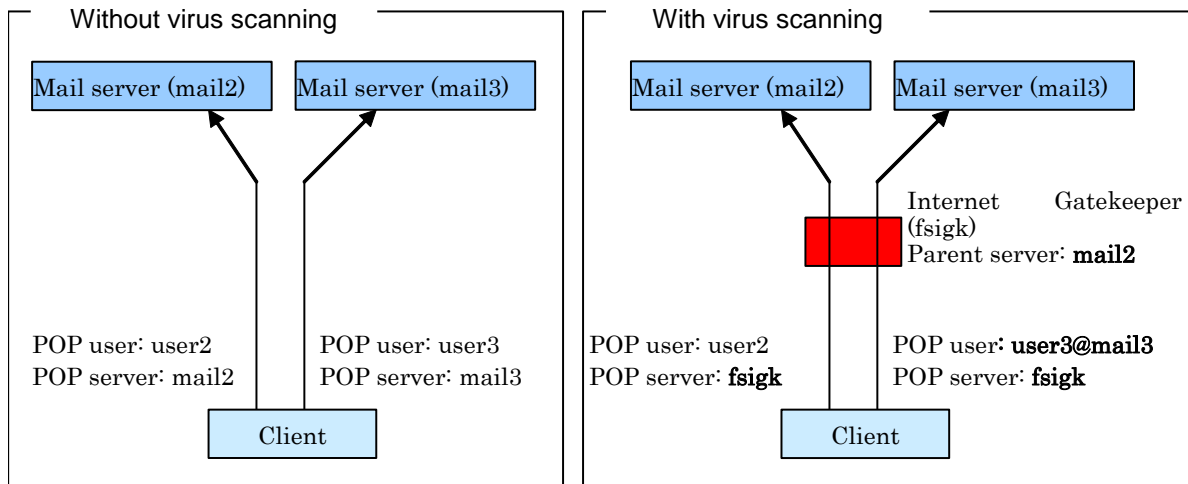
- **Without virus scanning**

To retrieve e-mail, the e-mail client connects to the mail server directly by using the POP protocol.

- **With virus scanning**

When virus scanning is used, Internet Gatekeeper stands between the client and mail server and operates as the POP server for the e-mail client. The client connects to the mail server through Internet Gatekeeper. The client retrieves e-mail that has been scanned for viruses. Although Internet Gatekeeper usually connects to the designated parent server, you can specify that the connection is created to any POP server. To do this, specify the POP user name in the format "<POP server user name>@<POP server name>".

POP Connection example



5.1.4 FTP Connection

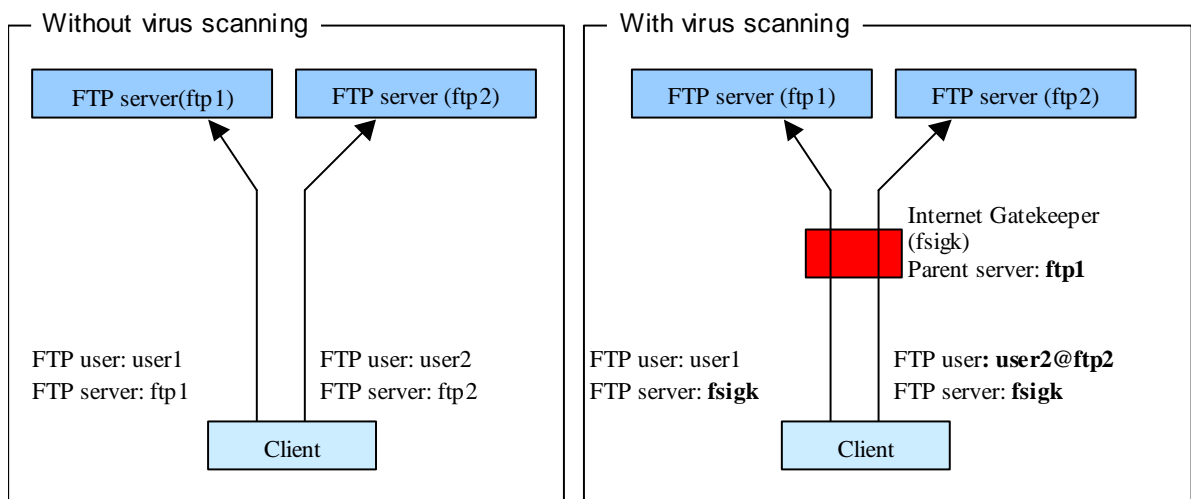
- **Without virus scanning**

To send and receive files, the FTP client connects to an FTP server directly by using the FTP protocol.

- **With virus scanning**

When virus scanning is used, Internet Gatekeeper stands between the client and server and operates as a proxy server for the FTP client. The client connects to the FTP server through Internet Gatekeeper. The client sends and receives files that have been scanned for viruses. If the FTP client does not support a proxy server, Internet Gatekeeper usually connects to the designated parent server. However, you can specify that the connection is created to any FTP server. To do this, specify the FTP user name in the format "<FTP server user name>@<FTP server name>".

FTP Connection example

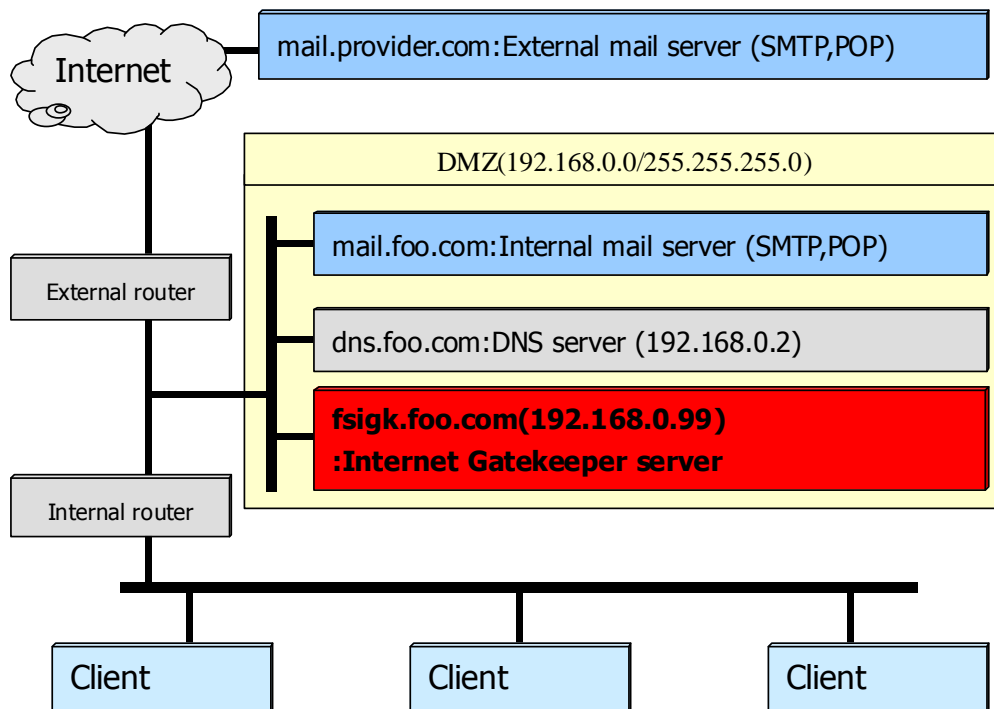


5.2 Network Configuration Examples

F-Secure Internet Gatekeeper for Linux operates as a proxy server, which is located between the client and the web and mail servers. The scenarios described here assume that Internet Gatekeeper is installed in a typical network configuration like the one shown below.



The network configuration below shows that the gateway is located in a DMZ network. However, installation in a DMZ is not necessary if connections from the Internet are not required.



5.3 Internet Gatekeeper Server Settings

To use F-Secure Internet Gatekeeper for Linux for virus scanning, configure the Internet Gatekeeper server in which the product is installed as follows.



Always specify the following settings:

- Service On/Off
Use the On and Off buttons in the web console for each proxy to enable or disable the service.
- Port number to use for each service
- Parent servers for SMTP and POP
Specify the [host name] and [port number] for your existing mail server.

5.3.1 Web Console

Use the web user interface to change the product settings. The web user interface is called the "web console".

5.3.1.1 Accessing the Web Console

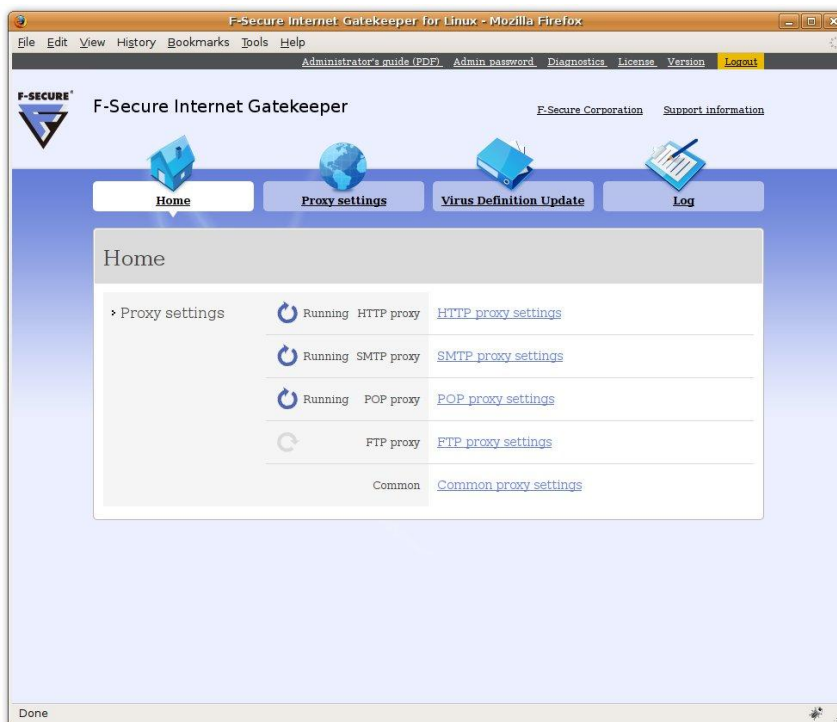
- 1 Access the following URL from your web browser.

http://<hostname>:9012/

(Where <hostname> is the domain name or IP address of the server where Internet Gatekeeper is installed.)

- 2 To log in, enter your user name and password in the connection dialog box.
The default account is: User name: **admin**, Password: **admin**

The Home page of the web console opens.

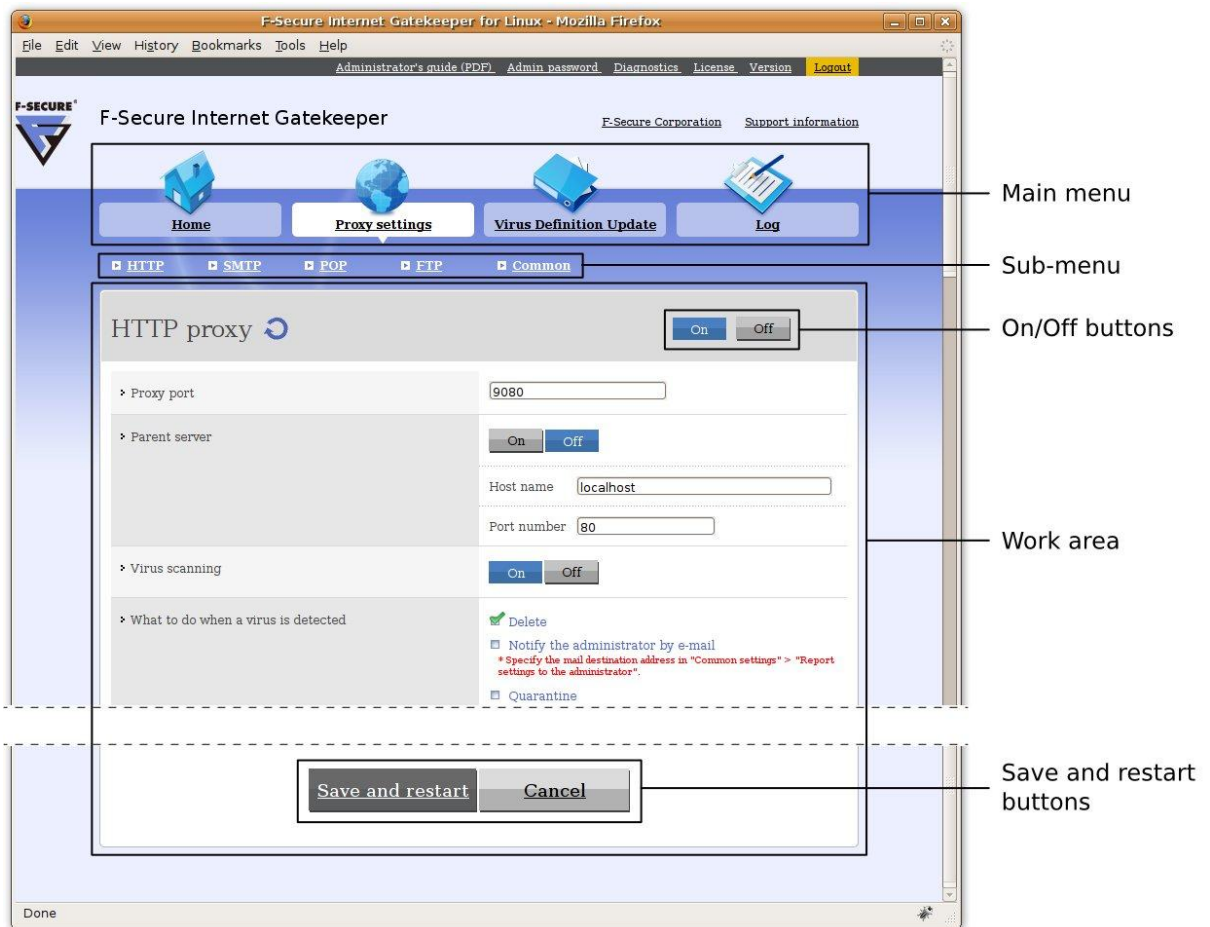




If you cannot connect to the web console, view the error log (/opt/f-secure/fsigk/log/admin/error.log) from the command line.

5.3.1.2 Web Console Layout

The web console consists of a menu on the left of the screen and a work area on the right. The example below shows the screen when you select **Proxy settings** from the main menu, and **HTTP** from the sub-menu.



Field	Description
Main menu	Select the category of settings you want to specify. A sub-menu appears under the main menu. The sub-menu is different for each item in the main menu.
Sub-menu	Click a menu item to show the corresponding settings page in the work area.
Work area	Area that contains the default settings. You can change them as required.
On and Off buttons	To enable a service, click On . To disable a service, Click Off .
Save and restart buttons	To save the settings and start the enabled services, click the Save and Restart button. To discard unsaved settings, click the Cancel button.

5.3.2 Typical Settings

In a typical product setup, the following settings are specified in the web console.

Proxy Settings

After editing the settings, click the **Save and Restart** button. The enabled services are started and the changed settings are applied.

Proxy Settings

HTTP proxy: **On**

Proxy port: **9080**

SMTP proxy: **On**

Proxy port: **25**

Global settings

Parent server

Host name: **mail.example.com**

Port number: **25**

POP proxy: **On**

Proxy port: **110**

Parent server:

Host name: **mail.example.com**

Port number: **110**

FTP proxy: **On**

Proxy port: **9021**

Common settings

Settings to notify the administrator

E-Mail address: **fsigkadmin@example.com**

SMTP server: (Host name: **mail.example.com**, Port number: **25**)

Other Settings

Specifies the other required settings.

Virus definition database

Automatic Updates

Update frequency: **Hourly**

Other

Administrator password

New password: **Enter password**



Note

This is the password used to log into the web console.

License

License key: **License key that you received when you purchased the software**

5.4 Client Settings

To use F-Secure Internet Gatekeeper for Linux for virus scanning, you need to change the proxy server setting in your web browser and the mail server setting in your e-mail client.

Web Browser Settings

Proxy server

Host name: **fsigk.example.com**

Port number: **9080**

Mail Client Settings

Internal mail box

SMTP server: **fsigk.example.com**

POP server: **fsigk.example.com**

External mail box

SMTP server: **fsigk.example.com**

POP server: **fsigk.example.com**

POP user name: **username@mail.provider.com**

6. Checking the Proxy Setup

After configuring the settings, follow the steps below to confirm that the software is working correctly.



If the software is not working correctly, use one of the following methods to view the error log.

- From the web console, select "HTTP", "SMTP", "POP", or "FTP" from the "Log" menu and then view the "Error log".
 - View the error log from the command line
(`/opt/f-secure/fsigk/log/{http,smtp,pop,ftp}/error.log`).



If you cannot connect to the Internet, run the "make eicar" command from the "/opt/f-secure/fsigk" directory to create a test virus file (eicar.com).

6.1 Checking the HTTP Proxy

Do the following and confirm that a virus detection warning appears:

Start your web browser and download the test virus (eicar) from the following location:

http://www.eicar.org/anti_virus_test_file.htm

6.2 Checking the SMTP Proxy

Do the following and confirm that the virus does not reach the e-mail recipient:

- 1 Start your web browser and download the test virus (eicar) from the following location:

http://www.eicar.org/anti_virus_test_file.htm



Clear the proxy setting in the browser. This prevents the test virus from being detected and deleted when it is downloaded.

- 2 Send an e-mail with eicar as an attachment.

6.3 Checking the POP Proxy

Do the following and confirm that the virus is detected:

- 1 Start your web browser and download the test virus (eicar) from the following location:

http://www.eicar.org/anti_virus_test_file.htm



Clear the proxy setting in the browser. This prevents the test virus from being detected and deleted when it is downloaded.

- 2 Send an e-mail with eicar as an attachment.



Set the e-mail client to send the e-mail directly rather than through the Internet Gatekeeper server. This prevents the test virus from being detected and deleted when it is sent.

- 3 Receive the e-mail.

6.4 Checking the FTP Proxy

Do the following and confirm that the virus is detected:

- 1 Start your web browser and download the test virus (eicar) from the following location:

http://www.eicar.org/anti_virus_test_file.htm



Clear the proxy setting in the browser. This prevents the test virus from being detected and deleted when it is downloaded.

- 2 Use FTP to send and receive the eicar file.

7. Advanced Settings

7.1 Web Console Settings

You can use the web console to change the settings as required. The settings are described below.

- ➔ For information on the web console, see “[Web Console](#)”, 20.

7.1.1 Proxy Settings



Note

The name in parentheses () is the item name in the settings file (conf/fsig.ini).

Proxy settings

Proxy Settings

Specifies how the virus scanning proxy works.

Click the **Save and Restart** button to apply the settings and restart the specified services. You can also use the `chkconfig` command to change the automatic startup settings.

7.1.1.1 HTTP Proxy

HTTP Proxy

HTTP Proxy (http_service)

Click the **On** and **Off** buttons to start or stop the HTTP proxy service.

Proxy port

Proxy Port (svcport)

Specifies the port number used by the proxy service.

Usually, you need to specify only the port number. To specify the port number, IP address, and interface name all together, use the following format:

Syntax: [A.A.A.A%EEE:PPP|A.A.A.A:PPP|%EEE:PPP|PPP]

(PPP: Port number, A.A.A.A: Address, EEE: Interface)

Examples: 9080, 10.0.0.2:9080, %eth0:9080, 10.0.0.2%eth0:9080



Note

- You can specify only one inbound port number. To listen for connections on more than one port, use the REDIRECT setting in the iptables function of Linux. For example, to listen for connections on both port 9080 and port 12345, set 9080 as the inbound port number. Use iptables to redirect port 12345 to port 9080. In this case, use the following command to set up iptables:


```
# iptables -t nat -A PREROUTING -p tcp -dport 12345 -j REDIRECT -to-port 9080
```

 After specifying the setting, save the iptables configuration:


```
# /etc/init.d/iptables save
```
- See your Linux distribution documentation for information about using and saving

iptables on your system.

Parent server

Parent Server (self_proxy / parent_server_host / parent_server_port)

All connections are forwarded to the specified server.

If you use more than one level of proxies, specify the parent proxy.

If the parent server is used as a reverse proxy, specify the web server.

Virus scanning

Do Virus Check (virus_check)

Enables or disables virus scanning.

We recommend that you enable this setting.



Virus scanning is not performed for HTTPS (SSL) because communication is encrypted.

What to do when a virus is detected

Action on Viruses

Delete

Delete (action={pass,delete})

Specifies whether to delete viruses. The detection event is recorded in the log, and a notification is sent to the administrator even if the virus is not deleted.

We recommend that you enable this setting.

Notify the administrator by e-mail

Notify Admin (notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in [Settings to notify the administrator](#) under “Common settings”. To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification from being detected as a virus. “Number” is a random number, which is set as admin_notification_id in the settings file during the installation.

Quarantine

Quarantine(keep) (quarantine)

Quarantines viruses. The viruses are quarantined in the directory that you can set in [Quarantine directory](#) under “Common settings”.

Specify this setting only if sufficient disk space is available.

Edit the virus detection message

Detection message

Edits the message that is shown when a virus is detected.

Enter the message by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

🔄 For information on variables and options, see “[Detection Notification Templates](#)”, 67.



- If you edit the message from the command line, you need to restart the service afterwards.
 - If you edit the virus detection message by using the web console, the following file is updated: /opt/f-secure/fsigk/conf/template_http.html.

HTTP proxy authentication

Proxy authentication (proxyauth_pam_auth)

Authenticates the proxy by using PAMs (Pluggable Authentication Modules). You can change the authentication method in the `/etc/pam.d/fsigk_http` file.

🔗 For more information, see "[Proxy authentication using Internet Gatekeeper](#)", 102.

Add or remove users

User DB

Edits the database of users who are permitted to connect. You can add, delete, and modify users and passwords.

Maximum number of simultaneous connections

Maximum connections (pre_spawn)

Specifies the maximum number of simultaneous connections from clients. The specified number of processes listens for connections from clients.

You can check the number of connections in "Internal process ID" in the access log (`access.log`).



- If you increase the maximum number of connections, more connections are allowed, but it requires more memory. Approximately 500 KB of memory is used per process.
- A warning is output to the error log if the maximum number of connections is reached.
- We recommend that you set an initial value of approximately 200 and then monitor the performance. The value of the setting is usually less than 2000. (The setting itself permits values up to 9999.)

Access control

Access Control

From these hosts

From: (acl_from)

Only accepts connections from the designated list of hosts.

If [DNS Reverse Lookup] is enabled, you can also specify `<host name>.<domain name>`.

🔗 For examples, see "[Access Control](#)", 65.



If you edit the "From these hosts" setting in the web console, the `http from` field is updated in `/opt/f-secure/fsigk/conf/hosts.allow`.
See man page `hosts_access(5)` for more information on the syntax used in the file.

To these hosts

To: (acl_to)

Only accepts connections to the designated list of hosts.

🔗 For examples, see "[Access Control](#)", 65.



If you edit the "To these hosts" setting in the web console, the `http to` field is updated in `/opt/f-secure/fsigk/conf/hosts.allow`.
See man page `hosts_access(5)` for more information on the syntax used in the file.

Exclude these targets from the virus scan

Skip scanning for:

User-Agent

User-Agent: (pass_user_agent, pass_user_agent_list)

Skips virus scanning for connections from clients with the specified User-Agent. Usually, all data is saved and transmitted to the client only after the virus scanning is completed. If you enable this setting, the data for connections from clients with the specified User-Agent is forwarded as soon as it is received. Use this setting for clients that use streaming or are at risk of timing out.

Separate each setting with a comma (","). The list is searched by using forward matching. The setting is case sensitive.

The maximum length of the setting is 1999 bytes.



Regardless of this setting, the following User-Agents are not scanned for viruses. User-Agents skipped by default:

- "Service Pack Setup" (service pack installer for Microsoft Windows)
- "Office Update" (update program for Microsoft Office)
- "Symantec LiveUpdate" (update program for Symantec definition files)
- "TMhtload" (update program for TrendMicro definition files)
- "BW-C" (update program for F-Secure definition files (AUA))
- "GETDBHTTP" (update program for F-Secure definition files (getdbhttp))
- "RealPlayer" (Real Player)
- "RMA" (Real Player)
- "NSPlayer" (Microsoft Windows Media Player)
- "urlgrabber" (update program for Linux YUM package)
- "Microsoft BITS" (Microsoft Windows Update)
- "Windows-Update-Agent" (Microsoft Windows Update)
- "Adobe Update Manager" (update program for Adobe)
- "Mozilla/4.0 (compatible; Win32; Commtouch Http Client" (This product's Spam Detection Engine)

Host name

Hosts: (acl_pass_to)

Skips virus scanning for connections to the specified hosts.

Usually, all data is saved and transmitted to the client only after the virus scanning has completed. If you enable his setting, the data for connections to the specified hosts is forwarded soon as it is received.

🔗 For examples, see "[Access Control](#)", 65.



If you edit the "Host name" setting in the web console, the http pass to field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

File name or extension

Files/Extensions: (pass_ext, pass_ext_list)

Skips virus scanning for files with the specified file names or extensions.

Usually, all data is saved and transmitted to the client only after virus scanning has completed. This setting specifies that the data in files with the specified file names or extensions is forwarded as soon as it is received.

Separate each name with a comma (",") by using backward matching (a file is skipped if the trailing characters of the file name match the specified file name or extension). The setting is not case sensitive.

The setting does not apply to files in archived files.

The maximum length of the setting is 1999 bytes.

File size

Filesize: (pass_filesize, pass_filesize_len)

Skips virus scanning for file data beyond the specified size.

Usually, all data is saved and transmitted to the client only after the virus scanning has completed. This setting specifies that the data beyond the specified length in a file is forwarded as soon as it is received.



Note that this setting may cause that viruses in large files are not detected.

DNS reverse lookup

DNS Reverse Lookup (reverselookup)

Looks up the DNS entry for the source IP address.

When DNS reverse lookup is enabled, you can use <host name>.<domain name> format to specify the [Access control]=[From these hosts] settings. Also, the host name of the accessing host is shown in the access log.

However, this setting reduces processing speed slightly.

Maximum scanning time

Maximum scanning time (vsd_scantimeout)

Sets a maximum time for scanning files.

If you use zero, scanning time is unlimited.

The default is 90 seconds.



If scanning takes a long time, this setting terminates scanning after the specified time. Note, however, that if you set a shorter scanning time, it limits the extent to which archived and other large files can be scanned.

Scan files that have been sent by POST and PUT methods

Scan sending files by POST/PUT method (virus_check_post)

Performs virus scans when files are sent.

If you disable this setting, the product scans only incoming files. If you enable the setting, the product scans both incoming and outgoing files. The product scans the following files: files contained in data that the POST method sends in multipart/form-data format, and files that the PUT method sends.

All data that the client sends in a POST or PUT operation is temporarily saved and scanned before the client connects to the server to forward the data. As a result, a delay may occur for POST/PUT sending and the speed may be somewhat slower.

The response line "HTTP/1.0 403 Forbidden" is returned if a virus is detected in a PUT operation.

This setting is ignored when virus scanning is disabled. (Virus scanning is not performed even if you enable this setting.)

Edit the virus detection message

Detection message

Edits the message which is shown when a virus is detected.

Enter the message by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

🔄 For information on variables and options, see "[Detection Notification Templates](#)", 67.



▪ If you edit the message from the command line, you need to restart the service afterwards.

Riskware scanning

Scan riskware (riskware_check)

Enables riskware scanning. This detects riskware as well as known viruses.

🔍 For more information about riskware, see “[Riskware](#)”, 119.

Skip these targets

Skip scanning for riskware: (pass_riskware)

Excludes the specified riskware from detection.

Specify the riskware by using the format "Category.Platform.Family". You can use wildcards (*) in the Category, Platform, and Family names. For example, "Client-IRC.*.*" excludes all riskware in the Client-IRC category.

The maximum length of the setting is 1999 bytes.

🔍 Separate each setting in the setup file with a semicolon (";").

Keep-alive connection

Keep-Alive connection (keepalive)

Uses a Keep-Alive connection (persistent connection). In practice, a Keep-Alive connection is only used if both the server and client support Keep-Alive and all the following conditions are met:

- Keep-Alive connection setting is enabled.
- The value of "Connection" in the response header of the HTTP/1.1 response is not "close". "Connection" or "Proxy-Connection" in the HTTP/1.0 response starts with "keep-alive".
- The Content-Length in the response header is 1 or more, and the response code is 304, 204, or 1xx.
- Content-Length does not appear more than once in the request header or response header.
- Not a virus detection response.
- The connection to the server was established successfully and no error occurred.
- Not FTP over HTTP.
- Not the CONNECT method.

Timeout

Timeout (keepalive_timeout)

Specifies a timeout (in seconds) for Keep-Alive connections of 1 second or more. After the HTTP response is complete, the session is disconnected once the specified time elapses.

Leaving a Keep-Alive connection open monopolizes a proxy process. If you increase the timeout value, make sure that there is a sufficient margin in the maximum number of simultaneous connections.

Anonymous proxy

Anonymous Proxy (anonymous)

Disables the sending of information about the proxy or client (Via and X-Forwarded-For headers) to the server.

Transparent proxy

Transparent Proxy mode (transparent)

Enables the transparent proxy mode.

If you use the HTTP proxy in transparent mode, you need to set the NAT redirection. To do this, use one of the following methods:

- Click the “[Edit NAT \(iptables\) redirect settings](#)” to use the "Edit NAT (iptables) redirect settings".

- Use the iptables command from the command line to specify the setting as follows. (The example shows the port number being set to 9800.)

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 9800
```

- ➦ For more information, see “[Transparent Proxy](#)”, 108.

NAT

NAT

Specifies the NAT redirection setting. To redirect all connections for port 80 to the HTTP proxy (port 9080), select the **HTTP redirect** checkbox.

Error message

Error message

Edits the message which is shown when an error occurs.

Enter the message by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

- ➦ For information on variables and options, see “[Detection Notification Templates](#)”, 67.



- If you edit an error message in the web console, the following file is updated:
/opt/f-secure/fsigk/conf/template_http_error.html.
- If you edit the message from the command line, you need to restart the service afterwards.

7.1.1.2 SMTP Proxy

SMTP proxy

SMTP Proxy (smtp_service)

Click the **On** and **Off** buttons to start or stop the SMTP proxy service.

Proxy port

Proxy Port (svcport)

Specifies the port number used by the proxy service. The standard port number is 25.

Usually, you need to specify only the port number. To specify the port number, IP address, and interface name all together, use the following format:

Syntax: [A.A.A.A%EEE:PPP|A.A.A.A:PPP|%EEE:PPP|PPP]

(PPP: Port number, A.A.A.A: Address, EEE: Interface)

Examples: 9025, 10.0.0.2:9025, %eth0:9025, 10.0.0.2%eth0:9025



- You can specify only one inbound port number. To listen for connections on more than one port, use the REDIRECT setting in the iptables function of Linux. For example, to listen for connections on both the standard SMTP port (25) and the submission port (587), set 25 as the inbound port number and use iptables to redirect port 587 to port 25. In this case, use the following command to setup iptables:


```
# iptables -t nat -A PREROUTING -p tcp -dport 587 -j REDIRECT --to-port 25
```

 After specifying the setting, save the iptables configuration:


```
# /etc/init.d/iptables save
```
- Because SSL communications for protocols such as SMTPs (TCP/port number 465) are encrypted, communications cannot be received directly regardless of whether iptables redirection is enabled or not. If necessary, install F-Secure Internet Gatekeeper for Linux so that communications are first decrypted by an SSL proxy, SSL accelerator, or similar. After this, the communications pass through Internet Gateway. Available general-purpose SSL proxies include stunnel and stone.
 - stunnel
 - <http://www.stunnel.org/>
 - <http://www.atmarkit.co.jp/fsecurity/rensai/securitytips/018stunnel.html>
 - stone
 - <http://www.gcd.org/sengoku/stone/Welcome.ja.html>
 - <http://www.gcd.org/sengoku/stone/>

Virus scanning

Do Virus Check (virus_check)

Enables or disables virus scanning.

We recommend that you enable this setting.

When you enable both virus and spam scanning, the virus scan result is handled first.

Global settings

Global Settings

These settings apply to all connections not specified in the LAN settings.

Virus e-mails may use spoofed (fake) sender and recipient addresses. The recommended setting for incoming e-mail is to delete or notify the recipient, and for outgoing mail, to delete or block sending.

Parent server

Parent Server (parent_server_host / parent_server_port)

Specifies the host name and port number of the destination SMTP server.

The standard port number is 25.
This setting is ignored in transparent mode.

What to do when a virus is detected

Action on Viruses (action)

Pass

Pass (action=pass)

Allows e-mail to pass even if a virus is detected.
In this case, the detection is recorded in the log, the administrator is notified, and X-Virus-Status: is added to the header.
This setting is not usually used.

Block

Delete (action=deny)

Blocks sending of infected e-mails.
The SMTP session returns the following error to notify the mailer and mail server directly.
554 Infected by [virus name]

Delete

Delete (action=blackhole)

Deletes infected e-mails. Does not send a detection message.

Notify recipients after deleting the mail

Delete and send to receiver (action=delete)

Deletes the virus and sends a virus detection message to the recipient by e-mail.
This setting is not typically used for outbound e-mails, because the recipient of infected e-mails may be spoofed.



If you choose to notify the recipient, it often means that the notification is sent to an unrelated third party.

Notify the sender by e-mail after deleting the mail

Delete and send back to sender (action=sendback)

Deletes the virus and sends a virus detection message to the sender by e-mail.
This setting is not typically used for inbound e-mails, because the sender of infected e-mails may be spoofed.



If you choose to notify the sender, it often means that the notification is sent to an unrelated third party.

Notify the administrator by e-mail

Notify Admin (notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in [Settings to notify the administrator](#) under "Common settings".

To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification message from being detected as a virus. "Number" is a random number, which is set as admin_notification_id in the settings file during the installation.

Quarantine

Quarantine(keep) (quarantine)

Quarantines viruses. The viruses are quarantined in the directory that you can set in [Quarantine directory](#) under “Common settings”. The viruses are stored in mailbox format.

Specify this setting only if sufficient disk space is available.

Edit the virus detection message

Detection message

Edits the message to be shown when a virus is detected when a file is being sent.

The text up to the first blank line contains the header.

Enter the message (including the Subject) by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

➡ For information on variables and options, see “[Detection Notification Templates](#)”, 67.



- If you edit the message from the command line, you need to restart the service afterwards.
 - If you edit the virus detection message by using the web console, the following file is updated: `/opt/f-secure/fsigk/conf/template_smtp.txt`.

Spam filtering

Do SPAM Check (spam_check)

Enables or disables spam filtering. Specify the spam detection settings in [Spam filtering method](#) under “Common settings”. “X-Spam-Status:” is added to the header if spam is detected.

If you specify RBL or SURBL as the spam filtering method, a delay of up to several hundred milliseconds occurs while waiting for a response from the RBL or SURBL server.

Because the objective is to block incoming spam, enable the [Hosts and networks within LAN](#) setting. It excludes outgoing e-mails from hosts on the LAN from spam checking.

If you enable both virus and spam scanning, the virus scan result is handled first.

Log and notify

Pass (spam_action=pass)

Allows the spam to pass. If an e-mail is classified as spam, “X-Spam-Status:” is added to the header. You can use the sorting function on the client to classify e-mail, in which the value of “X-Spam-Status:” starts with “Yes” as spam. The spam detection is recorded in the log and the administrator is notified.

Modify the message subject

Change subject (spam_action=change_subject, spam_change_subject_prefix)

Modifies the Subject of an e-mail that is classified as spam. If you specify a character string, it is prefixed to the Subject. The maximum number of characters is 99.

We recommend that you specify the text string in English. Although you can specify other languages as well, the text is encoded as UTF-8. Accordingly, if the subject of the incoming e-mail is encoded by using some other character set, the text may not be shown correctly in Outlook and other e-mail clients.

Delete

Delete (spam_action=blackhole)

Deletes spam e-mail. To avoid deleting e-mails that are incorrectly classified as spam, do not delete the e-mails at the gateway. Instead, sort the e-mail at the e-mail client (mailer).

Notify the administrator by e-mail*Notify Admin* (spam_notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in **Settings to notify the administrator** under “Common settings”.

To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification message from being detected as a virus. “Number” is a random number, which is set as `admin_notification_id` in the settings file during the installation.

Quarantine*Quarantine(keep)* (spam_quarantine)

Quarantines spam. Specify the directory, in which the viruses are quarantined, in **Quarantine directory** under “Common settings”. The spam is stored in mailbox format. Specify this setting only if sufficient disk space is available.

Restrict e-mail recipients*Restrict RCPT domains* (acl_rcpt)

Specifies a list of recipient domains. If a domain is not on this list, the e-mail that is sent to this domain is blocked.

The text after the first "@" character in the e-mail address is treated as the domain name. If you enable this setting, the addresses containing "!" and "%" are also blocked. E-mail addresses without a domain name are not blocked.

Even if you have enabled **SMTP authentication** or **POP-before-SMTP authentication**, e-mail to the specified domains can be sent without authentication.

🔗 For examples, see “[Access Control](#)”, 65.



Note

If you edit the [Restrict e-mail recipients] setting by using the web console, the `smtp rcpt` setting is updated in `/opt/f-secure/fsigk/conf/hosts.allow`.

SMTP authentication*SMTP authentication* (proxymail_auth)

Performs proxy authentication independently for each user.

If you have enabled also the **POP-before-SMTP authentication** setting, the e-mail is sent if either SMTP authentication or POP-before-SMTP authentication is successful.

If you have enabled also the **Restrict e-mail recipients** setting, e-mail to the specified domains can be sent even without authentication.

Authentication is performed using PAMs (Pluggable Authentication Modules). You can change the authentication method in the `/etc/pam.d/fsigk_smtp` file.

🔗 For more information, see “[Proxy authentication using Internet Gatekeeper](#)”, 102.

Add or remove users*User DB*

Edits the database of users who are permitted to connect. You can add, delete or modify users and passwords.

POP-before-SMTP authentication*POP-before-SMTP Authentication* (pbs)

Enables POP-before-SMTP authentication. If the SMTP proxy performs POP-before-SMTP authentication, run this together with the POP proxy. Client hosts (IP addresses) that are

authenticated through the POP proxy are permitted to use the SMTP proxy for a fixed time period.

If you use SMTP authentication simultaneously on the Internet Gatekeeper and mail server, e-mail can be sent if either SMTP authentication or POP-before-SMTP authentication is successful.

If you have enabled also the **Restrict e-mail recipients** setting, e-mail to the specified domains can be sent even without authentication.

➡ For examples, see “*Access Control*”, 65.

Timeout

Expire (pbs_lifetime)

How long POP-before-SMTP authentication remains valid (minutes).

LAN access settings

LAN Access settings (lan)

With these settings, you can specify different operation for connections from specific hosts and networks.

Hosts and networks within LAN

LAN hosts

Specifies the list of hosts and networks to which the **LAN access settings** apply.

If you have enabled **DNS Reverse Lookup**, you can also specify <host name>.<domain name>.

➡ For examples, see “*Access Control*”, 65.



If you edit the **Hosts and networks within LAN** setting by using the web console, the smtp lan field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

Parent server

Parent Server (lan_parent_server, lan_parent_server_host, lan_parent_server_port)

Specifies another SMTP server. Specify this setting if you want to use a different SMTP server than the one you specified in “Parent server”. This SMTP server is used for connections from the hosts that you specified in **Hosts and networks within LAN**.

The standard port number is 25.

What to do when a virus is detected

Action on Viruses (action)

Virus e-mails often use spoofed (fake) sender and recipient addresses. The recommended setting for incoming e-mail is to delete or notify the recipient, and for outgoing mail, to delete or block sending.

Log and notify

Pass (action=pass)

Allows e-mail to pass even if a virus is detected.

In this case, the detection is recorded in the log, the administrator is notified, and

X-Virus-Status: is added to the header.

This setting is not usually used.

Block and notify the sender

Delete (action=deny)

Blocks the sending of infected e-mails.

The SMTP session returns the following error to notify the mailer and mail server directly:

554 Infected by [virus name]

Delete

Delete (action=blackhole)

Deletes infected e-mails. Does not send a detection message.

Delete and notify recipients

Delete and send to receiver (action=delete)

Deletes the virus and sends a virus detection message to the recipient by e-mail.

This setting is not typically used for outbound e-mails, because the recipients of infected e-mails may be spoofed.



If you choose to notify the recipient of an infected outbound e-mail, it often means that a notification e-mail is sent to an unrelated third party.

Delete and notify the sender

Delete and send back to sender (action=sendback)

Deletes the virus and sends a virus detection message to the sender by e-mail.

This setting is not typically used for inbound e-mail, because the sender of infected e-mails may be spoofed.



If you choose to notify the sender of an infected inbound e-mail, it often means that a notification e-mail is sent to an unrelated third party.

Notify the administrator by e-mail

Notify Admin (notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in [Settings to notify the administrator](#) under “Common settings”.

To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification from being detected as a virus. “Number” is a random number, which is set as `admin_notification_id` in the settings file during the installation.

Quarantine

Quarantine(keep) (quarantine)

Quarantines viruses. The viruses are quarantined in the directory that you can set in [Quarantine directory](#) under “Common settings”. The viruses are stored in mailbox format.

Specify this setting only if sufficient disk space is available.

Edit the virus detection message

Detection message

Edits the message which is shown when a virus is detected in an outgoing file.

The text up to the first blank line contains the header.

Specify the message (including the Subject) by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

➔ For information on variables and options, see “[Detection Notification Templates](#)”, 67.



- If you edit the message from the command line, you need to restart the service afterwards.

- If you edit the **Detection message** setting by using the web console, the following file is updated:
/opt/f-secure/fsigk/conf/template_smtp_lan.txt.

Maximum number of simultaneous connections

Maximum connections (pre_spawn)

Specifies the maximum number of simultaneous connections from clients. The specified number of processes listens for connections from clients.

You can check the number of connections used in “Internal process ID” in the access log (access.log).



Note

- If you increase the value of this setting, the number of simultaneous connections is increased, but it requires more memory. Approximately 500 KB of memory is used per process.
- A warning is output to the error log if the maximum number of connections is reached.
- We recommend that you set an initial value of approximately 50 and then monitor the performance. The setting is usually set to a value of less than 200. (The setting itself permits values up to 9999.)

Access control

Access Control

From these hosts

From: (acl_from)

Only accepts connections from the designated list of hosts.

If you have enabled **DNS Reverse Lookup**, you can also specify <host name>.<domain name>.

🔗 For examples, see “[Access Control](#)”, 65.



Note

If you edit the **From these hosts** setting by using the web console, the smtp from field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

To these hosts

To: (acl_to)

Only accepts connections to the designated list of hosts.

🔗 For examples, see “[Access Control](#)”, 65.



Note

If you edit the **To these hosts** setting by using the web console, the smtp to field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

DNS reverse lookup

DNS Reverse Lookup (reverselookup)

Looks up the DNS entry for the source IP address.

If you enable DNS reverse lookup, you can use <host name>.<domain name> format to specify the [Access control]=[From] and [Hosts and networks within LAN] settings. Also, the host name of the accessing host is shown in the access log.

However, this setting reduces processing speed slightly.

Blocked e-mail content

Block for:

ActiveX

ActiveX (block_activex)

Blocks HTML e-mail with embedded ActiveX content.

The detection name is "FSIGK/POLICY_BLOCK_ACTIVEX".

When ActiveX content is detected, it is handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting. If you disable virus scanning, ActiveX content scanning is also disabled.

Scripts

Script (block_script)

Blocks HTML e-mail that contains scripts (JavaScript, VBScript, etc.).

The detection name is "FSIGK/POLICY_BLOCK_SCRIPT".

When scripts are detected, they are handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting. If you disable virus scanning, script scanning is also disabled.

Partial messages

Partial messages (block_partial_message)

Blocks divided e-mail messages. This blocks e-mail with a Content-Type field value of message/partial in the e-mail header.

The detection name is "FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE".

When a partial message is detected, it is handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting.

Encrypted and archived files

Encrypted files (block_encrypted)

Blocks mail that contains encrypted and archived files (ZIP, RAR).

The detection name is "FSIGK/POLICY_BLOCK_ENCRYPTED".

When an encrypted and archived file is detected, it is handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting. If you disable virus scanning, the scanning for encrypted and archived files is also disabled.

File name or extension

Files/extensions (block_ext,block_ext_list)

Blocks e-mail with the specified file names or extensions.

Separate each name with a comma (",") by using backward matching (a file is blocked if the trailing characters of the file name match the specified file name or extension). The setting is not case sensitive.

If you specify "ALL", all e-mails with attached files are blocked.

The setting does not apply to files contained in archived files.

The maximum length of the setting is 1999 bytes.

When a specified file name or extension is detected, it is handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting.

The detection name is "FSIGK/POLICY_BLOCK_EXT".

Example setting: .COM,.PIF,.EXE,.BAT

Exclude these targets from the virus scan

Skip scanning for:

File name or extension

Files/Extensions: (pass_ext, pass_ext_list)

Skips virus scanning for files with the specified file names or extensions.

Separate each name with a comma (",") by using backward matching (a file is skipped if the trailing characters of the file name match the specified file name or extension). The setting is not case sensitive.

The setting does not apply to files contained in archived files.

The maximum length of the setting is 1999 bytes.

Maximum scanning time

Maximum scanning time (vsd_scantimeout)

Sets a maximum time for scanning files.

If you set the value as zero, the scanning time is unlimited.

The default is 90 seconds.



If scanning takes a long time, this setting terminates the scanning after the specified time. Note, however, that if you set a shorter scanning time, it limits the extent to which archived and other large files can be scanned.

Riskware scanning

Scan riskware (riskware_check)

Enables riskware scanning. This detects riskware as well as known viruses.

➡ For more information about riskware, see "[Riskware](#)", 168.

Skip these targets

Skip scanning for riskware: (pass_riskware)

Excludes the specified riskware from detection.

Specify riskware by using the format "Category.Platform.Family". You can use wildcards (*) in the Category, Platform, and Family names. For example, "Client-IRC.*.*" excludes all riskware in the Client-IRC category.

The maximum length of the setting is 1999 bytes.

➡ Separate each setting in the setup file with a semicolon (;).

Scan the e-mail message body

Scan text body part (virus_check_text)

Scans the body of e-mail messages. However, attached text-format files and HTML-format e-mail body text are scanned regardless of this setting.

If you enable this setting, harmless remains of viruses may also be detected. The operating speed may also be slightly reduced.

Because the text-format e-mail body is not executed, you do not usually need to enable this setting.

Scan the whole HTML content in the e-mail

Scan whole html part (virus_check_wholehtml)

Scans those parts of the HTML content of an e-mail that probably do not execute viruses (unlike parts such as ActiveX and scripts).

If you enable this setting, some suspicious e-mail can also be detected (in addition to viruses).

The suspicious e-mail can be, for example, phishing e-mails or virus fragments. Enabling the setting also reduces the operating speed slightly. Because viruses contained in HTML are detected regardless of this setting, you do not usually need to enable this setting.

Anonymous proxy

Anonymous Proxy (anonymous)

Do not add header information (Received header) in the proxy.

Transparent proxy

Transparent Proxy mode (transparent)

Enables transparent proxy mode.

A NAT redirection setting is required when the proxy operates as a transparent proxy. Use one of the following methods to specify the NAT redirection setting:

- Use the "Edit NAT (iptables) redirect settings". To do this, click [Edit NAT \(iptables\) redirect settings](#).
- Use the iptables command from the command line to specify the setting as follows. (The example shows the port number being set to 9025.)

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 25 \
-j REDIRECT --to-port 9025
```

🔍 For more information, see "[Transparent Proxy](#)", 108.

Edit NAT (iptables) redirect settings

NAT

Specifies the NAT redirection settings. If you select the **SMTP redirect** checkbox, all connections for port 25 are redirected to the SMTP proxy (port 9025).

7.1.1.3 POP Proxy

POP Proxy

POP Proxy (pop_service)

Click the **On** and **Off** buttons to start or stop the POP proxy service.

Proxy port

Proxy Port (svcport)

Specifies the port number that the proxy service uses. The standard port number is 110.

Usually, you need to specify only the port number. To specify the port number, IP address, and interface name all together, use the following format:

Syntax: [A.A.A.A%EEE:PPP|A.A.A.A:PPP|%EEE:PPP|PPP]

(PPP: Port number, A.A.A.A: Address, EEE: Interface)

Examples: 9110,10.0.0.2:9110, %eth0:9110, 10.0.0.2%eth0:9110



Note

- You can specify only one inbound port number. To listen for connections on more than one port, use the REDIRECT setting in the iptables function of Linux. For example, to listen for connections on both the standard POP port (110) and 12345, set 110 as the inbound port number and use iptables to redirect port 12345 to port 110. In this case, use the following command to setup iptables:


```
# iptables -t nat -A PREROUTING -p tcp -dport 12345 -j REDIRECT -to-port 110
```

 After specifying the setting, save the iptables configuration:


```
# /etc/init.d/iptables save
```
- Because SSL communications for protocols such as POPs (TCP/port number 995) are encrypted, communications cannot be received directly regardless of whether iptables redirection is enabled or not. If necessary, install F-Secure Internet Gatekeeper for Linux so that communications are first decrypted by an SSL proxy, SSL accelerator, or similar. After this, the communications pass through the gateway. Available general-purpose SSL proxies include stunnel and stone.
 - stunnel
 - <http://www.stunnel.org/>
 - <http://www.atmarkit.co.jp/fsecurity/rensai/securitytips/018stunnel.html>
 - stone
 - <http://www.gcd.org/sengoku/stone/Welcome.ja.html>
 - <http://www.gcd.org/sengoku/stone/>

Parent server

Parent Server (parent_server_host / parent_server_port)

Specifies the host name and port number of the destination POP server.

The standard port number is 110.

This setting is ignored in transparent mode.

Virus scanning

Do Virus Check (virus_check)

Enables or disables virus scanning.

We recommend that you enable this setting.

When you enable both virus and spam scanning, the virus scan result is handled first.

What to do when a virus is detected

Action on Viruses

Delete

Delete (action={pass,delete})

Deletes viruses.

The e-mail that contains the virus is replaced with the information specified in the virus detection message.

The detection event is recorded in the log, a notification is sent to the administrator, and X-Virus-Status: is added to the header even if the virus is not deleted.

We recommend that you enable this setting.



It is not possible to delete the e-mail completely or block it from being delivered to the user. The reason for this is the POP protocol specifications.

Notify the administrator by e-mail*Notify Admin* (notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in [Settings to notify the administrator](#) under “Common settings”.

To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification from being detected as a virus. “Number” is a random number, which is set as admin_notification_id in the settings file during the installation.

Quarantine*Quarantine(keep)* (quarantine)

Quarantines e-mails that contain viruses. The viruses are quarantined in the directory that you can set in [Quarantine directory](#) under “Common settings”.

Specify this setting only if sufficient disk space is available.



Even if you enable this setting, it is not possible to delete the e-mail completely or block it from being delivered to the user. The reason for this is the POP protocol specifications.

Edit the virus detection message*Detection message*

Edits the message which is shown if a virus is detected when sending a file.

The text up to the first blank line contains the header.

Specify the message (including the Subject) by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

🔄 For information on variables and options, see “[Detection Notification Templates](#)”, 67.



- If you edit the message from the command line, you need to restart the service afterwards.
- If you edit the Detection message by using the web console, the following file is updated: /opt/f-secure/fsigk/conf/template_pop.txt.

Spam filtering*Do SPAM Check* (spam_check)

Enables or disables spam filtering. Specify the spam detection settings in [Spam filtering method](#) under “Common settings”. "X-Spam-Status:" is added to the header if spam is detected. When RBL or SURBL is used as the spam filtering method, a delay of up to several hundred milliseconds occurs while waiting for a response from the RBL or SURBL server. When you enable both virus and spam scanning, the virus scan result is handled first.

Pass*Pass* (spam_action=pass)

Allows the spam to pass. "X-Spam-Status:" is added to the header of e-mail that is classified as spam. You can use the sorting function on the client to classify e-mail in which the value of "X-Spam-Status:" starts with "Yes" as spam. The spam detection is recorded in the log and the administrator is notified.

Change subject

Change subject (spam_action=change_subject, spam_change_subject_prefix)

Modifies the Subject of an e-mail that is classified as spam. If you specify a character string, it is prefixed to the Subject. The maximum number of characters is 99.

We recommend that you specify the text string in English.

Although you can use other languages as well, the text is encoded as UTF-8. Accordingly, if the subject of the incoming e-mail is encoded by using, for example, ISO-2022-JP, the text may not be shown correctly in Outlook or other e-mail clients.

Notify the administrator by e-mail

Notify Admin (spam_notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in [Settings to notify the administrator](#) under "Common settings".

To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification from being detected as a virus.

"Number" is a random number, which is set as admin_notification_id in the settings file during the installation.

Quarantine

Quarantine(keep) (spam_quarantine)

Quarantines spam. The spam is quarantined in the directory that you set in [Quarantine directory](#) under "Common settings".

Specify this setting only if sufficient disk space is available.



Even if you enable this setting, it is not possible to delete the e-mail completely or block it from being delivered to the user. The reason for this is the POP protocol specifications.

Defining parent server by user

User Selective Parent (self_proxy)

Allows the client to select the POP server.

The user can specify the POP server by specifying their mailer user name in the format <user name>@<POP server name> (or <user name>#<POP server name>).

POP user restriction

PAM-based Account verification (proxyauth_pam_account)

Restricts which users can connect.

Authentication is performed using PAMs (Pluggable Authentication Modules). You can change the authentication method in the /etc/pam.d/fsigk_pop file.

🔗 For more information, see "[Proxy authentication using Internet Gatekeeper](#)", 102.

Add or remove users

User DB

Edits the database of users who are permitted to connect. You can add, delete, and modify users. The POP service uses the user database only to check user names. Because password authentication is performed by the POP server, the password in the user database is not used.

Maximum number of simultaneous connections

Maximum connections (pre_spawn)

Specifies the maximum number of simultaneous connections from clients. The specified number of processes listen for connections from clients.

You can check the number of connections used in "Internal process ID" in the access log (access.log).



- If you increase the value of this setting, the number of simultaneous connections is increased, but it requires more memory. Approximately 500 KB of memory is used per process.
- A warning is output to the error log if the maximum number of connections is reached.
- We recommend that you set an initial value of approximately 50 and then monitor the performance. The setting is usually set to a value of less than 200. (The setting itself permits values up to 9999.)

Access control

Access Control

From

From: (acl_from)

Only accepts connections from the designated list of hosts.

If you have enabled [DNS Reverse Lookup](#), you can also specify <host name>.<domain name>.

➡ For examples, see "[Access Control](#)", 65.



If you edit the [From these hosts] setting by using the web console, the pop from field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

To

To: (acl_to)

Only accepts connections to the designated list of hosts.

➡ For examples, see "[Access Control](#)", 65.



If you edit the [To these hosts] setting by using the web console, the pop to field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

DNS reverse lookup

DNS Reverse Lookup (reverselookup)

Looks up the DNS entry for the source IP address.

When you enable DNS reverse lookup, you can use <host name>.<domain name> format to specify the [Access control]=[From these hosts] settings. The host name of the accessing host is also shown in the access log.

However, this setting reduces processing speed slightly.

Blocked e-mail content

Block for:

ActiveX

ActiveX (block_activex)

Blocks HTML e-mail with embedded ActiveX content.

The detection name is "FSIGK/POLICY_BLOCK_ACTIVEX".

When ActiveX content is detected, it is handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting. If you disable virus scanning, ActiveX content scanning is also disabled.

Scripts

Script (block_script)

Blocks HTML e-mail that contains scripts (JavaScript, VBScript, etc.).

The detection name is "FSIGK/POLICY_BLOCK_SCRIPT".

When scripts are detected, they are handled in the same way as viruses. For more information, see the [What to do when a virus is detected](#) setting. If you disable virus scanning, script scanning is also disabled.

Partial messages

Partial messages (block_partial_message)

Blocks divided e-mail messages. This blocks e-mail with a Content-Type field value of message/partial in the e-mail header.

The detection name is "FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE".

When a partial message is detected, it is handled in the same as viruses. For more information, see the [What to do when a virus is detected](#) setting.

Encrypted archive files

Encrypted files (block_encrypted)

Blocks mail containing encrypted and archived files (ZIP, RAR).

The detection name is "FSIGK/POLICY_BLOCK_ENCRYPTED".

When an encrypted and archived file is detected, it is handled in the same as viruses. For more information, see the [What to do when a virus is detected](#) setting. If you disable virus scanning, the scanning for encrypted and archived files is also disabled.

File name or extension

Files/extensions (block_ext,block_ext_list)

Blocks e-mail with the specified file names or extensions.

Separate each name with a comma (",") by using backward matching (a file is blocked if the trailing characters of the file name match the specified file name or extension). The setting is not case sensitive.

If you specify "ALL", all e-mails with attached files are blocked.

The setting does not apply to files contained in archived files.

The maximum length of the setting is 1999 bytes.

The detection name is "FSIGK/POLICY_BLOCK_EXT".

When a specified file name or extension is detected, it is handled in the same as viruses.

For more information, see the [What to do when a virus is detected](#) setting.

Example setting: .COM,.PIF,.EXE,.BAT

Exclude these targets from the virus scan

Skip scanning for:

File name or extension

Files/Extensions: (pass_ext, pass_ext_list)

Skips virus scanning for files with the specified file names or extensions.

Separate each name with a comma (",") by using backward matching (a file is skipped if the trailing characters of the file name match the specified file name or extension). The setting is not case sensitive.

The setting does not apply to files contained in archived files.

The maximum length of the setting is 1999 bytes.

Maximum scanning time

Maximum scanning time (vsd_scantimeout)

Sets a maximum time for scanning files. If scanning takes a long time, this setting terminates scanning after the specified time. Note, however, that if you set a shorter scanning time, it limits the extent to which archived and other large files can be scanned. If you set the value as zero, the scanning time is unlimited. The default is 90 seconds.

Riskware scanning

Scan riskware (riskware_check)

Enables riskware scanning. This detects riskware as well as known viruses.

🔗 For more information about riskware, see "[Riskware](#)", 168.

Skip these targets

Skip scanning for riskware: (pass_riskware)

Excludes the specified riskware from detection.

Specify riskware by using the format "Category.Platform.Family". You can use wildcards (*) in the Category, Platform, and Family names. For example, "Client-IRC.*.*" excludes all riskware in the Client-IRC category.

The maximum length of the setting is 1999 bytes.

🔗 Separate each setting in the setup file with a semicolon (";").

Scan the e-mail message body

Scan text body part (virus_check_text)

Scans the body of e-mail messages. However, attached text-format files and HTML-format e-mail body text are scanned regardless of this setting. If you enable this setting, it reduces the operating speed slightly.

Because the text-format e-mail body is not executed, usually you do not need to enable this setting.

Scan the whole HTML content in the e-mail

Scan whole html part (virus_check_wholehtml)

Scans those parts of the HTML content of an e-mail that probably do not execute viruses (unlike parts such as ActiveX and scripts).

If you enable this setting, some suspicious e-mail can also be detected (in addition to viruses).

The suspicious e-mail can be, for example, phishing e-mails or virus fragments. Enabling the setting also reduces the operating speed slightly. Because viruses contained in HTML are detected regardless of this setting, you do not usually need to enable this setting.

Transparent proxy

Transparent Proxy mode (transparent)

Enables the transparent proxy mode.

A NAT redirection setting is required when the proxy operates as a transparent proxy. Use one of the following methods to specify the NAT redirection setting:

- Use the "Edit NAT (iptables) redirect settings". To do this, click [Edit NAT \(iptables\) redirect settings](#).
- Use the iptables command from the command line to specify the setting as follows. (The example shows the port number being set to 9110.)

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 110 -j REDIRECT --to-port 9110
```

- For more information, see "[Transparent Proxy](#)", 108.

Edit NAT (iptables) redirect settings

NAT

Specifies the NAT redirection settings. If you select the **POP redirect** checkbox, all connections for port 110 are redirected to the POP proxy (port 9110).

7.1.1.4 FTP Proxy

FTP proxy

FTP Proxy (ftp_service)

Click the **On** and **Off** buttons to start or stop the FTP proxy service.

Proxy port

Proxy Port (svcport)

Specifies the port number that is used by the proxy service. The standard port number is 21. Usually, you need to specify only the port number.

To specify the port number, IP address, and interface name all together, use the following format:

Syntax: [A.A.A.A%EEE:PPP|A.A.A.A:PPP|%EEE:PPP|PPP]

(PPP: Port number, A.A.A.A: Address, EEE: Interface)

Examples: 9021, 10.0.0.2:9021, %eth0:9021, 10.0.0.2%eth0:9021



- You can specify only one inbound port number. To listen for connections on more than one port, use the REDIRECT setting in the iptables function of Linux. For example, to listen for connections on both 21 and 12345, set 21 as the inbound port number and use iptables to redirect port 12345 to port 21. In this case, use the following command to set up iptables:

```
# iptables -t nat -A PREROUTING -p tcp -dport 12345 -j REDIRECT --to-port 21
```

After specifying the setting, save the iptables configuration:

```
# /etc/init.d/iptables save
```

Parent server

Parent Server (parent_server_host / parent_server_port)

Specifies the host name and port number of the destination FTP server.

The standard port number is 21.

This setting is ignored in transparent mode.

Virus scanning

Do Virus Check (virus_check)

Enables or disables virus scanning.

We recommend that you enable this setting.

What to do when a virus is detected

Action on Viruses

Delete

Delete (action={pass,delete})

Deletes viruses. The detection event is recorded in the log and a notification is sent to the administrator even if the virus is not deleted.

We recommend that you enable this setting.

Notify the administrator by e-mail

Notify Admin (notify_admin)

Sends a notification to the administrator by e-mail. Specify the e-mail address, mail server, and detection message in **Settings to notify the administrator** under "Common settings".

To separate notifications from standard e-mails, "X-Admin-Notification-Id: [number]" is added to the header. This also prevents the notification from being detected as a virus.

"Number" is a random number, which is set as admin_notification_id in the settings file during the installation.

Quarantine*Quarantine(keep)* (quarantine)

Quarantines viruses. The viruses are quarantined in the directory that you can set in

Quarantine directory under “Common settings”.

Specify this setting only if sufficient disk space is available.

Defining parent server by user*User Selective Parent* (self_proxy)

Allows the client to select the FTP server.

The user can specify the FTP server from the FTP client by specifying their user name in the format <user name>@<FTP server name> (or <user name>#<FTP server name>).

FTP user restriction*PAM-based Account verification* (proxyauth_pam_account)

Restricts which users can connect.

Authentication is performed using PAMs (Pluggable Authentication Modules). You can change the authentication method in the /etc/pam.d/fsigk_ftp file.

🔗 For more information, see " *Proxy authentication using Internet Gatekeeper*", 102.

Add or remove users*User DB*

Edits the database of users who are permitted to connect. You can add, delete, and modify users. The FTP service uses the user database only to check user names. Because the FTP server performs password authentication, the password in the user database is not used.

Maximum number of simultaneous connections*Maximum connections* (pre_spawn)

Specifies the maximum number of simultaneous connections from clients. The specified number of processes listen for connections from clients.

You can check the number of connections used in “Internal process ID” in the access log (access.log).



- If you increase the value of this setting, the number of simultaneous connections is increased, but it requires more memory. Approximately 500 KB of memory is used per process.
- A warning is output to the error log if the maximum number of connections is reached.
- We recommend that you set an initial value of approximately 10 and then monitor the performance. The setting is usually set to a value of less than 50. (The setting itself permits values up to 9999.)

Access control*Access Control***From these hosts***From:* (acl_from)

Only accepts connections from the designated list of hosts.

If you have enabled **DNS Reverse Lookup**, you can also specify <host name>.<domain name>.

🔗 For examples, see “*Access Control*”, 65.



If you edit the **From these hosts** setting by using the web console, the ftp from field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

To these hosts

To: (acl_to)

Only accepts connections to the designated list of hosts.

🔗 For examples, see “[Access Control](#)”, 65.



If you edit the **To these hosts** setting by using the web console, the ftp to field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

DNS reverse lookup

DNS Reverse Lookup (reverselookup)

Looks up the DNS entry for the source IP address.

When you enable DNS reverse lookup, you can use <host name>.<domain name> format to specify the [Access control]=[From these hosts] settings. The host name of the accessing host is also shown in the access log.

However, this setting reduces the processing speed of the system slightly.

Exclude these targets from the virus scan

Skip scanning for:

Host name

Hosts: (acl_pass_to)

Skips virus scanning for connections to the specified hosts.

Usually, all data is saved and transmitted to the client only after the virus scanning has completed. If you enable this setting, the data for connections to the specified hosts is forwarded as soon as it is received.

🔗 For examples, see “[Access Control](#)”, 65.



If you edit the **Host name** setting by using the web console, the ftp pass to field is updated in /opt/f-secure/fsigk/conf/hosts.allow.

File name or extension

Files/Extensions: (pass_ext, pass_ext_list)

Skips virus scanning for files with the specified file names or extensions.

Separate each name with a comma (",") by using backward matching (a file is skipped if the trailing characters of the file name match the specified file name or extension). The setting is not case sensitive.

The setting does not apply to files contained in archived files.

The maximum length of the setting is 1999 bytes.

File size

Filesize: (pass_filesize, pass_filesize_len)

Skips virus scanning for file data beyond the specified size.

Usually, all data is saved and transmitted to the client only after the virus scanning has completed. If you enable this setting, the data beyond the specified length in a file is forwarded as soon as it is received.



Note that this setting may cause that viruses contained in large files are not detected.

Maximum scanning time

Maximum scanning time (vsd_scantimeout)

Sets a maximum time for scanning files.

If you set the value as zero, the scanning time is unlimited.

The default is 90 seconds.



If scanning takes a long time, this setting terminates scanning after the specified time. Note, however, that if you set a shorter scanning time, it limits the extent to which archived and other large files can be scanned.

Riskware scanning

Scan riskware (riskware_check)

Enables riskware scanning. This detects riskware as well as known viruses.

- 🔗 For more information about riskware, see “[Riskware](#)”, 168.

Skip these targets

Skip scanning for riskware: (pass_riskware)

Excludes the specified riskware from detection.

You can specify riskware by using the format "Category.Platform.Family". You can use wildcards (*) in the Category, Platform, and Family names. For example, "Client-IRC.*.*" excludes all riskware in the Client-IRC category.

The maximum length of the setting is 1999 bytes.

- 🔗 Separate each setting in the setup file with a semicolon (";").

Transparent proxy

Transparent Proxy mode (transparent)

Enables the transparent proxy mode.

A NAT redirection setting is required when the proxy operates as a transparent proxy. Use one of the following methods to specify the NAT redirection setting:

- Use the "Edit NAT (iptables) redirect settings". To do this, click [Edit NAT \(iptables\) redirect settings](#).
- Use the iptables command from the command line to specify the setting as follows. (The example shows the port number being set to 9021.)

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 21 \
-j REDIRECT --to-port 9021
```

- 🔗 For more information, see “[Transparent Proxy](#)”, 108.

Edit NAT (iptables) redirect settings

NAT

Specifies the NAT redirection settings. If you select the [FTP redirect] checkbox, all connections for port 21 are redirected to the FTP proxy (port 9021).

7.1.1.5 Common Settings

Common settings

Common Settings

Admin notification settings

Admin notification settings

E-mail address

E-mail address (admin_mailaddr)

Specifies the administrator's e-mail address.

If you have enabled the **Notify the administrator by e-mail** option in the **What to do when a virus is detected** setting for a service, virus detection notifications are sent to this address. This address is also used in SMTP scanning as the sender address in notification e-mails sent back to senders.

You can specify multiple addresses, separated by commas (","). In this case, the first address in the list is used as the sender address.

The maximum length of the setting is 1999 bytes.

SMTP server

SMTP server (admin_mx_host/admin_mx_port)

Specifies the mail server which is used to send virus detection notifications to the administrator. The standard port number is 25.

Edit the notification message

Detection message

Edits the message which is shown when a virus is detected in a file being sent.

The text up to the first blank line contains the header.

Enter the message (including the Subject) by using the UTF-8 character set. The maximum length of the message is 9000 bytes.

🔗 For information on variables and options, see "[Detection Notification Templates](#)", 67.



- If you edit the message from the command line, you need to restart the service afterwards.
- If you edit [Detection message] by using the web console, the following file is updated: `/opt/f-secure/fsigk/conf/template_admin.txt`.

Temporary directory

Temporary directory (tmpdir)

Specifies the work directory. The directory is used for temporarily storing files that are being scanned for viruses.

The default is `/var/tmp/fsigk`.

Quarantine directory

Quarantine directory (quarantine_dir)

Specifies the directory for storing detected viruses. The directory is used, if you have enabled the **Quarantine** option for a service. Enable this setting only if sufficient disk space is available.

The default is `/var/tmp/quarantine`.

Spam filtering method

SPAM detection method

Specifies the spam filtering method. The line "X-Spam-Status: Yes(<product name>) with [<detection name>]" is added to the e-mail header if the mail is classified as spam.

If an e-mail matches multiple conditions, scanning is performed in the sequence: custom rules, spam detection engine, RBL, SURBL.

Custom filtering rules

Custom filtering rules

Specifies individual rules for identifying spam.

The detection name for the custom rules is "FSIGK/SPAM_LIST/CUSTOM/(rule number)/(detected header field name)".

You can specify up to 100 custom rules. You can also specify multiple character strings to scan for in each rule.

If you have enabled [Custom filtering rules](#), the line "CUSTOM <tab>custom.txt" is added to /opt/f-secure/fsigk/conf/spam/files.txt.

Edit the custom filtering rules

Edit the custom filtering rules

Use [Edit the custom filtering rules](#) to edit the list of spam filtering rules. An e-mail is classified as spam if it matches any of the specified conditions. Because the custom rules are applied first, before other filtering methods, the rules can be used as a black list and white list.

The list of rules is checked starting from the top. The different conditions that can be specified are described below. Please restart the service from the proxy's web console screen after editing these settings.

Field name

Specifies where to apply the rule. The available settings are described below.

- **Designated header field**
Applies the rule to specific header fields. If the field you want to specify is not in the list, select (Other...) and enter the field name in the "Other" field. You can enter up to 29 characters. The field name is not case sensitive.
- **File name**
Applies the rule to the name of attached files.
- **File size**
Applies the rule to the size of attached files. The condition is specified as a number of bytes. This performs a character string comparison. It does not test whether the numerical value is larger or smaller.
- **Text body**
Applies the rule to character strings in the e-mail's text body.
- **HTML body**
Applies the rule to character strings in the e-mail's HTML body. Carriage returns are treated as space characters.
- **Linked host**
Applies the rule to the host name part of the URLs contained in the e-mail.
- **Relay address**
Applies the rule to the IP addresses in the Received field. In SMTP scanning, the rule is applied also to the source IP address.

- **Always**
Always treat as spam or not spam.

Search string

Scanning searches for the specified character string in the part specified by the field name. You can specify multiple character strings to scan for, separated by commas (",").

You can use languages other than English (UTF-8). Enter difficult characters that in hexadecimal by using the format "%xFF". The "%" character itself is specified as "%%".



Caution

When you specify e-mail addresses, do not use forward or backward matching. If you use them, the e-mail address is not recognized correctly. This is because the From, To, and other headers contain additional characters before and after the e-mail address (example: "Xxx Yyy <aaa@example.com>").



Caution

If you use other language than English (for example, Japanese), the comparison is performed by using the UTF-8 codes. The Subject field and filename are converted to UTF-8 before being compared. The conversion is done for "encoded-word ("=?" charset "?" encoding "?" encoded-text "=?)" written in RFC-2047. To scan for character sets other than UTF-8 (such as Shift-JIS or Unicode), specify the codes as hexadecimal values.

For example, specify the following to search for the text "完全無料" in Shift-JIS format:

```
¥x8a¥xae¥x91¥x53¥x96¥xb3¥x97¥xbf
```

You can use utilities such as the following to perform the kanji code conversion.

Linux:

Use the iconv command as follows:

```
# echo -n '<search character string>' | iconv -f <character set currently used in Linux> -t <character set into which to convert> | od -t x 1
```

Example:

```
# echo -n '完全無料' | iconv -f EUC-JP -t SJIS | od -t x1
0000000 8a ae 91 53 96 b3 97 bf
0000010
```

* Insert "%x" in front of each hexadecimal value.

(Example: ¥x8a¥xae¥x91¥x53¥x96¥xb3¥x97¥xbf)

Windows:

Use a utility program such as the following:

StrHex(<http://www.pleasuresky.co.jp/strhex.php3>)

Comparison method

Specifies how to compare text.

Case sensitive

Distinguish between upper and lower case characters when comparing.

Prefix search

Compare whether the leading characters of the specified field match the character string.

In the text body, this checks whether the character string matches the leading characters of each line. Prefix search cannot be used for the HTML body.

Backward search

Compare whether the trailing characters of the specified field match the character string.

In the text body, this checks whether the character string matches the trailing characters of each line. Backward matching cannot be used for the HTML body.

Not

The rule is satisfied if there is no match with the specified character string.

“AND” with previous rule

The rule is satisfied if both the specified rule and the previous rule are satisfied. In this case, the previous rule is typically set to "no action".

“AND” with previous rule in the same MIME part

The rule is satisfied if both the specified rule and the previous rule are satisfied for the same MIME part. You can use this to specify a rule for both the Content-Type and file name of an attached file, for example.

In this case, the previous rule is typically set to "no action".



When you specify e-mail addresses, do not use forward or backward matching. If you use, the e-mail address is not recognized correctly. This is because the From, To, and other headers contain additional characters before and after the e-mail address (example: "Xxx Yyy <aaa@example.com>").

Filter as

Specifies the judgment result if the specified rule is satisfied. Select one of "spam", "not spam", or "no action".

The specified list of conditions is saved in `/opt/f-secure/fsigk/conf/spam/custom.txt`.

The file lists one condition per line. The "Judgment", "Field name", "Compare method", and "Text to scan for" are separated by tabs.

- The "Judgment" setting is specified as "BLACK" (spam), "WHITE" (not spam), or "NONE" (no action).
- "Field name" contains either a field name or "FILENAME" (file name), "FILESIZE" (file size), "TEXTBODY" (text body), "HTMLBODY" (HTML body), "URLHOST" (link host name), "RELAYIP" (relay addresses), or "ALWAYS" (always).
- "Compare method" contains "IGNORECASE" (not case sensitive), "HEADMATCH" (forward matching), "TAILMATCH" (backward matching), "NOT" (not equal), "AND" (AND with previous condition (same MIME part)), or "AND_SAMEPART" (AND with previous condition (same MIME part)).
- The character strings in "Text to scan for" are separated by commas (",").

Spam detection engine

Spam Detection Engine (spam_commtouch)

This setting enables or disables the spam detection engine. The spam detection engine enhances the spam scanning on both SMTP and POP proxies.

- Database updating proxy settings is also used for the spam detection engine proxy.
- The spam detection engine connects to the following server:
 - Host: ct-cache%d.f-secure.com (%d can be digit from 1 to 9)

- Port: TCP/80
- Protocol: HTTP
- The spam detection engine increases the memory consumption for SMTP and POP services.
- The Spam Detection Engine includes the detection name: FSIGK/SPAM_CT/[Class]/[ThreatLevel]/RefID

Class:

0: Messages that are confirmed, without doubt, as coming from a trusted source. This classification is very rarely used.

1: No information is available for this value. Status could not be determined at this time.

2: Messages that are sent to slightly larger than the average distribution.

3: Spam messages that originate from sources, which are not confirmed spammers.

4: Spam messages that originate from known spam sources (for example, zombies).

ThreatLevel:

0: Threat for virus could not be determined at this time.

1: Probable threat of virus in the message has been detected.

2: High likelihood of the message presenting a virus threat.

3: Confirmed that the message contains a virus.

RefID:

The RefID is a parameter that is returned by ctEngine with every message classification. It contains a transaction tracing code that can help to track the reason for the classification.

RBL*RBL* (spam_rbl)

These settings enable or disable the use of RBLs (Realtime Black Lists) for spam checking and specify the RBL servers which are used when checking for spam. Specify the servers separated by commas. Specify up to 199 characters.

E-mail is scanned by checking whether the source IP address (in the case of SMTP) and the IP addresses in the Received headers are registered in an RBL server. Although the RBL and SURBL servers are queried together, a delay of several hundred milliseconds occurs while waiting for the server replies. If no reply is received within one second, the operation times out and the e-mail is not identified as spam.

The maximum number of queries per e-mail is 32. Because three RBL servers are set by default, the number of addresses from the Received headers that can be checked is 9 or 10 (for SMTP, as the source address is also checked) or 10 or 11 (in the case of POP).

Excluded addresses are not counted.

The detection name for RBL is "FSIGK/SPAM_RBL/(detected address)[(RBL server name):(RBL reply address)]".

Detected address : Address registered in the RBL server

RBL server name : Name of the RBL server in which the address was found

RBL reply address : Reply address from the RBL server when spam is detected

SURBL querying is performed by looking up the name in the DNS. The DNS server to query is the first nameserver setting in `/etc/resolv.conf`.

By default, this setting is disabled.

Server

Server (spam_surbl_list)

Specifies the list of RBL servers. You can specify multiple servers, separated by commas (",").

(Initial setting: bl.spamcop.net, sbl-xbl.spamhaus.org, list.dsbl.org)

Addresses to be excluded

Skip address

Disables RBL checking for the specified addresses.

(Initial setting: 127.0.0.1 10. 192.168. 172.16.0.0/255.240.0.0)

🔗 For examples, see “[Access Control](#)”, 65.



Note

If you edit the [Addresses to be excluded] setting by using the web console, the spam rbl pass field is updated in `/opt/f-secure/fsigk/conf/hosts.allow`.

SURBL

SURBL (spam_surbl)

These settings enable or disable the use of SURBLs (SPAM URL Realtime Black Lists) for spam checking and specify the SURBL servers which are used when checking for spam.

Specify the servers separated by commas. Specify up to 199 characters.

E-mail is scanned by checking whether the domain name part of the URLs contained in the text body or HTML body of the e-mail is registered in a SURBL server. Although the RBL and SURBL servers are queried together, a delay of several hundred milliseconds occurs while waiting for the server replies. If no reply is received within one second, the operation times out and the e-mail is not identified as spam. The maximum number of queries per e-mail is 32.

The detection name for SURBL is "FSIGK/SPAM_SURBL/(detected domain name)[(SURBL server name):(SURBL reply address)]".

When spam is detected by checking an SURBL:

Detected domain name : Domain name registered in the SURBL server

SURBL server name : Name of the SURBL server in which the name was found

SURBL reply address : Reply address from the SURBL server when spam is detected

SURBL querying is performed by looking up the name in the DNS. The DNS server to query is the first nameserver setting in `/etc/resolv.conf`.

By default, this setting is disabled.

Server

Server (spam_surbl_list)

Specifies the list of SURBL servers. You can specify multiple servers separated by commas (",").

(Initial setting: multi.surbl.org)

7.1.2 Virus Definition Database

Virus definition update

Virus definition update

Manual update

Manual Update

Updates virus definition files to the latest version. Updating may take some time as the virus definition databases are downloaded from the Internet.

Use the dbupdate command to update the definition file.

The dbupdate command retrieves files from <http://fsbserver.f-secure.com/> using the AUA (Automatic Update Agent, "fsaua" command) to the "databases" directory.



If the virus definition databases fail to download, check if you can connect to the following URL: **<http://fsbserver.f-secure.com/>**. A simple text message should be shown indicating that you have reached the F-Secure Automatic Update Server. In addition, check the log file (`/opt/f-secure/fsigk/log/dbupdate.log`, `/opt/f-secure/fsigk/log/fsaua.log`) for any problems.



The configured proxy information is stored in `/opt/f-secure/fsigk/conf/dbupdate.conf` with the following information:

<code>use_proxy=[yes no]</code>	Specifies whether the proxy is used or not
<code>http_proxy_host=</code>	Specifies the host name of the proxy server
<code>http_proxy_port=</code>	Specifies the port number of the proxy server
<code>use_proxyauth=</code>	Specifies whether proxy authorization is used or not
<code>http_proxyauth_user=</code>	Specifies the user name used for proxy authorization
<code>http_proxyauth_pass=</code>	Specifies the password used for proxy authorization



To download definition files from Policy Manager, specify `UPDATEURL=http://<host name>:<port number>/` in `/opt/f-secure/fsigk/conf/dbupdate.conf`.



- You can check the version number of virus definition files with "`cd /opt/f-secure/fsigk; make show-dbversion`". You can obtain the version of the definition file for each engine (Aquarius, Hydra (FS-Engine)) from "[Version]... File_set_visible_version=YYYY-MM-DD_XX" in `databases/aqualnx32.xxx/aquarius-linux-update.txt` and `databases/fse.xxx/FS@hydra.ini`. The overall version of virus definition files is the highest version number amongst the versions of each engine.

Automatic updates

Automatic Update

This function updates the definition file periodically (at hourly intervals).

Updates are performed by the `fsupdated` daemon, `fsaua` daemon and `dbupdate` command.



If the virus definition databases fail to download, check if the files can be downloaded from the following URL: **<http://fsbserver.f-secure.com/>** In addition, check the log file (`/opt/f-secure/fsigk/log/dbupdate.log`, `/opt/f-secure/fsigk/log/fsaua.log`) for

any problems.



The configured proxy information is stored in `/opt/f-secure/fsigk/conf/dbupdate.conf` with the following information:

`use_proxy=[yes|no]` Specifies whether the proxy is used or not
`http_proxy_host=` Specifies the host name of the proxy server
`http_proxy_port=` Specifies the port number of the proxy server
`http_proxyauth=` Specifies whether proxy authorization is used or not
`http_proxyauth_user=` Specifies the user name which is used for proxy authorization
`http_proxyauth_pass=` Specifies the password which is used for proxy authorization



To download definition files from Policy Manager, specify `UPDATEURL=http://<host name>:<port number>/` in `/opt/f-secure/fsigk/conf/dbupdate.conf`.



- You can check the version number of virus definition files with “`cd /opt/f-secure/fsigk; make show-dbversion`”.

You can obtain the version of the definition file for each engine (Aquarius, Hydra (FS-Engine)) from “[Version]... File_set_visible_version=YYYY-MM-DD_XX” in `databases/aqualnx32.xxx/aquarius-linux-update.ini` and `databases/fse.xxx/FS@hydra.ini`. The overall version of virus definition files is the highest version number amongst the versions of each engine.

7.1.3 Logs

Logs

Log

Shows the log recorded for each service.

You can download and show up to 1000 lines of log entries.

🔗 For information logs, see “[Logs](#)”, 75.

HTTP

SMTP

POP

FTP

Access logs

Detection logs

Information logs

Error logs

Virus definition database update logs

Shows the log of definition file updates.

7.1.4 Top Menu

Admin password

Admin password

Changes the password that you need to log into the web console.



If you edit the "Admin password" setting by using the web console, the following file is updated:
`/opt/f-secure/fsigk/conf/fsigk.htdigest`.
 (The format is the same as in the `htdigest` authentication file used by Apache.)

Diagnostics

Diagnostics

Downloads the diagnostic information file (`diag.tar.gz`). The diagnostic information file contains information for troubleshooting, including product settings, system settings, and log information.



Download the `/opt/f-secure/fsigk/diag.tar.gz` file created by the "`cd /opt/f-secure/fsigk; make diag`" command.
 When contacting support, please send the diagnostic information file (`diag.tar.gz`) if possible.

License

License

Enter or show license information.

You do not need to restart the services after setting the license information. However, you need to start the service if it has halted because the license has expired.



If you edit the [Admin password](#) setting by using the web console, the following file is updated:
`/opt/f-secure/fsigk/conf/fsigk.htdigest`.

Version

Version

Shows the operating environment and version information of the product.

Logout

Logout

Logs out from the web console.

7.2 Access Control

You can use the proxy and other settings to control access based on the host and network.

Specify the settings as described below.



Access control uses tcpwrapper. For more information about tcpwrapper, run "man 5 hosts_access" from the command line.

Setting examples:

123.456.789.123 999.999.999.999

Permit connections for the IP addresses "123.456.789.123" and "999.999.999.999".

host.domain.jp

Permit connections for the host name "host.domain.jp".

This does not permit connections for "xxx.host.domain.jp".

.domain.jp

Permit connections for host names that end in ".domain.jp".

This permits connections for "xxx.domain.jp", but not for "domain.jp".

domain.jp .domain.jp

Permit connections for "domain.jp" and domains that are part of "domain.jp".

This permits connections for both "xxx.domain.jp" and "domain.jp".

192.168.

192.168.0.0/255.255.0.0

Permit connections for networks in which the addresses are specified in the form 192.168.3.4.

"255.255.255.255" cannot be specified as the netmask.

ALL

Permit connections from all hosts.

ALL EXCEPT 10.0.0.2 192.168.0.2

Permit connections from all IP addresses except 10.0.0.2 and 192.168.0.2.

ALL EXCEPT 192.168.0.0/255.255.0.0

Permit connections for networks other than 192.168.0.0/255.255.0.0.

.domain.jp EXCEPT 10.0.0.2 192.168.0.2

Permit connections for host names that end in ".domain.jp" unless the IP address is 10.0.0.2 or

192.168.0.2.

/etc/fsigk_allow_list.txt

Permit connections from addresses contained in the list file (/etc/fsigk_allow_list.txt). Specify each address in the list file on a separate line or delimited by spaces.

ALL EXCEPT /etc/fsigk_deny_list.txt

Block connections from addresses or hosts contained in the list file (/etc/fsigk_deny_list.txt) and permit all other connections. Specify each address in the list file on a separate line or delimited by spaces.

What to do if a line contains more than 2047 bytes

The access control setting file (`/opt/f-secure/fsigk/conf/hosts.allow`) permits a maximum of 2047 bytes per line. Use the following methods if you want to specify lines longer than 2047 bytes.

- Specify the list in a separate file

Specify the host.domain list in a separate file (e.g. `/etc/fsigk_smtp_rcpt_allow_list.txt`) as follows:

```
aaa.com  
bbb.com  
ccc.com
```

Then, specify the file (e.g. `/etc/fsigk_smtp_rcpt_allow_list.txt`) in the access control setting. You can use this method when you specify a list of hosts in the web console or in the access control settings file (`/opt/f-secure/fsigk/conf/hosts.allow`).

```
smtp_rcpt: /etc/fsigk_smtp_rcpt_allow_list.txt
```

- Specify multiple lines in the file

Specify multiple lines in the access control settings file (`/opt/f-secure/fsigk/conf/hosts.allow`) as follows.

In this case, the web console screen only shows the top line.

```
Example:      smtp_rcpt: aaa.com bbb.com ccc.com  
             smtp_rcpt: ddd.com eee.com fff.com
```

7.3 Detection Notification Templates

You can specify a header in the top line of the detection notification template.

When sending a notification e-mail to the sender or administrator from the SMTP service, you can specify "From: name@domain" in the initial part. This specifies the header's From line and the Envelope From ("MAIL FROM:" command address). However, you cannot change the Envelope From for notifications sent to recipients.

UTF-8 character set can be used in the "Subject:" and "From:" fields.

Note that you need to restart the service after editing the template.

Variables that can be used in virus detection messages

`${SERVICE_TYPE}`

Service type ("http" or "smtp" or "pop" or "ftp")

`${DETECTION_NAME}`

Virus or other detection name (W95/Klez.H@mm, etc.)

`${VIRUS_INFO_URL}`

URL for information about a virus

Example: "http://cgi.f-secure.com/cgi-bin/search.cgi?q=W32/NetSky.D@mm"

`${CLIENT_HOST}`

Client host name



Note

To show the host name, you must enable [DNS Reverse Lookup] in the web console.

`${CLIENT_ADDR}`

Client IP address

`${SERVER_HOST}`

Server host name (the server which is connected to from the Internet Gatekeeper)

`${SERVER_ADDR}`

Server IP address (the server which is connected to from the Internet Gatekeeper)

`${STATUS}`

Response code (the same value as is shown in the access log)

`${METHOD}`

Request method



Note

For HTTP, this is the HTTP request method (GET, POST, etc.). For FTP, "PUT" indicates sending and "GET" indicates receiving. For other services, the method is always "GET".

`${URL}`

URL of the accessed site

`${CONTENT_TYPE}`

Value indicating the Content-Type (Example: text/html)

`${CONTENT_LENGTH}`

Size of the transferred file (number of bytes)

`${FILENAME}`

Name of the detected file

`${QUARANTINE_FILE}`

Name of the quarantined file

`${TIME}`

Access time (number of seconds since 1970/01/01)

`${TIME_STR}`

Access time in text format (Example: 'Tue May 7 16:16:17 2002')

`#{HEADER}`
Content of the header

`#{TEXT}`
Content of the text message

`#{MAILFROM}`
SMTP sender address (the address passed to the "MAIL FROM:" command)

`#{RCPTTO}`
SMTP recipient addresses (the addresses passed to the "RCPT TO:" command, separated by commas (","))

`#{MESSAGE_ID}`
Value of the Message-Id field in the SMTP e-mail header

`#{ERROR_STR}`
Error message (the same information as PROXY-ERROR in the access log)

`#{ACTION}`
Action which is taken when a virus is detected (the same information that is recorded in the access log)

`#{PATH_QUERY}`
Path and query part of the URL (only applies to the HTTP service)

`#{X_FORWARDED_FOR}`
X-Forwarded-For header field (only applies to the HTTP service)

7.4 Expert Options

Reference Information for Expert Options

Usually, you do not need to specify any other settings than those available through the web console and described in this manual. However, a number of expert options are available for handling special cases or requirements. For more information, see the following file:

`/opt/f-secure/fsigk/doc/expert-options-fsigk-EN.txt`

Using Expert Options

The expert options include settings that are highly likely to change in future versions and are not settings that normally need to be specified. Because these options may be dependent on the particular system environment and may not work the way the user expects, please confirm that the options work correctly on your system before you use them.

If you need to use the expert options and set them on your system, please notify the support center. Based on the understanding of how the options are used in practice, we will investigate whether we can add them to the standard options and support them on the web console screens.

8. Command-line Tools



You do not need to use command-line operations daily. Please refer to this chapter if command-line operations are required.

The proxy function of Internet Gatekeeper is automatically started when changes are made to its settings in the Web Console, or during system start-up via `/etc/rc.d/init.d/`. In such cases, the proxy auto-start command (`rc.fsigk_{http,smtp,pop,ftp}`) should be started first. The auto-start command initializes the proxy execution command (`fsigk`).

8.1 Auto-Start

Overview of operations:

Starts, stops, and restarts the proxy execution command (`fsigk`), Web Console, and virus verification daemon (`fsavd`) when the computer is started with the auto-start command (`initscript`). Launch the virus verification engine before you start each proxy service.

Command names:

```
/opt/f-secure/fsigk/rc.fsigk_http http proxy auto-start command
/opt/f-secure/fsigk/rc.fsigk_smtp smtp proxy auto-start command
/opt/f-secure/fsigk/rc.fsigk_pop pop proxy auto-start command
/opt/f-secure/fsigk/rc.fsigk_ftp ftp proxy auto-start command
/opt/f-secure/fsigk/rc.fsigk_fsavd Virus verification engine
/opt/f-secure/fsigk/rc.fsigk_fsasd SPAM verification engine
/opt/f-secure/fsigk/rc.fsigk_admin Web Console auto-start command
```

Options:

```
start      Starts the proxy
stop       Stops the proxy
restart    Restarts the proxy
status     Displays the status of the proxy
```

Command examples:

Restart the http proxy

```
# /opt/f-secure/fsigk/rc.fsigk_http restart
```

Configure the http proxy to auto-start

```
# ln -s /opt/f-secure/fsigk/rc.fsigk_http /etc/init.d/fsigk_http
# chkconfig --add fsigk_http
# chkconfig fsigk_http on
```

8.2 Proxy Execution

Overview of operations:

Executes a proxy according to the set options or with a configuration file.

Usually, you need to specify `/opt/f-secure/fsigk/conf/fsigk.ini` as the configuration file.

Command names:

```
cd /opt/f-secure/fsigk; ./fsigk
```



Move the `fsigk` command to the `/opt/f-secure/fsigk/` directory before using it.

Options:

If you specify multiple options, the last option is prioritized:

```
--http          Uses the http protocol (default when started with "fsigk_http")
--smtp          Uses the smtp protocol (default when started with "fsigk_smtp")
--pop           Uses the pop protocol (default when started with "fsigk_pop")
--ftp           Uses the ftp protocol (default when started with "fsigk_ftp")
-f <inifile>    Reads the settings of "inifile" as the configuration file
                Usually, you need to specify /opt/f-secure/fsigk/conf/fsigk.ini as the
                configuration file.
                Specify the protocol before this option:
--daemon        Starts in the background
-q              Stops the detailed display
-P <port>       Listens to the specified port number
-h             Displays a list of options
```

Command examples:

Start a HTTP proxy (default)

```
# cd /opt/f-secure/fsigk; ./fsigk --daemon --http -f conf/fsigk.ini
```

Starting a HTTP proxy

- Start in the foreground

```
# cd /opt/f-secure/fsigk; ./fsigk --http -f conf/fsigk.ini
```

Starting a HTTP proxy

- Start in the foreground
- Display detailed information

```
# cd /opt/f-secure/fsigk; ./fsigk -v --http -f conf/fsigk.ini
```

Starting a HTTP proxy

- Start in the foreground
- Display detailed information
- Listen to port 9080

```
# cd /opt/f-secure/fsigk; ./fsigk -v --http -f conf/fsigk.ini -P 9080
```

8.3 Virus Definition Updates

Overview of operations:

Updates virus definition files.

Updating may take some time because virus definition files are downloaded from the Internet.

You can specify proxy settings in `conf/dbupdate.conf`.

Update process

The `dbupdate` command retrieves files from `http://fsbserver.f-secure.com/` by using AUA (Automatic Update Agent, "fsaua" command) and temporarily saves the files in the update directory. The files are then copied to the "databases" directory.



If the virus definition files fail to download, check if the files can be downloaded from the following URL:

`http://fsbserver.f-secure.com/`

In addition, check the logs file (`/opt/f-secure/fsigk/log/dbupdate.log`, `/opt/f-secure/fsigk/log/fsaua.log`) for any problems.



The configured proxy information is stored in `/opt/f-secure/fsigk/conf/dbupdate.conf` with the following information:

<code>use_proxy=[yes no]</code>	Specifies whether the proxy is used or not
<code>http_proxy_host=</code>	Specifies the host name of the proxy server
<code>http_proxy_port=</code>	Specifies the port number of the proxy server
<code>http_proxyauth=</code>	Specifies whether proxy authorization is used or not
<code>http_proxyauth_user=</code>	Specifies the user name which is used for proxy authorization
<code>http_proxyauth_pass=</code>	Specifies the password which is used for proxy authorization



To download virus definition databases from Policy Manager, specify "UPDATEURL=http://host name:port number/" in `/opt/f-secure/fsigk/conf/dbupdate.conf` with the host name and port number used by Policy Manager.



- You can check the version number of virus definition database files with "`cd /opt/f-secure/fsigk; make show-dbversion`".

The version number of database files for each engine (Aquarius, Hydra(FS-Engine)) corresponds to "[Version]... File_set_visible_version=YYYY-MM-DD_XX" in `databases/aquinx32.xxx/aquarius-linux-update.ini` and `databases/fse.xxx/FS@hydra.ini`. The version number of the entire virus definition file is determined by the highest version number among all of the version numbers in each engine.

You can specify proxy settings in `conf/dbupdate.conf`.

Command names:

`/opt/f-secure/fsigk/dbupdate`

Options:

`--help` Displays a quick help which lists command-line options.

`--auto` Definition files are not downloaded synchronously. Instead, the definition files previously downloaded by F-Secure Automatic Update Agent are updated. This option is used to fully automate virus definition updates.

`fsdbupdate9.run`

Definition files are not downloaded from the Internet. Instead, they are carried on by using specified databases (`fsdbupdate9.run`). (databases are imported)

Configuration file:

```
/opt/f-secure/fsigk/conf/dbupdate.conf
use_proxy=[yes|no]   Specifies whether a proxy is used or not
http_proxy_host=     Specifies the host name of the proxy server
http_proxy_port=     Specifies the port number of the proxy server
http_proxyauth=     Specifies whether proxy authorization is used or not
http_proxyauth_user= Specifies the user name which is used for proxy authorization
http_proxyauth_pass= Specifies the password which is used for proxy authorization
UPDATEURL=http://host name:port number/
                    Specifies the URL of Policy Manager in cases when the virus definitions are to be
                    downloaded from Policy Manager
```

Command examples:

Update virus definitions.

```
# cd /opt/f-secure/fsigk; ./dbupdate
```

Import from a specific definition file (`fsdbupdate9.run`).

```
# cd /opt/f-secure/fsigk; ./dbupdate fsdbupdate9.run
```

Exit codes:

You can obtain the update results with the following exit codes.

Exit code	Description
0	There are no new updates. Nothing is updated.
1	The system failed to update databases. For details, see the program output and log files at <code>/opt/f-secure/fsigk/log/dbupdate.log</code> and <code>/opt/f-secure/fsigk/log/fsaua.log</code> .
2	Virus definition databases were successfully updated.



Note

An exit code over 128 indicates a termination signal. For example, if the exit code is 143, $143-128=15$ (SIGTERM) is the signal. You can check the Linux signal numbers with commands such as "man 7 signal".

Log files:

Update results are written to the following log files. When troubleshooting, refer to these files:

```
/opt/f-secure/fsigk/log/dbupdate.log
/opt/f-secure/fsigk/log/fsaua.log
```

8.4 Restarting All Services

Overview of operations:

Restarts all services (`http`, `smtp`, `pop`, `ftp`, `admin`) that are enabled. This command operates in the same way as the restart option in the web console.

Command names:

```
cd /opt/f-secure/fsigk; make restart
```

Command examples:

Restart all services that are enabled.

```
# cd /opt/f-secure/fsigk; make restart
```

8.5 Creating Diagnostic Information

Overview of operations:

Creates a diagnostic information file (`diag.tar.gz`) in the `/opt/f-secure/fsigk` directory. The diagnostic information file contains configuration information about the product, system, and log files. The information is needed for troubleshooting.



Note

When contacting support, please send the diagnostic information file (`diag.tar.gz`) if possible.

Command names:

```
cd /opt/f-secure/fsigk; make diag
```

Command examples:

Create a diagnostic information file.

```
# cd /opt/f-secure/fsigk; make diag
```

9. Logs

F-Secure Internet Gatekeeper for Linux records access status, virus detection status, and error occurrences to log files. The log files are saved in `/opt/f-secure/fsigk/log/` and a directory is created for each service.

9.1 Log Files

9.1.1 Access Logs

All accesses to servers through the product are saved into access logs.

Logs are formatted in the following manner.



You can use various log analyzing tools because the logs saved by the product are compatible with the Squid log format. For setting examples of Webalizer, see “[Log Analysis Tools](#)”, 99.

Log format

Connection statuses are recorded one line at a time. Each item below is separated with a space.

- Time
The access time from the client. Displays the number of seconds from epoch time (1970/01/01 00:00:00(UTC)) in milliseconds.
- Connection time
Displays how long the client was connected in milliseconds.
- Client host
Displays the host of the client. When reverse lookup is available, the host name is displayed. If not, the IP address is displayed.
- Processing results
Returns [Cache status] / [HTTP status code].
Cache status is not used. TCP_MISS is always used.
The HTTP status code is the HTTP response status code (3 digit number) to be sent to the client. 200 is returned for non-HTTP successful connections, 500 when a error occurs, and 000 in other cases (including when connections are terminated immediately after connecting without any data relay).
- File size
The size of the file transferred.
- Request method
The HTTP request method (GET, POST, etc.) when HTTP is used. PUT is applicable when FTP is used. In other cases, GET is used.
- URL
Displays the URL accessed.

When pop is used, the URL is "pop://POP user name@POP server name:port number".
 When smtp is used, the URL is "mail:destination".

- User name
 Displays the user name when proxy authentication is used.
 "-" is recorded if authentication is not used.
- Hierarchy code
 Returns "[Hierarchy string]/IP address of destination".
 [Hierarchy string] is not used. "DIRECT" is always used.
- Content-Type
 Displays the Content-Type of the file to be transferred. "-" is used when not available.
- Detection information
"DETECT-STAT:[Detection results]:[Virus name]:[File name]:[Quarantined file name]:" is returned.

Detection results	Either INFECTED (Virus detected), SPAM (Spam detected), or CLEAN (No virus detected)
Virus name	Name of the virus
File name	Name of the file being transferred
Quarantined file name	The name of the file as it is stored in the quarantine directory This is set only if the quarantine of infected files is enabled.

- Action
"ACTION:[Action]:" is returned.

Action	Either of the following actions are returned according to the detection results: <ul style="list-style-type: none"> • NONE Nothing is done (No detection) • PASS Detected but passed (logged) • DELETE Deleted (If SMTP is used, a notification is sent to the recipient after the file is deleted) • DENY Detected with SMTP and blocked • SENDBACK Notification sent to the sender with SMTP • BLACKHOLE Deleted with SMTP (no notification to the sender) • CHANGE_SUBJECT Spam detected with SMTP and the subject is changed
--------	---

- Proxy information
"PROXY-STAT:[Service type]:[Internal process ID]:[Process ID] :[IP address of host]:[Number of processed files]:[Number of checks]:[Detection time]:[Detection details]:" is returned.

Service type	Indicates the service type (http, smtp, pop, ftp)
Internal process ID	Indicates the internal process ID (identifier starts with 0) used for the process. In general, smaller numbers have higher priority. [internal process ID]+1) applies to the simultaneous number of connections during startup of the corresponding access.
Process ID	Indicates the process ID that is used for the process
IP Address of host	Indicates the IP Address of the host
Number of processed files	Indicates the number of requests processed in the same session. Starts with 1 and increments by 1 for each access log generated in the same session. For POP, 1 is always used.
Number of checks	The number of virus checks executed in one connection (the number applies to the number of times since the last time an access log was

	generated)
Detection time	The time (milliseconds) spent on virus checks executed in one connection (the time applies to the time elapsed since the last time an access log was generated)
Detection details	Displays the detection details with the following strings separated by a comma: <ul style="list-style-type: none"> • VSD_ENCRYPTED Encrypted file • VSD_MAXNESTED Maximum allowed nest value was reached • VSD_SCANTIMEOUT Scan time reached the timeout value • OVER_FILESIZE Size of the file is greater than the file size limit for scanning • PASS_TO Matches a host name excluded from scanning • PASS_USER_AGENT Matches a User-Agent excluded from scanning • PASS_EXT Matches a file name and extension excluded from scanning (HTTP and FTP only)

- Protocol information

Logs the unique information of each protocol. Enabled for the HTTP/SMTP service only.

SMTP service:

"PROTOCOL-STAT:[sender address]:[Message-ID]:" is returned.

Sender address	SMTP sender address ("MAIL FROM:" Argument address of command) (Displayed with URL encode.)
Message-ID	Argument address of command (Displayed with URL encode.)

HTTP service:

"PROTOCOL-STAT:[Protocol details]:[X-Forwarded-For]:" is returned.

KEEPALIVE	Displays the detection details with the following strings separated by a comma: <ul style="list-style-type: none"> • KEEPALIVE: Keep-Alive connection (Persistent-Connection) executed in the corresponding session. • PROGRESS* A download progress dialog, which is displayed in the corresponding session (if the advanced option of "progress" is set). • TRICKLE: Before the download completes in the corresponding session, a transfer is started by using trickle (if the advanced option of "trickle" is set).
X-Forwarded-For	X-Forwarded-For Field of the request header (Displayed with URL encode.)

- Error information

Displays error information occurring from a proxy process.

"PROXY-ERROR:[Error information]:" is returned.

Error message	The following error message is displayed (Displayed with URL encode.) Common for all protocols <ul style="list-style-type: none"> • CONNECT (Host name: Port number / Connection error message An error message listed in "Connection error messages" (168) appears. <p>HTTP</p> <p>An error message listed in "HTTP Error Responses"</p>
---------------	--

	<p>" (151) appears.</p> <p>SMTP</p> <ul style="list-style-type: none"> • SERVER/ERROR Reply(MAIL): buf=[XXX] Error response when the "MAIL FROM" command to the SMTP server is sent • SERVER/ERROR Reply(RCPT): buf=[XXX] Error response when the " RCPT TO " command to the SMTP server is sent • SERVER/ERROR Reply(AUTH): buf=[XXX] Error response when the " AUTH " command to the SMTP server is sent • PROXY/550 Relaying denied. Relaying denied by the Internet Gatekeeper. Displayed if the relaying is denied due to recipient domain restrictions or authentication. (If relays are accepted from clients, you must set the corresponding client address from the host within the LAN or enable the PbS/SMTP authentication. If relays are accepted externally, you must set the recipient domains.)
--	--

9.1.2 Virus and Spam Detection Logs

Logs are recorded if viruses or spam are detected during data transfer.

- ➡ The format of the logs is identical with those covered in "[Access Logs](#)", 75.

9.1.3 Error Logs

Logs are recorded when an error occurs. Refer to the error logs if the program is not working properly. Error logs are formatted in the following manner. The format and text of the messages may change in the future if necessary.

Error message format

Time (seconds) [Date Time Port Internal process ID Client IP address:Client host Client host name:Client port number server IP address:Server host name:Server port number] Error message

The date and time indicates the time when the error occurred. The first time displays the number of seconds from epoch time (1970/01/01 00:00:00(UTC)) in milliseconds.

For errors relating with OS system calls, the following is added to the end of the error message:

```

/streerror (Error code)=Error message
      Error code: Error code for system calls
      Error message: Error message for system calls

```

Error message content

Message

```

###ERROR### bind(port=Port number,addr=Address). # Please check whether
other service(mail/web server,etc...) is already running on port Port
number." /streerror(98)=Address already in use

```

Description

The service cannot be started because the configured port and address cannot be reached. The product stands by to receive the port number specified by the bind() Linux system call. This error is displayed when bind() fails because the specified port number is already in use.

Solution

Check the other service that uses the same port. Stop the service if it is not needed. If the service is needed, configure the port of the service and the port used by the product to be different.

You can check the process used by each port and address by using "netstat -anp"

("system/netstat_anp.txt" for diagnostic information).

Message

```
###ERROR### Maximum connections: warning: Client connections reached maximum
connections (maximum connections) . More request will be blocked/rejected. If
there is many warnings, please increase 'Maximum Connections'
settings (pre_spawn value of fsigk.ini) of this service. (provisional value
will be good value as start line).
```

Description

Logged when the maximum number of client connections is reached. When the maximum number of connections is reached, processing continues only after the number of connections is decreased.

The backlog (backlog of Linux listen() system call) is set to 5 when the maximum number of connections is reached. For this reason, up to 6 TCP connect requests can be “ESTABLISHED” normally when the maximum number of connections is reached and for connect requests beyond the limit, “SYN_RECV” is assigned as the connection status. Processing does not continue even for TCP connections responded by Linux if the maximum number of connections is reached. You can check the maximum number of connections by looking at the Internal process ID (“PROXY-STAT:[Service type]:[Internal process ID]:..”) in the access logs. The internal process IDs (identifier starts with 0) with smaller numbers have higher priority. Therefore, [internal process ID]+1 applies to the simultaneous number of connections during the startup of the corresponding access.

In addition, you can check the ESTABLISH status of the corresponding port numbers with the netstat command:

```
# netstat -anp | grep :9080 | grep ESTABLISHED | wc -l
(Port 9080 is used in the example)
```

Solution

- Situation:** only a small number of messages appear (for example, 1 error every hour), the product appears to be working fine, and the number of increased connections can be considered temporary.
Solution: you do not need to change any settings.
- Situation:** the scan timeout value is set to 90 seconds by default. If it is disabled (set to 0) or changed to a bigger value, scanning can take a long time for a specific file. This may cause the number of connections to reach the maximum.
Solution: reset the timeout value to the default value of 90 seconds.
- Situation:** if there is a network problem between the product and the server or client, the number of connections may reach the maximum.
Solution: fix the network problem.
- Situation:** if the above cases do not apply (several errors are logged, scan timeout value is not changed, no network problems exist) and servers cannot be accessed, the number of connections needed may be over the maximum value set.
Solution: increase the maximum number of connections as needed.
 If the number of client connections that are needed cannot be determined, configure the following provisional values to test the system. After testing the system, revise the settings if needed. Usually, the maximum number of connections should be set to under 2000 connections.

- HTTP 200
- SMTP 50
- POP 50
- FTP 10



If you increase the maximum number of connections, more connections are allowed, but it requires more memory. Approximately 500 KB of memory is used for each connection.

Message

```
###ERROR### notify_admin:gethostbyname error:admin_mx_host=[Host name] hstrerror=[Error details]
```

Description

The SMTP server ("admin_mx_host" in /opt/f-secure/fsigk/conf/fsigk.ini), which is configured to send notifications to the administrator after a virus or spam detection, could not be retrieved.

Solution

Check if the configured host name of the SMTP server can be retrieved.

Message

```
###ERROR### notify_admin:cannot connect to admin mail server[Host name:Port number] /
strerror(xxx)=xxx
```

Description

Connection to the SMTP server ("admin_mx_host", "admin_mx_port" in /opt/f-secure/fsigk/conf/fsigk.ini), which is configured to send notifications to the administrator after a virus or spam detection, was successful. However, an error occurred.

Solution

Check if the host name and port number of the configured SMTP server can be accessed.

Message

```
###ERROR### notify_admin:smtp error:[Send command name]: buf=[Response line]
/strerror(xxx)=xxx
```

Description

The response message using SMTP for sending notifications to the administrator after a virus or spam detection returned an error.

The send command indicates the SMTP connection status. It can be either "HELO/MAIL FROM/RCPT TO/DATA/QUIT" (when each command is sent), "GREETING" (when the connection is started) or "DATA END" (when data has been sent).

Solution

Check the [Response line] if mail can be sent to the configured SMTP server.

Message

```
###ERROR### semget failure. Childnum(pre_spawn=[Maximum connections])
may be large. If needed, maximum semaphore number(SEMMNI)
can increase by adding like 'kernel.sem=250 128000 32 512' on
'/etc/sysctl.conf' and running 'sysctl -p'./strerror(28)=No space
left on device
```

Description

The service could not be started because the semaphore could not be secured.

Solution

If a service process (fsigk_XXX) is terminated, for example by the “kill -KILL” command, an error can occur if semaphores are not released and left in the system process. In this case, restart the server (Operating System). You can check the semaphores that are currently used at “/proc/sysvipc/sem”.

If the maximum number of connections is set to a large number, this error is more likely to occur because more semaphores are needed. Set the maximum number of connections to under 2000 connections. Use a larger number only if it is absolutely necessary. Usually, the maximum number of connections should not be set to over 2000 connections.

The product requires semaphores according to the number of processes. You may sometimes need to increase the number of semaphores that the operating system can use. This may happen, for example, when the maximum number of connections needs to be increased or if other processes are using a large number of semaphores. To increase the number of semaphores:

- 1 Add the following line to /etc/sysctl.conf:

```
kernel.sem=250 128000 32 512
```

- 2 Run the following command:

```
# sysctl -p
```

- 3 Check that the number of semaphores has been configured. Use the following command:

```
# cat /proc/sys/kernel/sem
250 128000 32 512
```

Message

```
###ERROR### sendfile timeout: No data can send while 120 sec. There maybe
temporary network trouble between receiver.) / URL=[...] ...
```

Description

Logged when a session is disconnected because no data could be sent for 120 seconds.

Solution

Check if there are any problems in the network.

Message

```
###ERROR### get_response_header: Too Large Header
```

Description

Is displayed when a HTTP response header is too large (over 10 KB). The service is working without any problems.

Solution

Check if the problem occurs for a specific URL or browser.

Message

```
###ERROR### main:diskspace_check: not enough disk space in temporary
directory [Directory name].
```

Description

Is displayed when the temporary directory has less than 5 MB of free space. The service does not start.

Solution

Free up disk space in the temporary directory.

Message

```
###ERROR### realthimescan_check : cannot open [%s]. Realtime virus scan seems
be enabled. Please stop realtime virus scan, or exclude scanning for temporary
directory [Directory name].
```

Description

Is displayed when another anti-virus software is found and real-time virus protection is enabled for the temporary directory. The service does not start.

Solution

Disable real-time virus protection altogether or disable it against the temporary directory.

Message

```
###ERROR### smtp_data_cmd_senddata:[Action on detection]:smtp error:[Send
command name]: buf=[Response line] /strerror(xxx)=xxx
```

Description

The response message using SMTP for sending notifications to the sender/recipient after a virus or spam detection returned an error.

The options for [What to do when a virus is detected] are "Block", "Notify recipients after deleting the mail", and "Delete".

The send command indicates the SMTP connection status. It can be either "RSET/MAIL FROM/RCPT TO/DATA/QUIT" (when each command is sent), or "DATA END" (when data has been sent).

Solution

Check the [Response line] and see if mail can be sent to the SMTP server.

Message

```
###ERROR### smtp_data_cmd_itr:AUTH buf=[Response line] /strerror(XXX)=XXX
```

Description

Is displayed when a response code during SMTP authentication with the SMTP server returns an irregular code (besides 334, 5xx, 235). The [Response line] represents the response message from the SMTP server.

Solution

Check if the response message from the SMTP server is correct. If there are no problems, please send the diagnostic information and the results of the packet capture (tcpdump) being authenticated to F-Secure.

Message

```
###ERROR### ftp_noop_callback:NOOP command reply error [Response line]
/strerror(XXX)=XXX
```

Description

Is displayed when a NOOP command sent to a FTP server returns a response other than 200.

Solution

Check if the FTP server is disconnected or if it is correctly responding to the NOOP command.

Solution

Check if the response message from the SMTP server is correct. If there are no problems, please send the diagnostic information and the results of the packet capture (tcpdump) being authenticated to F-Secure.

Message

```
###ERROR### XXXX /strerror(23)=Too many open files in system
```

Description

Displays a message which indicates that there are too many open files.

This message appears when the number of open files has reached the maximum allowed limit on the system.

You can check the number of file handles at `/proc/sys/fs/file-nr` in the following way:

```
(Display command) cat /proc/sys/fs/file-nr
```

```
[Allocated file handles] [File handles being used] [Maximum allowed files handles]
```

```
(Example: # cat /proc/sys/fs/file-nr
```

```
1864    504    52403)
```

Solution

Check if there are any processes that are using a lot of file handles. You can use, for example, the "lsof" command.

If there are no problems in the system and the number of file handles being used is approaching the maximum, increase the file handles by changing "`/proc/sys/fs/file-max`" in the following way:

1. Add the following line to `sysctl.conf` (the maximum number of file handles is changed to 65535):

```
fs.file-max = 65535
```

2. Run the following command to apply the changes:

```
sysctl -p
```

Message

```
###ERROR### XXX cannot open [/var/tmp/fsigk/proxytmp-xxx]/strerror(2)=No
such file or directory
```

Description

Is displayed when a temporary file used by the product cannot be opened.

Solution

Check if the temporary file has been deleted by a command or another program.

Message

```
###ERROR### Cannot find tproxy(version2) interface.
```

Description

Is displayed when TPROXY usage settings (Source IP retained, `transparent_tproxy=yes`) are carried on and the tproxy patch is not working.

Solution

The tproxy patch may not be applied to the kernel.

Check if `/proc/net/tproxy` exists.

If you use Turbolinux 10 Server, please note the following:

- kernel-2.6.8-5 or later must be used

Check that the kernel version is 2.6.8-5 or later by using the `uname -a` command.

If the kernel version is old, update the kernel of Turbolinux10 to the latest one.

The `- iptable_tproxy` module must be implemented.

Check if the `"iptable_tproxy"` module is included in the results from the `"lsmod"` command.

If it is not, include the module by following the steps below:

1. In `/etc/sysconfig/iptables-config`, set iptables to read `iptable_tproxy` by editing the

`IPTABLES_MODULES` line in the following way:

```
IPTABLES_MODULES="iptable_tproxy"
```

2. Restart iptables

```
# /etc/rc.d/init.d/iptables restart
```

3. Check if `/proc/net/tproxy` exists

4. Restart the Internet Gatekeeper

If a previous version of `tproxy(version1)` is used, add `"transparent_tproxy_version=1"` to the configuration file and restart the service. Please note that `tproxy version1` may not be supported in the future. For this reason, we recommend that you use `version2`.

Message

```
###ERROR### vsd_start() error
```

Description

Virus definition files or the scanning engine library could not be loaded.

Solution

If virus definition files or files used by scanning engines are deleted, overwrite the installation with the following command:

For rpm package:

```
# rpm -Uvh --force fsigk-xxx-0.i386.rpm
```

For deb package:

```
# dpkg -r fsigk
```

```
# dpkg -i fsigk-xxx_all.deb
```

If SELinux is used, check if there are errors in `/var/log/messages` to see if policies are denying the process from loading. In addition, disable SELinux to check if the error occurs. You can disable SELinux by editing "SELINUX=disabled" in `/etc/sysconfig/selinux`. After that, restart the server.

Message

```
###ERROR### main:quit_signal:child(nnn)
stopped. (sig=17[SIGCHLD], si_code=3[CLD_DUMPED], status=xxx, childid=-1, cur
_pid=xxx, pid=xxx)
###ERROR### main:core dumped(child proxy process). Please send core
file(core or core.xxx) on the installation directory and diag.tar.gz to
support center.
###ERROR### Error recovery: restarting service...
```

Description

The proxy process was terminated abnormally (core dump). In addition, the service was restarted. The 3 error messages appear consecutively.

Solution

The service is restarted and recovered automatically so it can be used again. The service is stopped while it is being restarted (approx. 10 seconds).

If this message appears, there is a good chance that a problem exists in the product.

In order to have F-Secure take a look at the problem, please send all of the files which begin with "core" in the installation directory (`/opt/f-secure/fsigk/`) to F-Secure.

If you are not using the latest version of the product, please update to the latest version if possible.

Message

```
###ERROR### main/accept_loop/accept(s=x):/strerror(104)=Connection reset
by peer
```

Description

This message can appear if you use kernel 2.2 and if you disconnect immediately after the connection is established. The product can work properly even if this message appears.

Solution

Kernel 2.2 is not supported anymore. If possible, update your distribution.

Message

```
###ERROR### LICENSE_ERROR#ret=-1#msg=License Expired
```

Description

The evaluation license of the product has expired.

Solution

Purchase a license and enter the license key to activate the product.

Message

```
###ERROR### Commtouch database error: Initial database update may be on going.
Wait a moment. (dlopen(/databases/commtouchunix.0/libfsasd-lnx32.so)
failed. dlerror(): ./databases/commtouchunix.0/libfsasd-lnx32.so: cannot
open shared object file: No such file or directory)
###ERROR### Commtouch database error: Initial database update may be on going.
Wait a moment. (FsasFunctionsInitialize? failed.)
```

Description

These two errors mean that there is no database for commtouch spam scanning engine.

Solution

Wait for a while until initial database downloading is done.

Message

```
###ERROR### fsas_open_session(/fsasd-socket) failed.
```

Description

This error means that there is no 'fsasd' process running.

Solution

Please start fsasd services by running `"/etc/init.d/rc.fsigd_fsasd start"` or `"/etc/init.d/rc.virusgw_fsasd start"`.

Message

```
###ERROR### fsav_open_session: Cannot connect to fsavd's
socket(/fsavd-socket-0). fsavd may be not running. Please run
'rc.fsigk_fsavd restart' to restart fsavd.
```

Description

The socket (/fsavd-socket-0) of the scan engine (fsavd) could not be reached. The scan engine (fsavd) may not be running.

Solution

The scan engine (fsavd) starts automatically if it is run from the web console. If the proxy service is run from the command-line, the scan engine (fsavd) must be started in advance. Restart the scan engine with the “/opt/f-secure/fsigk/rc.fsigk_fsavd restart” command.

Message

(Other messages)

Description

An unusual error may have occurred.

Solution

Please send the error log files and diagnostic information to F-Secure for inspection.

9.1.4 Information Logs

The information log (info.log) records any other general information.

Message format:

```
Time (seconds) [Date Time Port Internal process ID Client IP address:Client host Client
host name:Client port number server IP address:Server host name:Server port
number] message
```

The date and time indicates the time when the error occurred. The first time displays the number of seconds from epoch time (1970/01/01 00:00:00(UTC)) in milliseconds.



Note

The format and text of the messages may change in the future if necessary.

Messages at service startup

Message

```
main: ### START ### (argv=[/opt/f-secure/fsigk/fsigk_xxx --daemon --http -f
conf/fsigk.ini ],ver=[Version],pid=Process ID)
```

Description

A message which indicates the start of a service. The message is displayed when a service is started.

Message

```
main: entering daemon mode. (daemon pid=4923)
```

Description

A message which indicates that daemon mode is used. The message is displayed when a service is started.

Message

```
main:entering debug mode...
```

Description

Is displayed when the product is started in debug mode.

Message

main: accept_loop(sock=Socket number,pid=Process number). Starting to accept connection on each proxy process.

Description

A message which indicates the start of a proxy process. The message is displayed when a service is started.

Messages at service stoppage**Message**

main: ### STOP ### (ver=[Version number], pid=プロセス ID, sig=15[SIGTERM])

Description

A message which indicates the end of a service. The message is displayed when a service is stopped.

Message

main:signal_handler(sig=15[SIGTERM], errno=0[Success], code=0[SI_USER], status=0[], pid=xxxx, uid=0)/cur_pid=xxxx

Description

A message which indicates that the SIGTERM signal of a proxy process has been received. The message is displayed when a service is stopped.

Messages while the service is active**Message**

is_alivesocket:recv=XXX, Client closed connection. Client may be cancel the session. url=[YYY], elapsed=TTTms

Description

Is displayed when a client closes a connection before the normal protocol process finishes. The message may appear when a client cancels a session.

TTT represents the elapsed time since the monitoring session started.

Message

is_alivesocket:recv=XXX, Client closed connection. Client may be cancel the session. url=[YYY], elapsed=TTTms

Description

Is displayed when a client closes a connection before the normal protocol process finishes. The message may appear when a client cancels a session.

TTT represents the elapsed time since the monitoring session started.

Message

```
is_server_alivesocket: select(s=AAA):ret=BBB,cur_pid=CCC: Server closed
connection while transaction. There may be timeout on the server because of
no traffic. (elapsed=TTTms)
```

Description

Is displayed when a server closes a connection before the normal protocol process finishes. This message may appear when a session timeout occurs on the server side.

TTT represents the elapsed time since the monitoring session started.

Message

```
sendfile canceled: n=AAA, written=BBB, filelen=CCC writesize=DDD
```

Description

Is displayed when a file transfer to a client or server is canceled. AAA represents the response code of the sendfile system call. BBB represents the size of the sent file. CCC represents the file size. DDD represents the data size being transferred.

Message

```
reverselookup: gethostbyaddr(XXX) failed. herror=EEE(EEE).
```

Description

A reverse lookup error occurred when trying to get the address (XXX).

Message

```
http_forward_response_storeforward_trickle_send: sendfile canceled: ret=AAA,
tmpfile_offset=BBB, bytes=CCC: errno=xxx(xxx)
```

Description

The product uses trickle functions when relaying to clients. This message is displayed when file relays are canceled. AAA represents the response code of the sendfile system call. BBB represents the number of bytes before the transfer.

CCC represents the file size. DDD represents the data size being transferred.

Message

```
file uploading is interrupted by client.
```

Description

Is displayed when a file upload that uses the HTTP service (from a client to the product) is canceled.

Message

```
From: %s:%d(%s) To: %s:%d(%s) Message-Id: %s Infected: %d VirusName: %s
```

Description

Using the SMTP service, a mail that contains “From: Client address: From Client port (sender address)”, “To: Server address: To server port (Recipient address)”, “Message-Id: Message ID” is sent.

The scan results are “Infected: Scan results (detection found when not 0)” and “Virusname: Virus name”.

Message

```
ERROR DATAEND url=[XXX] buf=[YYY]
```

Description

The mail server returned the error code YYY. This happened when the mail server was sending a mail to XXX with the DATA command by using the SMTP service.

Message

```
Access Denied from [Address:Host name]
```

Description

Access was denied because access restrictions are enabled and the corresponding server was not found in the list of connections.

Message

```
Access Denied to [Address:Host name]
```

Description

Access was denied because access restrictions are enabled and the corresponding server was not found in the list of connections.

Message

```
read extra CRLF for POST method
```

Description

When sending data with the POST method in Internet Explorer, an unneeded CRLF is normally added.

This message appears when the unneeded CRLF code is removed. The product can work properly even if this message appears.

(Note: Microsoft Knowledge Base 823099

Extra CRLF Character Is Added to a POST Request That Is Sent to an HTTP 1.1 Server

<http://support.microsoft.com/default.aspx?scid=kb;en-us;823099&Product=ie600>)

Message

```
ERROR Reply(DATA) url=[%s] buf=[%s]
ERROR Reply(DATAEND): url=[%s] buf=[%s]
ERROR Reply(MAIL): buf=[%s]
ERROR Reply(RCPT): buf=[%s]
ERROR Reply(AUTH): buf=[%s]
ERROR Reply(QUIT): buf=[%s]
ERROR Reply(NOOB): buf=[NULL], error=...(...)
ERROR Reply(NOOB): buf=[%s]
```

Description

Is displayed when an error response is returned against the command sent to the SMTP server using the SMTP service. A response message is included in buff-xxx. The command name (DATAEND represents the body of the mail sent) is indicated in parenthesis.

9.2 Splitting/Rotating Log Files

Log files are saved as a single file by default and not split into multiple files. To split log files, use the `logrotate` command.

To set up a split rotation for log files by using the sample configuration file:

- 1 Set the configuration file

Copy the Sample configuration file (`/opt/f-secure/fsigk/misc/logrotate.fsigk`) to `/etc/logrotate.d/virusg`.

```
# cp /opt/f-secure/fsigk/misc/logrotate.fsigk /etc/logrotate.d/fsigk
```

- 2 Edit the configuration file

Specify the rotation interval as needed.

- 3 Check that the logs are properly rotating

Run the following command to make sure that logs are rotated.

```
# logrotate -f /etc/logrotate.d/fsigk
```

9.3 Time Display Conversion Tool

Most logs display the time in seconds elapsed from epoch time. With the `logconv` tool, the date fields of year, month, date, hour, minute, and second can be added to the beginning of the date line in a log file.

You can run the `logconv` tool with the following command. The options may be omitted.

```
# /opt/f-secure/fsigk/misc/logconv <Log file name>
```

(From Windows, you can run it from “/opt/f-secure/fsigk/misc/logconv.exe”.)

Options

<code>--tail [num]</code>	Outputs the log entries corresponding to the last [num] lines from the end of the log.
<code>--tailsec [sec]</code>	The log entries recorded in the last [sec] seconds are output.
<code>--cgi</code>	Used when invoking with CGI.
<code>--today</code>	The logs recorded for the current day are output.
<code>--noconv</code>	Time conversion is not performed.
<code>-r</code>	Converts the converted data back to its original form.

The converted results appear in the standard output. If you add the `--tail <num>` option, log entries from the end of the log file are displayed according to the specified number.

The `logconv` command can handle up to a 2 GB log file. For files larger than 2 GB, use the `head` or `tail` command to split or extract the log data.

In the web console, the converted information will appear when the access or detection log is viewed.

9.4 Log Analysis Tools

The access logs used by the product are compatible with Squid format. This makes it possible to use various log analysis tools, such as Webalizer.

You can perform the daily access analysis with Webalizer by running the following command:

```
# touch /opt/f-secure/fsigk/log/{http,smtp,pop,ftp}/logtool/webalizer.conf
```

In addition, set crontab with the following commands:

```
0 1 * * * cd /opt/f-secure/fsigk/log/http/logtool/;
/usr/bin/webalizer ../access.log -F squid -o .
```

Log results are saved to the `/opt/f-secure/fsigk /log/http/logtool/` directory. You can view the analysis results at `"http://xxx:xx/log/http/logtool/"` after logging into the web console.



Note

A source patch (`misc/webalizer-xxx.detect-stat.patch-xxx`) that additionally displays virus information can be used if needed.

To apply the patch:

```
# tar -zxvf webalizer-2.xx-xx-src.tgz
# patch -p1 < webalizer-2.xx-xx.detect-stat.patch-x.xx
# ./configure
# make
# make install
```

You can also use commercial log analyzing tools such as Sawmill. Sawmill and other similar tools make it possible to perform a more detailed log analysis, which includes virus information. For information on Sawmill, see the following link:

<http://www.sawmill.net/>

9.5 External Output of Logs

Logs are saved as files by default. However, they can be output to other formats such as syslog. Use pipes in the external command to redirect the output. To set the external output, specify the configuration file (`/opt/f-secure/fsigk/conf/fsigk.ini`) in the following way:

```
access_log=|<External command> (For access logs)
detect_log=|<External command> (For virus logs)
info_log=|<External command> (For information logs)
error_log=|<External command> (For error logs)
```

For example, to output SMTP virus detection information and error information to the `local0` facility and the `err` level of syslog, add the following setting to the “smtp” group in `/opt/f-secure/fsigk/conf/fsigk.ini`.

```
[smtp]
detect_log=|logger -t fsigk -p local0.err
error_log=|logger -t fsigk -p local0.err
```

To output files simultaneously, use the following settings:

```
[smtp]
detect_log=|tee -a log/smtp/detect.log | logger -t fsigk -p local0.err
error_log=|tee -a log/smtp/error.log | logger -t fsigk -p local0.err
```

After editing the configuration file, restart the service by selecting Proxy setting on the web console or running the `rc.fsigk_smtp` command.

10. Other Settings

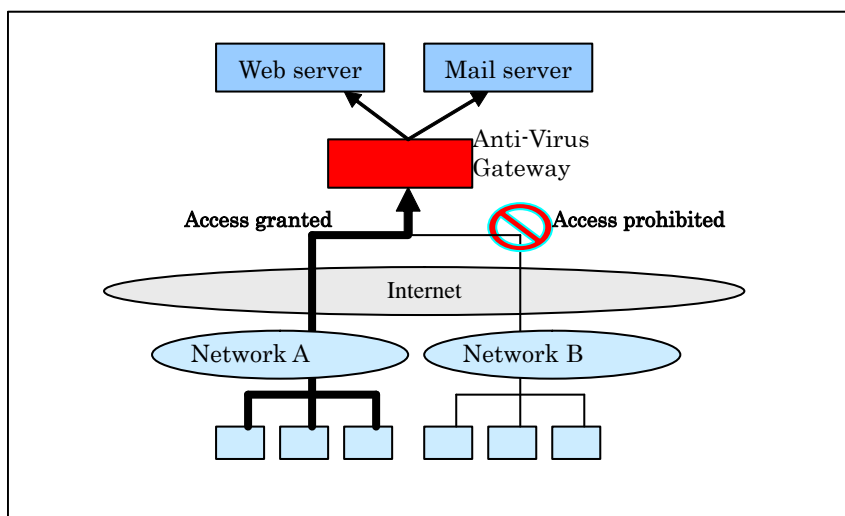
This chapter describes additional settings, which you can configure for the product. For most users, the settings described in “*Typical Configurations*” (15) provide enough security. However, some users may require additional security. In this case, the examples in this chapter may be useful.

10.1 Access Authentication

To prevent unauthorized access to Internet Gatekeeper, you can define that hosts which access Internet Gatekeeper from the Internet are authenticated.

You can configure Access Authentication in the following way.

10.1.1 Host Authentication



If the host which accesses the gateway is fixed, you can use IP addresses and host names to set access control. In this case, you can set proxy settings in the web console. You can also use the IP filtering (iptables) setting of Linux to set access control.

The following example limits access to hosts which have the following IP address and subnet:
192.168.1.0/255.255.255.0.

Proxy Access Control

You can configure access control by using the **Access control** options. To apply restrictions which are based on host names, you must first enable "DNS Reverse Lookup".

- ➔ For more information, see "[Access Control](#)", 65.

Proxy settings

Proxy settings

HTTP proxy

Access control

From these hosts : **Enabled**

(Example: 192.168.1.0/255.255.255.0)

DNS reverse lookup: **Enable to restrict by host names**

SMTP proxy

Access control

From these hosts : **Enabled**

(Example: 192.168.1.0/255.255.255.0)

DNS reverse lookup: **Enable to restrict by host names**

POP proxy

Access control

From these hosts : **Enabled**

(Example: 192.168.1.0/255.255.255.0)

DNS reverse lookup: **Enable to restrict by host names**

FTP proxy

Access control

From these hosts : **Enabled**

(Example: 192.168.1.0/255.255.255.0)

DNS reverse lookup: **Enable to restrict by host names**

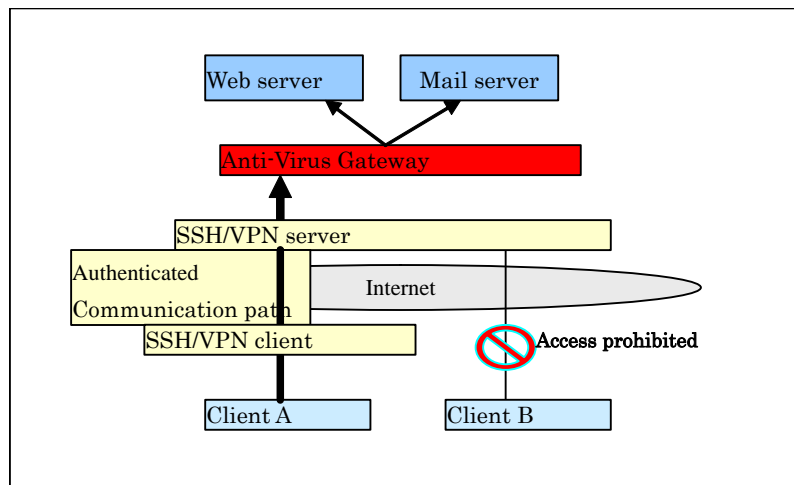
IP filtering (iptables)

You can configure access control which is based on IP addresses by using iptables. The following shows you a configuration example:

- iptables commands

```
# iptables -A INPUT -s 192.168.1.0/255.255.255.0 -j ACCEPT
# iptables -A INPUT -j DROP
```

10.1.2 Authentication using Virtual Networks



To set up authentication by using a virtual network, you must first set up a TCP/IP communication path between the client and Internet Gatekeeper by using a virtual network (SSH/VPN, etc.), which must be authenticated. The client connects to Internet Gatekeeper through the authenticated path. In addition, only authenticated client is able to connect to the gateway.

This section describes settings, which apply if you use SSH (F-Secure SSH, openssh, TTSSH, etc.).



Note

For example, the following software use SSH:

- Reflection for Secure IT (previously known as "F-Secure SSH")
<http://www.attachmate.com/en-US/Products/Host+Connectivity/Security/Reflection+for+Secure+IT>
 Server/Client. SSH2 support. OS: Windows/UNIX.
 GUI. Japanese language support. Technical support.
- Openssh <http://www.openssh.com/>
 Server/Client. SSH2 support. OS: mainly UNIX.
- Teraterm/TTSSH <http://hp.vector.co.jp/authors/VA002416/>
 Client. GUI. Japanese language support. OS: Windows.
- Putty <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
 Client. SSH2 support. GUI. OS: Windows.
- PortForwarder <http://www.fuji-climb.org/pf/JP/>
 Client. GUI for port forwarding. OS: Windows.

Settings

- 1 Install an SSH server to the same server (or a computer on the network) as F-Secure Linux Internet Gatekeeper.



For certain Linux distributions (such as Red Hat 7 and later versions), openssh is installed by default.

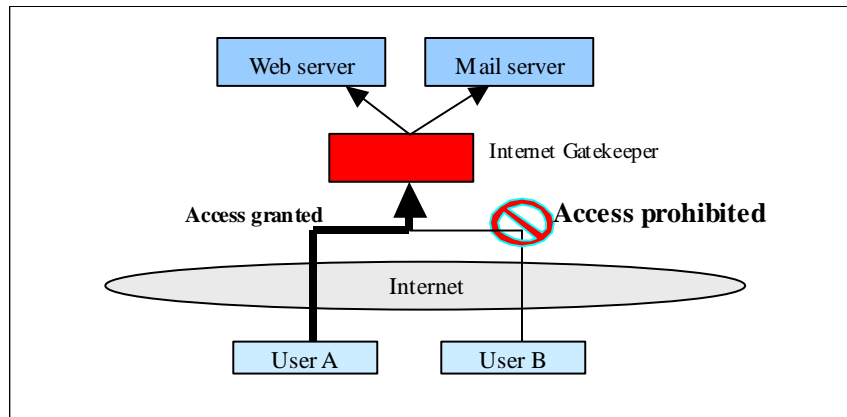
- 2 Install a SSH client to the client computer that accesses the SSH server.
- 3 Change the port forwarding setting of the SSH client so that Internet Gatekeeper becomes the localhost destination.

Set the Config file in the following way. In the example below, the SSH server host is "ssh-server", the SSH user name is "ssh-username", and the Internet Gatekeeper host is "fsigk".

```
Host ssh-server
  User ssh-username
  LocalForward 25 virus-gw:25
  LocalForward 110 virus-gw:110
  LocalForward 9080 virus-gw:9080
```

- 4 Connect the SSH client to the SSH server.
- 5 Change the web browser's proxy setting and the mail client settings as follows:
 - Web browser's proxy : **http://localhost:9080/**
 - Mail client:
 - SMTP server : **localhost**
 - POP server : **localhost**
- 6 Check that viruses are scanned while browsing the web and while sending and receiving e-mails.

10.1.3 Proxy Authentication using Internet Gatekeeper



F-Secure Internet Gatekeeper for Linux can authenticate each user with a password. The authentication method differs depending on the protocol; HTTP proxy authentication is used for HTTP services, SMTP authentication for SMTP services, POP user names for POP services, and FTP user names for FTP services.

User Authentication (PAM Authentication)

You can set authentication settings independently for each user.

You can add, delete, or edit users from the “User Database”.



Note

To open the “User Database” on the web console, click “Proxy settings”. Select “Add or remove users” from the corresponding service page.

POP, FTP Service

For POP and FTP services, F-Secure Internet Gatekeeper for Linux checks whether a user name exists in the user database.

If multiple servers are used, specify “user name@server name” or “user name@server name”. To allow all users for a specific server, specify “@server name”.



Note

- The user name is specified on the client side.
- The password is authenticated on the server side.

The settings are stored in `userdb.txt` in the `/opt/f-secure/fsigk/conf/pam/` directory.

If you edit the settings directly, update the `userdb.db` database file with the `create_userdb userdb.db < userdb.txt` command.

You can also edit the PAM configuration files (`/etc/pam.d/fsigk_{http,smtp,pop,ftp}`) and use external authentication methods such as UNIX account, NIS, LDAP, and Radius. These PAM configuration files are the symbolic links of

`/opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pam`. Do not edit the files at `/opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pam` directly because they are overwritten when updated. If you edit the PAM settings, delete the symbolic links at `/etc/pam.d/fsigk_{http,smtp,pop,ftp}` and create copies of the `/opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pam` files to be used for editing.



To prevent the files from being overwritten during updates, remove the symbolic links and create copies before editing the configuration files.

Proxy Settings

Proxy settings

HTTP proxy

HTTP proxy authentication: **On**

Add or remove users: Add, delete, or edit users on the “Add or remove users” page.

SMTP proxy

Global settings

SMTP authentication: **On**

Add or remove users: Add, delete, or edit users on the “Add or remove users” page.

POP proxy

POP user restriction: **On**

Add or remove users: Add, delete, or edit users on the “Add or remove users” page.

FTP proxy

FTP user restriction: **On**

Add or remove users: Add, delete, or edit users on the “Add or remove users” page.

SMTP Service

The following settings allow SMTP services without authentication to clients who are located within the LAN, and to senders from specific mail servers, addresses and networks.

Proxy settings

SMTP proxy

LAN access settings: **On**

Hosts and networks within LAN: **Specify allowed clients**

(Clients within the LAN, mail servers, etc.)

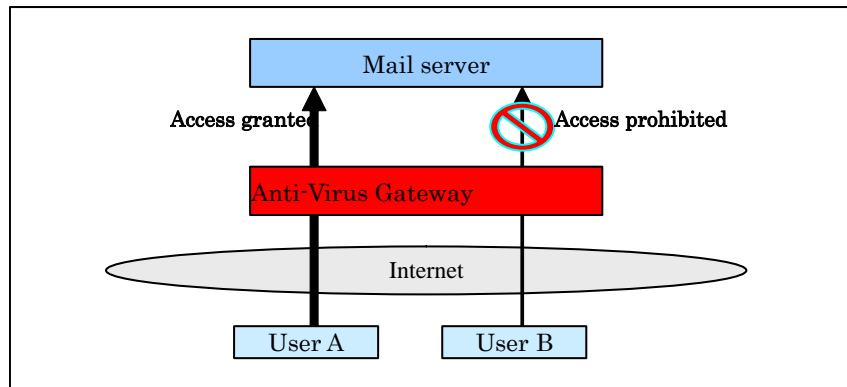
Because e-mails from the Internet are delivered to mail servers through the product, the corresponding mail servers must be allowed to deliver without authentication. The following settings describe how you can configure this.

Proxy settings

SMTP proxy

Restrict e-mail recipients: **On / Specify mail server domains**

10.1.4 Authentication by Mail Servers



F-Secure Internet Gatekeeper uses POP and SMTP authentication on the server side. The product works as a proxy to enable access from clients to the mail server. Therefore, user authenticating functions based on POP and SMTP authentication by mail servers can be used as is.

To use the SMTP authentication on the mail server, disable the SMTP authentication setting for F-Secure Linux Internet Gatekeeper. To disable SMTP authentication for the product:

- Open the web console
SMTP proxy > Global settings and turn off **SMTP authentication**.

If you use APOP, disable the parent server setting of the product. To disable the parent server:

- Open the Web Console
POP proxy > turn off **Defining parent server by user**.

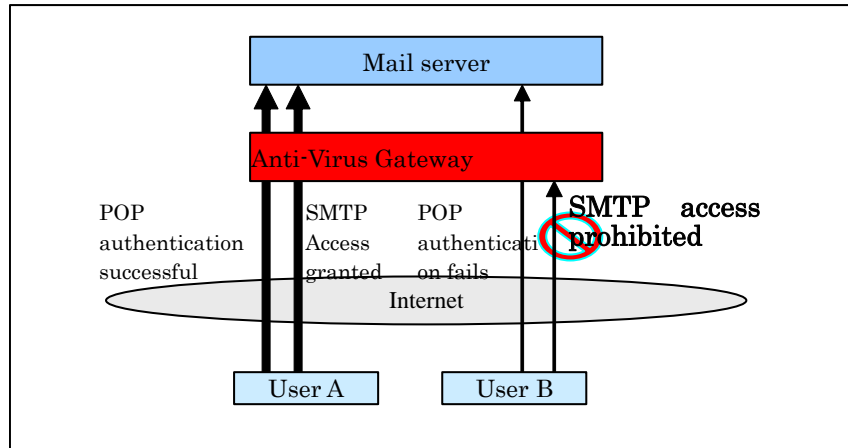


Note

Due to protocol specifications, you cannot use APOP if **Defining parent server by user** is enabled. If you want to use APOP, make sure that you do either of the following:

- Turn off **Defining parent server by user**.
You can do this in the web console.
POP proxy > Defining parent server by user: **Off**
- Use a transparent proxy.
For more information about using a transparent proxy, see "*Transparent Proxy*", 108.

10.1.5 Authentication using POP-before-SMTP



SMTP services can be accessed using POP-before-SMTP. If POP-before-SMTP is used, user authentication for a POP connection is performed before a SMTP service is accessed. Access to the SMTP service is limited to IP addresses that have passed POP authentication within a specified time. In addition, POP-before-SMTP authentication is performed in F-Secure Internet Gatekeeper for Linux. This is because the IP address of the product is always assigned to the IP address of the sender's mail server.

To use POP-before-SMTP authentication, configure the SMTP and POP services in the following way.

Proxy Settings

Proxy settings

SMTP proxy: **On**

Global settings

POP-before-SMTP authentication: **On**

Timeout: Specify the time in minutes during which the authentication is effective
(Example: 2)

POP proxy: **On**

The following settings allow services without authentication to clients within the LAN and to senders from specific mail servers, addresses and networks:

Proxy settings

SMTP proxy

LAN access settings: **On**

Hosts and networks within LAN: **Specify allowed clients**

(Clients within the LAN, mail servers, etc.)

Because e-mails from the Internet are delivered to mail servers through the product, the corresponding mail servers must be allowed to deliver without authentication. The following describes how you can configure this:

Proxy settings

SMTP proxy

Restrict e-mail recipients: **On / Specify mail server domains**

The database file for POP-before-SMTP is stored in the following way:

Database format : BerkeleyDB 1.85
Directory : Temporary directory (Default: /var/tmp/fsigk)
File name : pbs.db
Key : Client IP address
Data : POP authentication time (seconds elapsed from epoch time (1970/1/1 00:00:00))



Note

You can check information on the current database by running “db1_dump -p pbs.db” and other commands.



Caution

Every time a service is restarted, all the information in the database for POP-before-SMTP is deleted.

10.2 Transparent Proxy

F-Secure Internet Gatekeeper for Linux can work as a transparent proxy for each service (HTTP, FTP, SMTP, POP). In this way, you can perform virus scans for services without having to change settings for each user.

The following table displays which settings you need to change for the product to work as a transparent proxy. The settings apply when the host name of the mail server is assigned to the host name of Internet Gatekeeper (through proxy and DNS settings).

				Proxy mode		Transparent proxy mode	
				Install phase only	Mail server DNS change	Router	Bridge
Client settings	POP	User name	Specific server	○	○	○	○
			Any server	×	×	○	○
		Server host name	Specific server	×	○	○	○
			Any server	×	×	○	○
	SMTP	Server host name	Specific server	×	○	○	○
			Any server	N/A	N/A	○	○
	HTTP/FTP	Proxy server name		×	×	○	○
Cancel a virus scan			Yes	Yes	N/A	N/A	
Network settings	DNS			○	×	○	○
	Routing			○	○	×	○
Proxy Settings	Parent server setting			×	×	○	○
	IP address setting			×	×	×	×
	NAT (iptables) setting			○	○	×	×
	Kernel setting			○	○	○	×

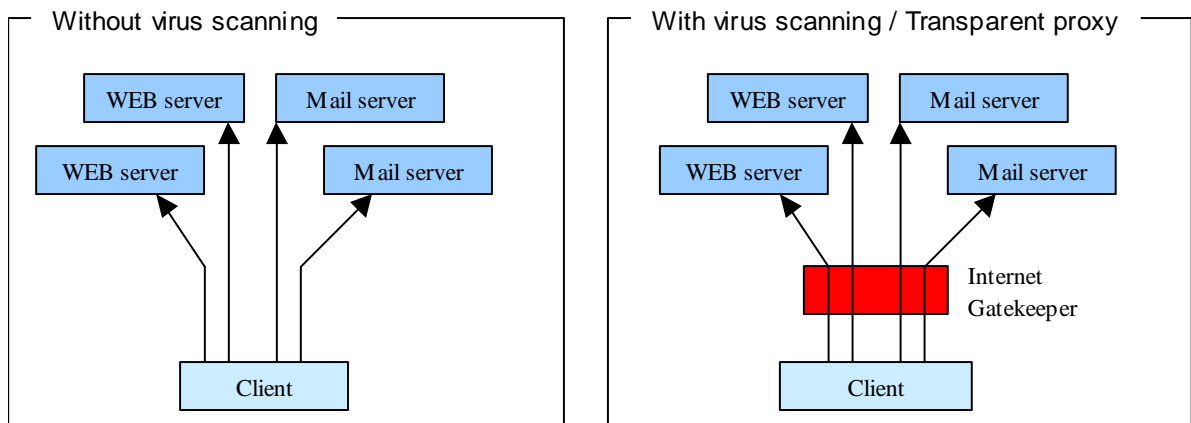
10.2.1 Transparent Proxy Details

Normally, clients access web servers and mail servers directly.

To use F-Secure Internet Gatekeeper for Linux as a transparent proxy, you must install it on the IP routing between clients and servers.

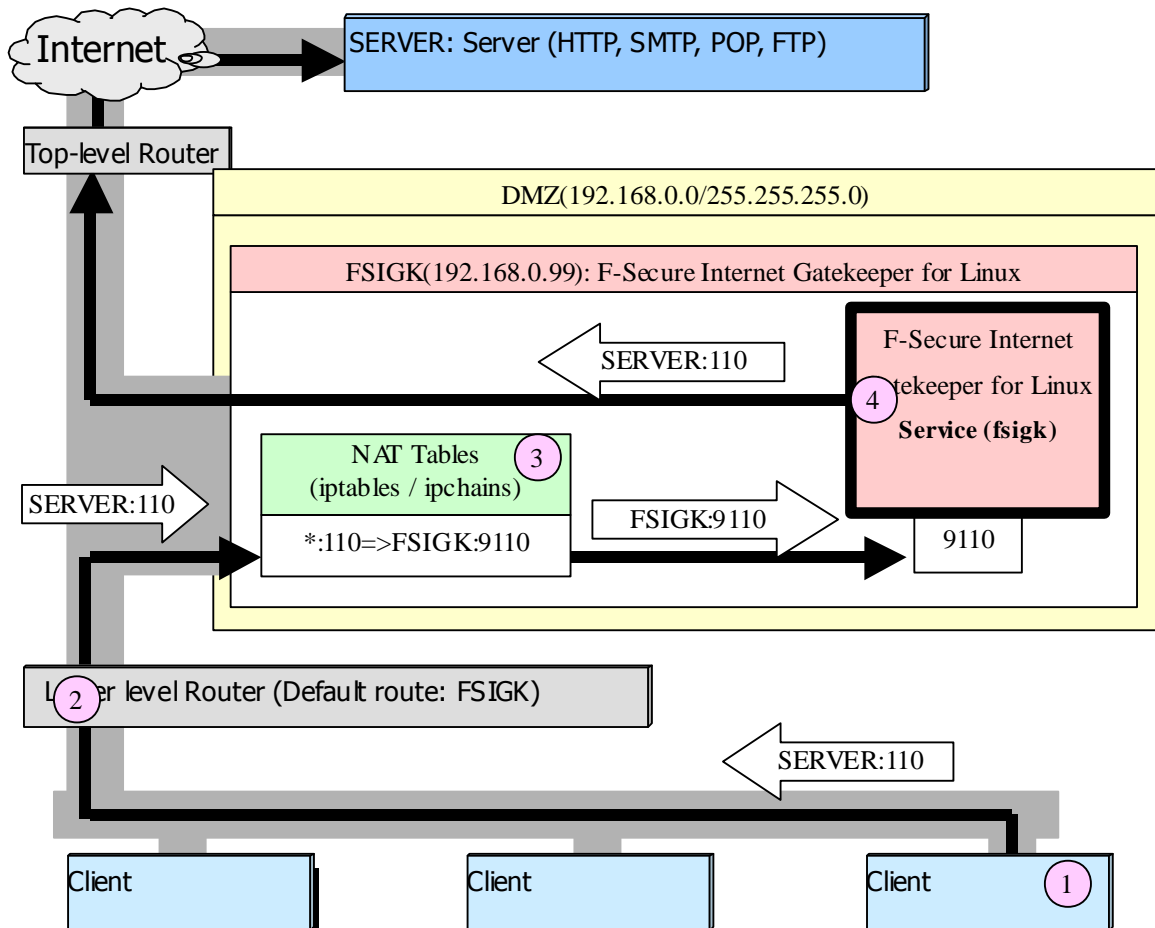
The product relays the access and performs a virus scan during the relay by capturing connections from clients to servers and by creating another connection to servers. In this way, clients can directly access servers, and clients' traffic is scanned, without having to change the client configuration.

Setting Example



10.2.2 Transparent Proxy – Router Mode

To function as a transparent proxy in router mode, you must install Internet Gatekeeper on a computer, which acts as a router between the clients and the servers. This diagram below illustrates how to set up the product as a transparent proxy in a DMZ network.



Overview of operations:

The following describes how clients connect to servers when F-Secure Internet Gatekeeper for Linux is set up as a transparent proxy:

- 1 The client starts a connection to a service port (example 110) of a server (SERVER).
- 2 The NAT (lower-level) router relays the access request from the client to F-Secure Internet Gatekeeper for Linux (FSIGK) that is set on the default route.
- 3 FSIGK redirects the access request from the client to FSIGK:9110 on the basis of the NAT setting in iptables, and stores the original access destination (SERVER:110).
- 4 FSIGK listens to the access at VIRUS:9110 and retrieves the access request replaced by iptables. Afterwards, Internet Gatekeeper retrieves the original destination (SERVER:110) which has been stored in iptables and sends the access request to the original destination (SERVER:110).

Settings

To use a transparent proxy in proxy mode, configure the network and server associated with F-Secure Internet Gatekeeper for Linux in the following way:

- 1 Open the web console. Select **Proxy settings** and then start up each service in transparent proxy mode:

Proxy Settings

Proxy settings

HTTP proxy: **On**

Port Number: **9080**

Transparent proxy: **On**

SMTP proxy: **On**

Proxy port: **9025**

Transparent proxy: **On**

POP proxy: **On**

Proxy port: **9110**

Transparent proxy: **On**

FTP proxy: **On**

Proxy port: **9021**

Transparent proxy: **On**

After configuring the settings, check that the client can access the port of each service (9080, 9025, 9110, 9021) on Internet Gatekeeper.

2 Change the access destination of the client to FSIGK:9110 by changing iptables on Internet Gatekeeper.

- Configuring the web console:

From the web console, select “HTTP”, “SMTP”, “POP”, or “FTP” from the “Proxy settings” menu. Select **Edit NAT (iptables) redirect settings** in “Transparent proxy”.

On the “Edit NATA (iptables) redirect settings” page, check that NAT redirect is enabled for each service. Click **Save**. Store the settings with the following command:

```
/etc/rc.d/init.d/iptables save
```

- Configuring with the iptables command:

Run the following commands to make sure that iptables is operating normally and unneeded ipchains are not working:

```
FSIGK# /etc/rc.d/init.d/ipchains stop
FSIGK# chkconfig ipchains off
FSIGK# /etc/rc.d/init.d/iptables restart
```

Next, run the following commands to redirect the server access to each service (http(80), smtp(25), pop(110), ftp(21)) to 9080, 9025, 9110, 9021 of FSIGK:

```
FSIGK# iptables -t nat -A PREROUTING ¥
        -p tcp --dport 80 -j REDIRECT --to-port 9080
FSIGK# iptables -t nat -A PREROUTING ¥
        -p tcp --dport 25 -j REDIRECT --to-port 9025
FSIGK# iptables -t nat -A PREROUTING ¥
        -p tcp --dport 110 -j REDIRECT --to-port 9110
FSIGK# iptables -t nat -A PREROUTING ¥
        -p tcp --dport 21 -j REDIRECT --to-port 9021
```

Save the settings by running the following command:

```
FSIGK# /etc/rc.d/init.d/iptables save
```

Note! See your Linux distribution documentation for information on how to store and modify iptables.



Note

You can change the iptable settings also by running the following command:

```
/opt/f-secure/fsigk/misc/rc.transparent
```

After setting the iptables, check that Internet Gatekeeper that uses the converted port (FSIGK:9080, FSIGK:9025, FSIGK:9110, FSIGK:9021) can be accessed when a client accesses the pre-converted service (FSIGK:80, FSIGK:25, FSIGK:110, FSIGK:21).

- 3 Change the default route of the NAT (lower-level) router to FSIGK to let all data communication pass through FSIGK.

If the router is running Linux, run the following commands:

```
NAT-router# route del -net default
NAT-router# route add -net default gw 192.168.0.99
```

To apply the settings after restart, change the GATEWAY variables (`/etc/sysconfig/network`, `/etc/sysconfig/network-scripts/ifcfg-eth0`) in the NAT router. Save the settings.

Check that Internet Gatekeeper (FSIGK: 9080, FSIGK: 9025, FSIGK: 9110, FSIGK: 9021) can accept access from clients to all server services (http(80), smtp(25), pop(110), ftp(21)).

- 4 To enable communication (other than virus scans) for services (http, smtp, pop, ftp) on FSIGK, run the following command, which enables routing:

```
FSIGK# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Make the following change to `/etc/sysctl.conf` in FSIGK to enable routing after restart.

```
net.ipv4.ip_forward = 1
```

Check that communication from clients is possible.

- 5 Check that virus scans can be performed when a client accesses a server.



Caution

When a service accesses a server from Internet Gatekeeper, the IP address of the product is normally assigned as the IP address of the service source.

For FTP data sessions, in Passive mode, the destination address from the client and the source address from Internet Gatekeeper to the server are usually assigned to the address of the product. In Active mode, the destination address from the server and the source address from Internet Gatekeeper to the client are usually assigned to the address of the product. If FTP communication cannot be used, check if it is denied by a firewall.

When accessing a server from Internet Gatekeeper or when an IP address needs to be retained during a FTP data session, the kernel needs to be patched with `tproxy`.

➊ For more information, see "`transparent_tproxy`" in the separate "`Expert options`" document.



Caution

Configure the settings so that the communication files and tasks used by the firewall settings of Linux (iptables) are not denied.

The following communication chains must be allowed:

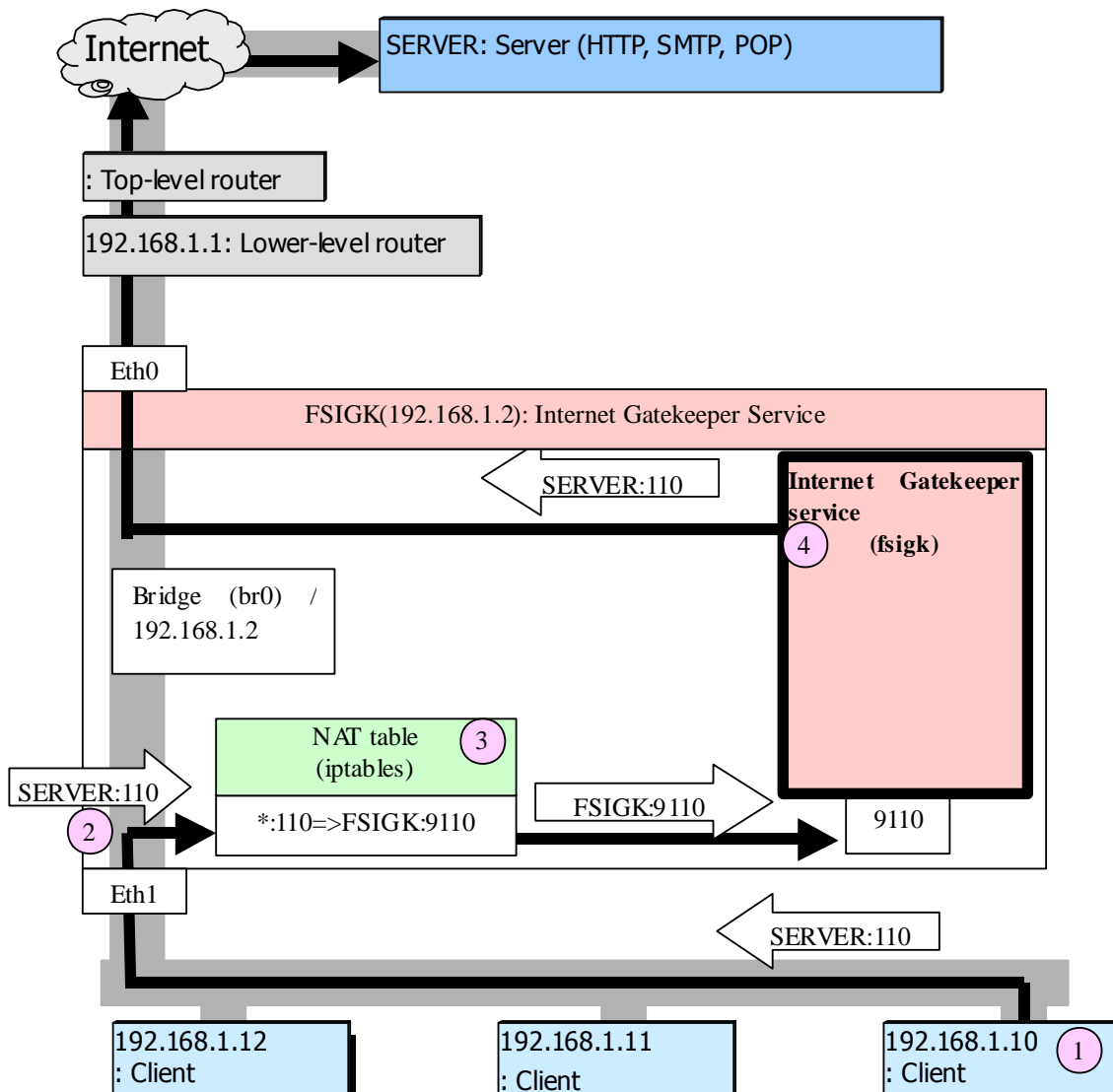
- All communication by the OUTPUT chain
- All communication by the FORWARD chain
- Communication to the listen ports used by Internet Gatekeeper (9080,9025,9110,9021) for the INPUT chain. Data session communication rules relating to FTP (if FTP is used)

If there are communication errors, disable the firewall and check the communication status.

10.2.3 Transparent Proxy – Bridge Mode

F-Secure Internet Gatekeeper for Linux can also operate as a bridge while acting as a transparent proxy. If you configure the product in bridge mode, virus scanning functions can be provided to clients without having to change any settings on clients and networks.

In order to set up a transparent proxy in bridge-mode, you need to set up an Internet Gatekeeper computer that has 2 or more interfaces and place it between clients and servers. You may need to recompile the Linux kernel if the bridging functionality is not enabled by default in your distribution, or if you use Linux version 2.4. Because the product works as a bridge, both of the interfaces, while on different physical networks, are on the same logical IP network.



Overview of operations:

The following describes how clients connect to servers when F-Secure Internet Gatekeeper for Linux is set up as a transparent proxy:

- 1 The client starts a connection to a service port (example 110) of a server (SERVER).
- 2 Access requests from clients pass through F-Secure Internet Gatekeeper for Linux, which is placed as a bridge between clients and the NAT (lower-level) router.
- 3 FSIGK redirects the access request from the client to FSIGK:9110 based on the NAT setting in iptables and stores the original access destination (SERVER:110).
- 4 FSIGK listens to the access at VIRUS:9110 and retrieves the access request replaced by iptables. Afterwards, Internet Gatekeeper retrieves the original destination (SERVER:110), which is stored in iptables, and sends the access request to the original destination (SERVER:110).

Settings

To use a transparent proxy in bridge mode, configure the network and server associated with F-Secure Internet Gatekeeper for Linux in the following way:

- 1 Open the web console. Select Proxy settings. Start up each service in transparent proxy mode:

Proxy settings

HTTP proxy	: On
Proxy port	: 9080
Transparent proxy	: On
SMTP proxy	: On
Proxy port	: 9025
Transparent proxy	: On
POP proxy	: On
Proxy port	: 9110
Transparent proxy	: On
FTP proxy	: On
Proxy port	: 9021
Transparent proxy	: On

After configuring the settings, check that the client can access the port of each service (9080, 9025, 9110, 9021) on Internet Gatekeeper.

- 2 If you use Linux kernel 2.4, apply a patch to the kernel and recompile with the following settings. If you use Linux kernel 2.6, you do not need to perform the following steps (recompiling the kernel).

- **Required Software:**

[OS] Linux 2.4.21 (or later)

(The Linux Kernel Archives: <http://www.kernel.org/>)

[ebtables + br-netfilter (kernel patch)] ebttables-brnf_vs_2.4.21.diff.gz (or later)

(ebtables: <http://ebtables.sourceforge.net/>)

- **Kernel settings:**

[Code maturity level options]=[Prompt for development and/or incomplete code/drivers] : ON

[Network Options]=[Network packet filtering (replaces ipchains)] : ON

[Network Options]=[IP: Netfilter Configurations] : Set all ON

[Network Options]=[802.1d Ethernet Bridging] : ON

- 3 To set the bridge, change the IP address, netmask, default root, and interface name in `/opt/f-secure/fsigk/misc/rc.bridge` and launch the bridge as a startup script. You need the `brctl` command to set the bridge. If it is not available, install a package which includes the `brctl` command (for example, the “bridge-utils” package).



Note

If a subnet exists under the network structure, apply routing settings as needed.

```
# cp /opt/f-secure/fsigk/misc/rc.bridge /etc/rc.d/init.d/bridge
# /etc/rc.d/init.d/bridge start
# chkconfig --add bridge
```

Check that communication works between interfaces (`eth0,eth1`) on both sides.

- 4 Change the access destination of the client to FSIGK:9110. Do it on the server at the access destination by changing iptables on Internet Gatekeeper.

Next, run the following commands to redirect the server access to each service (`http(80)`, `smtp(25)`, `pop(110)`, `ftp(21)`) to 9080, 9025, 9110, 9021 of FSIGK.

```
FSIGK# iptables -t nat -A PREROUTING ¥
      -p tcp --dport 80 -j REDIRECT --to-port 9080
FSIGK# iptables -t nat -A PREROUTING ¥
      -p tcp --dport 25 -j REDIRECT --to-port 9025
FSIGK# iptables -t nat -A PREROUTING ¥
      -p tcp --dport 110 -j REDIRECT --to-port 9110
FSIGK# iptables -t nat -A PREROUTING ¥
      -p tcp --dport 21 -j REDIRECT --to-port 9021
```

Save the settings by running the following command:

```
FSIGK# /etc/rc.d/init.d/iptables save
```



Note

You can make iptable setting changes also by running the following command:
`/opt/f-secure/fsigk/misc/rc.transparent`

5 Check that virus scans can be performed when a client accesses a server.



Caution

When a service accesses a server from Internet Gatekeeper, the IP address of the product is normally assigned as the IP address of the service source. For this reason, the IP address and routing settings must be applied to the Internet Gatekeeper server.

For FTP data sessions, in Passive mode, the destination address from the client and the source address from Internet Gatekeeper to the server are usually assigned to the address of the product. In Active mode, the destination address from the server and the source address from the Internet Gatekeeper to the client are usually assigned to the address of the product. If FTP communication cannot be used, check if it is denied by a firewall.

When Internet Gatekeeper accesses a server, or when an IP address needs to be retained during a FTP data session, the kernel needs to be patched with tproxy.

➔ For more information, see "[transparent_tproxy](#)" in the separate "[Expert options](#)" document.



Caution

Configure the settings so that the communication files and tasks used by the firewall settings of Linux (iptables) are not denied.

The following communication chains must be allowed:

- All communication by the OUTPUT chain
- All communication by the FORWARD chain
- Communication to the listen ports used by Internet Gatekeeper (9080, 9025, 9110, 9021) for the INPUT chain. Data session communication rules relating to FTP (if FTP is used)

If there are communication errors, disable the firewall and check the communication status.



Note

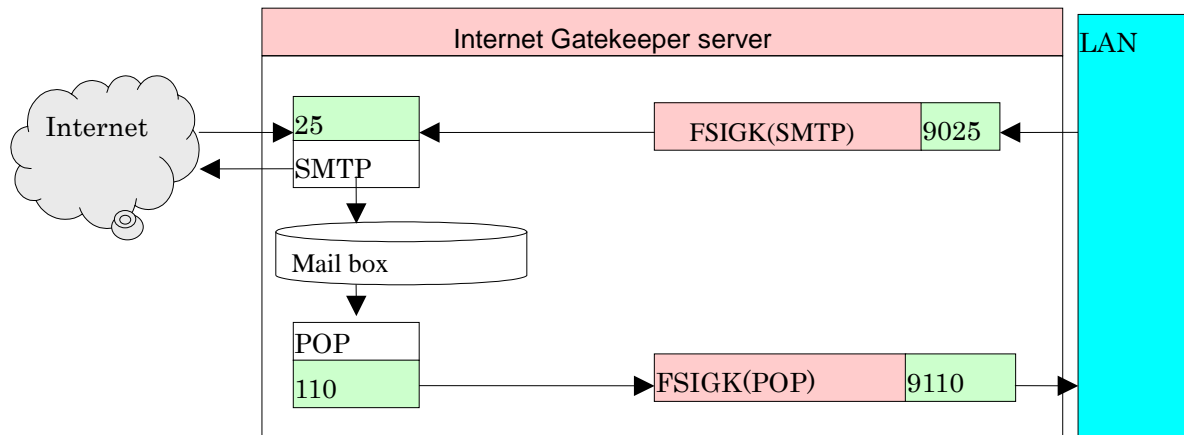
Reference URLs:

- Net:Bridge – The Linux Foundation
<http://www.linux-foundation.org/en/Net:Bridge>
- ebttables
<http://ebtables.sourceforge.net/>

10.3 Coexisting with mail servers

F-Secure Internet Gatekeeper for Linux can operate in the same computer as the mail server. If the product is implemented in the same computer as a mail server, you must change the IP address or the normal port number (25 or 110) of either the mail server or the product. We recommend that you change the port number of Internet Gatekeeper instead of the mail server.

10.3.1 Changing the Port Number of Internet Gatekeeper



If you specify a different port number for Internet Gatekeeper, it is possible to use the product and a mail server in the same computer. The following example uses ports 9025 and 9110 for Internet Gatekeeper.

Settings for F-Secure Internet Gatekeeper for Linux

Set the port numbers used by the product to 9025 and 9110 at the web console:

Proxy settings

SMTP proxy

Proxy port: **9025**

Parent server: (Host name: **localhost** , Port number: **25**)

POP proxy

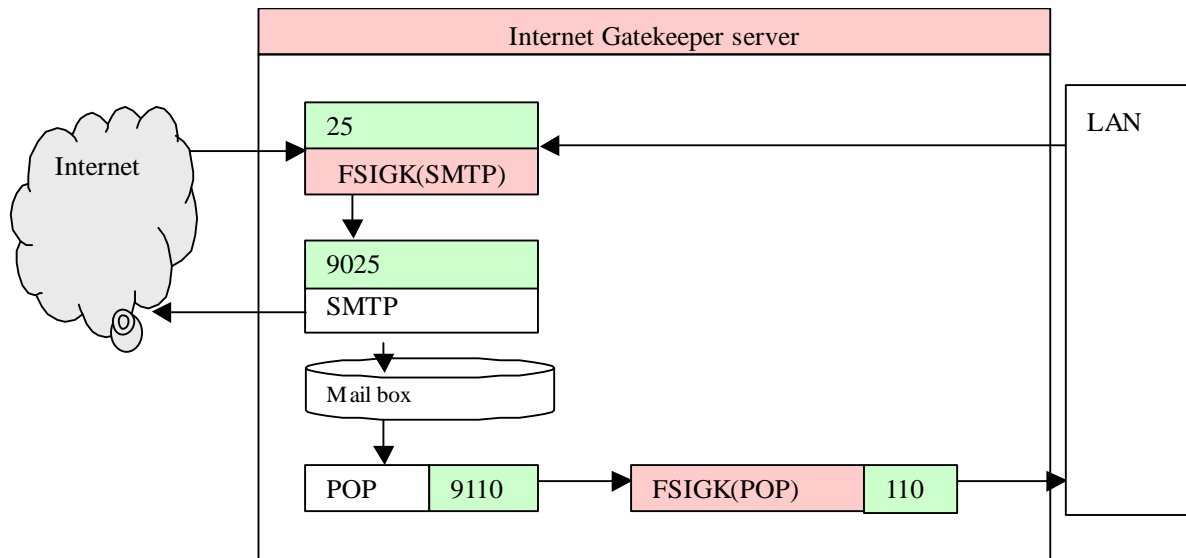
Proxy port: **9110**

Parent server: (Host name: **localhost** , Port number: **110**)

Client settings

Set the port numbers used by the SMTP and POP servers to 9025 and 9110.

10.3.2 Changing the Port Number of the Mail Server



If you specify a different port number for the mail server, it is possible to use the product and a mail server in the same computer. The following example uses ports 9025 and 9110 for the mail server. Because virus scans are performed using SMTP, Internet Gatekeeper does not need the POP settings, and they can be skipped.

Mail server settings

Change the SMTP server port to 9025, and the POP server port to 9110.

- **Using sendmail:**

- 1 Make the following change in `/etc/sendmail.cf` or `/etc/mail/sendmail.cf`.

```
O DaemonPortOptions=Port=9025
```

- 2 Restart sendmail.

```
# /etc/rc.d/init.d/sendmail restart
```

- **Using ipop3d + xinetd:**

- 1 Make the following change in `/etc/xinetd.d/ipop3`.

```
port = 9110
```

- 2 Restart xinetd.

```
# /etc/rc.d/init.d/xinetd restart
```

- **Using qmail+tcpserver:**

Make the following change in `/var/qmail/rc`.

```
/usr/local/bin/tcpserver -R -x /etc/tcp.smtp.cdb -u qmaild -g qmail 0 9025 ¥
/var/qmail/bin/qmail-smtpd | /var/qmail/bin/splogger smtpd 3 &
```

- **Using qmail-popup + xinetd:**

- 1 Make the following change in `/etc/xinetd.d/qmail-popup`.

```
port = 9110
```

- 2 Restart xinetd.

```
# /etc/rc.d/init.d/xinetd restart
```

- **Using postfix:**

- 1 Set the smtpd service port in `/etc/postfix/master.cf` as follows:

```
9025 inet n - n - - smtpd
```

- 2 Restart postfix.

```
# postfix reload
```

Settings for F-Secure Internet Gatekeeper for Linux

Set the port numbers of the parent server to 9025 and 9110 at the web console:

Proxy settings

SMTP proxy: **On**

Proxy port: **25**

Global settings

Parent server

Host name: **localhost**

Port number: **9025**

POP proxy: **On**

Proxy port: **110**

Parent server:

Host name: **localhost**

Port number: **9110**

If e-mails are to be received from the outside, restrict the recipient domains to prevent third-party relays. The following example restricts mail to `your_domain1.com` and `your_domain2.com`.

Proxy settings

SMTP proxy

Global settings

Restrict e-mail recipients: **your_domain1.com your_domain2.com**

As outbound access is denied by restricting recipient domains, allow access from clients within the LAN. The following example enables IP addresses specified in 192.168.1.xxx and 192.168.2.xxx.

Proxy settings

SMTP proxy

LAN access settings: **On**

Hosts and networks within LAN: **192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0**

The following example uses POP-before-SMTP to enable data to be sent outside:

Proxy settings

SMTP proxy: **On**

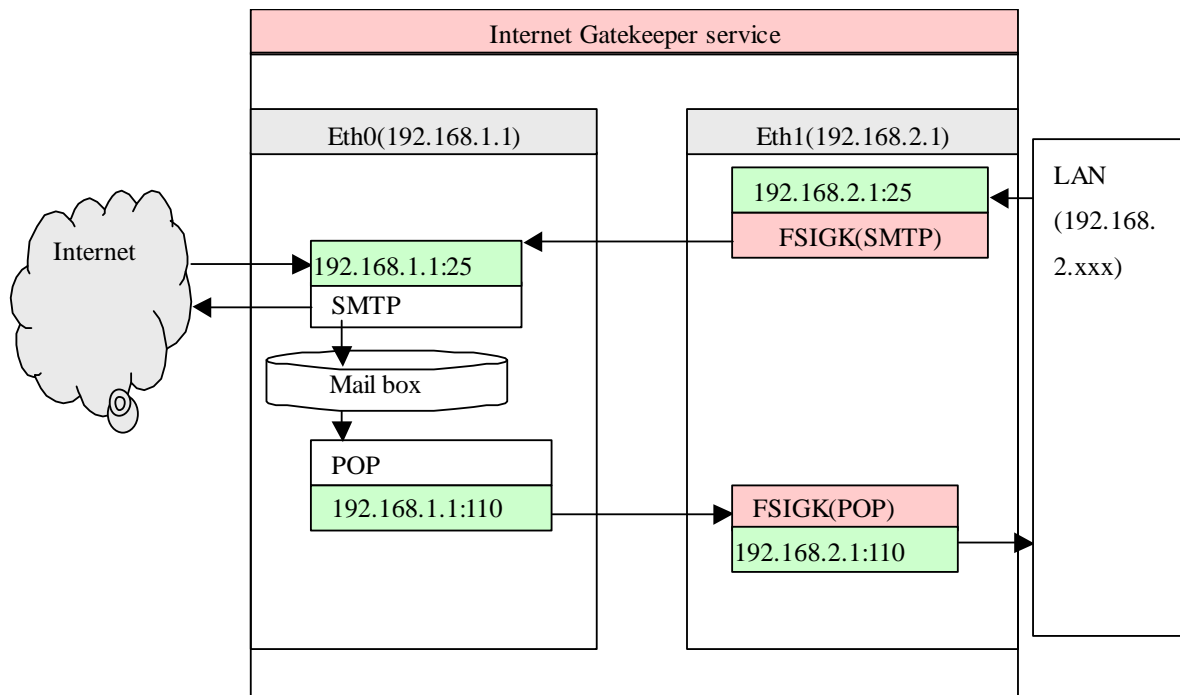
Global settings

POP-before-SMTP authentication: **On**

POP proxy: **On**

If the mail server performs SMTP authentication, you do not have to change any settings.

10.3.3 Changing the IP Address



If F-Secure Internet Gatekeeper for Linux and a mail server use a different interface (IP address), it is possible to use the product and a mail server in the same computer with the same port number. In the following example, the mail server listens to eth0 (192.168.1.1) and Internet Gatekeeper listens to eth1 (192.168.2.1).

If you only have one physical interface, you can generate a virtual interface with the IP Alias function. For example, the following command generates the virtual interface "eth0:1(192.168.1.2)":

```
# ifconfig eth0:1 192.168.1.2 netmask 255.255.255.0
```

Copy `/etc/sysconfig/network-scripts/ifcfg-eth0` to `ifcfg-eth0:1` and rewrite the file to `DEVICE="eth0:1"`. Set the `IPADDR`, `NETMASK`, `NETWORK`, and `BROADCAST` variables in the file.

Mail server settings

Set the listening interface of the mail server to `eth0(192.168.1.1)`.

- **Using sendmail:**

- 1 Make the following change in `/etc/sendmail.cf` or `/etc/mail/sendmail.cf`.

```
O DaemonPortOptions=Port=smtp,Addr=192.168.1.1
```

- 2 Restart sendmail.

```
# /etc/rc.d/init.d/sendmail restart
```

- **Using ipop3d + xinetd:**

- 1 Make the following change in `/etc/xinetd.d/ipop3`.

```
bind=192.168.1.1
```

- 2 Restart xinetd.

```
# /etc/rc.d/init.d/xinetd restart
```

- **Using qmail+tcpserver:**

Make the following changes in `/var/qmail/rc`.

```
/usr/local/bin/tcpserver -R -x /etc/tcp.smtp.cdb -u qmaild -g qmail 192.1.168.1.1 25 ¥  
/var/qmail/bin/qmail-smtpd | /var/qmail/bin/splogger smtpd 3 &
```

- **Using qmail-popup + xinetd:**

- 1 Make the following change in `/etc/xinetd.d/qmail-popup`.

```
bind=192.168.1.1
```

- 2 Restart xinetd.

```
# /etc/rc.d/init.d/xinetd restart
```

- **Using postfix:**

- 1 Set the smtpd service address in `/etc/postfix/master.cf` as follows:

```
192.168.1.1:25 inet n - n - - smtpd
```

- 2 Restart postfix.

```
# postfix reload
```

Settings for F-Secure Internet Gatekeeper for Linux

Set the port numbers of the parent server to 192.168.2.1.25 and 192.168.2.1.110. Specify the parent server to be the mail server (192.168.1.1:25, 192.168.1.1:110) at the web console.

Proxy settings

SMTP proxy: **On**

Proxy port: **192.168.2.1:25**

Global settings

Parent server:

Host name: **192.168.1.1**

Port number: **25**

POP proxy: **On**

Proxy port: **192.168.2.1:110**

Parent server:

Host name: **192.168.1.1**

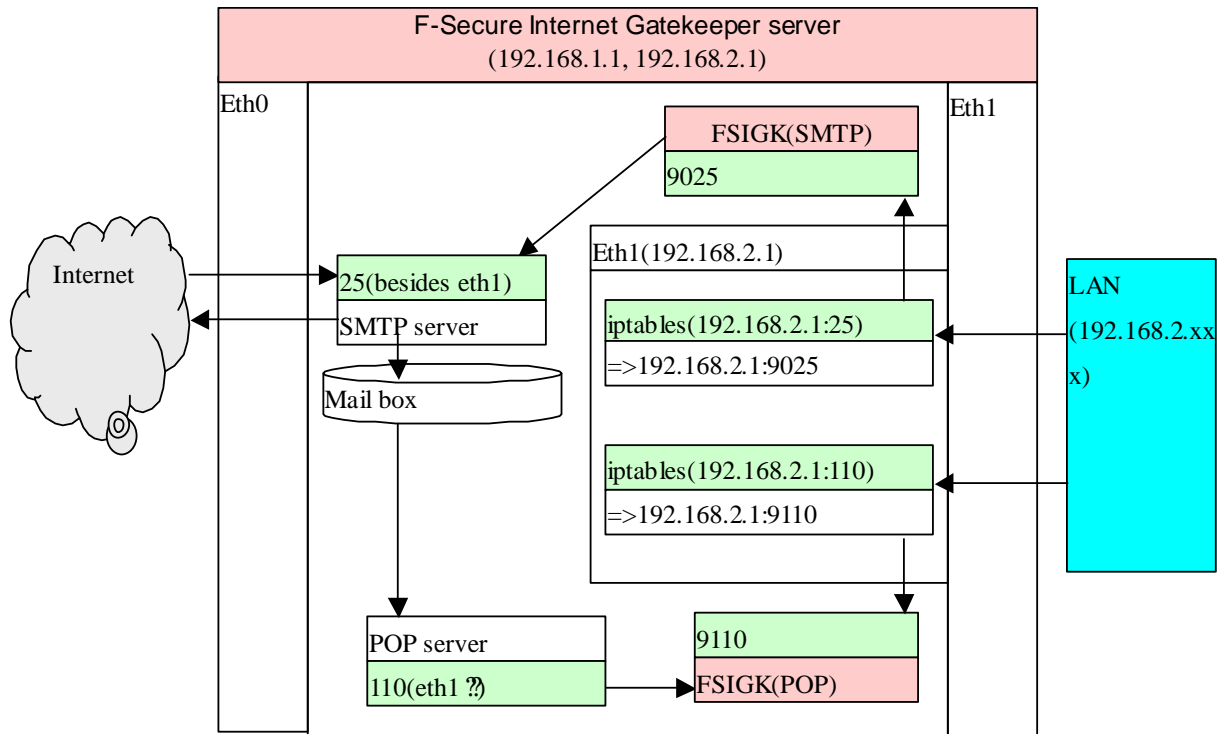
Port number: **110**

Client settings

Set the mail server to 192.168.2.1.

Make sure that the client can send and receive mails.

10.3.4 Changing IP Addresses with iptables



If F-Secure Internet Gatekeeper for Linux and a mail server use a different interface, it is possible to use the product and a mail server in the same computer with the same port number. You can redirect the access to default ports (25, 100) in specific interfaces to Anti-Virus (9025, 9110). You can do it with the NAT setting in the iptables.

The following example uses two interfaces, eth0 (192.168.1.1) and eth1 (192.168.2.1). Access from eth1 ports 25 and 110 is changed to ports 9025 and 9110. The eth1 interface is used for Internet Gatekeeper, and the eth0 interface (and localhost) is used for the mail server access.

If you have only one physical interface, you can generate a virtual interface with the IP Alias function. For example, the following command generates the virtual interface "eth0:1(192.168.1.2)":

```
# ifconfig eth0:1 192.168.1.2 netmask 255.255.255.0
```

Copy /etc/sysconfig/network-scripts/ifcfg-eth0 to ifcfg-eth0:1 and rewrite the file to DEVICE="eth0:1". Set the IPADDR, NETMASK, NETWORK, and BROADCAST variables in the file.

iptables setting for the Gateway server

Follow these instructions to redirect the access to ports 25 and 110 of eth1 (192.168.2.1) to 9025 and 9110.

- iptables – commands:

```
# iptables -t nat -A PREROUTING -d 192.168.2.1 -p tcp --dport 25 -j REDIRECT
¥
    --to-port 9025
# iptables -t nat -A PREROUTING -d 192.168.2.1 -p tcp --dport 110 -j REDIRECT
¥
    --to-port 9110
# /etc/rc.d/init.d/iptables save
```

Settings for F-Secure Internet Gatekeeper for Linux

Set the port numbers of the parent server to 9025 and 9110, and the parent server to be the mail server (localhost:25, localhost:110) at the web console.

Proxy settings

SMTP proxy: **On**

Proxy port: **9025**

Global settings

Parent server

Host name: **localhost**

Port number: **25**

POP proxy: **On**

Proxy port: **9110**

Parent server:

Host name: **localhost**

Port number: **110**

Client settings

Set the mail server to 192.168.2.1.

Make sure that the client can send and receive mails.

10.4 Scanning Viruses Before Saving Mail to the Mail Server

By default, virus scans are performed on all inbound e-mails that are sent to the mail server by using the specified POP protocol. For this reason, you do not need to make any changes to the mail server. It is also possible to check inbound e-mails in SMTP before they are saved to the mail server. The following example uses a single F-Secure Internet Gatekeeper for Linux server to check both outbound and inbound e-mails for viruses.

Overview of operations:

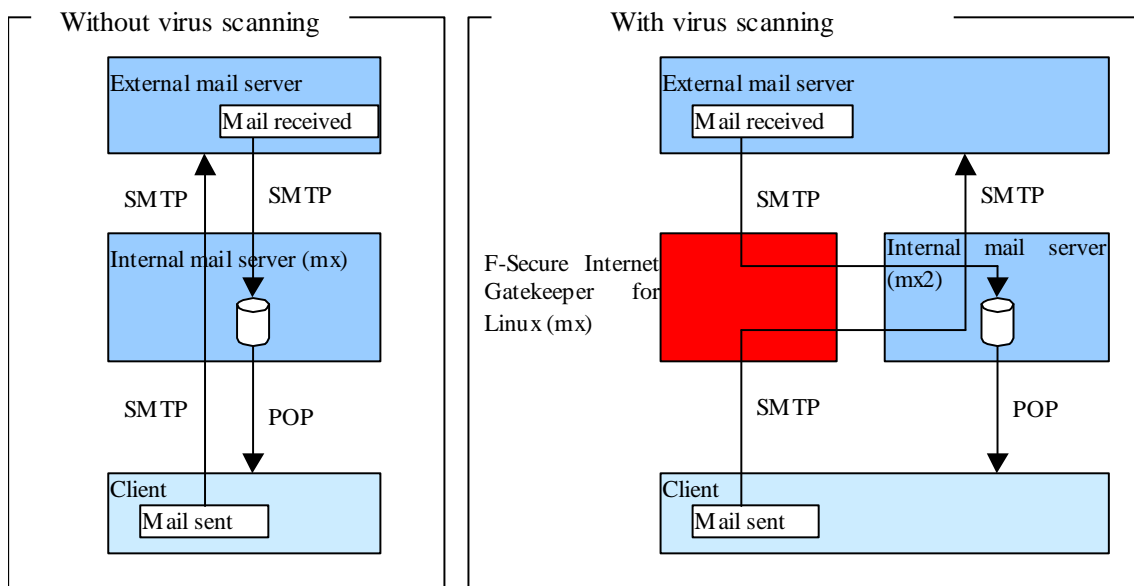
- **Without virus scanning**

If F-Secure Internet Gatekeeper for Linux is not implemented, outbound e-mails are transferred through an internal mail server to the destination mail server. Inbound e-mails are stored in an internal mail server, and users can retrieve them by using the POP protocol.

- **With virus scanning**

If F-Secure Internet Gatekeeper for Linux is implemented, the product scans outbound e-mails for viruses. After that the e-mails are delivered to the destination mail server by using the internal mail server. After the product has scanned inbound e-mails for viruses, the e-mails are stored on an internal mail server. Users can retrieve them by using the POP protocol. In addition, restrictions are applied to outbound e-mails to prevent open relays (third-party relays) and e-mail abuse.

Setting Example



Settings

- 1 Set up F-Secure Internet Gatekeeper for Linux under a temporary host name (virus-gw) and apply the following proxy settings:

Proxy settings

SMTP proxy: **On**

Proxy port: **25**

Global settings

Parent server:

Host name: **<IP address of internal mail server>**

Port number: **25**

Restrict e-mail recipients: **On**

/ <Domain name of internal e-mail accounts>

(Example: example.com)

LAN access settings: **On**

Hosts and networks within LAN: **<Hosts within LAN>**

(Example: 192.168.1.0/255.255.255.0)

192.168.2.0/255.255.255.0)

- 2 Configure the internal mail server so that e-mails from virus-gw can be sent to other mail servers.

- **Using sendmail:**

- ① Add the following line to `/etc/mail/access`:

```
<IP address of virus-gw (Example: 192.168.0.99)> RELAY
```

- ② Run `make` at `/etc/mail`.

```
# cd /etc/mail/ ; make
```

- ③ Restart sendmail.

```
# /etc/rc.d/init.d/sendmail restart
```

- **Using qmail+tcpserver:**

- ① Make the following changes in `/var/qmail/rc`.

```
/usr/local/bin/tcpserver -R -x /etc/tcp.smtp.cdb -u qmaild -g qmail 0 smtp ¥  
/var/qmail/bin/qmail-smtpd | /var/qmail/bin/splogger smtpd 3 &
```

- ② Make the following changes in `/etc/tcp.smtp`.

```
<IP address of virus-gw (Example: 192.168.0.99)>:allow,RELAYCLIENT=""  
<Network within LAN (Example: 192.168.1.)>:allow,RELAYCLIENT=""  
:allow
```

- ③ Convert to `cdb` format with the following command:

```
# tcprules tcp.smtp.cdb tcp.smtp.tmp < tcp.smtp
```

- **Using postfix:**

① Add the following line to `/etc/postfix/main.cf`:

```
mynetworks=<IP address of virus-gw (Example: 192.168.0.99)>,<Network  
within LAN  
(Example: 192.168.1.0/24.)>
```

② Restart postfix.

```
# postfix reload
```

- 3 Check that e-mails can be sent from the internal network to an external mail server by using virus-gw. Check also that outbound e-mails are limited to the specified domain.
- 4 Change the host name of the internal mail server to "mx2" and the host name of Internet Gatekeeper to "mx" in the DNS settings. Change the mail server (MX record of DNS) of the internal domain to "mx" (Internet Gatekeeper).
- 5 Check that e-mails can be sent from the internal network to an external mail server by using mx. Check also that outbound e-mails are limited to the specified domain.
- 6 After the DNS cache has expired, check that e-mails can be sent internally through external mail servers. In addition, check that inbound and outbound e-mails are scanned for viruses.

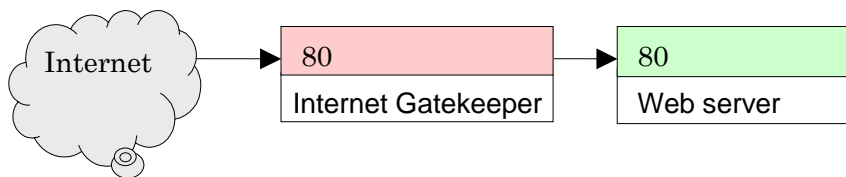
10.5 Reverse Proxy Settings

F-Secure Internet Gatekeeper for Linux can be set up as a reverse proxy to scan connections from a client to a specific web server.

It is also possible to implement the product as a transparent proxy, which makes it possible for a single Internet Gatekeeper to scan multiple web servers. To implement a transparent proxy, see “*Transparent Proxy*”, 108.

10.5.1 Reverse Proxy – Typical Settings

If the product is implemented both on a web server and on a separate server, it must be placed in front of the web server for it to appear as a web server on the Internet. The following diagram illustrates the setting.



Internet Gatekeeper settings

At the web console, configure the proxy port and parent server port to 80:

Proxy settings

HTTP proxy: **On**

Proxy port: **80**

Parent server:

Host name: **Web server**

Port number: **80**

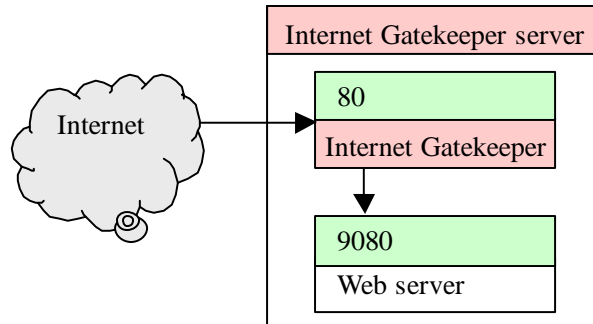
DNS/Web Server settings

Set the IP address (as seen from the Internet) of the web server to the address of the Gateway. You can do this by using one of the methods below:

- **Method 1 – Change the IP address at the web server**
Change the IP address of the previous web server. Set the previous IP address as the IP address of the product.
- **Method 2 – Change the IP address assigned to the web server by using the DNS server**
Using the DNS settings, set the IP address (as seen from the Internet) of the web server as the address of Internet Gatekeeper.

10.5.2 Coexisting with Web Servers

F-Secure Internet Gatekeeper for Linux can operate in the same computer as a web server. By specifying a different port number for the web server, it is possible to use the product and a web server in the same computer. The following example uses ports 9080 for the web server.



Web Server settings

Change the HTTP server port to 9080.

- **Using Apache**

- 1 Make the following change in `/etc/httpd/conf/httpd.conf`.

```
Listen 9080
```

- 2 Restart Apache.

```
# /etc/rc.d/init.d/httpd restart
```

Internet Gatekeeper settings

At the web console, configure the proxy port and parent server port to 80.

Proxy settings

HTTP proxy: **On**

Proxy port: **80**

Parent server:

Host name: **localhost**

Port number: **9080**

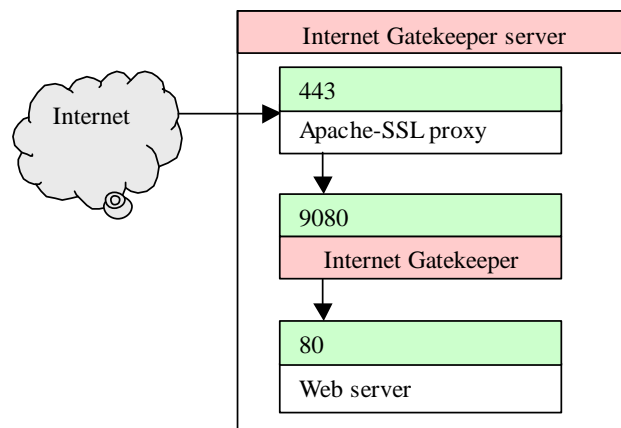
10.5.3 Implementing a HTTPS (SSL) Server

F-Secure Internet Gatekeeper for Linux cannot scan HTTPS (SSL) data because they are encrypted. To scan a connection from a specific HTTP (SSL) server, decrypt the data with a SSL proxy or SSL accelerator first, and then scan the data with the product.

For example, if you use Apache, set Apache to function as a SSL proxy and place F-Secure Internet Gatekeeper in the HTTP communication section.

The Apache-SSL proxy, Internet Gatekeeper, and the web server can be used on separate computers or on the same computer.

The following diagram illustrates the Apache configuration file when the product is used with a SSL proxy and a web server.



Apache-SSL settings

In the following example, port 443 is used first to listen to data. Afterwards, port 9080 is relayed to decrypt data.

Settings

```
# https access
Listen 443
<VirtualHost _default_:443>
  AddDefaultCharset Off
  ProxyPass / http://127.0.0.1:9080/
  ProxyPassReverse / http://127.0.0.1:9080/
  SSLEngine on
  SSLCertificateFile /etc/pki/tls/certs/localhost.crt
  SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
# SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
# SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
  SSLOptions +StdEnvVars
  SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
</VirtualHost>
```

Internet Gatekeeper settings

At the web console, configure the proxy port to 9080 and the parent server port to 80.

Proxy settings

HTTP proxy: **On**

Proxy port: **9080**

Parent server:

Host name: **localhost**

Port number: **80**

Web Server settings

The web server uses port 80.

11. Product Specifications

11.1 Product Specifications

The following describes the specifications for F-Secure Internet Gatekeeper for Linux.

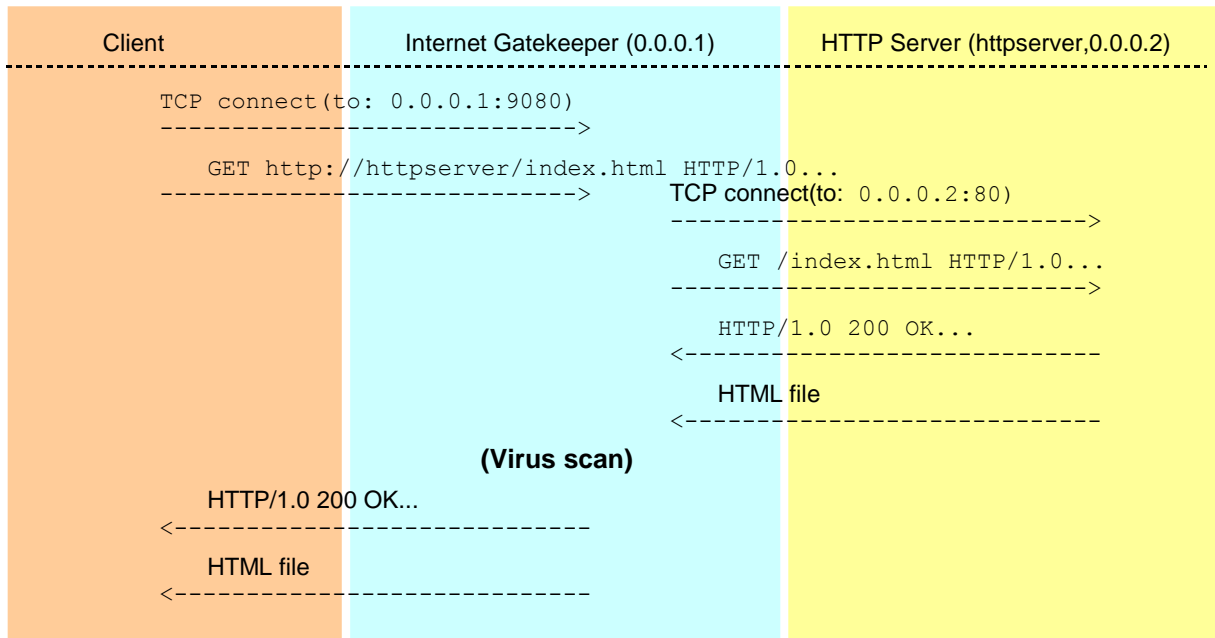
Web console - Supported languages	English/Japanese
Web console - Authentication timeout	300 seconds
Installer	rpm, deb,tar.gz
Supported network protocols	IPv4(RFC791) / TCP(RFC793)
Supported application protocols	HTTP, FTP, SMTP, POP
Supported modes	Proxy, Transparent router, Bridge
HTTP methods that can be scanned	GET/POST/PUT
HTTP methods that can be used	GET/POST/PUT/HEAD/CONNECT/OPTIONS,/DELETE/TRACE/PROPFIND/PROPPATCH/COPY/MOVE/LOCK/UNLOCK, and other similar response methods * Virus scanning cannot be performed for CONNECT (SSL/HTTPS) because the data is encrypted
Supported HTTP proxy schemas	http://,ftp://
Supported HTTP protocol specifications	HTTP/1.0(RFC1945), HTTP/0.9(RFC1945), HTTP/1.1 (RFC2616), WEBDAV(RFC2518) (HTTP/1.1 responses are automatically converted to HTTP/1.0)
Supported HTTP authentication methods	HTTP proxy authentication (Basic)
Maximum HTTP transfer size	Limited by the amount of available disk space
Maximum HTTP URL length	2098 bytes
SMTP commands that can be scanned	DATA
SMTP commands that can be used	HELO/EHLO/MAIL/RCPT/DATA/RSET/VERFY/EXPN/HELP/NOOP/QUIT/XFORWARD/AUTH
Supported SMTP protocol specifications	SMTP(RFC 2821), SMTP Auth(RFC2554)
Supported SMTP authentication methods	SMTP Auth(PLAIN, LOGIN), POP-before-SMTP
Maximum SMTP mail size that can be transferred	2,000,000,000 bytes
POP commands that can be	RETR/STOR

scanned	
POP commands that can be used	USER/PASS/APOP/UIDL/TOP/STAT/LIST/RETR/DELE/NOOP/RSET/QUIT/ AUTH, and other similar response commands * APOP cannot be used if "Defining parent server by user" is enabled and the product is running as a proxy
Supported POP protocol specifications	POP3(RFC1939), POP3 Auth(RFC1734) * APOP cannot be used if "Defining parent server by user" is enabled and the product is running as a proxy
Supported POP authentication methods	User name (variable of the USER command)
Maximum POP transfer size	2,000,000,000 bytes
FTP commands that can be scanned	RETR/STOR/STOU/APPE
FTP commands that can be used	USER/PASS/RETR/LIST/NLST/STOR/STOU/APPE/QUIT/PORT/PASV, and similar response commands
Supported FTP protocol specifications	FTP (RFC959)
Supported FTP authentication methods	User name (argument of the USER command)
Maximum FTP transfer size	Limited by the amount of available disk space
Maximum file size that can be scanned	2GB (for archive files, 2GB is the limit before and after the files are extracted)
Archive files that can be scanned	ZIP, ARJ, LZH, CAB, RAR, TAR, GZIP, BZIP2 up to six levels of nesting
Semaphores used	Number of semaphores for each process (SEMMS): Under 250 Number of semaphore identifiers (SEMMNI): Limited to (Maximum number of simultaneous connections / 25) + 10 for each service (http, smtp, ftp, pop, admin)
Shared memory used	Number of shared memory identifiers (SHMMNI): Limited to 10 for each service (http, smtp, ftp, pop, admin) Memory size (SHMMAX): Limited to 1MB for each service (http, smtp, ftp, pop, admin)

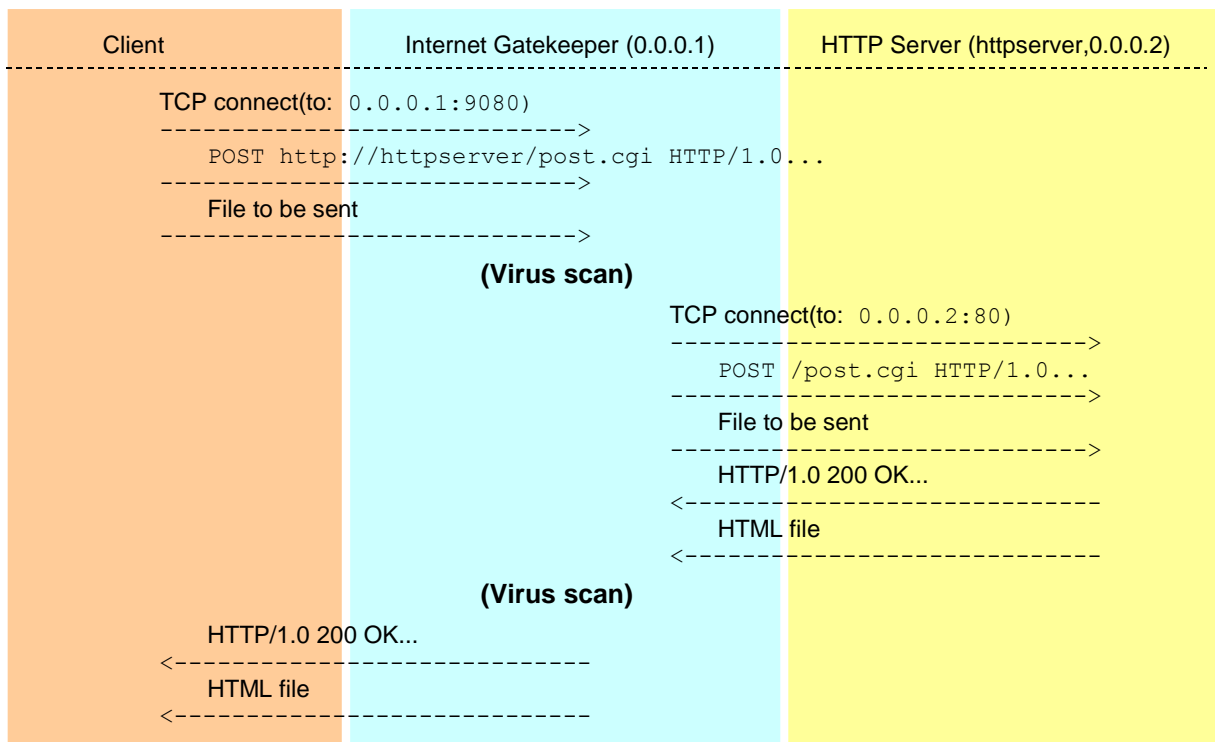
11.2 HTTP Proxy Process

This section describes how common protocols are processed with the HTTP proxy.

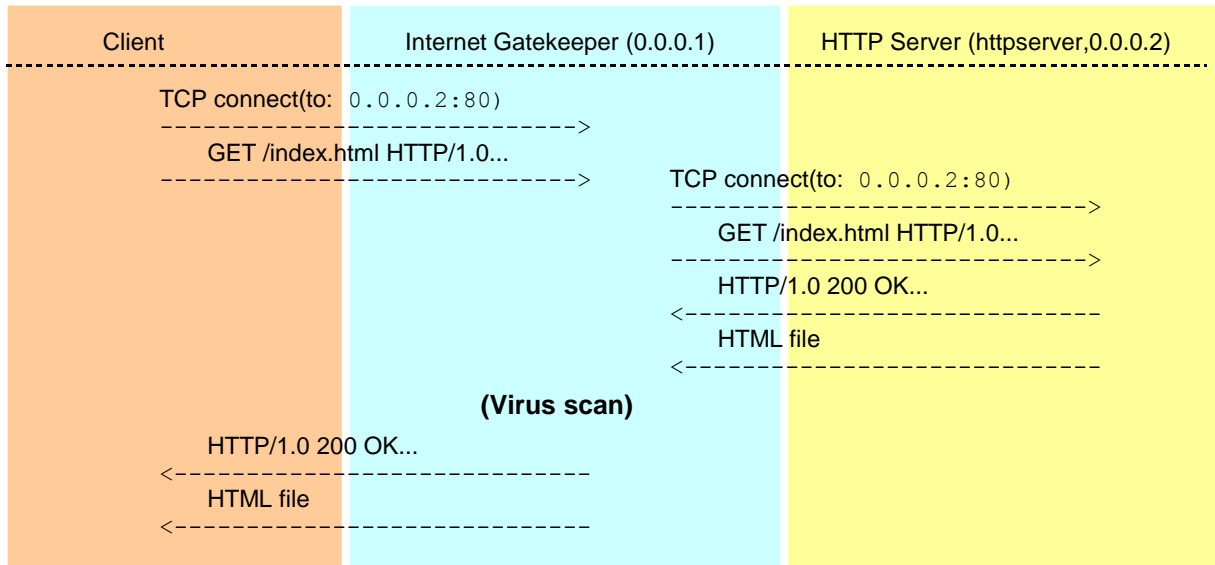
Proxy mode, GET method



Proxy mode, POST method (scans files when they are sent)



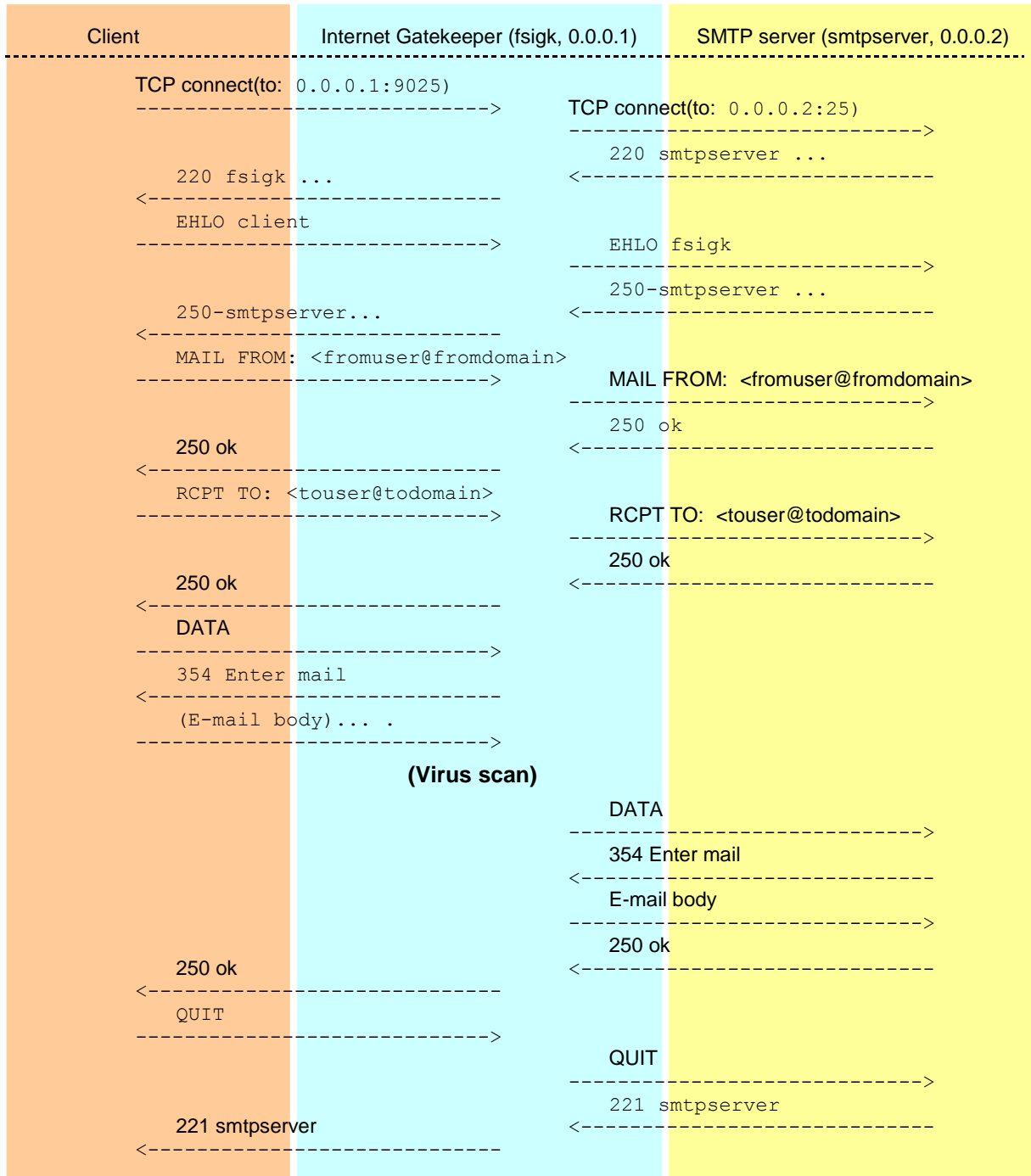
Transparent Proxy mode (Router or Bridge), GET method



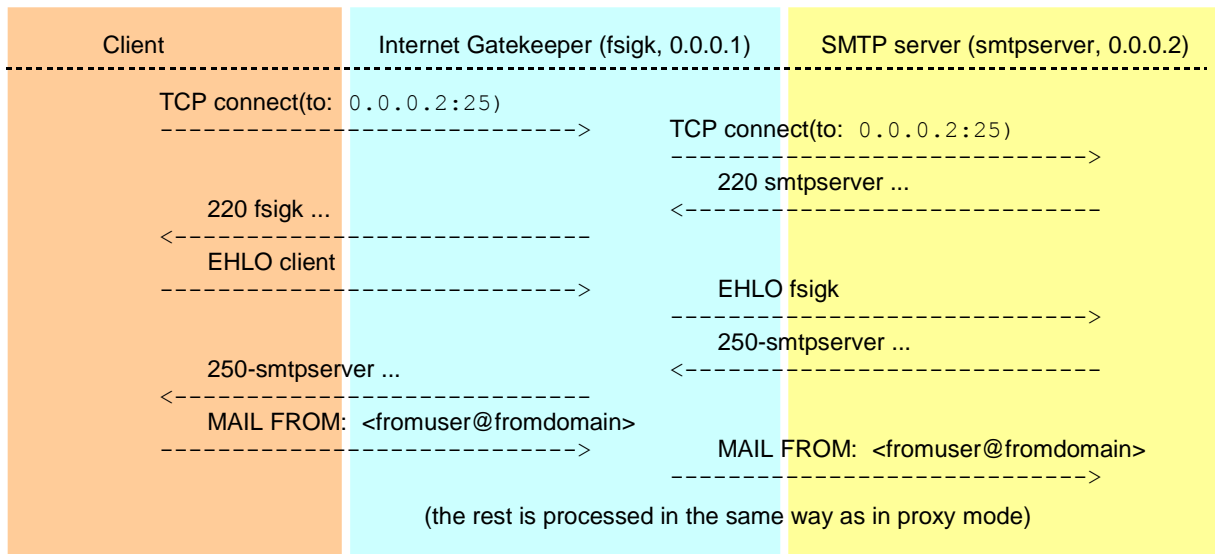
11.3 SMTP Proxy Process

This section describes how common protocols are processed with the SMTP proxy.

Proxy mode



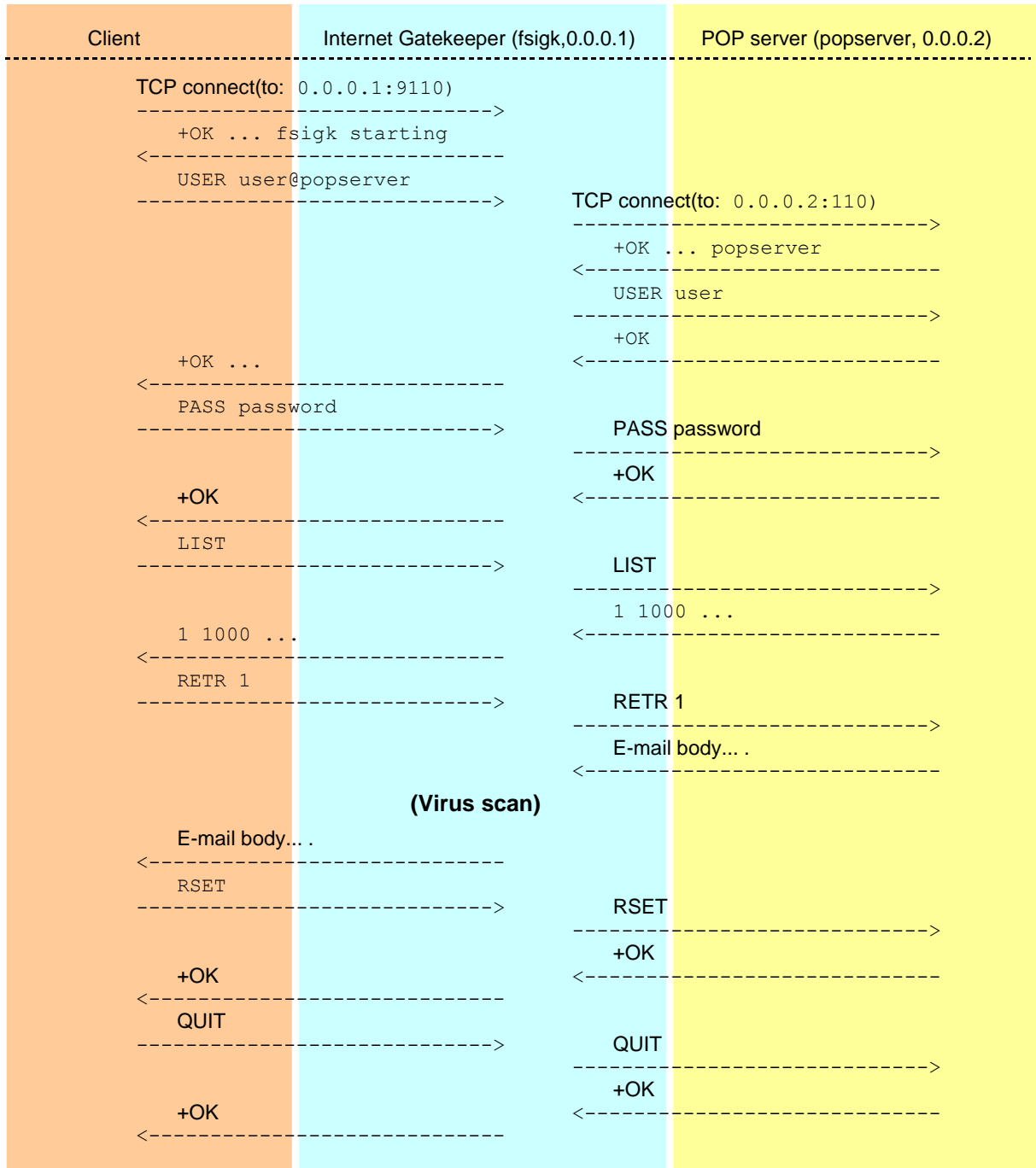
Transparent Proxy mode (Router or Bridge)



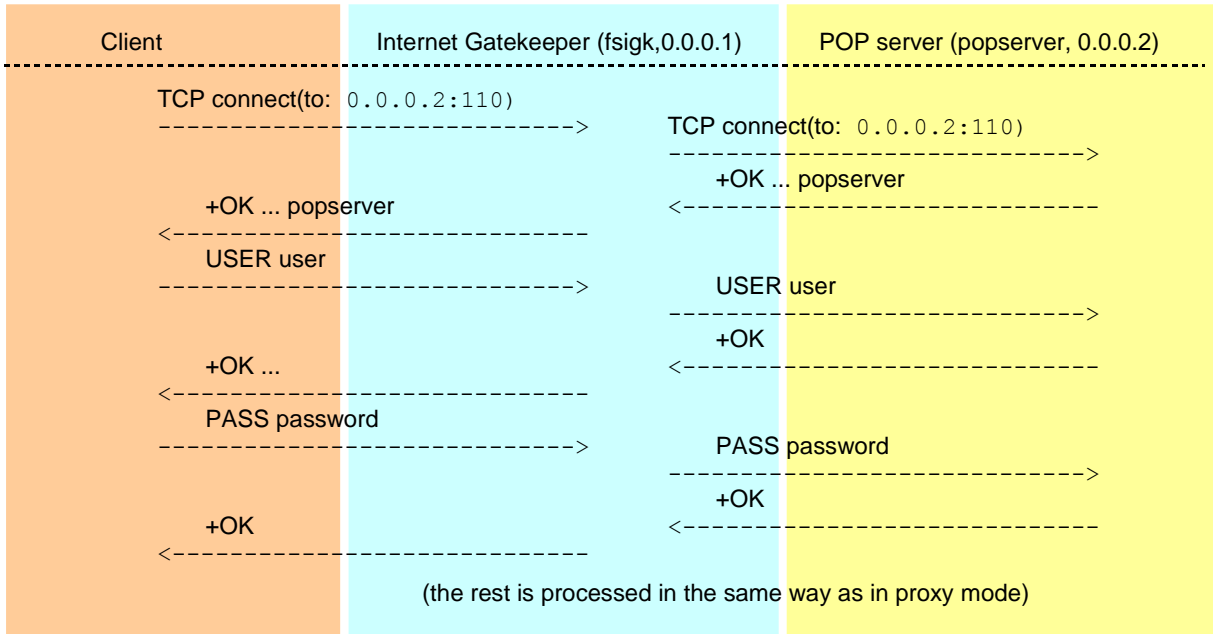
11.4 POP Proxy Process

This section describes how common protocols are processed with the POP proxy.

Proxy mode



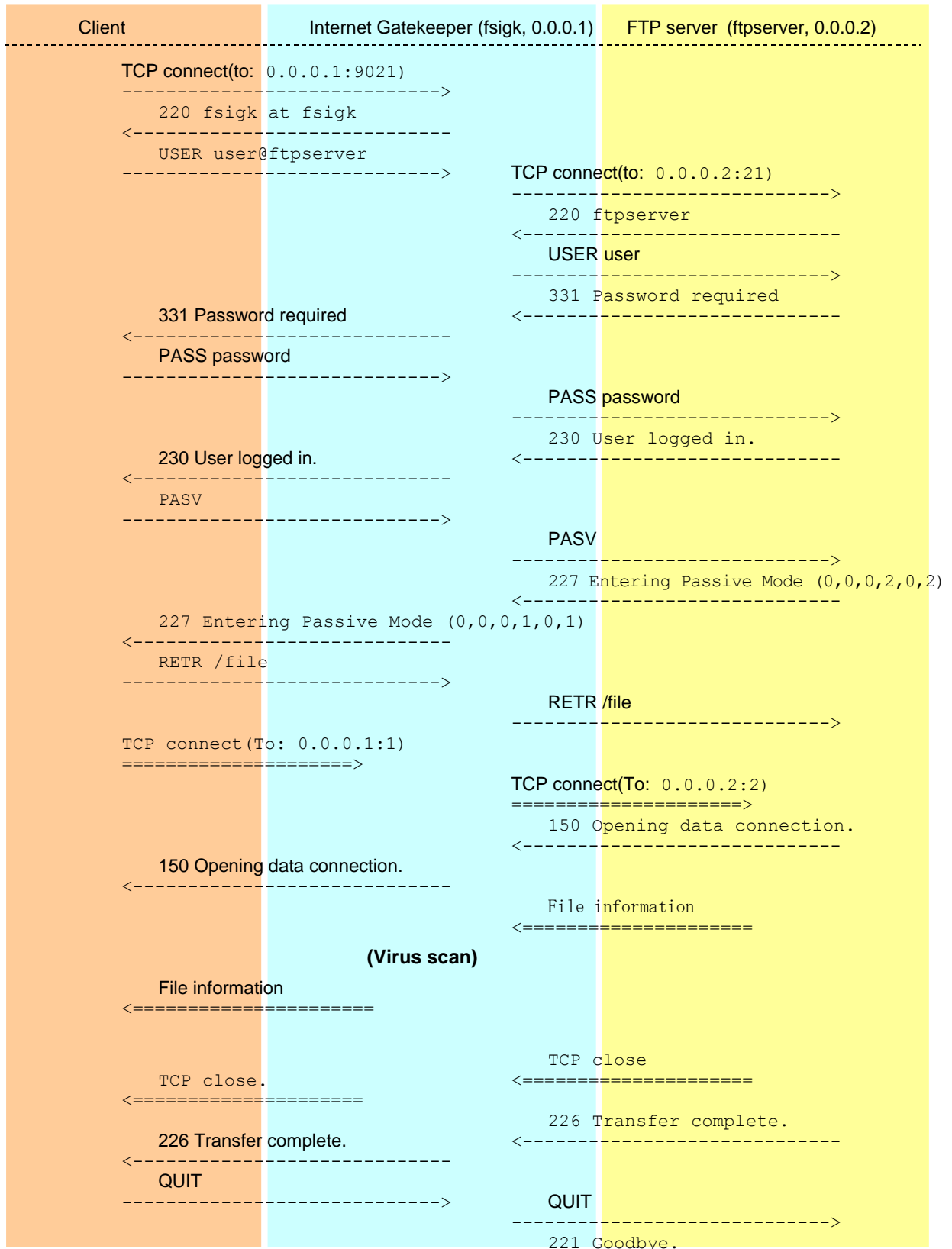
Transparent mode (Router or Bridge)



11.5 FTP Proxy Process

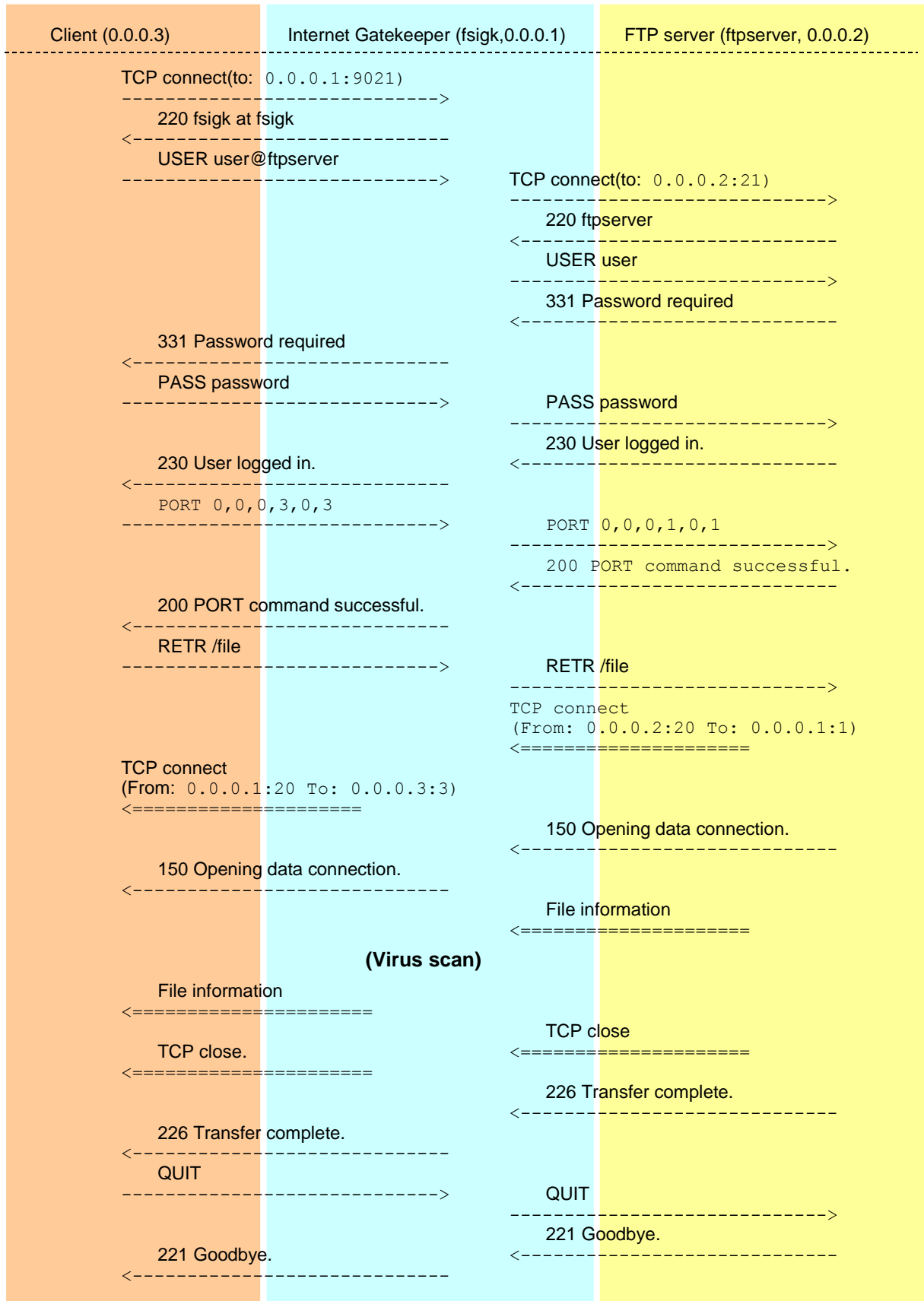
The FTP service relays both the control session and data session. This section describes how common protocols are processed with the FTP proxy.

Proxy mode, Passive FTP



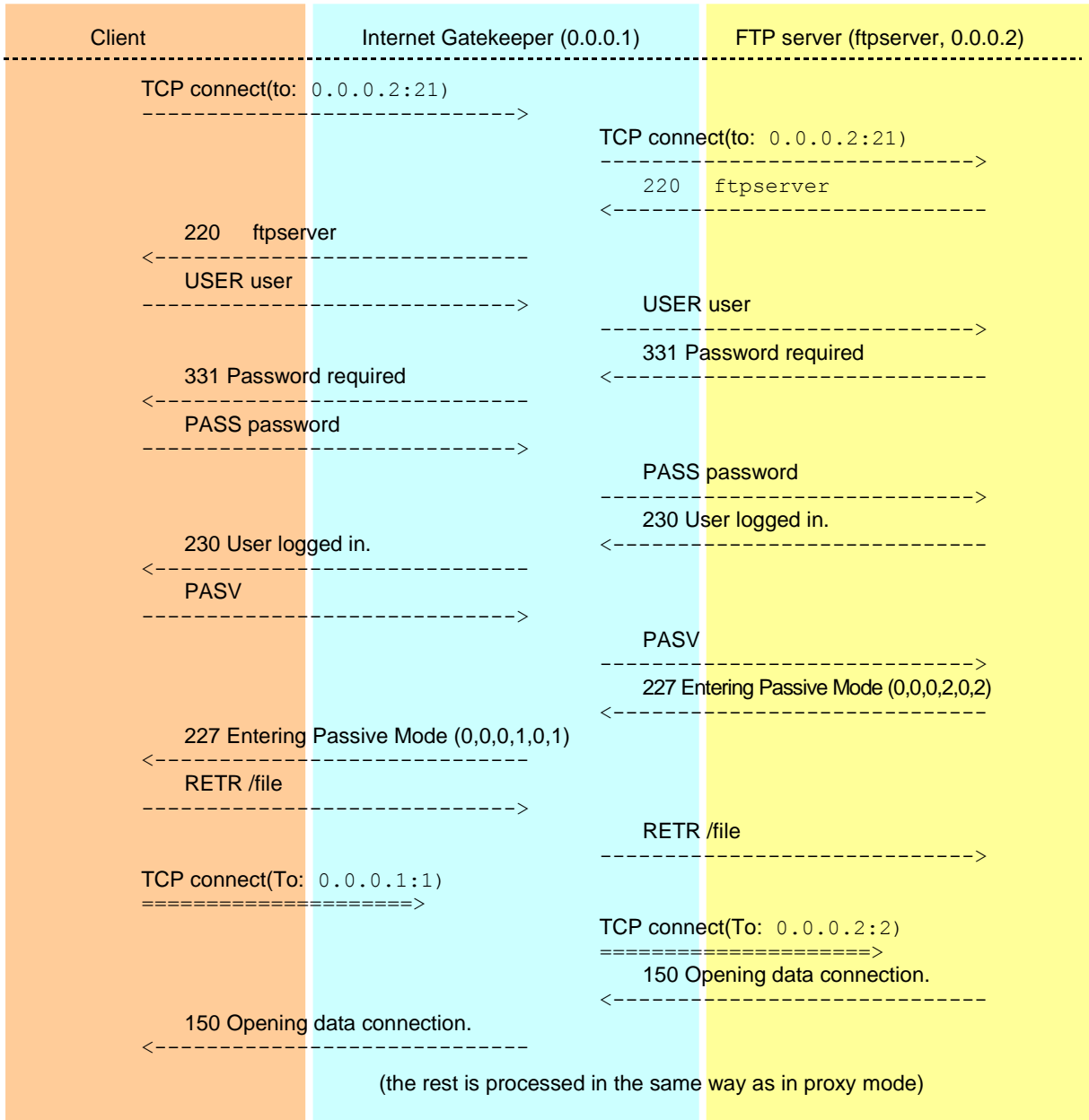
221 Goodbye. <-----
 <-----

Proxy mode, Active FTP

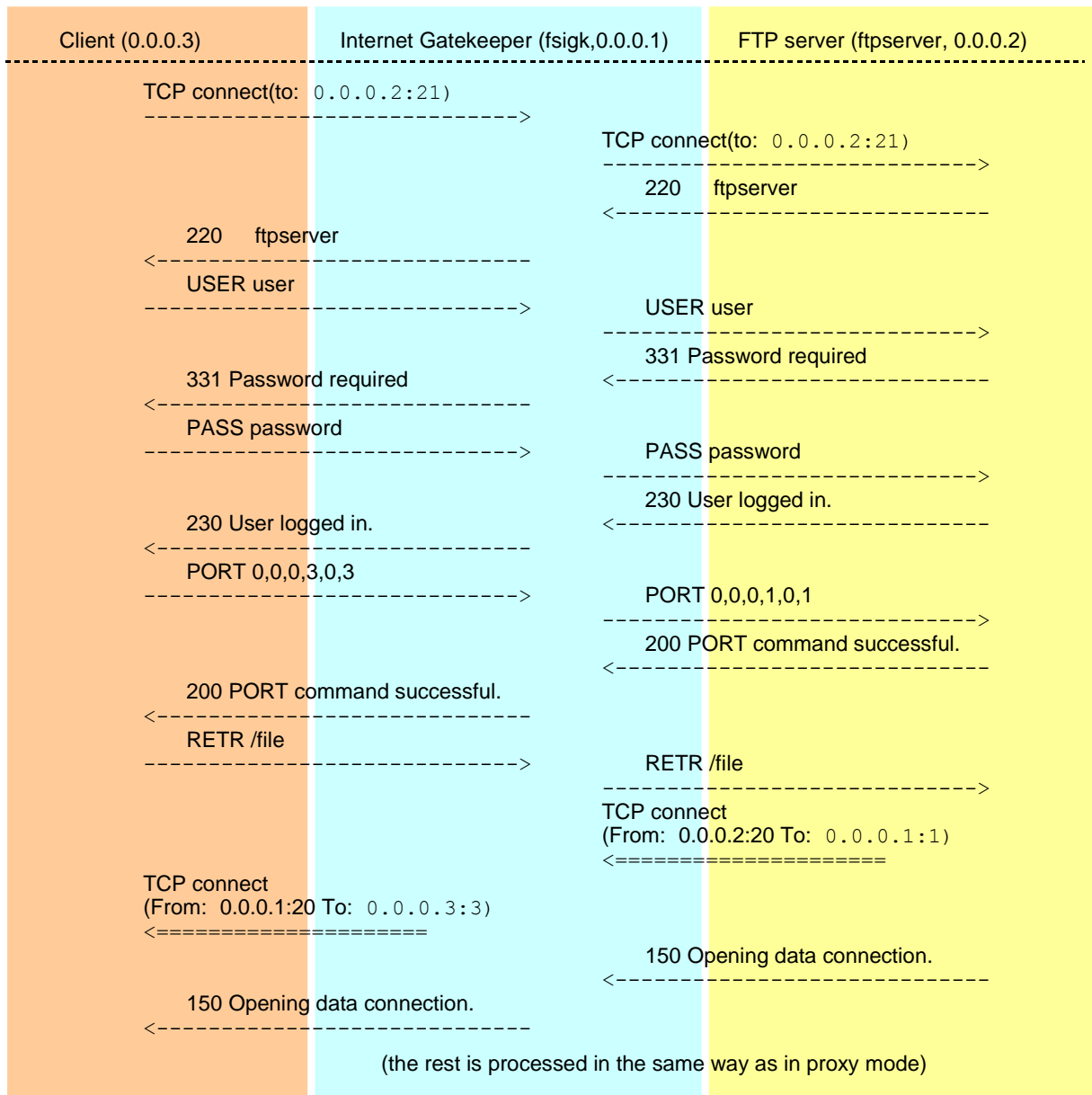


(Virus scan)

Transparent mode (Router or Bridge), Passive FTP




Transparent mode (Router or Bridge), Active FTP



11.6 HTTP Error Responses

The section describes errors that occur during the HTTP access. You can change the messages which are shown to the clients. You can do this by editing the error message template file (`/opt/f-secure/fsigk/conf/template_http_error.html`).

Server connection error

Description	Access to the server failed
Response code	503
Reason	Service Unavailable
Message	Connection error message.  For connection error messages, see " Connection Error Messages ", 171.

Request method length error

Description	The length of the request method exceeds the limit (98 bytes)
Response code	400
Reason	Bad Request
Message	Too long Request Method

Request method character error

Description	The request method contains an invalid character (the character is under the character code 0x20)
Response code	400
Reason	Bad Request
Message	Illegal method character.

Request URL length error

Description	The length of the request URL exceeds the limit (2098 bytes)
Response code	414
Reason	Request-URI Too Long
Message	Request-URI Too Long

Request URL character error

Description	The request URL contains an invalid character (the character is under the character code 0x20)
Response code	400
Reason	Bad Request
Message	Illegal URL character.

Request URL format error

Description	The request URL has an invalid format
Response code	400
Reason	Bad Request
Message	Invalid URL format

Request version length error

Description	The HTTP version of the request exceeds the limit (98 bytes)
Response code	400
Reason	Bad Request
Message	Too long Request Version

Request version error

Description	The request HTTP version specified is a version other than "HTTP/1.0", "HTTP/1.1" or "(HTTP/0.9)"
Response code	505
Reason	HTTP Version Not Supported
Message	Only support HTTP/0.9, HTTP/1.0, HTTP/1.1

Proxy authentication error

Description	Proxy authentication failed
Response code	407
Reason	Proxy Authentication Required
Message	Proxy Authentication Required
Additional header	Proxy-Authenticate: Basic realm="input proxy user/pass"

11.7 HTTP Request and Response Headers

HTTP request and response headers are not changed for the most part but the following headers are changed by the product.

Request header:

- Request line
If the request version is "HTTP/1.1", it is changed to "HTTP/1.0"
If a parent server or transparent proxy is not set up, the part in front of the path name of the URL is removed
(Example: http://xxx:yyy/aaa/iii/uuu => /aaa/iii/uuu)
- Connection
The Connection header is removed.
If the connection is Keep-Alive, Connection: Add Keep-Alive.
- Proxy-Connection
The Proxy-Connection header is removed.
- Via
If an anonymous proxy is used, the header is not changed.
Otherwise, the following change is made:
Via : 1.0 Host name: Port (Product name)
If a Via header exists, it is added to the end with a ",".
- X-Forwarded-For
If an anonymous proxy is used, the header is not changed.
Otherwise, the IP address of the connecting source is added as follows:
X-Forwarded-For: IP Address of connecting source
If an X-Forwarded-For header exists, it is added to the end with a ",".
- Keep-Alive
The current Keep-Alive header is removed
- Trailer
The current Trailer header is removed
- Proxy-Authorization
If Proxy authentication is enabled, it is removed

Response header:

- Response line
If the response header version is "HTTP/1.1", it is changed to "HTTP/1.0"
- Connection
The current Connection header is removed
If the connection is Keep-Alive, the following is added.
 Connection: Keep-Alive
- Proxy-Connection
The current Proxy-Connection header is removed
- Proxy-Support
If a "WWW-Authenticate" header exists and the proxy has no parent server and is not transparent, the following information is added:
 Proxy-Support Session-Based-Authentication
(`"Proxy-Support: Session-Based-Authentication "` is needed if a proxy uses NTLM authentication and other authentication methods. See RFC-4559 for more details.)

11.8 SMTP Command Responses

Usually, server responses are relayed to clients during SMTP connections. However, sometimes they can be generated by F-Secure Internet Gatekeeper for Linux. The product generates the following messages:

[Response message] (Product name)

(Example: 500 Unknown Command: "TEST" (F-Secure/fsigk_smtp/230/gwdev.gw.f-secure.co.jp))

DATA command response

Message	354 Enter mail
Reason	Starts to receive e-mail data that is being transferred.

Message	250 Message accepted for delivery
Reason	Indicates that the e-mail data has been received.

Message	554 SENDBACK:smtp error[COMMAND] (Server Reply: XXX)
Reason	Indicates that an error response (XXX) was returned for the sendback command (COMMAND) used to notify the sender. COMMAND can be either RSET/MAIL or FROM/RCPT TO.

Message	250 Message accepted for delivery
Reason	Indicates that the e-mail data has been received.

Message	554 Too long message
Reason	The data size has exceeded the maximum. The maximum size is 2 GB, or the value specified at block_messagesize/block_message_len in the expert options.

Message	554 Infected by [Detection name]
Reason	This message appears when a virus is detected and if "Deny" is selected as the action when viruses are detected.

Connection responses

Message	421 server open error (Host port) errmsg=[XXX]
Reason	Access to the specified host and port failed. ERRMSG displays the contents covered in " Connection Error Messages ", 164.

Message	421 Cannot get correct greeting message from mail server (Host port). return code=DDD
Reason	The greeting message after connecting to the SMTP server is invalid. Is displayed if the response code from the SMTP server is not 220.

Other command responses

Message	500 Too long line
Reason	The length of the command line exceeds 9999 bytes.

Responses from commands other than HELO, EHLO, AUTH, QUIT, RSET

Message	500 Authentication Required"
Reason	The authentication for sending e-mails is not complete. Is displayed in the following cases: <ul style="list-style-type: none"> - If POP-before-SMTP or SMTP authentication is enabled - Authentication is not successful - The connection is not from the LAN - Recipient domain restrictions are not applied

HELO/EHLO command responses

Message	421 (COMMAND) disconnected from (Host: Port)
Reason	The server was disconnected when COMMAND was executed. The COMMAND can be either HELO or EHLO.

MAIL command responses

Message	501 Syntax error ("MAIL FROM:").
Reason	The MAIL command is invalid (FROM is missing).

RCPT command responses

Message	500 RCPT command must begin with "RCPT TO:."
Reason	The RCPT command is invalid (TO is missing).

Message	250 Recipient ok"
Reason	The relay was denied. Is displayed when recipient domains are restricted and authentication is not completed.

AUTH command responses

Message	504 this mechanism not available
Reason	Authentication methods other than PLAIN and LOGIN are not supported.

Message	235 ok authed
Reason	Authentication is successful. Is displayed only when SMTP authentication is performed by F-Secure Internet Gatekeeper for Linux. If authentication is done on the SMTP server side, the SMTP

	server response is relayed.
--	-----------------------------

Message	535 authorization failed
Reason	Authentication failed. Is displayed only when SMTP authentication is performed by F-Secure Internet Gatekeeper for Linux. If authentication is done on the SMTP server side, the SMTP server response is relayed.

Message	500 disconnected from server(AUTH).
Reason	The server disconnected during authentication.

Unknown commands

Message	500 Unknown Command: "COMMAND"
Reason	The specified command (COMMAND) is not supported.

11.9 SMTP Commands – Operations

During SMTP connections, commands executed from clients are operated in the following way.



The [Product name] is by default "F-Secure/fsigk_smtp/Version/Host name".
You can change the product name by editing "product_name=" (see expert options for details).

Client connections

- 1 Connects to the server.
- 2 If the server access fails:
 - ① The following is sent to the client: 421 server open error([Server host]:[Server port])
errmsg=[connection error message]
 - ➊ For connection error messages, see "[Connection Error Messages](#)", 162.
 - ➋ The session ends.
 - ② The session ends.
- 3 Receives a response from the server.
- 4 If the response code is other than 220, the connection is terminated.
- 5 The following is sent to the client: 200 [Host name] [Product name]

Command-lines

- 1 If a line is greater than 9998 bytes:
 - ① The following is sent to the client: 500 Too long line ([Product name])
 - ② The connection is terminated.
- 2 If the following conditions are met, and a command other than HELO, EHLO, AUTH, QUIT, RSET is received:
 - POP-before-SMTP or SMTP authentication is enabled
 - Authentication is not successful
 - The connection is not from the LAN
 - Recipient domain restrictions are not applied
 - ① The following is sent to the client: 500 Authentication Required ([Product name])
- 3 If 1 and 2 above do not apply, the command is executed.

HELO command

- 1 The following is sent to the server: HELO [Host name]
- 2 Receives a response from the server.
- 3 The following is sent to the client: [Server response information]

EHLO command

- 1 The following is sent to the server: EHLO [Host name]
- 2 Receives a response from the server.
- 3 The following option lines are deleted from the response information.
CHUNKING, BINARYMIME, PIPELINING, STARTTLS
- 4 Set the response and maximum message size to the smallest value (default: 2,000,000,000) from the server in the SIZE option.
- 5 If proxy authentication is enabled, add the following option line to the response information.
250-AUTH PLAIN LOGIN
- 6 The following is sent to the client: [Response information]

MAIL command

- 1 If the syntax of the command is invalid:
 - ① The following is sent to the client: 501 Syntax error (MAIL FROM:) ([Product name])
- 2 The following is sent to the server: [Client response information]
- 3 Receives a response from the server.
- 4 The following is sent to the client: [Server response information]

RCPT command

- 1 If the syntax of the command is invalid:
 - ① The following is sent to the client: 500 RCPT command must begin with "RCPT TO:" ([Product name])
- 2 If recipient domains are restricted and authentication is not complete (Recipient (RCPT) domain restrictions are enabled and PbS (POP-before-SMTP)/SMTP authentication is not complete (destination domains and domain connections from the LAN are not related))
 - ① The following is sent to the client: 550 Relaying denied. ([Product name])
- 3 The following is sent to the server: [Client response information]
- 4 Receives a response from the server.
- 5 The following is sent to the client: [Server response information]
- 6 If the response code is other than 250:
 - ① The session ends.

AUTH command

- 1 If SMTP authentication is enabled:
 - ① If authentication passes:
 - 1) The following is sent to the client: 235 ok authed ([Product name])
 - ② If authentication fails:
 - 1) The following is sent to the client: 535 authorization failed ([Product name])
 - ③ If the authentication method is other than PLAIN or LOGIN:
 - 1) The following is sent to the client: 504 this mechanism not available ([Product name])
- 2 If SMTP authentication is disabled:
 - ① The authentication request and response are transferred between the server and client.

DATA command

- 1 The following is sent to the client: 354 Enter mail ([Product name])
- 2 Mail data is received.
- 3 Mail data is scanned for viruses or spam.
- 4 If a virus or spam is detected:
 - ① Virus logs are recorded.
 - ② A notification is sent to the administrator (if notification sending is enabled).
- 5 If the e-mail size is greater than the maximum message size:
 - ① The following is sent to the client: 554 Too long message ([Product name])
- 6 If a virus or spam is detected and action on detection is set to "Clean", "Do nothing" or "Change subject":
 - ① If "Deny" is set as the action:
 - 1) The following is sent to the server: RSET
 - 2) Receives a response from the server.
 - 3) If the response code is other than 250, the session ends.
 - 4) The following is sent to the client: 554 Infected by [Detection name] ([Product name])
 - ② If "Notify the sender" is set as the action
 - 1) The following is sent to the server: RSET
 - 2) If the response code is other than 250:
 - a) The following is sent to the client: 554 :SENDBACK:smtp error[RSET]: (Server Reply: [Server response information]) ([Product name])
 - 3) The following is sent to the server: MAIL FROM: [Template sender or administrator address]
 - 4) If the response code is other than 250:
 - a) The following is sent to the client: 554 SENDBACK:smtp error[MAIL FROM] (Server Reply: [Server response information]) ([Product name])
 - 5) The following is sent to the server: RCPT TO: <Sender address>
 - 6) If the response code other than 250:
 - a) The following is sent to the client: 554 SENDBACK:smtp error[RCPT TO] (Server Reply: [Server response information]) ([Product name])
 - ③ If the action on detection is set to "Notify the sender" or "Notify the recipient":
 - 1) The following is sent to the server: DATA
 - 2) If the response code other than 354:
 - a) The command terminates.
 - 3) The following is sent to the server:


```
Received: from [Client host name] ([Client IP address])
by [Host name] (Product name) ;
[Current time (RFC822 format)]
```
 - 4) If spam is detected:
 - a) The following is sent to the server: X-Spam-Status: Yes(Product name) with [Detection name]
 - 5) If a virus is detected:
 - a) The following is sent to the server: X-Virus-Status: infected(Product name) with [Detection name]
 - 6) The following is sent to the server: Data: [Date field information of the e-mail received]
 - 7) If "Notify the sender" is set as the action:
 - a) The following is sent to the server: To: [Sender address of the e-mail received]
 - 8) If "Notify the recipients" is set as the action:

- a) The following is sent to the server: To: [Recipient address of the e-mail received]
- b) The following is sent to the server: CC: [CC address of the e-mail received]
- 9) If the From field is not included in the infected e-mail notification template:
 - a) The following is sent to the server: From: [Administrator's e-mail address]
- 10) The following is sent to the server: Content-Transfer-Encoding: 7bit
- 11) The information of the detection notification message is sent.
- 12) The following is sent to the server: "¥r¥n.¥r¥n"
- 13) The following is sent to the client: Server response information
- 14) If the response code is other than 250:
 - a) The session ends.
- ④ If "Delete" is set as the action:
 - 1) The following is sent to the server: RSET
 - 2) If the response code is other than 250:
 - a) The session ends.
 - 3) The following is sent to the client: 250 Message accepted for delivery ([Product name])
- 7 If (6) above does not apply:
 - ① The following is sent to the server: DATA
 - ② If the response code is other than 354:
 - 1) The following is sent to the client: [Server response information]
 - 2) The command terminates.
 - ③ If anonymous proxy mode is not enabled:
 - 1) The following is sent to the server:

Received: from [Client host name] ([Client IP address])
by [Host name] (Product name) ;
[Current time (RFC822 format)]
 - 2) If spam is detected:
 - a) The following is sent to the server: X-Spam-Status: Yes([Product name]) with [Detection name]
 - 3) If a virus is cleaned:
 - a) The following is sent to the server: X-Virus-Status: disinfected([Product name]) from [Detection name]
 - 4) If infected by a virus:
 - a) The following is sent to the server: X-Virus-Status: infected([Product name]) with [Detection name]
 - 5) If viruses or spam are not detected:
 - a) The following is sent to the server: X-Virus-Status: clean([Product name])
 - ④ The following is sent to the server: E-mail information
 - ⑤ The following is sent to the client: Server response information
- 8 Access log is recorded.

RSET/XFORWARD/NOOP/EXPN command

- 1 The following is sent to the server: [Client response information]
- 2 Receives a response from the server.
- 3 The following is sent to the client: [Server response information]

Unknown commands

- 1 The following is sent to the server: 500 Unknown Command: "[Command received]" ([Product name])

11.10 POP Commands – Operations

During POP connections, commands executed from clients are operated in the following way.



The [Product name] is by default "F-Secure/fsigk_pop/Version/Host name".
You can change the product name by editing "product_name=" (see expert options for details).

Client connections

- 1 If "Defining parent server by user" is disabled or transparent mode is enabled:
 - ① The server is accessed.
 - ② If access fails:
 - 1) The following is sent to the client: -ERR Can't Connect to (Server host: Server port)
errmsg=[Connection error message]
➡ For connection error messages, see "[Connection Error Messages](#)", 162.
 - 2) The session ends.
 - ③ Receives a response from the server.
 - ④ The following is sent to the client: [Server response information]
- 2 If (2) above does not apply:
 - ① The following is sent to the client: +OK [Product name] starting.

Command lines

- 1 If a line is greater than 998 bytes:
 - ① The following is sent to the client: -ERR Too long line
- 2 If not connected to a server and a command other than USER/QUIT is sent:
 - ① The following is sent to the client: -ERR please use USER command at first.
- 3 If 1 and 2 above do not apply, the command is executed.

USER command

- 1 If "Defining parent server by user" is disabled or transparent mode is enabled:
 - ① The following is sent to the server: Client response information
- 2 If (1) above does not apply:
 - ① If user authentication is enabled:
 - 1) If the user is not added:
 - a) The following is sent to the client: -ERR Invalid Account Auth.
 - ② If the user name contains "@" or "#":
 - 1) The server specified by the last "@" or "#" is accessed.
 - ③ If (2) above does not apply:
 - 1) If the parent server is empty:
 - a) The following is sent to the client: -ERR USER format is USER username@hostname or username#hostname
 - b) The command terminates.
 - 2) Connects to the parent server.

- ④ If the connection fails:
 - 1) The following is sent to the client: -ERR Can't Connect to (Server host: Server port)
errmsg=[Connection error message]
 - ➡ For connection error messages, see “[Connection Error Messages](#)”, 162.
- ⑤ The following is sent to the server: USER [User name]
- ⑥ Receives a response from the server.
- ⑦ The following is sent to the client: [Server response information]

QUIT command

- 1 If connected to a server:
 - ① The following is sent to the server: [Client request information]
 - ② Receives a response from the server.
 - ③ The following is sent to the client: [Server response information]
- 2 If (1) above does not apply:
 - ① The following is sent to the client: +OK Quit

PASS/APOP/AUTH commands

- 1 If user restriction with the APOP command is enabled:
 - ① If the user is not added:
 - 1) The following is sent to the client: -ERR Invalid Account Auth.
- 2 The following is sent to the server: Client response information
- 3 Receives a response from the server.
- 4 If the server response is successful:
 - ① Add the client IP address to the POP-before-SMTP database.

RETR command

- 1 The following is sent to the server: Client response information
- 2 Mail is received.
- 3 Mail is scanned for viruses and spam.
- 4 If a virus or spam is detected:
 - ① Virus logs are recorded.
 - ② A notification is sent to the administrator (if enabled).
- 5 If a virus is detected and the action on detection is “Delete”:
 - ① The following is sent to the client:
 - Received from FSIGK: Current time(RFC822 format)
 - X-Virus-Status: infected([Product name]) with [Detection name]
 - Date: [Date of header] (If it exists)
 - To: [To of header] (If it exists)
 - Cc: [Cc of header] (If it exists)
 - [Information of the detection notification message]

6 If (5) above does not apply:

① If a virus or spam is detected:

1) The following is sent to the client: Received: from FSIGK: Current time(RFC822 format)

② If spam is detected:

1) The following is sent to the client: X-Spam-Status: Yes(Product name) with [Detection name]

③ If a virus is detected:

1) The following is sent to the client: X-Virus-Status: disinfected(%s) from [Detection name]

④ If a virus is detected:

1) The following is sent to the client: X-Virus-Status: infected(%s) with [Detection name]

⑤ The following is sent to the client: E-mail information

Other commands

1 The following is sent to the server: [Client response information]

2 Receives a response from the server.

3 The following is sent to the client: [Server response information]

11.11 FTP Commands – Operations

During FTP connections, commands executed from clients are operated in the following way.



The [Product name] is by default "F-Secure/fsigk_ftp/Version/Host name".
You can change the product name by editing "product_name=" in the expert options.

Client connections

1 If "Defining parent server by user" is disabled or transparent mode is enabled:

① The server is accessed.

② If access fails:

1) The following is sent to the client: -500 Can't Connect to (Server host: Server port)
errmsg=[Connection error message]

➡ For connection error messages, see "[Connection Error Messages](#)", 162.

2) The session ends.

③ Receives a response from the server.

④ The following is sent to the client: [Server response information]

2 If (1) above does not apply:

① The following is sent to the client: 220 [Product name] at Host name starting.

Command lines

1 If a line is greater than 998 bytes:

① The following is sent to the client: 500 Too long line

2 If not connected to a server and a command other than USER/QUIT is sent:

① The following is sent to the client: 530 please use USER command at first.

3 If 1 and 2 above do not apply, the command is executed.

USER command

1 If "Defining parent server by user" is disabled or transparent mode is enabled:

① The following is sent to the server: Client response information

- 2 If (1) above does not apply:
 - ① If user authentication is enabled:
 - 1) If the user is not added:
 - a) The following is sent to the client: 500 Invalid Account Auth.
 - ② If the user name contains "@" or "#":
 - 1) The server specified by the last "@" or "#" is accessed.
 - ③ If (2) above does not apply:
 - 1) If the parent server is empty:
 - a) The following is sent to the client: 500 USER format is USER username@hostname or username#hostname
 - b) The command terminates.
 - 2) Connects to the parent server.

- ④ If the connection fails:
 - 1) The following is sent to the client: -500 Can't Connect to (Server host: Server port)
errmsg=[Connection error message]
 - ➡ For connection error messages, see “[Connection Error Messages](#)”, 162.
- ⑤ The following is sent to the server: USER [User name]
- ⑥ Receives a response from the server.
- ⑦ The following is sent to the client: [Server response information]

QUIT command

- 1 If connected to a server:
 - ① The following is sent to the server: [Client response information]
 - ② Receives a response from the server.
 - ③ The following is sent to the client: [Server response information]
- 2 If (2) above does not apply:
 - ① The following is sent to the client: 221 Quit

PASV command

- 1 The following is sent to the server: PASV
- 2 Receives a response from the server.
- 3 The following is sent to the client: 227 Entering Passive Mode (xx,xx,xx,xx,yy,yy)
(xx is the IP address of the proxy and yy is the proxy port)

PORT command

- 1 The following is sent to the client: PORT (xx,xx,xx,xx,yy,yy)
(xx is the IP address of the proxy and yy is the proxy port)
- 2 Receives a response from the server.
- 3 The following is sent to the client: [Server response information]

RETR/LIST/NLST/STOR/STOU/APPE commands

- 1 If PASV/PORT commands are not executed:
 - ① The following is sent to the client: 530 please use PORT/PASV command at first.
 - ② The command terminates.
- 2 If the mode is PASV:
 - ① Waits for a data session to connect.
 - ② If the source of the data session and control session are different:
 - 1) The following is sent to the client: 530 Invalid Connection Source.
 - 2) The command terminates.
 - ③ Connects to the server with the data session.
 - ④ Receives a response from the server.
 - ⑤ The following is sent to the client: Server response information
 - ⑥ If the response code is other than 1xx:
 - 1) The command terminates.

- 3 If the mode is Active:
 - ① Receives a response from the server.
 - ② If the response code is other than 1xx:
 - 1) The command terminates.
 - ③ Connects to the client with the data session.
 - ④ If the client connection fails:
 - 1) Information of the detection notification message: 530 Cannot connect client
 - 2) The session ends.
- 4 The file is received.
- 5 If the command is other than LIST/NLST:
- 6 If a virus is detected:
 - ① The following is sent to the client: 530 Infected by [Detection name]
 - ② The command ends.
- 7 The file is transferred.

Other commands

- 1 The following is sent to the server: [Client response information]
- 2 Receives a response from the server.
- 3 The following is sent to the client: [Server response information]

11.12 Connection Error Messages

This section describes error messages that appear when a connection to a server fails.

```
CONNECT(Host: Port)/connect: [Connection error details]
```

Connect request to the IP address of a server failed.

Connections are performed using the `connect()` system call of Linux. The "Connection error details" contains the error message of `connect()` system call which in most cases will be one of the following:

- Connection refused : The server denied the connection.
- Connection timed out : A timeout occurred while trying to access the server.
- Network is unreachable : The network on the server could not be reached.

```
CONNECT(Host: Port)/connect timeout(>$1 sec)
```

A timeout occurred because the connection could not be established within the specified time (\$1).

This error is displayed only when the server connect timeout setting in the expert options is enabled.

```
CONNECT(Host: Port)/connect cancelled
```

Is displayed when the connection was canceled by the client.

```
CONNECT(Host: Port)/hostname lookup error: [Host name lookup error details]
```

Failed to lookup the host name.

Host name lookups are performed using the `gethostbyname()` function of Linux(glibc). The "Connection error details" contains the error message of the `gethostbyname()` function which in most cases is one of the following:

- Unknown host : The specified host could not be found.

Host name lookup failure : Failed to look up the specified host.
(Occurs, for example, when a response from the DNS server could not be reached. If there is no problem on the DNS server, check if you can look up the host name from the Linux Internet Gatekeeper server by using nslookup.

Unknown server error : Error in the DNS server.

No address associated with name : IP address of the specified host could not be found.

CONNECT(Host: Port)/Access Inhibited by Proxy(FSIGK)

Connection was denied due to access control settings on the destination.

11.13 Service Process List

F-Secure Linux Internet Gatekeeper uses the following processes to provide its services.

`tomcat (java)`

Web application server used for the web console of the product.

Tomcat uses Java. It uses a single process and it can use multiple threads. It uses approximately 100 MB of memory.

`fsigk_http`

Process used to provide HTTP service.

It makes HTTP communication between clients and servers possible.

To process sessions, the specified maximum number of simultaneous connections is used for processing, and another single process is used for administration.

In addition, the process also communicates with the virus scanning process (`fsavd`) as needed.

Communication is processed by using the UNIX domain socket (`fsavd-socket-0` in the install directory).

Up to 500 KB of memory cannot be shared per process.

`fsigk_smtp`

Process used to provide SMTP service.

It makes SMTP communication between clients and servers possible.

To process sessions, the specified maximum number of simultaneous connections is used for processing, and another single process is used for administration.

In addition, the process also communicates with the virus scanning process (`fsavd`) and spam scanning process (`fsasd`) as needed. Communication is processed by using the UNIX domain socket (`fsavd-socket-0` and `fsasd-lnx32-socket` in the install directory).

Up to 500 KB of memory cannot be shared per process.

`fsigk_pop`

Process used to provide POP service.

It makes POP communication between clients and servers possible.

To process sessions, the specified maximum number of simultaneous connections is used for processing, and another single process is used for administration.

In addition, the process also communicates with the virus scanning process (`fsavd`) and spam scanning process (`fsasd`) as needed. Communication is processed by using the UNIX domain socket (`fsavd-socket-0` and `fsasd-lnx32-socket` in the install directory).

Up to 500 KB of memory cannot be shared per process.

`fsigk_ftp`

Process used to provide FTP service.

It makes FTP communication between clients and servers possible.

To process sessions, the specified maximum number of simultaneous connections is used for processing, and another single process is used for administration.

In addition, the process also communicates with the virus scanning process (`fsavd`) as needed.

Communication is processed by using the UNIX domain socket (`fsavd-socket-0` in the install directory).

Up to 500 KB of memory cannot be shared per process.

`fsavd`

Handles the virus scanning process. The number of processes it uses varies depending on the usage. The process uses a minimum of 2 processes, and the maximum number of processes it can use for each service is equal to the logical number of CPUs in the system (2 CPUs: 2 processes, 4 CPUs: 4 processes). In addition, the process uses a single process for administration.

Around 50 MB of memory cannot be shared per process.

`fsasd`

Handles the SPAM scanning process. The number of threads it uses varies depending on the usage. The process uses a minimum of 2 threads,

The daemon uses around 40 MB of memory

11.14 Detection Names

If F-Secure Internet Gatekeeper for Linux detects a virus, the virus name is recorded in a log. Detailed information on viruses can be found on the following web page:

<http://www.f-secure.com/v-descs/>

If you specify certain conditions, the product can detect other information besides viruses. These detection names begin with "FSIGK/" and they are listed below:

FSIGK/POLICY_FORMAT_MIME_BOUNDARY

Invalid character in the boundary section of the mail header
(Invalid character: "", codes below 0x1f, codes above 0x7f)

FSIGK/POLICY_FORMAT_MIME_FILENAME

Invalid character in the file name section of the mail header
(Invalid character: Codes below 0x1f (not including 0x1b))

FSIGK/POLICY_BLOCK_ENCRYPTED

Encrypted file (if encrypted files are denied)

FSIGK/POLICY_BLOCK_SCRIPT

HTML file including scripts (if scripts are denied)

FSIGK/POLICY_BLOCK_ACTIVEX

HTML file including ActiveX (if ActiveX is denied)

FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE

Partial message (if partial messages are denied)

FSIGK/POLICY_BLOCK_MAXNESTED

Archive file that contains more than the allowed nest levels
(if the maximum nest level of archive files is denied in block_maxnested=yes)

FSIGK/POLICY_BLOCK_SCANTIMEOUT

Scan times out
(if scans are denied if they reach the maximum allowed time which is set in block_scantimeout=yes)

FSIGK/POLICY_BLOCK_MESSAGESIZE

Mail size is greater than the maximum size allowed
(if the mail size is set or if a mail is greater than 2 GB (block_messagesize_len=xxx))

FSIGK/POLICY_BLOCK_FILESIZE

File size is greater than the maximum size allowed
(If the file size limit is set in block_filesize=yes)

FSIGK/SPAM_LIST/CUSTOM/(Condition number)/(Header field name)

Spam detected by a specific condition.
The condition number indicates the number of lines detected in the database file.

FSIGK/SPAM_LIST/UCE/([Condition number])/(Header field))

Spam detected by a database (Unsolicited advertisements).

The condition number indicates the number of lines detected in the database file.

FSIGK/SPAM_LIST/ADVERTISEMENT/(Condition number)/ (Header field name)

Spam detected by a database (general advertisements).

The condition number indicates the number of lines detected in the database file.

FSIGK/SPAM_LIST/HTMLMAIL/(Condition number)/ (Header field name)

Spam detected by a database (HTML-based e-mails).

The condition number indicates the number of lines detected in the database file.

FSIGK/SPAM_LIST/VIRUSERROR /(Condition number)/ (Header field name)

Spam detected through a database (Virus and spam notification e-mails).

The condition number indicates the number of lines detected in the database file.

FSIGK/SPAM_LIST/ERROR/(Condition)/ (Header field name)

Spam detected by a database (Error mail).

The condition number indicates the number of lines detected in the database file.

FSIGK/SPAM_RBL/(Detected address)[(RBL server name): (RBL response address)]

Spam detected by RBL inspection:

Detected address : Address registered in the RBL server

RBL server name : Name of the RBL server in which the address was found

RBL reply address : Reply address from the RBL server when spam was detected

FSIGK/SPAM_SURBL/(Detected domain name)[(SURBL server name): (SURBL response address)]

When spam is detected by SURBL inspection:

Detected domain name : Domain name registered on the SURBL server

SURBL server name : Name of the SURBL server in which the name was found

SURBL reply address : Reply address from the SURBL server when spam was detected

11.15 Riskware

Riskware is not malware. Riskware is not designed specifically to harm the computer, but it has security-critical functions that may harm the computer if misused. These programs perform some useful but potentially dangerous functions.

Examples of such programs are:

- Remote administration programs (Example: VNC)
- Instant messaging programs (Example: IRC)

Programs for transferring files over the internet from one computer to another

- Internet phone programs (VoIP)

If a program is identified as riskware but it is explicitly installed and correctly set up and used, it is less likely to be harmful.

Riskware detected by F-Secure Internet Gatekeeper for Linux are given the detection name of "Catagoriy.Platform.Family".

Riskware categories:

- Adware
- AVTool
- Client-IRC
- Client-SMTP
- CrackTool
- Dialer
- Downloader
- Effect
- FalseAlarm
- Joke
- Monitor
- NetTool
- Porn-Dialer
- Porn-Downloader
- Porn-Tool
- Proxy
- PSWTool
- RemoteAdmin
- RiskTool
- Server-FTP
- Server-Proxy
- Server-Telnet
- Server-Web
- Tool

Riskware platforms:

Apropos
BAT
Casino
ClearSearch
DOS
DrWeb
Dudu
ESafe
HTML
Java
JS
Linux
Lop
Macro
Maxifiles
NAI
NaviPromo
NewDotNet
Palm
Perl
PHP
Searcher
Solomon
Symantec
TrendMicro
UNIX
VBA
VBS
Win16
Win32
Wintol
ZenoSearch

12. Copyright Information

Copyright (c) 1993-2004 F Secure Corporation. All Rights Reserved.

Portions

Copyright (c) 1991-2004 Kaspersky Labs, Ltd.

Copyright (c) 2003 Commtouch(R) Software Ltd

This product may be covered by one or more F Secure patents, including the following: B2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233.

F-Secure Internet Gatekeeper for Linux includes the following software. License information for the software can be found in the respective doc/ directory of each software.

➔ More information can be found at the URLs of the original packages.

tcp_wrappers(libwrap.a)

Original Package: <ftp://ftp.porcupine.org/pub/security/index.html>

pam_userdb

Original Package: <http://www.kernel.org/pub/linux/libs/pam/>

zip

Original Package: <http://www.info-zip.org/pub/infozip/>

BerkeleyDB 1.85

Original Package: <http://www.sleepycat.com/download/>

SHA-1 in C

Original Package: <ftp://ftp.funet.fi/pub/crypt/hash/sha/sha1.c>

Perl-Compatible Regular Expressions

Original Package: <http://www.pcre.org/>

libaes

Original Package: <http://sourceforge.net/projects/libaes/>

Digest::Perl::MD5

Original Package: <http://search.cpan.org/~delta/Digest-Perl-MD5-1.8/lib/Digest/Perl/MD5.pm>

Text::Iconv

Original Package: <http://search.cpan.org/~mpiotr/Text-Iconv-1.4/Iconv.pm>

jcode.pl

Original Package: <ftp://ftp.ij.ad.jp/pub/IIJ/dist/utashiro/perl/>

JRE (Java(TM) Platform, Standard Edition Runtime Environment)

Original Package: <http://java.sun.com/javase/downloads/index.jsp>

Apache Tomcat

Original Package: <http://tomcat.apache.org/>

Apache Myfaces(Myfaces Core / Myfaces Tomahawk)

Original Package: <http://myfaces.apache.org/>

GNU wget

Original Package: <http://www.gnu.org/software/wget/>

Location: "tool/wget" on installation directory

License: GPL