{http://program.farit.ru/images/program-logo.gif?nolink&350x30}}

{http://program.farit.ru/images/space.gif?nolink&4x2}}

Free Clamav Anti-Virus, Kaspersky Anti-Virus (AVP), Sophos Anti-Virus, Trend Micro, Dr.Web and SpamAssassin Anti-Spam External Filter (Plugin) for CommuniGate Pro.

http://program.farit.ru/doc/cgpav.html

**Description**

It is used to scan all email messages that are transferred via the CommuniGate Pro mail server **www.stalker.com****

Clamav, free and open-source: **www.clamav.net****
Kaspersky Anti-Virus: **www.avp.ru****
Sophos Anti-Virus: **www.sophos.com**** Sophie daemon for Sophos: **www.vanja.com****
Trend Micro: **www.antivirus.com**** Trophie daemon for Trend Micro: **www.vanja.com****
Dr.Web: **www.sald.com****
SpamAssassin Anti-Spam: **www.spamassassin.org****

The main distribution site for cgpav: **program.farit.ru****
The first versions of cgpav were developed and supported by Damir Bikmuhametov.

**How it works**

The program reads requests from its standard input in the form:
seqNum FILE fileName
for example:
1111 FILE Queue/111111.msg

Then it parses the input line and adds a new element into the query list structure, containing the seqnum and filename. The program creates a child process for each element from the list that sends the request to the anti-virus daemon through the socket and waits for the result. It sends the file name for scanning constructed in the form: cgpro_home + / + filename.
The number of child processes depends on the number of the Enqueuer processors in the CommuniGate Pro settings and the value of max_childs in the configuration file cgpav.conf. These numbers should be equal and > 1. 10 is a good choice.

Depending on the anti-spam and anti-virus response codes, the program prints out to the standard output different response.

When a message is not infected and it is not spam, it prints:
seqNum OK
Also, it answers OK in all “problem” situations: a timeout while virus scanning, either the anti-virus or anti-spam daemon is not responding, etc.

When a message is infected, the program prints something like:
seqNum ERROR “WARNING! Your message is infected by VIRUS: I-Worm.Sircam.c”
When a message is detected to be spam, it prints:
seqNum ERROR “You are a known spammer.\\nYour message was rejected”
When CommuniGate Pro receives such a response, it creates an Undeliverable message that includes the text sent in the program response.

It can also silently **DISCARD** messages without delivering to recipient, **ADDHEADER** - adds the special headers when a virus or spam were detected allowing an end user to filter such messages in his own mail program. Certainly, no normal user wants to receive viruses, so you should choose the reject or discard actions for infected messages. But the program can mark some “good” messages as spam, so it's better to leave the final decision to the end users by defining addheader for spam_action.

If your users have mail programs that cannot filter by the headers, you can add a Rule that rewrites the Subject field of messages. This Rule should be run after the Rule that invokes cgpav. It can match using the special spam header or the spam score. For the latter, you should change the default symbol indicating the spam score from '*' to '+' because '*' is a special symbol in the cgpro rules. Use the option spam_level_char to redefine the symbol.

The program can send additional notification messages about an infected message to the sender and recipients by writing notification messages to the Submitted directory. The PIPE module of CommuniGate Pro scans this directory periodically and sends all messages in it.
You can enable the notification texts in several languages messages in the configuration file.
It can also send notifications to the postmaster of the whole mail server and the postmasters of the virtual domains.

When there is some temporary malfunction, the program prints something like:
seqNum REJECTED “Antiviral filter unavailable. Will try later”
This situation can happen, for example, when the daily virus base updater script reloads the anti-virus daemon.
The mail message is not rejected, it is stored in the CommuniGate Pro queue for the further processing. Though, the mail flow will stop at that moment. cgpro will try to supply this and other messages from the queue for the filter processing again and again.

If the sequential count of the REJECTED messages exceeds the max_errors parameter in the configuration file, the program will answer OK until the anti-virus daemon will start functioning.

cgpav uses the standard spamd SpamAssassin daemon. The default action is to add the header 'X-Spam-Status: Yes' to the messages for which the spam score exceeds required_hits. Users can filter such messages in their mail clients or create a rule in CommuniGate Pro to store them in a special folder.

Moreover, you can define another action when the spam score is more than extra_spam_score, e.g. discard (silently remove messages). It's rather high and is useful in cleaning your mail server from the obvious spam as most users do nothing in order to use the above mentioned header.

An example of the web-interface in php for the end users is included. The users can customise the spam hits, actions, disable some tests and can create the Rule to store the identified spam in the special folder.

**Installation**

Unpack the sources:
gzip -cd cgpavXXX.tar.gz

- sophos based anti-virus daemon. Follow instructions for it.
As at the time of writing run ./configure, copy sophie.cfg and sophie.savi into /etc and edit them.

sophie.savi.individual would be a good example for sophie.savi
I recommend to change user and group in sophie.cfg to root or the user your CommuniGate Pro works under.

You can compile scan_file.c in sample_appls/sock to test the daemon.

Then add an entry into cron to run sophosupdate.pl daily or more often.

**TREND MICRO:**

Place libvsapi.so and pattern file into /etc/iscan dir. They can be downloaded for evaluation **www.antivirus.org****
Download Trophie daemon **www.vanja.com****
./configure –with-user=root –with-group=root

**DR.WEB:**

In the file /etc/drweb/drweb32.ini set path to Unix socket:
Socket=/var/run/drwebd.socket
User 'drweb' must be in the 'mail' group to have ability of accessing /var/CommuniGate/Queue dir. Or run drwebd by 'root', in drweb32.ini:
User = root
Run drwebdc to check functioning of the drwebd daemon.

**SPAMASSASSIN:**

If you want to install SpamAssassin, download it from **www.spamassassin.org****.

Compile it:
perl Makefile.PL
make
make test
make install

Or download an rpm or deb package for your distribution.

Test it by running:
spamassassin -t < sample-spam.txt > sample-spam.txt
spamassassin -t < sample-nonspam.txt > sample-nonspam.txt

Check if sample-spam.txt marked as being spam message.

**Configuration**

The configuration file **cgpav.conf**** should reside in /var/CommuniGate/Settings, /var/CommuniGate or /etc directories.
The program first scans the /var/CommuniGate/Settings directory, then /var/CommuniGate, and /etc, it will use the first found cgpav.conf. You can change this behaviour by editing cthe fg.c source or by adding the option -f while running cgpav:
./cgpav -f /var/elsewhere/cgpav.conf

If the program can't find any cgpav.conf file or if you have omitted some required parameters in it, it will use the defaults from cfg.h

Most values in cgpav.conf are good for the standard cgpro and anti-virus installations. If you store the user settings for spamassassin in the database, set the password for the database user.

Some options are multiline, usually enumerations separated by commas. You can continue them on the next line adding the option name in front. Use as many lines as you wish.

It may be useful to include your networks where outgoing mail can come from in the local_networks option. Then your outgoing mail will not be scan for spam decreasing the server load. Don't forget to exclude any relays that can redirect the incoming mail.

### Testing

You may save some time if you first configure cgpav in the DEBUG mode:
CFLAGS="-g -DDEBUG" ./configure
cgpav will show more debug information in this mode and it will work in the single process mode.
Don't forget to reconfigure it back:
./configure

Copy a file with a virus (named, for example, eicar.com) to the /var/CommuniGate directory.

Run the Filter from the command line by typing ./cgpav
Then enter something like:
1 FILE eicar.com

If you see something like
1 ERROR "WARNING! Your message was infected by VIRUS: EICAR-AV-Test"
then cgpav works fine.

If you see only
1 OK
then the program doesn't find viruses.

Kaspersky:
First look into the log file of kavdaemon (/root/kavscan.rpt). If you see that kavdaemon have found the virus you can uncomment the response line in the function avp_scan_file in avpcomm.c file.
In Linux responses are: 0x134 (octal) for infected and 0x130 for good. In Sparc Solaris: 0x1340000 and 0x1300000

### Installation into CommuniGate Pro

Check documentation from their site: **www.stalker.com****

SETTINGS→Rules
Priority Name
10 virus scan

Click to Edit
Data

Message Size greater than 1024

Action
ExternalFilter

Go to the Settings→General→Helpers
and in the menu Content Filtering add the path to the program

Mark Content Filtering
Program Path: cgpav
if it is located in the CommuniGate Pro home directory or write there the absolute path to it.

Leave parameters “Time-out” and “Auto-Restart in the new versions of CommuniGate Pro disabled. Change them only if cgpav crashes. Certainly, cgpav has been made to be very reliable and to avoid crash problems.

**Configuring SpamAssassin**

The SpamAssassin testing is disabled by default. You must be very careful with it as it can reject some useful mail. It's not the 5 minute work!

After installing SpamAssassin you must fire up some fast database. MySQL www.mysql.com is the best choice, also PostgreSQL is supported. You have to install libmysqlclient-dev or postgresql-dev package, or have headers and libs. Also, install the Perl DBI and DBD modules for your database. Here we will mention only the use of MySQL, you must adjust the configuration for PostgreSQL.

We store every user's own preferences in the database.
Connect to mysql as root:
mysql -u root -p
and create a new database named, for example, spamassassin:
mysql>CREATE DATABASE spamassassin;
Then create and grant priviliges to a user named, for example, spamassassin:
mysql>GRANT ALL ON spamassassin.* TO spamassassin@localhost IDENTIFIED BY 'secretpassword';
Certainly, secretpassword must be your own password.
Exit from the database.

Then create the table userpref:
CREATE TABLE userpref (
username varchar(100) NOT NULL,
preference varchar(30) NOT NULL,
value varchar(100) NOT NULL,
prefid int(11) NOT NULL auto_increment,
PRIMARY KEY (prefid),
INDEX (username)
) TYPE=MyISAM;

You can find the file userpref.sql in the directory spam/sql.
Run from the command line:
mysql -u spamassassin -p spamassassin < userpref.sql

Download and compile the DBI and DBD Perl modules for your database search.cpan.org. Or install

them from packages or rpm.

Go to the spamassassin configuration directory: /etc/mail/spamassassin or /etc/spamassassin. Add to the local.cf file these lines:

| | |
|---|---|
| user_scores_dsn | DBI:mysql:spamassassin:localhost |
| user_scores_sql_username | spamassassin |
| user_scores_sql_password | secretpassword |

Parameter user_scores_dsn must be in the form:
user_scores_dsn DBI:driver:database:hostname[:port]
Adjust it for your own database.

If you'll use spamd on the localhost, it's better to connect to it through the unix socket. If it's installed on another computer, use the tcp socket. Set the appropriate value in cgpav.conf:
spamassassin_socket_type = unix

If you use the unix socket, set running parameters for spamd like:
-d -m 10 -x -q -u mail –socketpath=/var/run/spam
In case of the tcp socket:
-d -m 10 -x -q -u mail -i spamd.daemon.ip -p 783 -A your.mail.server.ip
Where spamd.server.ip - IP-address of the spamd server, your.mail.server.ip - IP-address of your mail server from which it connects to the spamd server. You can set several IPs separated by comma.

Check spamd with the help of the spamc program:
spamc -U /var/run/spam < sample-spam.txt > sample-spam.log
I recommend you to add -D (debug) option to the spamd parameters, it will give detailed information in the log files.

Create the file 50_whitelist.cf in the SpamAssassin's configuration directory and add domains of your trusted neighbours:
whitelist_from *@*.gooddomain.com

You can also create the 50_blacklist.cf file to add the known spammer sites:
blacklist_from *@flowgo.com
Good blacklist can be found here: www.stearns.org/sa-blacklist/

You can even create your own rules using the regular expressions. Note: scores may be negative. File 55_head_tests_my.cf:

| | |
|---|---|
| header MY_GIRL | Subject =~ /my.{1,15}darling/i |
| describe MY_GIRL | Subject: That's my dear girl |
| score MY_GIRL | -10.0 |

File 55_body_tests_my.cf:

| | |
|---|---|
| body MY_BOSS | /Your.{1,15}boss/i |
| describe MY_BOSS | Boss want something again |
| score MY_BOSS | 3.0 |

Set up the interface for user self-adjustment of the spam actions, required_hits, white and black lists. An example in php is available in the spam/www/php directory. It will authorize against CommuniGate

Pro on the 106 port. You can use any other tool or interface that can manipulate the database.
Note: you must always insert the full user's e-mail address into the username field, not just his name. jeorge@domain.com is correct, jeorge is incorrect.

### Known problems

If you disable-enable antivir in Content Filtering in CommuniGate Pro Settings→Helper Settings, the old cgpav process becomes zombie.

Don't worry. You must reload CommuniGate to kill them.

### Licence

The program is licenced under GPL.

Certainly, you must get your own licence for commercial Anti-Virus daemons.

### Suggestions for Kaspersky

Again, add path to CommuniGate Queue directory into Anti-Virus starting script (/etc/init.d/kavdaemon) and into Antivirus Base updating script (/opt/AVP/kavupdater.sh or cron script) parameters:
DPARMS=”-I0 -Y /var/CommuniGate/Queue“
Or simply add path into AvpUnix.ini [Object]→Names with star * sign in front of.

Insert UpdatePath line into AvpUnix.ini to allow downloading of virus updates (Can be run daily by cron):
UpdatePath=ftp://ftp.kaspersky.ru/updates/
Or use another ftp-site from the Updates.lst file.

Don't waste resources by changing parameter -I0 (just scan for viruses) to -I2 (virus curing). Files in messages are packed by MIME and Anti-Virus can't cure them. Also CommuniGate doesn't like when somebody changes the size of posted messages.

Please, change this setting in defUnix.prf:

[Options]
ParallelScan=Yes

[Report]
Report=No

Enable reporting only on the testing stage.

### Suggestions for Sophos

I included the virus IDE updater script sophosupdate.pl You might not have some Perl modules to run it, for example, Archive::Zip. Download them from your OS's distribution site or from **search.cpan.org****

### Suggestions for SpamAssassin

In the cron directory you can find the program delete_old_mail, using which you can automatically delete old messages from the Spam folder where spam messages are stored.

The required module CLI.pm can be found here: www.stalker.com/CGPerl



If you use the Bayes filter in SpamAssassin, adjust these options in its settings carefully:
bayes_path
bayes_journal_max_size
bayes_expiry_max_db_size
bayes_auto_learn_threshold_spam

You can find triggered spam test names in the message header X-Spam-Status. Analyse their scores by running a message through command
spamassassin -t < test_message > test_message.log

If some of the tests work undesirably, disable them by setting their score to 0 or lowering it.

### How to check messages for other servers in domain

For example, you have the server mail.domain.ru with installed virus filter and you want to protect another mail server alpha.domain.ru.

In Settings→Router add the line
Relay: alpha.domain.ru = alpha.domain.ru@alpha.domain.ru.25.smtp

In DNS record add MX lines:

| | | | | |
|---|---|---|---|---|
| alpha | IN | MX | 10 | mail.domain.ru. |
| | IN | MX | 20 | |

### Logging

The program logs the information about all messages with viruses using the standard syslog local0 facility.
You can find log lines in the main syslog file:
Jan 1 00:00:11 mail cgpav: Virus: I-Worm.BadtransII From: anna@mail.host.ru To: antivirus@test.ru

You can change the parameter log_facility in cgpav.conf in order to use another logging facility (mail, local0 - local7)

If you want to redirect all antivirus messages somewhere else you can do it by editing the file /etc/syslog.conf
local0.* -/var/log/virus.log

### Authors

Programmed by Damir Bikmukhametov and Farit Nabiullin.
Solaris patch for AVP by Vitaly from afn.ru
Sophie and Trophie daemons by Vanja Hrustic **www.vanja.com****
UUdeview library by Frank Pilhofer **www.fpx.de****
SpamAssassin by Jastin Mason **www.spamassassin.org****
spamd by Craig R Hughes