

F-Secure Corporation

Integrating F-Secure Internet Gatekeeper with Zarafa Communication Server

White Paper



F-Secure Corporation
10/22/2012

Overview

F-Secure Internet Gatekeeper for Linux is a gateway solution that provides malware and spam protection for SMTP and POP3 protocols. It has an easy to use web user interface and can act as a transparent proxy for HTTP/FTP, and supports proxy authentication in both HTTP and SMTP with user verification for FTP and POP3.

F-Secure Internet Gatekeeper interoperates with firewall and e-mail gateway solutions, scanning web and e-mail traffic passing through the gateway. It runs on a variety of Linux distributions and standard server hardware, is cost-effective and easy to deploy and manage. Through the remainder of this document the solution will simply be referred to as IGK.

The main purpose of this document will be to demonstrate how to set up IGK to provide malware and spam protection for SMTP for a Zarafa Communication Server, although it could also be used in combination with the Zarafa gateway (POP3/IMAP) and even the HTTP functions to scan attachments up/downloads for Zarafa Webaccess.

System Requirements for F-Secure Internet Gatekeeper

These are the minimum hardware requirements for IGK:

- ✓ CPU: x86 compatible (2Ghz or faster recommended)
- ✓ Memory: 512 MB (1 GB or more recommended)
- ✓ Disk space: 5 GB (20 GB recommended)

The following 32-bit Linux distributions are officially supported:

- ✓ Asianux Server 3
- ✓ Asianux 2.0 (MIRACLE LINUX 4.0)
- ✓ Asianux 1.0 (MIRACLE LINUX 3.0)
- ✓ CentOS 4/5
- ✓ Debian GNU/Linux 5/6
- ✓ Red Hat Enterprise Linux 3/4/5/6
- ✓ SuSE Linux Enterprise Server 9/10/11
- ✓ Turbolinux 10 Server/11 Server
- ✓ Ubuntu 8.04/10.04

The following 64-bit Linux distributions are officially supported:

- ✓ Asianux Server 3
- ✓ Asianux 2.0 (MIRACLE LINUX 4.0)
- ✓ CentOS 5
- ✓ Debian GNU/Linux 5/6

- ✓ Red Hat Enterprise Linux 4/5/6
- ✓ SuSE Linux Enterprise Server 9/10/11
- ✓ Turbolinux 10 Server/11 Server
- ✓ Ubuntu 8.04/ 10.04

If you do not find your Linux distribution on the list above please check the latest release available here:

http://www.f-secure.com/en/web/business_global/support/downloads/-/carousel/view/79

Or contact your your local F-Secure partner for up to date product information.

System Requirements for Zarafa Communication Server

About Zarafa Collaboration Server, please check with your local Zarafa partner for any changes to the below.

To run Zarafa ZCS the computer must:

- ✓ Be x86 compatible (2Ghz or faster recommended)
- ✓ Have at least 1G of RAM (or more see the number off users recommended)
- ✓ Have at least 50 GB of free disk space (or more see number off users recommended)

Zarafa delivers a collaboration suite with access support for outlook, webaccess and mobile devices.

Zarafa ZCM is available on the following linux distributions:

OS Release	Supported CPU Architectures
RHEL 5	i386, x86_64, ia64*
RHEL 6	i686, x86_64
SLES 10	i586, x86_64, ia64*
SLES 11	i586, x86_64, ia64*
Debian 5.0 (Lenny)	i386, x86_64, ia64*
Debian 6.0 (Squeeze)	i386, x86_64
Ubuntu 8.04 LTS (Hardy)	i386, x86_64
Ubuntu 10.04 LTS (Lucid)	i386, x86_64

Setting it up

The server used in this example has the following configuration:

- ✓ One RedHat RHEL 5 x86_64 server
- ✓ 1 GB memory
- ✓ 50GB disk space
- ✓ MTA Postfix 2.2

Because this document covers adding F-Secure IGK to the Zarafa solution, we assume that the Zarafa is already up and running with postfix as MTA. All the software runs on the same server, so only one process can run on the default SMTP port 25. For that reason postfix is moved to port 9025.

Installation of F-secure IGK

F-Secure IGK can be downloaded from F-Secure’s website:

http://www.f-secure.com/en/web/business_global/support/downloads/-/carousel/view/79

The following steps will install IGK:

```
# tar xzvf f-secure-internet-gatekeeper-for-linux-4.07.3280.tar.gz
# cd f-secure-internet-gatekeeper-for-linux-4.07.3280
# rpm -hvi fsigk-4.07.3280-0.i386.rpm

Preparing...                               ##### [100%]
 1:fsigk                                   ##### [100%]

make[1]: Entering directory `/var/tmp/fsigk-4.07.3280'
-----
Preparing installation directory(/opt/f-secure/fsigk) ...
-----
-----
Stopping running proxies...
-----
-----
Installing program files to /opt/f-secure/fsigk ...
-----
```

```
-----  
Installing pattern files (AUA) ...  
-----  
-----  
Installing configuration files...  
-----  
Using database: userdb.db  
dbfile=[userdb.db.tmp.db]  
dbfile=[address.db.tmp.db]  
-----  
Version Up configuration files...  
-----  
=== version up /opt/f-secure/fsigk/conf/fsigk.ini from [407] to [407] ===  
-----  
Installing initscripts ...  
-----  
-----  
Installing pam configuration files ...  
-----  
-----  
Starting services...  
-----  
Starting /opt/f-secure/fsigk/fsaua/bin/fsaua: [ OK ]  
Starting fsupdated: [ OK ]  
Starting fsasd: [ OK ]  
Starting F-Secure Anti-Virus daemon (/opt/f-secure/fsigk/fssp/sbin/fsavd). Starting  
Tomcat(WebUI for fsigk): [ OK ]  
cp /opt/f-secure/fsigk/dbupdate /opt/f-secure/fsigk/fssp/bin/dbupdate  
-----  
Install succeeded!  
Please access following URL for starting proxy
```

<http://zarafa.f-secure.local:9012/>

(default user:admin, default password:admin)

 make[1]: Leaving directory `/var/tmp/fsigk-4.07.3280'

Configuration of F-secure IGK

Access the web GUI at <http://localhost:9012>, and log in with the default username and password (admin/admin).

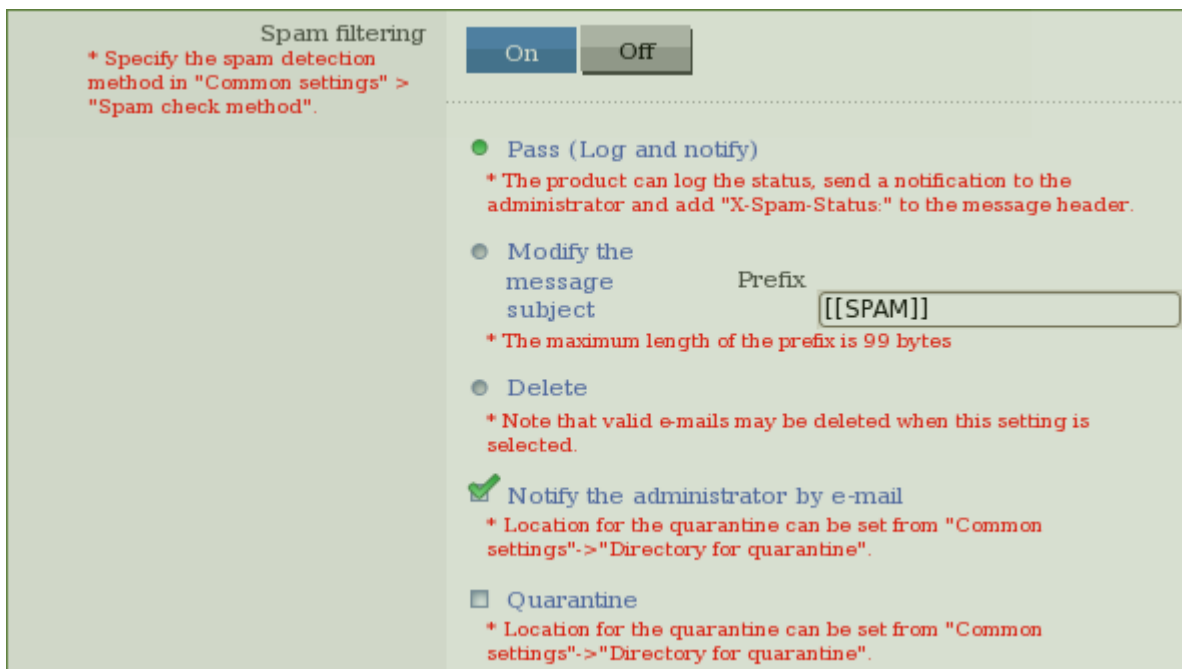


Under 'Proxy settings', make the following changes:

- Set 'SMTP proxy' to "ON"
- Set 'Proxy port' to "25"
- Set 'Virus scanning' to "ON"
- Under 'Global settings', set 'Host name' to "zarafa.f-secure.local" and 'Port number' to "9025"



Turn spam filtering on and choose the relevant options for handling messages detected as spam:



Turn riskware scanning on and enable IGK to scan the whole email message and content:

	* The maximum length is 1999 bytes.
▷ Maximum scanning time	<input type="text" value="90"/> seconds * "0" means "no time restriction". In case that "0" or large value is set, it will take long time for scanning, so that processing of proxy may be suspended.
▷ Riskware scanning	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
	Skip these targets: <input style="width: 100%; height: 30px;" type="text"/> * To specify multiple items, type each entry on a separate line. * The maximum length is 1999 bytes.
▷ Scan the e-mail message body	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
▷ Scan the whole HTML content in the e-mail	<input checked="" type="button" value="On"/> <input type="button" value="Off"/>
▷ Anonymous proxy Do not add the header information (Received header) on the proxy.	<input type="button" value="On"/> <input checked="" type="button" value="Off"/>

To restrict SMTP relaying, add the domains handled by the Zarafa server.

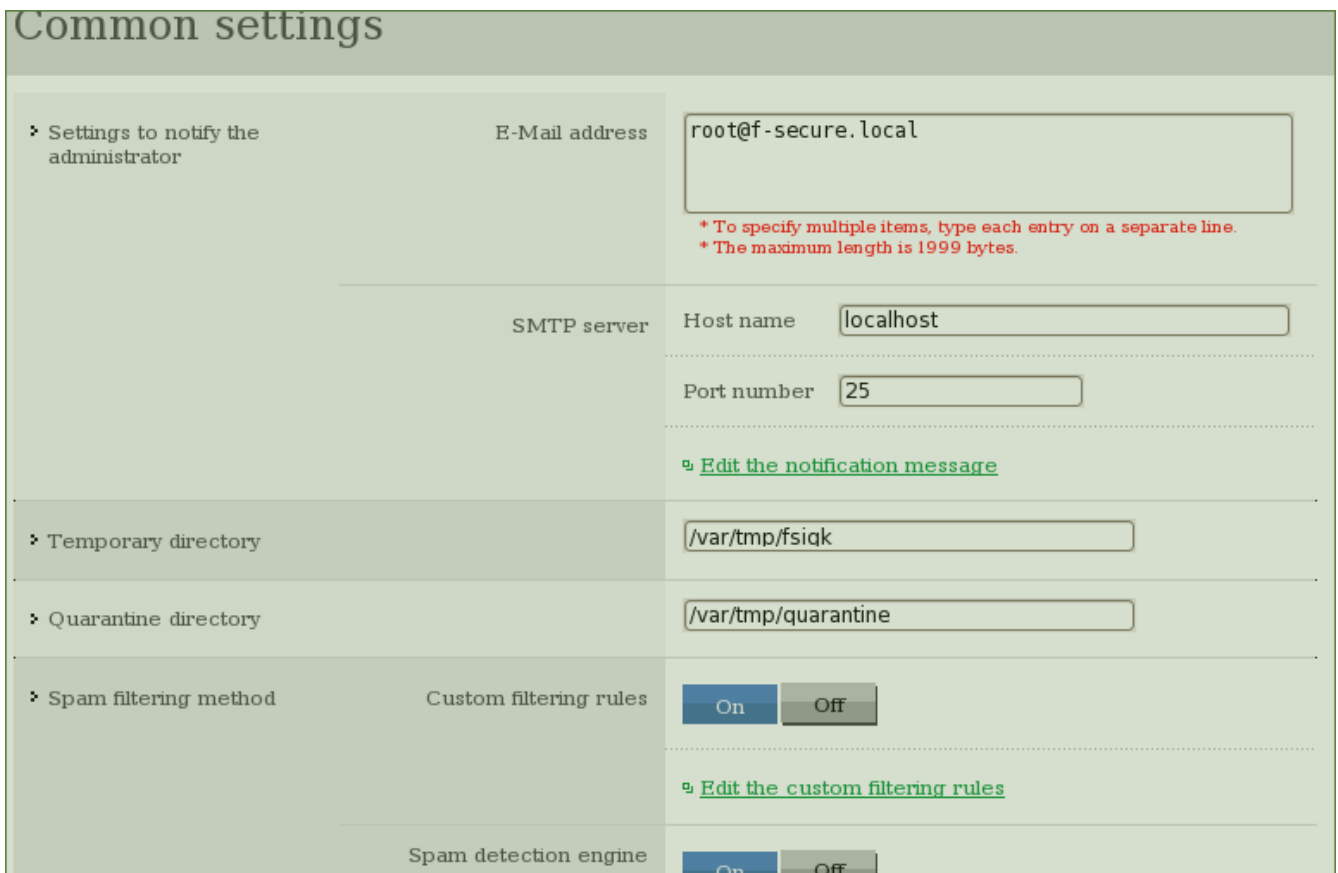
Restrict e-mail recipients
 * Specify destination domains.

* To specify multiple items, type each entry on a separate line.
 * The maximum length is 1999 bytes.

Save and restart.



Under the 'Proxy settings' tab, choose 'Common settings'.



Under 'Spam filtering method', enable both custom filtering rules and spam detection engine.

<p>RBL (Real-time Black List)</p> <p>If the RBL is turned on, the product filters the e-mail as spam if its source IP address (in SMTP) or the IP address in the "Received" header can be found in the RBL.</p>	<p><input type="button" value="On"/> <input checked="" type="button" value="Off"/></p> <hr/> <p>Server</p> <p>bl.spamcop.net sbl-xbl.spamhaus.org</p> <p><i>* To specify multiple items, type each entry on a separate line. * The maximum length is 1999 bytes.</i></p> <hr/> <p>Addresses to be excluded</p> <p>127. 10. 192.168. 172.16.0.0/255.240.0.0</p> <p><i>* To specify multiple items, type each entry on a separate line. * The maximum length is 1999 bytes.</i></p>
<p>SURBL (SPAM URL Real-time Black List)</p> <p>If the SUREBL is turned on, the product filters the e-mail as spam if the domain name part of any URL in the text body or HTML code can be found in the SURBL.</p>	<p><input type="button" value="On"/> <input checked="" type="button" value="Off"/></p> <hr/> <p>Server</p> <p>multi.surbl.org</p> <p><i>* To specify multiple items, type each entry on a separate line. * The maximum length is 1999 bytes.</i></p>

Save and restart to activate the settings.

Changing the license

To convert from the evaluation license to a corporate license, choose 'License' from the main page:



Configuration of Postfix MTA

IGK is receiving email on the standard SMTP port 25 with this configuration, and is delivering messages to `zarafa.f-secure.local` (the ZCS running on the same server) on port 9025. To make Postfix listen on this port, change the configuration file `/etc/postfix/master.cf`

Change the line

```
smtp      inet  n       -       n       -       -       smtpd
```

to

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

then restart postfix:

```
# service postfix restart
```

Configuring zarafa dagent

To deliver messages detected as spam to the users "Junk mail" folder, edit `/etc/zarafa/dagent.cfg`

Change the line

```
spam_header_value=Yes
```

to

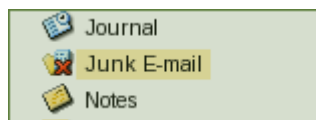
```
spam_header_value=Yes (F-Secure/fsigk_smtp/407/zarafa.f-secure.local)
```

Adjust the hostname and IGK version number as needed.

Restart dagent

```
service zarafa-dagent restart
```

ZCS will now deliver spam to the users “Junk E-mail” folder:



Further Reading

Release notes, manuals and installation binaries for IGK and other F-Secure products can be found here:

http://www.f-secure.com/en/web/business_global/support/downloads

An evaluation license for IGK for 30 days can be requested here:

http://www.f-secure.com/en/web/business_global/trial

Known things to consider

The IPv6 protocol needs to be disabled on Linux with the current version. Support for IPv6 is planned for IGK 5.0.