

F-Secure Internet Gatekeeper

Contents

Chapter 1: Welcome to F-Secure Internet Gatekeeper.....	5
1.1 Features.....	6
Chapter 2: Deployment.....	8
2.1 System requirements.....	9
2.2 Installing the product.....	9
2.2.1 Installing an rpm package.....	9
2.2.2 Installing a tar.gz package.....	9
2.3 Upgrading the product	10
2.3.1 Upgrading Internet Gatekeeper, international version.....	10
2.3.2 Upgrading Internet Gatekeeper, Japanese version	10
2.4 Uninstallation.....	12
2.4.1 Uninstalling the rpm package.....	12
2.4.2 Uninstalling the tar.gz package.....	12
Chapter 3: Typical configurations.....	13
3.1 Traffic scanning.....	14
3.1.1 HTTP connection.....	14
3.1.2 SMTP connection.....	14
3.1.3 POP connection	15
3.1.4 FTP connection	15
3.2 Network configuration examples.....	16
3.3 Internet Gatekeeper server settings	17
3.3.1 Accessing the web user interface.....	17
3.3.2 Typical configuration.....	18
3.3.3 Client settings.....	18
3.4 Using HTTP proxy for services that require a network access	19
3.5 Checking the product setup.....	19
Chapter 4: Using the product.....	20
4.1 HTTP proxy.....	21
4.1.1 Editing HTTP proxy settings.....	21
4.2 SMTP proxy.....	22
4.2.1 Editing SMTP proxy settings.....	22
4.3 POP proxy.....	26
4.3.1 Editing POP proxy settings.....	26
4.4 FTP proxy.....	28
4.4.1 Editing FTP proxy settings.....	28
4.5 ICAP service.....	30
4.5.1 Editing ICAP service settings.....	30

4.6 Global settings.....	31
4.6.1 Editing Global settings.....	31
4.7 Virus definition updates.....	33
4.7.1 Updating virus definition database.....	33
4.8 System information.....	34
4.8.1 Viewing system information.....	34
4.8.2 System information status.....	34
4.8.3 Run diagnostics.....	34
4.8.4 Download log files.....	34
4.8.5 Back up and restore the configuration.....	34
4.9 License.....	35
4.9.1 Updating the product license.....	35
4.9.2 Viewing the privacy policy.....	35
4.10 Admin password.....	35
4.10.1 Changing the password.....	35
Chapter 5: Advanced settings.....	36
5.1 Proxy settings.....	37
5.1.1 HTTP proxy.....	37
5.1.2 SMTP proxy	39
5.1.3 POP proxy.....	42
5.1.4 FTP proxy.....	44
5.1.5 Common settings	45
5.2 Virus scanning ICAP service settings	46
5.2.1 ICAP daemon settings	47
5.2.2 ICAP response headers	48
5.2.3 ICAP service daemon temporary files	49
5.2.4 ICAP error and status codes	50
5.3 Access control	50
5.4 Notification templates	52
5.4.1 Admin notification template.....	52
5.4.2 Virus detection notification templates	53
5.4.3 Error message template	53
5.5 Expert options	53
Chapter 6: Command-line tools.....	55
6.1 Taking new settings into use.....	56
6.2 Auto-start commands.....	56
6.3 Proxy execution	57
6.4 Virus definition updates	58
6.5 Restarting all services	61
6.6 Creating diagnostic Information	61
Chapter 7: Logs	62
7.1 Log files	63
7.1.1 Access logs	63

7.1.2 Virus and spam detection logs	67
7.1.3 Error logs.....	67
7.1.4 Information logs	68
7.2 Using Syslog with the F-Secure Anti-Spam daemon.....	68
7.3 Splitting and rotating log files	68
7.4 Time display conversion tool	68
7.5 Log analysis tools	69
7.6 External output of logs	70

Chapter 8: Other settings.....71

8.1 Access authentication.....	72
8.1.1 Host authentication.....	72
8.1.2 Authentication using virtual networks.....	73
8.1.3 Proxy authentication using Internet Gatekeeper	74
8.1.4 Authentication by mail servers	77
8.1.5 Authentication using POP-before-SMTP	78
8.2 Transparent proxy.....	79
8.2.1 Transparent proxy details.....	80
8.2.2 Transparent proxy in the router mode.....	81
8.2.3 Transparent proxy in the bridge mode.....	84
8.3 Coexisting with mail servers.....	86
8.3.1 Changing the port number of Internet Gatekeeper.....	86
8.3.2 Changing the port number of the mail server.....	87
8.3.3 Changing the IP address.....	89
8.4 Scanning viruses before saving mail to the mail server.....	92
8.5 Reverse proxy settings.....	94
8.5.1 Typical reverse proxy settings.....	94
8.5.2 Coexisting with web servers.....	95
8.5.3 Implementing a HTTPS (SSL) server.....	95

Chapter 9: Product specifications97

9.1 Specification summary.....	98
9.2 HTTP proxy process	100
9.3 SMTP proxy process	101
9.4 POP proxy process	102
9.5 FTP proxy process	103
9.6 HTTP error responses	107
9.7 HTTP request and response headers	109
9.8 SMTP command responses	111
9.9 SMTP commands - operations	113
9.10 POP commands - operations	116
9.11 FTP commands - operations	118
9.12 Connection error messages.....	120
9.13 Service process list.....	120
9.14 Detection names.....	121
9.15 Riskware	123

Welcome to F-Secure Internet Gatekeeper

Topics:

- [Features](#)

Highly effective and easy to manage protection solution for corporate networks at the gateway level.

Malware can enter an organization's network in many different ways. The most common source of infection used to be email, but today many web sites are filled with programs containing harmful and malicious content. Users can get infected through downloading such content by simply visiting websites which have been infected by malicious code. This kind of harmful data not only endangers security, but also decreases employee productivity, increases legal liability concerns, and wastes network bandwidth.

The easiest and most effective way to stop harmful content spreading via the Internet is to stop it already at the gateway level of the network. The product scans all incoming email, web and file transfer traffic and stops viruses and other malware before they can spread to corporate servers and end-users' desktops.

It blocks malware that can endanger confidential corporate data, waste network bandwidth and increase legal liability concerns. It can filter out specified file types such as non-work related movie or audio content which affect the productivity of an organization. The product is also flexible and easy to deploy, and can act as a transparent proxy.

The product meets all the needs of corporate networks and is cost-effective and easy to deploy and manage.

1.1 Features

The key features and benefits of the product.

The product protects a range of different networks against viruses:

- Internal company networks
- ISP networks
- Home networks
- A single computer that monitors the network access by all computers on the company, ISP, or home network.
- Does not use any resources from other computers on the network.
- Easy to install and administer on an existing network.
- Can be used both on large and small networks, also on less powerful computers.

Monitor web browsing and email traffic

- HTTP
- FTP
- SMTP
- POP

Simple installation

- Runs in almost all Linux environments
- Combines all functions in a single computer
- Can be installed as an rpm 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 product configuration file.

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 email can be sent to the administrator when a virus is detected
- The header and body of the notification email 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

Antivirus

- 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 incorrect detections 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 email body to detect spam by using customized conditions
- Uses the Spam detection engine
- Can use a Realtime Black List (RBL) to detect spam from the sender's email address
- Can use a SPAM URL Realtime Black List (SURBL) to detect spam that contains spam domain URLs in the email body
- Adds predefined text (such as "[[SPAM]]") to the email subject to allow easy sorting

Virus scanning ICAP service

- Support virus scanning ICAP service.
- The daemon fsicapd implements the ICAP protocol, as described in RFC 3507.
- The data is scanned using F-Secure technologies.
- It enables user to integrate virus scanning into third party HTTP proxy as long as the proxy can operate as an ICAP client and send the appropriate requests.

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 emails to allow easy sorting

Deployment

Topics:

- [*System requirements*](#)
- [*Installing the product*](#)
- [*Upgrading the product*](#)
- [*Uninstallation*](#)

This chapter describes how to deploy and install, the product in your network environment.

2.1 System requirements

For the latest information on minimum and recommended system requirements, see the product release notes.

2.2 Installing the product

Instructions how to deploy and install the product.

Use either the rpm package or tar.gz package to install the product.



Note: We recommend that you install the product using the rpm package if possible.

2.2.1 Installing an rpm package

Install the product by using the rpm package in a distribution that belongs to the Red Hat family of Linux distributions.

To install the product by using the rpm package:

Double-click the installation package, or run the following command on the command line with root privileges:

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

2.2.2 Installing a tar.gz package

Install the product using the tar.gz package if you cannot use the rpm package or you want to specify installation options during the installation.

To install the product by using the tar.gz package:

Run the following command on the command line with root privileges:

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



Important: We recommend that you use `make install` command for the installation and do not use any installation options for the default installation.

A list of installation options:

Option	Action	Instructions for use
<code>prefix=[dir]</code>	Specifies the installation directory.	We recommend that you install the product in the default installation directory (<code>/opt/f-secure/fsigk</code>).
<code>suffix=[name]</code>	Adds a suffix to the executable file and other command names (fsigk) to distinguish between each copy.	Use this option if you install multiple copies of the product on the same server. The suffix must be less than two characters.
<code>lang=[ja en]</code>	Specifies the language of the product. The available languages are "ja" (Japanese) and "en" (English).	If you do not specify the language, the installation sets it automatically. If the system time zone is JST or the LANG

Option	Action	Instructions for use
		environment variable starts with "ja", the product is installed in Japanese. Otherwise, the installation language is English.
<code>adminport=[num]</code>	Specifies a port number for the web console.	Use this option when you install multiple copies of the product on the same server. If you do not specify the port, the installation uses the default port (9012).

Command examples

To install the whole product, run the following command on the command line with root privileges:

```
# make install
```

To install another copy of the product on the same server, run the following command on the command line with root privileges:

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

2.3 Upgrading the product

Depending on your previously installed product version, use one of the following methods to upgrade the product.

2.3.1 Upgrading Internet Gatekeeper, international version

To upgrade an international version of F-Secure Internet Gatekeeper, follow the standard installation instructions.

If you are using Internet Gatekeeper version 4.06 or later, you do not need to uninstall the previous version before you upgrade the product. If you have an earlier version, uninstall it before you install the latest version.

2.3.2 Upgrading Internet Gatekeeper, Japanese version

If you are using a Japanese version of the product, follow these instructions to install the new, international product version.

Upgrade with an rpm package

Upgrade the product by using the rpm package in a distribution that belongs to the Red Hat family of Linux distributions.



Note: Run the following commands with root privileges.

To upgrade the product by using the rpm package:

1. Back up your current configuration.

```
# cd /opt/f-secure/fsigk
# tar zcvf conf-bak.tgz conf/
# cp conf-bak.tgz <back up directory>
```

2. Uninstall the old product version.

```
# rpm -e virusgw
```

3. Prepare the system for the new version.

a) Create the installation directory.

```
# mkdir -p /opt/f-secure/fsigk
```



Note: You must use the default installation directory when you install the product using an rpm package.

b) Copy your old configuration to the installation directory.

```
# cd /opt/f-secure/fsigk
# cp <back up directory>/conf-bak.tgz /opt/f-secure/fsigk/
# tar zxvf conf-bak.tgz
```

c) Rename the configuration file.

```
# cd conf
# mv virusgw.ini fsigk.ini
```

4. Install the new version of the product.

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

Upgrade with a tar.gz package

Upgrade the product using the tar.gz package if you cannot use the rpm package.



Note: Run the following commands with root privileges.

To upgrade the product by using the tar.gz package:

1. Back up your current configuration.

```
# cd <installation directory>
# tar zcvf conf-bak.tgz conf/
# cp conf-bak.tgz <back up directory>
```

2. Uninstall the old product version.

```
# cd <installation directory>
# make uninstall
# rm -rf <installation directory>
```

3. Prepare the system for the new version.

a) Create the installation directory.

```
# mkdir -p <installation directory>
```

b) Copy your old configuration to the installation directory.

```
# cd <installation directory>
# cp <back up directory>/conf-bak.tgz <installation directory>/
# tar zxvf conf-bak.tgz
```

c) Rename the configuration file.

```
# cd conf
# mv virusgw.ini fsigk.ini
```

4. Install the new version of the product.

```
# tar zxvf fsigk-xxx.tar.gz
# cd fsigk-xxx
# make install prefix=<installation directory>
```



Note: If you install the product to the default installation directory (/opt/f-secure/fsigk), you do not need to use the prefix option with the installation command.

2.4 Uninstallation

Follow the appropriate instructions depending on whether you installed the product by using the rpm or the tar.gz package.

2.4.1 Uninstalling the rpm package

This topic describes how to uninstall the product if it was installed with an rpm package.

To uninstall the rpm package:

1. Open the command line.
2. Run the following command with root privileges:

```
# rpm -e fsigk
```

The uninstallation removes installed files, deletes the configuration settings and shuts down the service.

2.4.2 Uninstalling the tar.gz package

This topic describes how to uninstall the product if it was installed with an tar.gz package.

To uninstall the tar.gz package:

1. Open the command line.
2. Run the following commands with root privileges:

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

The uninstallation removes installed files, deletes the configuration settings and shuts down the service.

Typical configurations

Topics:

- [*Traffic scanning*](#)
- [*Network configuration examples*](#)
- [*Internet Gatekeeper server settings*](#)
- [*Using HTTP proxy for services that require a network access*](#)
- [*Checking the product setup*](#)

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.

3.1 Traffic scanning

The following section describes how HTTP, SMTP, POP, and FTP connections operate when virus scanning is not used and when the product scans for viruses.

3.1.1 HTTP connection

How the product scans web browser traffic.

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

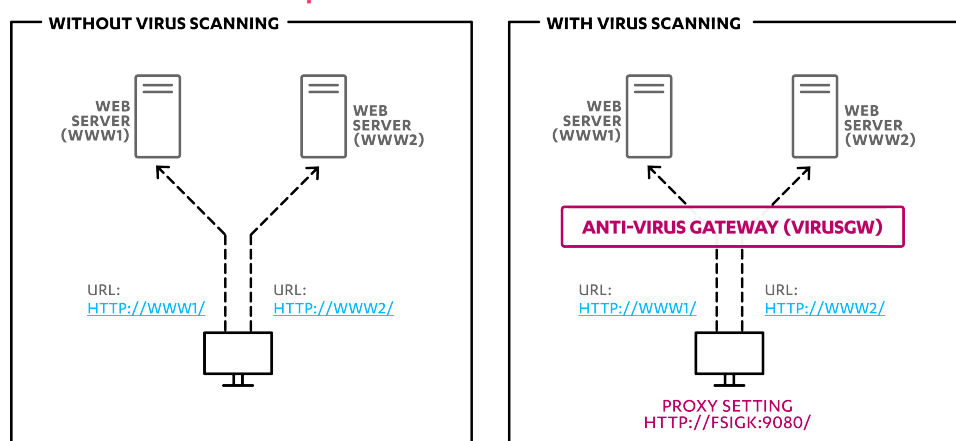


Figure 1: How HTTP connection works without and with virus scanning.

3.1.2 SMTP connection

How the product scans SMTP protocol email traffic.

Without virus scanning

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

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 email client. The client connects to the SMTP server through Internet Gatekeeper. The client sends outbound email to mail servers on the Internet. Internet Gatekeeper forwards the mail through the outbound mail server.

SMTP connection example

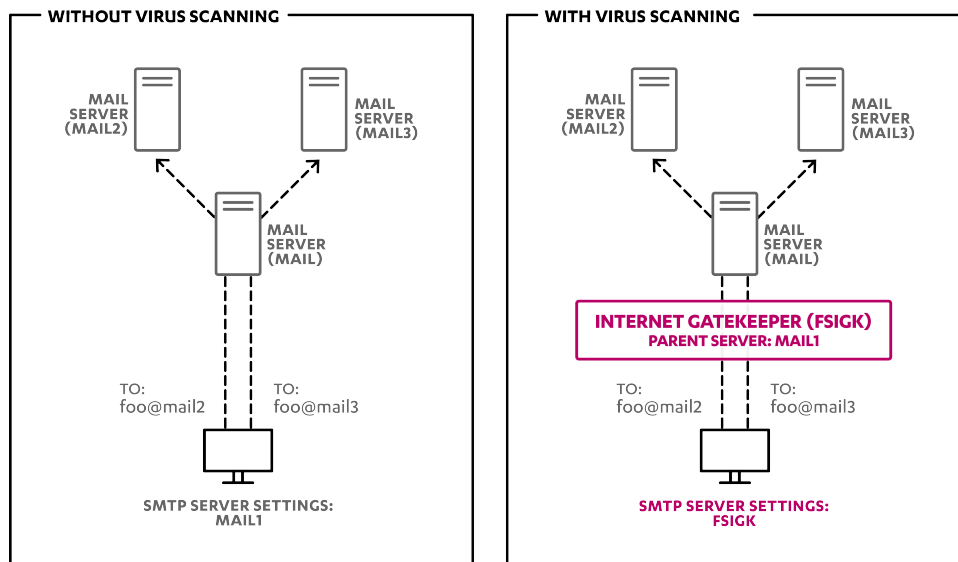


Figure 2: How SMTP connection works without and with virus scanning.

3.1.3 POP connection

How the product scans POP protocol email traffic.

Without virus scanning

To retrieve email, the email 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 email client. The client connects to the mail server through Internet Gatekeeper. The client retrieves email 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

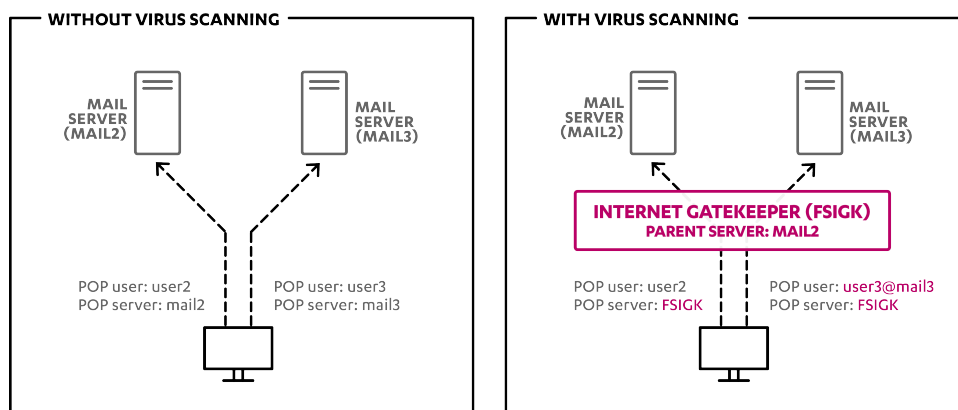


Figure 3: How POP connection works without and with virus scanning.

3.1.4 FTP connection

How the product scans FTP file transfers.

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

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

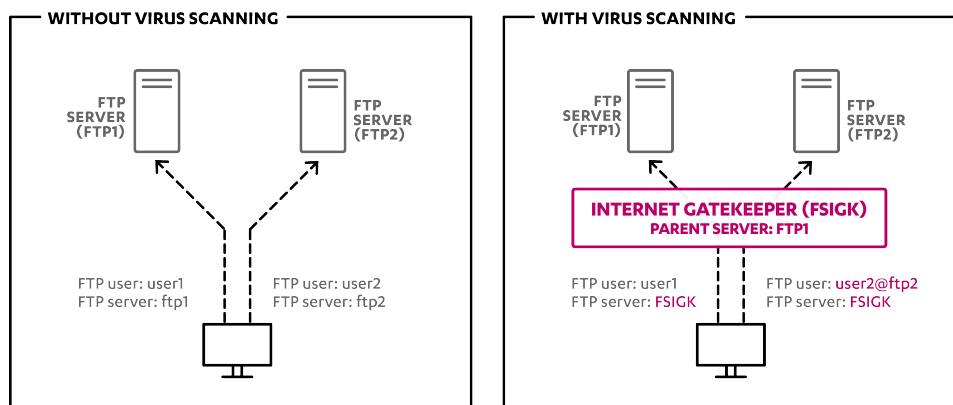


Figure 4: How FTP connection works without and with virus scanning.

3.2 Network configuration examples

F-Secure Internet Gatekeeper 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.



Note: The network configuration example 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.

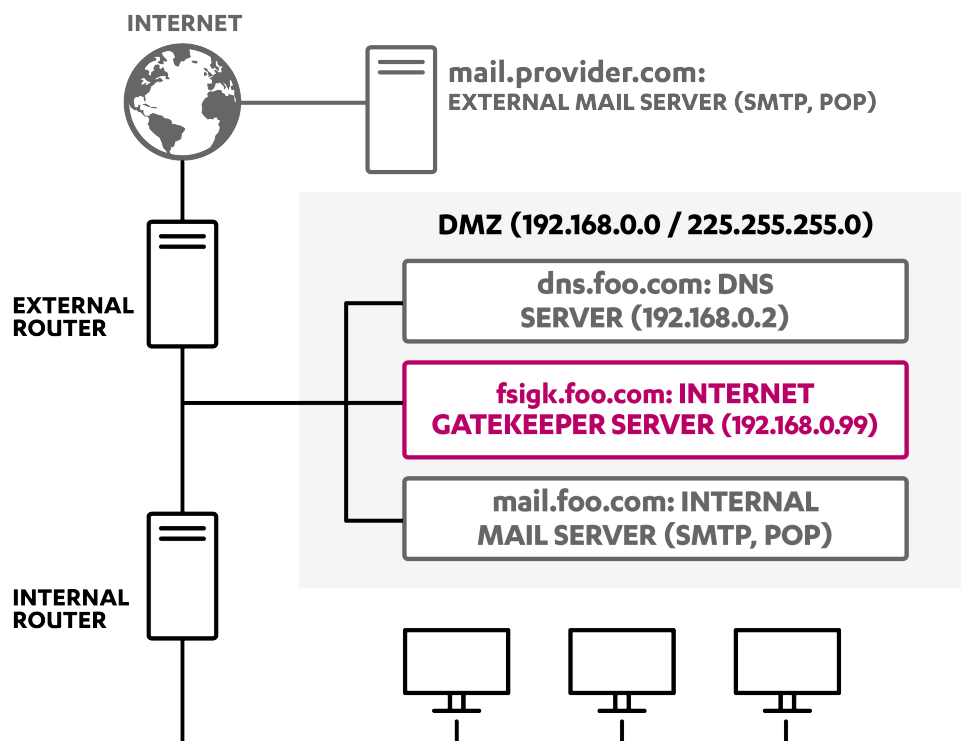


Figure 5: The network configuration example with the product located in a DMZ network.

3.3 Internet Gatekeeper server settings

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

3.3.1 Accessing the web user interface

Use the web user interface to change the product settings.

To access the web user interface, follow these instructions:

1. Open the following URL with your web browser: `http://<hostname>:9012/`
`<hostname>` is the domain name or the IP address of the server where the product is installed.
2. Enter your user name and password to log in.
 By default, the user name is `admin` and the password is `admin`.

 **Tip:** Open the **Admin password** tab to change your password.

3. The **Home** page of the web console opens after you have logged in.

After you log in, you can click **Change language** to select the language for the web user interface.

Registering the product

Enter your purchased license key to use the full license version of the product.

When you install the product, it is in the evaluation version mode. To upgrade the product to the full license version, follow these steps:

1. Open the web user interface.
2. Open the **License** settings.
3. Enter your purchased license key in the **License key** field.
4. Click **Save**.
5. Restart the product to take the full license into use.

3.3.2 Typical configuration

After you have completed the installation, edit the proxy settings to suit your network environment.

To configure the product, follow these instructions:

1. Open the web user interface.
2. Edit the HTTP proxy settings to scan the web traffic for malware.
 - a) Open the **HTTP** settings.
The **General** settings tab opens.
 - b) Turn on **HTTP proxy**.
 - c) Make sure that **Proxy port** is 9080.
3. Edit the SMTP proxy settings to scan emails that are transferred via SMTP protocol for malware.
 - a) Open the **SMTP** settings.
The **General** settings tab opens.
 - b) Turn on **SMTP proxy**.
 - c) Make sure that **Proxy port** is 9025.
 - d) Open the **Global** settings tab.
 - e) Set the name of the SMTP server that you use in the **Parent server hostname** field.
For example, mail.example.com.
 - f) Set the mail server port number in the **Parent server port number** field.
For example, 25.
4. Edit the POP proxy settings to scan emails that are transferred via POP protocol for malware.
 - a) Open the **POP** settings.
The **General** settings tab opens.
 - b) Turn on **POP proxy**.
 - c) Make sure that **Proxy port** is 9110.
 - d) Turn on **Parent server**.
 - e) Set the name of the POP server that you use in the **Parent server hostname** field.
For example, mail.example.com.
 - f) Set the mail server port number in the **Parent server port number** field.
For example, 110.
5. Edit the FTP proxy settings to scan files that are transferred via ftp protocol for malware.
 - a) Open the **FTP** settings.
The **General** settings tab opens.
 - b) Turn on **FTP proxy**.
 - c) Make sure that **Proxy port** is 9021.
6. Edit the administrator notifications settings.
 - a) Open **Global settings**.
The **Admin notification settings** tab opens.
 - b) Set the email address for notifications in the **E-mail addresses** field.
For example, fsigkadmin@example.com.
 - c) Set the mail server address that sends notifications in the **SMTP server host name** field.
For example, mail.example.com.
 - d) Set the mail server port number in the **Port number** field.
For example, 25.

You need to restart the product to take new settings into use.

3.3.3 Client settings

Change proxy server settings in user's web browsers and mail server settings in email clients to take the product into use.

Edit the following settings to start using the product in your network environment:

1. Edit the web browser settings.

- a) Go to the proxy server settings in the web browser.
 - b) Set the host name and port number where you installed the product as the proxy (for example, `fsigk.example.com` and `9080`).
2. Edit the email client settings.
- a) Go to the mail server settings in the email client.
 - b) Set the host name where you installed the product as the SMTP server and POP server for both internal and external emails (for example, `fsigk.example.com`).

 **Note:** You do not need to change the POP user name.

3.4 Using HTTP proxy for services that require a network access

Several product features require an HTTP access to F-Secure services, including automatic updates (fsaua) and spam detection (fsasd) which can be configured in the `/opt/f-secure/fsigk/conf/fsigk.ini` file.

Edit the following settings in the `/opt/f-secure/fsigk/conf/fsigk.ini` configuration file.

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.

 **Note:** Security Cloud (OrspService) uses a separate configuration option `orspservice_http_proxy` in `/opt/f-secure/fsigk/conf/fsigk.ini`.

3.5 Checking the product setup

Make sure that the product is working correctly after you have set up the proxy.

To check the proxy settings that you have configured after installing the product:

1. Download the anti-malware test file from the Eicar web site: http://www.eicar.org/anti_virus_test_file.htm.
2. To check that the SMTP proxy settings are working, send an email with eicar as an attachment via SMTP.
3. To check that the POP proxy settings are working, send an email with eicar as an attachment via POP.
4. To check that the FTP proxy settings are working, use FTP to send and receive the eicar file.

If the product does not scan all traffic that it should, see the error log:

`/opt/f-secure/fsigk/log/{http,smtp,pop,ftp}/error.log`.

Using the product

Topics:

- [*HTTP proxy*](#)
- [*SMTP proxy*](#)
- [*POP proxy*](#)
- [*FTP proxy*](#)
- [*ICAP service*](#)
- [*Global settings*](#)
- [*Virus definition updates*](#)
- [*System information*](#)
- [*License*](#)
- [*Admin password*](#)

After you have made sure that the product is installed correctly and working, you can configure its settings to suit your needs.

4.1 HTTP proxy

When you use the product as an HTTP proxy to scan the web traffic for viruses, web browsers connect to web servers through the product and receive web pages after those have been scanned for harmful content.

4.1.1 Editing HTTP proxy settings

Follow these instructions to edit the HTTP proxy settings.

1. In the web user interface, go to **Service settings > HTTP**.
2. Edit HTTP proxy settings on the **General** tab.
3. After changing the settings, click **Save and reload**.

HTTP proxy general settings

These settings are on the **Service settings > HTTP > General** tab in the web user interface.

HTTP proxy Turn HTTP proxy on or off.

Proxy port Specify the port number for the proxy service.



Note: You can specify only one inbound port. 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 and use iptables to redirect port 12345 to port 9080.

To do this, use the following command to set up iptables:

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

Then, save the iptables configuration:

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

For more information about iptables, see the documentation of your Linux distribution.

Virus scanning Turn the virus scanning on or off.



Note: HTTPS (SSL) traffic cannot be scanned for viruses because the communication is encrypted.

Scan files sent via POST or PUT method Specify whether to scan files that are sent by using POST and PUT methods of the HTTP protocol.

Notify the administrator when a virus is detected Send a virus detection message to the administrator when the virus scanning finds infected content.

To specify the email address and the mail server that you want to use, go to the **Global settings > Admin notification settings** page.

To edit the notification message, edit the file `/opt/f-secure/fsigk/conf/template_admin.txt`. The product adds an X-Admin-Notification-Id field to the notification message header.



Note: If you edit the notification message, you need to restart the service for the change to take effect.

Maximum number of simultaneous connections Specify the maximum number of connections that clients can have at any time. The specified number of processes listen for connections from clients.

To check the number of connections, see `Internal process ID` in the HTTP access log (`access.log`).

 **Note:** Increasing the maximum number of simultaneous connections requires more memory. One process uses approximately 500 KB or memory.

 **Tip:** We recommend that you set the initial value to 200 and monitor the performance. Usually, this value is set to less than 2000. The maximum value that is allowed is 9999.

Exclude these targets from the virus scan

User agent (web browser): Specify web browsers that are excluded from the virus scan.

Host name: Specify hosts that are excluded from the virus scan.

File name or extension: Specify files that are excluded from the virus scan based on their name or extension.

Maximum file size in bytes: Specify files that are excluded from the virus scan based on their size.

Maximum scanning time in seconds

Set the maximum time that can be used to scan a file.

You can terminate the virus scan if it takes too long time. By default, the value is 90 seconds. To make scanning time unlimited, set the value to 0.

 **Note:** Archives and other large files require longer time to scan than smaller files.

Parent server

If the product should connect to the web via a parent proxy, turn this setting on and set the host name and the server port for the parent proxy. If the product connects directly to the web, turn this setting off.

Parent server hostname Specify the host name of the parent proxy server.

Parent server port number Specify the port number of the parent proxy server.

4.2 SMTP proxy

When you use the product as an SMTP proxy to scan the emails for viruses, email clients connect to the SMTP server through the product. They send and receive emails after they have been scanned for spam and harmful content.

4.2.1 Editing SMTP proxy settings

Follow these instructions to edit the SMTP proxy settings.

1. In the web user interface, go to **Service settings > SMTP**.
2. Edit SMTP proxy settings on the **General** tab.
3. Edit settings on the **Global settings** tab to change settings for all connections that are not specified on the **LAN access settings**.
4. Edit settings on the **LAN access settings** tab to specify different operations for connections within a specific network or hosts.
5. Edit settings on the **Spam filter settings** tab to specify spam detection settings.
6. After changing the settings, click **Save and reload**.

SMTP proxy general settings

These settings are on the **Service settings > SMTP > General** tab in the web user interface.

SMTP proxy Turn SMTP proxy on or off.

Proxy port Specify the port number for the proxy service.



Note: You can specify only one inbound port. 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 and use iptables to redirect port 12345 to port 9080.

To do this, use the following command to set up iptables:

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

Then, save the iptables configuration:

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

For more information about iptables, see the documentation of your Linux distribution.

The product cannot receive encrypted traffic, such as SMTPS (TCP/port number 465) connections, directly, whether you use iptables to redirect connections or not. To scan encrypted traffic, you need to use an SSL proxy or accelerator to decrypt the traffic first before passing it through the product.

Virus scanning

Turn the virus scanning on or off.

Maximum number of simultaneous connections

Specify the maximum number of connections that clients can have at any time. The specified number of processes listen for connections from clients.

To check the number of connections, see `Internal process ID` in the HTTP access log (`access.log`).



Note: Increasing the maximum number of simultaneous connections requires more memory. One process uses approximately 500 KB or memory.



Tip: We recommend that you set the initial value to 200 and monitor the performance. Usually, this value is set to less than 2000. The maximum value that is allowed is 9999.

Blocked e-mail content

Encrypted and compressed files: Block all e-mails, which contain encrypted archive files (ZIP, RAR).

File name or extension

Exclude these targets from the virus scan

File name or extension: Specify files that are excluded from the virus scan based on their name or extension.

Maximum scanning time in seconds

Set the maximum time that can be used to scan a file.

You can terminate the virus scan if it takes too long time. By default, the value is 90 seconds. To make scanning time unlimited, set the value to 0.



Note: Archives and other large files require longer time to scan than smaller files.

SMTP proxy global settings

These settings are on the **Service settings > SMTP > Global settings** tab in the web user interface.

Parent server hostname

Specify the host name of the parent proxy server.

Parent server port number

Specify the port number of the parent proxy server.

What to do when a virus is detected	Choose actions to take when a virus is found. Pass: Only log the event but allow the infected content to pass. Block and notify the sender: Block the infected content and send a 554 <code>Infected by [virus name]</code> error to the sender. Delete: Delete the infected email without any notifications. Notify recipients after deleting the mail: Delete the infected content and send a virus detection message to recipients of the original message. Notify sender by e-mail after deleting the mail: Delete the infected content and send a virus detection message to the sender. Notify the administrator by e-mail: Send a virus detection message to the administrator when the virus scanning finds infected content. To specify the email address and the mail server that you want to use, go to the Global settings > Admin notification settings page. To edit the notification message, edit the file <code>/opt/f-secure/fsigk/conf/template_admin.txt</code>. The product adds an <code>X-Admin-Notification-Id</code> field to the notification message header.  Note: If you edit the notification message, you need to restart the service for the change to take effect. Quarantine: Turn the quarantine on or off. When you use the quarantine, the product moves infected content and spam messages to the quarantine directory. Infected emails and spam messages are stored in the mailbox format. To specify the quarantine directory, edit go to Global settings > Directory settings and edit Quarantine directory.
--	---

SMTP proxy LAN access settings

These settings are on the **Service settings > SMTP > LAN access settings** tab in the web user interface.

LAN access settings	Turn this setting on to use different virus scanning settings for LAN connections.
Hosts and networks within LAN	Specify hosts and networks to which the LAN access settings apply. If you use DNS Reverse Lookup, you can use the format: <code><host name>.<domain name></code> .
Parent server	If the product should connect to the web via a parent proxy, turn this setting on and set the host name and the server port for the parent proxy. If the product connects directly to the web, turn this setting off.
Parent server hostname	Specify the host name of the parent proxy server.
Parent server port number	Specify the port number of the parent proxy server.
What to do when a virus is detected	Choose actions to take when a virus is found. Pass: Only log the event but allow the infected content to pass. Block and notify the sender: Block the infected content and send a 554 <code>Infected by [virus name]</code> error to the sender. Delete: Delete the infected email without any notifications. Notify recipients after deleting the mail: Delete the infected content and send a virus detection message to recipients of the original message. Notify sender by e-mail after deleting the mail: Delete the infected content and send a virus detection message to the sender. Notify the administrator by e-mail:

Send a virus detection message to the administrator when the virus scanning finds infected content.

To specify the email address and the mail server that you want to use, go to the **Global settings > Admin notification settings** page.

To edit the notification message, edit the file `/opt/f-secure/fsigk/conf/template_admin.txt`. The product adds an `X-Admin-Notification-Id` field to the notification message header.



Note: If you edit the notification message, you need to restart the service for the change to take effect.

Quarantine: Turn the quarantine on or off.

When you use the quarantine, the product moves infected content and spam messages to the quarantine directory. Infected emails and spam messages are stored in the mailbox format.

To specify the quarantine directory, edit go to **Global settings > Directory settings** and edit **Quarantine directory**.

SMTP proxy spam filter settings

These settings are on the **Service settings > SMTP > Spam filter** tab in the web user interface.

Spam filtering

Turn the spam filtering on or off. When the spam filtering is on, the product adds `X-Spam-Status` field to the header of detected spam messages.



Tip: Use LAN access settings to block incoming spam and exclude outgoing e-mails from the spam filtering.

What to do when a spam is detected

Choose actions to take when a spam message is found.

Pass: Allow spam messages through. Email clients can use `X-Spam-Status` message header field to filter spam.

Modify the message subject: Modify the `Subject` field of the spam email. Enter the prefix that is added to the message subject.



Note: The prefix is encoded in UTF-8. If the subject of the spam email uses some other character encoding, it may not show correctly in some email clients.

Delete: Delete the spam email.



Tip: To avoid deleting emails that are incorrectly classified as spam, do not delete the emails at the gateway. Instead, allow spam messages through and filter spam with email clients.

Notify the administrator by e-mail: Send a spam detection message to the administrator when the spam filtering finds spam.

To specify the email address and the mail server that you want to use, go to the **Global settings > Admin notification settings** page.

To edit the notification message, edit the file `/opt/f-secure/fsigk/conf/template_admin.txt`. The product adds an `X-Admin-Notification-Id` field to the notification message header.



Note: If you edit the notification message, you need to restart the service for the change to take effect.

Quarantine: Turn the quarantine on or off.

When you use the quarantine, the product moves infected content and spam messages to the quarantine directory. Infected emails and spam messages are stored in the mailbox format.

To specify the quarantine directory, edit go to **Global settings > Directory settings** and edit **Quarantine directory**.

4.3 POP proxy

When you use the product as a POP proxy to scan the emails for viruses, email clients connect to the mail server through the product and receive emails after they have been scanned for spam and harmful content.

4.3.1 Editing POP proxy settings

Follow these instructions to edit POP proxy settings.

1. In the web user interface, go to **Service settings > POP**.
2. Edit POP proxy settings on the **General** tab.
3. Edit setting on the **SPAM filter settings** tab to specify spam detection settings.
4. After changing the settings, click **Save and reload**.

POP proxy general settings

These settings are on the **Service settings > POP > General** tab in the web user interface.

POP proxy Turn POP proxy on or off.

Proxy port Specify the port number for the proxy service.



Note: You can specify only one inbound port. 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 and use iptables to redirect port 12345 to port 9080.

To do this, use the following command to set up iptables:

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

Then, save the iptables configuration:

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

For more information about iptables, see the documentation of your Linux distribution.

The product cannot receive encrypted traffic, such as SMTPS (TCP/port number 465) connections, directly, whether you use iptables to redirect connections or not. To scan encrypted traffic, you need to use an SSL proxy or accelerator to decrypt the traffic first before passing it through the product.

Virus scanning Turn the virus scanning on or off.

What to do when a virus is detected Choose actions to take when a virus is found.



Note: With the POP protocol, you cannot block recipients from receiving messages completely.

Delete: Replace the infected email with a virus detection message. The product adds an X-Virus-Status field to the infected message header even when you choose not to delete the message.

Notify the administrator by e-mail:

Send a virus detection message to the administrator when the virus scanning finds infected content.

	To specify the email address and the mail server that you want to use, go to the Global settings > Admin notification settings page. To edit the notification message, edit the file <code>/opt/f-secure/fsigk/conf/template_admin.txt</code>. The product adds an <code>X-Admin-Notification-Id</code> field to the notification message header.  Note: If you edit the notification message, you need to restart the service for the change to take effect. Quarantine: Turn the quarantine on or off. When you use the quarantine, the product moves infected content and spam messages to the quarantine directory. Infected emails and spam messages are stored in the mailbox format. To specify the quarantine directory, edit go to Global settings > Directory settings and edit Quarantine directory.
Maximum number of simultaneous connections	Specify the maximum number of connections that clients can have at any time. The specified number of processes listen for connections from clients. To check the number of connections, see <code>Internal process ID</code> in the HTTP access log (<code>access.log</code>).  Note: Increasing the maximum number of simultaneous connections requires more memory. One process uses approximately 500 KB or memory.  Tip: We recommend that you set the initial value to 200 and monitor the performance. Usually, this value is set to less than 2000. The maximum value that is allowed is 9999.
Exclude these targets from the virus scan	File name or extension: Specify files that are excluded from the virus scan based on their name or extension.
Maximum scanning time in seconds	Set the maximum time that can be used to scan a file. You can terminate the virus scan if it takes too long time. By default, the value is 90 seconds. To make scanning time unlimited, set the value to 0.  Note: Archives and other large files require longer time to scan than smaller files.
Parent server	If the product should connect to the web via a parent proxy, turn this setting on and set the host name and the server port for the parent proxy. If the product connects directly to the web, turn this setting off.  Note: Although the product usually connects to a designated parent server, you can specify connections to any POP server. To do this, use the following format with POP user names: <code><POP server user name>@<POP server name></code>.
Parent server hostname	Specify the host name of the parent proxy server.
Parent server port number	Specify the port number of the parent proxy server.

POP proxy spam filter settings

These settings are on the **Service settings > POP > Spam filter** tab in the web user interface.

Spam filtering Turn the spam filtering on or off. When the spam filtering is on, the product adds `X-Spam-Status` field to the header of detected spam messages.

What to do when a spam is detected

Choose actions to take when a spam message is found.



Note: With the POP protocol, you cannot block recipients from receiving messages completely. Use the message subject prefix to filter spam with e-mail clients.

Pass: Allow spam messages through. Email clients can use `X-Spam-Status` message header field to filter spam.

Modify the message subject: Modify the `Subject` field of the spam email. Enter the prefix that is added to the message subject.



Note: The prefix is encoded in UTF-8. If the subject of the spam email uses some other character encoding, it may not show correctly in some email clients.

Notify the administrator by e-mail: Send a spam detection message to the administrator when the spam filtering finds spam.

To specify the email address and the mail server that you want to use, go to the **Global settings > Admin notification settings** page.

To edit the notification message, edit the file `/opt/f-secure/fsigk/conf/template_admin.txt`. The product adds an `X-Admin-Notification-Id` field to the notification message header.



Note: If you edit the notification message, you need to restart the service for the change to take effect.

Quarantine: Turn the quarantine on or off.

When you use the quarantine, the product moves infected content and spam messages to the quarantine directory. Infected emails and spam messages are stored in the mailbox format.

To specify the quarantine directory, edit go to **Global settings > Directory settings** and edit **Quarantine directory**.

4.4 FTP proxy

When you use the product as an FTP proxy to scan file transfers for viruses, clients connect to FTP servers through the product. Clients send and receive files after they have been scanned for harmful content.

4.4.1 Editing FTP proxy settings

Follow these instructions to edit the FTP proxy settings.

1. In the web user interface, go to **Service settings > FTP**.
2. Edit POP proxy settings on the **General** tab.
3. After changing the settings, click **Save and reload**.

FTP proxy general settings

These settings are on the **Service settings > FTP > General** tab in the web user interface.

FTP proxy

Turn FTP proxy on or off.

Proxy port

Specify the port number for the proxy service.



Note: You can specify only one inbound port. 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 and use iptables to redirect port 12345 to port 9080.

To do this, use the following command to set up iptables:

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

Then, save the iptables configuration:

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

For more information about iptables, see the documentation of your Linux distribution.

Virus scanning

Turn the virus scanning on or off.

What to do when a virus is detected

Choose actions to take when a virus is found.

Delete: Delete the infected email without any notifications.

Notify the administrator by e-mail:

Send a virus detection message to the administrator when the virus scanning finds infected content.

To specify the email address and the mail server that you want to use, go to the **Global settings > Admin notification settings** page.

To edit the notification message, edit the file `/opt/f-secure/fsigk/conf/template_admin.txt`. The product adds an `X-Admin-Notification-Id` field to the notification message header.



Note: If you edit the notification message, you need to restart the service for the change to take effect.

Quarantine: Turn the quarantine on or off.

When you use the quarantine, the product moves infected content and spam messages to the quarantine directory. Infected emails and spam messages are stored in the mailbox format.

To specify the quarantine directory, edit go to **Global settings > Directory settings** and edit **Quarantine directory**.

Maximum number of simultaneous connections

Specify the maximum number of connections that clients can have at any time. The specified number of processes listen for connections from clients.

To check the number of connections, see `Internal process ID` in the HTTP access log (`access.log`).



Note: Increasing the maximum number of simultaneous connections requires more memory. One process uses approximately 500 KB or memory.



Tip: We recommend that you set the initial value to 200 and monitor the performance. Usually, this value is set to less than 2000. The maximum value that is allowed is 9999.

Exclude these targets from the virus scan

Host name: Specify hosts that are excluded from the virus scan.

File name or extension: Specify files that are excluded from the virus scan based on their name or extension.

Maximum file size in bytes: Specify files that are excluded from the virus scan based on their size.

Maximum scanning time in seconds

Set the maximum time that can be used to scan a file.

You can terminate the virus scan if it takes too long time. By default, the value is 90 seconds. To make scanning time unlimited, set the value to 0.



Note: Archives and other large files require longer time to scan than smaller files.

Parent server

If the product should connect to the web via a parent proxy, turn this setting on and set the host name and the server port for the parent proxy. If the product connects directly to the web, turn this setting off.



Note: Although the product usually connects to a designated parent server, you can specify connections to any FTP server. To do this, use the following format with FTP user names: `<FTP server user name>@<FTP server name>`.

Parent server hostname

Specify the host name of the parent proxy server.

Parent server port number

Specify the port number of the parent proxy server.

4.5 ICAP service

The Internet Content Adaptation Protocol (ICAP) is used to implement virus scanning in transparent proxy servers.

The ICAP daemon implements the REQMOD, RESPMOD, and OPTIONS methods of the ICAP protocol.

If a REQMOD or RESPMOD request contains an encapsulated HTTP body, it is scanned for viruses. If it contains harmful content, the product replaces it with a web page that informs users that the content has been blocked.

4.5.1 Editing ICAP service settings

Follow these instructions to edit the ICAP service settings.

ICAP service requires that fsicapd daemon is running on the system.

1. In the web user interface, go to **Service settings > ICAP**.
2. Edit ICAP proxy settings on the **General** tab.
3. After changing the settings, click **Save and reload**.

ICAP service general settings

These settings are on the **Service settings > ICAP > General** tab in the web user interface.

ICAP service

Turn virus scanning on the ICAP service on or off. By default, the ICAP service listens to port 1344 for ICAP requests. Configure the proxy that uses the ICAP service to send requests to the daemon.

Bind address

Specify the network address or hostname to which the ICAP daemon binds.

By default, the daemon binds only to the local interface (127.0.0.1) for increased security. Use the value 0.0.0.0 to bind the daemon to all addresses.

Bind port

Specify the port number that the ICAP service listens. By default, the standard port is 1344.

Maximum number of simultaneous connections

Specify the maximum number of connections that ICAP daemon can have at any time. When the limit is reached, new clients receive an ICAP response with the status code 503, which indicates overload. By default, the value is 500.

Maximum scanning time in seconds

Set the maximum time that can be used to scan a file.

You can terminate the virus scan if it takes too long time. By default, the value is 90 seconds. To make scanning time unlimited, set the value to 0.



Note: Archives and other large files require longer time to scan than smaller files.

Connection timeout in seconds

Specify a timeout for connections. If an ICAP request has not completed before the timeout, the product closes the connection to the client. By default, the value is 600 seconds.

4.6 Global settings

Edit global settings to specify the administrator's email address, locations of the working directory and the quarantine directory, and spam filter settings that apply to all other spam filtering rules.

4.6.1 Editing Global settings

Follow these instructions to edit the global settings.

1. In the web user interface, go to **Global settings**.
2. Edit settings on the **Admin notification settings** tab to specify the administrator's email address and the mail server that sends notifications.
3. Edit settings on the **Directory settings** tab to change where temporary files and quarantined content is stored.
4. Edit settings on the **Spam filter settings** tab to change spam filter settings that affect both SMTP and POP proxies.
5. After changing the settings, click **Save and reload**.

Global administrator notification settings

These settings are on the **Global settings > Admin notification settings** tab in the web user interface.

Email addresses	Specify the administrator's email address. The product sends email notifications to this address, when you use the Notify the administrator by email setting. This address is also used as the sender address in notification emails in SMTP proxy settings. If you specify multiple addresses, the first address is used as the sender address.
SMTP server host name	Specify the mail server that sends virus detection notifications to the administrator.
Port number	Specify the port number on the mail server that sends virus detection notifications to the administrator. By default, the port number is 25.

Global directory settings

These settings are on the **Global settings > Directory settings** tab in the web user interface.

Temporary directory	Specify the work directory that is used to store files temporarily, which are being scanned for viruses. By default, the directory is <code>/var/tmp/fsigk</code> .
Quarantine directory	Specify the directory where detected viruses are stored when you use the quarantine. By default, the directory is <code>/var/tmp/quarantine</code> .

Global spam filter settings

These settings are on the **Global settings > Spam filter settings** tab in the web user interface.

Cloud-based spam scanning	Turn the cloud-based spam scanning on or off. The cloud-based spam scanning improves the spam detection rate on both SMTP and POP proxies.
Real-time black list (RBL)	Realtime black lists are used to publish the addresses of computers or networks that are linked to spamming. When this setting is on, the spam filtering uses Real-time Black Lists to detect spam messages.

An email is detected as spam if the source IP address (when using SMTP) and IP addresses in the received headers field are registered in an RBL server.



Note: If the RBL operation timeouts if no reply is received within one second, the email is not marked as spam.

Real-time black list servers	Specify real-time black list servers that you want to use. By default, the product uses <code>bl.spamcop.net</code> , <code>sbl-xbl.spamhaus.org</code> .
Addresses to be excluded	Do not use real-time black lists to check emails for the specified addresses. By default, <code>127.0.0.1</code> <code>10.</code> <code>192.168.</code> <code>172.16.0.0/255.240.0.0</code> addresses are excluded.
Spam URL real-time black list (SURBL)	SURBL servers collect and maintain lists of hosts that usually appear in spam messages. When this setting is on, the product searches email message bodies for links to these spam hosts.
Spam URL realtime black list servers	Specify SURBL servers that you want to use. By default, the product uses <code>multi.surbl.org</code> .

Global custom filter settings

These settings are on the **Global settings > Custom filter settings** tab in the web user interface.

You can use custom filtering rules to search for a string in a message header or body and either allow or disallow filtered messages.

Custom filtering rules Turn custom filtering rules on or off.

Rule scope Select the part of the message header or body where you want to search for the filtered string.



Tip: Select **Match always** to have the rule always match. For example, you can use this to create a rule that disallows all messages that are not otherwise allowed.

Rule scope: other message headers Select **Other** as the rule scope and specify the alternative message header that you want to search.

Match strings Specify strings that are searched for in the message. If any of the specified strings matches, the action of the rule is carried out.

Any leading or trailing spaces are ignored.

Match options Select additional options to match the string.

Match prefix	The string must be found at the beginning of the field or message part.
Match suffix	The string must be found at the end of the field or message part.
Case-sensitive match	The string must match the case exactly as entered.
Negate match	The rule is applied when the string is not found in the header field or message part.
"AND" with previous rule	The rule is applied only if the previous rule was applied as well.
"AND" with previous rule in same MIME part	The rule is applied only if the previous rule was applied in the same MIME part of the message.

Action Select whether the product should either allow or disallow messages that match the rule. Select **Chain with next rule** to combine the current filtering rule with the next filter on the rules list.

New rule number Select the filtering rule order.

Creating custom filtering rules

Follow these instructions to create custom mail filtering rules.

1. In the web user interface, go to **Global settings > Custom filter settings**.
2. Make sure that **Custom filtering rules** is **On**.
3. In **Rule scope**, select the message header field or body where you want to find strings.
4. In **Match strings**, enter strings that you want to match.
5. Modify your search with **Match options** if needed.
6. In **Action**, choose whether this rule allows or disallows messages that it matches. To combine the rule with another rule, select **Chain with next rule**.
7. In **New rule number**, choose the order in which your filtering rules take place.
The rule order is important; the first rule that finds a match is the one that is applied.
8. Click **Add rule** to add the rule to the rule number position that you selected.
 **Tip:** You can change the rule order later with **Move rule up** and **Move rule down** buttons.
9. Click **Save and reload** to take new rules into use.

4.7 Virus definition updates

To ensure an always up-to-date protection against the latest threats, keep virus definition databases up to date.

F-Secure updates virus definition databases typically multiple times a day. When automatic updates are on, the product retrieves the latest updates automatically.

4.7.1 Updating virus definition database

Follow these instructions to update the virus definition database.

 **Note:** When automatic updates are on, the product keeps the virus definition database updated automatically.

1. In the web user interface, go to **Virus definition updates**.
2. Click **Update now**.

Virus definition update settings

These settings are on the **Virus definition updates > Settings** tab in the web user interface.

Automatic updates	Turn automatic virus database updates on or off. When this setting is on, the product keeps the installed virus database up-to-date automatically.
Virus database version	Displays current database versions for scanning engines. Click Update now to check for the latest updates.
Proxy server	If the product needs to connect to the web via a proxy server, turn this setting on and set the host name and the server port for the proxy. If the product connects directly to the web, turn this setting off.
Proxy host name	Specify the host name of the proxy server.
Port number	Specify the port number of the proxy server.
HTTP proxy authentication	If the proxy uses authentication, turn this setting on and set the user name and password to set the authorization credentials.
User name	Specify the user name to authenticate to the proxy.
Change password	Specify the password to authenticate to the proxy.

4.8 System information

Under system information, you can view information about the installed product, run diagnostics, and back up and restore your settings.

4.8.1 Viewing system information

Follow these instructions to view the system information.

In the web user interface, go to **System information**.

4.8.2 System information status

These statistics are on the **System information > Status** tab in the web user interface.

Product version	Displays the currently installed product version and build number.
License expiration date	Displays the license status and its expiration date.
Virus database versions	Displays the current database versions for scanning engines.
Scan engines	Displays installed scanning engines.
Date	Displays the system date and time on the server where the product is installed.

4.8.3 Run diagnostics

When you contact the product support, provide them with the diagnostics information file (`diag.tar.gz`).

To create the diagnostics information file, follow these instructions:

1. In the web user interface, go to **System information > Diagnostics**.
2. Click the **Download diagnostics file** link.

4.8.4 Download log files

You can download and view the product log files with the web user interface.

To download a log file to view it:

1. In the web user interface, go to **System information > Download log files** tab.
The web user interface shows the log files in the product directory.
2. Click the name of the log that you want to view.
HTTP, SMTP, POP, FTP, and ICAP logs are in their own directories.

4.8.5 Back up and restore the configuration

You can back up the configuration to restore your settings later, for example after you upgrade the product.

Create a backup configuration

Create a backup configuration to save all your settings in an archive file.

To back up your settings:

1. In the web user interface, go to **System information > Backup and restore > Backup** tab.
2. Click **Backup configuration**.
The product compresses your settings into a `tar.gz` archive file.
3. Save the archive file for later use.

Restore the backed up configuration

You can restore your saved settings at any time.

To restore your settings:

1. In the web user interface, go to **System information > Backup and restore > Restore** tab.
2. Click **Browse** and select the archive file that you want to restore.
3. Click **Upload** to take the backed up settings into use.

4.9 License

On **License information** pages, you can update your product license and view the privacy policy.

4.9.1 Updating the product license

When you install the product, it is installed with an evaluation version license. You can update the product to the full license version with the web user interface.

To view and update your product license, follow these instructions:

1. In the web user interface, go to **License > License**.
License status displays your current license status and its expiration date.
2. To enter your new license key, type it into **License key** field.
3. Click **Save**.

4.9.2 Viewing the privacy policy

We seek to protect your privacy. The privacy policy describes the basic principles of how we process our customers' personal data.

To view the privacy policy, follow these instructions:

In the web user interface, go to **License > Privacy policy**.

4.10 Admin password

You need the password to log in to the web user interface.

4.10.1 Changing the password

Follow these instructions to change your administrator's password.

1. In the web user interface, go to **Admin password**.
2. Enter your current password in the **Old password** field.
3. Enter your new password in the **New password** field and enter it again on **Confirm new password** to make sure you typed it correctly.
4. Click **Save**.

Advanced settings

Topics:

- [Proxy settings](#)
- [Virus scanning ICAP service settings](#)
- [Access control](#)
- [Notification templates](#)
- [Expert options](#)

The configuration file contains advanced settings that you cannot configure with the web user interface.

If you need to make further changes to your configuration, use the `/opt/f-secure/fsigk/conf/fsigk.ini` configuration file to change the settings as required.

Save the configuration file after modifying the settings and restart the specified service by running `/opt/f-secure/fsigk/rc.fsigk_{http,smtp,pop,ftp} restart` command.

5.1 Proxy settings

Proxy settings specify how the virus scanning proxy works.

5.1.1 HTTP proxy

Advanced HTTP proxy settings.

What to do when a virus is detected

Delete
(`action={pass,delete}`)

Specify whether to delete detected 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.

Quarantine (quarantine)

Set `quarantine=yes` to enable the virus quarantine.

Set the `quarantine_dir` option under common settings in the configuration file to specify where viruses are quarantined.

Specify this setting only if sufficient disk space is available.

HTTP proxy authentication

Proxy authentication
(`proxyauth_pam_auth`)

Set `proxyauth_pam_auth=yes` to authenticate the proxy by using PAMs (Pluggable Authentication Modules).

To change the authentication method, edit the `/etc/pam.d/fsigk_http` file.

Add or remove users

Use the following commands using the files in

`/opt/f-secure/fsigk/conf/pam/` directory to add, delete, and modify users and passwords.

```
# echo -e username'/t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_http.txt
# ./create_userdb userdb_http.db < userdb_http.txt
```

Access control

From these hosts Set `acl_from=yes` to only accept connections from the designated list of hosts.
(`acl_from`)



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_from` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

To these hosts
(`acl_to`)

Set `acl_to=yes` to only accept connections to the designated list of hosts.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_from` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

DNS reverse lookup

DNS reverse lookup (`reverselookup`)

Set `reverselookup=yes/no` to look up the DNS entry for the source IP address.

This setting slightly reduces the processing speed.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format with the `[Access control]=[From these hosts]` settings. Also, the host name of the accessing host is shown in the access log.

Riskware scanning

Scan riskware (`riskware_check`)

Set `riskware_check=yes` to enable riskware scanning.

This detects riskware as well as known viruses.

Skip these targets (`pass_riskware`)

Exclude the specified riskware from detection.

Specify the riskware by using the format `Category.Platform.Family`.

The maximum length of the setting is 1999 bytes. Separate each setting in the setup file with a semicolon (;).



Tip: You can use wildcards (*) in the Category, Platform, and Family names. For example, `Client-IRC.*.*` excludes all riskware in the Client-IRC category.

Keep-Alive connection (`keepalive`)

Set `keepalive=yes` to use Keep-Alive connections (persistent connections).

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:

- The `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 (`keepalive_timeout`)

Specify 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 and transparent proxy modes

Anonymous proxy (`anonymous`)

Set `anonymous=yes` to enable the anonymous proxy. Anonymous proxy does not send information about the proxy or client (Via and X-Forwarded-For headers) to the server.

Transparent proxy mode (`transparent`)

Set `transparent=yes` to enable the transparent proxy mode.

If you use the proxy in transparent mode, you need to set the NAT redirection. Use the `iptables` command from the command line to specify the setting as follows:

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp --dport
80 \
-j REDIRECT --to-port 9080
```

Check file reputation with Security Cloud

ORSP file check (`orsp_file_check`)

Set `orsp_file_check=yes` to use F-Secure's Security Cloud to check files against constantly updating white and blacklists.

This can improve the reaction time against the new threats and decrease the load on system resources, which would be otherwise used to scan common files. By default, the value is "no", which means that no information is transmitted to Security Cloud.



Note: When using this feature, any information that is transmitted to F-Secure's servers is handled anonymously. For more information, see the `real-time-protection-network-policy.txt` file that is installed with the product.

File reputation check timeout (`orsp_timeout`)

Set the time (in milliseconds) that the product waits for response from Security Cloud when `orsp_file_check` is set to `yes` before the product scans the file locally.

The default value is 5000 (5 seconds).

5.1.2 SMTP proxy

Advanced SMTP proxy settings.

SMTP proxy authentication

SMTP authentication (`proxyauth_pam_auth`)

Set `proxyauth_pam_auth=yes` to perform the proxy authentication independently for each user.

Authentication is performed using PAMs (Pluggable Authentication Modules). To change the authentication method, edit the `/etc/pam.d/fsigk_smtp` file.



Note: If you have enabled also the `POP-before-SMTP` authentication setting, the email is sent if either SMTP authentication or POP-before-SMTP authentication is successful.

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

Add or remove users

Use the following commands using the files in `/opt/f-secure/fsigk/conf/pam/` directory to add, delete, and modify users and passwords.

```
# echo -e username'/t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_smtp.txt
# ./create_userdb userdb_smtp.db < userdb_smtp.txt
```

POP-before-SMTP authentication

POP-before-SMTP authentication (`pbs`)

Set `pbs=yes` to enable the 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, email can be sent if either SMTP authentication or POP-before-SMTP authentication is successful.



Note: If you have enabled also the Restrict email recipients setting, email to the specified domains can be sent even without authentication.

Timeout (pbs_lifetime) Set how long the POP-before-SMTP authentication remains valid (minutes).

Access control

From these hosts (acl_from) Set `acl_from=yes` to only accept connections from the designated list of hosts.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_from` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

To these hosts (acl_to) Set `acl_to=yes` to only accept connections to the designated list of hosts.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_to` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

DNS reverse lookup

DNS reverse lookup (reverselookup)

Set `reverselookup=yes/no` to look up the DNS entry for the source IP address.

This setting slightly reduces the processing speed.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format with the `[Access control]=[From these hosts]` settings. Also, the host name of the accessing host is shown in the access log.

Blocked email content

ActiveX (block_activex) Set `block_activex=yes` to block HTML emails with embedded ActiveX content.

When ActiveX content is detected, it is handled in the same way as viruses. If you disable virus scanning, ActiveX content scanning is also disabled.

The detection name is `FSIGK/POLICY_BLOCK_ACTIVEX`.

Scripts (block_script) Set `block_script=yes` to block HTML emails that contain scripts (JavaScript, VBScript, and similar).

When scripts are detected, they are handled in the same way as viruses. If you disable virus scanning, script scanning is also disabled.

The detection name is `FSIGK/POLICY_BLOCK_SCRIPT`.

**Partial messages
(block_partial_message)** Set `block_partial_message=yes` to block divided email messages. This blocks email with a Content-Type field value of message/partial in the email header.

When a partial message is detected, it is handled in the same way as viruses.

The detection name is `FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE`.

Riskware scanning

**Scan riskware
(riskware_check)** Set `riskware_check=yes` to enable riskware scanning.

This detects riskware as well as known viruses.

**Skip these targets
(pass_riskware)** Exclude the specified riskware from detection.

Specify the riskware by using the format `Category.Platform.Family`.

The maximum length of the setting is 1999 bytes. Separate each setting in the setup file with a semicolon (";").



Tip: You can use wildcards (*) in the Category, Platform, and Family names. For example, `Client-IRC.*.*` excludes all riskware in the Client-IRC category.

Scan the email message

**Scan text body part
(virus_check_text)** Set `virus_check_text=yes` to scan the body of email messages. Note that attached text-format files and HTML-format email 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 email body is not executed, you do not usually need to enable this setting.

**Scan whole html part
(virus_check_wholehtml)** Set `virus_check_wholehtml=yes` to scan the whole HTML part of email (parts of the HTML content of an email that most likely do not execute viruses, unlike parts such as ActiveX and scripts).

If you enable this setting, some suspicious email can also be detected (in addition to viruses). The suspicious email can be, for example, phishing emails 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 and transparent proxy modes

**Anonymous proxy
(anonymous)** Set `anonymous=yes` to enable the anonymous proxy mode.

Anonymous proxy does not add header information (Received header).

**Transparent proxy mode
(transparent)** Set `transparent=yes` to enable the transparent proxy mode.

If you use the proxy in transparent mode, you need to set the NAT redirection. Use the iptables command from the command line to specify the setting as follows:

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

5.1.3 POP proxy

Advanced POP proxy settings.

POP user restriction

PAM-based account verification (proxyauth_pam_account)

Set `proxyauth_pam_account=yes` to restrict users that can connect. Authentication is performed using PAMs (Pluggable Authentication Modules). To change the authentication method, edit the `/etc/pam.d/fsigk_pop` file.

Add or remove users

Use the following commands using the files in `/opt/f-secure/fsigk/conf/pam/` directory to add, delete, and modify users and passwords.

```
# echo -e username'/t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_pop.txt
# ./create_userdb userdb_pop.db < userdb_pop.txt
```

Access control

From these hosts (acl_from) Set `acl_from=yes` to only accept connections from the designated list of hosts.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_from` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

To these hosts (acl_to)

Set `acl_to=yes` to only accept connections to the designated list of hosts.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_to` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

DNS reverse lookup

DNS reverse lookup (reverselookup)

Set `reverselookup=yes/no` to look up the DNS entry for the source IP address.

This setting slightly reduces the processing speed.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format with the `[Access control]=[From these hosts]` settings. Also, the host name of the accessing host is shown in the access log.

Blocked email content

ActiveX (block_activex)

Set `block_activex=yes` to block HTML emails with embedded ActiveX content.

When ActiveX content is detected, it is handled in the same way as viruses. If you disable virus scanning, ActiveX content scanning is also disabled.

The detection name is `FSIGK/POLICY_BLOCK_ACTIVEX`.

Scripts (`block_script`)

Set `block_script=yes` to block HTML emails that contain scripts (JavaScript, VBScript, and similar).

When scripts are detected, they are handled in the same way as viruses. If you disable virus scanning, script scanning is also disabled.

The detection name is `FSIGK/POLICY_BLOCK_SCRIPT`.

Partial messages (`block_partial_message`)

Set `block_partial_message=yes` to block divided email messages. This blocks email with a Content-Type field value of `message/partial` in the email header.

When a partial message is detected, it is handled in the same way as viruses.

The detection name is `FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE`.

Encrypted archive files (`block_encrypted`)

Set `block_encrypted=yes` to block emails that contain encrypted and archived files (ZIP, RAR).

When an encrypted and archived file is detected, it is handled in the same as viruses. If you disable virus scanning, the scanning for encrypted and archived files is also disabled.

The detection name is `FSIGK/POLICY_BLOCK_ENCRYPTED`.

File name or extension (`block_ext,block_ext_list`)

Set `block_ext=yes` to block emails with the specified file names or extensions.

The setting is not case sensitive and uses backward matching (a file is blocked if the trailing characters of the file name match the specified file name or extension). Separate each name with a comma (","). For example: `.COM, .PIF, .EXE, .BAT`

Specify `ALL` to block all emails with attached files. The setting does not apply to files contained in archived files.

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

The maximum length of the setting is 1999 bytes.

The detection name is `FSIGK/POLICY_BLOCK_EXT`.

Riskware scanning

Scan riskware (`riskware_check`)

Set `riskware_check=yes` to enable riskware scanning.

This detects riskware as well as known viruses.

Skip these targets (`pass_riskware`)

Exclude the specified riskware from detection.

Specify the riskware by using the format `Category.Platform.Family`.

The maximum length of the setting is 1999 bytes. Separate each setting in the setup file with a semicolon (";").



Tip: You can use wildcards (*) in the Category, Platform, and Family names. For example, `Client-IRC.*.*` excludes all riskware in the Client-IRC category.

Scan the email message

Scan text body part (`virus_check_text`)

Set `virus_check_text=yes` to scan the body of email messages. Note that attached text-format files and HTML-format email 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 email body is not executed, you do not usually need to enable this setting.

**Scan whole html part
(virus_check_wholehtml)**

Set `virus_check_wholehtml=yes` to scan the whole HTML part of email (parts of the HTML content of an email that most likely do not execute viruses, unlike parts such as ActiveX and scripts).

If you enable this setting, some suspicious email can also be detected (in addition to viruses). The suspicious email can be, for example, phishing emails 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 mode

**Transparent proxy
(transparent)**

Set `transparent=yes` to enable the transparent proxy mode.

If you use the proxy in transparent mode, you need to set the NAT redirection. Use the iptables command from the command line to specify the setting as follows:

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

5.1.4 FTP proxy

Advanced FTP proxy settings.

FTP user restriction

**PAM-based account
verification
(proxyauth_pam_account)**

Set `proxyauth_pam_account=yes` to restrict users that can connect.

Authentication is performed using PAMs (Pluggable Authentication Modules). To change the authentication method, edit the `/etc/pam.d/fsigk_ftp` file.

Add or remove users

Use the following commands using the files in `/opt/f-secure/fsigk/conf/pam/` directory to add, delete, and modify users and passwords.

```
# echo -e username'/t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_ftp.txt
# ./create_userdb userdb_ftp.db < userdb_ftp.txt
```

Access control

**From these hosts
(acl_from)** Set `acl_from=yes` to only accept connections from the designated list of hosts.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_from` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See `man page hosts_access(5)` for more information on the syntax used in the file.

**To these hosts
(acl_to)**

Set `acl_to=yes` to only accept connections to the designated list of hosts.



Note: If you enable this setting in the configuration file, then specify the list of hosts in the `<protocol>_from` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file. Reload the configuration by running `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command. See man page `hosts_access(5)` for more information on the syntax used in the file.

DNS reverse lookup**DNS reverse lookup
(reverselookup)**

Set `reverselookup=yes/no` to look up the DNS entry for the source IP address.

This setting slightly reduces the processing speed.



Tip: Enable DNS Reverse Lookup to use the `<host name>.<domain name>` format with the `[Access control]=[From these hosts]` settings. Also, the host name of the accessing host is shown in the access log.

Riskware scanning**Scan riskware
(riskware_check)**

Set `riskware_check=yes` to enable riskware scanning.

This detects riskware as well as known viruses.

**Skip these targets
(pass_riskware)**

Exclude the specified riskware from detection.

Specify the riskware by using the format `Category.Platform.Family`.

The maximum length of the setting is 1999 bytes. Separate each setting in the setup file with a semicolon (;).



Tip: You can use wildcards (*) in the Category, Platform, and Family names. For example, `Client-IRC.*.*` excludes all riskware in the Client-IRC category.

Transparent proxy mode**Transparent proxy
(transparent)**

Set `transparent=yes` to enable the transparent proxy mode.

If you use the proxy in transparent mode, you need to set the NAT redirection. Use the `iptables` command from the command line to specify the setting as follows:

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

5.1.5 Common settings

Advanced settings that are common to all product components.

RBL (spam_rbl)

Set `spam_rbl=yes` to use of Realtime Black Lists (RBL) for spam checking.

Specify the servers separated by commas, maximum 199 characters.

When RBLs are used for spam checking, the source IP address (in the case of SMTP) and the IP addresses in the Received headers of emails are checked to see whether they are registered in an RBL server.

The maximum number of checked addresses per email is 32. By default, three RBL servers are set so 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 with POP. Excluded addresses are not counted.

By default, this setting is disabled.

The detection name for RBL is `FSIGK/SPAM_RBL/(detected address) [(RBL server name) : (RBL reply address)]`, where:

- Detected address = the address registered in the RBL server,
- RBL server name = the name of the RBL server in which the address was found, and
- RBL reply address = the reply address from the RBL server when spam is detected.

Server (spam_surbl_list) Specify the list of RBL servers. To specify multiple servers, separate them by commas (",").

By default: `bl.spamcop.net, sbl-xbl.spamhaus.org`

Addresses to be excluded Edit the `spam_rbl_pass` field in the global section of the `/opt/f-secure/fsigk/conf/fsigk.ini` file to disable RBL checking for the specified addresses.

By default: `127.0.0.1 10. 192.168. 172.16.0.0/255.240.0.0`

SURBL (spam_surbl)

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

Set `spam_surbl=yes/no` to enable or disable the setting.

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

When SURBLs are used for spam checking, the domain name parts of the URLs contained in the text body or HTML body of emails are checked to see whether they are registered in a SURBL server.

 **Note:** RBL and SURBL servers are queried together, but several hundred millisecond delay can occur while waiting for replies. If no reply is received within one second, the operation times out and the email is not identified as spam.

The DNS server that is used in SURBL queries is the first `nameserver` setting in `/etc/resolv.conf`.

The maximum number of queries per email is 32.

By default, this setting is disabled.

The detection name for SURBL is `FSIGK/SPAM_SURBL/(detected domain name) [(SURBL server name) : (SURBL reply address)]`, where:

- 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

Server (spam_surbl_list) Specify the list of SURBL servers. To specify multiple servers, separate them by commas (",").

By default: `multi.surbl.org`

5.2 Virus scanning ICAP service settings

The ICAP daemon implements the REQMOD, RESPMOD and OPTIONS methods of the ICAP protocol. If a REQMOD or RESPMOD request contains an encapsulated HTTP body, it will be scanned for viruses.

If an infected file is found, the ICAP daemon modifies the content for the response by replacing it with a HTML page informing the user that the content has been blocked. Editing virus notification templates to edit this HTML page.

The ICAP daemon recognizes the optional `Allow: 204` ICAP header, and when it is present, responds with the status code 204 if the requests needs no modification. It is recommended that the client proxy is configured to allow 204 responses when possible, to reduce network load and the amount of required disk space.

ICAP service requires that `fsicapd` daemon is running. You can change the settings mentioned in the following section by adding these to `[ICAP]` section of the product configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`.

You need to restart the daemon using `/opt/f-secure/fsigk/rc.fsigk_fsicapd restart` command after modifying the settings.

5.2.1 ICAP daemon settings

Scan limits

Maximum scan size (max_scan_size)	This value limits the size of content to scan. If the ICAP request contains an HTTP body larger than this limit, the request is allowed without scanning. A value of -1 disables the limit. It is recommended to have a scan size limit in place to prevent proxy delays caused by long scanning times, and limit the amount of temporary disk space the ICAP daemon uses. The default value is 2147483648 (2 GB).
Scan timeout blocking (scan_timeout_block)	If the maximum scanning time is reached while scanning, treat the content as infected and block it. The default is "no", which means that the content is not blocked if no infection is found within the allowed scanning time.
Block scan timeout contents (scan_timeout_block)	Set <code>scan_timeout_block=yes</code> to block contents if the scan times out. If set to no, the product treats the contents as clean if the scan times out. By default, the setting is disabled.

Check file reputation with Security Cloud

ORSP file check (orsp_file_check)	Set <code>orsp_file_check=yes</code> to use F-Secure's Security Cloud to check files against constantly updating white and blacklists. This can improve the reaction time against the new threats and decrease the load on system resources, which would be otherwise used to scan common files. By default, the value is "no", which means that no information is transmitted to Security Cloud.  Note: When using this feature, any information that is transmitted to F-Secure's servers is handled anonymously. For more information, see the <code>real-time-protection-network-policy.txt</code> file that is installed with the product.
File reputation check timeout (orsp_timeout)	Set the time (in milliseconds) that the product waits for response from Security Cloud when <code>orsp_file_check</code> is set to <code>yes</code> before the product scans the file locally. The default value is 5000 (5 seconds).

Email scanning

Enable email scanning (enable_email_services)	Set <code>enable_email_services=yes</code> to scan emails and check spam via ICAP service. By default, the setting is on.
Anti-spam daemon library path (fsasd_libpath)	Set the directory path where <code>fsicapd</code> searches for the <code>fsasd</code> library.

fsicapd searches for directories that have the following format: `<fsasd_libpath>.<timestamp>`. It uses the latest directory based on the timestamp. The specified path must be an absolute path.

Do not change the default path unless you move the database directory to a non-default location.

Anti-spam daemon socket path (fsasd_sockpath) Set the path of fsasd server socket.

The specified path must be an absolute path.

Do not change the default path unless you move the fsasd socket to a non-default location.

Riskware scanning

Block riskware (block_riskware) Set `block_riskware=yes` to enable riskware and grayware detection.

By default, the setting is disabled.

Archive scanning

Archive scanning (scan_archives) Set `scan_archives=yes` to scan files inside archives.

If the archive scanning is disabled, ICAP service scans archive files but does not extract files inside the archive itself.

Block encrypted archives (block_encrypted_archives) Set `block_encrypted_archives=yes` to block encrypted archive files.

If the setting is enabled and an archive cannot be scanned because it is encrypted, the product reports an infection with the name `Encrypted_archive`. If the setting is disabled, the product reports the encrypted archive as clean if the scanning fails.

This setting has effect only when the `scan_archives` setting is enabled.

Maximum archive nested level (max_nested) Set the number of maximum level of nested archives to be scanned. The product scans nested archives up to this depth.

This setting has effect only if the `scan_archives` setting is enabled.

Block nested archive (block_archive_max_nested) Set `block_archive_max_nested=yes` to block archives that exceed the maximum nested level. If the setting is enabled and an archive cannot be scanned because it exceeds the maximum depth limit for nested archives (the `max_nested` value) the product reports an infection with the name `Archive_max_nested`.

This setting has effect only when the `scan_archives` setting is enabled.

5.2.2 ICAP response headers

We recommend that ICAP clients use the 'Allow:204' ICAP header when possible. That way the server can respond to clean requests with a short response.

When an infection has been found, fsicapd responds with ICAP result code 200 (assuming that no error happened). Information of the infection is available in the following ICAP response headers:

Header	Description	Value	Note
X-Fsecure-Scan-Result	Reports the scanning result. This header is included in all REQMOD and RESPMOD responses	'clean', 'infected', 'suspected', 'grayware', 'spam', or 'whitelisted'	If the message is both spam and malware, the malware detection takes precedence
X-Fsecure-Infection-Name	Reports the infection name	The infection name as a string	The header is not included if the scan result is clean
X-Fsecure-FSAV-Duration	Reports the actual time that scanning daemon fsavd took to scan the infection	The scan time as a number (in seconds)	The header is only included for the operations that were actually done to get the scan result
X-Fsecure-Transaction-Duration	Reports the total time used to process a single request. This is the number of seconds between the time the server finished receiving the ICAP request headers and the time the ICAP response headers were generated	The total time as a number (in seconds)	
X-Fsecure-Spamcheck-Duration	Reports the scan time that spam scanning daemon fsasd took to scan for spam	The total time as a number (in seconds)	
X-Fsecure-Infected-Filename	Reports the name of the file that was detected as infected	The file name as a string	This header is not included if the name of the file is not known. The filename can be reported only if detection was caused by a file inside an archive or in a MIME email attachment. The file name is URL encoded so that it can contain non-ASCII characters

5.2.3 ICAP service daemon temporary files

When ICAP service daemon (fsicapd) scans an HTTP request or response body, the encapsulated body is decoded from chunked encode format and written to a temporary file, which exists until the ICAP request is complete.

The number and maximum size of such temporary files depend on fsicapd's settings and behavior of the ICAP client as follows:

- The total number of temporary files is at most the number of connected clients (`max_conn`). If an ICAP request contains the `Allow: 204` header, a limit for the scan size is set (`max_scan_size`) and the maximum size of the temporary file is this value.
- If ICAP request does not contain the `Allow: 204` header, or no size limit is set, the whole body will be stored. In this case, there is no upper limit for the size of the temporary file.

The administrator should allocate enough disk space and configure scan limits and maximum number of connections carefully to avoid running out of temporary disk space. If `fsicapd` fails to write to a temporary file while handling an ICAP request, the client will be served a response with error code 500. The proxy using the ICAP service should be configured to handle these appropriately to prevent it accidentally passing through infected content.

5.2.4 ICAP error and status codes

The following table lists the ICAP status codes are implemented and returned by the ICAP service daemon when appropriate.

Code	Reason
200	ICAP server returns a possibly modified response or request. Also used for successful OPTIONS responses.
204	The HTTP request or response is clean. The proxy should use the original request or responses without modification
400	ICAP protocol error: failed to parse ICAP request from client
500	Internal error: ICAP daemon most likely out of disk space or memory
503	The allowed maximum number id connections already reached, service overloaded



Note: For a more thorough explanation of the ICAP protocol, refer to RFC 3507 and the documentation of the HTTP proxy that you intend to use as the ICAP client.

5.3 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.



Note: The access control uses `tcpwrapper`. For more information about `tcpwrapper`, run `man 5 hosts access` from the command line.

These examples show how to specify proxy service settings in the `/opt/f-secure/fsigk/conf/fsigk.ini` configuration file for the following settings:

- From these hosts (`acl_from`)
- To these hosts (`acl_to`)
- Restrict email recipients (`acl_rcpt`)
- Host name (`acl_pass_to`)

- Address to be excluded (`spam_rbl_pass`)

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.com	Permit connections for the host name "host.domain.com". This does not permit connections for "xxx.host.domain.com".
.domain.com	Permit connections for host names that end in ".domain.com". This permits connections for "xxx.domain.com", but not for "domain.com".
domain.com .domain.com	Permit connections for "domain.com" and domains that are part of "domain.com". This permits connections for both "xxx.domain.com" and "domain.com".
192.168. (or: 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 1.2.3.4 4.5.6.7	Permit connections from all IP addresses except 1.2.3.4 and 4.5.6.7.
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.com EXCEPT 999.999.999.999 987.654.321.123	Permit connections for host names that end in ".domain.com" unless the IP address is 999.999.999.999 or 987.654.321.123.
/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 2000 bytes

The access control settings in the `/opt/f-secure/fsigk/conf/fsigk.ini` file permits a maximum of 2000 bytes per line. Use the following method if you want to specify lines longer than 2000 bytes.

1. 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
```

- Specify the file (for example, `/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 access control settings file (`/opt/f-secure/fsigk/conf/fsigk.ini`).

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

5.4 Notification templates

Edit all notification templates in the `/opt/f-secure/fsigk/conf/en(jp)` directory in English or Japanese language.



Note: If you edit the templates from the command line, you need to restart the respective service afterwards.

5.4.1 Admin notification template

Edit the admin detection notification template file `template_admin.txt` to change the message that the product uses to notify the administrator.

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

When sending a notification email to the sender or administrator from the SMTP service, 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: You need to restart the service after editing the template.

Variables that can be used in virus detection messages

<code>\${SERVICE_TYPE}</code>	Service type ("http" or "smtp" or "pop" or "ftp")
<code>\${DETECTION_NAME}</code>	Virus or other detection name (W95/Klez.H@mm, etc.)
<code>\${VIRUS_INFO_URL}</code>	URL for information about a virus
	Example: "http://cgi.f-secure.com/cgi-bin/search.cgi?q=W32/NetSky.D@mm"
<code>\${CLIENT_HOST}</code>	Client host name
	Note: To show the host name, you must enable [DNS Reverse Lookup]
<code>\${CLIENT_ADDR}</code>	Client IP address
<code>\${SERVER_HOST}</code>	Server host name (the server which is connected to from the Internet Gatekeeper)
<code>\${SERVER_ADDR}</code>	Server IP address (the server which is connected to from the Internet Gatekeeper)
<code>\${STATUS}</code>	Response code (the same value as is shown in the access log)
<code>\${METHOD}</code>	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".

<code>\${URL}</code>	URL of the accessed site
<code>\${CONTENT_TYPE}</code>	Value indicating the Content-Type (Example: text/html)
<code>\${CONTENT_LENGTH}</code>	Size of the transferred file (number of bytes)
<code>\${FILENAME}</code>	Name of the detected file
<code>\${QUARANTINE_FILE}</code>	Name of the quarantined file
<code>\${TIME}</code>	Access time (number of seconds since 1970/01/01)
<code>\${TIME_STR}</code>	Access time in text format (Example: 'Tue May 7 16:16:17 2002')
<code>\${HEADER}</code>	Content of the header
<code>\${TEXT}</code>	Content of the text message
<code>\${MAILFROM}</code>	SMTP sender address (the address passed to the "MAIL FROM:" command)
<code>\${RCPTTO}</code>	SMTP recipient addresses (the addresses passed to the "RCPT TO:" command, separated by commas (","))
<code>\${MESSAGE_ID}</code>	Value of the Message-Id field in the SMTP email header
<code>\${ERROR_STR}</code>	Error message (the same information as PROXY-ERROR in the access log)
<code>\${ACTION}</code>	Action which is taken when a virus is detected (the same information that is recorded in the access log)
<code>\${PATH_QUERY}</code>	Path and query part of the URL (only applies to the HTTP service)

5.4.2 Virus detection notification templates

Virus detection notification templates for HTTP, SMTP, POP proxies are in the `conf` directory.

The `conf` directory, by default `/opt/f-secure/fsigk/conf/`, contains template files `template_http.html`, `template_http_post.html`, `template_http_blocked.html`, `template_smtp.txt`, `template_smtp_lan.txt`, and `template_pop.txt`.

The ICAP detection notification template is in:

`/opt/f-secure/fsigk/fsicapd/templates/fsicapd_infected.html`.

Templates contain 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 900 bytes.



Note: `/opt/f-secure/fsigk/` is the default installation directory for the Internet Gatekeeper.

5.4.3 Error message template

Edit the error message template `template_http_error.html` to change the message that is shown when an error occurs.

Enter the message by using the UTF-8 character set. The maximum length of the message is 900 bytes.

5.5 Expert options

Reference information for expert options

Usually, you do not need to specify any other settings than those available through the configuration file 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.

Command-line tools

Topics:

- [*Taking new settings into use*](#)
- [*Auto-start commands*](#)
- [*Proxy execution*](#)
- [*Virus definition updates*](#)
- [*Restarting all services*](#)
- [*Creating diagnostic Information*](#)

Use command-line tools to use the product from the command-line.

You do not need to use command-line commands regularly as you can use the web console for the common operations.

6.1 Taking new settings into use

When you make changes to configuration files, you need to restart the proxy to take new settings into use.

 **Note:** The proxy restarts automatically when you change settings in the web console.

To restart proxy:

Run the proxy auto-start command: `rc.fsigk_{http,smtp,pop,ftp}`
The auto-start command initializes and starts the proxy (`fsigk`).

6.2 Auto-start commands

You can use the auto-start commands to start, stop, and restart proxies and the virus verification engine.

Overview of operations

Auto-start commands (`initscript`) can be used to start, stop, and restart the proxy execution command (`fsigk`) or the virus verification daemon(`fsavd`).

 **Note:** Launch the virus verification engine before you start each proxy service.

Command names

<code>/opt/f-secure/fsigk/rc.fsigk_http</code>	HTTP proxy auto-start command
<code>/opt/f-secure/fsigk/rc.fsigk_smtp</code>	SMTP proxy auto-start command
<code>/opt/f-secure/fsigk/rc.fsigk_pop</code>	POP proxy auto-start command
<code>/opt/f-secure/fsigk/rc.fsigk_ftp</code>	FTP proxy auto-start command
<code>/opt/f-secure/fsigk/rc.fsigk_fsavd</code>	Virus verification engine
<code>/opt/f-secure/fsigk/rc.fsigk_admin</code>	Web console auto-start command

Options

<code>start</code>	Starts the proxy
<code>stop</code>	Stops the proxy
<code>restart</code>	Restarts the proxy
<code>status</code>	Displays the status of the proxy

Restarting the HTTP proxy

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

Configuring 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
```

6.3 Proxy execution

Overview of operations

Executes a proxy according to the set options in the 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
```

 **Note:** `fsigk` command must be executed from the installation directory.

Options:

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

<code>--http</code>	Uses the <code>http</code> protocol (default when started with <code>fsigk_http</code>)
<code>--smtp</code>	Uses the <code>smtp</code> protocol (default when started with <code>fsigk_smtp</code>)
<code>--pop</code>	Uses the <code>pop</code> protocol (default when started with <code>fsigk_pop</code>)
<code>--ftp</code>	Uses the <code>ftp</code> protocol (default when started with <code>fsigk_ftp</code>)
<code>-f <inifile></code>	Reads the settings of <code>inifile</code> 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:

<code>--daemon</code>	Starts in the background
<code>-q</code>	Stops the detailed display

<code>-P <port></code>	Listens to the specified port number
<code>-h</code>	Displays a list of options

Command examples

Start a HTTP proxy (default)

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

- Start in the foreground

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

- Start in the foreground
- Display detailed information

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

- 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
```

6.4 Virus definition updates

Updates virus definition files.

Overview of operations

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

Specify update proxy settings in the updates section of `/opt/f-secure/fsigk/conf/fsigk.ini`.

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.

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

 **Note:** The configured proxy information is stored in `/opt/f-secure/fsigk/conf/fsigk.ini` 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

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

 **Note:** Check the version number of virus definition database files with the `cd /opt/f-secure/fsigk; make show-dbversion` command.

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/aquilnx32/aquarius-linux-update.ini` and `databases/fse/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.

If you change proxy settings in the configuration file `conf/fsigk.ini`, reload the configuration by running the `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` command.

Command names

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

<code>--help</code>	Displays a quick help which lists command-line options.
<code>--auto</code>	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.

`fsdbupdate.run`

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

Configuration file

`/opt/f-secure/fsigk/conf/fsigk.ini`

<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
<code>updateurl=http://host name:port number/</code>	Specifies the URL of Policy Manager in cases when the virus definitions are to be downloaded from Policy Manager.

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`

Exit codes

The update results use 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. For more information, check the Linux signal numbers with commands such as `man 7 signal`.

Command examples

Update virus definitions.

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

Import from a specific definition file (fsdbupdate.run).

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

6.5 Restarting all services

Overview of operations

Restarts all services (http, smtp, pop, ftp, admin) that are enabled.

Command names

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

Command examples

Restart all services that are enabled.

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

6.6 Creating diagnostic information

Overview of operations

Create 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.



Tip: Send the diagnostic information file (diag.tar.gz) when contacting support.

Command names

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

Command examples

Create a diagnostic information file.

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

Logs

Topics:

- [Log files](#)
- [Using Syslog with the F-Secure Anti-Spam daemon](#)
- [Splitting and rotating log files](#)
- [Time display conversion tool](#)
- [Log analysis tools](#)
- [External output of logs](#)

F-Secure Internet Gatekeeper records access status, virus detection status, and error occurrences to log files.

The log files are saved in the `/opt/f-secure/fsigk/log/` directory and a directory is created for each service.

7.1 Log files

7.1.1 Access logs

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

The product saves logs in the Squid log compatible format. Logs are formatted in the following manner.

Log format

Connection statuses are recorded one line at a time. Each item 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. Status code 200 is returned for non-HTTP successful connections, 500 when an 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 <code>pop://POP_user_name@POP_server_name:port_number</code> . When smtp is used, the URL is <code>mail:destination</code> .	
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	Returns "DETECT-STAT:[Detection results]:[Virus name]:[File name]:[Quarantined file name]::".	
	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	Returns "ACTION:[Action]:".	
Action	Either of the following actions are returned according to the detection results:	
	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	Returns "PROXY-STAT:[Service type]:[Internal process ID]:[Process ID] :[IP address of host]:[Number of processed files]:[Number of checks]:[Detection time]:[Detection details]:".	
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: 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 Returns "PROTOCOL-STAT:[sender address]:[Message-ID]:".
	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

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

KEEPALIVE	Displays the detection details with the following strings separated by a comma: 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. Returns "PROXY-ERROR:[Error information]:".

Error message	The following error message is displayed (Displayed with URL encode.): CONNECT (Host name: Port number / Connection error message. Common for both HTTP and SMTP protocols. HTTP An HTTP error response message appears. SMTP 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.)

7.1.2 Virus and spam detection logs

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



Note: The format of the logs is identical with access logs.

7.1.3 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.

Error message format

- Time (seconds)
- Internal process ID
- Log level
- [Internal location information]
- [Client address/Client port number/Client side file descriptor]
- [Server address/Server port number/Server side file descriptor]
- Error message

The time indicates the time when the error occurred. It is displayed counting from epoch time (1970/01/01 00:00:00(UTC)) in seconds and microseconds.

For errors relating with OS system calls, the following is inserted before the error message: `System call=Error message(Error code)`

- System call: the call that failed
- Error message: error message for system calls
- Error code: error code for system calls



Note: For more information on the error message content, see the F-Secure knowledge base article: <http://community.f-secure.com/t5/E-mail-and-Web/Internet-Gatekeeper-error-logs/ta-p/17436>

7.1.4 Information logs

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

Message format

- Time (seconds)
- Internal process ID
- Log level
- [Internal location information]
- [Client address/Client port number/Client side file descriptor]
- [Server address/Server port number/Server side file descriptor]
- 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:** For more information on the message content, see the F-Secure knowledge base article: <http://community.f-secure.com/t5/E-mail-and-Web/Internet-Gatekeeper-error-logs/ta-p/17438>

7.2 Using Syslog with the F-Secure Anti-Spam daemon

The F-Secure Anti-Spam daemon can log its actions in the default system log.

To set the syslog option for the F-Secure Anti-Spam daemon (`fsasd`):

Edit the `/opt/f-secure/fsigk/conf/fsigk.ini` configuration file and specify the `fsasd_syslog_facility` option in the global section.

By default, the logging value is `LOG_LOCAL0`.

 **Note:** For more information, refer to the Syslog documentation to change the default value.

7.3 Splitting and 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 follow the steps:

1. Set the configuration file

Copy the Sample configuration file (`/opt/f-secure/fsigk/misc/logrotate.fsigk`) to `/etc/logrotate.d/fsigk`.

```
# 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
```

7.4 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>
```

If you use Windows, run the tool with `/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.

7.5 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.

Run the following command to perform the daily access analysis with Webalizer:

```
# 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.



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
```



Tip: You can also use commercial log analyzing tools such as Sawmill. With Sawmill and other similar tools, you can perform a more detailed log analysis, which includes virus information. For information on Sawmill, see <http://www.sawmill.net/>.

7.6 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:

- For access logs: `access_log=|<External command>`
- For virus logs: `detect_log=|<External command>`
- For information logs: `info_log=|<External command>`
- For error logs: `error_log=|<External command>`

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, run the `/opt/f-secure/fsigk/rc.fsigk_{http,smtp,pop,ftp} restart` command to restart the service.

Other settings

Topics:

- [*Access authentication*](#)
- [*Transparent proxy*](#)
- [*Coexisting with mail servers*](#)
- [*Scanning viruses before saving mail to the mail server*](#)
- [*Reverse proxy settings*](#)

This chapter describes additional settings, which you can configure for the product.

For most users, the typical configuration provides enough security. However, some users may require additional security. In this case, the examples in this chapter may be useful.

8.1 Access authentication

To prevent unauthorized access to Internet Gatekeeper, you can define that hosts which access Internet Gatekeeper from the Internet are authenticated.

8.1.1 Host authentication

If the host which accesses the gateway is fixed, you can use IP addresses and host names to set the access control.

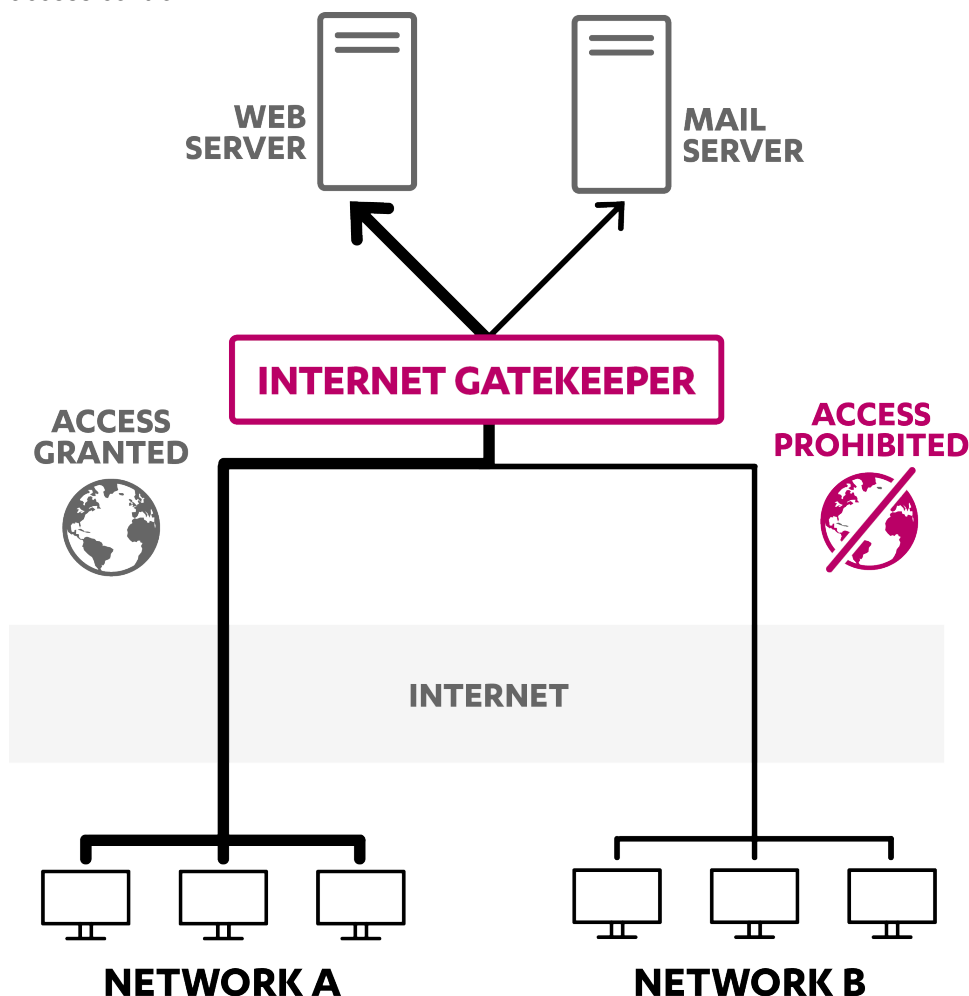


Figure 6: Setting up the access control with IP addresses.

In this case, you can set proxy settings in the configuration file. You can also use the IP filtering (iptables) setting of Linux to set access control.

Proxy access control example

This example limits access to hosts which have the following IP address and subnet: 192.168.1.0/255.255.255.0.

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**.

Edit the following **Access control** settings under **HTTP proxy**, **SMTP proxy**, **POP proxy**, and **FTP proxy** settings:

- **From these hosts (acl_from):** Enabled (Example: 192.168.1.0/255.255.255.0)
- **DNS reverse lookup (reverselookup):** Enable to restrict by host names

IP filtering (iptables) example

You can configure access control which is based on IP addresses by using `iptables`. The following shows you a configuration example:

```
# iptables -A INPUT -s 192.168.1.0/255.255.255.0 -j ACCEPT
# iptables -A INPUT -j DROP
```

8.1.2 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.

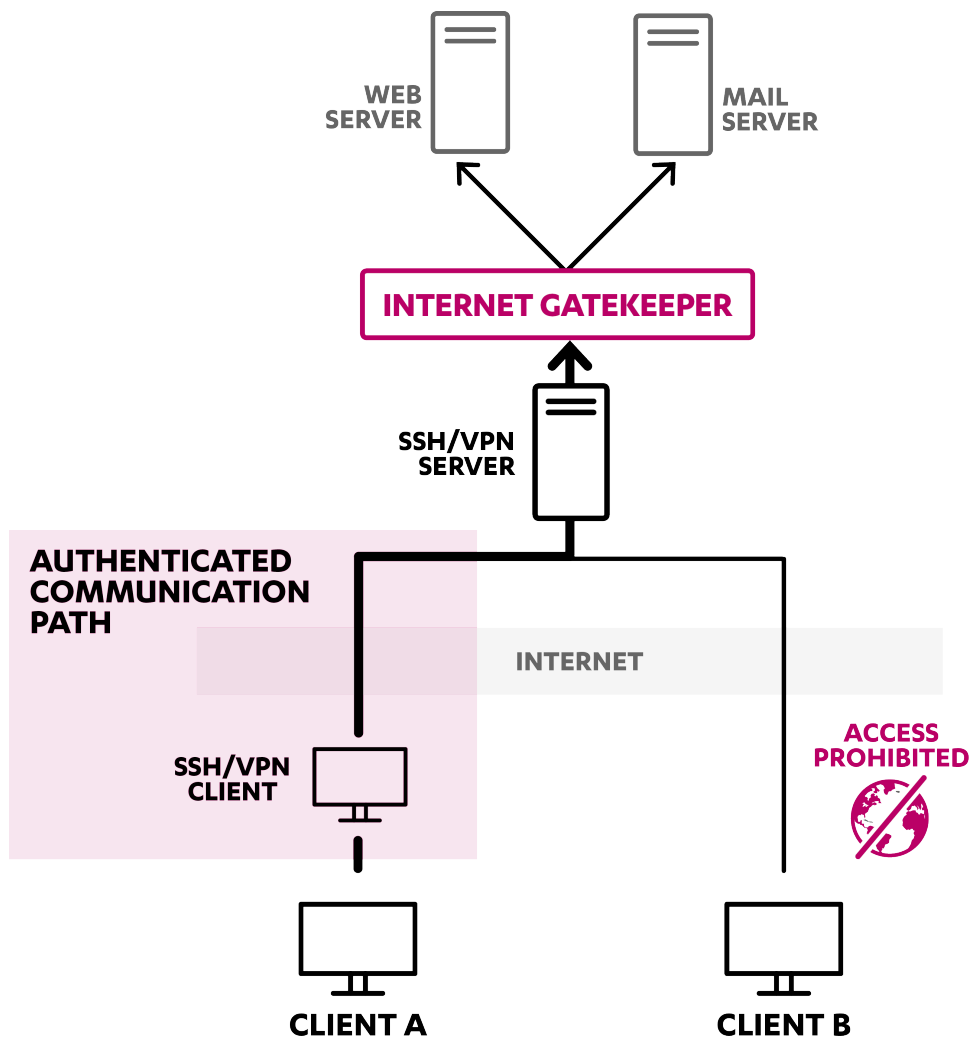


Figure 7: The client connects to Internet Gatekeeper through the authenticated path. In addition, only the authenticated client can connect to the gateway.

This section describes settings, which apply if you use SSH (openssh, TTSSH, etc.).

Settings

1. Install an SSH server to the same server (or a computer on the network) as F-Secure Linux Internet Gatekeeper.



Note: 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 this example, 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/
 - SMTP mail server: localhost
 - POP mail server: localhost
6. Check that viruses are scanned while browsing the web and while sending and receiving emails.

8.1.3 Proxy authentication using Internet Gatekeeper

F-Secure Internet Gatekeeper 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.

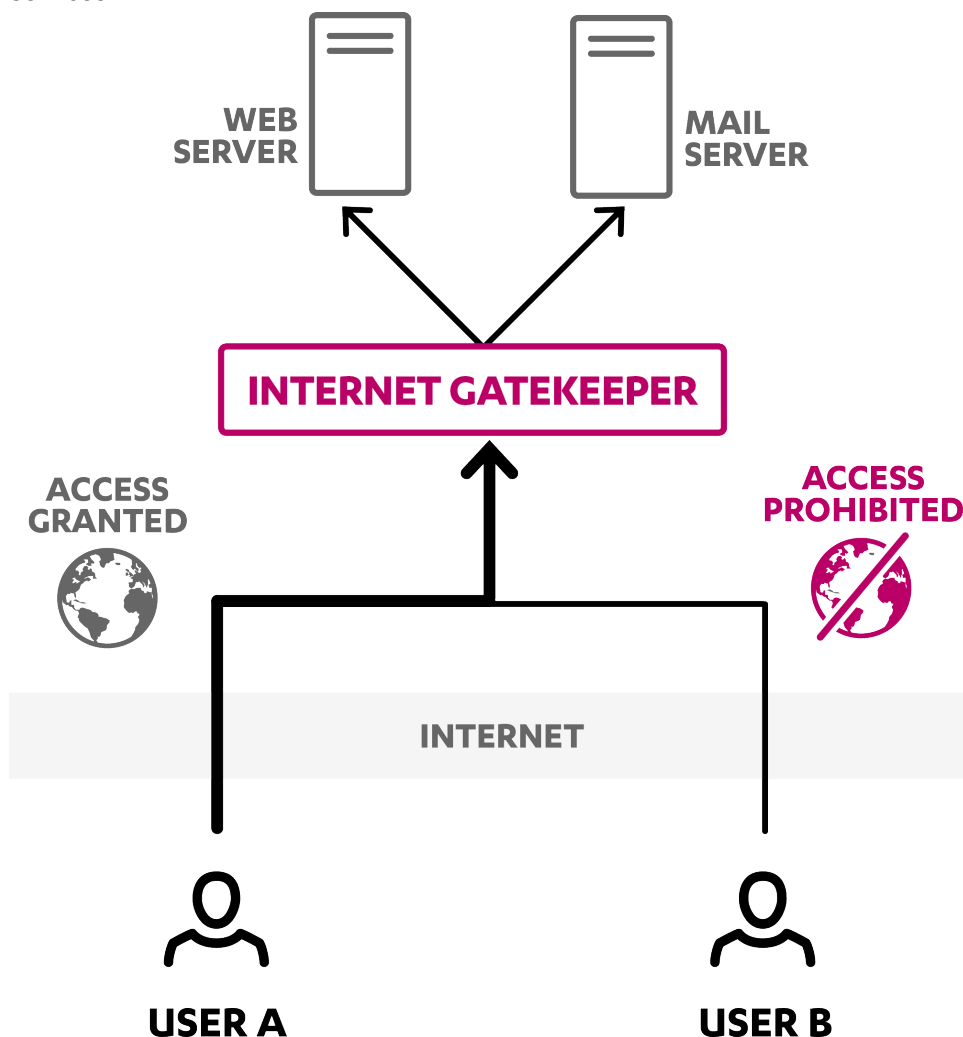


Figure 8: Using the product to authenticate users.

User authentication (PAM Authentication)

You can edit the list of users who are permitted to connect in each proxy setting.

POP, FTP service

For POP and FTP services, F-Secure Internet Gatekeeper checks whether a user name exists in the user database.

If multiple servers are used, specify “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 and the password is authenticated on the server side.

The settings are stored in the `/opt/f-secure/fsigk/conf/pam/userdb.txt` file.

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`. 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.



Note: 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. To prevent the files from being overwritten during updates, remove the symbolic links and create copies before editing the configuration files.

Edit the following proxy settings under **HTTP proxy**, **SMTP proxy**, **POP proxy**, and **FTP proxy**:

- **{HTTP,SMTP,POP,FTP} proxy authentication (proxyauth_pam_auth)=yes**
- **Add or remove users:** Add, delete, or edit users on the **Add or remove users** setting.

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.

Edit **Proxy settings > SMTP proxy > LAN access settings (lan)=yes**

- **Hosts and networks within LAN:** Specify allowed clients (Clients within the LAN, mail servers, etc.)
- Edit `smtp_lan` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of hosts and networks to which the LAN access settings apply

Because emails 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.

Edit **Proxy settings > SMTP proxy**

- **Restrict e-mail recipients (acl_rcpt)=yes** to specify mail server domains
- Edit `smtp_rcpt` field in the `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of domains to which the settings apply.

8.1.4 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.

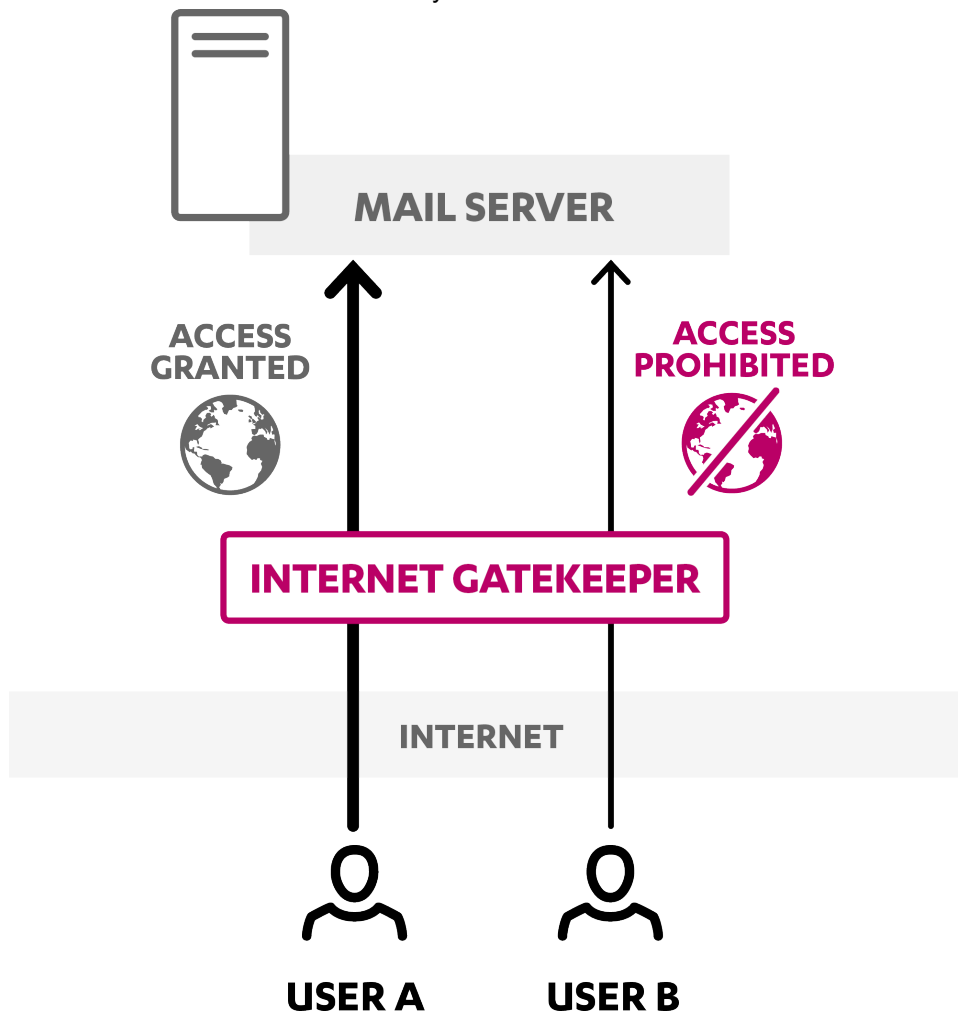


Figure 9: Using the SMTP authentication on the mail server.

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:

1. Open the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini` from command line.
2. Under **SMTP proxy**, set `proxyauth_pam_auth=no` to disable the SMTP authentication.

If you use APOP, disable the parent server setting of the product. To disable the parent server setting for POP proxy:

1. Open the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini` from command line.
2. Under **POP proxy**, set `self_proxy=no` to disable **Defining parent server by user** setting.

👉 **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**.
- Set `self_proxy=no` for POP proxy.
- Use a transparent proxy.

8.1.5 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.

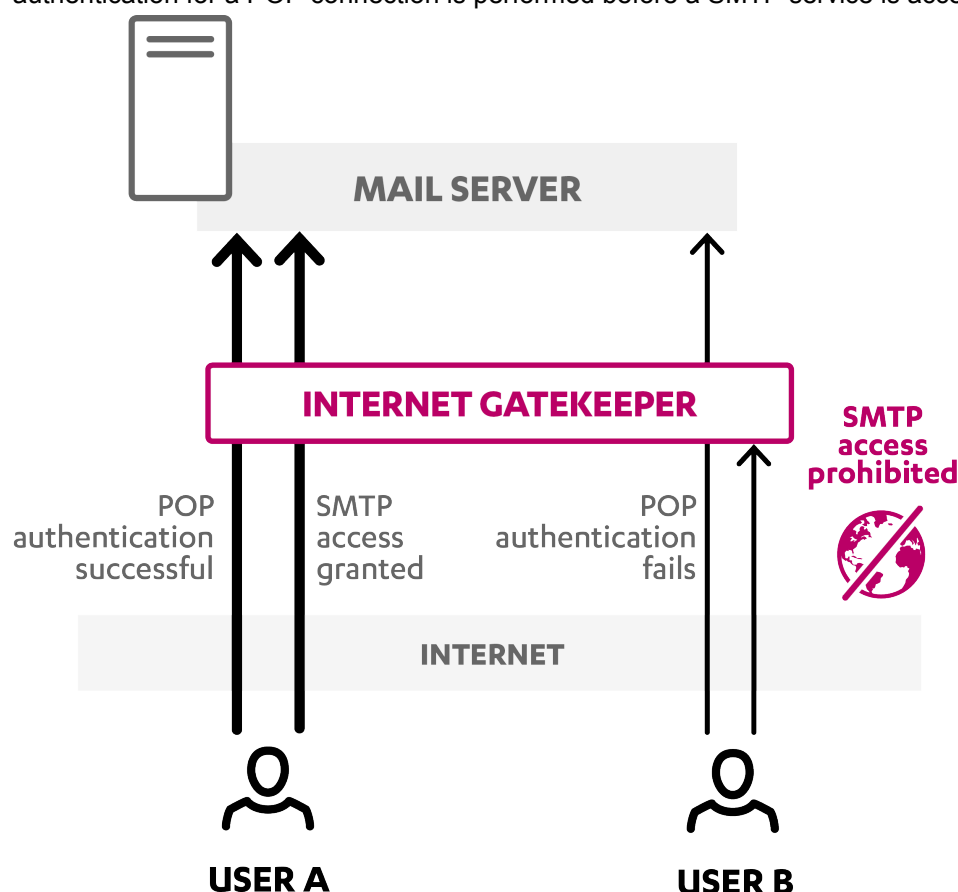


Figure 10: Using the POP-before-SMTP authentication.

Access to the SMTP service is limited to IP addresses that have passed POP authentication within a specified time. In addition, the POP-before-SMTP authentication is performed in F-Secure Internet Gatekeeper. This is because the IP address of the product is always assigned to the IP address of the sender's mail server.

To use the POP-before-SMTP authentication, configure the SMTP and POP services in the following way:

1. Edit **Proxy settings > SMTP proxy (smtp_service)=yes > Global settings**
 - **POP-before-SMTP authentication (pbs)=yes**
 - **Timeout (pbs_lifetime):** Specify the time in minutes during which the authentication is effective (Example: pbs_lifetime=2)
2. Edit **Proxy settings > POP proxy (pop_service)=yes**.
3. The following settings allow services without authentication to clients within the LAN and to senders from specific mail servers, addresses and networks. Edit **Proxy settings > SMTP proxy > LAN access settings (lan)=yes**
 - **Hosts and networks within LAN:** Specify allowed clients (Clients within the LAN, mail servers, etc.)
 - Edit `smtp_lan` field in `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of hosts and networks to which the LAN access settings apply.
4. Because emails from the Internet are delivered to mail servers through the product, the corresponding mail servers must be allowed to deliver without authentication. Edit **Proxy settings > SMTP proxy**
 - **Restrict e-mail recipients (acl_rcpt)=yes** to specify mail server domains.

- Edit `smtp_rcpt` field in `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of domains to which the settings apply.

The database file for the POP-before-SMTP authentication is stored in the following way:

Database format:	BerkeleyDB 1.85
Directory:	Temporary directory (by default, <code>/var/tmp/fsigk</code>)
File name:	<code>pbs.db</code>
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`.

 **Important:** Every time a service is restarted, all the information in the database for POP-before-SMTP is deleted.

8.2 Transparent proxy

F-Secure Internet Gatekeeper 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).

Settings				Proxy mode		Transparent proxy mode	
				Install phase only	Mail server DNS change	Router	Bridge
Client	POP	User name	Specific server	O	O	O	O
			Any server	x	x	O	O
		Server host name	Specific server	x	O	O	O
			Any server	x	x	O	O
	SMTP	Server host name	Specific server	x	O	O	O
			Any server	N/A	N/A	O	O
	HTTP/FTP	Proxy server name		x	x	O	O
Cancel a virus scan			Yes	Yes	N/A	N/A	

Settings		Proxy mode		Transparent proxy mode	
Network	DNS	O	x	O	O
	Routing	O	O	x	O
Proxy	Parent server setting	x	x	O	O
	IP address setting	x	x	x	x
	NAT (iptables) setting	O	O	x	x
	Kernel setting	O	O	O	x

 **Note:** If a subnet exists under the network structure, apply routing settings as needed.

 **Note:** FTP over HTTP is not supported in the transparent proxy mode.

8.2.1 Transparent proxy details

Normally, clients access web servers and mail servers directly. To use F-Secure Internet Gatekeeper 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

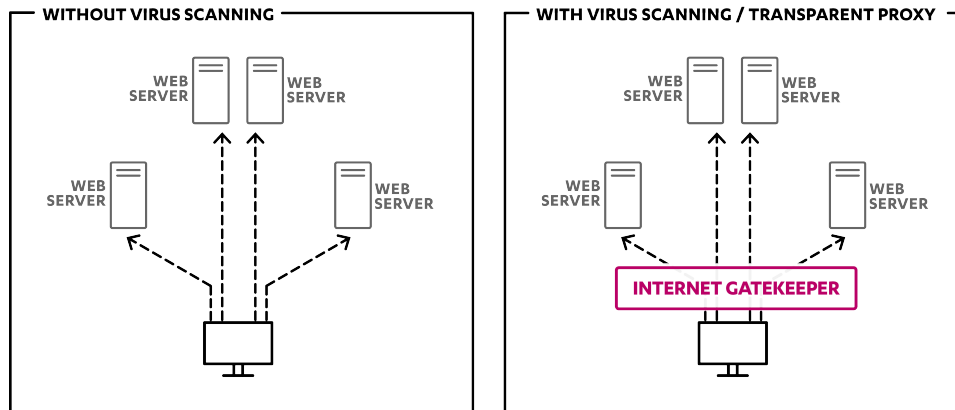


Figure 11: How the client accesses web servers when the product works as a transparent proxy.

8.2.2 Transparent proxy in the router mode

To function as a transparent proxy in the router mode, you must install Internet Gatekeeper on a computer, which acts as a router between the clients and the servers.

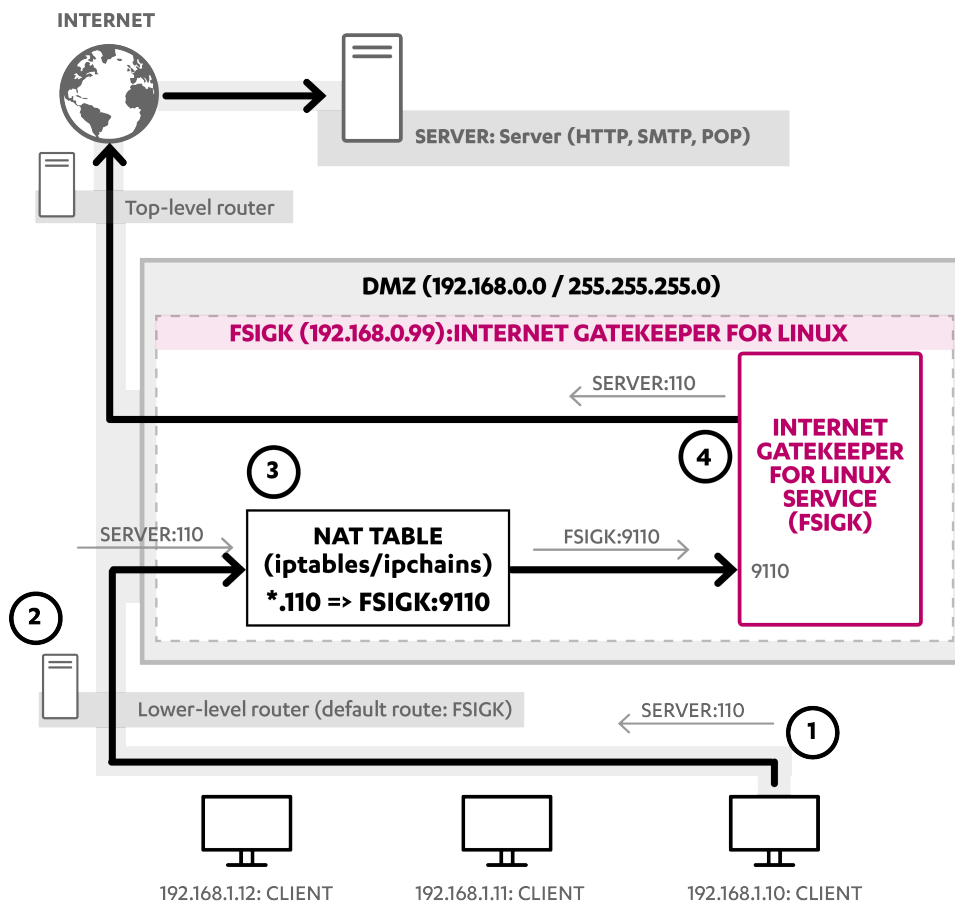


Figure 12: Setting up the product as a transparent proxy in a DMZ network

Overview of operations:

The following describes how clients connect to servers when F-Secure Internet Gatekeeper 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 (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 the router mode, configure the network and server associated with F-Secure Internet Gatekeeper in the following way:

1. Open the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini` and edit the proxy settings to start up each service in transparent proxy mode:

- **HTTP proxy (http_service)=yes**
 - Port Number (svcport)=9080
 - Transparent proxy (transparent)=yes
- **SMTP proxy (smtp_service)=yes**
 - Proxy port (svcport)=9025
 - Transparent proxy (transparent)=yes
- **POP proxy (pop_service)=yes**
 - Port Number (svcport)=9110
 - Transparent proxy (transparent)=yes
- **FTP proxy (ftp_service)=yes**
 - Port Number (svcport)=9021
 - Transparent proxy (transparent)=yes

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.
 - a. 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
```

- b. 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
```

- c. 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
```

4. 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)).

5. 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
```

6. 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.

7. Check that virus scans can be performed when a client accesses a server.



Note:

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.



Note:

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.

8.2.3 Transparent proxy in the bridge mode

F-Secure Internet Gatekeeper 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 the 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. Because the product works as a bridge, both of the interfaces, while on different physical networks, are on the same logical IP network.

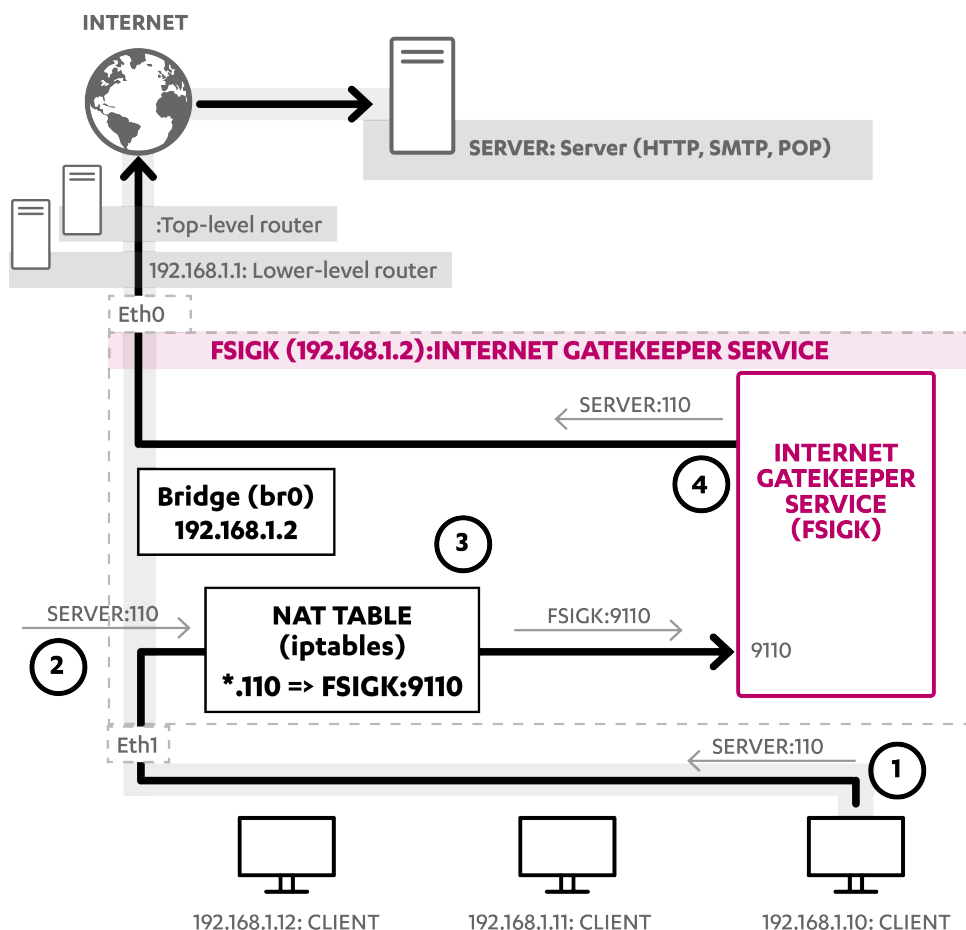


Figure 13: Setting up a transparent proxy in the bridge mode.

Overview of operations:

The following describes how clients connect to servers when F-Secure Internet Gatekeeper 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, 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 in the following way:

1. Open the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini` and edit the proxy settings to start up each service in transparent proxy mode:

- **HTTP proxy (http_service)=yes**
 - Port Number (svcport)=9080
 - Transparent proxy (transparent)=yes
- **SMTP proxy (smtp_service)=yes**
 - Proxy port (svcport)=9025
 - Transparent proxy (transparent)=yes
- **POP proxy (pop_service)=yes**
 - Port Number (svcport)=9110
 - Transparent proxy (transparent)=yes
- **FTP proxy (ftp_service)=yes**
 - Port Number (svcport)=9021
 - Transparent proxy (transparent)=yes

After configuring the settings, check that the client can access the port of each service (9080, 9025, 9110, 9021) on Internet Gatekeeper.

2. 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).

```
# 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.

3. 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.
4. 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
```

5. 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.`

6. Check that virus scans can be performed when a client accesses a server.



Note:

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.



Note:

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.linuxfoundation.org/collaborate/workgroups/networking/bridge>

8.3 Coexisting with mail servers

F-Secure Internet Gatekeeper 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.

8.3.1 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.

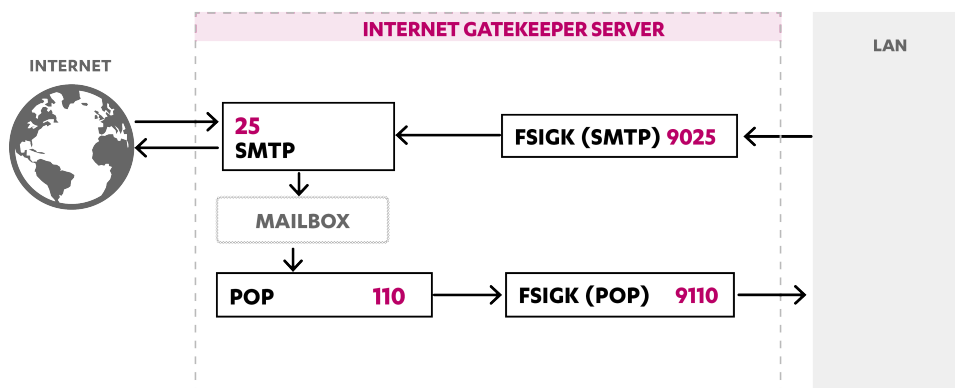


Figure 14: Using ports 9025 and 9110 for Internet Gatekeeper.

The following example uses ports 9025 and 9110 for Internet Gatekeeper.

1. In F-Secure Internet Gatekeeper, set the port numbers used by the product to 9025 and 9110 in the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`:

- **Proxy settings > SMTP proxy**
 - **Proxy port (svcport)=9025**
 - **Parent server:** (parent_server_host=localhost , parent_server_port=25)
- **Proxy settings > POP proxy**

- **Proxy port (svcport)=9110**
- **Parent server:** (parent_server_host=localhost , parent_server_port=25)

2. In the client, set the port numbers used by the SMTP and POP servers to 9025 and 9110.

8.3.2 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.

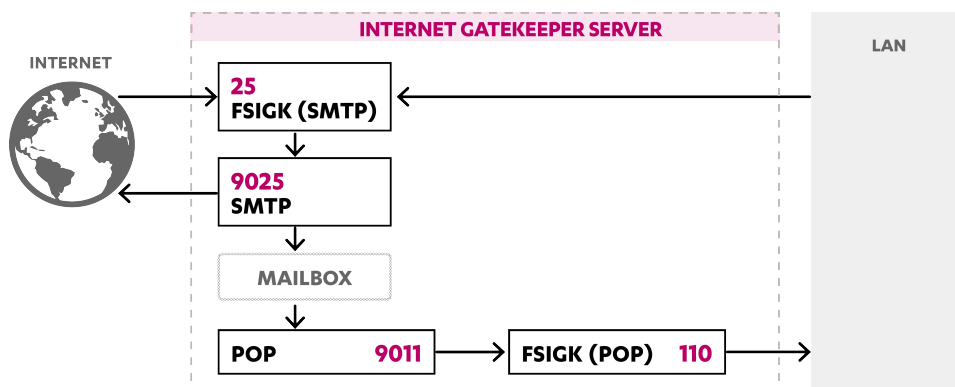


Figure 15: Using ports 9025 and 9110 for the mail server.

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.

1. On the mail server, 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`.

```
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**:

1. 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. 1 Set the smtpd service port in `/etc/postfix/master.cf` as follows:

```
9025 inet n - n - - smtpd
```

2. Restart postfix.

```
# postfix reload
```

2. In F-Secure Internet Gatekeeper, set the port numbers of the parent server to 9025 and 9110 in the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`:

- **Proxy settings > SMTP proxy (smtp_service)=yes**
 - **Proxy port (svcport)=25**
 - **Global settings > Parent server**
 - **Host name (parent_server_host)=localhost**
 - **Port number (parent_server_port)=9025**
- **Proxy settings > POP proxy (pop_service)=yes**
 - **Proxy port (svcport)=110**
 - **Parent server:**
 - **Host name (parent_server_host)=localhost**
 - **Port number (parent_server_port)=9110**

Restricting the recipient domains to prevent third-party relays

To restrict mail to your_domain1.com and your_domain2.com, edit **Proxy settings > SMTP proxy > Global settings > Restrict e-mail recipients (acl_rcpt)=yes**.

Edit `smtp_rcpt` field in `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of domains to which the settings apply.

Allow access from clients within the LAN

As outbound access is denied by restricting recipient domains, allow access from clients within the LAN. To enable IP addresses specified in 192.168.1.xxx and 192.168.2.xxx, edit **Proxy settings > SMTP proxy > LAN access settings (lan)=yes**.

- **Hosts and networks within LAN:** 192.168.1.0/255.255.255.0
192.168.2.0/255.255.255.0
- Edit `smtp_lan` field in `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of hosts and networks to which the LAN access settings apply.

Using POP-before-SMTP to enable data to be sent outside

Edit **Proxy settings > SMTP proxy (smtp_service)=yes > Global settings.**

- **POP-before-SMTP authentication (pbs)=yes**
- **POP proxy (pop_service)=yes**

If the mail server performs SMTP authentication, you do not have to change any settings.

8.3.3 Changing the IP address

If F-Secure Internet Gatekeeper 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.

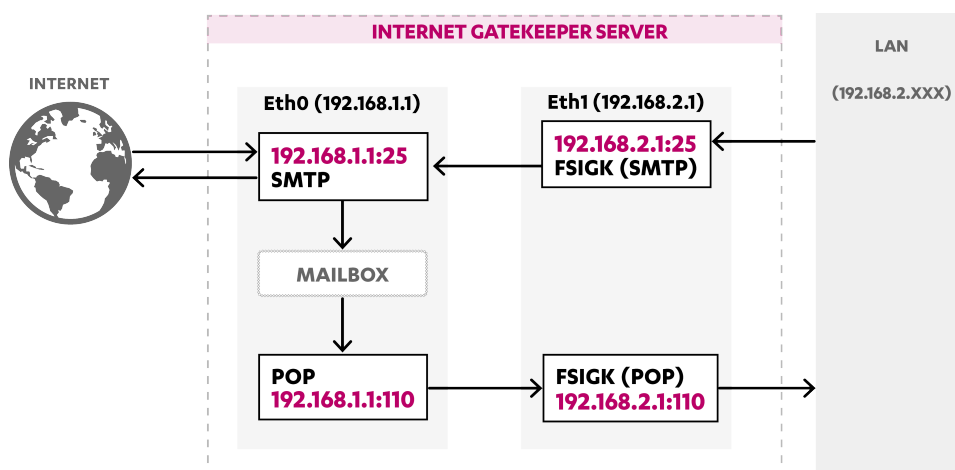


Figure 16: The mail server listens to eth0 (192.168.1.1) and Internet Gatekeeper listens to eth1 (192.168.2.1)

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.

1. On the mail server, 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`.

```
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**:

1. Make the following change 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. 1 Set the smtpd service port in `/etc/postfix/master.cf` as follows:

```
192.168.1.1:25 inet n - n - - smtpd
```

2. Restart postfix.

```
# postfix reload
```

2. In F-Secure Internet Gatekeeper, 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) in the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`:

- **Proxy settings > SMTP proxy (smtp_service)=yes**

- **Proxy port (svcport)=192.168.2.1:25**
- **Global settings > Parent server**
 - **Host name (parent_server_host)=192.168.1.1**
 - **Port number (parent_server_port)=25**

- **Proxy settings > POP proxy (pop_service)=yes**

- **Proxy port (svcport)=192.168.2.1:110**
- **Parent server:**
 - **Host name (parent_server_host)=192.168.1.1**
 - **Port number (parent_server_port)=110**

3. Set the mail server to 192.168.2.1.

Make sure that the client can send and receive mails.

Changing IP addresses with iptables

If F-Secure Internet Gatekeeper 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.

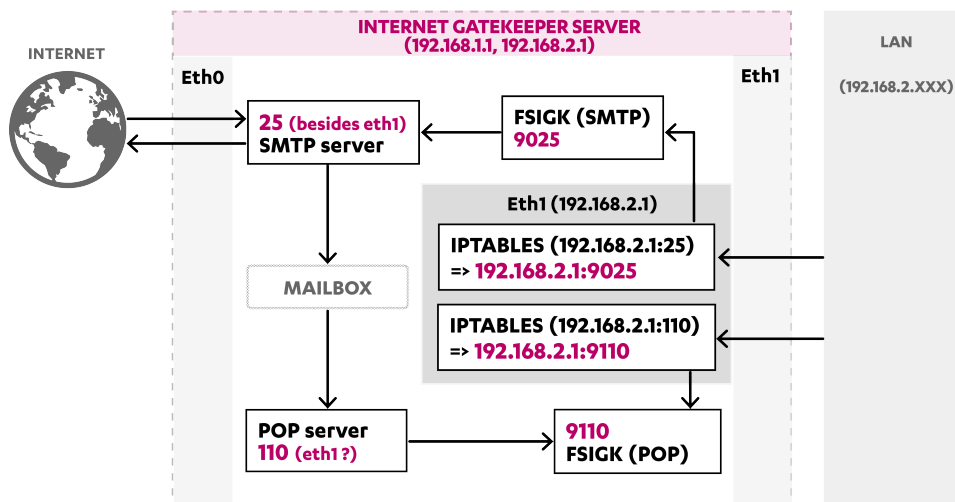


Figure 17: Redirecting the access to default ports.

You can redirect the access to default ports (25, 100) in specific interfaces to the product (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

To redirect the access to ports 25 and 110 of eth1 (192.168.2.1) to 9025 and 9110, use the following 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

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) in the configuration file /opt/f-secure/fsigkconf/fsigk.ini.

- **Proxy settings > SMTP proxy (smtp_service)=yes**
 - **Proxy port (svcport)=9025**
 - **Global settings > Parent server**
 - **Host name (parent_server_host)=localhost**
 - **Port number (parent_server_port)=25**

- **Proxy settings > POP proxy (pop_service)=yes**
 - **Proxy port (svcport)=9110**
 - **Parent server:**
 - **Host name (parent_server_host)=localhost**
 - **Port number (parent_server_port)=110**

Client settings

Set the mail server to 192.168.2.1 and make sure that the client can send and receive mails.

8.4 Scanning viruses before saving mail to the mail server

By default, virus scans are performed on all inbound emails 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 emails in SMTP before they are saved to the mail server.

The following example uses a single F-Secure Internet Gatekeeper server to check both outbound and inbound emails for viruses.

Overview of operations:

Without virus scanning

If F-Secure Internet Gatekeeper is not implemented, outbound emails are transferred through an internal mail server to the destination mail server. Inbound emails 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 is implemented, the product scans outbound emails for viruses. After that the emails are delivered to the destination mail server by using the internal mail server. After the product has scanned inbound emails for viruses, the emails are stored on an internal mail server. Users can retrieve them by using the POP protocol. In addition, restrictions are applied to outbound emails to prevent open relays (third-party relays) and email abuse.

Setting example

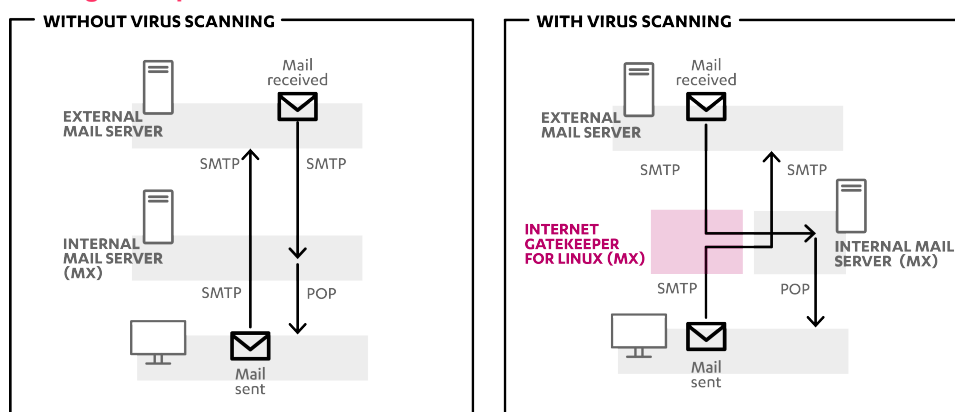


Figure 18: Scanning inbound mails for viruses before saving mail to the server.

Settings

1. Set up F-Secure Internet Gatekeeper under a temporary host name (virus-gw) and apply the following proxy settings in the configuration file:
 - **Proxy settings > SMTP proxy (smtp_service)=yes**
 - **Proxy port (svcport)=25**
 - **Global settings > Parent server**
 - **Host name (parent_server_host)=<IP address of internal mail server>**

- **Port number (parent_server_port)=25**
- **Global settings > Restrict e-mail recipients (acl_rcpt)=yes**
 - Edit `smtp_rcpt` field in `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of domains to which the LAN access settings apply.
- **LAN access settings (lan)=yes**
 - **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)
 - Edit `smtp_lan` field in `/opt/f-secure/fsigk/conf/fsigk.ini` file to specify the list of hosts and networks to which the LAN access settings apply.

2. Configure the internal mail server so that emails 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>
```

(For example: 192.168.1.0/24.)

2. Restart `postfix`.

```
# postfix reload
```

3. Check that emails can be sent from the internal network to an external mail server by using virus-gw. Check also that outbound emails 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 emails can be sent from the internal network to an external mail server by using mx. Check also that outbound emails are limited to the specified domain.
6. After the DNS cache has expired, check that emails can be sent internally through external mail servers. In addition, check that inbound and outbound emails are scanned for viruses.

8.5 Reverse proxy settings

F-Secure Internet Gatekeeper 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.

8.5.1 Typical reverse proxy 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.



Figure 19: Setting up a reverse proxy.

Internet Gatekeeper settings

In the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`, configure the proxy port and parent server port to 80:

- **Proxy settings > HTTP proxy (http_service)=yes**
 - **Proxy port (svcport)=80**
 - **Parent server:**
 - **Host name (parent_server_host)=Web server**
 - **Port number (parentServer_port)=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:

- **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.
- **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.

8.5.2 Coexisting with web servers

F-Secure Internet Gatekeeper 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.

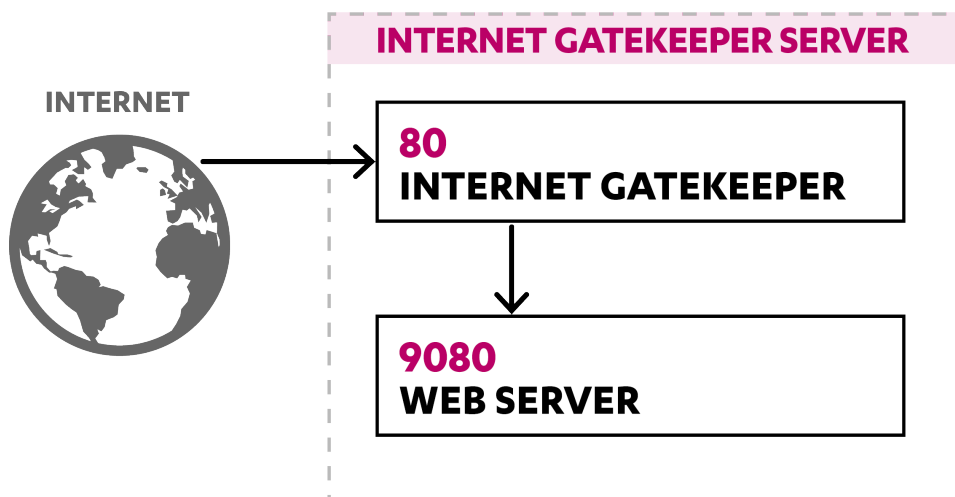


Figure 20: Using port 9080 for the web server.

Web server settings

Using Apache, change the HTTP server port to 9080.

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

In the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`, configure the proxy port and parent server port to 80.

- **Proxy settings > HTTP proxy (http_service)=yes**
 - **Proxy port (svcport)=80**
 - **Parent server:**
 - **Host name (parent_server_host)=localhost**
 - **Port number (parentServer_port)=9080**

8.5.3 Implementing a HTTPS (SSL) server

F-Secure Internet Gatekeeper 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.

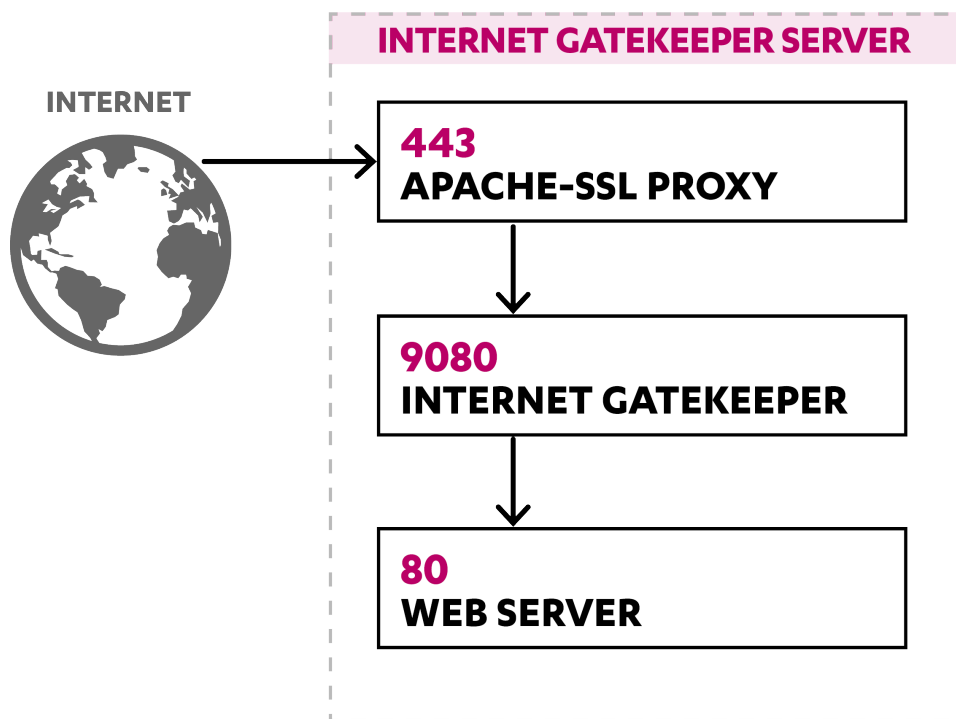


Figure 21: The Apache configuration file when the product is used with a SSL proxy and a web server.

Apache-SSL settings

In the following example, port 443 is used first to listen to data. Afterwards, port 9080 is relayed to decrypt data.

```
# 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

In the configuration file `/opt/f-secure/fsigk/conf/fsigk.ini`, configure the proxy port to 9080 and the parent server port to 80.

- **Proxy settings > HTTP proxy (http_service)=yes**
 - **Proxy port (svcport)=9080**
 - **Parent server:**
 - **Host name (parent_server_host)=localhost**
 - **Port number (parentServer_port)=9080**

Web server settings

The web server uses port 80.

Product specifications

Topics:

This section describes the specifications for F-Secure Internet Gatekeeper.

- [*Specification summary*](#)
- [*HTTP proxy process*](#)
- [*SMTP proxy process*](#)
- [*POP proxy process*](#)
- [*FTP proxy process*](#)
- [*HTTP error responses*](#)
- [*HTTP request and response headers*](#)
- [*SMTP command responses*](#)
- [*SMTP commands - operations*](#)
- [*POP commands - operations*](#)
- [*FTP commands - operations*](#)
- [*Connection error messages*](#)
- [*Service process list*](#)
- [*Detection names*](#)
- [*Riskware*](#)

9.1 Specification summary

Installer	rpm, tar.gz
Supported network protocols	IPv4(RFC791) / TCP(RFC793)
Supported application protocols	HTTP, FTP, SMTP, POP, ICAP
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/VRIFY/ 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

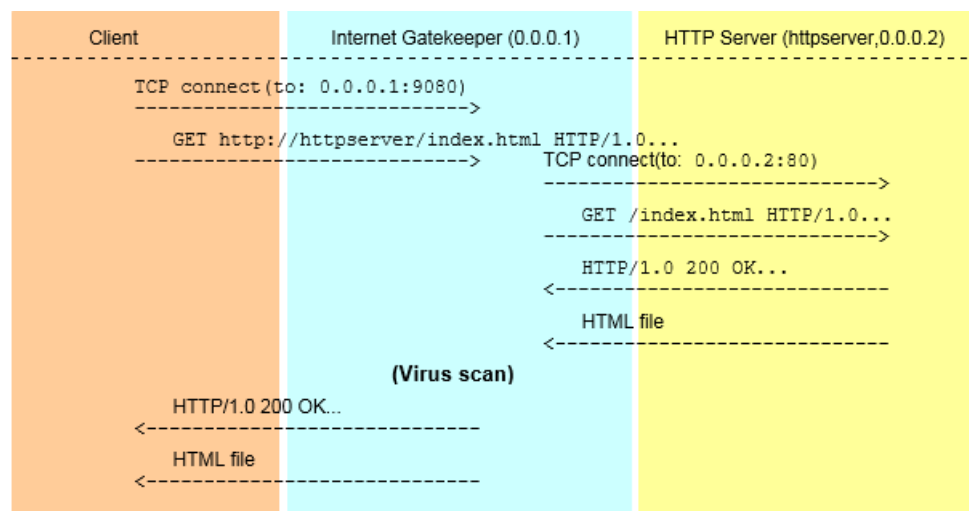
POP commands that can be scanned	RETR/STOR
POP commands that can be used	USER/PASS/APOP/UIDL/TOP/STAT/LIST/RETR/DELE/NOOP/RSET/QUIT/AUTH, and other similar response commands * APOP cannot be used if “Defining parent server by user” is enabled and the product is running as a proxy
Supported POP protocol 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)

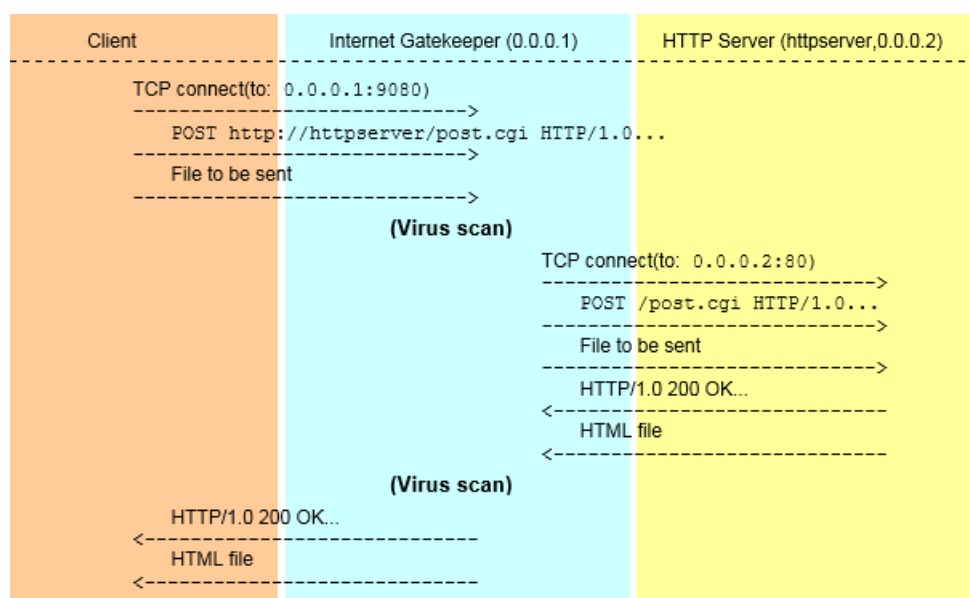
9.2 HTTP proxy process

This section describes how common protocols are processed with the HTTP proxy.

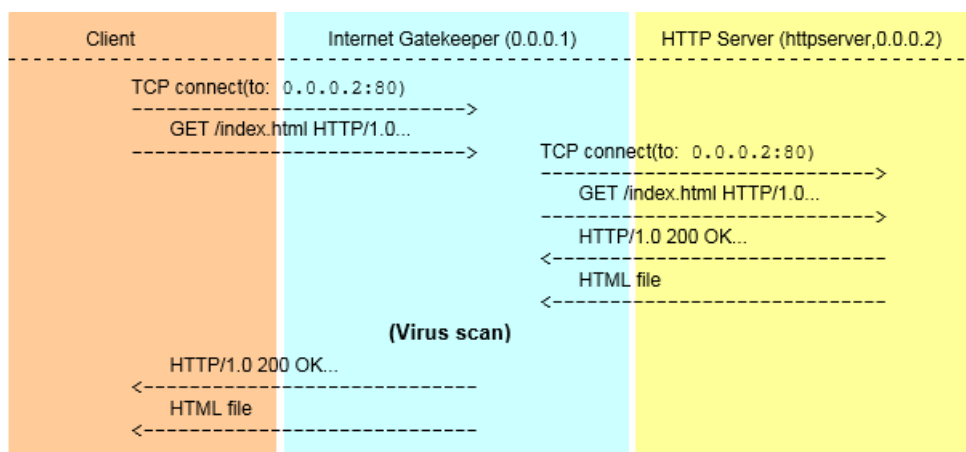
Proxy mode, GET method



Proxy mode, POST method (scans files when they are sent)



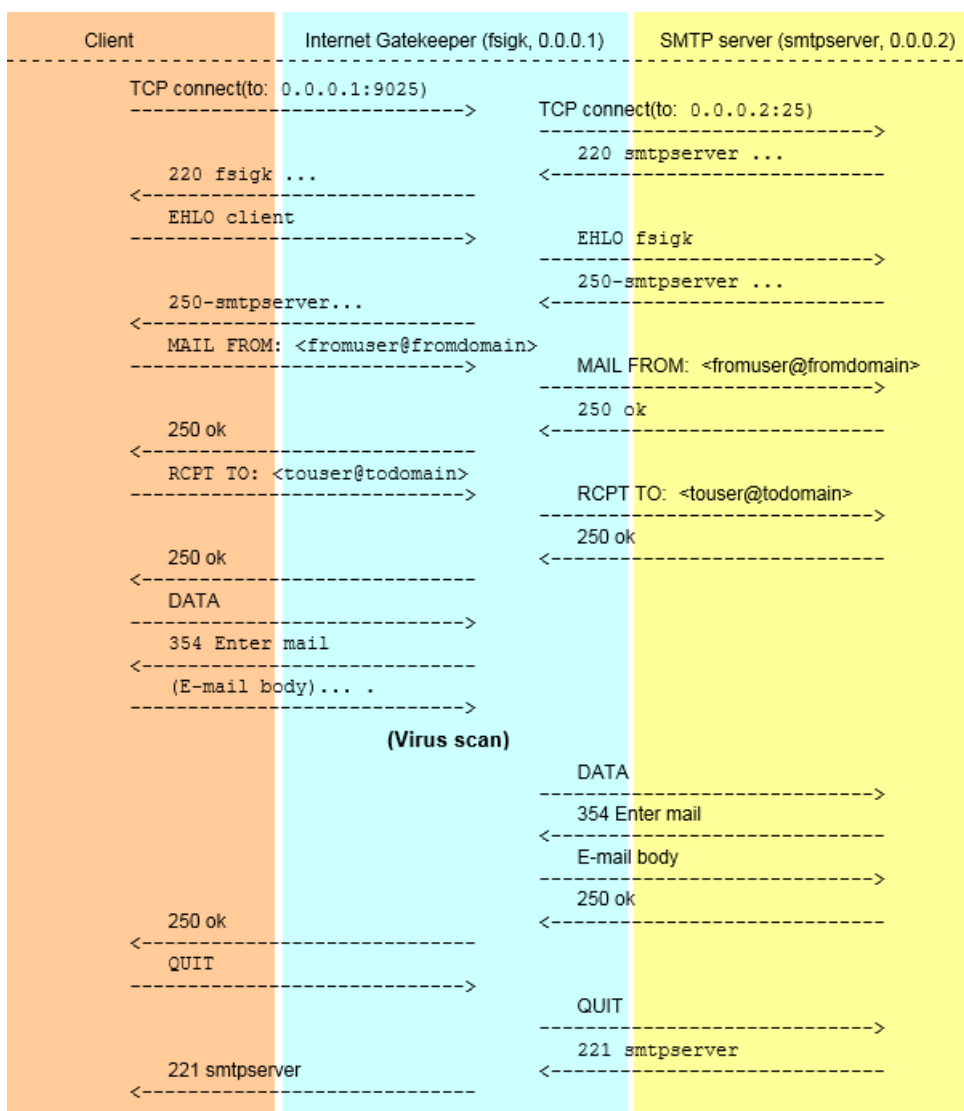
Transparent proxy mode (router or bridge), GET method



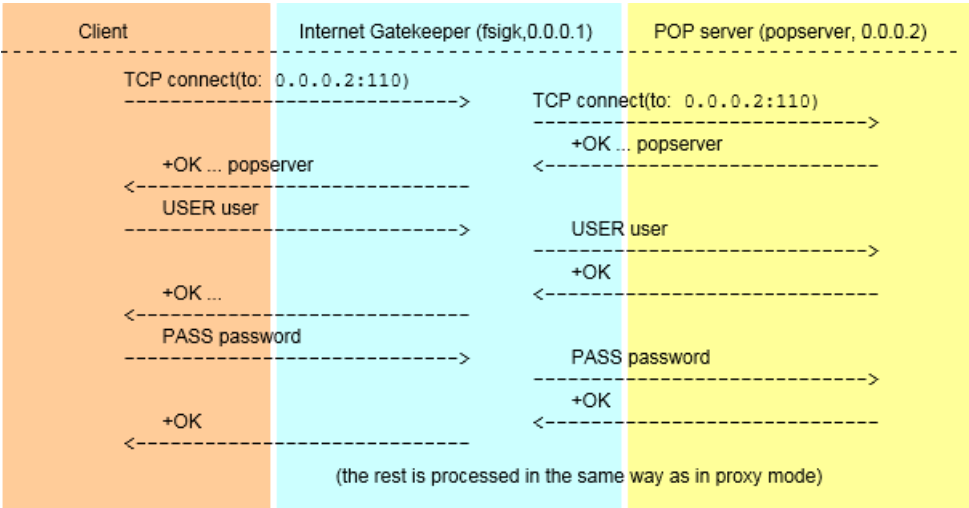
9.3 SMTP proxy process

This section describes how common protocols are processed with the SMTP proxy.

Proxy mode



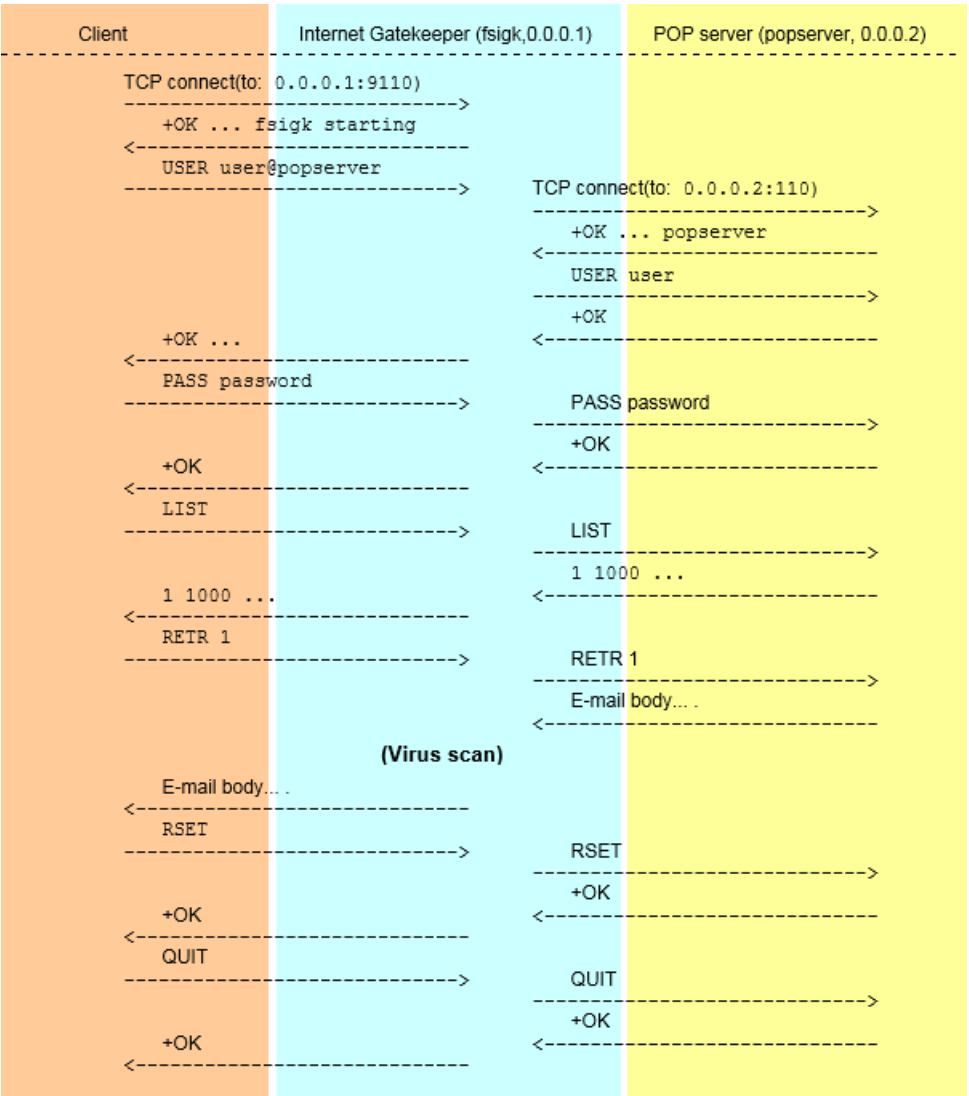
Transparent proxy mode (router or bridge)



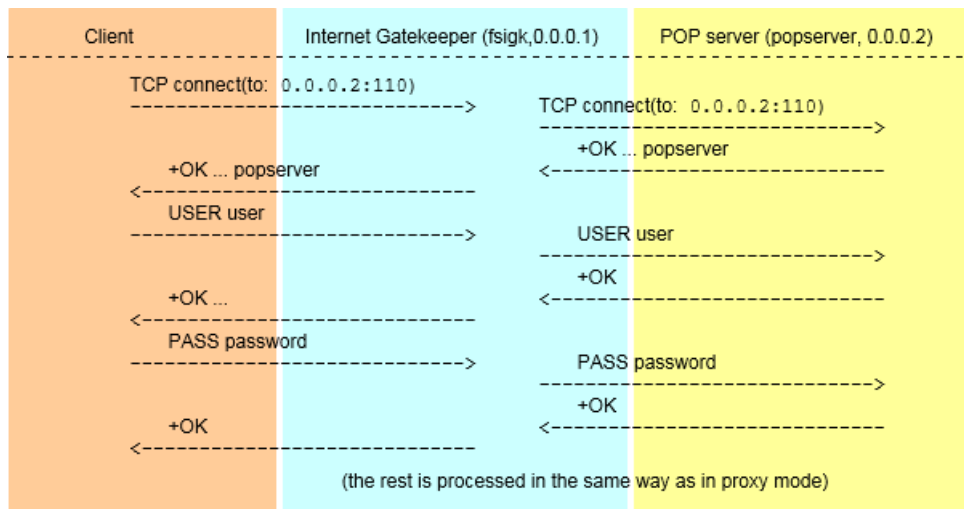
9.4 POP proxy process

This section describes how common protocols are processed with the POP proxy.

Proxy mode



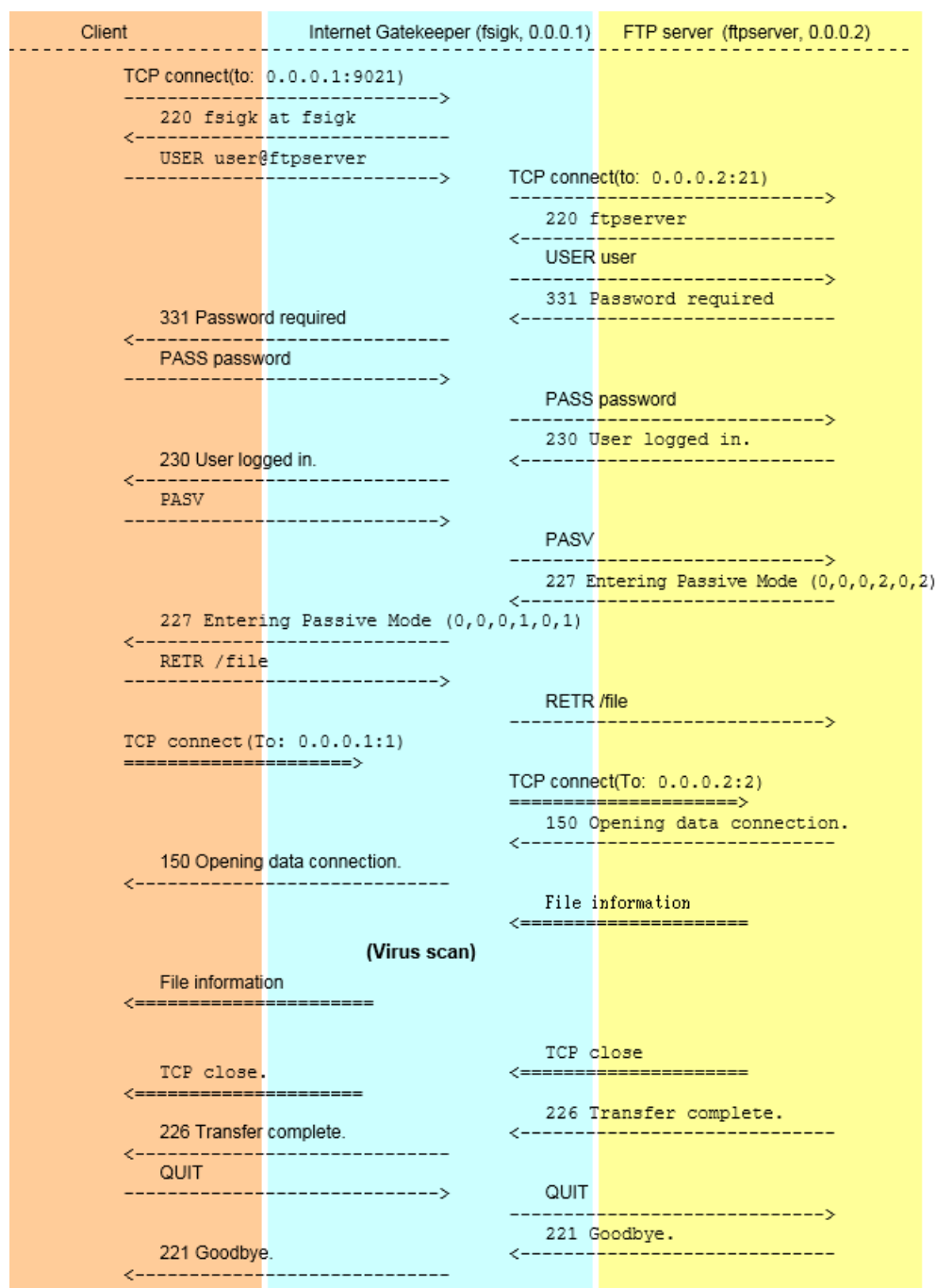
Transparent mode (router or bridge)



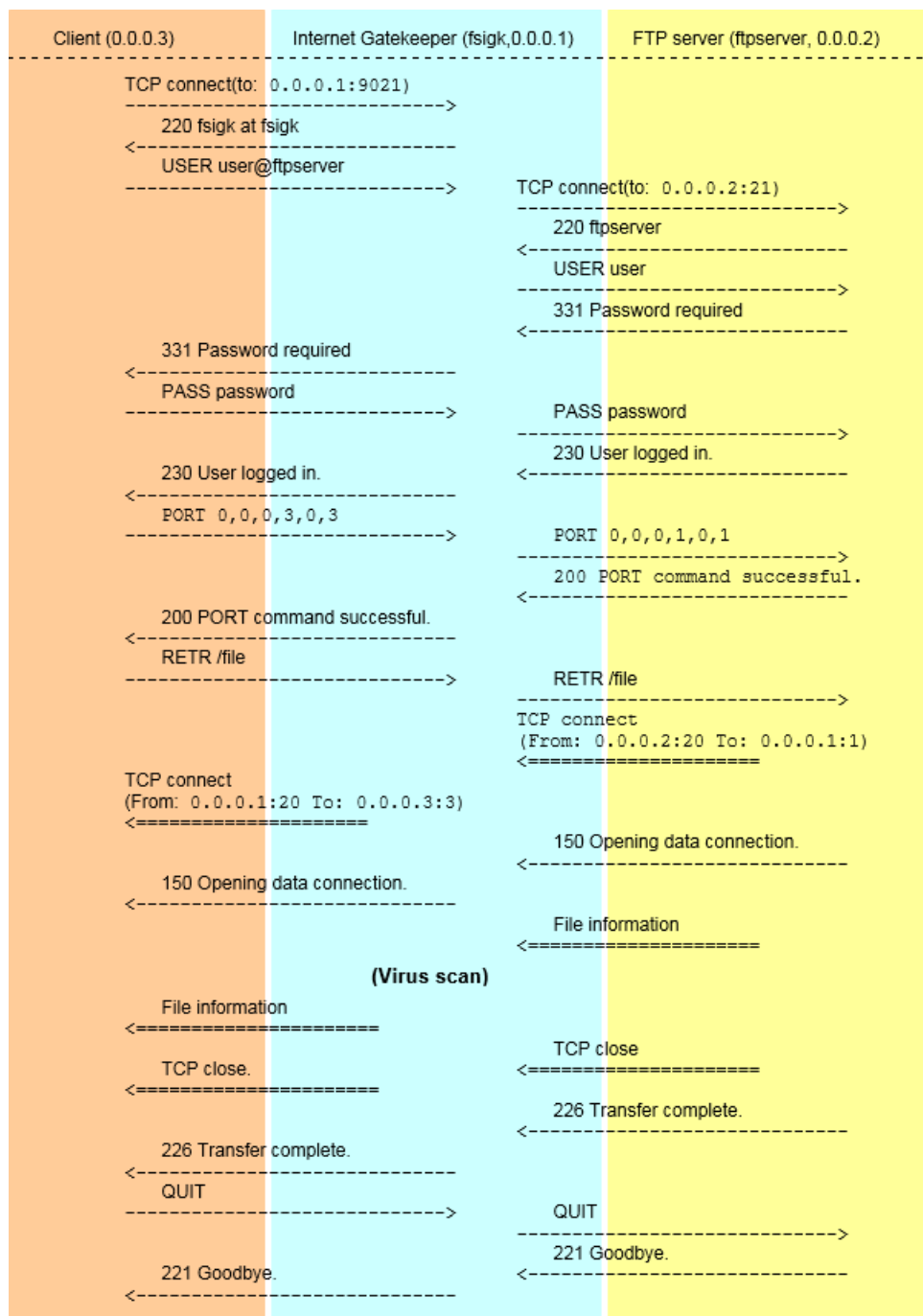
9.5 FTP proxy process

The FTP service relays both the control session and data session. This section describes how common protocols are processed with the FTP proxy.

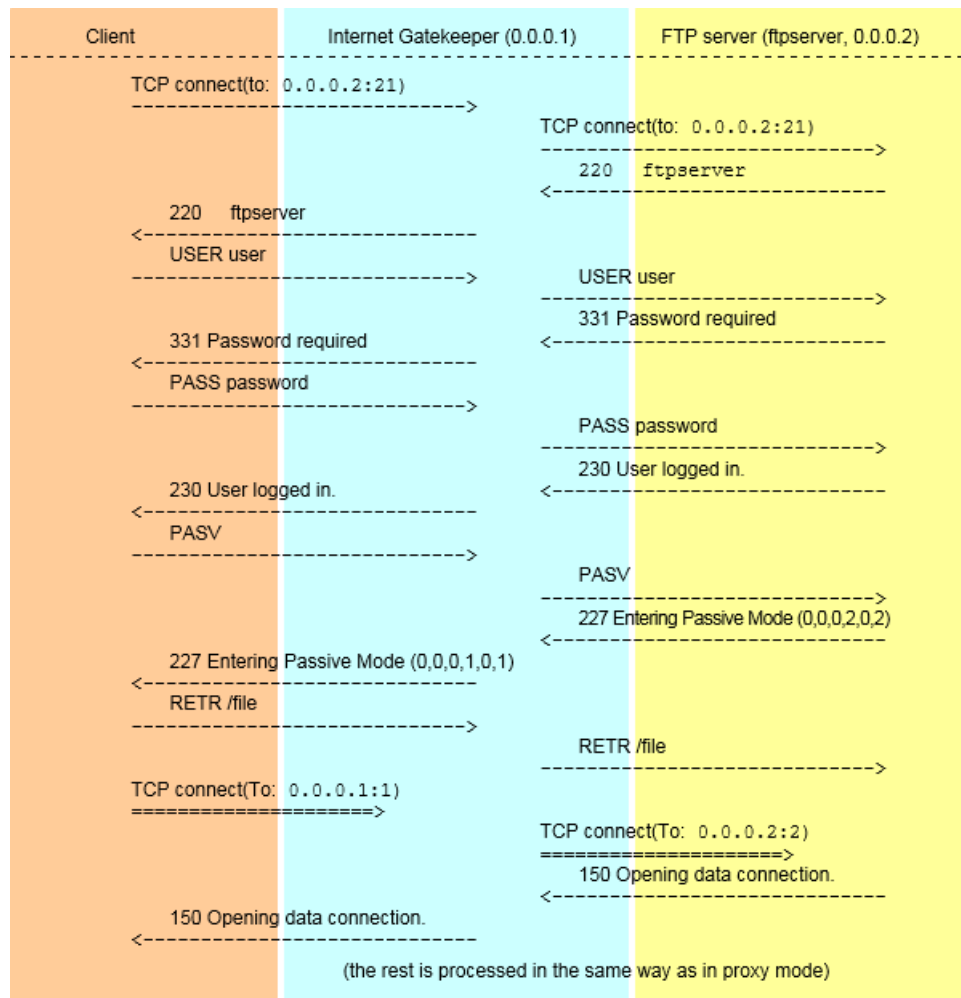
Proxy mode, passive FTP



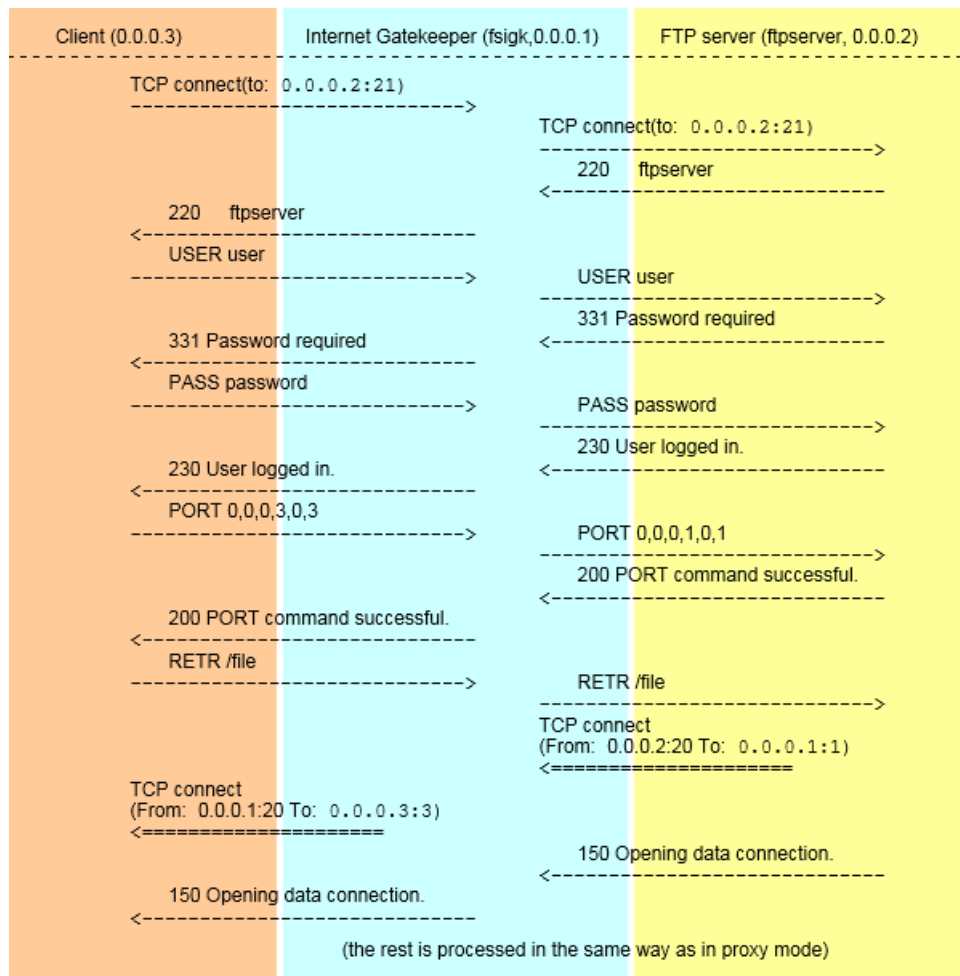
Proxy mode, active FTP



Transparent mode (router or bridge), passive FTP



Transparent mode (router or bridge), active FTP



9.6 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.

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"

9.7 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. For 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.)

9.8 SMTP command responses

Usually, server responses are relayed to clients during SMTP connections. However, sometimes they can be generated by F-Secure Internet Gatekeeper. 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))

Message	Reason
DATA command response	
354 Enter mail	Starts to receive email data that is being transferred.
250 Message accepted for delivery	Indicates that the email data has been received.
554 SENDBACK:smtp error[COMMAND] (Server Reply: XXX)	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.
554 Too long message	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.
554 Infected by [Detection name]	This message appears when a virus is detected and if "Deny" is selected as the action when viruses are detected.

Connection responses

421 server open error (Host port) errmsg=[XXX]	Access to the specified host and port failed. ERRMSG displays the contents of the connection error message.
421 Cannot get correct greeting message from mail server (Host port). return code=DDD	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

500 Too long line	The length of the command line exceeds 9999 bytes.
-------------------	--

Responses from commands other than HELO, EHLO, AUTH, QUIT, RSET

Message	Reason
500 Authentication Required	The authentication for sending emails is not complete. Is displayed in the following cases: • 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

421 (COMMAND) disconnected from (Host: Port)	The server was disconnected when COMMAND was executed. The COMMAND can be either HELO or EHLO.
--	--

MAIL command responses

501 Syntax error ("MAIL FROM:").	The MAIL command is invalid (FROM is missing).
----------------------------------	--

RCPT command responses

500 RCPT command must begin with "RCPT TO:."	The RCPT command is invalid (TO is missing).
250 Recipient ok	The relay was denied. Is displayed when recipient domains are restricted and authentication is not completed.

AUTH command responses

504 this mechanism not available	Authentication methods other than PLAIN and LOGIN are not supported.
235 ok authed	Authentication is successful. Is displayed only when SMTP authentication is performed by F-Secure Internet Gatekeeper. If authentication is done on the SMTP server side, the SMTP server response is relayed.
535 authorization failed	Authentication failed. Is displayed only when SMTP authentication is performed by F-Secure Internet Gatekeeper. If authentication is done on the SMTP server side, the SMTP server response is relayed.
500 disconnected from server(AUTH).	The server disconnected during authentication.

Unknown commands

Message	Reason
500 Unknown Command: "COMMAND"	The specified command (COMMAND) is not supported.

9.9 SMTP commands - operations

During SMTP connections, commands executed from clients are operated in the following way.

 **Note:** 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:
 - a. The following is sent to the client: `421 server open error ([Server host]:[Server port]) errormsg=[connection error message]`
 - b. 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:
 - a. The following is sent to the client: `500 Too long line ([Product name])`
 - b. 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

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:

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:

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))

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. The session ends if the response code is other than 250.

AUTH command

1. If SMTP authentication is enabled:

- If authentication passes, the following is sent to the client: 235 ok authenticated ([Product name])
- If authentication fails, the following is sent to the client: 535 authorization failed ([Product name])
- If the authentication method is other than PLAIN or LOGIN, the following is sent to the client: 504 this mechanism not available ([Product name])

2. If SMTP authentication is disabled, 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:
 - a. Virus logs are recorded.
 - b. A notification is sent to the administrator (if notification sending is enabled).
5. If the email size is greater than the maximum message size, 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":
 - a. If "Deny" is set as the action:
 - a. The following is sent to the server: RSET
 - b. Receives a response from the server.
 - c. If the response code is other than 250, the session ends.
 - d. The following is sent to the client: 554 Infected by [Detection name] ([Product name])

- b. If “Notify the sender” is set as the action:
 - a. The following is sent to the server: RSET
 - b. If the response code is other than 250, the following is sent to the client: 554 :SENDBACK:smtp error[RSET]: (Server Reply: [Server response information]) ([Product name])
 - c. The following is sent to the server: MAIL FROM: [Template sender or administrator address]
 - d. If the response code is other than 250, the following is sent to the client: 554 SENDBACK:smtp error[MAIL FROM] (Server Reply: [Server response information]) ([Product name])
 - e. The following is sent to the server: RCPT TO: <Sender address>
 - f. If the response code other than 250, the following is sent to the client: 554 SENDBACK:smtp error[RCPT TO] (Server Reply: [Server response information]) ([Product name])
 - c. If the action on detection is set to “Notify the sender” or “Notify the recipient”:
 - a. The following is sent to the server: DATA
 - b. The command terminates, if the response code other than 354
 - c. The following is sent to the server: Received: from [Client host name] ([Client IP address]) by [Host name] ([Product name]); [Current time (RFC822 format)]
 - d. If spam is detected, the following is sent to the server: X-Spam-Status: Yes(Product name) with [Detection name]
 - e. If a virus is detected, the following is sent to the server: X-Virus-Status: infected(Product name) with [Detection name]
 - f. The following is sent to the server: Data: [Date field information of the e-mail received]
 - g. If “Notify the sender” is set as the action, the following is sent to the server: To: [Sender address of the e-mail received]
 - h. 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]
 - i. If the From field is not included in the infected email notification template, the following is sent to the server: From: [Administrator’s e-mail address]
 - j. The following is sent to the server: Content-Transfer-Encoding: 7bit
 - k. The information of the detection notification message is sent.
 - l. The following is sent to the server: "\r\n.\r\n"
 - m. The following is sent to the client: Server response information
 - n. The session ends if the response code is other than 250
 - d. If “Delete” is set as the action:
 - a. The following is sent to the server: RSET
 - b. The session ends if the response code is other than 250:
 - c. The following is sent to the client: 250 Message accepted for delivery ([Product name])
7. If the previous step does not apply:
- a. The following is sent to the server: DATA
 - b. If the response code is other than 354:
 - a. The following is sent to the client: [Server response information]
 - b. The command terminates.

c. If anonymous proxy mode is not enabled:

- a. The following is sent to the server: `Received: from [Client host name] ([Client IP address]) by [Host name] ([Product name]); [Current time (RFC822 format)]`
- b. If spam is detected, the following is sent to the server: `X-Spam-Status: Yes([Product name]) with [Detection name]`
- c. If a virus is cleaned, the following is sent to the server: `X-Virus-Status: disinfected([Product name]) from [Detection name]`
- d. If infected by a virus, the following is sent to the server: `X-Virus-Status: infected([Product name]) with [Detection name]`
- e. If viruses are not detected, the following is sent to the server: `X-Virus-Status: clean([Product name])`

d. The following is sent to the server: E-mail information

e. 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])`

9.10 POP commands - operations

During POP connections, commands executed from clients are operated in the following way.



Note: 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:

- a. The server is accessed.
- b. If access fails:
 - a. The following is sent to the client: `-ERR Can't Connect to (Server host: Server port) errmsg=[Connection error message]`
 - b. The session ends.
- c. Receives a response from the server.
- d. The following is sent to the client: `[Server response information]`

2. If step 2 above does not apply, the following is sent to the client: `+OK [Product name] starting.`

Command lines

1. If a line is greater than 998 bytes, 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, the following is sent to the client: `-ERR please use USER command at first.`
3. If steps 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, the following is sent to the server: Client response information
2. If the previous step does not apply:
 - a. If user authentication is enabled, but the user is not added, the following is sent to the client: `-ERR Invalid Account Auth.`
 - b. If the user name contains “@” or “#”, the server specified by the last “@” or “#” is accessed.
 - c. If the previous step does not apply:
 - a. If the parent server is empty, the following is sent to the client: `-ERR USER format is USER username@hostname or username#hostname` and the command terminates.
 - b. Otherwise, the command is connected to the parent server.
 - d. If the connection fails, the following is sent to the client: `-ERR Can't Connect to (Server host: Server port) errmsg=[Connection error message]`
 - e. The following is sent to the server: `USER [User name]`
 - f. Receives a response from the server.
 - g. The following is sent to the client: `[Server response information]`

QUIT command

1. If connected to a server:
 - a. The following is sent to the server: `[Client request information]`
 - b. Receives a response from the server.
 - c. The following is sent to the client: `[Server response information]`
2. If not connected to a server, the following is sent to the client: `+OK Quit`

PASS /APOP /AUTH commands

1. If user restriction with the APOP command is enabled, and if the user is not added, 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, 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:
 - a. Virus logs are recorded.
 - b. A notification is sent to the administrator (if enabled).
5. If a virus is detected and the action on detection is “Delete”, 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 the previous step does not apply:
 - If a virus or spam is detected, the following is sent to the client: `Received: from FSIGK: Current time(RFC822 format)`
 - If spam is detected, the following is sent to the client: `X-Spam-Status: Yes(Product name) with [Detection name]`

- If a virus is detected, the following is sent to the client: `X-Virus-Status: disinfected(%s)` from `[Detection name]`
- If a virus is detected, the following is sent to the client: `X-Virus-Status: infected(%s)` with `[Detection name]`

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]`

9.11 FTP commands - operations

During FTP connections, commands executed from clients are operated in the following way.

-  **Note:** 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:
 - a. The server is accessed.
 - b. If access fails, the following is sent to the client: `-500 Can't Connect to (Server host: Server port) errmsg=[Connection error message]` and the session ends.
 - c. Receives a response from the server.
 - d. The following is sent to the client: `[Server response information]`
2. If the previous step does not apply, 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, 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, the following is sent to the client: `530 please use USER command at first.`
3. If steps 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, the following is sent to the server: `Client response information`
2. If the previous step does not apply:
 - a. If user authentication is enabled, but the user is not added, the following is sent to the client: `500 Invalid Account Auth.`
 - b. If the user name contains "@" or "#", the server specified by the last "@" or "#" is accessed.
 - c. If the previous step does not apply:
 - a. If the parent server is empty, the following is sent to the client: `500 USER format is USER username@hostname or username#hostname` and the command terminates.
 - b. Otherwise, the command is connected to the parent server.
 - d. If the connection fails, the following is sent to the client: `-500 Can't Connect to (Server host: Server port) errmsg=[Connection error message]`
 - e. The following is sent to the server: `USER [User name]`
 - f. Receives a response from the server.
 - g. The following is sent to the client: `[Server response information]`

QUIT command

1. If connected to a server:
 - a. The following is sent to the server: `[Client request information]`
 - b. Receives a response from the server.
 - c. The following is sent to the client: `[Server response information]`
2. If not connected to a server, 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)`, where:
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)`, where:
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:
 - a. The following is sent to the client: `530 please use PORT/PASV command at first.`
 - b. The command terminates.
2. If the mode is PASV:
 - a. Waits for a data session to connect.
 - b. If the source of the data session and control session are different, the following is sent to the client:
`530 Invalid Connection Source`, and the command terminates.
 - c. Connects to the server with the data session.
 - d. Receives a response from the server.
 - e. The following is sent to the client: `Server response information`
 - f. The command terminates if the response code is other than 1xx.
3. If the mode is Active:
 - a. Receives a response from the server.
 - b. The command terminates if the response code is other than 1xx.
 - c. Connects to the client with the data session.
 - d. If the client connection fails:
 - a. Information of the detection notification message: `530 Cannot connect client`
 - b. The session ends.
4. The file is received.
5. If the command is other than LIST/NLST and a virus is detected, the following is sent to the client: `530 Infected by [Detection name]`, and the command ends.
6. 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]`

9.12 Connection error messages

This section describes error messages that appear when a connection to a server fails.

CONNECT (Host: Port) /connect: Connect request to the IP address of a server failed.

[Connection error details]

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 Failed to lookup the host name.

lookup error: [Host name

lookup error details]

Host name lookups are performed using the getaddrinfo() function of Linux (glibc). The error details contain the human-readable string reported by gai_strerror().

CONNECT (Host: Port) /Access Inhibited by Proxy(FSIGK) Connection was denied due to access control settings on the destination.

9.13 Service process list

F-Secure Linux Internet Gatekeeper uses the following processes to provide its services.

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 scanning engine process (fsavd) as needed. Communication is processed by using the UNIX domain socket (fsavd-socket-0-fsav 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 scanning engine process (fsavd) as needed. Communication is processed by using the UNIX domain socket (fsavd-socket-0-fsav 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 scanning engine process (fsavd) as needed. Communication is processed by using the UNIX domain socket (fsavd-socket-0-fsav 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 scanning engine process (fsavd) as needed. Communication is processed by using the UNIX domain socket (fsavd-socket-0-fsav in the install directory). Up to 500 KB of memory cannot be shared per process.
fsavd	Handles the scanning engine process. The number of fsavd processes is configured in the file /opt/f-secure/fsigk/fssp/etc/fssp.conf with option daemonMaxScanProcesses. The default value is 40. The service is controlled by the /etc/init.d/fsigk_fsavd script. Up to 50 MB of memory cannot be shared per process.
fsicapd_service	Process used to provide ICAP virus scanning service. It makes ICAP service available for HTTP proxy proxy. To process sessions, the specified maximum number of simultaneous connections is used for processing.

9.14 Detection names

If F-Secure Internet Gatekeeper 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/en/web/labs_global/threats/descriptions

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 emails). The condition number indicates the number of lines detected in the database file.						
FSIGK/SPAM_LIST/VIRUSEROR /(Condition number)/ (Header field name)	Spam detected through a database (Virus and spam notification emails). 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: <table> <tr> <td>Detected address</td><td>Address registered in the RBL server</td></tr> <tr> <td>RBL server name</td><td>Name of the RBL server in which the address was found</td></tr> <tr> <td>RBL reply address</td><td>Reply address from the RBL server when spam was detected</td></tr> </table>	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
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

9.15 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 are given the detection name of "Catagory.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