Avira AntiVir WebGate (Suite)

Kurzanleitung

AVIRA

Inhaltsverzeichnis

1. In welchen Umgebungen kann es eingesetzt werden? 4

2. Installation 4
2.1 Interaktive Installation 4
2.2 Automatische Installation 6

3. Empfohlene Basiskonfiguration 7
3.1 HTTPPort: Port für die Überwachung von HTTP-Verbindungen 7
3.2 FTPPort: Port für die Überwachung von FTP-Verbindungen 7
3.3 Quarantäneverzeichnis 7
3.4 Logdatei festlegen 7
3.5 Qualität der Ausgabe definieren 8
3.6 Heuristik auf Stufe Mittel aktivieren 8
3.7 Erkennung von Macroviren in Office-Dokumenten aktivieren 8

4. Was kann zusätzlich konfiguriert werden? 9
4.1 Proxyeinstellungen 9
4.2 Aktiviere ICAP Server 9
4.3 Erlaube HTTPS Tunnel 9
4.4 Fortschrittsanzeige 10
4.5 X-Header 10
4.6 Zugriffsberechtigter Adressraum 10

5. Besonderheiten 10
5.1 Squid als Proxyserver 10
5.2 ICAP Konfiguration 11

6. Updatekonfiguration 11
6.1 Sinnvolle Werte für ein Update 12
6.1.1 Mittlere und große Unternehmen 12
6.1.2 Kleine Unternehmen 12
6.1.3 Kunden mit Schmalband-Anschlüssen (Modem/ISDN): 12
6.1.4 Internet Service Provider 12

7. WebGate Suite Feature 13

1. In welchen Umgebungen kann es eingesetzt werden?

- Als Proxyserver mit HTTP sowie FTP über HTTP-Überwachung
- Kann sowohl vor als auch hinter einem weiteren Proxyserver fungieren
- Als Integration in eine ICAP-Umgebung (Internet Content Adaptation Protocol)
- Als Zugangskontrolle auf Basis von Client IP-Adresse oder Zielport

2. Installation

2.1 Interaktive Installation

► Laden Sie sich das aktuelle TGZ-Paket auf Ihren Server:
http://www.avira.com/de/download/product/avira-antivir-webgate

► Dekomprimieren Sie die heruntergeladene Datei durch die Eingabe von:

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

► Daraufhin können Sie diese entpacken:

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

► Wechseln Sie in das Verzeichnis mit:

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

Das Installationsverzeichnis für Avira AntiVir WebGate ist wie folgt gegliedert:

`bin`	-	Ausführbare Dateien
`cert`	-	Avira Zertifikat
`doc`	-	Dokumentationen
`etc`	-	Konfigurationsdateien
`legal`	-	Lizenzbestimmungen 3rd-Party Bestandteile
`script`	-	Shell Skripte
`smcpkg`	-	AMC-spezifische Dateien
`templates`	-	Standard-Templates für WebGate
`vdf`	-	Basisvirendefinitionen
`.installrc`	-	Produktinformationsdatei
`build.dat`	-	Produkt Build Version
`install`	-	Hauptinstallationsskript
`install_list_webgate`	-	Zu installierende Dateien und Rechte
`LICENSE`	-	Avira GmbH Software License Agreement
`LICENSE.DE`	-	Avira GmbH Software Lizenzbestimmungen
`README`	-	Beschreibung Installationspaket
`README.uninstall`	-	Beschreibung Deinstallationsroutine
`uninstall`	-	Deinstallationsroutine
`uninstall_smcplugin.sh`	-	Deinstallationsskript für AMC-Plugin

► Führen Sie daraufhin die Installation aus durch die Eingabe von:

```
./install
```

und folgen dann dem Installationsdialog.

Haben Sie bereits eine Installation zu einem früheren Zeitpunkt durchgeführt, können Sie die Installation zusätzlich beschleunigen:

```
$ ./install –fast
```

Folgende Abfragen sind empfohlen und sollten übernommen werden:

```
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 Automatische Installation

Wenn Sie eine komplett automatische (unattended) Installation durchführen wollen, können Sie die Installationsvariante verwenden, die auch von der AMC intern verwendet wird:

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

Alle Einstellungen für die automatische Installation befinden sich in der angegebenen INF-Datei.
Sie könnten also auch eine Kopie mit Ihren eigenen Einstellungen verwenden und so zum Beispiel einen größeren Rollout durchführen, oder sich einfach die tägliche Arbeit vereinfachen.

./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. Empfohlene Basiskonfiguration

Einen Großteil der Konfigurationsparameter von WebGate finden Sie in der Produkt-Konfigurationsdatei unter */etc/avira/avwebgate.conf*.

Nachfolgend finden Sie die von uns empfohlenen Einstellungen nach der Installation, sofern diese gewünscht sind:

3.1 HTTPPort: Port für die Überwachung von HTTP-Verbindungen

Beispiel: `HTTPPort 8080`

Dies lässt WebGate auf dem Port 8080 nach Anfragen scannen. Sofern hier bereits ein anderer Proxyserverdienst läuft, muss dieser Port entsprechend geändert werden.

3.2 FTPPort: Port für die Überwachung von FTP-Verbindungen

Beispiel: `FTPPort 2121`

Auf Wunsch bietet WebGate auch einen FTP Proxydienst an.
Sofern hier bereits ein anderer Proxyserverdienst läuft, muss dieser Port entsprechend geändert werden.

3.3 Quarantäneverzeichnis

Beispiel: `MoveConcerningFilesTo /home/quarantine`

Bei einem Fund wird die Datei in das Quarantäneverzeichnis verschoben und umbenannt. Dadurch ist die Datei einerseits für den User nicht mehr zugänglich, wird aber auch nicht z.B. im Falle eines False Positive gelöscht oder verändert.

3.4 Logdatei festlegen

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

Legt die Logdatei des OnAccess-Scanners fest. Standardmäßig wird in das Syslog geschrieben.

3.5 Qualität der Ausgabe definieren

```
LogLevel 4
```

Dies setzt einen mittleren LogLevel. Alarme (wie z.B. Virenfund), Fehlermeldungen (z.B. fehlerhafte ACL Konfiguration) und Warnungen (z.B. im Falle eines verschlüsselten Archives) werden protokolliert.

3.6 Heuristik auf Stufe Mittel aktivieren

```
HeuristicsLevel 2
```

Ein guter Mix zwischen Erkennung und Früherkennung. Dies verhindert eine Vielzahl möglicher False Positives.

3.7 Erkennung von Macroviren in Office-Dokumenten aktivieren

```
HeuristicsMacro yes
```

Wir empfehlen den Scan in Office-Dokumenten für eine bestmögliche Überwachung

4. Was kann zusätzlich konfiguriert werden?

Diese Einstellungen sollten vorher bedacht und nur optional bei Bedarf eingetragen werden! Die Werte müssen entsprechend angepasst werden.

4.1 Proxyeinstellungen

Die folgenden Proxyeinstellungen sind eventuell nötig um einen entsprechenden Proxyserver vor WebGate zu schalten.

```
HTTPProxyServer your.proxy

HTTPProxyPort 3128

HTTPProxyUsername username

HTTPProxyPassword password

FTPProxyServer your.proxy

FTPProxyPort 2121
```

4.2 Aktiviere ICAP Server

Dies aktiviert den ICAP Server von WebGate. Der Dienst läuft dann zusätzlich auf dem gewählten Port. Der ICAP Server unterstützt sowohl reqmod (Request modification) als auch respmod (Response modification).

Squid unterstützt ICAP 1.0 erst mit der Version 3.x!

```
ICAPPort 1344
```

4.3 Erlaube HTTPS Tunnel

WebGate blockt standardmäßig den HTTPS-Datenstrom damit dieser nicht gescannt werden kann.
Sofern Sie dennoch HTTPS-Seiten tunneln möchten, können Sie den folgenden Parameter setzen:

```
AllowHTTPSTunnel 1
```

4.4 Fortschrittsanzeige

Zeigt eine Seite im Browser an, welche bei größeren Downloads eine Fortschrittsanzeige ausgibt.
Zusätzlich muss ein Intervall in Sekunden festgelegt werden (z.B. 3), welches ein Refresh-Kommando an den Browser schickt.
Das Aktivieren und Konfigurieren der Fortschrittsanzeige erfolgt über einen einzelnen Parameter, der wie folgt definiert wird:

```
RefreshInterval 3
```

4.5 X-Header

Der folgende Parameter fügt den X-Header des Clients in der Anfrage hinzu, um nachgeschaltete Proxyserver über den tatsächlich anfragenden Client zu informieren:

```
AddXForwardedForHeader 1
```

4.6 Zugriffsberechtigter Adressraum

Dies legt die zugriffsberechtigen Clients bzw. Adressräume fest.
Unberechtigte Clients, die auf WebGate zugreifen möchten, werden blockiert:

```
AllowClientAddresses 127.0.0.1 192.168.0.0/16
```

5. Besonderheiten

5.1 Squid als Proxyserver

Dies sendet alle Anfragen vom Client an Squid durch WebGate. Dadurch wird die Nutzung der Squid-Proxyfunktionen ermöglicht.

Benötigte Einstellungen in der *squid.conf*:

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

acl ALL src all

never_direct allow ALL
```

5.2 ICAP Konfiguration

Durch das Starten des im Punkt 4.2 beschriebenen ICAP Servers kann Squid als ICAP-Client fungieren, um Anfragen zu verarbeiten.

Benötigte Einstellungen in der *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
```

Hinweis:
Wenn Sie Squid 3.0 oder eine frühere Version verwenden, müssen Sie folgende Parameter ändern:
adaption_service_set -> icap_class
adaption_access -> icap_class

6. Updatekonfiguration

Um Ihre AntiVir Installation auf dem aktuellen Stand zu halten, werden zwei Arten von Updates bei der Installation eingerichtet:

- Scannerupdate (nur Scanner & Engine & VDF)
- Produktupdate (Guard Programmdateien)

Dies kann im Allgemeinen sehr interessant für Sie sein, wenn Sie Programmupdates als besonders sensibel betrachten. Dadurch erhalten Sie die Möglichkeit auf einem separaten Testsystem zunächst einen Audit durchzuführen, bevor Sie die neue Version produktiv einsetzen.

Die Einstellungen für das Update finden Sie nach der Installation in folgender Datei:

/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 Sinnvolle Werte für ein Update

Je nach Zielgruppe empfehlen wir unseren Kunden mindestens 2-3 mal am Tag ein Update durchzuführen.

6.1.1 Mittlere und große Unternehmen

Beispiel: jede Stunde

/etc/cron.d/avira_updater:

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

6.1.2 Kleine Unternehmen

Beispiel: alle 3 Stunden

/etc/cron.d/avira_updater:

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

6.1.3 Kunden mit Schmalband-Anschlüssen (Modem/ISDN):

Beispiel: alle 8 Stunden

/etc/cron.d/avira_updater:

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

6.1.4 Internet Service Provider

Für Internet Service Provider empfiehlt es sich natürlich, deutlich öfter nach neuen

Signaturen zu schauen. Daher sollte die Frequentierung der Updateaufrufe deutlich höher angelegt sein, z.B. alle 15 Minuten. So ist sichergestellt, dass Sie immer zeitnah die neuesten Signaturen einsetzen.
/etc/cron.d/avira_updater:

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

7. WebGate Suite Feature

Mit dem WebGate Suite Feature ist es möglich, bestimmte Kategorien von Webseiten zu blockieren.
Dazu gehören u.a. Pornografie, Phishing, Malware und Betrug.

Es existieren folgende Filterkategorien:

Nummer	Kategorie
0	Pornographie
1	Erotik/Sex
2	Badekleidung/Unterwäsche
3	Shopping
4	Auktionen/Kleinanzeigen
5	Behörden
6	Nichtregierungsorganisationen
7	Städte/Regionen/Länder
8	Bildung/Erziehung
9	Politische Parteien
10	Religion
11	Sekten
12	Rechtswidrige Handlungen

13	Computerkriminalität
14	Extreme politische Gruppierungen/Hassreden/Diskriminierung
15	Warez/Hacking/Illegale Software
16	Gewalt/Grausamkeit
17	Glücksspiel/Lotterie
18	Computerspiele
19	Spielzeug
20	Kino/Fernsehen
21	Freizeiteinrichtungen/Vergnügen/Themenparks
22	Kunst/Museen/Mahnmale/Denkmäler
23	Musik
24	Literatur/Bücher
25	Humor/Comics
26	Nachrichten/Zeitungen/Zeitschriften
27	Web-Mail
28	Chat
29	Newsgroups/Foren/Blogs
30	Mobilfunk
31	Digitale Postkarten
32	Suchmaschinen/Webkataloge/Portale
33	Software/Hardware/Händler
34	Kommunikationsdienste
35	IT-Sicherheit/IT-Informationen
36	Webseitenübersetzung
37	Anonyme Proxies

38	Illegale Drogen
39	Alkohol
40	Tabak
41	Selbsthilfe/Sucht
42	Dating-Agenturen/Partnervermittlungen
43	Restaurants/Bars
44	Reise
45	Mode/Kosmetik/Schmuck
46	Sport
47	Immobilien/Wohnen/Architektur/Möbel
48	Natur/Umwelt/Tiere
49	Persönliche Homepages
50	Stellensuche
51	Börsenmakler/Aktien
52	Finanzdienstleistungen/Investment/Versicherungen
53	Banken/Home-Banking
54	Fahrzeuge/Verkehrswesen
55	Waffen/Militär
56	Gesundheit
57	Schwangerschaftsabbruch
59	Spam-URLs
60	Malware
61	Phishing-URLs
62	Instant Messaging
63	Betrug

66 Wirtschaft allgemein

73 Bannerwerbung

76 Soziale Netzwerke
77 Business Networking

78 Soziale Medien

79 Web-Speicher

Die entsprechenden Parameter können Sie in der */etc/avira/avwebgate.conf* anlegen, um bestimmte Kategorien zu blockieren.

Folgendes Beispiel blockiert Seiten der Kategorien Pornographie (0) bis Badekleidung/Unterwäsche (2), rechtswidrige Handlungen (12), extreme politische Gruppierungen/Hassreden/Diskriminierung (14), sowie Phishing-URLs (61):

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

Weitere Informationen und Einstellungsmöglichkeiten von AntiVir WebGate (Suite) finden Sie im Benutzerhandbuch oder in unserer Wissensdatenbank unter

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

Ausgabe Q3-2012

AVIRA

live *free.*™

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

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de