Avira AntiVir WebGate (Suite)

HowTo

AVIRA

Table of contents

1. In which environments can it be utilized?

- As a proxy server with HTTP monitoring or FTP via HTTP monitoring
- It can work at the front end or back end of another proxy server
- As an integreation into an ICAP environment (Internet Content Adaption Protocol)
- As an access control based on a client IP-address or a target port

2. Installation

2.1 Interactive installation

► Please download the latest TGZ-package onto your server:
http://www.avira.com/en/download/product/avira-antivir-webgate

► Decompress the downloaded file by entering:

```
gzip -d antivir-webgate-prof.tar.gz
```

► Then, unpack it by entering:

```
tar -xvf antivir-webgate-prof.tar
```

► Change into that directory with:

```
cd antivir-webgate-prof-<version>
```

The installation directory for Avira AntiVir WebGate is structured as follows:

`bin`	-	Executable files
`cert`	-	Avira certificate
`doc`	-	documentations
`etc`	-	configuration files
`legal`	-	license agreement for 3rd-party tools
`script`	-	shell scripts
`smcpkg`	-	AMC-specific files
`templates`	-	standard templates for WebGate
`vdf`	-	basic virus definitions
`.installrc`	-	product information file
`build.dat`	-	product build version
`install`	-	main installation script
`install_list_webgate`	-	installation files and permissions
`LICENSE`	-	Avira GmbH software license agreement
`LICENSE.DE`	-	Avira GmbH software license agreement
`README`	-	description installation package
`README.uninstall`	-	description uninstall routine
`uninstall`	-	uninstall routine
`uninstall_smcplugin.sh`	-	uninstall script for AMC-plugin

► Now perform the installation by entering:

```
./install
```

and then follow the installation dialog.

If you have already performed an installation at an earlier point in time, you can further accelerate the installation:

```
$ ./install -fast
```

The following queries are recommended and should be adopted:

```
Would you like to setup Engine and Signature updates as cron
task ? [y]

Please specify the interval to check. Recommended values are
daily or 2 hours. available options: d [2]

Please specify if boot scripts should be set up.
Set up boot scripts [y]
```

2.2 Automatic installation

If you want to perform a completely automatic (unattended) installation, you can use the installation option that is also used internally by the AMC:

```
$ ./install --fast --inf=./smcpkg/setup.inf
```

All settings for the automatic installation can be found in the mentioned INF-file. Therefore, you could also use a copy with your own settings. This would enable you to perform a major rollout or simply improve your daily tasks.

./smcpkg/setup.inf:

```
SAVAPI3_ADDLINK=y

WEBGATE_ADDLINK=y

WEBGATE_AUTOSTART=y

UPDATER_INSTALL=y

UPDATER_ADDLINK=y

UPDATER_ADDCRONJOB=y

UPDATER_CYCLE_SIG_EN=2h

UPDATER_CYCLE_PROD=n

SMC_INSTALL=y

ANTIVIR_CONFIG=n

LICENSE_AGREEMENT=y

REPLACE_CRONJOB=n

REPLACE_CRONJOB_PRODUCT=n
```

3. Recommended base configuration

You can find a majority of the configuration parameters of WebGate in the product configuration file at */etc/avira/avwebgate.conf*.

Next, you will find the recommended settings after the installation, if you so wish:

3.1 HTTPPort: Port for monitoring HTTP-connections

Example: `HTTPPort 8080`

This makes WebGate scan on Port 8080 for queries. The port needs to be changed accordingly as long as there is another service of a proxy server running.

3.2 FTPPort: Port for monitoring FTP-connections

Example: `FTPPort 2121`

WebGate also offers a FTP proxy service, if you so wish.
The port needs to be changed accordingly as long as there is another service of a proxy server running.

3.3 Quarantine directory

Example: `MoveConcerningFilesTo /home/quarantine`

In case of a detection the file will be moved into the quarantine directory and renamed. Therefore, the file will on one hand not be accessible anymore for the user and on the other hand will not be changed or deleted e.g. in case of a false positive.

3.4 Setting the log file

Example: `LogFile /var/log/avwebgate.log`

Sets the log file of the OnAccess-scanner. The Syslog will be used by default.

3.5 Defining the quality of the output

```
LogLevel 4
```

This will set a medium LogLevel. Alerts (e.g. a virus detection), error messages (e.g. a faulty ACL configuration) and warnings (e.g. in case of an encrypted archive) will be logged.

3.6 Activating heuristics on a medium level

```
HeuristicsLevel 2
```

A good mixture between detection and early detection. This will prevent a high number of false positives.

3.7 Activating the detection of macro viruses in office documents

```
HeuristicsMacro yes
```

We recomment the scan in office documents for the best monitoring possible.

4. What can be configured additionally?

These configurations should be planned in advance and only be added if needed. The values have to be adopted accordingly.

4.1 Proxy settings

The following proxy settings are possibly necessary to connect the corresponding proxy server in front of WebGate.

```
HTTPProxyServer your.proxy

HTTPProxyPort 3128

HTTPProxyUsername username

HTTPProxyPassword password

FTPProxyServer your.proxy

FTPProxyPort 2121
```

4.2 Activating the ICAP server

This will activate the ICAP server of WebGate. The service will then run additionally on the selected port. The ICAP server supports the reqmod (request modification) as well as respmod (response modification).

Squid will support ICAP 1.0 only from version 3.x!

```
ICAPPort 1344
```

4.3 Allowing HTTPS Tunnel

To prevent it from being scanned, WebGate blocks the HTTPS-data stream by default.
However, if you still want to tunnel HTTPS pages, you can set the following parameters:

```
AllowHTTPSTunnel 1
```

4.4 Progress bar

Shows a page in the browser that will display a progress bar during major downloads. Additionally, the interval needs to be set in seconds (e.g. 3), which will send a refresh command to the browser.
The activation and configuration of the progress bar can be done using a single parameter that needs to be defined as follows:

```
RefreshInterval 3
```

4.5 X-Header

The following parameter adds the X-header of the client in the query to inform backend proxy servers about the actual requesting client.

```
AddXForwardedForHeader 1
```

4.6 Address range with access permissions

This will set the clients or address ranges with access permission.
Unauthorized clients that want to have access to WebGate, will be blocked.

```
AllowClientAddresses 127.0.0.1 192.168.0.0/16
```

5. Particular features

5.1 Squid as a proxy server

This will send all queries from the client to squid via WebGate. Thus, the use of the squid proxy function willl be enabled.

Required settings within the squid.conf:

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default

acl ALL src all

never_direct allow ALL
```

5.2 ICAP configuration

Squid can function as a ICAP-client to process queries by starting the ICAP server mentioned at 4.2.

Required settings within the *squid.conf*

```
icap_enable on

icap_service service_1 reqmod_precache  0 icap://[WEBGATE_
HOST]:1344/reqmod

icap_service service_2 respmod_precache 0 icap://[WEBGATE_
HOST]:1344/respmod

adaption_service_set class_1 service_1
adaption_service_set class_2 service_2

adaption_access class_1 allow all
adaption_access class_2 allow all
```

Note:
If you are using Squid 3.0 or earlier you need to change the following parameters:
adaption_service_set -> icap_class
adaption_access -> icap_class

6. Update configuration

Two types of updates will be set up during the installation to keep your AntiVir installation up to date:

- Scanner update (only scanner & engine & VDF)
- Product update (Guard, program files)

This can be generally very interesting for you if you consider program updates as a particularly sensitive issue. Thus, you will get the possibility to perform an audit on a separate test system prior to using the new version productively.

After the installation, you will find the settings for the update in the following file:

/etc/cron.d/avira_updater:

```
00 */2 * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=Scanner
15 12 * * Tu root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=WebGate
```

6.1 Useful settings for an update

Depending on the target group, we recommend for our customers to perform an update at least 2 or 3 times a day.

6.1.1 Medium and large businesses

Example: every hour

/etc/cron.d/avira_updater:

```
* */1 * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=Scanner
```

6.1.2 Small businesses

Example: every 3 hours

/etc/cron.d/avira_updater:

```
* */3 * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=Scanner
```

6.1.3 Customers with narrowband connections (modem/ISDN):

Example: every 8 hours

/etc/cron.d/avira_updater:

```
* */8 * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=Scanner
```

6.1.4 Internet service provider

For internet service providers it is of course recommended to look significantly more frequently for new signatures. Therefore, the frequency of update requests should be set considerably higher, e.g. every 15 minutes. This ensures that you always use the latest signatures.

/etc/cron.d/avira_updater:

```
*/15 * * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=Scanner
```

7. WebGate Suite feature

The WebGate Suite feature allows you to block certain categories of web sites. Those include e.g. sites with pornography, phishing, malware and fraud.

The following filter categories are available:

Numeric value	Category
0	Pornography
1	Erotica/Sex
2	Swimwear/Lingerie
3	Shopping
4	Auctions/Classified Ads
5	Governmental Organizations
6	Non-Governmental Organizations
7	| Cities/Regions/Countries
8	Education
9	Political Parties
10	Religion
11	Sects

12	Illegal Activities
13	Computer Crime
14	Political Extreme/Hate/Discrimination
15	Warez/Hacking/Illegal Software
16	Violence/Cruelty
17	Gambling/Lottery
18	Computer Games
19	Toys
20	Cinema/Television
21	Recreational Facilities/Amusement/Theme Parks
22	Art/Museums/Memorials/Monuments
23	Music
24	Literature/Books
25	Humor/Comics
26	General News/Newspapers/Magazines
27	Web-Mail
28	Chat
29	Newsgroups/Bulletin Boards/Blogs
30	Mobile Telephony
31	Digital Postcards
32	Search Engines/Web Catalogs/Portals
33	Software/Hardware/Distributors
34	Communication Services
35	IT-Security/IT-Information

36	Website Translation
37	Anonymous Proxies
38	Illegal drugs
39	Alcohol
40	Tobacco
41	Self-Help/Addiction
42	Dating-Agencies/Relationships
43	Restaurants/Bars
44	Travel
45	Fashion/Cosmetics/Jewelry
46	Sport
47	Real Estate/Living/Architecture/Furniture
48	Nature/Environment/Animals
49	Personal Homepages
50	Job Search
51	Investment Brokers/Stocks
52	Financial Services/Investment/Insurances
53	Banking/Home Banking
54	Vehicles/Transportation
55	Weapons/Military
56	Health
57	Abortion
59	Spam-URLs
60	Malware

61 Phishing-URLs

62 Instant Messaging

63 Fraud
66 General Economics

73 Banner Advertising

76 Social Networking
77 Business Networking

78 Social Media

79 Web Storage

You can set the corresponding parameters in */etc/avira/avwebgate.conf* to block certain categories.

The following example blocks pages of the category Pornography (0) up to Swimwear/Lingerie (2), Illegal Activities (12), Political Extreme/Hate/Discrimination (14), as well as Phishing URLs (61):

```
BlockCategories 0-2 12 14 61
```

You can find further information and configuration options of Avira AntiVir WebGate (Suite) in the manual or in our knowledge base at

http://www.avira.com/en/support-for-business-knowledgebase-search

Issued Q3-2012

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile +49 7542-500 3000
www.avira.com